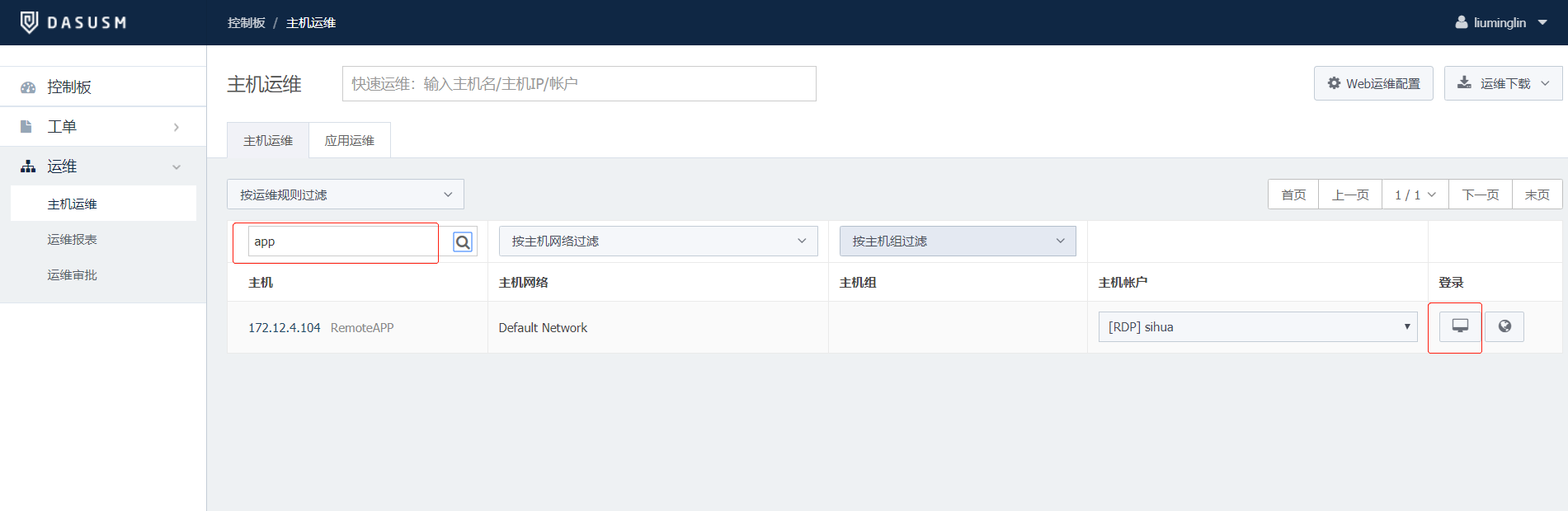
1. 把本地镜像上传到跳板机
2. 登录堡垒机：<https://172.12.0.1/index.php/om/omapp>

点主机运维→web运维工具

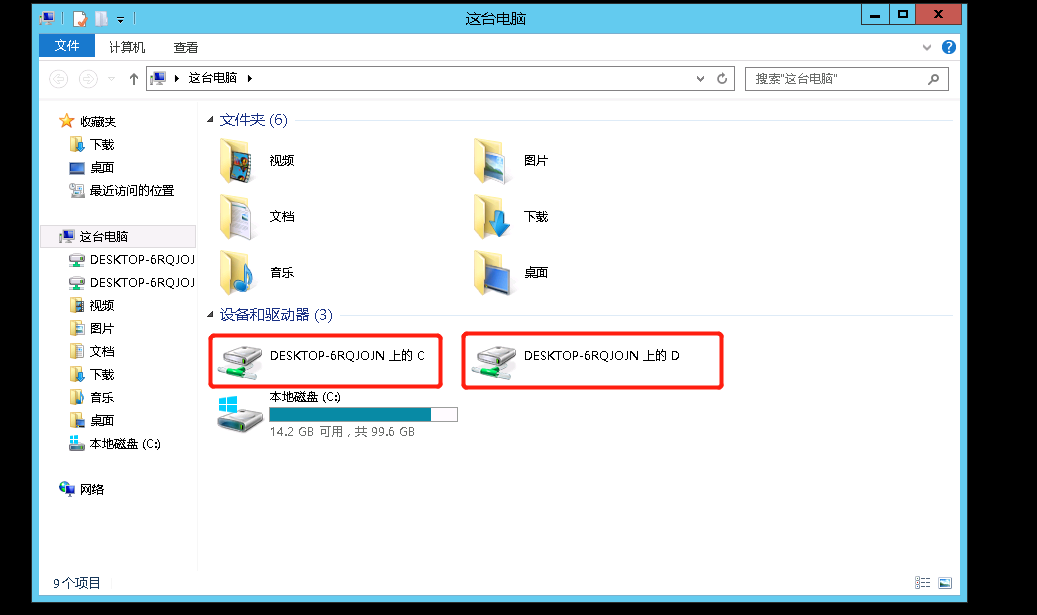


1. 点击主机运维搜索App

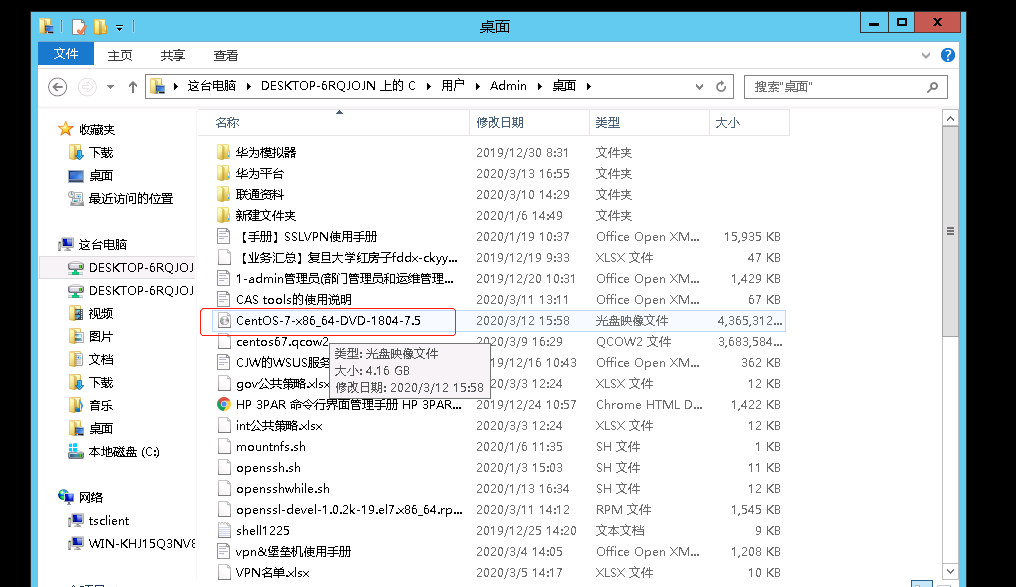


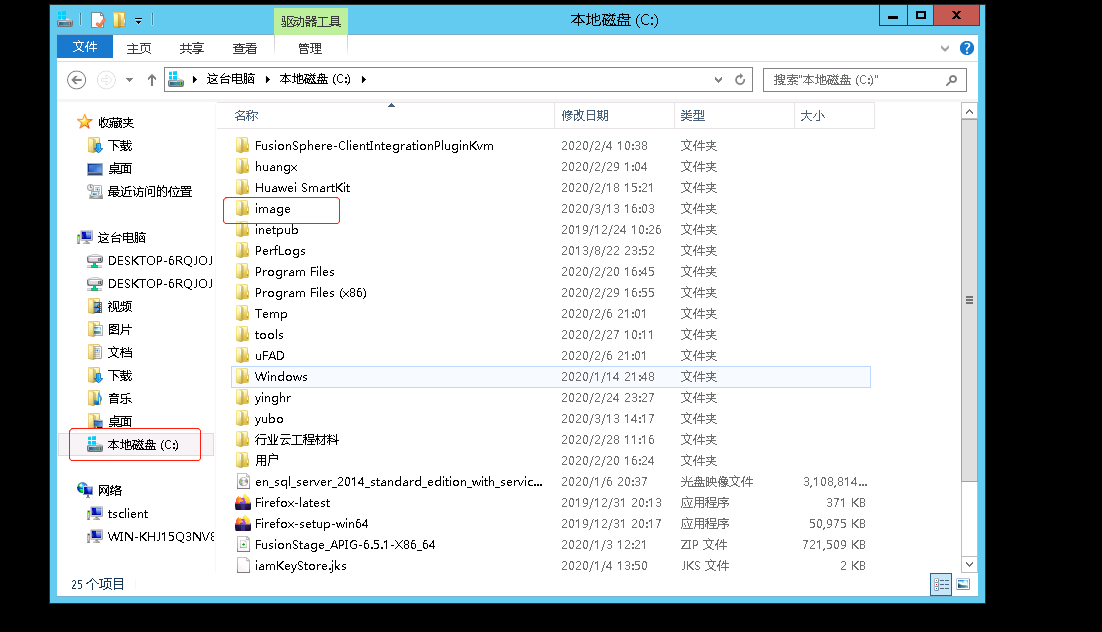


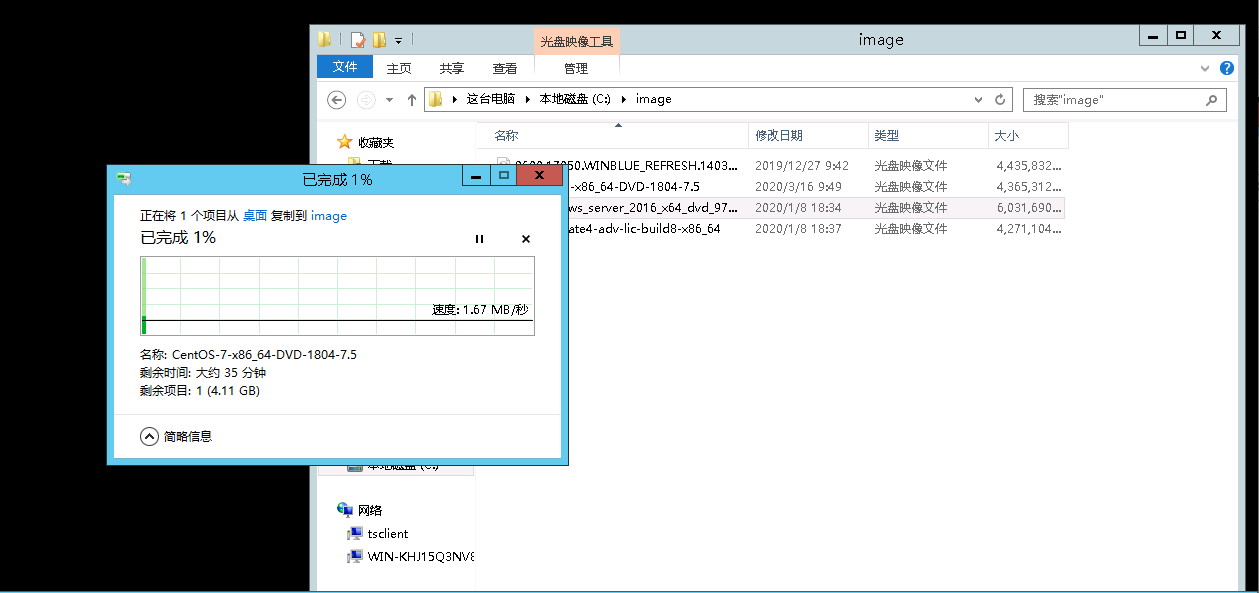
1. 打开可以看到本地的盘符



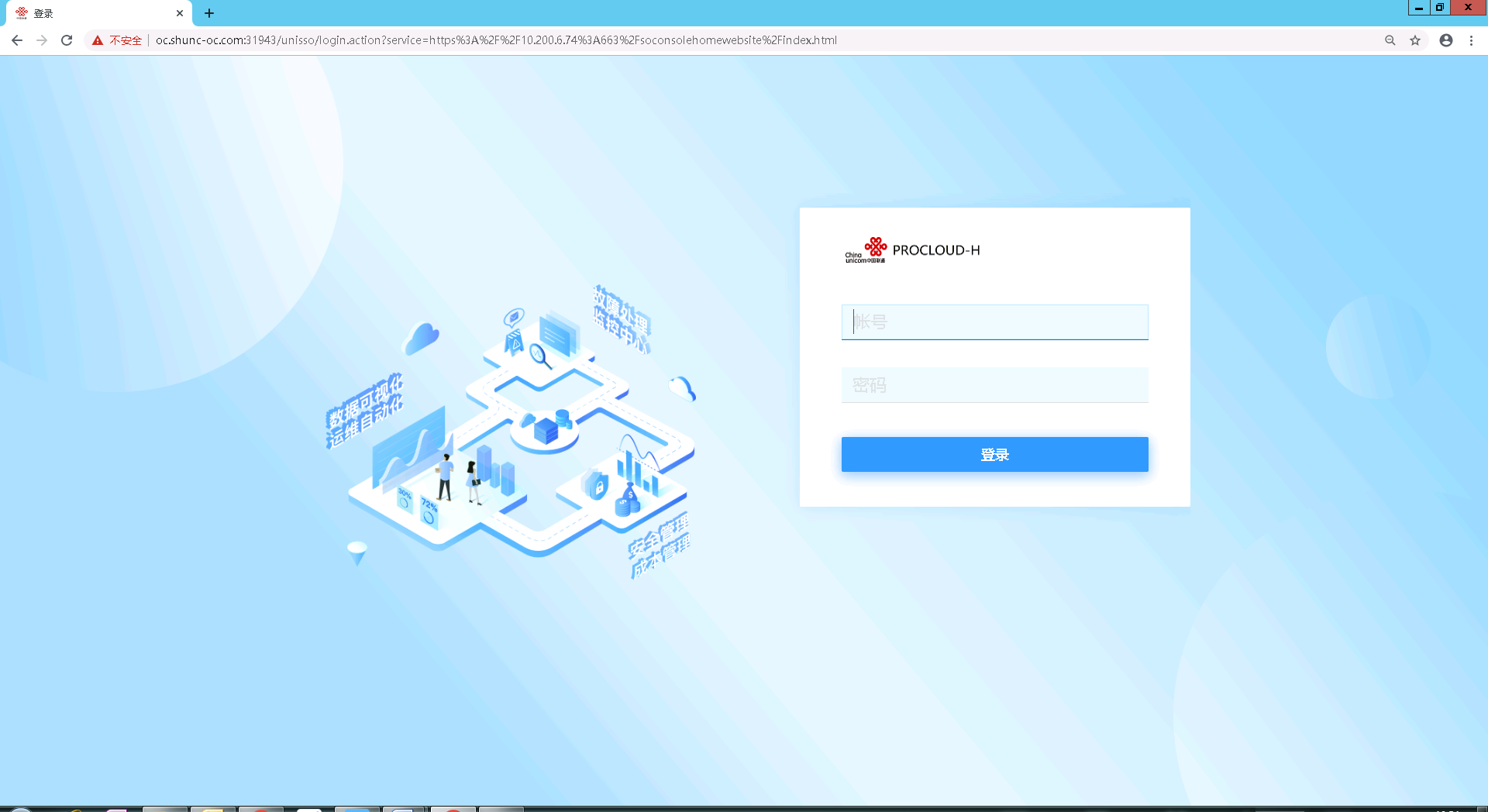
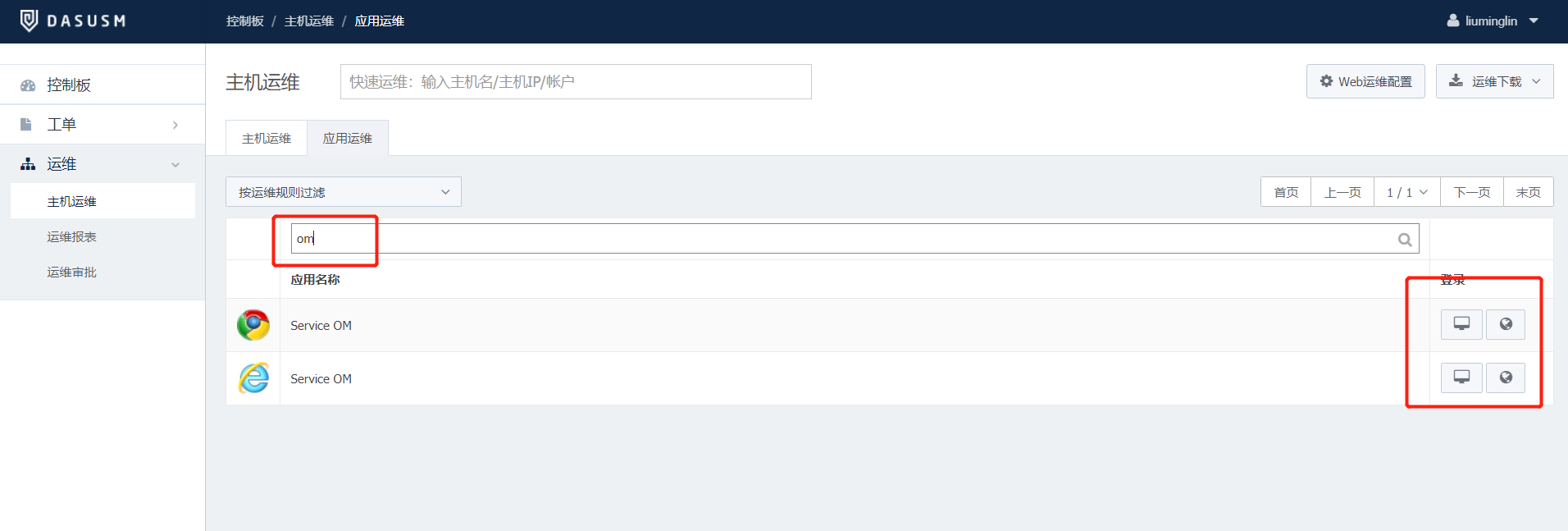
1. 找到要上传的镜像并复制



1. 进入C盘并找到image文件目录进入
2. 将复制的镜像放在image目录里



1. 登录OM用户密码：admin/Huawei12#$

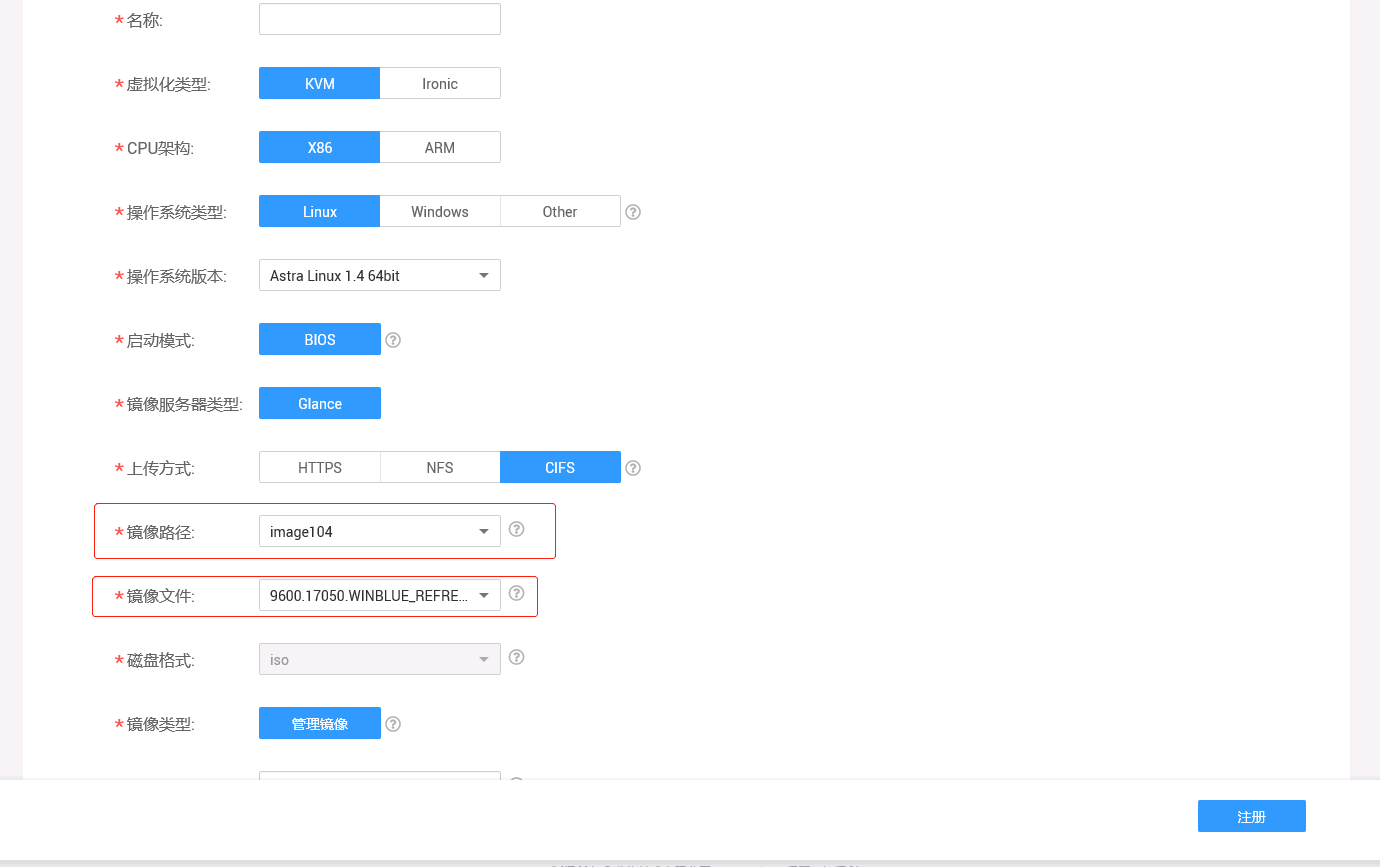


1.选被级联层，点击管理镜像点注册镜像

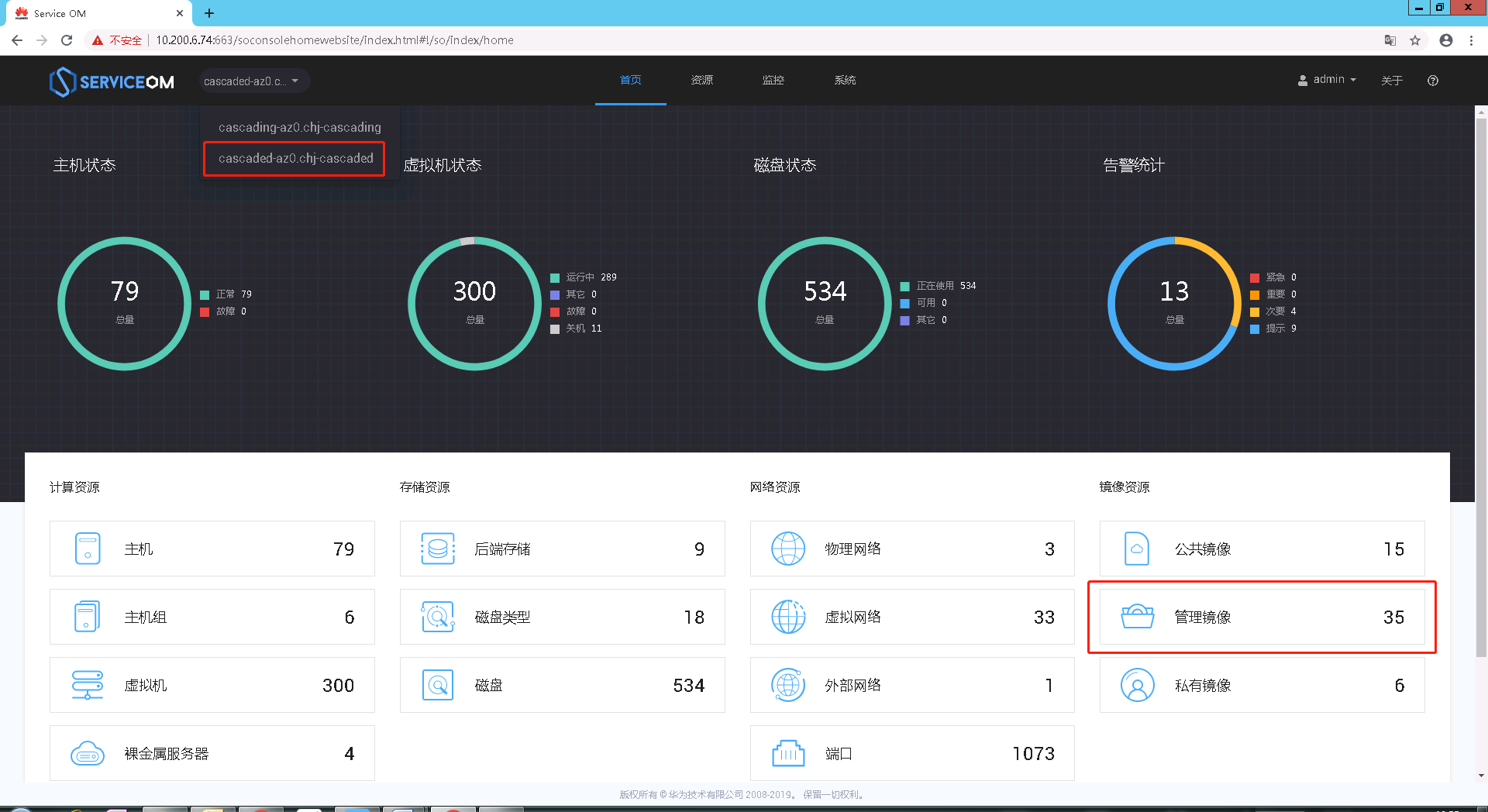


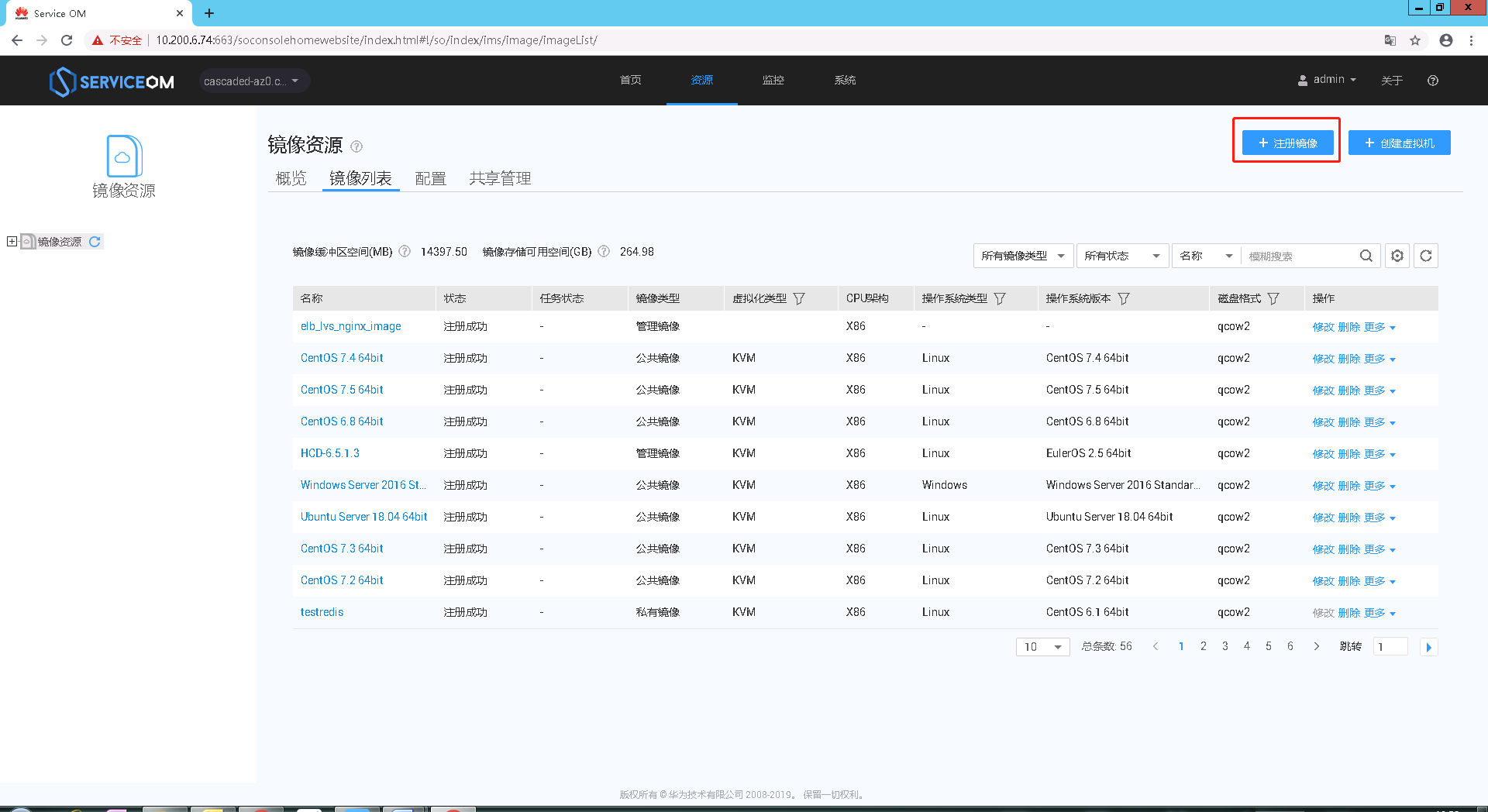


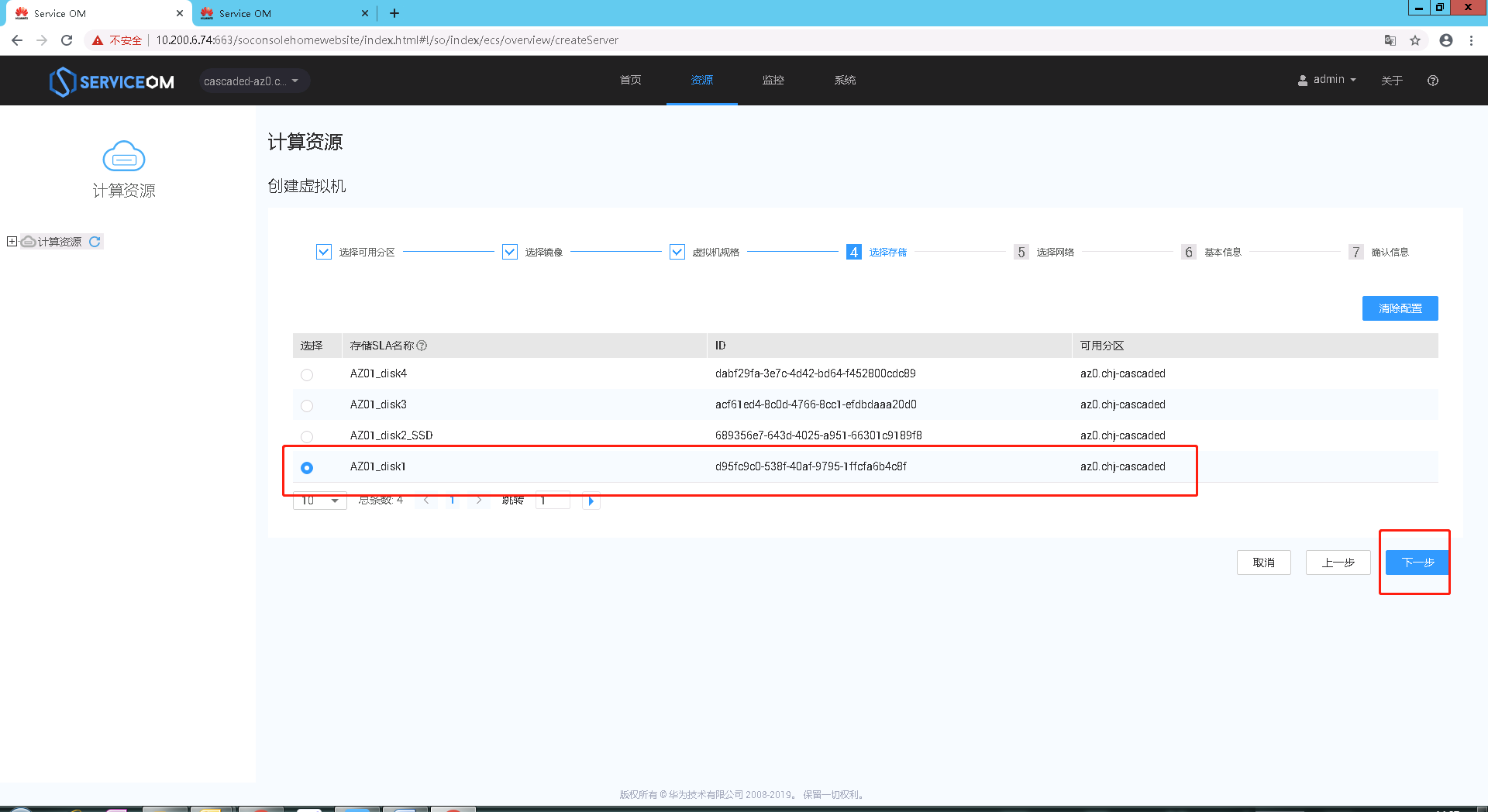
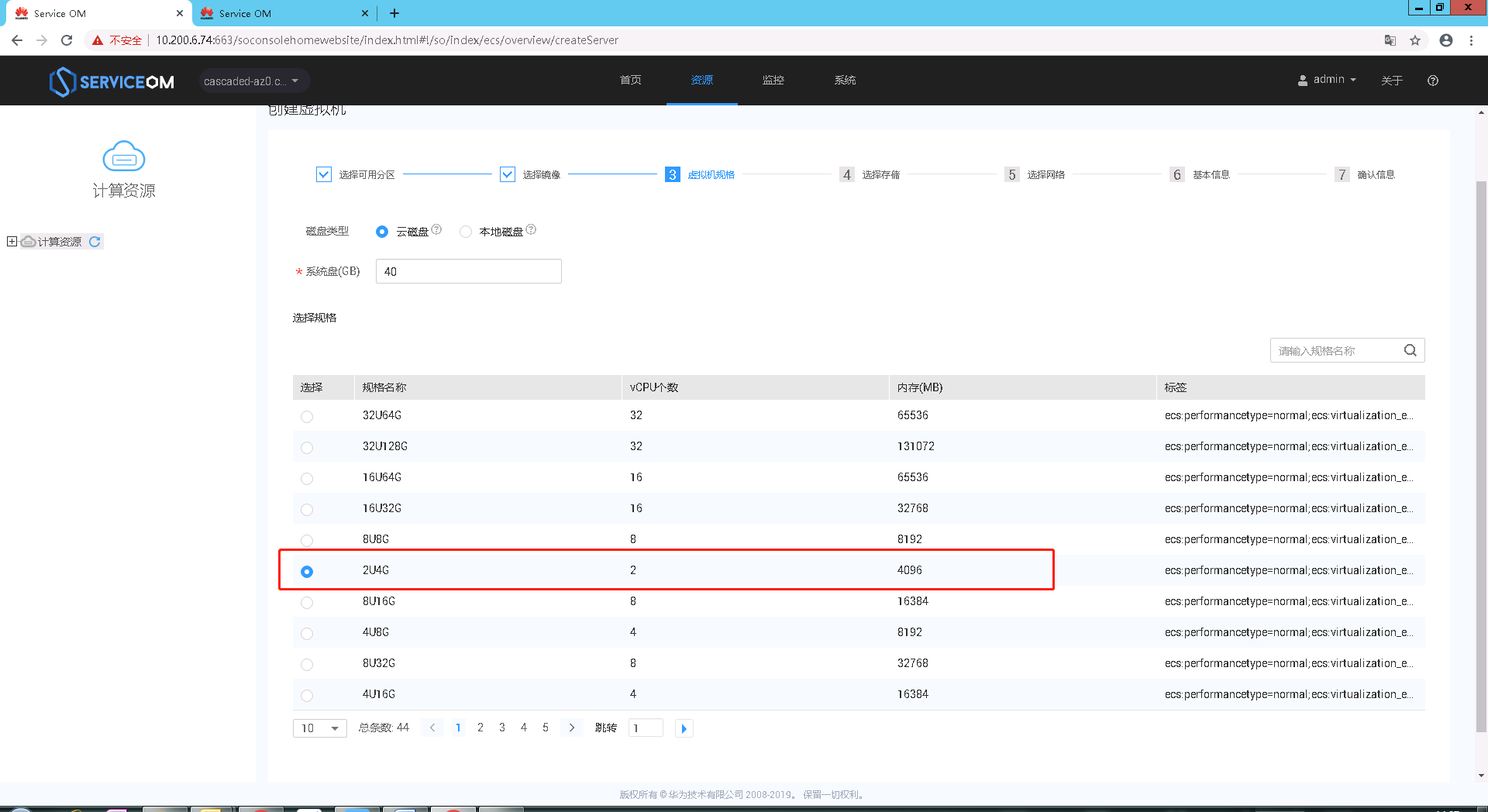
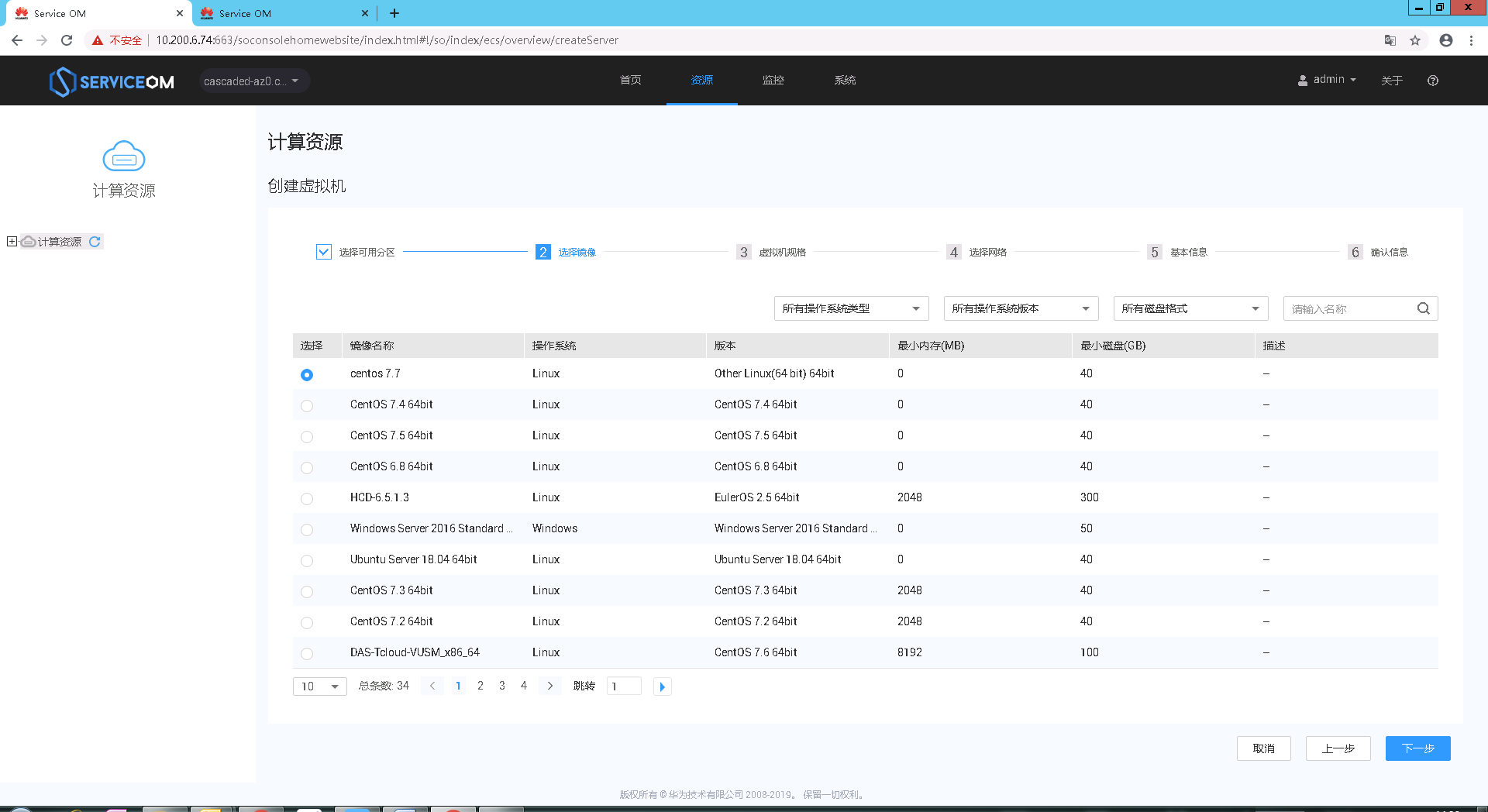
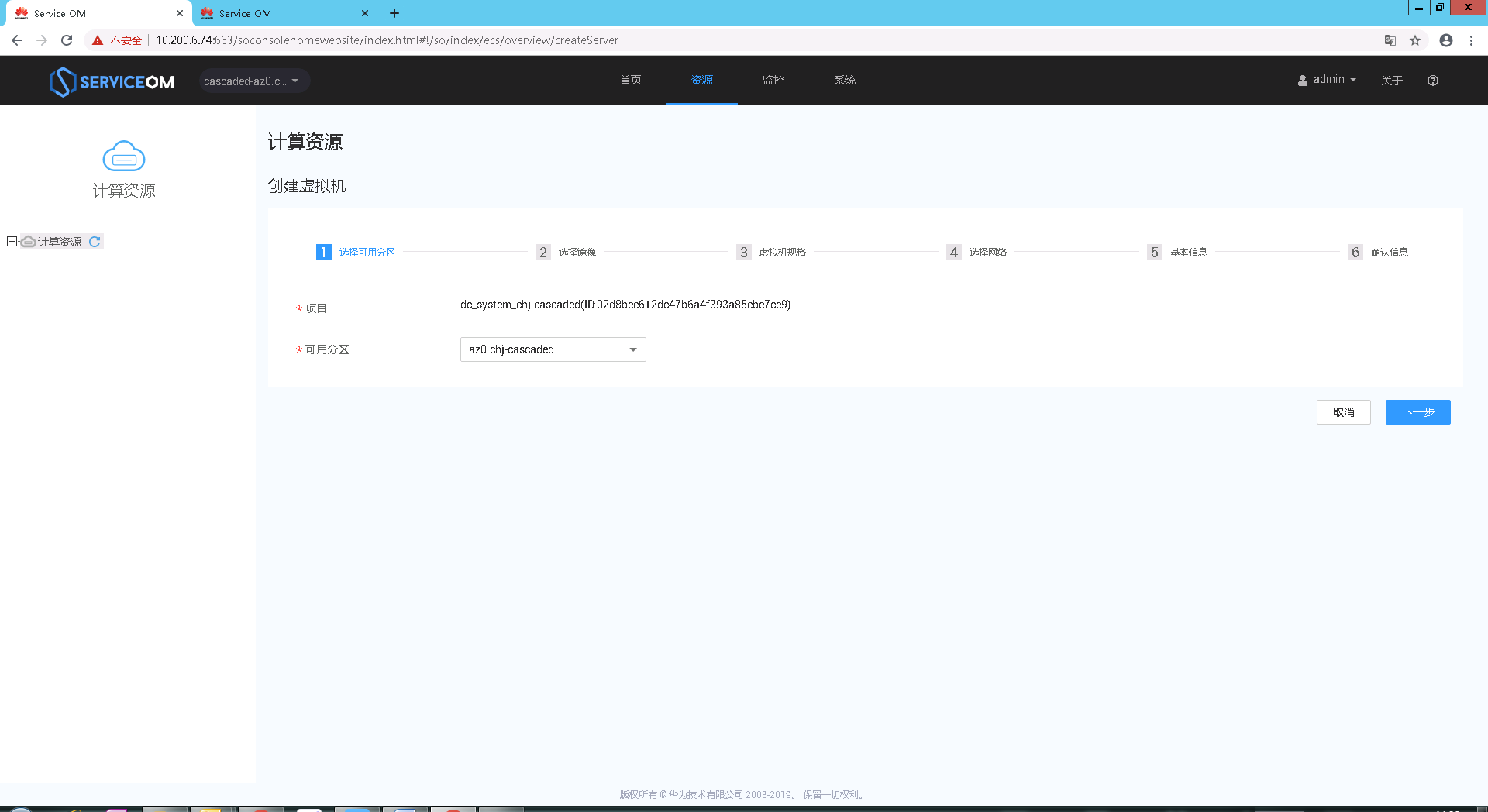
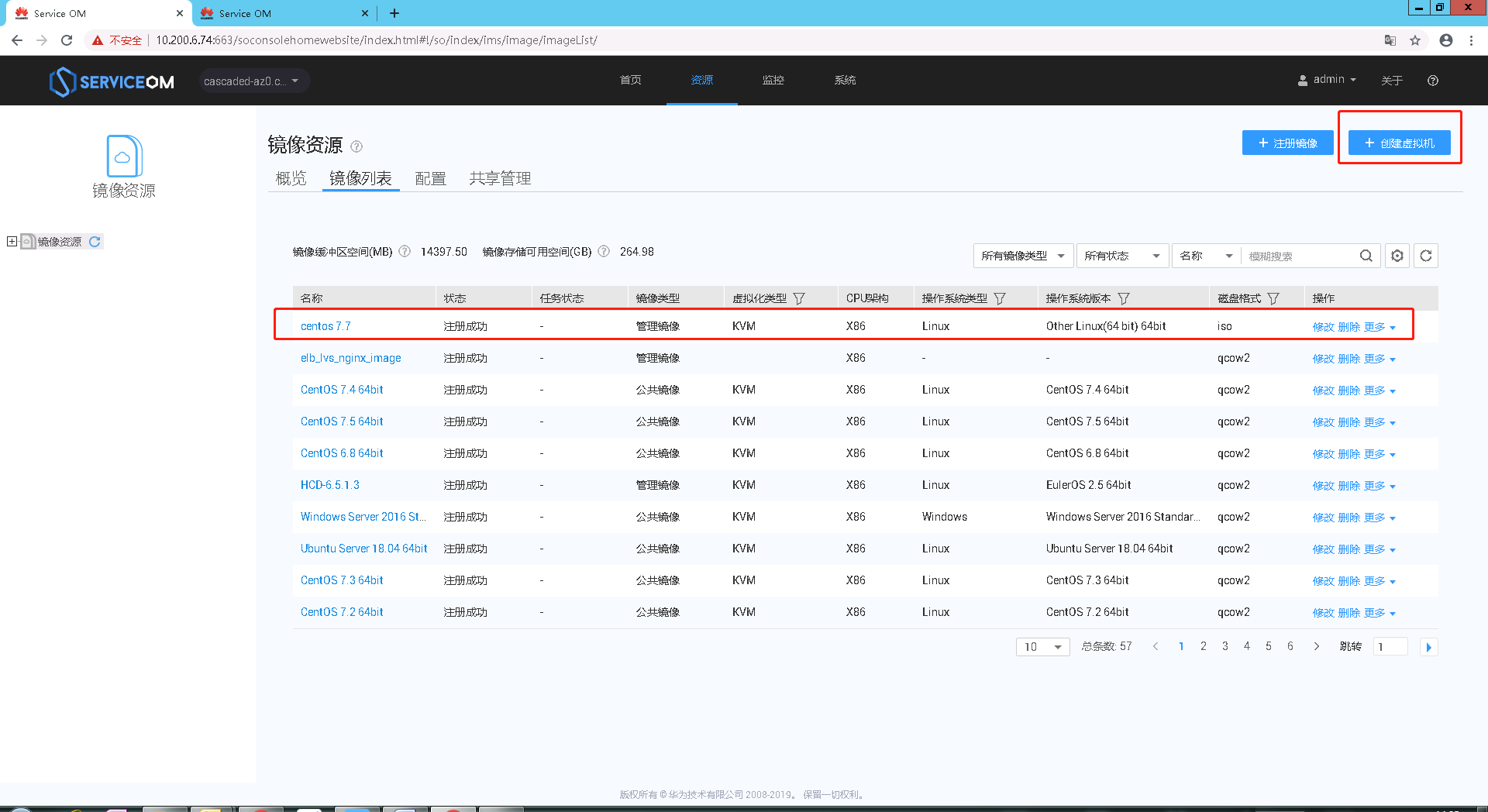
2.上传ISO，操作系统版本选择要上传的系统版本，镜像镜像路径选image104,镜像文件选自己需要上传的镜像，最小磁盘：Linux40G /Windows50G

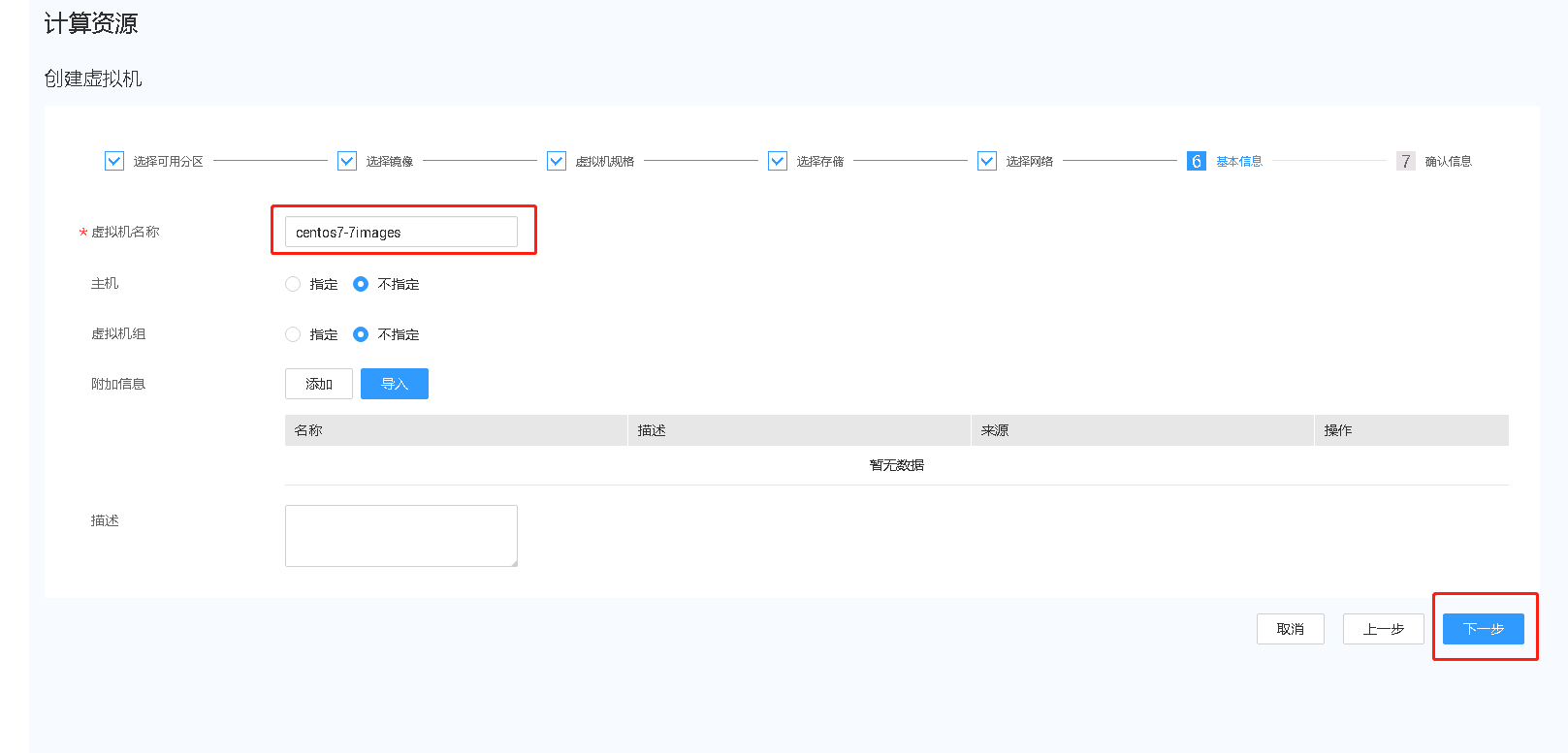
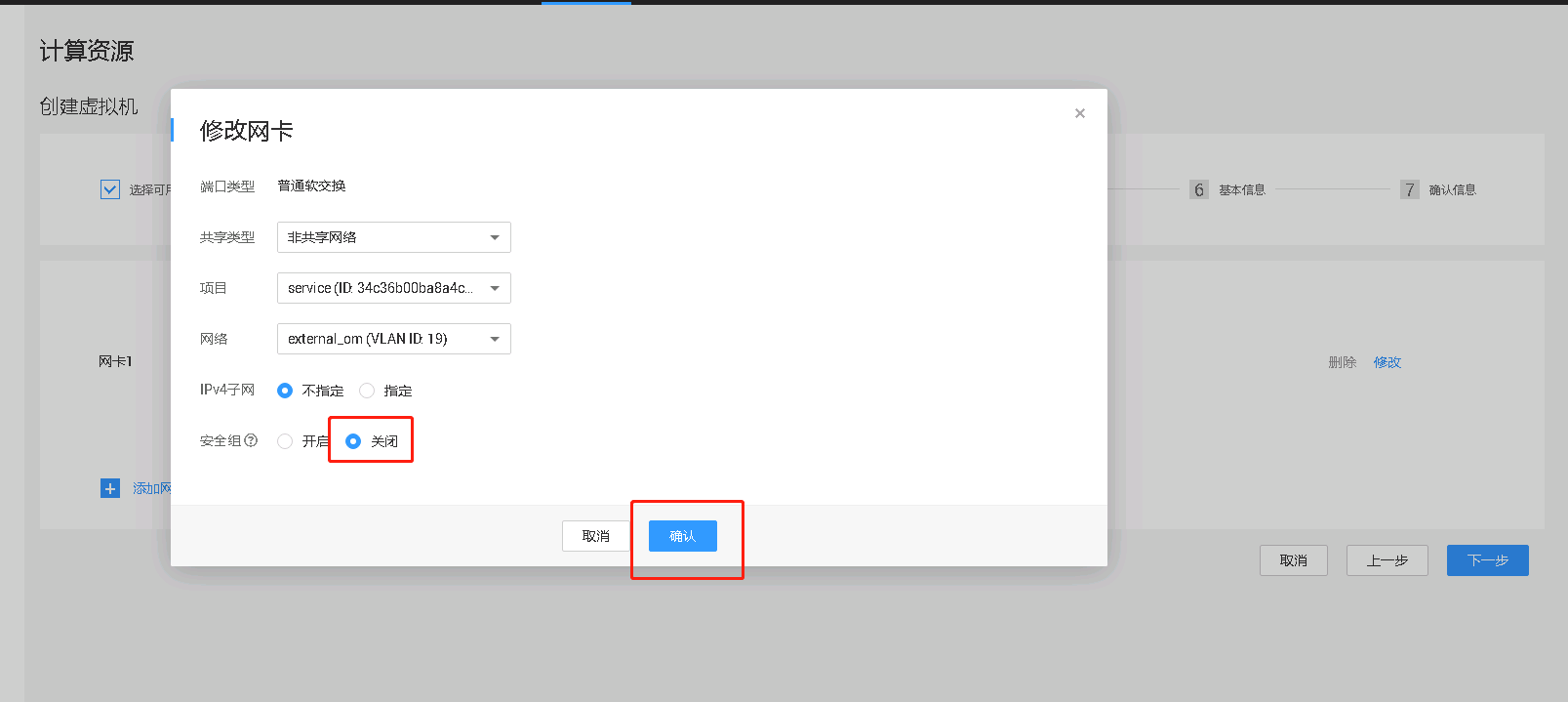


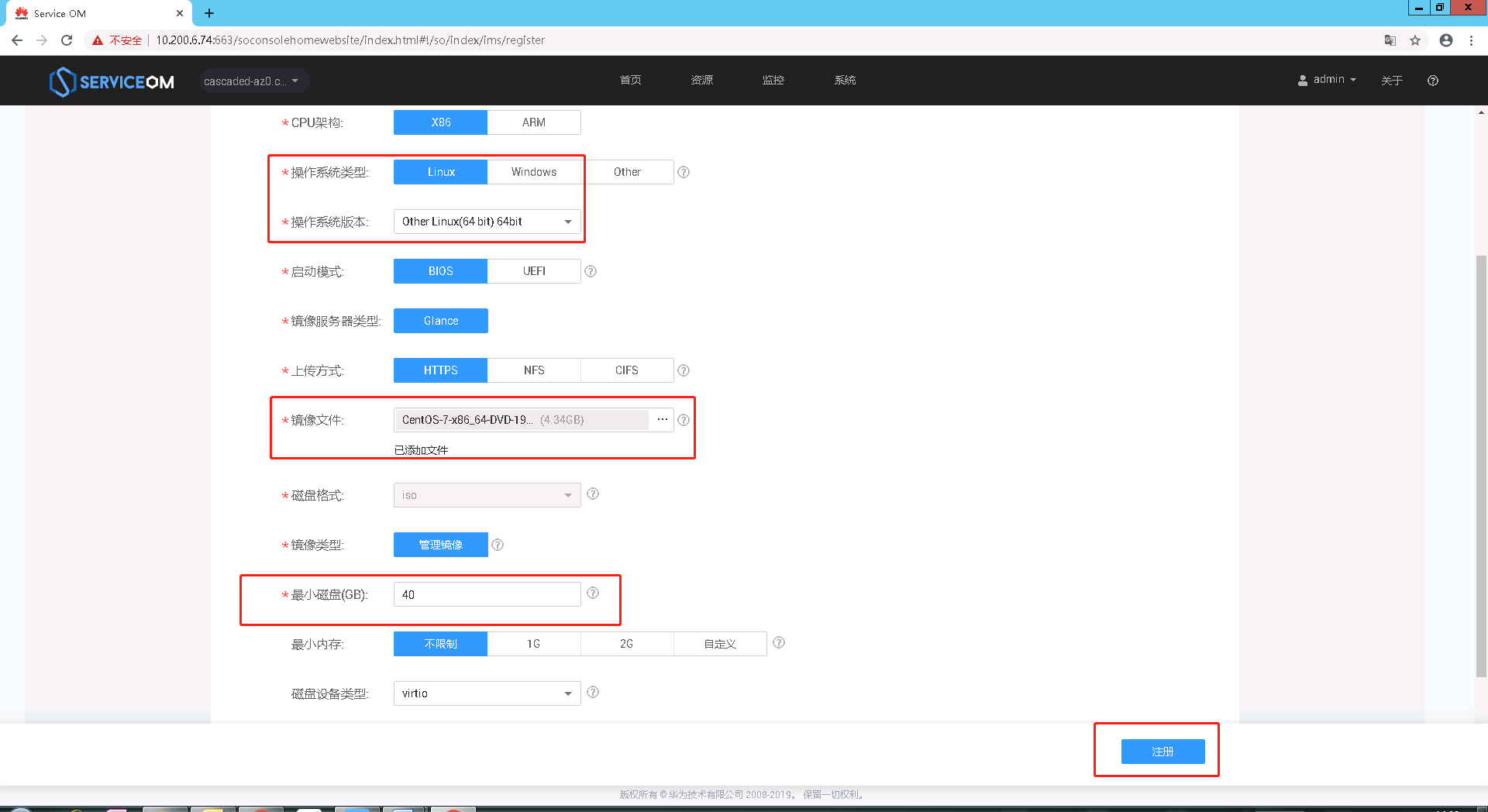
2、选择被级联层，点击管理镜像



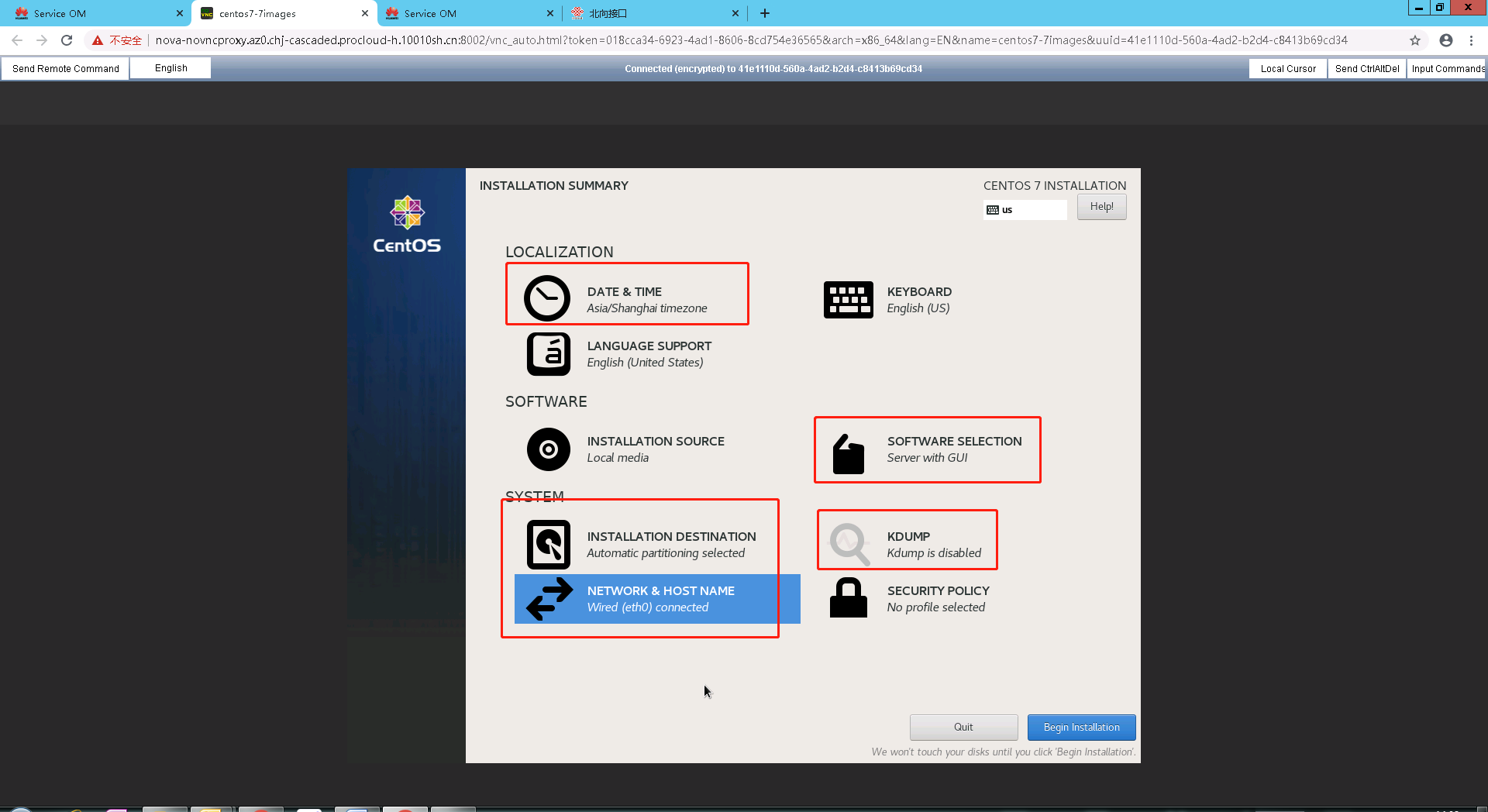
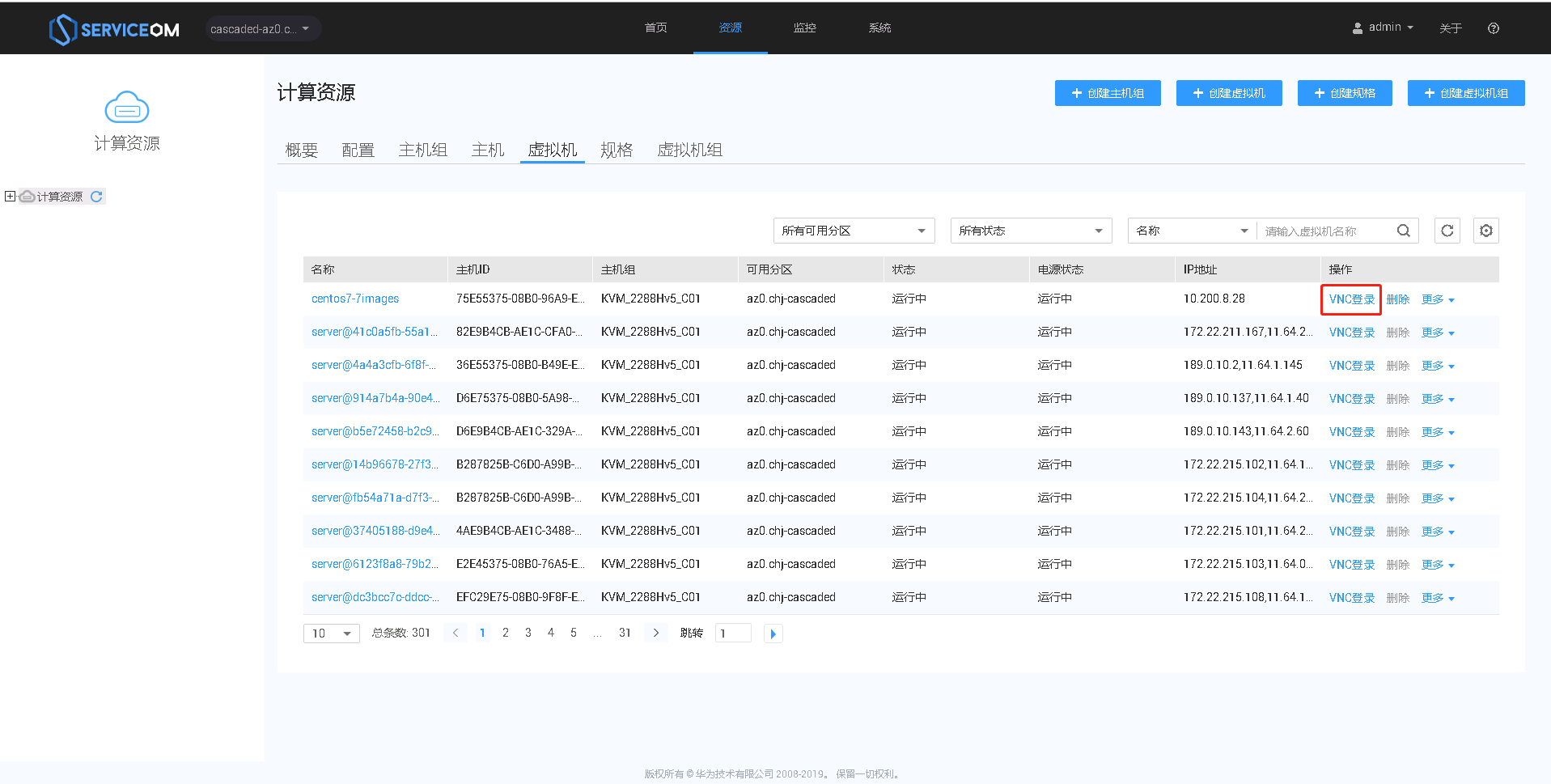


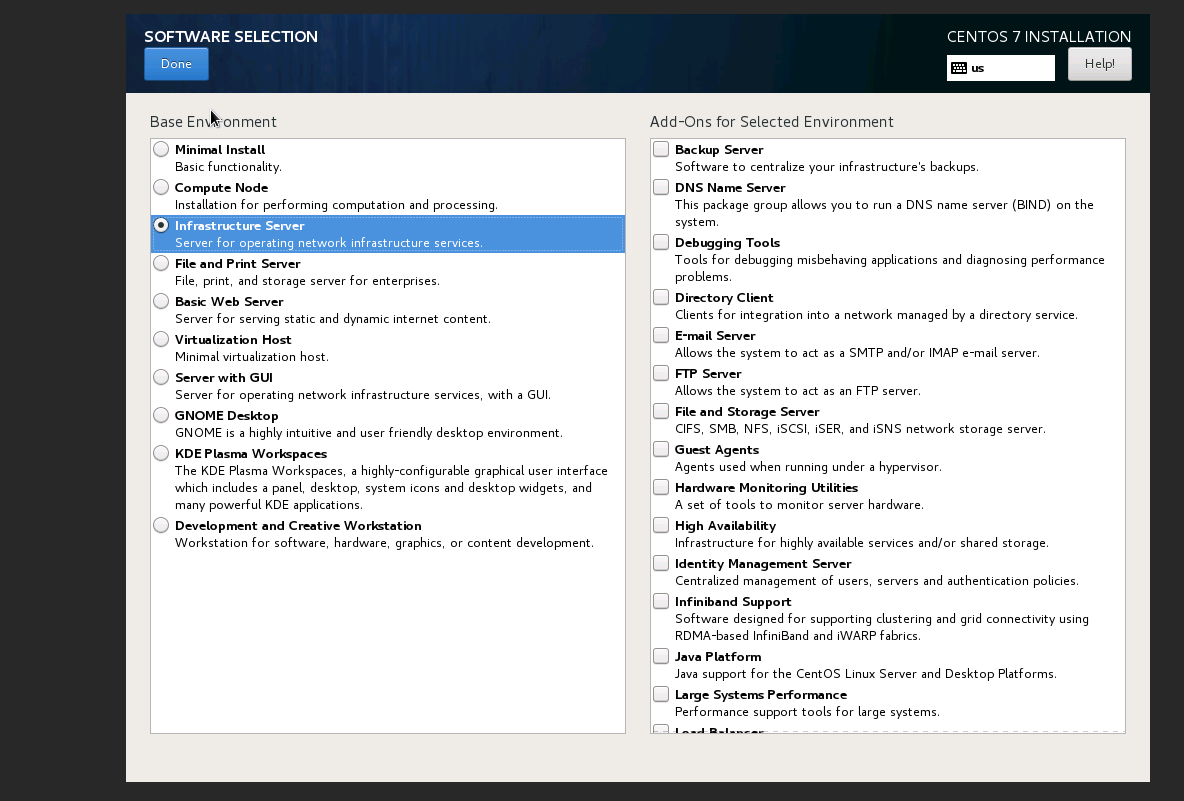






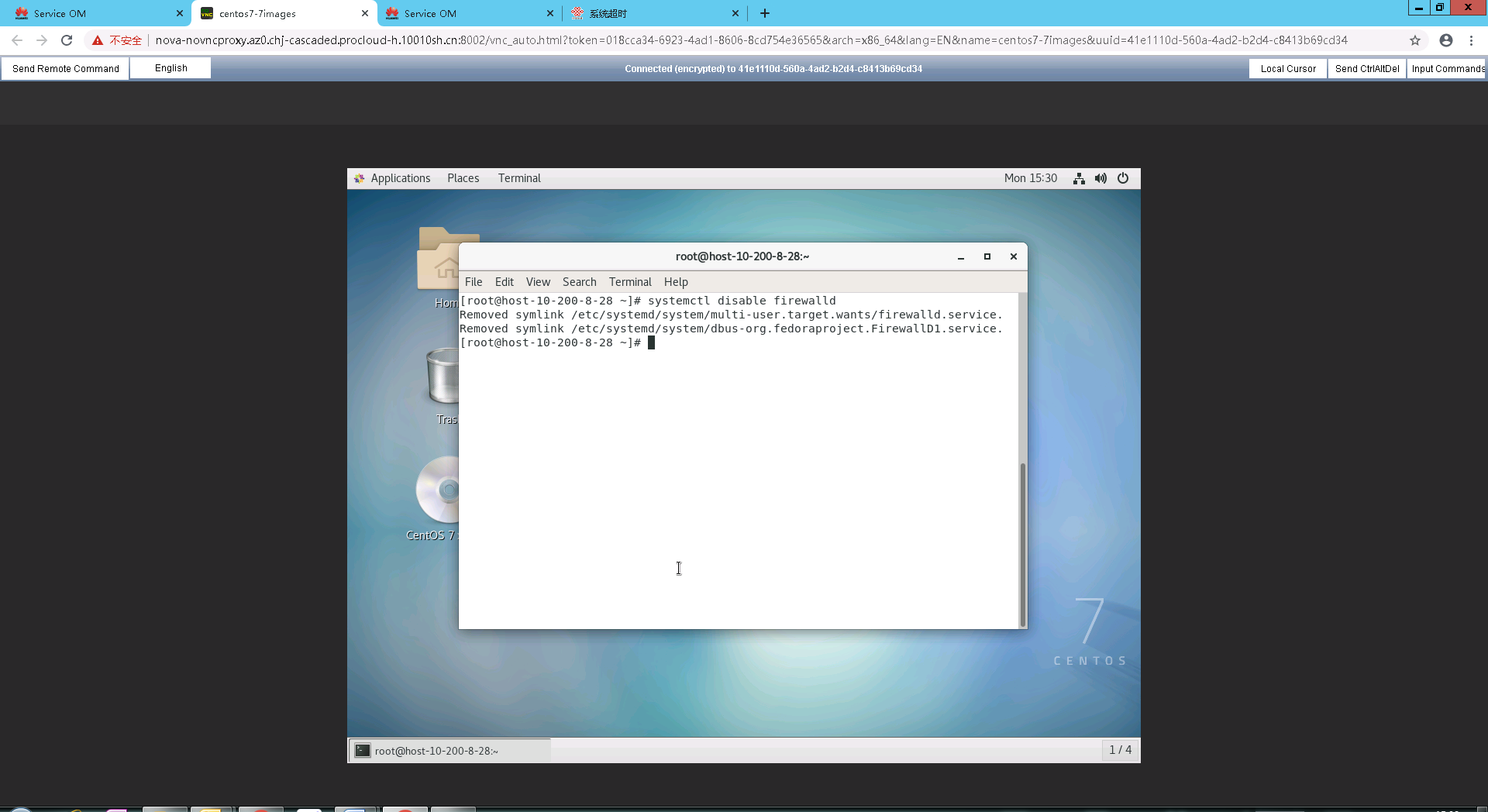
## 安装操作系统

1. 点击vnc登录，安装操作系统

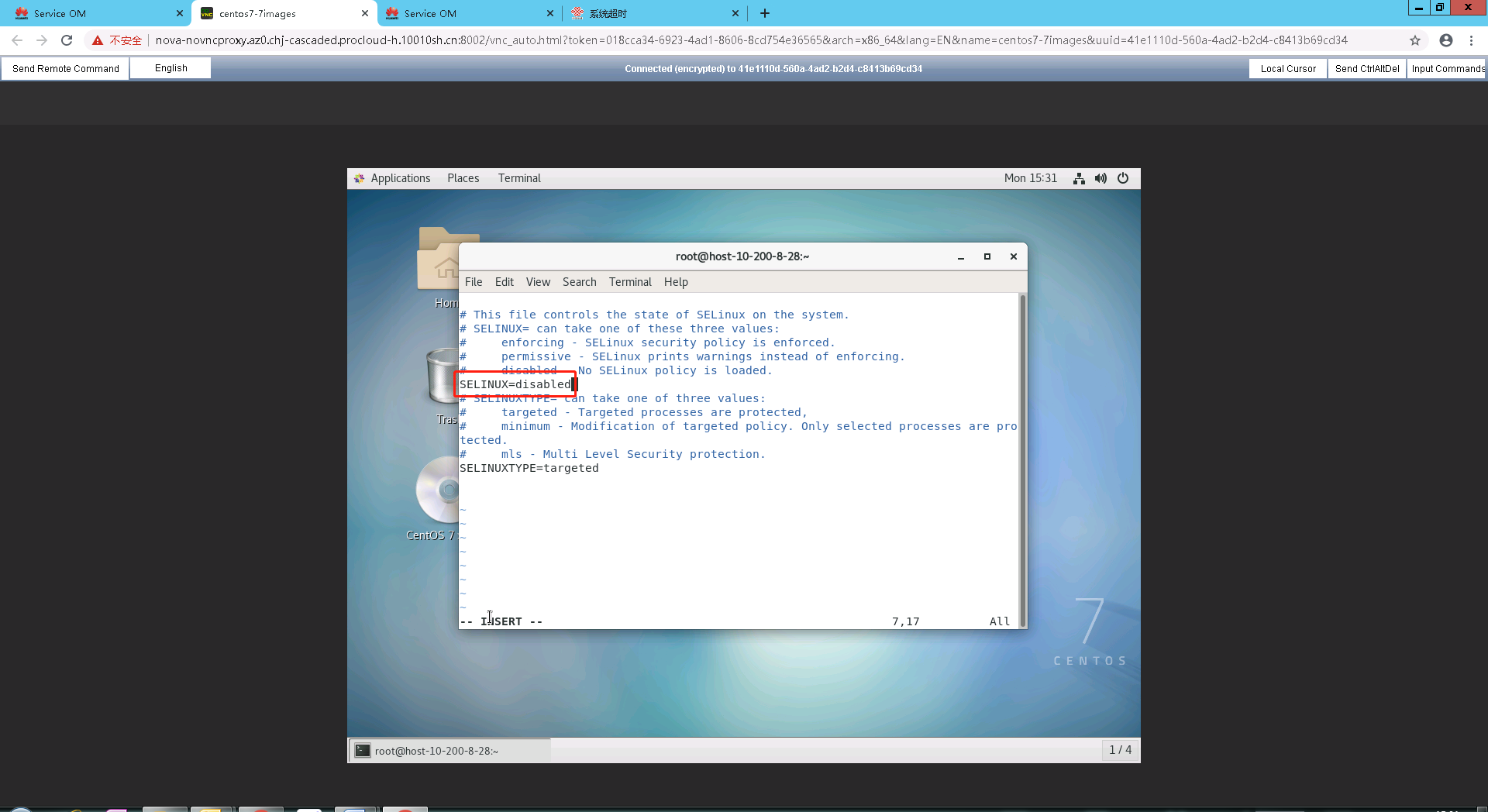


1. 镜像安装时统计将普通用户密码设置为guest/9ol.)P:?，root密码设置为ShUnc@123

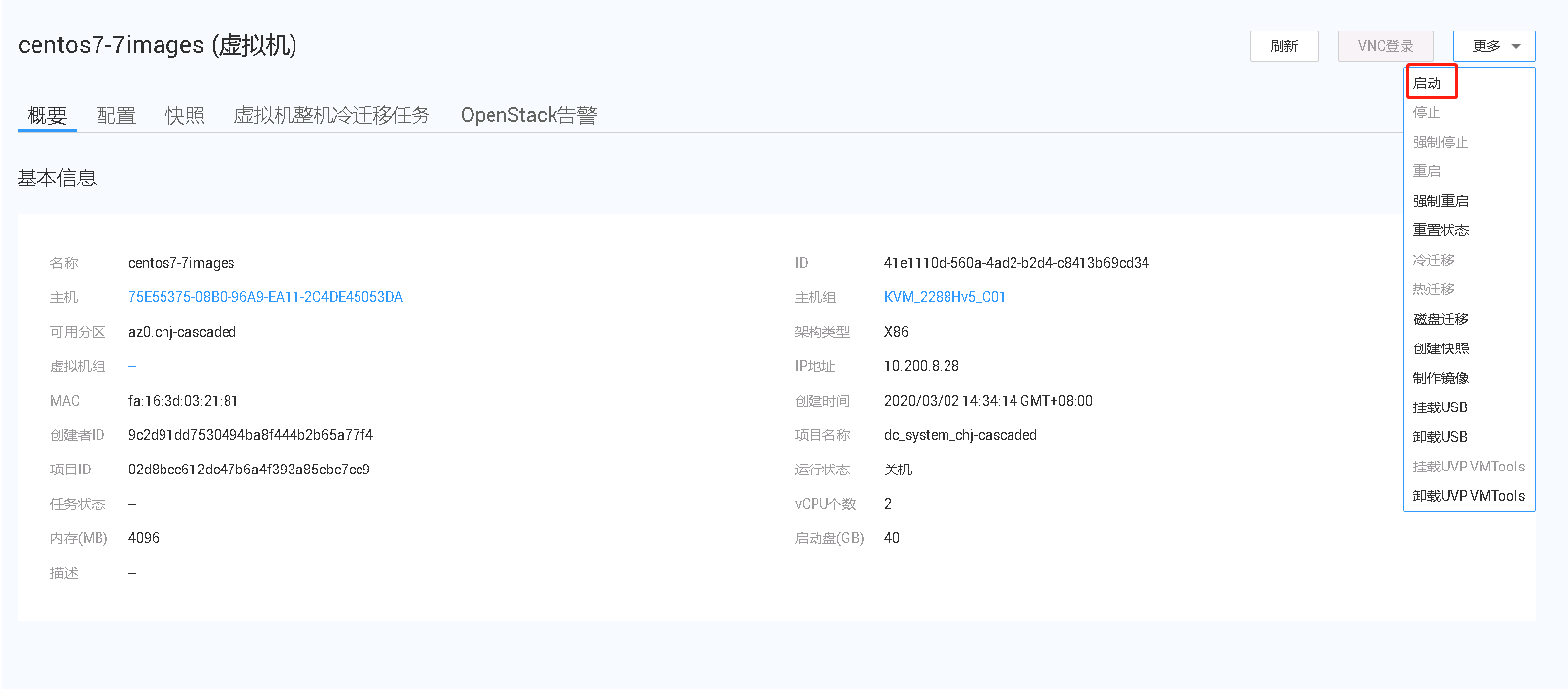
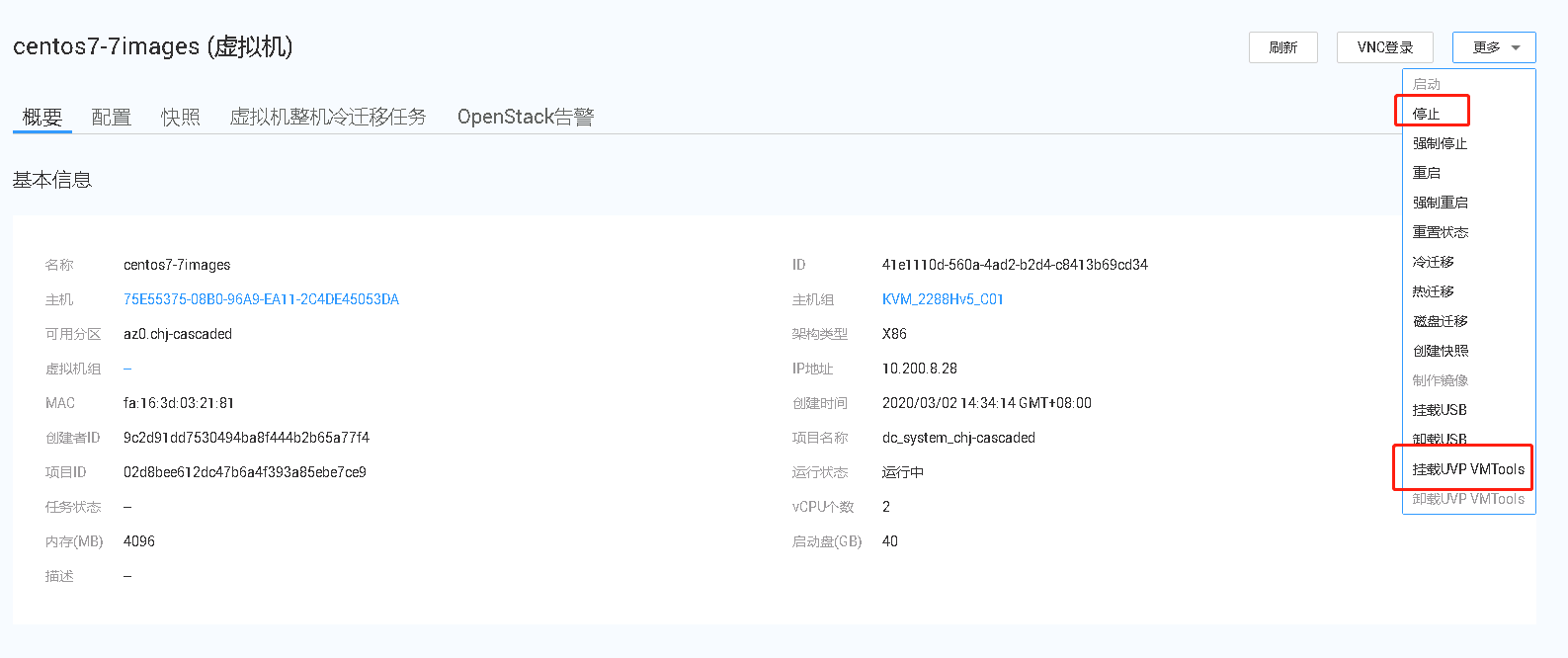
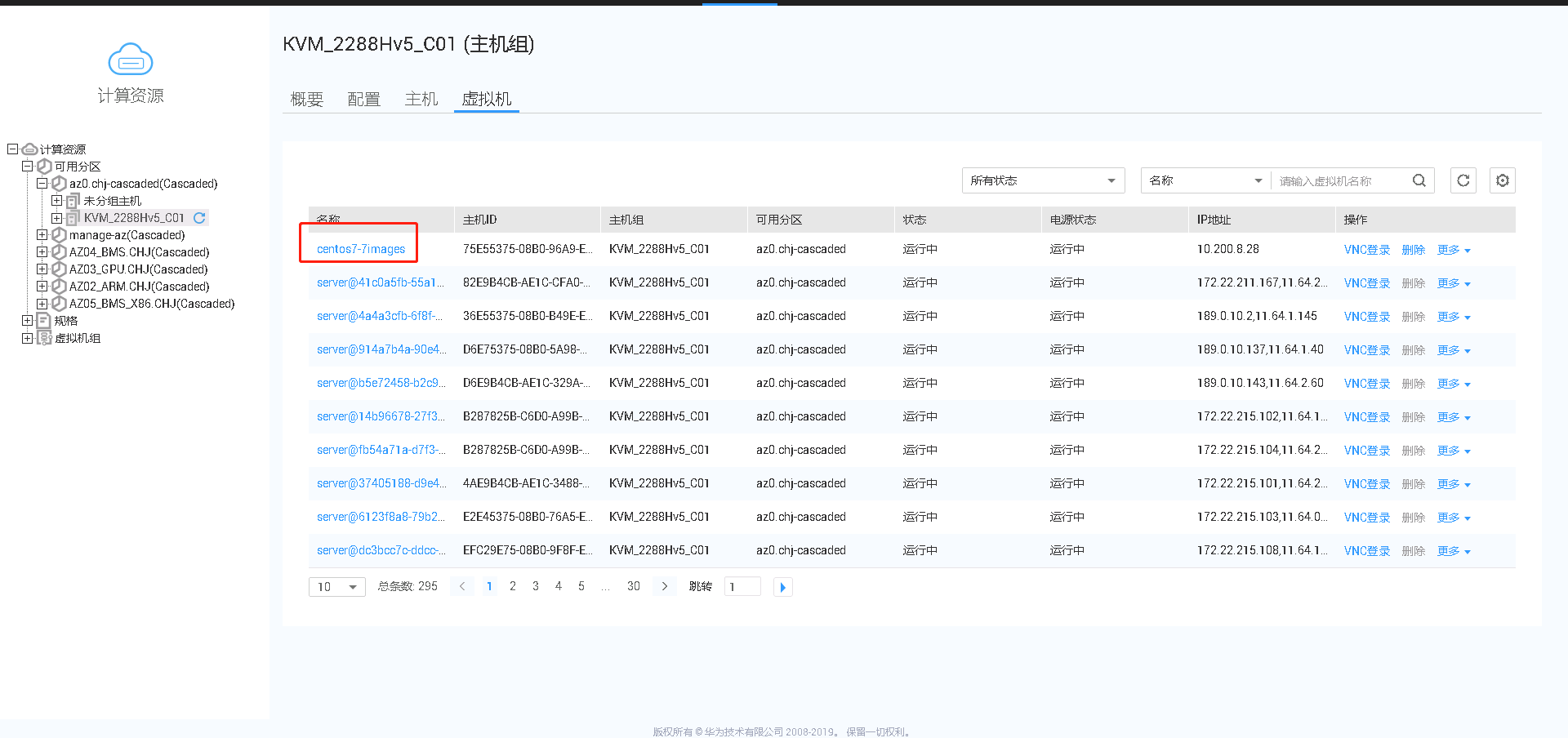
3、关闭系统防火墙



4、关闭系统selinux



5、挂载uvp vmtools



6、修改网卡配置文件

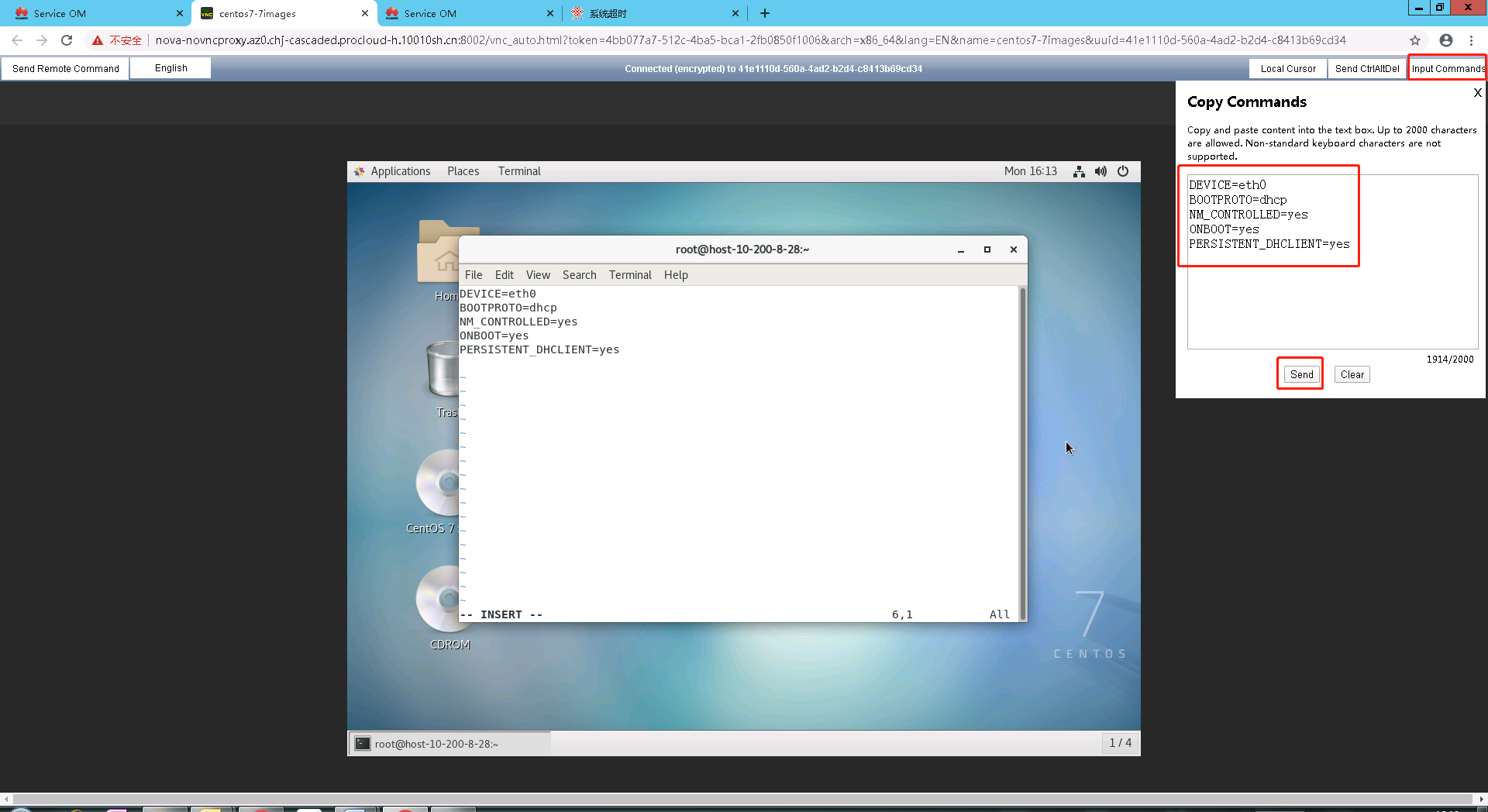
DEVICE=eth0

BOOTPROTO=dhcp

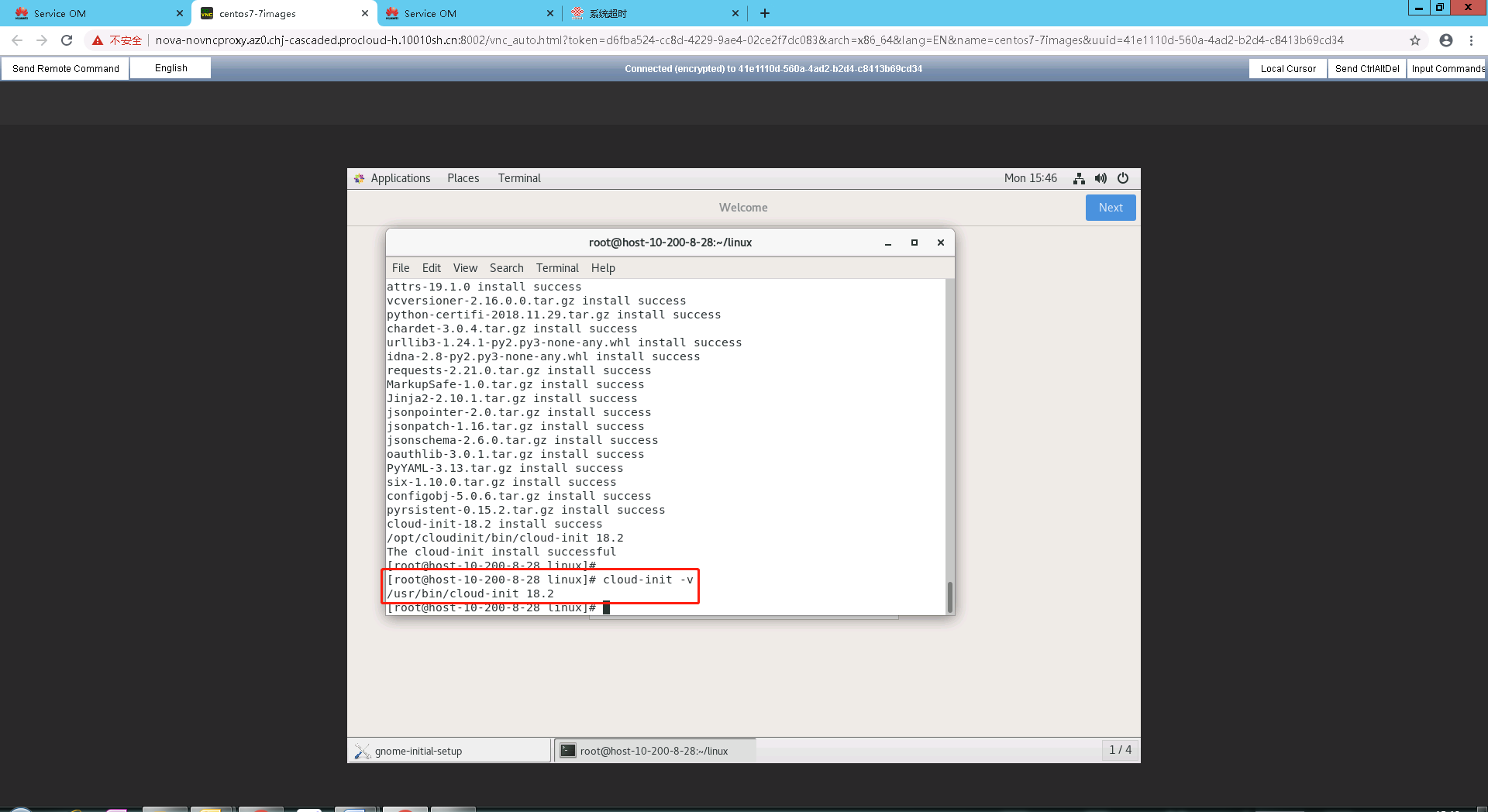
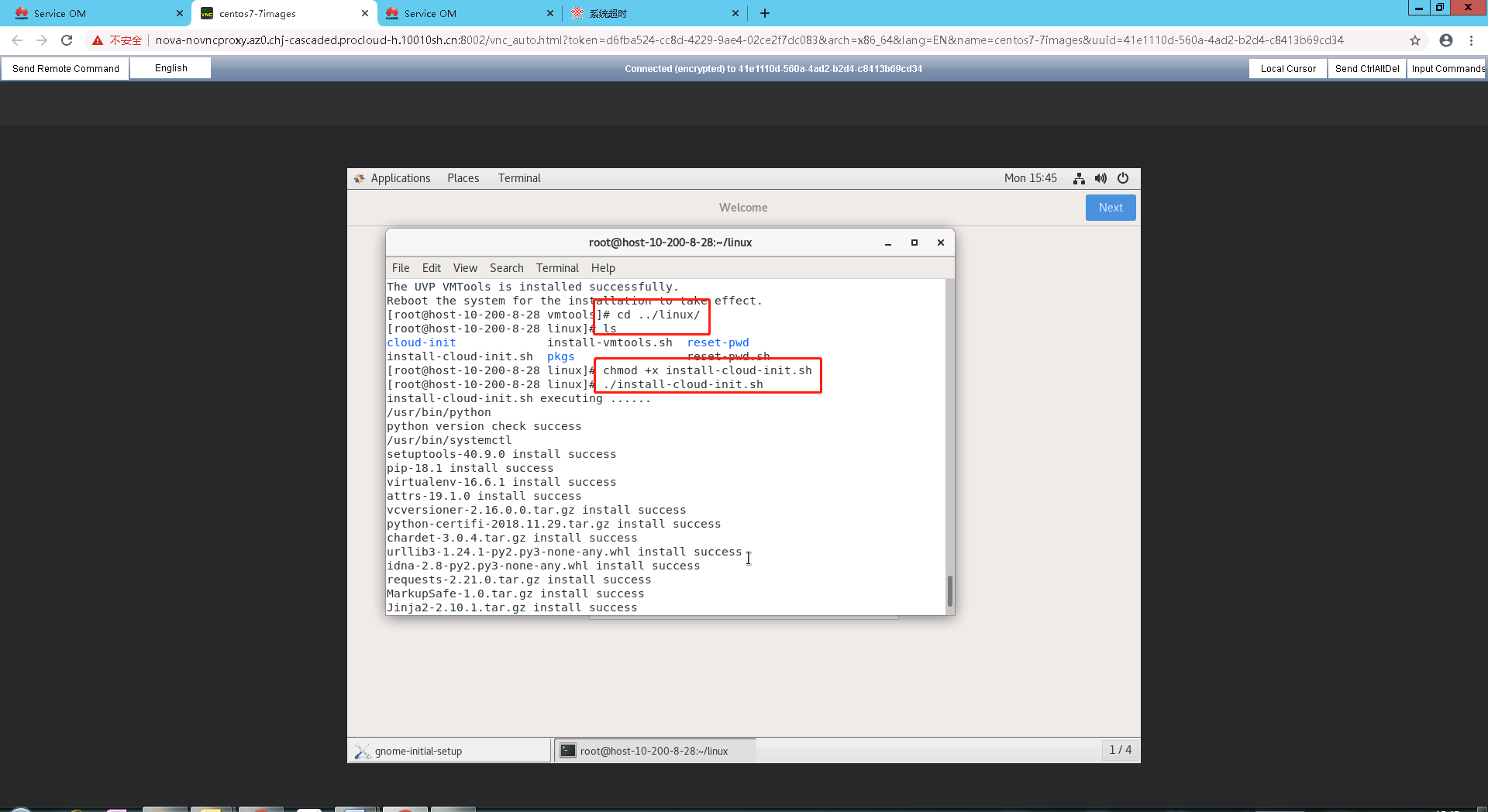
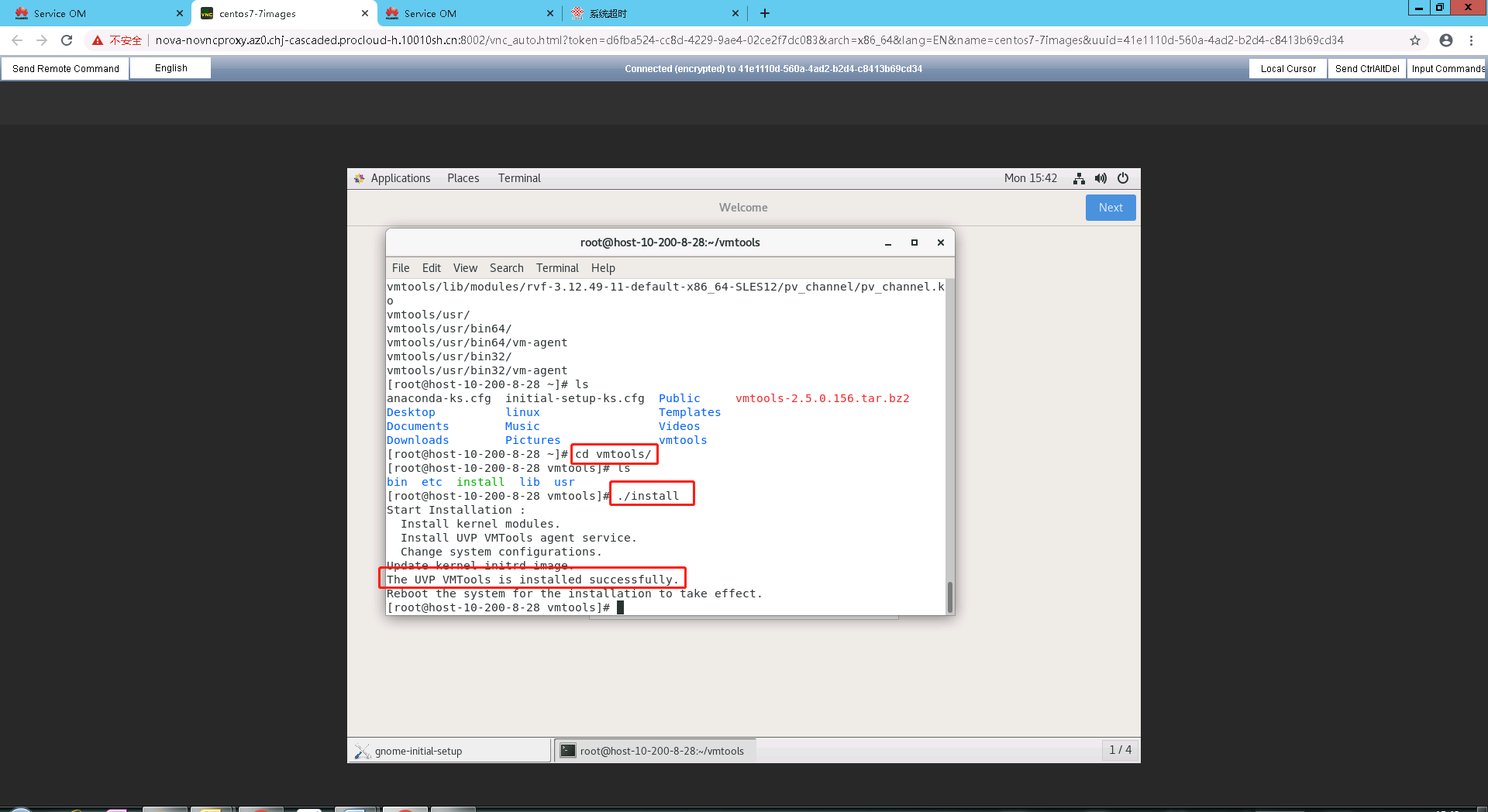
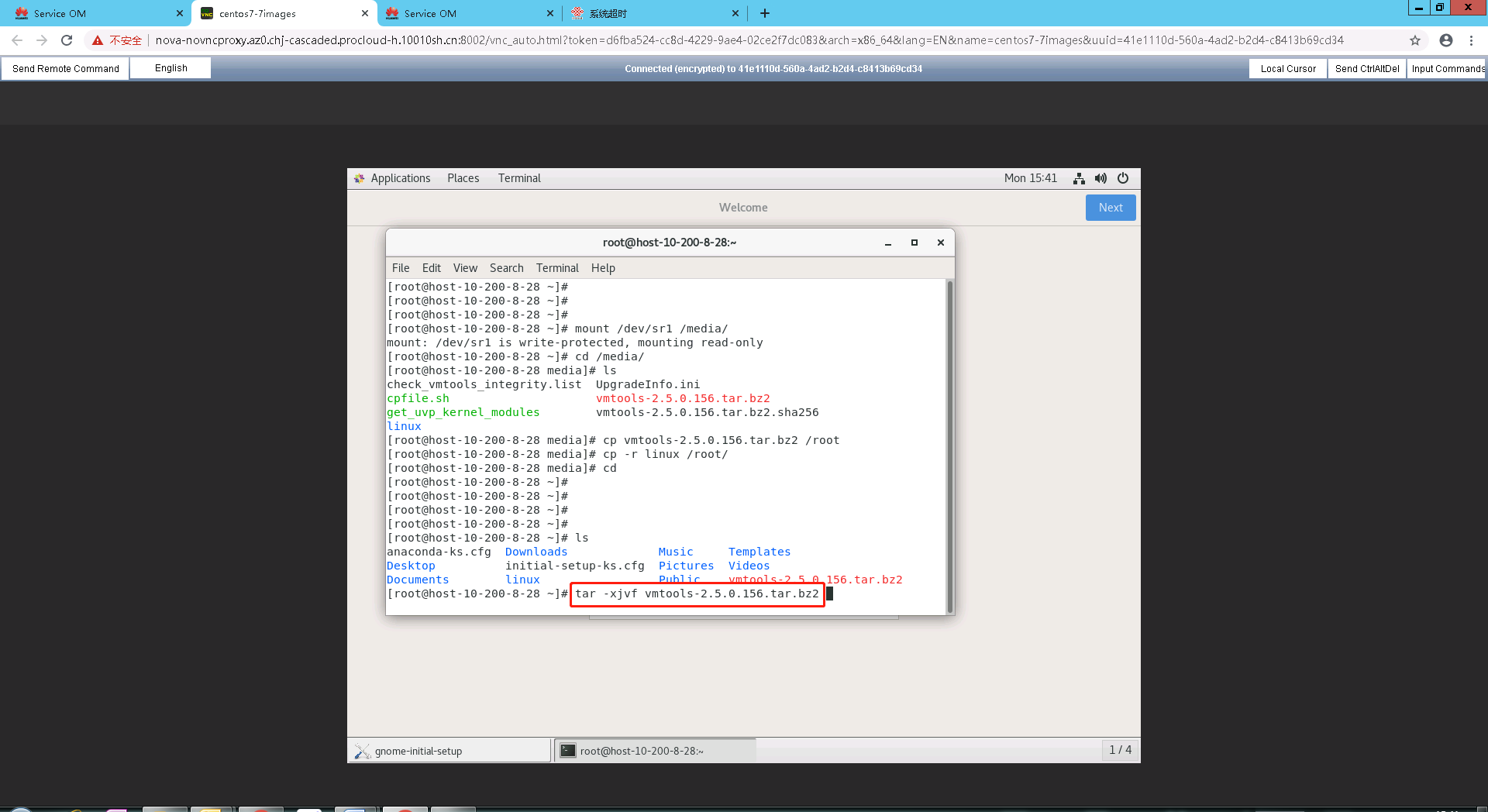
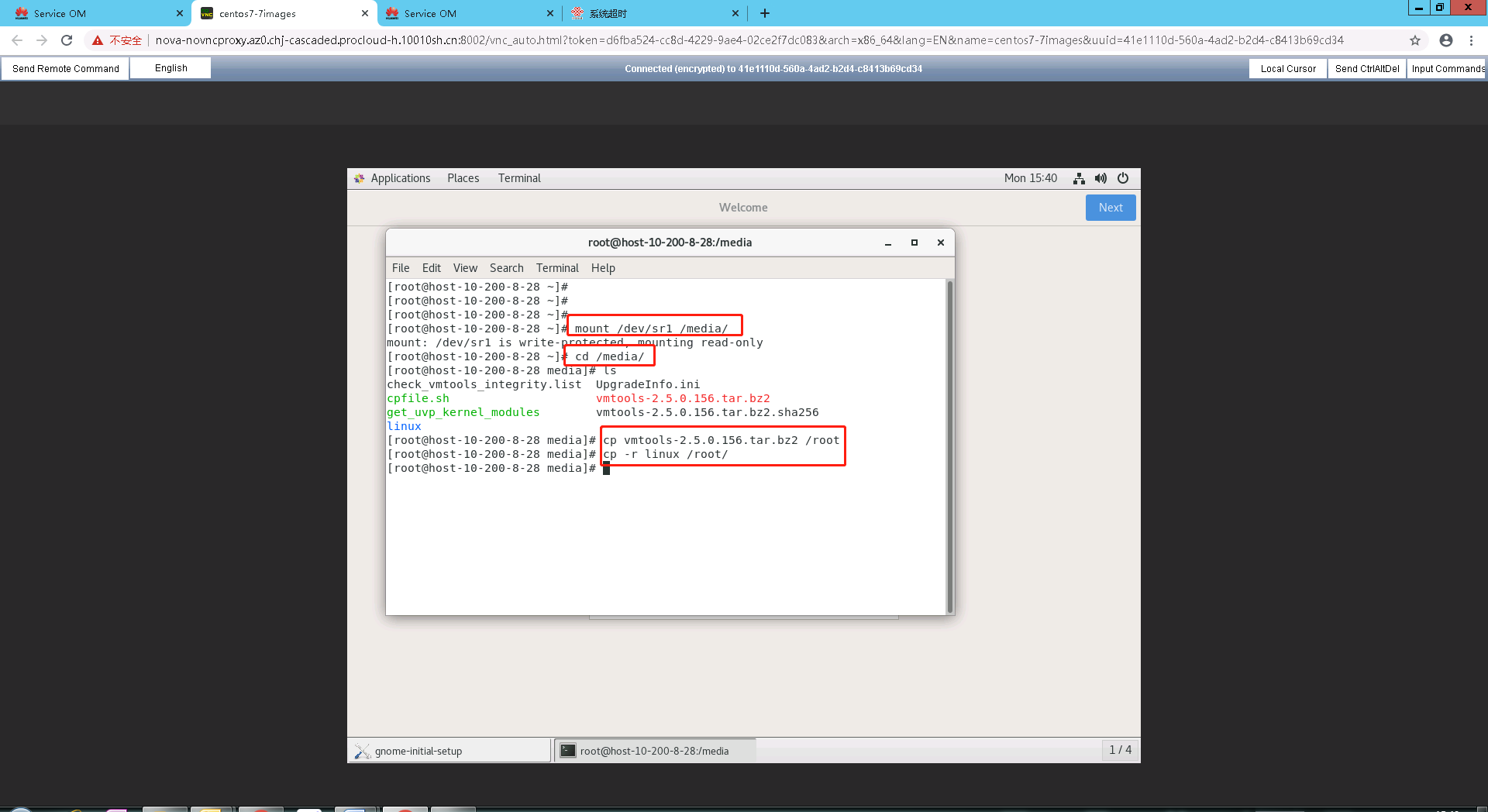
NM\_CONTROLLED=yes

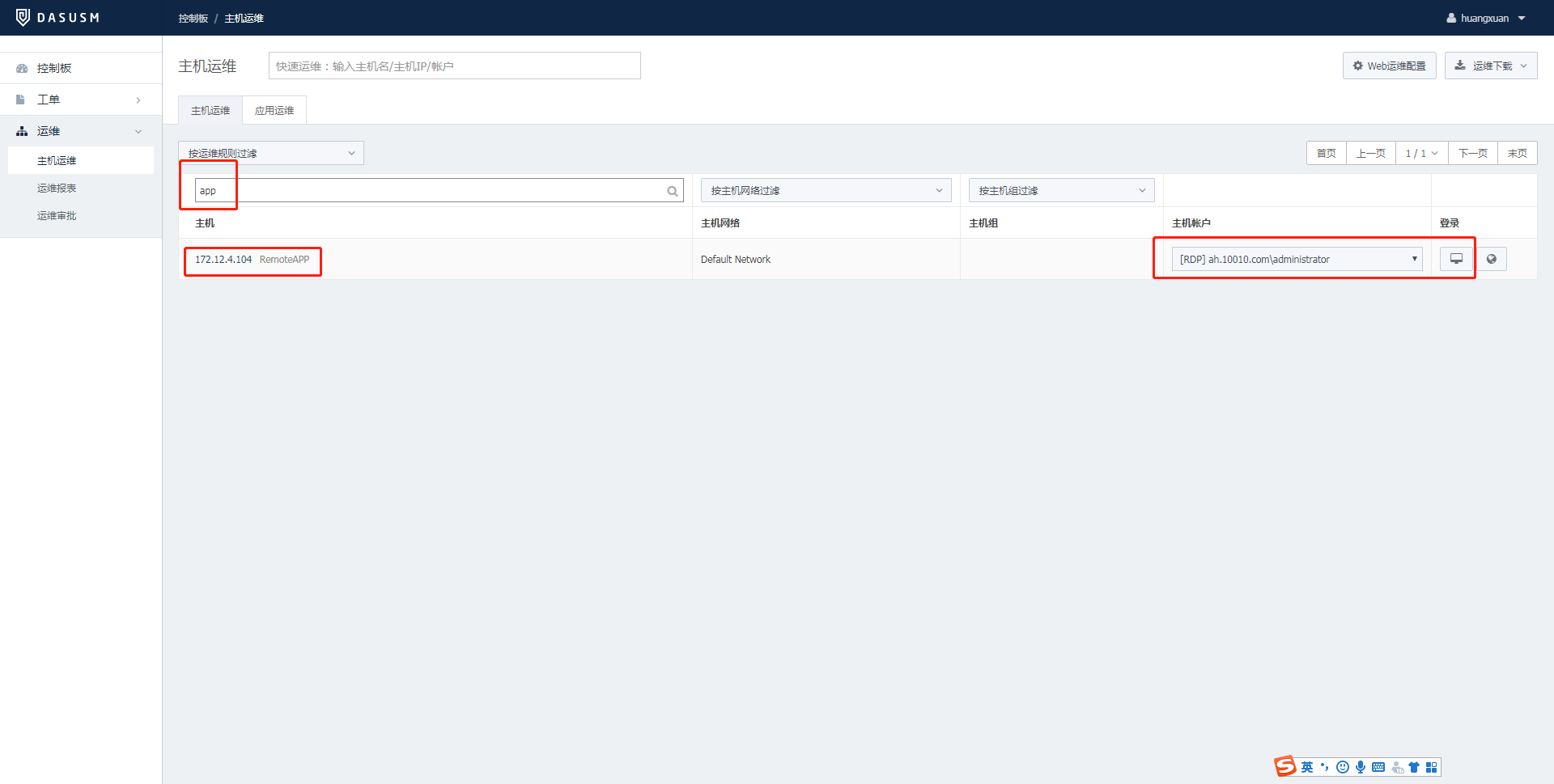
ONBOOT=yes

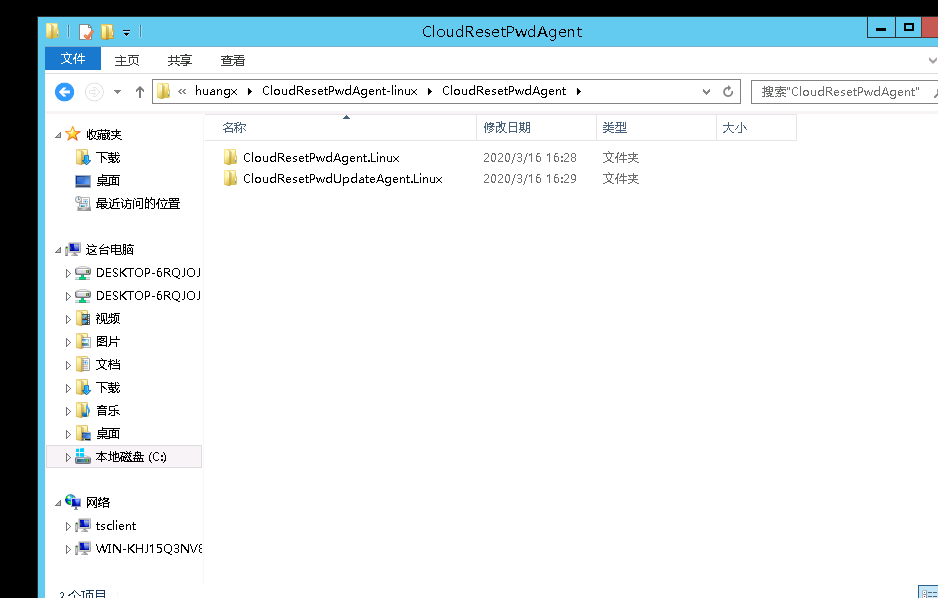
PERSISTENT\_DHCLIENT=yes

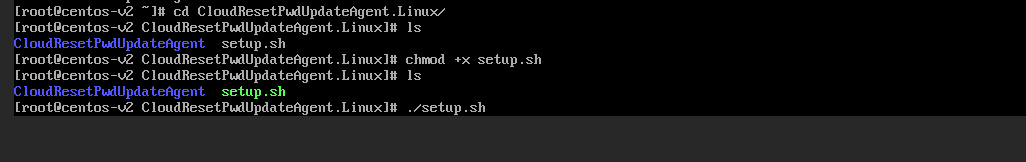
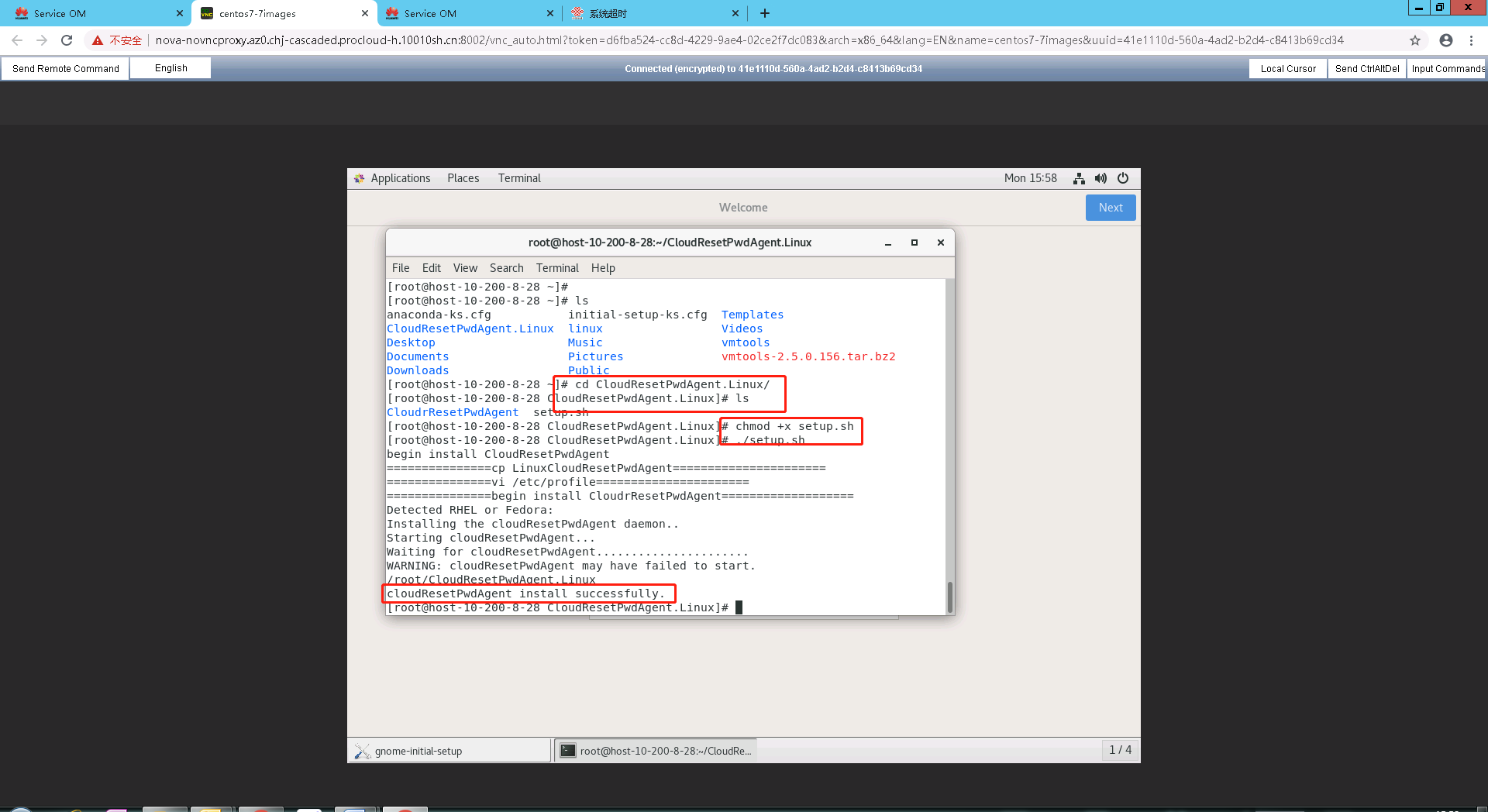
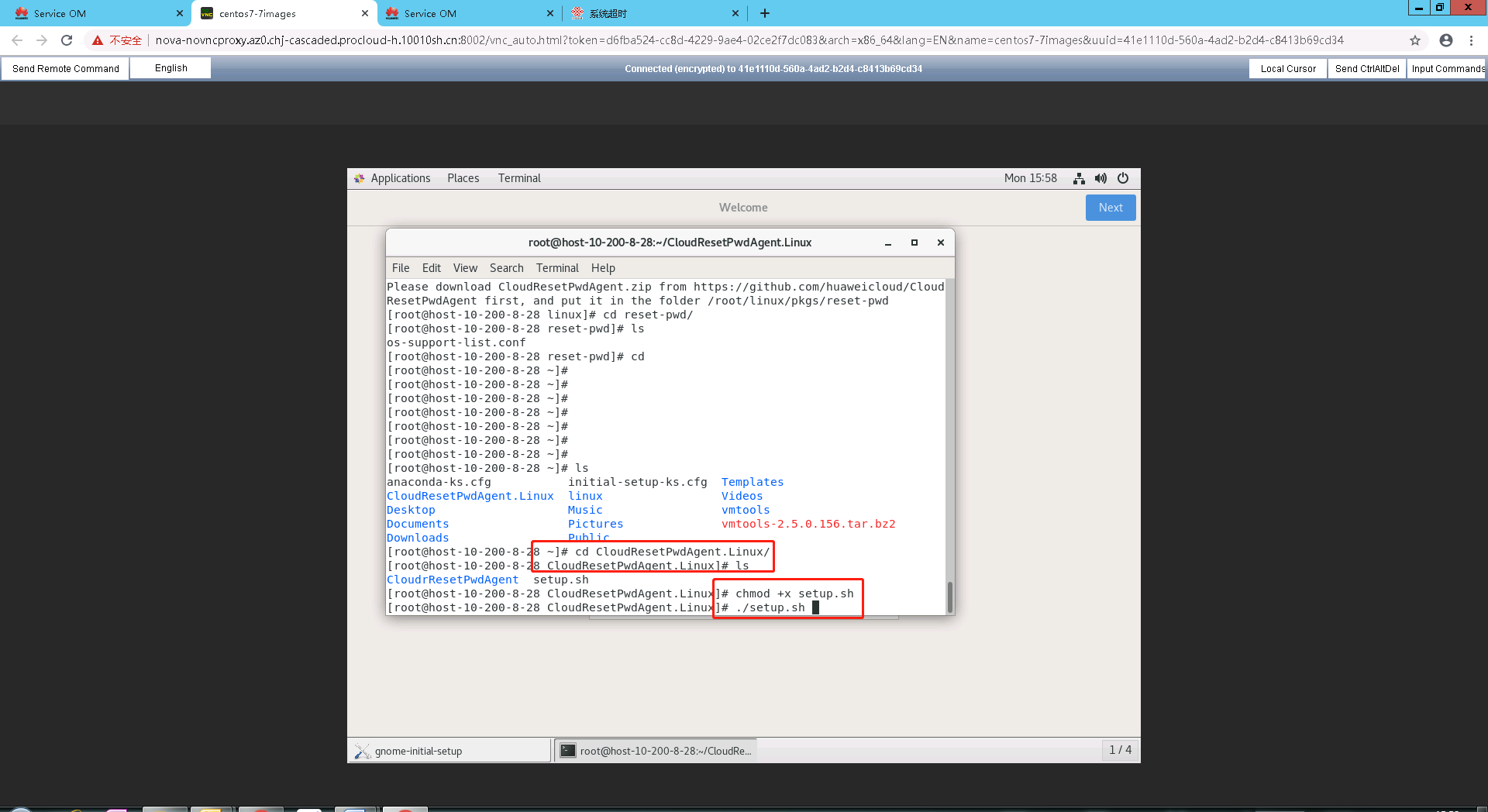


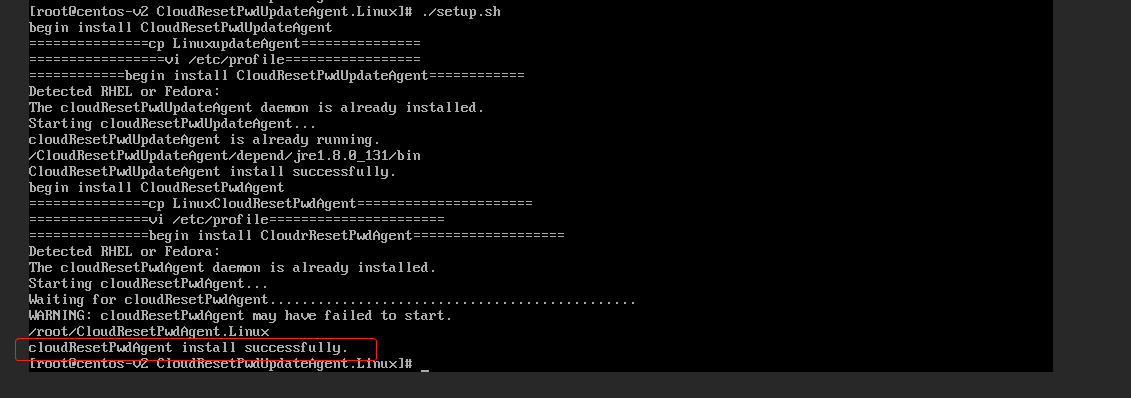
7、安装vmtools和cloud-init，安装完后重启。vmtools用来做系统监控及驱动、cloud-init用来注入root密码



8、安装密码重置插件CloudResetPwdUpdateAgent.Linux，CloudResetPwdAgent.Linux(104跳板机没有联网，只能先下载到本地，压缩，然后本地WinSCP通过公网传到虚拟机内，解压) 







cloudResetPwdAgent添加到系统服务中

cat >/etc/systemd/system/cloudResetPwdAgent.service <<EOT

[Unit]

Description=cloudResetPwdAgent service

Wants=local-fs.target

Requires=local-fs.target

[Service]

Type=simple

ExecStart=/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start

RemainAfterExit=yes

ExecStop=/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script stop

KillMode=none

[Install]

WantedBy=multi-user.target

EOT

systemctl start cloudResetPwdAgent.service

systemctl enable cloudResetPwdAgent.service

systemctl status cloudResetPwdAgent.service

cat >/etc/systemd/system/cloudResetPwdUpdateAgent.service <<EOT

[Unit]

Description=cloudResetPwdUpdateAgent service

Wants=local-fs.target

Requires=local-fs.target

[Service]

Type=simple

ExecStart=/CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script start

RemainAfterExit=yes

ExecStop=/CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script stop

KillMode=none

[Install]

WantedBy=multi-user.target

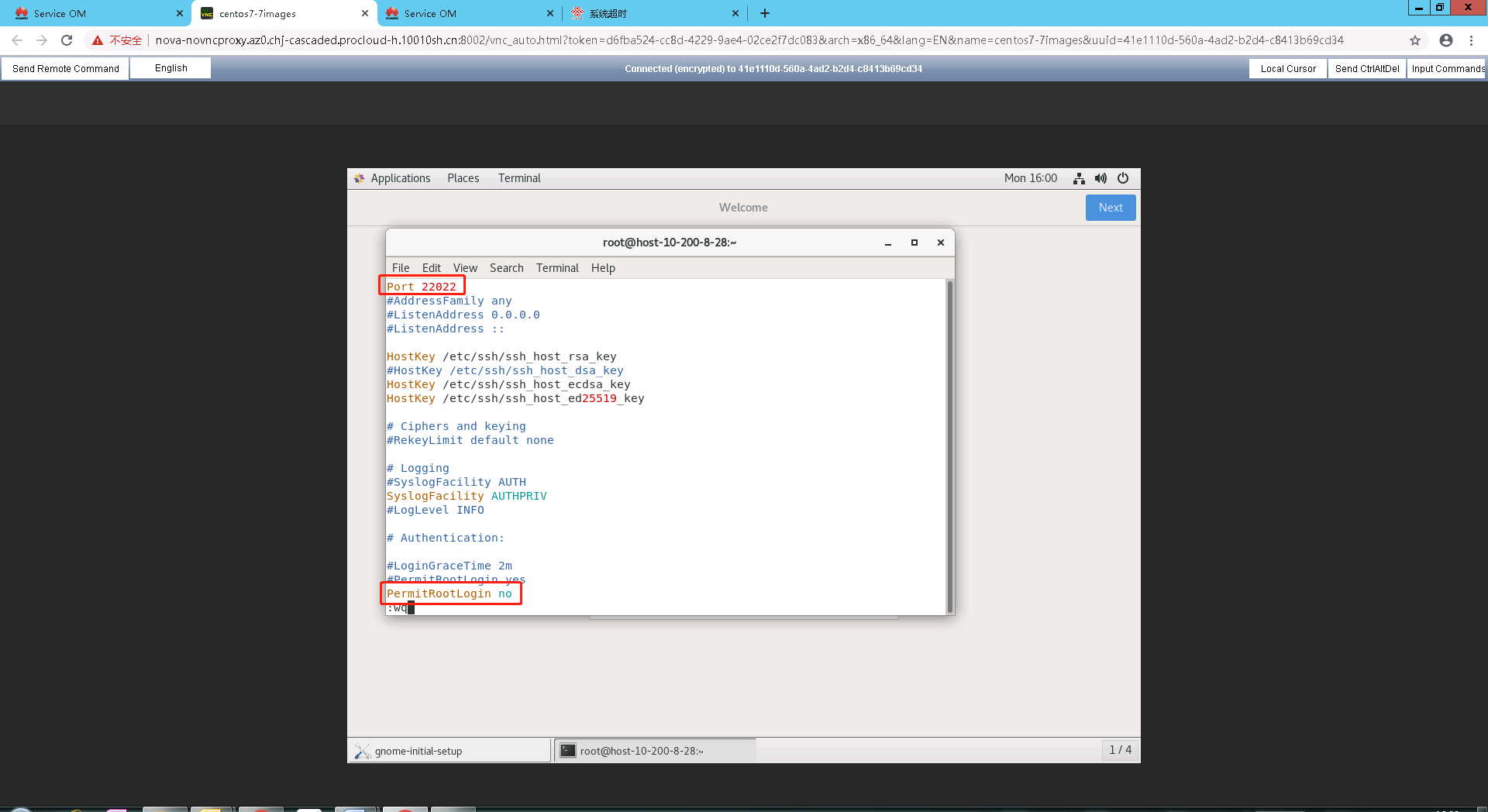
EOT

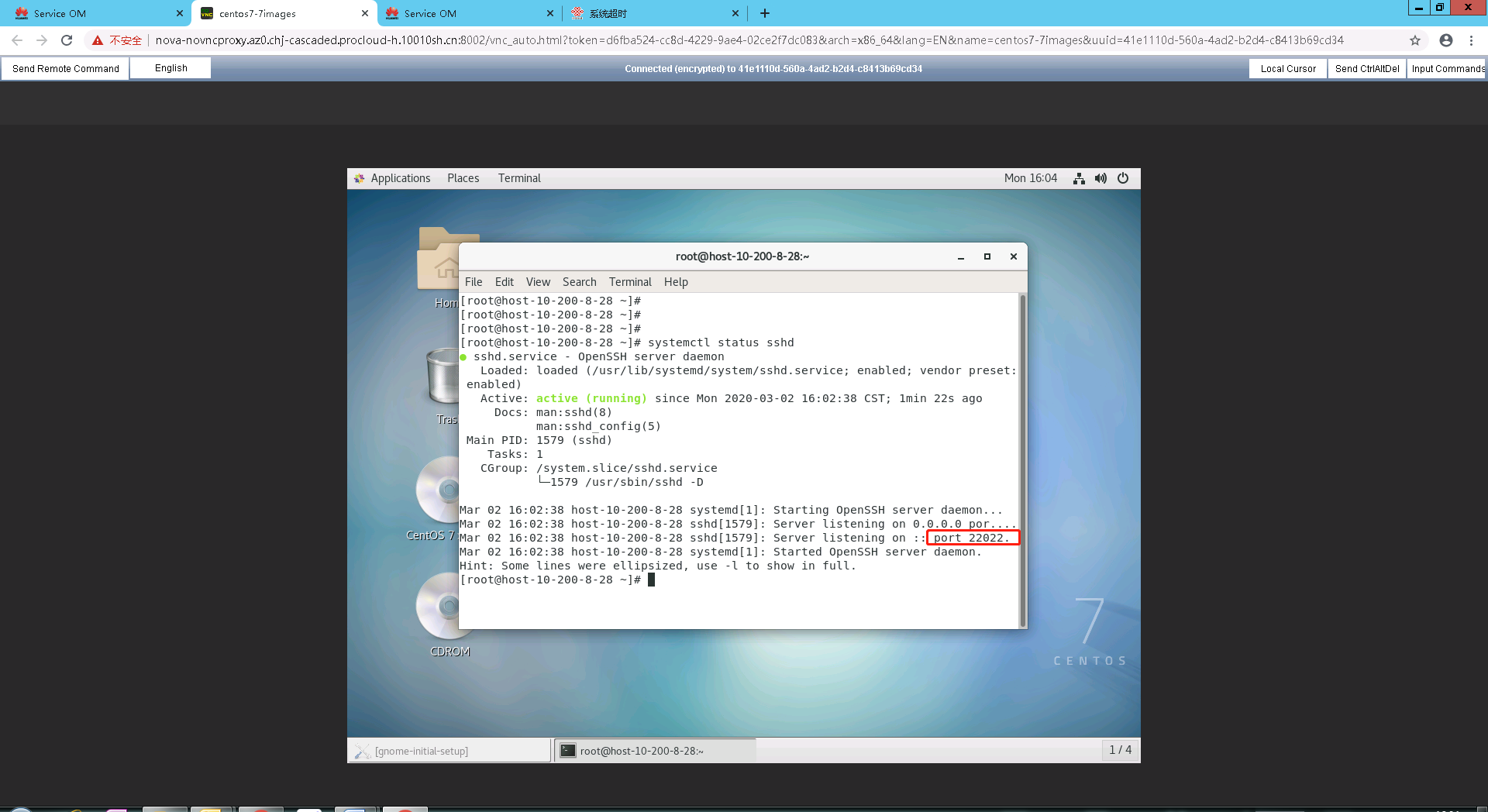
systemctl start cloudResetPwdUpdateAgent.service

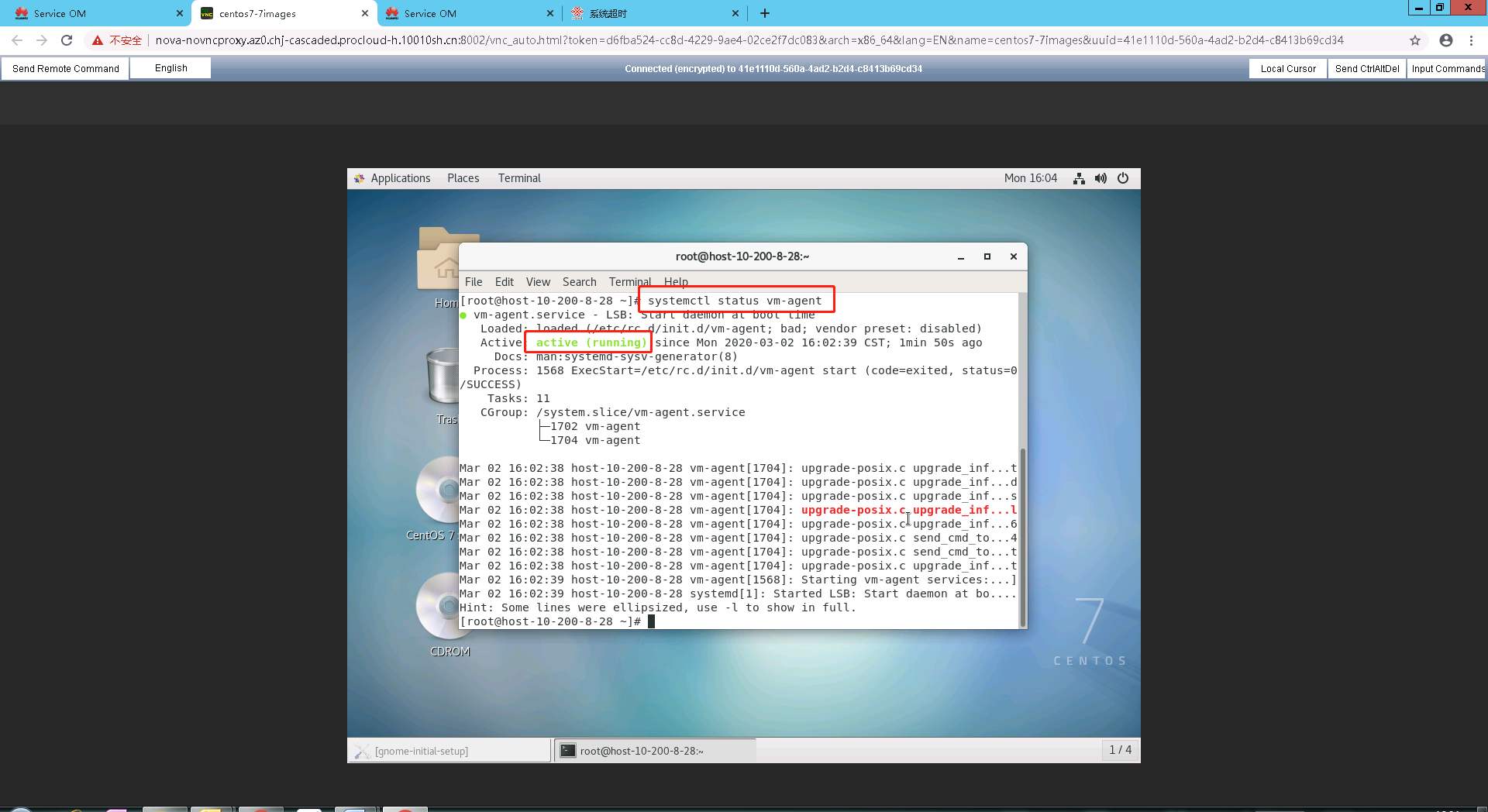
systemctl enable cloudResetPwdUpdateAgent.service

systemctl status cloudResetPwdUpdateAgent.service

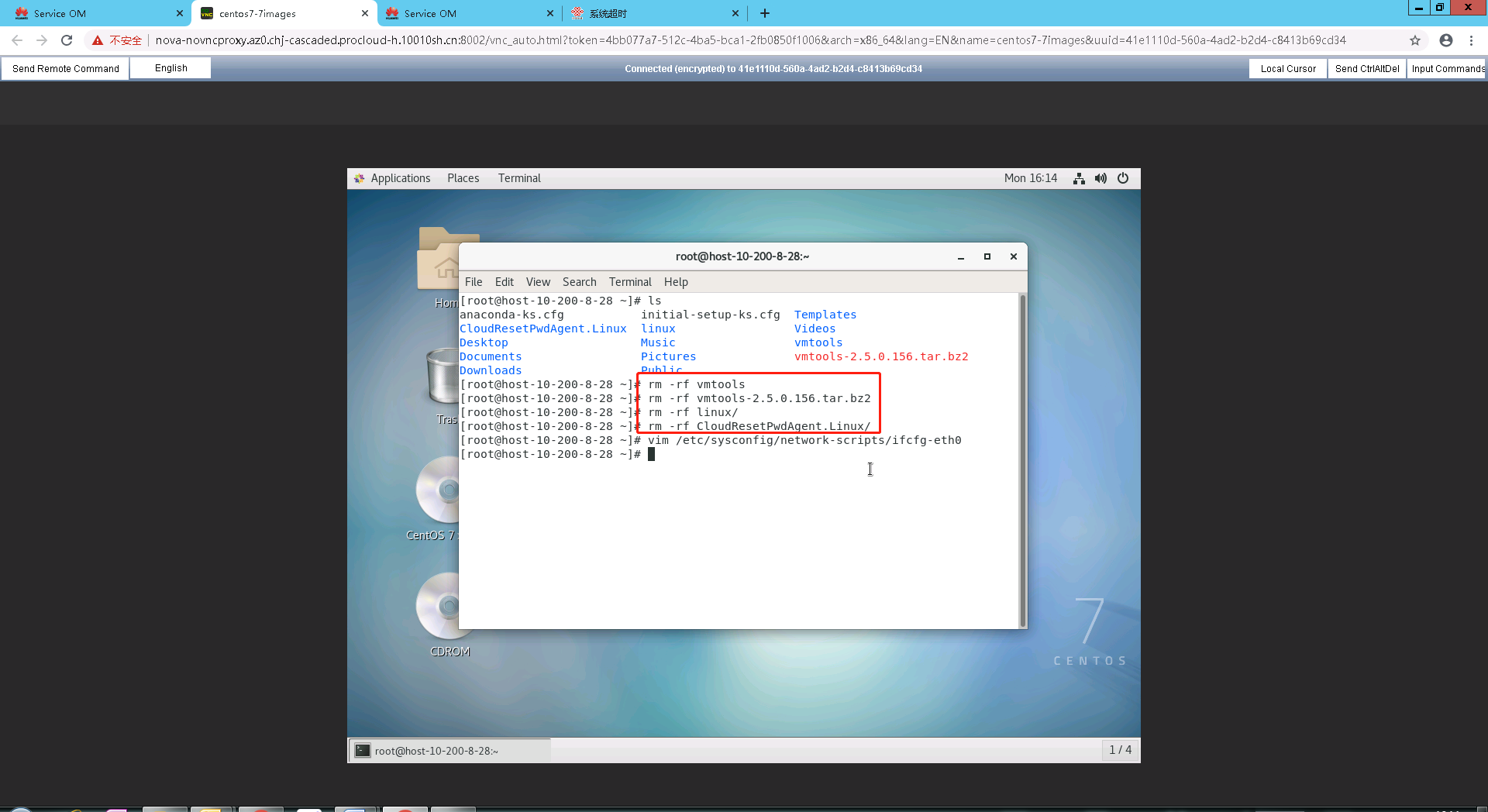
9、修改ssh端口为22022并禁止root登录



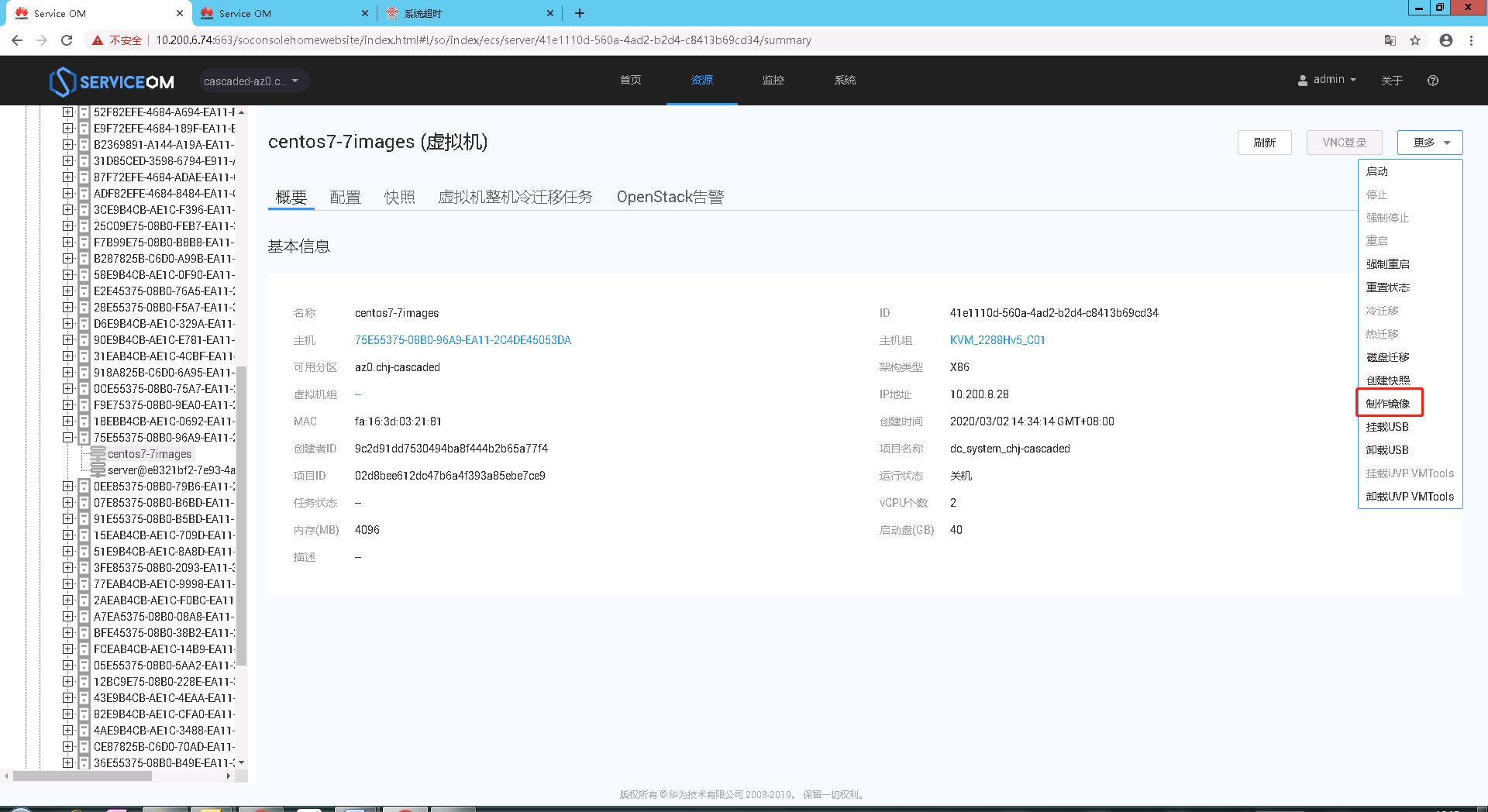
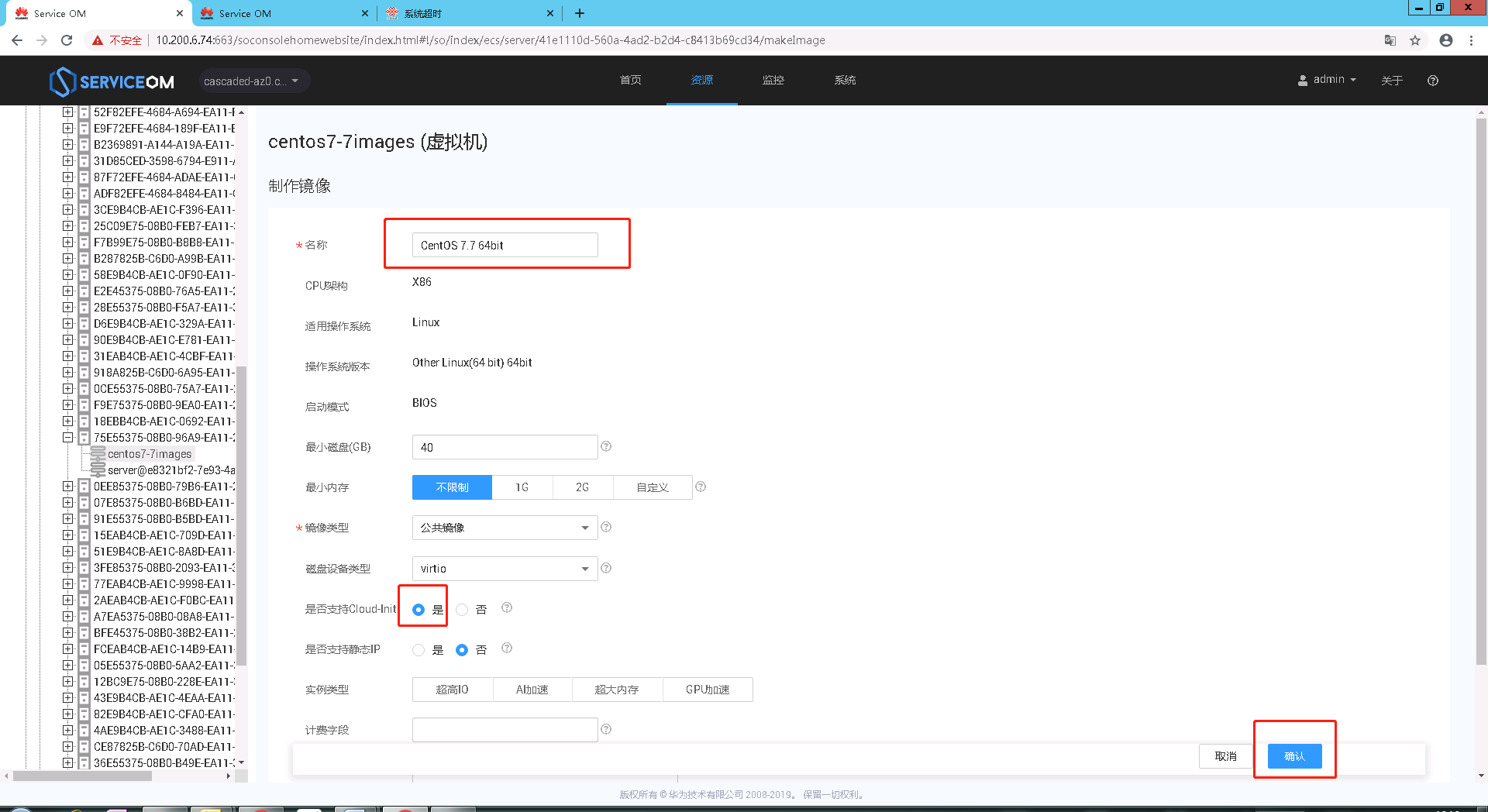


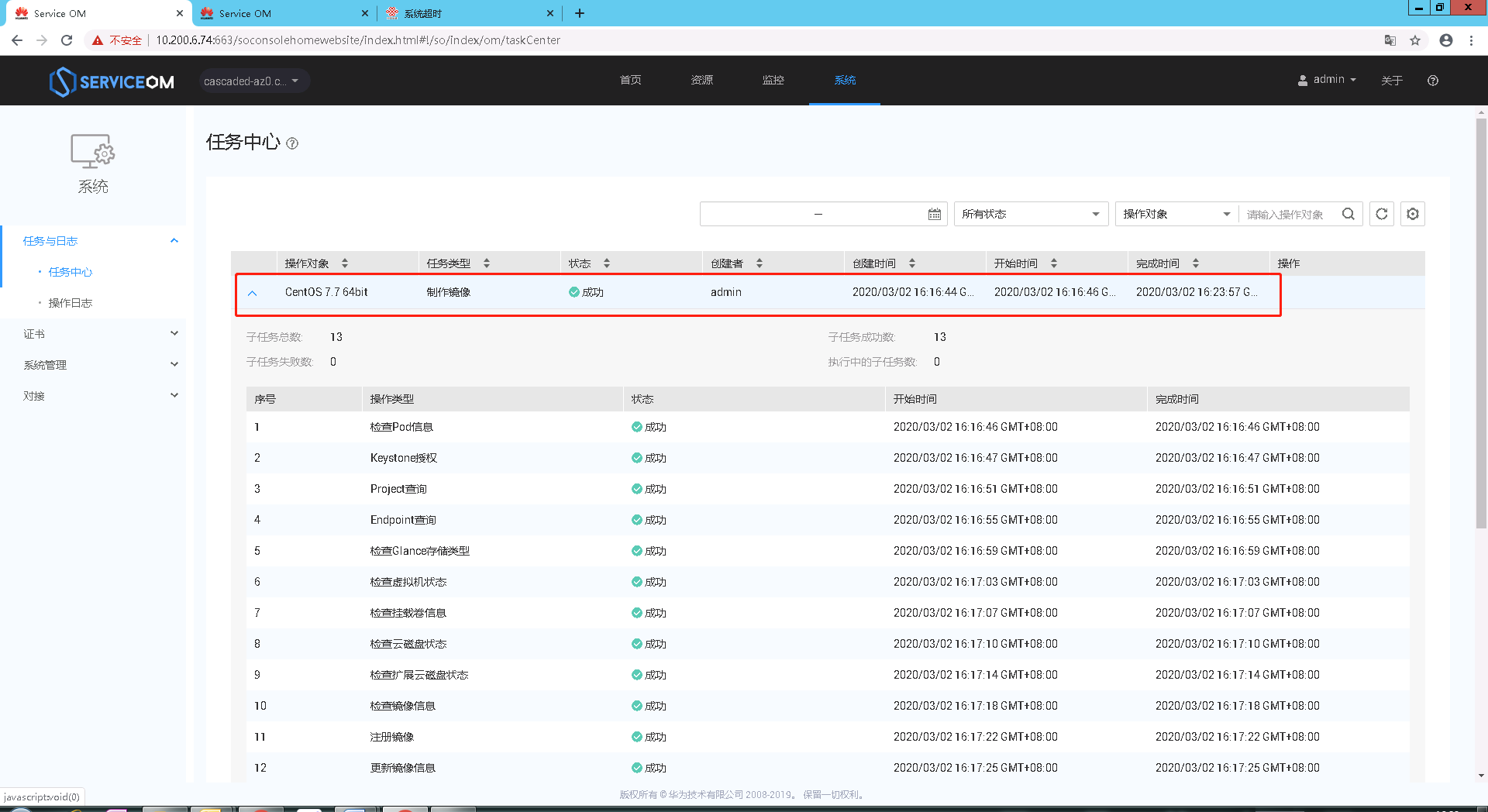


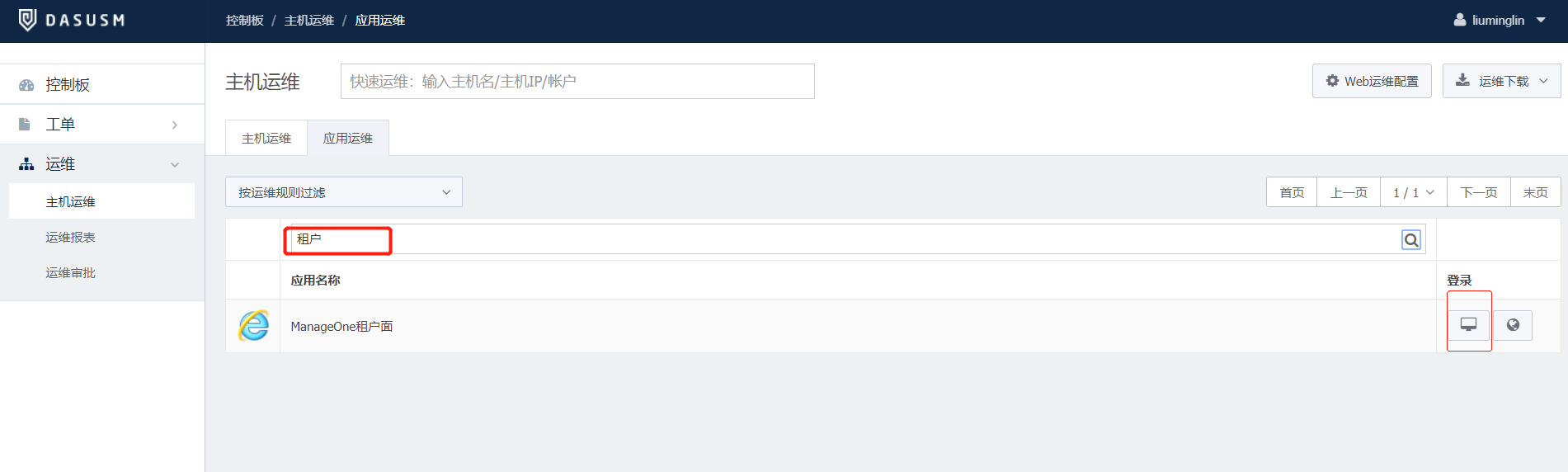
10、删除之前上传的文件及文件夹后关机

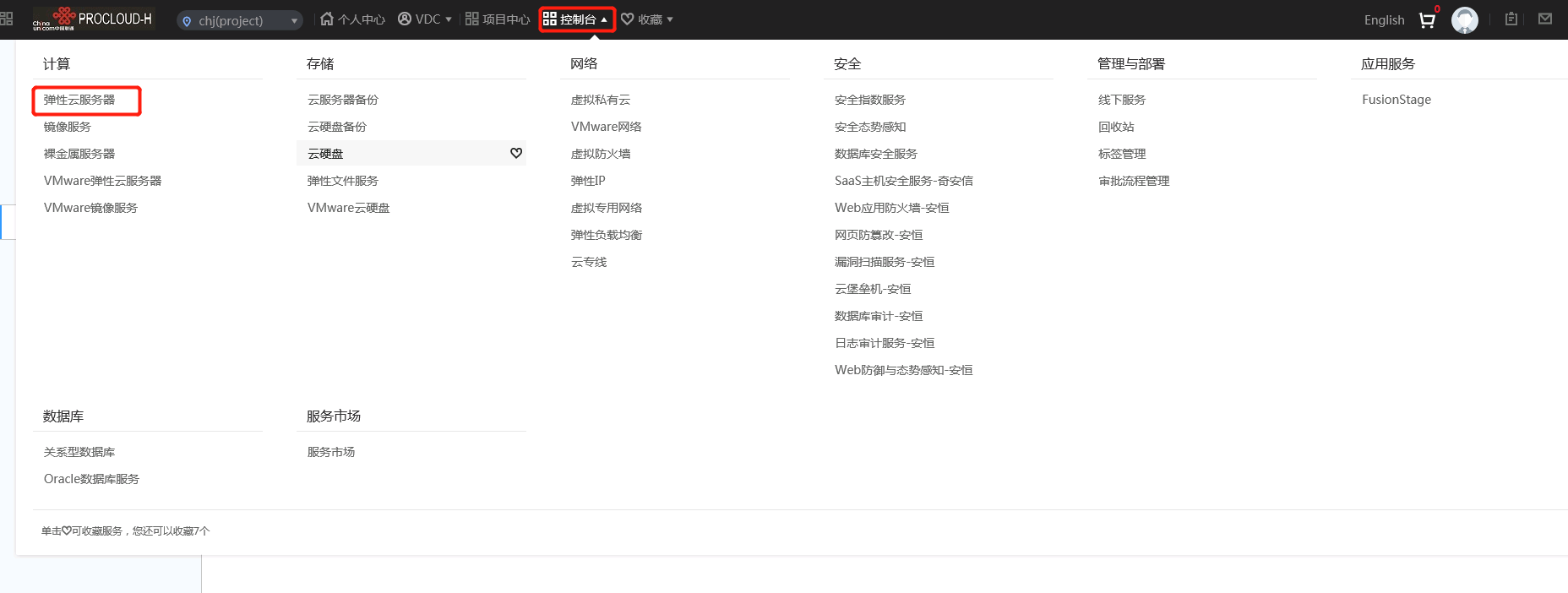


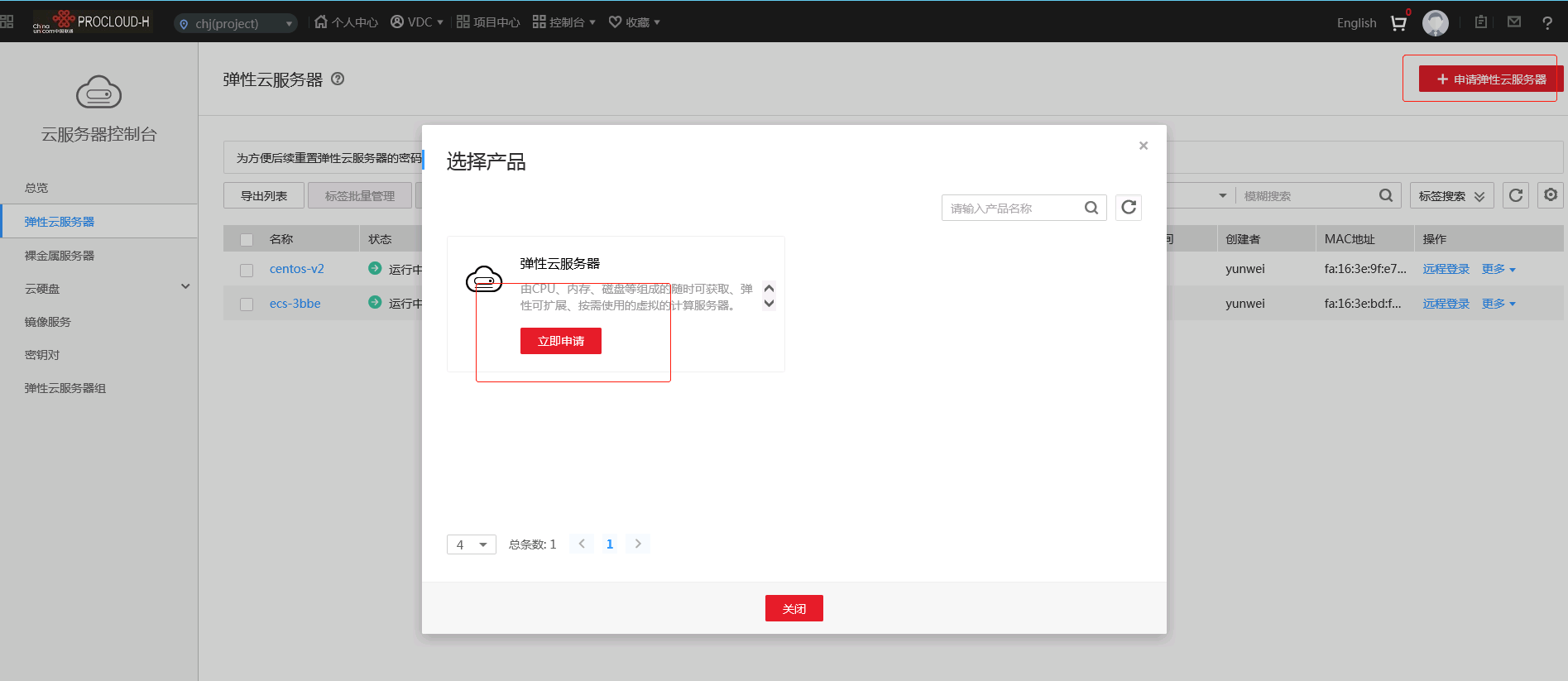
## 转换为公共镜像

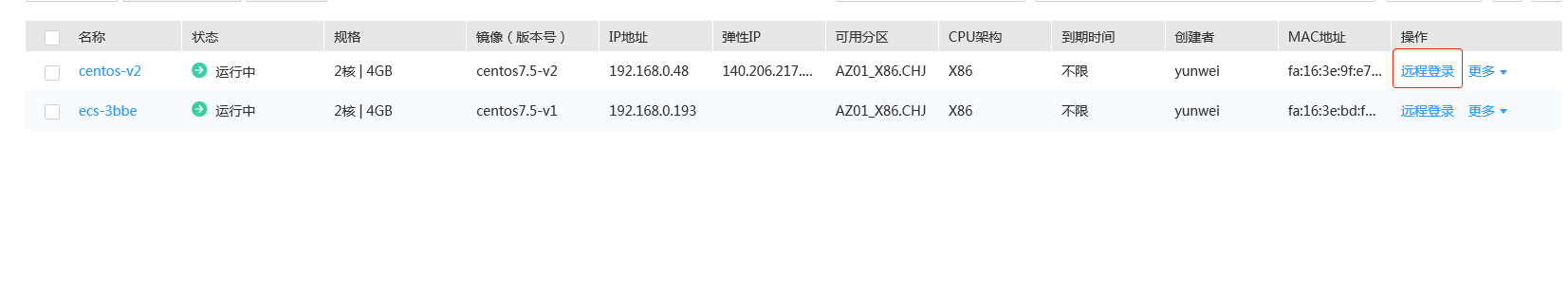


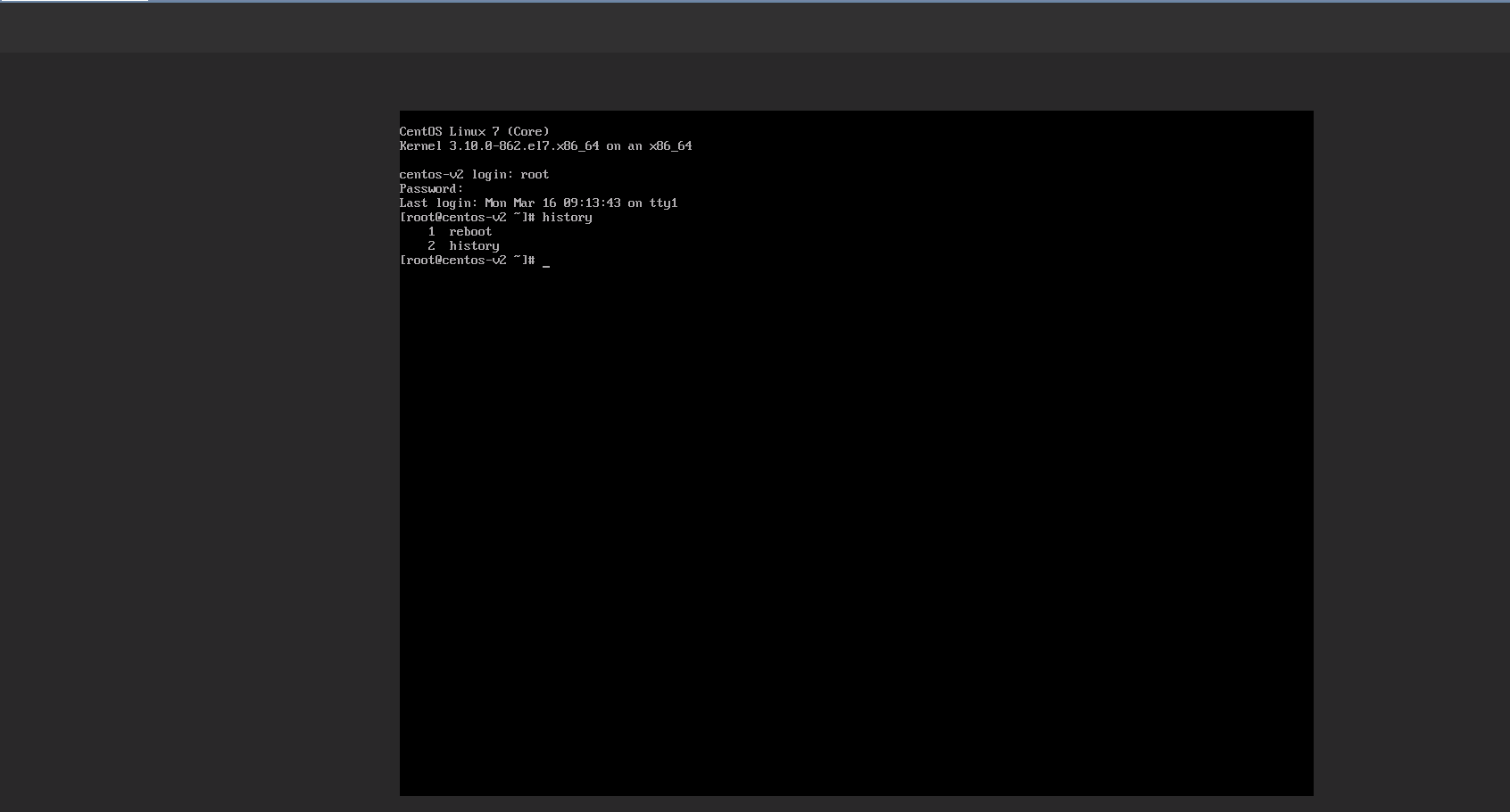
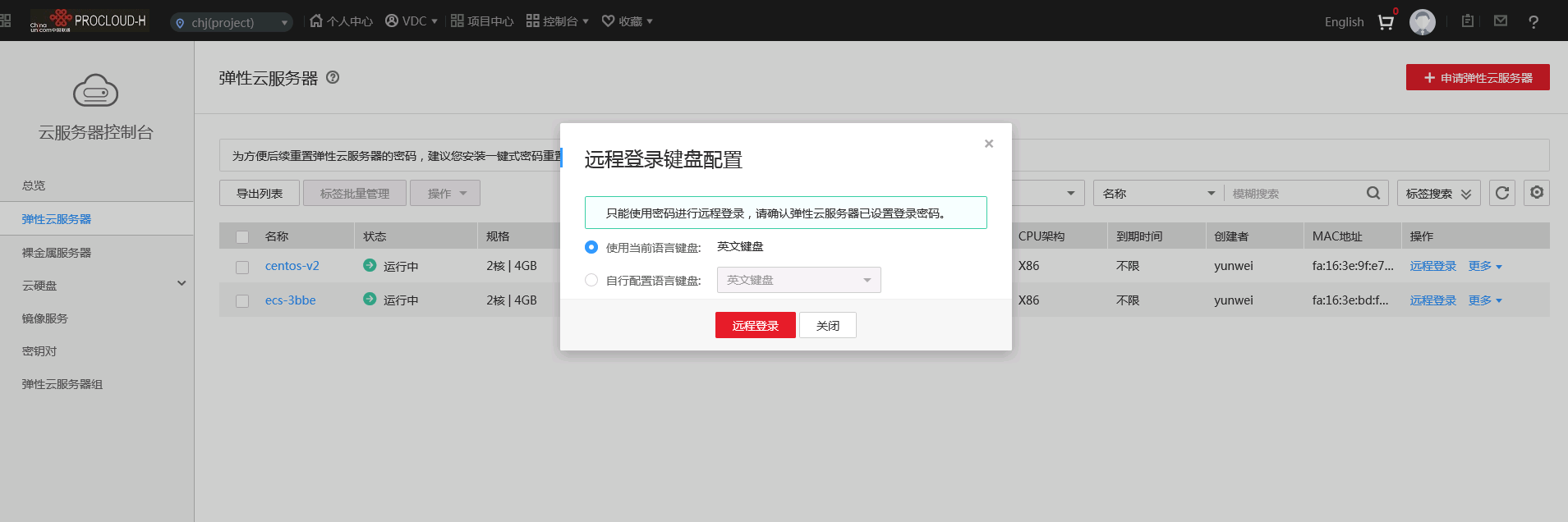
1. 升级ssh,由于om无法连接外网，去租户升级
2. 在堡垒机主机运维→应用运维搜索租户,登录用户密码：yunwei/Huawei@12
3. 申请一台弹性云服务器镜像选刚刚制作的镜像





1. 下发完成后登录点远程登录





### 修改密码

说明：

1. 设置root默认密码，密码：ShUnc@123

2、设置普通用户登录密码，密码：9ol.)P:?

命令：

Passwd 选项 值 [选项 值...]

例如：

Passwd guest

设置默认密码：9ol.)P:?

### 关闭NetworkManager

systemctl disable NetworkManager

systemctl stop NetworkManager

1. 设置指定用户：guest

/etc/pam.d/sshd文件中增加如下内容：

auth required pam\_listfile.so item=user sense=allow file=/etc/sshusers onerr=fail

1. /etc/sshusers文件中增加如下内容：

guest

### 设置账号策略

说明：

1. 账号密码策略基于pam实现，依赖pam\_cracklib模块，redhat系列默认安装，debian系列默认没有安装；（请根据操作系统进行设置）
2. /etc/profile、/etc/login.defs设置密码策略和登陆超时；
3. 密码复杂度通过/etc/pam.d/system-auth这个文件来实现的；
4. redhat系列命令：
5. sed -i "s/^\(PASS\_MAX\_DAYS\).\*/\1 90/" /etc/login.defs 90天修改密码
6. sed -i "s/^\(PASS\_MIN\_LEN\).\*/\1 12/" /etc/login.defs 12位密码长度
7. （6系列系统） sed –i ‘/^pass.\* pam\_cracklib.\*/s/$/& difok=3 minlen=12 ucredit=-1 lcredit=-1 ocredit=-1 dcredit=-1/’ /etc/pam.d/system-auth

（7系列系统） sed –i ‘/^pass.\* pam\_pwquality.\*/s/$/& difok=3 minlen=12 ucredit=-1 lcredit=-1 ocredit=-1 dcredit=-1/’ /etc/pam.d/system-auth

必须包含至少一个小写字母、数字、特殊字符，密码长度至少12位,必须有3个字符要与旧密码不同；

1. **(difok)**定义新密码中必须有几个字符要与旧密码不同；
2. **(minlen)** 定义用户密码的最小长度；
3. **(ucredit)**定义用户密码中必须包含多少个大写字母；
4. **(lcredit)** 定义用户密码中必须包含多少个小些字母;
5. **(0credit)** 定义用户密码中必须包含多少个特殊字符（除数字、字母之外）；
6. 强制用户首次登陆改密码：
7. usermod -L guest
8. chage -d 0 guest
9. usermod -U guest

### openssh漏洞修复

1. 操作系统为centos7.X
2. 安装必要的依赖包
3. yum -y install gcc openssl-devel
4. 下载最新版本 Zlib
5. Zlib 官方网站：<http://www.zlib.net/>
6. wget <http://www.zlib.net/zlib-1.2.11.tar.gz>
7. 编译安装 Zlib

# tar -xzvf zlib-1.2.11.tar.gz

# cd zlib-1.2.11

# ./configure --prefix=/usr/local/zlib

# make

# make install

1. 更新sshd
2. wget https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-8.1p1.tar.gz
3. 关闭sshd

systemctl stop sshd

1. 卸载旧的ssh

#cp -r /etc/ssh /etc/ssh.old #备份一些之前的文件

#rpm -qa|grep openssh

#rpm -e --nodeps openssh-clients-6.6.1p1-31.el7.x86\_64

#rpm -e --nodeps openssh-6.6.1p1-31.el7.x86\_64

#rpm -e --nodeps openssh-server-6.6.1p1-31.el7.x86\_64

#rpm -qa|grep openssh

1. 修改相应文件权限

#chmod 600 /etc/ssh/ssh\_host\_rsa\_key

#chmod 600 /etc/ssh/ssh\_host\_ecdsa\_key

#chmod 600 /etc/ssh/ssh\_host\_ed25519\_key

1. 解压编译安装

# tar -zxvf openssh-8.1p1.tar.gz

# cd openssh-8.1p1

# ./configure --prefix=/usr --sysconfdir=/etc/ssh --with-md5-passwords --with-privsep-path=/var/lib/sshd

# make

# make test

# make install

1. 添加root登录权限

echo "PermitRootLogin yes" >> /etc/ssh/sshd\_config

1. 安装后环境配置

cp -p contrib/redhat/sshd.init /etc/init.d/sshd（在源码安装目录）

chmod +x /etc/init.d/sshd

chkconfig --add sshd

chkconfig sshd on

chkconfig --list sshd

1. 重启sshd

systemctl restart sshd

1. 检查升级

ssh –V

1. 禁止远程root远程登录
2. 修改远程端口

vi /etc/ssh/sshd\_config  
找到PermitRootLogin，将后面的yes改为no，把前面的注释#取消 （禁止用户远程登录）

找到Port 22 修改为22022 ，把前面的注释#取消（修改远程端口）

service sshd restart （根据操作版本使用重启命令）

密码重置插件无法开机自启动怎么处理？

Red Hat 7系列、Oracle 7系列或CentOS 7系列

1.执行如下命令，打开rc.local文件。

chmod +x /etc/rc.d/rc.local

vim /etc/rc.d/rc.local

2.按“i”进入编辑模式，在文件末尾补充如下内容：

/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start

/CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script start

3.按“Esc”后，输入:wq，按“Enter”，保存设置并退出。

### 清除历史操作记录

echo “” > /root/.bash\_ history

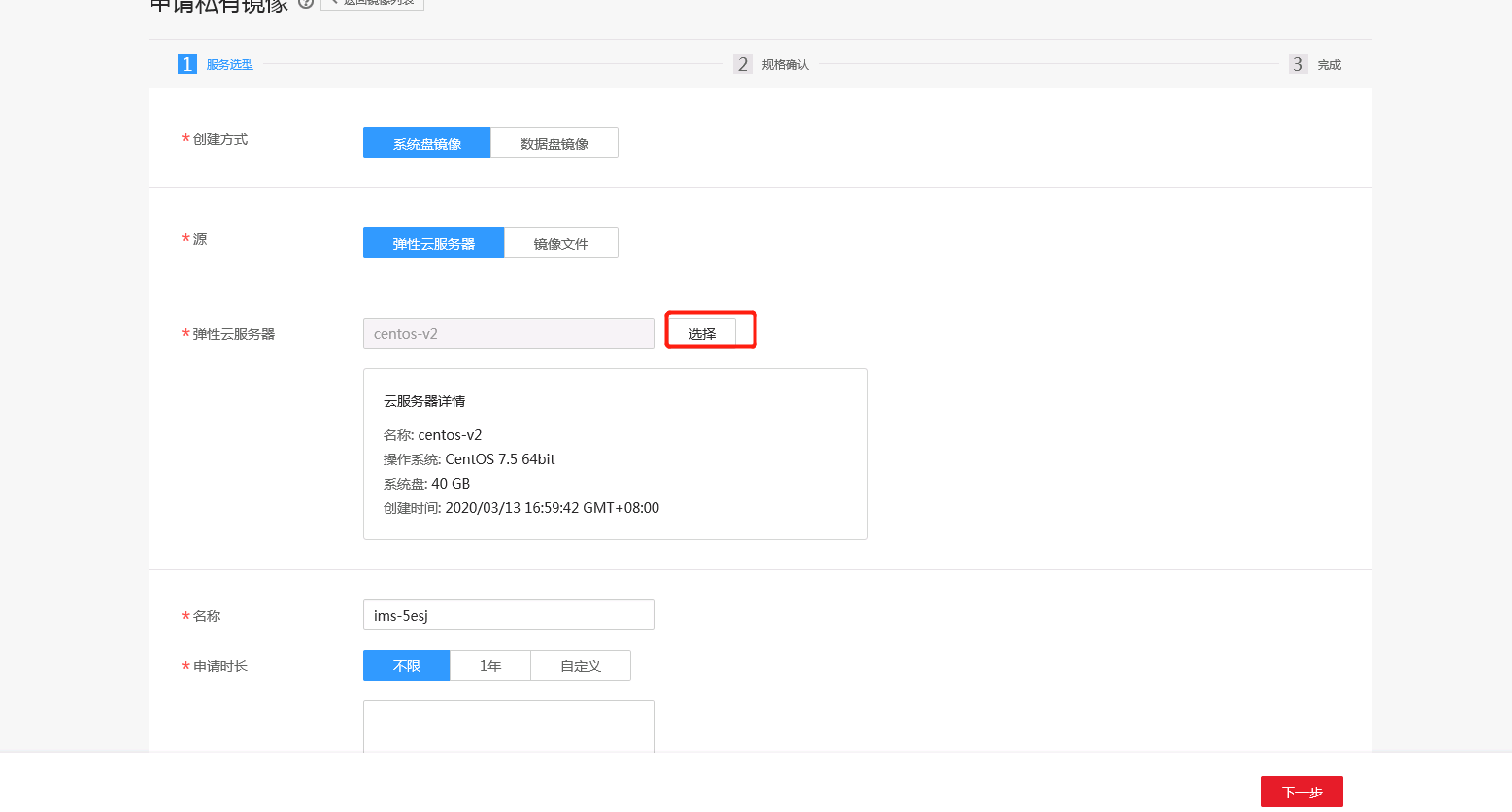
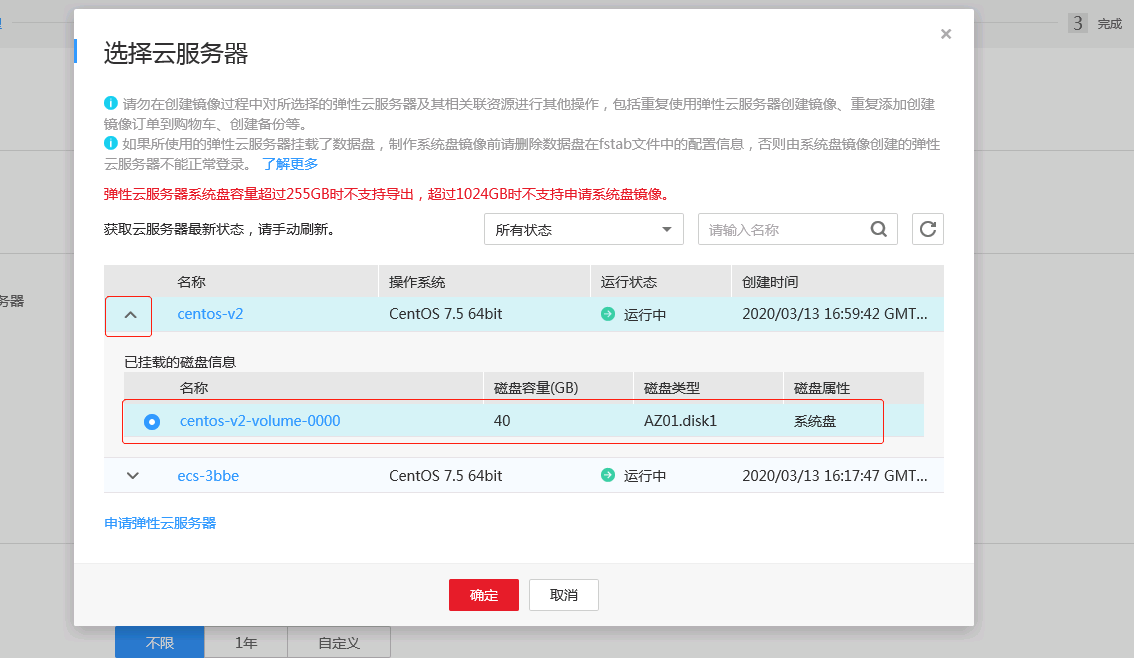
history -c

1. 制作私有镜像

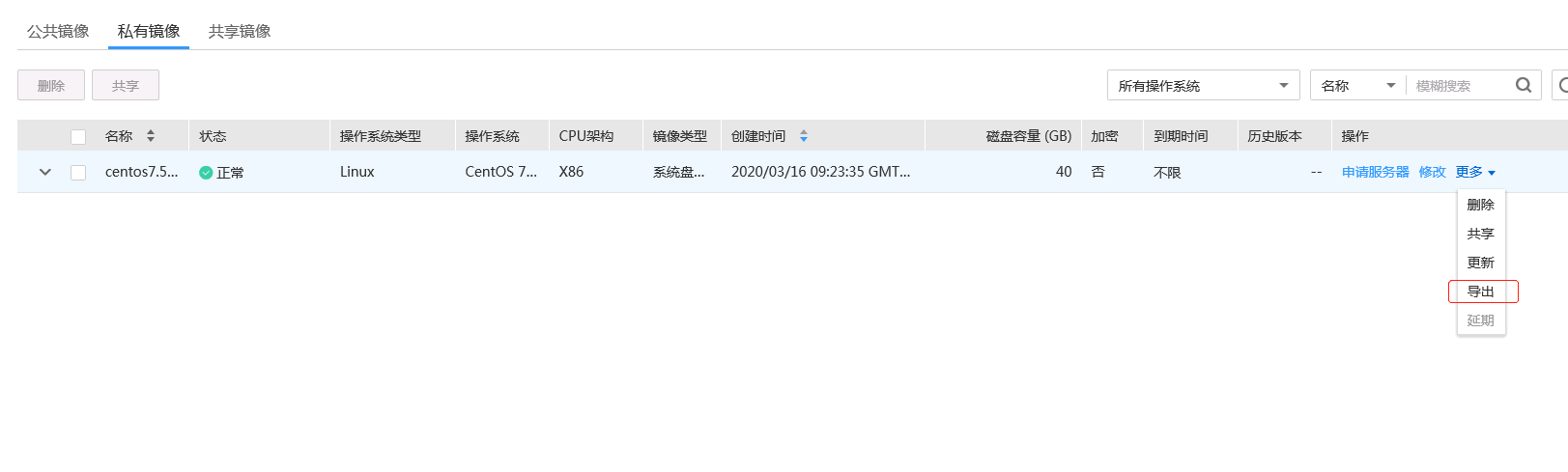
1.点击更多选择制作镜像



2.需要转成镜像的云服务器然后确定

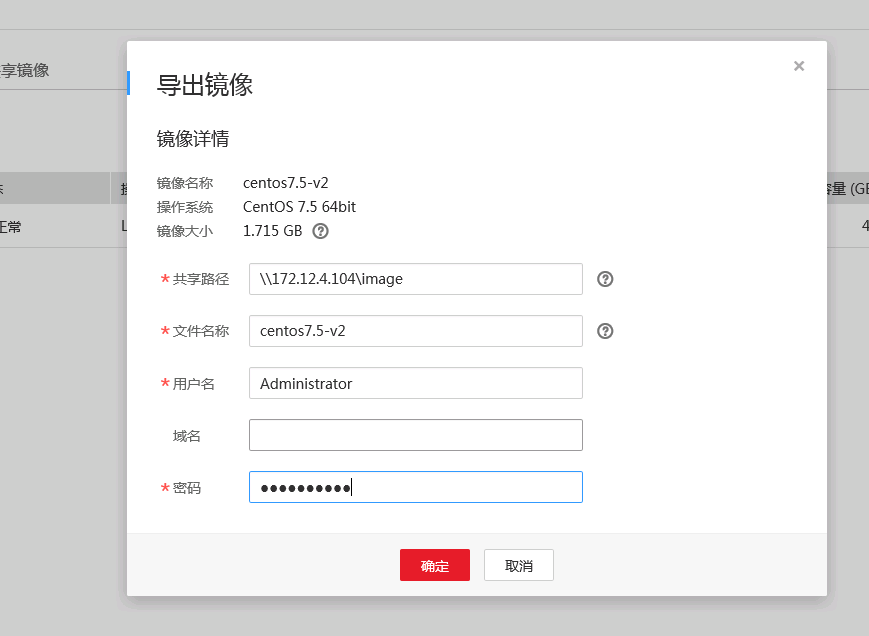


3.导出镜像

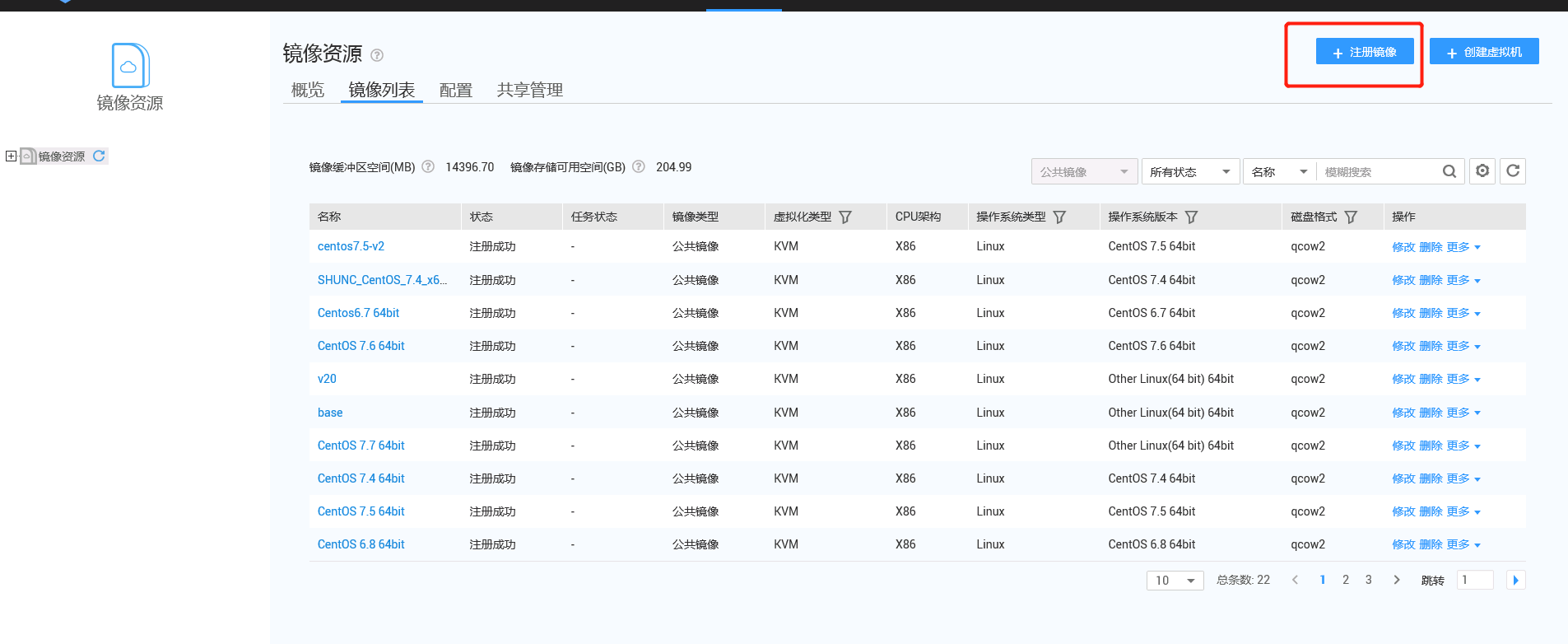
导出路径：[\\172.12.4.104\image](file:///\\172.12.4.104\image)

用户名：Administrator

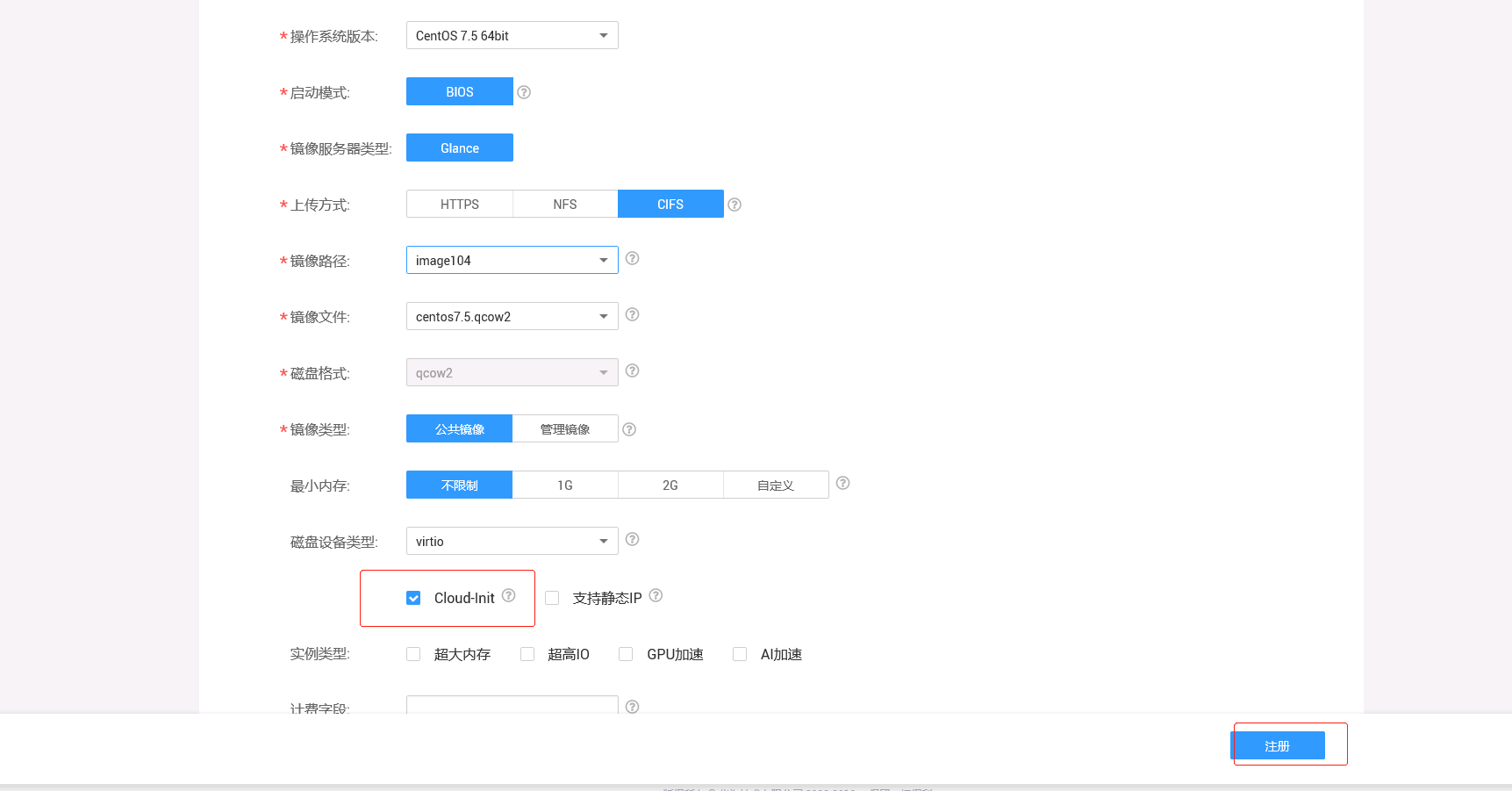
密码：1h8lsQt.@@





1. 登录om把导出的私有镜像转为公共镜像
2. 点击公共镜像，然后注册镜像 
3. 操作系统版本选择对应的系统版本，上传方式选择CIFS,镜像路径选择image104，镜像文件选择要上传的镜像文件，勾选cloud-init，然后点注册





注册成功入下

注册完成后，用新镜像下发一台虚机查看是否正常