

H3C SecCenter CSAP-vNTA 流量探针 开局指导书

Copyright © 2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 产品介绍	1-4
2 在裸金属上安装 CSAP-vNTA-1000	2-4
2.1 安装环境	2-4
2.1.1 硬件环境	2-4
2.2 在裸金属服务器上安装 CSAP-NTA-V1000	2-4
2.2.1 通过 ISO 安装 CSAP-NTA-V1000	2-5
2.2.2 配置管理口地址	2-10
3 在虚拟机上安装 CSAP-vNTA-200	3-10
3.1 安装环境	3-10
3.1.1 硬件环境	3-10
3.1.2 软件环境	3-11
3.2 在 VMware 平台安装 CSAP-NTA-V200	3-11
3.2.1 通过 ISO 安装 CSAP-NTA-V200	3-11
3.2.2 通过 PXE 方式安装 CSAP-NTA-V200	3-17
3.2.3 通过 PXE 无人值守方式安装 CSAP-NTA-V200	3-19
3.3 在 KVM 平台安装 CSAP-NTA-V200	3-21
3.3.1 通过 ISO 安装 CSAP-NTA-V200	3-21
3.3.2 通过 PXE 安装 CSAP-NTA-V200	3-28
3.3.3 通过 PXE 无人值守方式安装 CSAP-NTA-V200	3-35
3.4 在 CAS 平台安装 CSAP-NTA-V200	3-41
3.4.1 CAS 平台	3-41
3.4.2 通过 ISO 安装 CSAP-vNTA-200	3-47
4 业务配置	4-59
4.1 组网说明	4-59
4.2 License	4-59
4.2.1 License 基本介绍	4-59
4.2.2 特征库升级	4-60
4.3 web 配置流量探针服务器	4-61
4.3.1 探针日志上传到态势感知平台 web 配置过程	4-62
4.3.2 命令行参考	4-71
5 升级 NTA 产品软件版本	4-75
5.1 启动文件简介	4-75

5.2 升级方式简介	4-76
5.3 通过 Web 升级产品	4-77
5.3.1 升级前的准备	4-77
5.3.2 通过 Web 升级 CSAP-NTA-V200 的启动文件	4-77
5.4 通过命令行升级产品	4-78
5.4.1 升级前的准备	4-78
5.4.2 使用 TFTP 协议升级 CSAP-NTA-V200 的启动文件	4-79
5.4.3 使用 FTP 协议升级 CSAP-NTA-V200 的启动文件	4-81
5.4.4 重启 CSAP-NTA-V200 设备	4-84
5.5 通过 ISO 升级产品	4-85
6 恢复产品	4-86
7 附录 B: OVS bridge	4-87
7.1 配置 OVS bridge	4-87
7.2 配置 OVS 网卡的 MTU	4-90
7.3 删除 OVS bridge 配置	4-90
8 KVM 和 VMware 平台安装	4-91
8.1 VMware 平台安装	4-91
8.2 KVM 平台安装	4-96
8.2.2 配置网络参数	4-109
8.2.3 关闭 SE Linuxfuwu	4-111
8.2.4 在 KVM 虚拟化平台配置 Linux bridge	4-111
9 附录 C: 10G 网卡在虚拟平台的加载 (Intel 82599 VF 为例)	4-114
9.1 Intel 82599 VF 网卡概述	4-114
9.2 服务器 BIOS 设置	4-114
9.3 服务器虚拟平台设置	4-115
9.3.1 VMWare 平台加载 Intel 82599 VF 网卡	4-115
9.3.2 KVM 平台加载 Intel 82599 VF 网卡	4-120
9.3.3 CAS 平台加载 Intel 82599 VF 网卡	4-125
10 附录 D: PXE Server 搭建	4-131
10.1 CentOS 系统下环境搭建	4-131
10.1.2 安装并配置 DHCP	4-132
10.1.3 安装并配置 TFTP	4-133
10.1.4 安装并配置 http	4-133
10.1.5 安装并配置 NFS	4-134
10.1.6 关闭防火墙	4-134

10.1.7 安装并配置 syslinux	4-135
10.2 Ubuntu 系统下环境搭建.....	4-136
10.2.2 安装并配置 DHCP	4-137
10.2.3 安装并配置 TFTP	4-138
10.2.4 安装并配置 http.....	4-138
10.2.5 安装并配置 NFS.....	4-139
10.2.6 配置 server	4-139

1 产品介绍

H3C 网络全流量威胁分析探针是一款功能强大的软件化安全产品，包括 H3C SecCenter CSAP-NTA-V1000、H3C SecCenter CSAP-NTA-V200 两个型号。能够监控和保护虚拟环境的安全，为虚拟化数据中心和云计算网络代理全面的安全防护，帮助企业构建完善的数据中心和云计算网络安全解决方案。配合 H3C 安全威胁发现与运用管理平台，实现全流量检测、存储、分析，有效发现各种网络威胁，及时预警。

其中，CSAP-NTA-V200 安装在标准服务器虚拟机上；CSAP-NTA-V1000 直接安装在裸金属服务器上。

2 在裸金属上安装 CSAP-vNTA-1000

CSAP-NTA-V1000 仅支持在物理服务器上安装。

2.1 安装环境

2.1.1 硬件环境

CSAP-NTA-V1000 对服务器的最低配置需求如[错误!未找到引用源。](#)所示。

表2-1 硬件环境

项目	需求
处理器	1个CPU（主频不小于2.0GHz）
内存	16GB以上
硬盘	1个HD，32GB
网卡	至少2个网卡，最大支持16个网卡
网卡类型	<ul style="list-style-type: none">• Interl 82599/X710/I350/X722

注意:(1) X2020—G 服务器目前支持 Interl 网卡有 I350/82599/X710/722, 产品名称为 NIC-GE-4P-360T-L3 的 mLOM 网卡暂不支持，目前正在定制。

(2)X722 网卡 D060SP17 版本之后开始支持（包括 D060SP17）

2.2 在裸金属服务器上安装CSAP-NTA-V1000

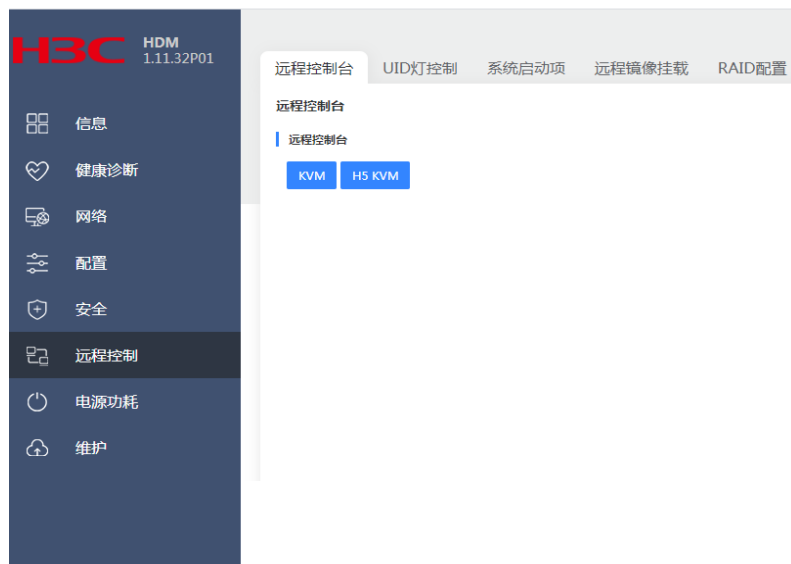
本节以硬件平台 H3C X2020-G 服务器为例，来介绍 CSAP-NTA-V1000 在裸金属服务器上的安装过程。

2.2.1 通过 ISO 安装 CSAP-NTA-V1000

1. 利用 HDM 访问裸金属服务器

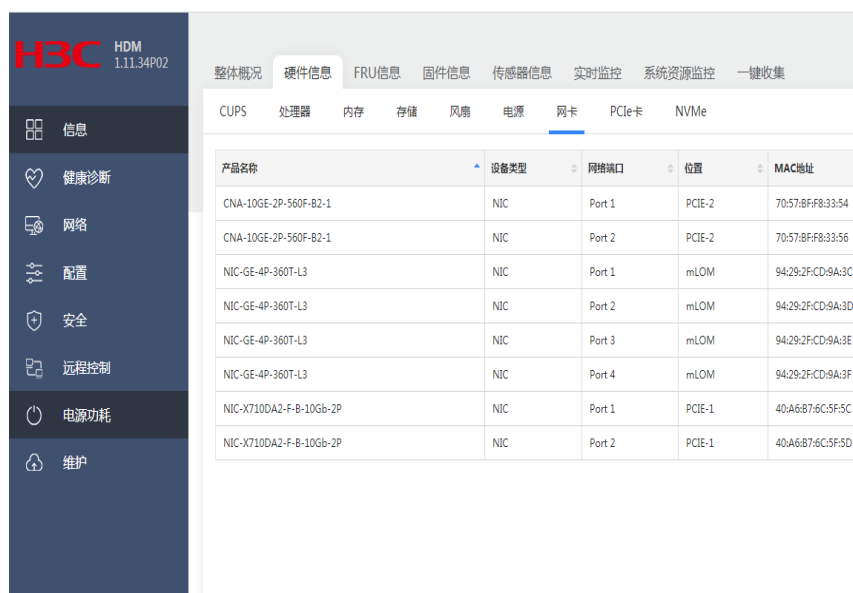
- (1) 交换机的网线需要先链接到服务器的 HDM 口上。
- (2) 在浏览器中输入服务器的 HDM 地址，例如：<https://192.168.100.179/index.html>。
- (3) 打开网页后，会出现[错误!未找到引用源。](#)所示界面，选择[远程控制台->远程控制台-> H5 KVM]。登录默认密码：`admin/Password@_`

图2-1 登录服务器



- (4) 查看网卡信息，选择信息—硬件信息—网卡。

图2-2 网卡信息

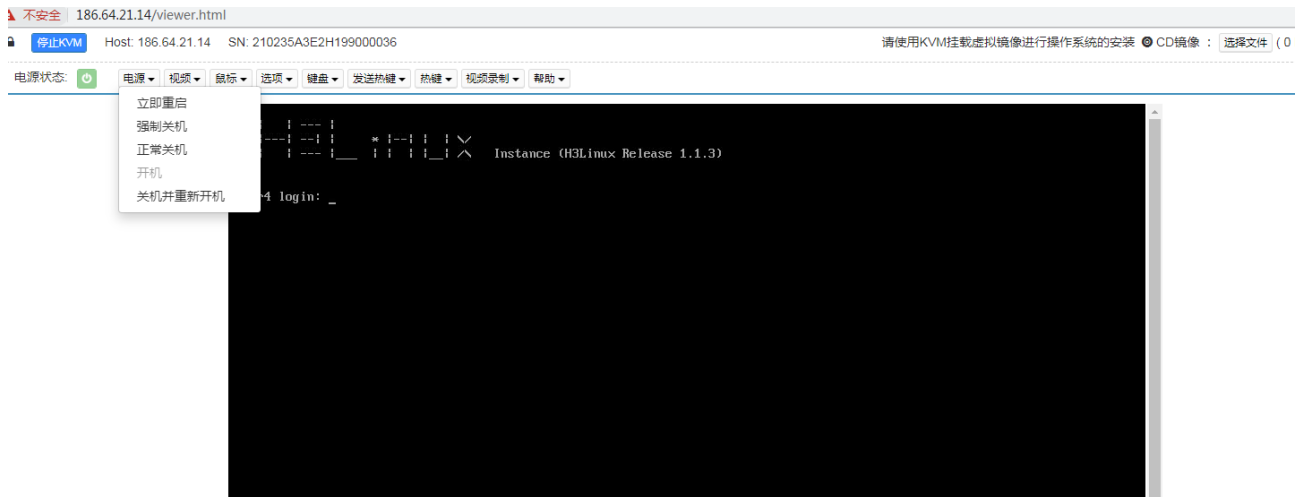
The screenshot shows the H3C HDM 1.11.34P02 web interface. The left sidebar is the same as in Figure 2-1. The main content area has a top navigation bar with tabs: 整体概况, 硬件信息 (selected), FRU信息, 固件信息, 传感器信息, 实时监控, 系统资源监控, 一键收集. Below this, there's a sub-section for '网卡' (Network Cards) with a table of details.

产品名称	设备类型	网络端口	位置	MAC地址
CNA-10GE-2P-560F-82-1	NIC	Port 1	PCIe-2	70:57:BF:F8:33:54
CNA-10GE-2P-560F-82-1	NIC	Port 2	PCIe-2	70:57:BF:F8:33:56
NIC-GE-4P-360T-L3	NIC	Port 1	mLOM	94:29:2F:CD:9A:3C
NIC-GE-4P-360T-L3	NIC	Port 2	mLOM	94:29:2F:CD:9A:3D
NIC-GE-4P-360T-L3	NIC	Port 3	mLOM	94:29:2F:CD:9A:3E
NIC-GE-4P-360T-L3	NIC	Port 4	mLOM	94:29:2F:CD:9A:3F
NIC-XT100A2-F-8-10Gb-2P	NIC	Port 1	PCIe-1	40:A6:87:6C:5F:5C
NIC-XT100A2-F-8-10Gb-2P	NIC	Port 2	PCIe-1	40:A6:87:6C:5F:5D

注意：X2020-G 服务器目前支持 Intel 网卡有 I350/82599/X710/X722，产品名称为 NIC-GE-4P-360T-L3 的 mLOM 网卡暂不支持，目前正在定制。

(5) 登录成功后, 打开 H5 kvm 会出现[错误!未找到引用源。](#)所示界面,点击电源--立即重启。

图2-3 成功登录服务器

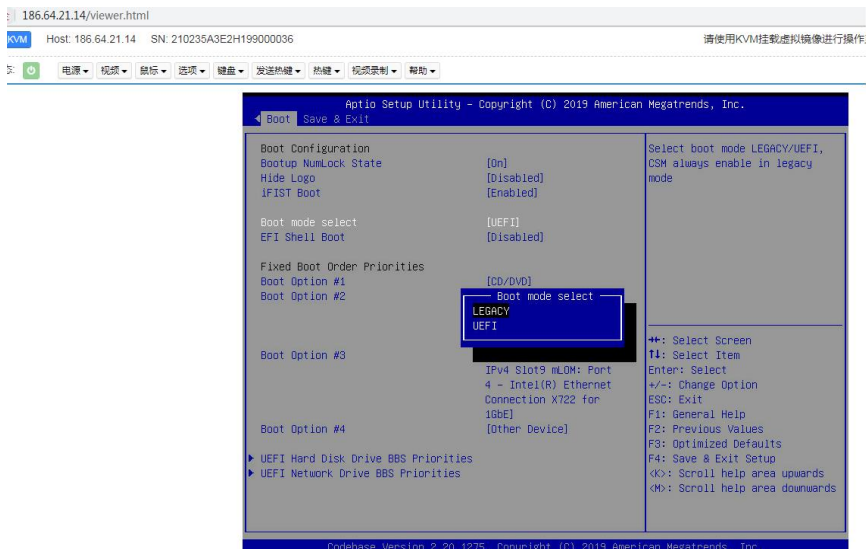


在下图界面, 点按"Esc"按键进入 BIOS 界面, 如下图:

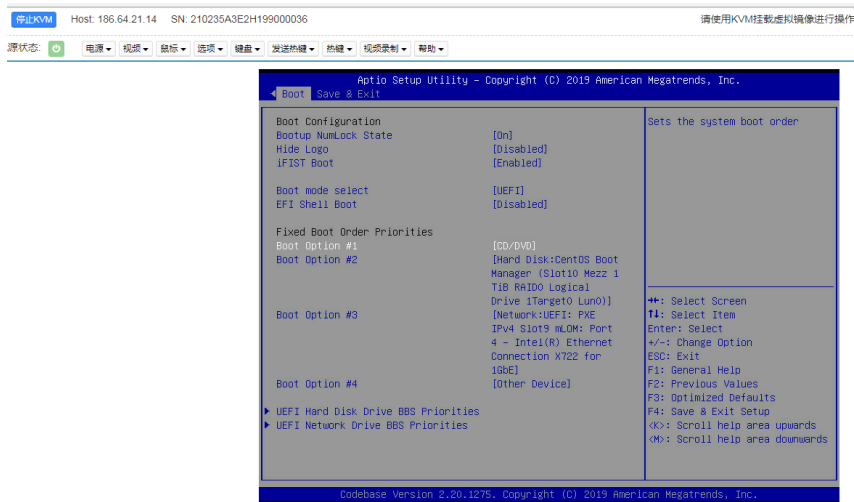


进入 BIOS 界面后, 选择 boot 界面, 该界面 Boot mode select 模式更改为'legacy',如图 2-4 所示。

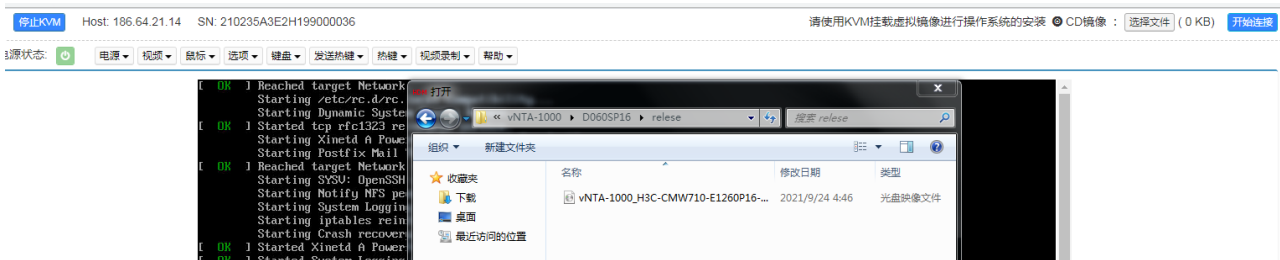
图2-4



如下图 第一启动项更改为 CD/DVD，第二启动项更改为硬盘启动，最后保存配置



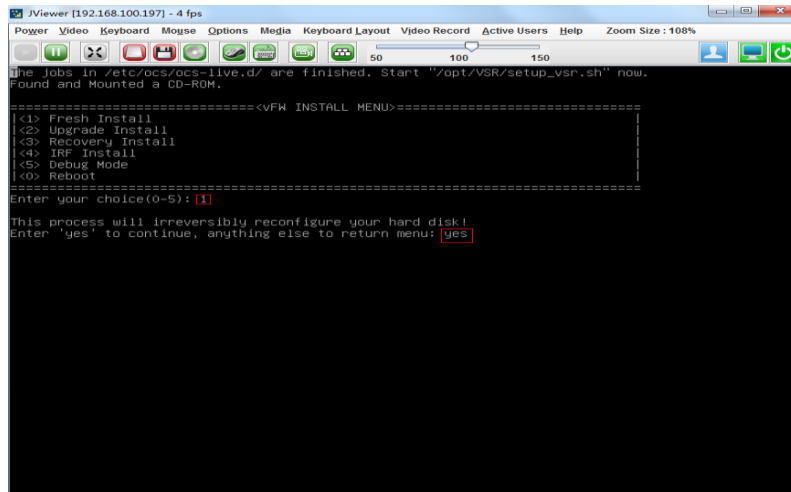
(6) 点击左上角选择文件--选中需要安装的 ISO 文件—开始连接，连接虚拟机的 CD 设备到 CSAP-vNTA-1000 的安装 ISO 文件上，等待虚拟机自动读取安装映像，如下图



2. 安装 CSAP-NTA-V1000

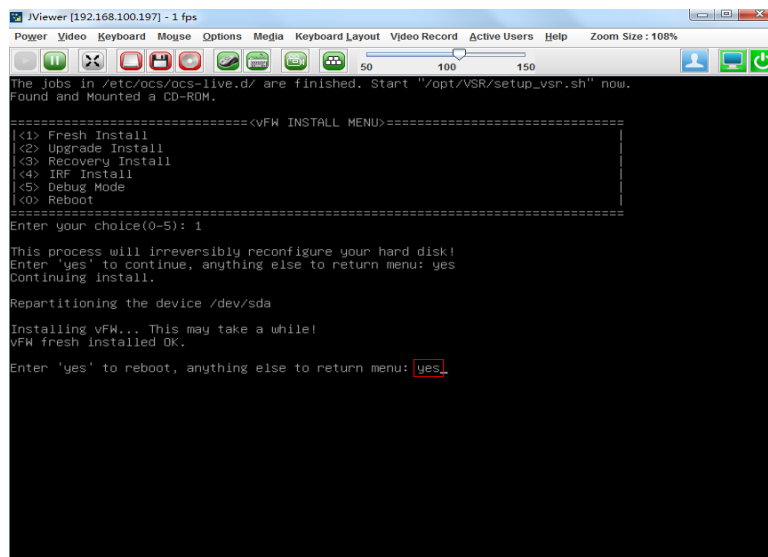
(1) 服务器重启后，系统加载 ISO 文件，进入安装界面。选择<1>进行安装，并输入“yes”确认，系统将会自动完成安装，如图 2-5 所示。安装时间大约需要二十分钟左右。

图 2-5 安装启动界面



(2) 输入“yes”重启系统，完成 CSAP-NTA-V1000 的安装，如图 2-6 所示。服务器重启时间较长，大约需要五六分钟。

图 2-6 重启系统



说明

安装完成后，在设备上执行 `display version` 命令后，有可能出现显示的可用 CPU 数量仅为 1 的情况。可以通过在 BIOS 中配置 `disable x2apic` 来使可用 CPU 数量显示正确。具体方法：在 BIOS 界面选择 "Advanced"（高级）> "CPU Configuration"（CPU 配置）> "x2APIC" > "Disabled"（禁用）。

弹出图 2-7 界面后，直接按“Enter”键。重启系统后，完成 vNTA-1000 安装。

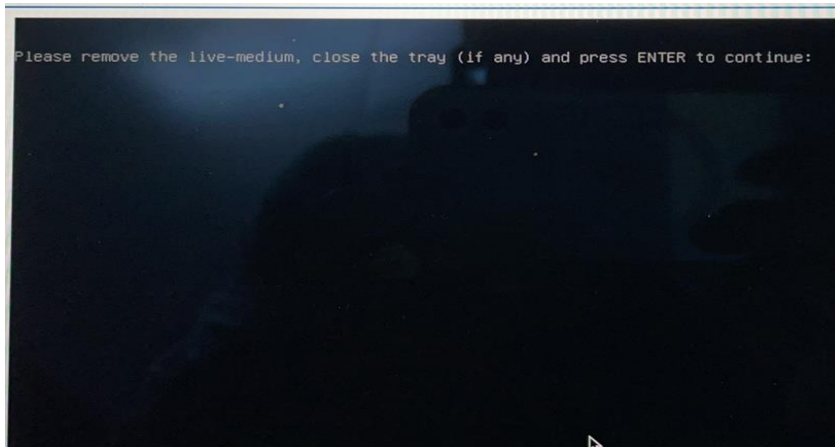


图 2-7

2.2.2 配置管理口地址

进入系统后,选择一个管理接口配置 IP 地址、管理方式以及缺省路由并将管理口加入 management,安全域内保存配置,如下图所示。探针默认密码: admin/admin

图 2-8 配置网络

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]int GigabitEthernet 1/0
[H3C-GigabitEthernet1/0]ip address 186.8.0.160 24
[H3C-GigabitEthernet1/0]qu
[H3C]ip route-static 0.0.0.0 0 186.8.0.1
[H3C]security-zone name Management
[H3C-security-zone-Management]import interface GigabitEthernet 1/0
[H3C-security-zone-Management]qu
[H3C]save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/SWAN-Basic-Managerb390af66-1869-4b88-9ea2-37be619bb765.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/SWAN-Basic-Managerb390af66-1869-4b88-9ea2-37be619bb765.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to device successfully.
[H3C]
```

注意: 配置管理口的接口,不用再加入黑洞,否则会导致网络不通。

3 在虚拟机上安装 CSAP-vNTA-200

CSAP-NTA-V200 安装并运行在服务器的虚拟机上,支持多种虚拟平台。

3.1 安装环境

3.1.1 硬件环境

CSAP-NTA-V200 对虚拟机的最低配置需求如[表 3-1](#)所示。

表3-1 硬件环境

项目	需求
处理器	至少需要配置1个vCPU
内存	<ul style="list-style-type: none">1 vCPU (主频 \geq 2.0 GHz): 2GB 及以上4 vCPU (主频 \geq 2.0 GHz): 4GB 及以上8 vCPU (主频 \geq 2.0 GHz): 8GB 及以上
硬盘	1个vHD, 8GB
网卡	至少2个虚拟网卡,最大支持16个虚拟网卡
虚拟网卡类型	<ul style="list-style-type: none">E1000 (VMware ESXi, Linux KVM)

项目	需求
	<ul style="list-style-type: none"> • VMXNET3 (VMware ESXi) • VirtIO (Linux KVM, H3C CAS) • Interl 82599 VF (VMware ESXi, Linux KVM) Interl x710 VF (Linux KVM)

3.1.2 软件环境

CSAP-NTA-V200 支持的虚拟化平台如表 3-2 所示。

表3-2 软件环境

虚拟化平台	平台软件版本
VMware ESXi	VMware ESXi 4.1, 5.0, 5.1, 5.5
Linux KVM	Linux KVM (Linux Kernel > 2.6.25), the recommended Linux distributions: <ul style="list-style-type: none"> • CentOS 7 • Ubuntu 12.10 • RedHat Enterprise Linux (RHEL) 6.3 • Suse Server 11SP2
H3C CAS	H3C CAS 2.0

3.2 在VMware平台安装CSAP-NTA-V200

在 VMware 平台上，CSAP-NTA-V200 可以通过以下三种方式进行安装：

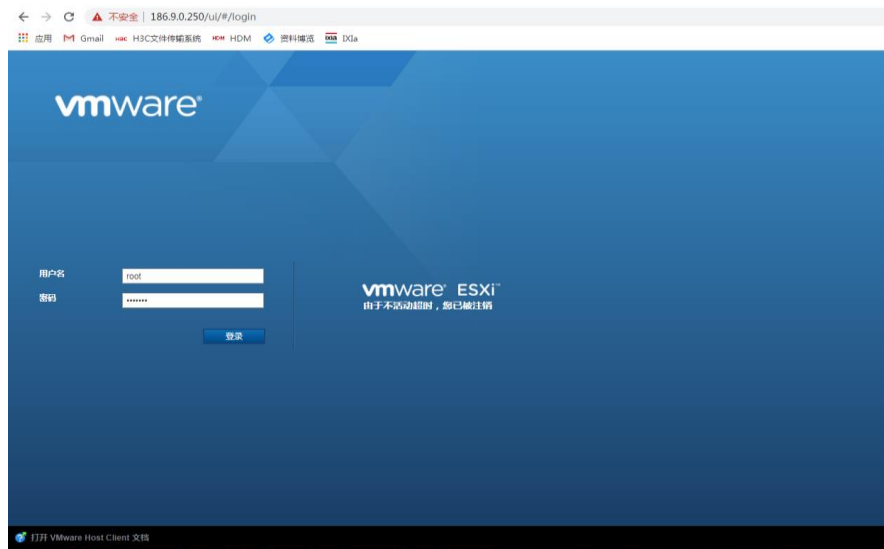
- [通过 ISO 安装 CSAP-NTA-V200](#)
- [通过 PXE 方式安装 CSAP-NTA-V200](#)
- [通过 PXE 无人值守方式安装 CSAP-NTA-V200](#)

3.2.1 通过 ISO 安装 CSAP-NTA-V200

1. 新建虚拟机

- (1) 使用浏览器打开输入安装 VMware 平台时创建的 IP，如：<https://186.9.0.250/ui/#/login>。进入 VMware 云计算管理平台登录界面，如下图所示。输入登录的用户名、密码，点击<登录>按钮，用户名和密码为安装 VMware 平台时，创建的用户名和密码。

图3-1 登录虚拟机服务器

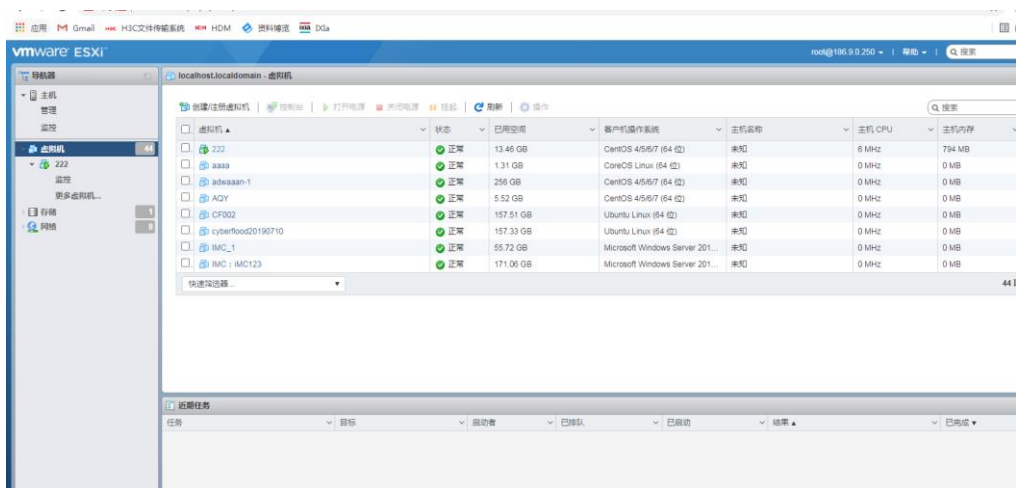


 说明

- VMware 虚拟机服务器的登录用户名及密码为安装 VMware 平台时，输入的用户名、密码。
- 登录过程中有安全证书告警界面出现时，请点击<忽略>按钮，忽略证书界面信息。
- VMware 平台安装过程见附录 8

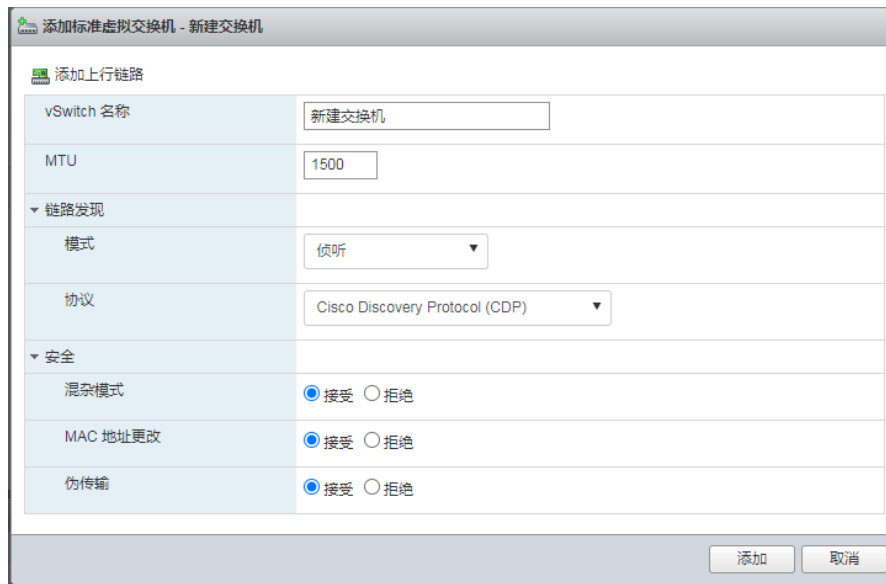
登录成功后，会出现图 3-2 所示界面。

图3-2 成功登录虚拟机服务器



(2) 添加虚拟交换机。选择网络-虚拟交换机-添加，**注意：网卡模式要设置混杂模式**，如下图

图3-3 创建虚拟网卡



(3) 建立存储池。选择存储-数据存储-新建，如图



(4) 选择[文件 > 新建]菜单，开始新建一个虚拟机，进入图 3-4 所示配置界面。进下图所示配置界面。操作系统系列选择其他，系统版本选择“其他（32 位）”然后点击<下一步>。

图3-4 创建一个新的虚拟机



- (5) 为虚拟机分配 CPU 的数量，然后点击<下一步>，如[图 3-5](#)所示。至少需要配置 1 个 vCPU（主频不小于 2.0GHz）。如果是多核的情况下，例如 4 核，1*2 的划分和 4*4 的划分效果是一样的。

图3-5 指定虚拟机 CPU 的分配数量



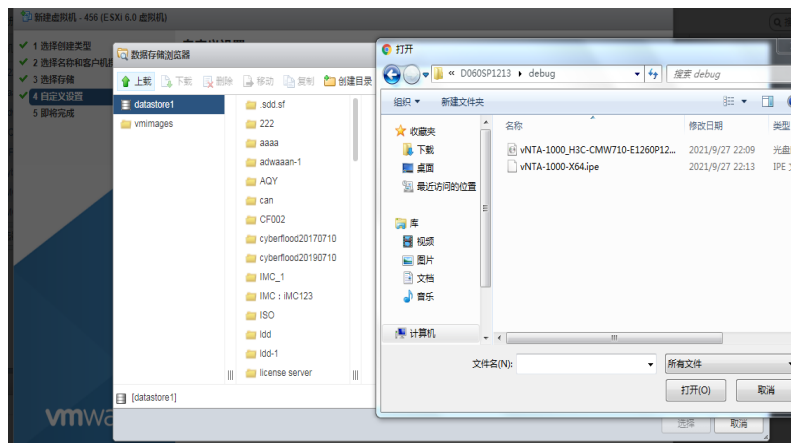
- (6) 选择虚拟机的内存分配数量，然后点击<下一步>。虚拟机的内存需要至少配置 2GB。
- (7) 选择虚拟机的网卡分配数量，然后点击<下一步>，如[图 3-6](#)所示。需要按照至少 2 个虚拟网卡，最大支持 16 个虚拟网卡来配置。增加网卡时，选择最上面一行添加网卡适配器。**注意：**不同的网卡需要选择不同的网卡是适配器类型。如果安装完虚拟机识别不到网卡，可修改是配置类型，且网卡模式为混杂模式，见本章的（2）章节。

图3-6 指定虚拟机网卡类型



(8) 添加镜像文件。选择 CD/VCD---数据存储文件---弹出以下界面后选择上载---选择需要安装的 ISO 文件

图3-7 加载镜像



(9) 选上载完镜像文件后，选择镜像文件-点击选择，然后点击<下一步>，如图 3-8 所示。

图3-8 指定使用的硬盘类型



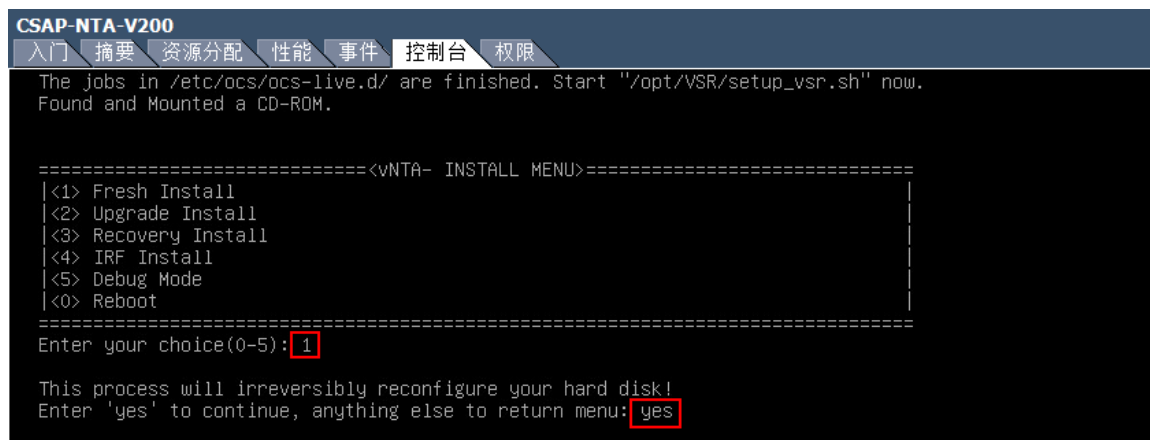
(10) 点击<完成>按钮，完成虚拟机的创建。虚拟机创建成功后，会出现在左侧的设备导航栏中。

(11) 添加 10G 网卡。VMware 添加 10G 网卡与 CAS 平台方法相同，详情请参考 3.4.2 章节中 3.

2. 安装 CSAP-NTA-V200

(1) 虚拟机自动加载安装 ISO 文件，进入安装界面。在安装界面选择<1>进行安装，并输入“yes”确认，如图 3-9 所示。系统将会自动完成安装。

图3-9 安装启动界面



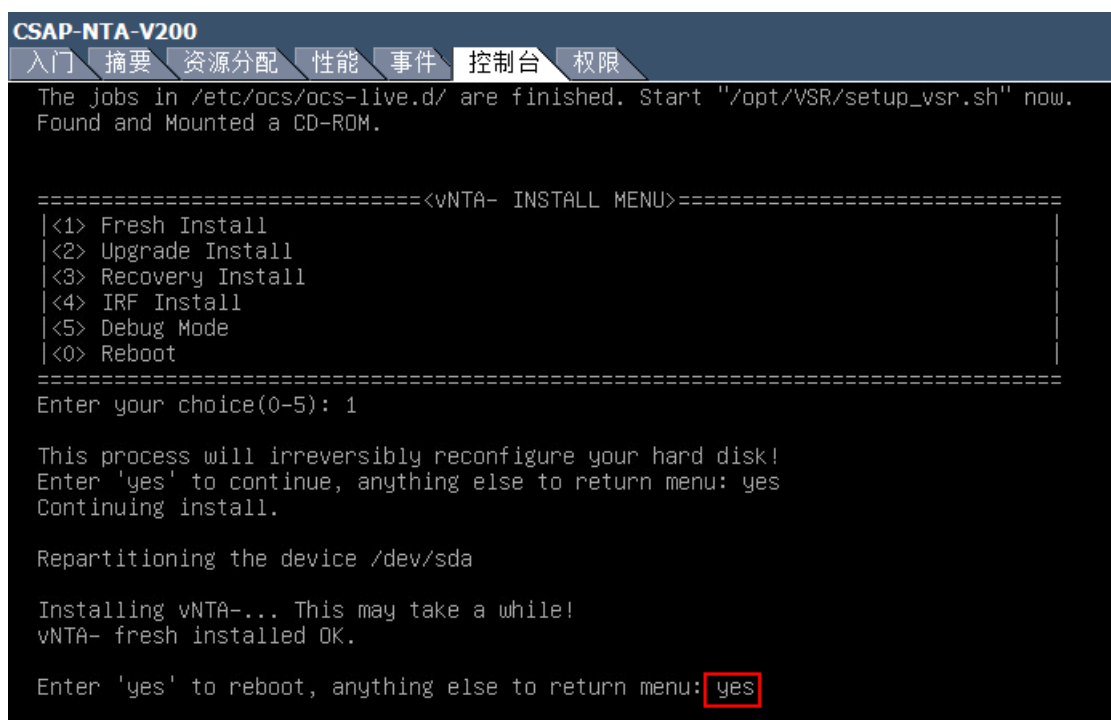
```
CSAP-NTA-V200
入门 摘要 资源分配 性能 事件 控制台 权限
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "/opt/VSR/setup_vsr.sh" now.
Found and Mounted a CD-ROM.

=====<vNTA- INSTALL MENU>=====
|<1> Fresh Install
|<2> Upgrade Install
|<3> Recovery Install
|<4> IRF Install
|<5> Debug Mode
|<0> Reboot
=====
Enter your choice(0-5): 1

This process will irreversibly reconfigure your hard disk!
Enter 'yes' to continue, anything else to return menu: yes
```

(2) 然后输入“yes”重启系统，完成 CSAP-NTA-V200 的安装，如图 3-10 所示。

图3-10 完成 CSAP-NTA-V200 的安装



```
CSAP-NTA-V200
入门 摘要 资源分配 性能 事件 控制台 权限
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "/opt/VSR/setup_vsr.sh" now.
Found and Mounted a CD-ROM.

=====<vNTA- INSTALL MENU>=====
|<1> Fresh Install
|<2> Upgrade Install
|<3> Recovery Install
|<4> IRF Install
|<5> Debug Mode
|<0> Reboot
=====
Enter your choice(0-5): 1

This process will irreversibly reconfigure your hard disk!
Enter 'yes' to continue, anything else to return menu: yes
Continuing install.

Repartitioning the device /dev/sda

Installing vNTA-... This may take a while!
vNTA- fresh installed OK.

Enter 'yes' to reboot, anything else to return menu: yes
```

(3) 进入探针默认密码 admin/admin。

3.2.2 通过 PXE 方式安装 CSAP-NTA-V200



提示

本章节只给出 PXE Client 的安装方法，PXE Server 的搭建方法请参见“10 附录 D: PXE Server 搭建”或者自行网络查找。

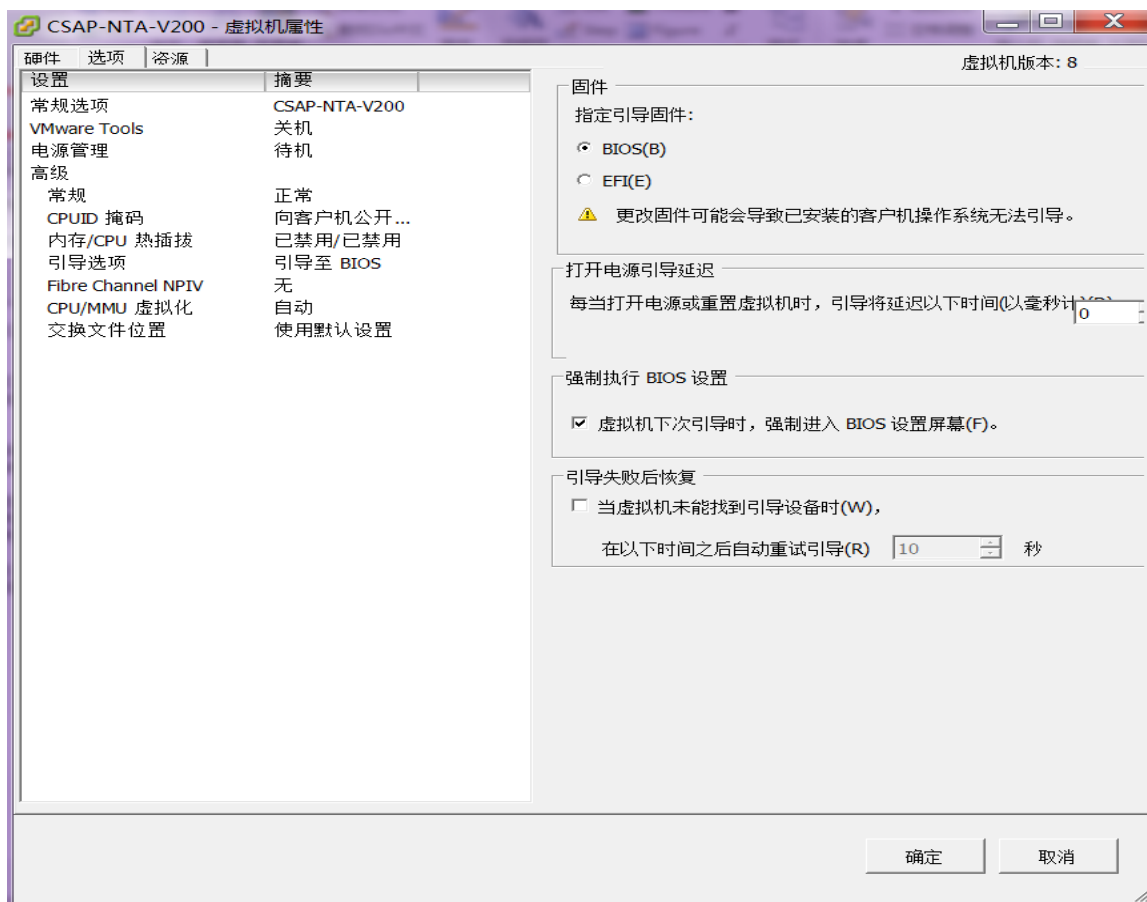
1. 新建虚拟机


新建虚拟机的方法请参见“3.2.1 1. 新建虚拟机”。

2. 设置虚拟机从网络启动

(1) 在左侧的设备导航栏中选中新建的虚拟机，单击右键选择“编辑虚拟机设置”，然后点击“选项”页签，如图 3-11 所示。在“强制 BIOS 设置”选项前打勾，点击<确定>。

图3-11 选择强制进入 BIOS 设置

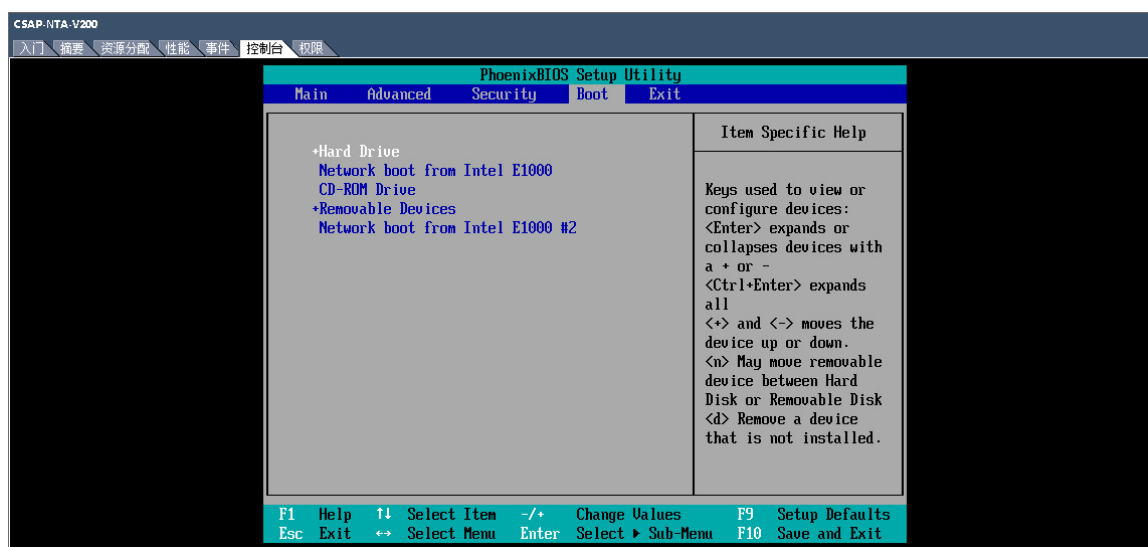


(2) 在设备导航栏中选中新建的虚拟机，点击  启动虚拟机。进入控制台选择 Boot 页签，设置第二优先通过 Network boot from xx 接口启动，如图 3-12 所示，然后按 F10 保存配置并退出。



请保证选择接口的物理链路到 PXE Server 是可达的。本节以 Network boot from Intel E1000 为例。

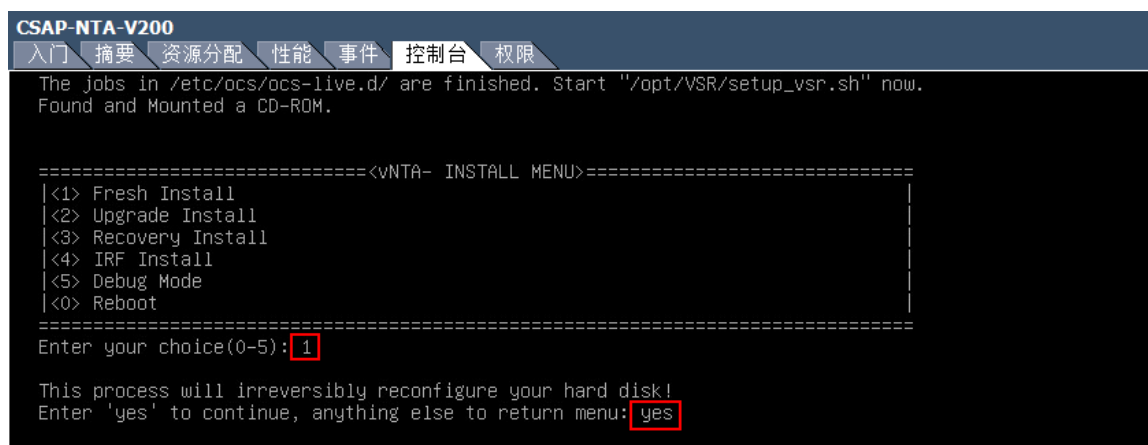
图3-12 设置第二优先通过 Network 启动



3. 安装 CSAP-NTA-V200

- (1) 虚拟机自动从 PXE Server 下载所需文件，进入安装界面。在安装界面选择<1>进行安装，并输入“yes”确认，如图 3-13 所示。系统将会自动完成安装。

图3-13 安装启动界面



- (2) 然后输入“yes”重启系统，完成 CSAP-NTA-V200 的安装，如图 3-14 所示。

图3-14 完成 CSAP-NTA-V200 的安装

```
CSAP-NTA-V200
入门 摘要 资源分配 性能 事件 控制台 权限
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "/opt/VSR/setup_vsr.sh" now.
Found and Mounted a CD-ROM.

=====<vNTA- INSTALL MENU>=====
|<1> Fresh Install
|<2> Upgrade Install
|<3> Recovery Install
|<4> IRF Install
|<5> Debug Mode
|<0> Reboot
=====
Enter your choice(0-5): 1

This process will irreversibly reconfigure your hard disk!
Enter 'yes' to continue, anything else to return menu: yes
Continuing install.

Repartitioning the device /dev/sda

Installing vNTA-... This may take a while!
vNTA- fresh installed OK.

Enter 'yes' to reboot, anything else to return menu: yes
```

(3) 进入系统默认用户名和密码：admin/admin。

3.2.3 通过 PXE 无人值守方式安装 CSAP-NTA-V200



提示

本章节只给出 PXE Client 无人值守的安装方法，PXE Server 的搭建方法请参见“10 附录 D：PXE Server 搭建”或者自行网络查找。

PXE Server 搭建时，修改 syslinux 配置参数 `ocs_live_run="/opt/VSR/setup_vsr_pxe.sh unattended fresh "`。

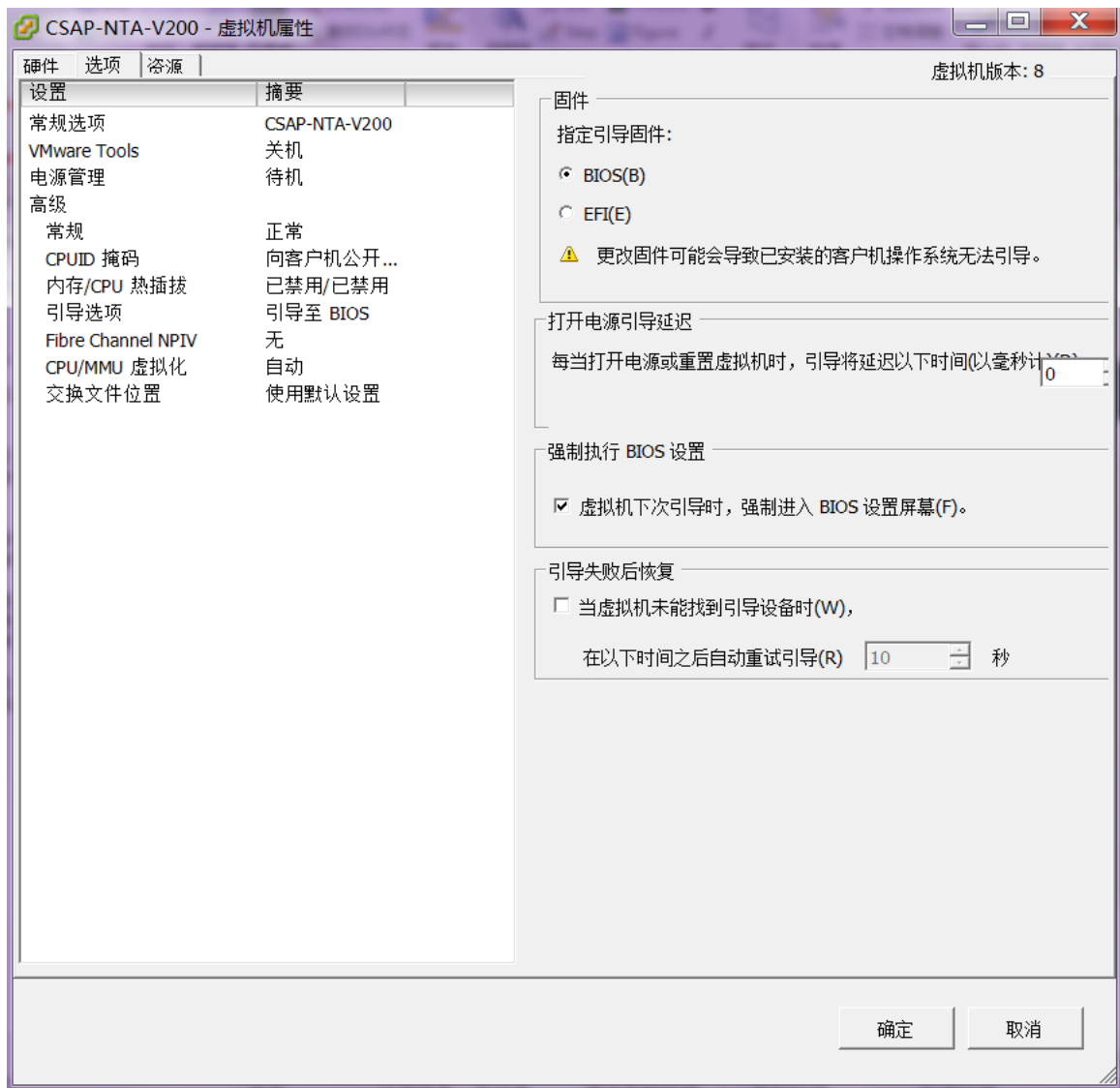
1. 新建虚拟机


新建虚拟机的方法请参见“[3.2.1 1. 新建虚拟机](#)”。

2. 设置虚拟机从网络启动

(1) 在左侧的设备导航栏中选中新建的虚拟机，单击右键选择“编辑虚拟机设置”，然后点击“选项”页签，如[图 3-11](#)所示。在“强制 BIOS 设置”选项前打勾，点击<确定>。

图3-15 选择强制进入 BIOS 设置

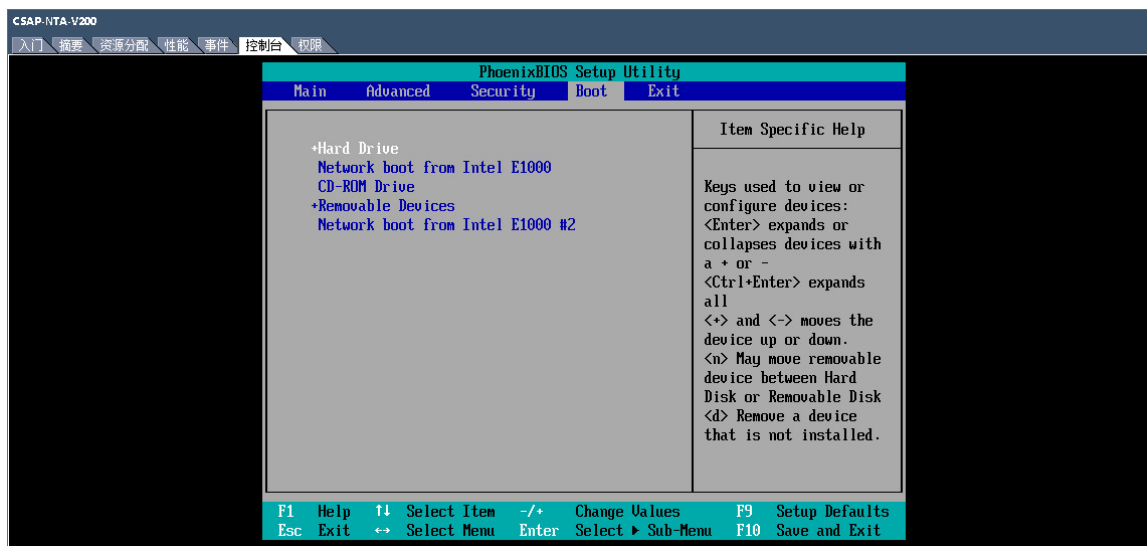


- (2) 在设备导航栏中选中新建的虚拟机，点击  启动虚拟机。通过 Console 口可以选择 Boot 页签，设置第二优先通过 Network boot from xx 接口启动，如图 3-12 所示，然后按 F10 保存配置并退出。

 注意

请确定选择接口的物理链路到 PXE Server 是可达的。本节以 Network boot from Intel E1000 为例。

图3-16 设置第二优先通过 Network 启动



3. 安装 CSAP-NTA-V200

虚拟机自动从 PXE Server 下载所需文件，系统将会自动完成安装。

进入探针默认用户名和密码：admin/admin。

3.3 在KVM平台安装CSAP-NTA-V200

3.3.1 通过 ISO 安装 CSAP-NTA-V200

1. 新建虚拟机

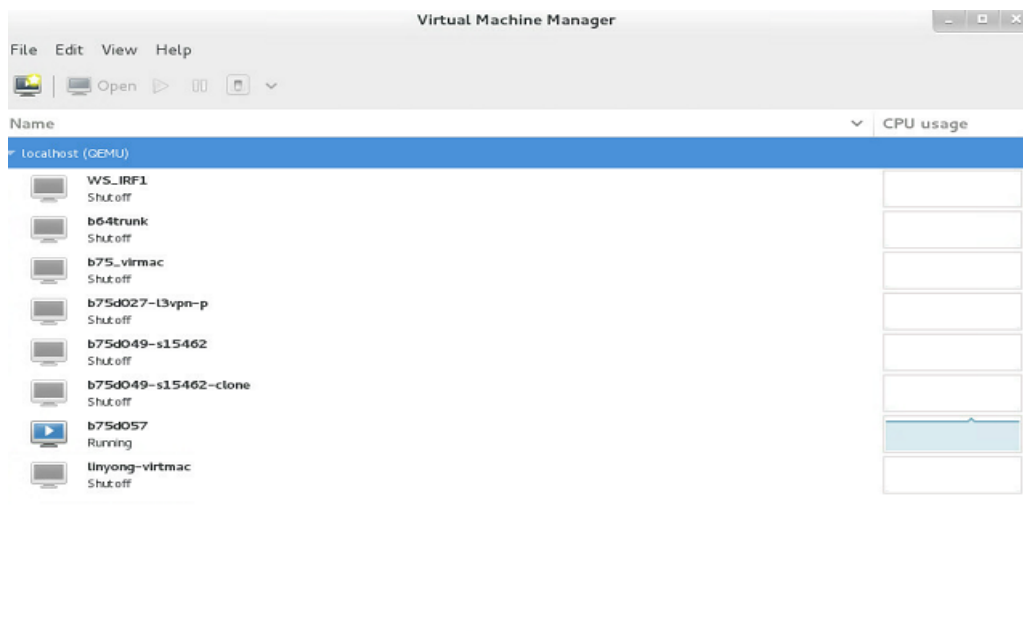
(1) 运行 Virtual Machine Manager 软件。运行成功之后会出现管理界面，如[图 3-17](#)所示。



注意

KVM 平台安装过程见附录 8。

图3-17 Virtual Machine Manager 管理界面



 说明

Virtual Machine Manager 是图形化的管理软件且为 Linux 操作系统的选装软件。请在安装宿主机 Linux 操作系统的时候启用图形化管理界面，并选择安装 Virtual Machine Manager 软件。


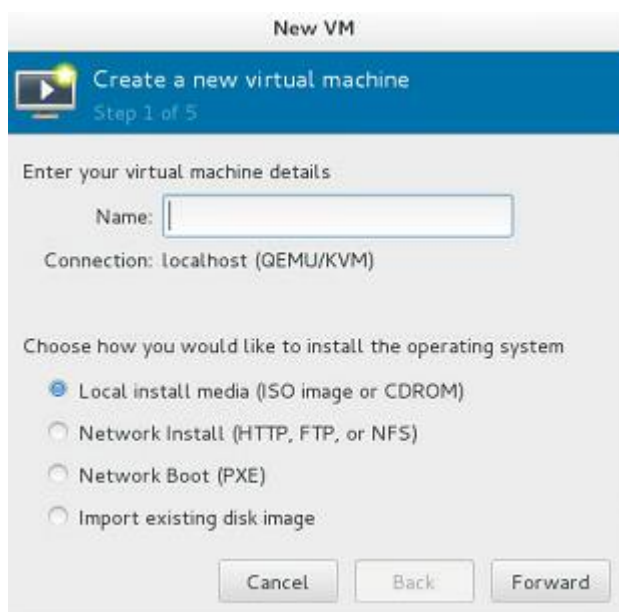
- (2) 点击  图标，开始新建一个虚拟机。在图 3-18 所示的配置界面，为新建的虚拟机创建设备名，然后选择从本地安装，点击<Forward>。

图3-18 创建一个新的虚拟机



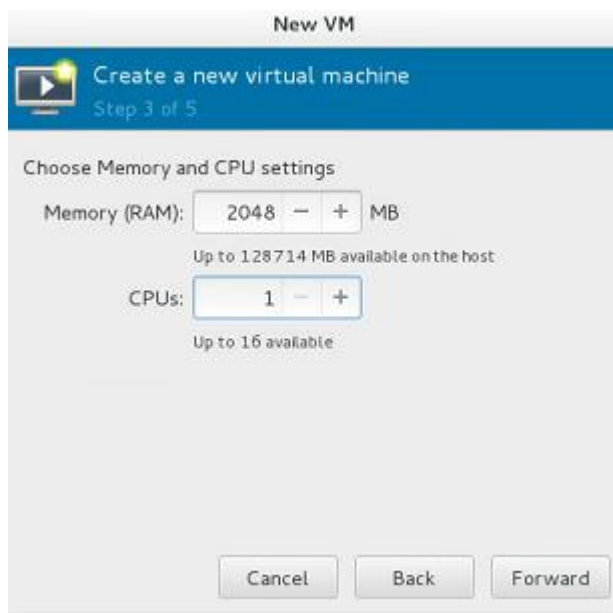
- (3) 在图 3-19 所示界面中选择使用 ISO 映像，点击<Browse>，选择安装 CSAP-NTA-V200 的 ISO 文件后，点击<Forward>。

图3-19 选择安装 CSAP-NTA-V200 的 ISO 文件



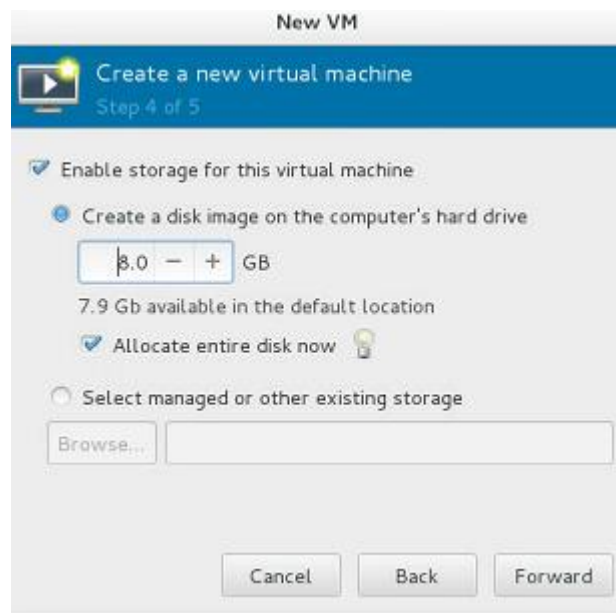
- (4) 选择虚拟机 CPU 和内存的分配数量，然后点击<Forward>，如图 3-20 所示。CPU 至少需要配置 1 个 vCPU（主频不小于 2.0GHz），内存至少需要配置 2GB。

图3-20 指定虚拟机 CPU 和内存的分配数量



- (5) 选择虚拟机的硬盘空间分配数量，然后点击<Forward>，如图 3-21 所示。至少需要配置 1 个 vHD，8GB。

图3-21 指定虚拟机硬盘空间的分配数量



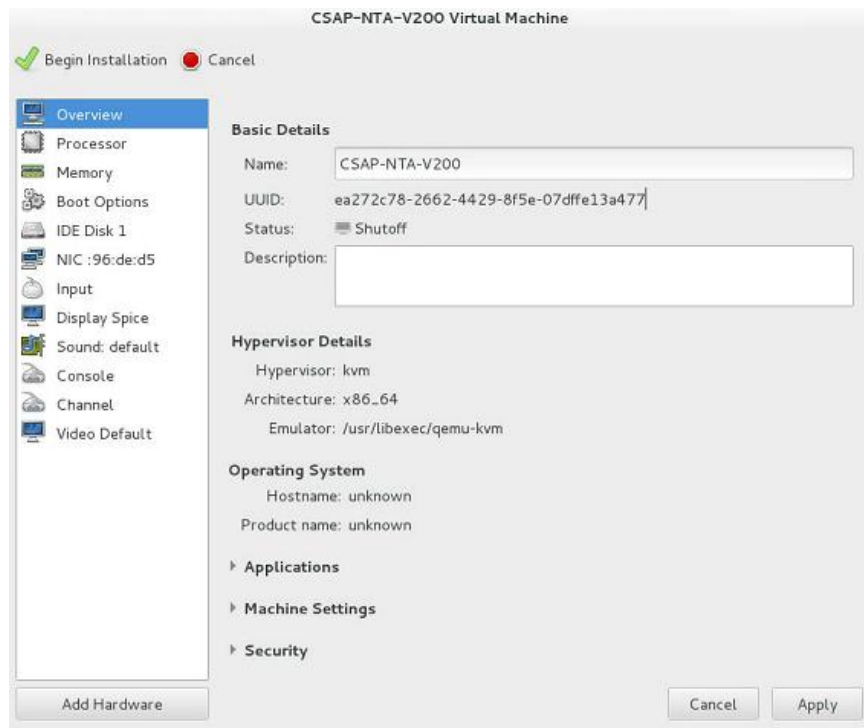
- (6) 其它高级选项的配置，勾选“Customize configuration before install”选项，然后点击<完成>，如图3-22所示。

图3-22 其它高级选项配置



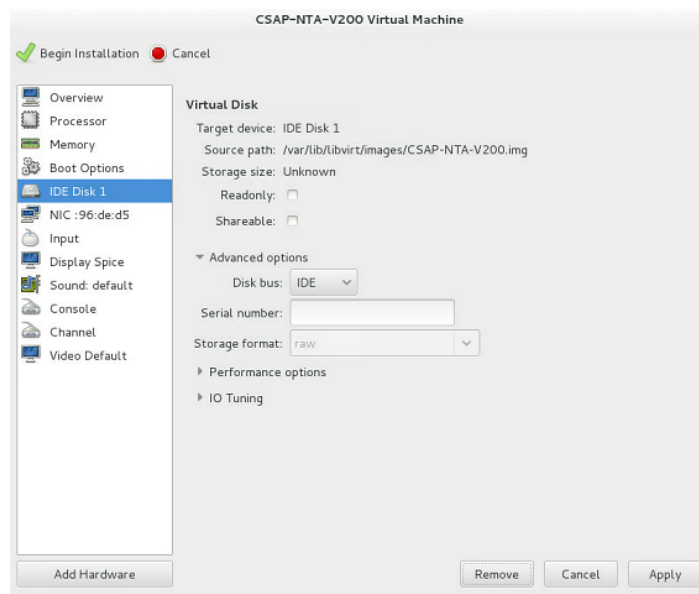
- (7) 由于勾选了“Customize configuration before install”在安装前自定义配置，完成虚拟机的基本配置后，会出现自定义配置界面，如图 3-23 所示。

图3-23 自定义配置界面



- (8) 在自定义配置界面左侧的列表框中选择<Disk 1>，进入磁盘配置界面。将磁盘总线（Disk bus）指定成 IDE，并点击<Apply>，如图 3-24 所示。

图3-24 配置磁盘总线



- (9) 在自定义配置界面左侧的列表框中选择<NIC>，进入网卡配置界面。有两种配置方式，如图 3-25 或图 3-26 所示。建议使用方式二设置网卡。其中 br0 的创建方法可参见[错误!未找到引用源。错误!未找到引用源。](#)。配置好后点击<Apply>。

图3-25 配置网卡方式一

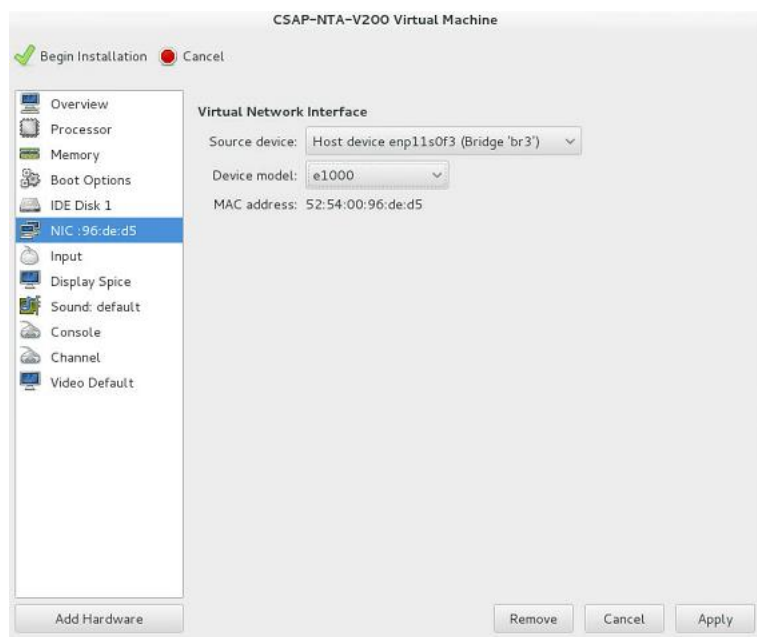
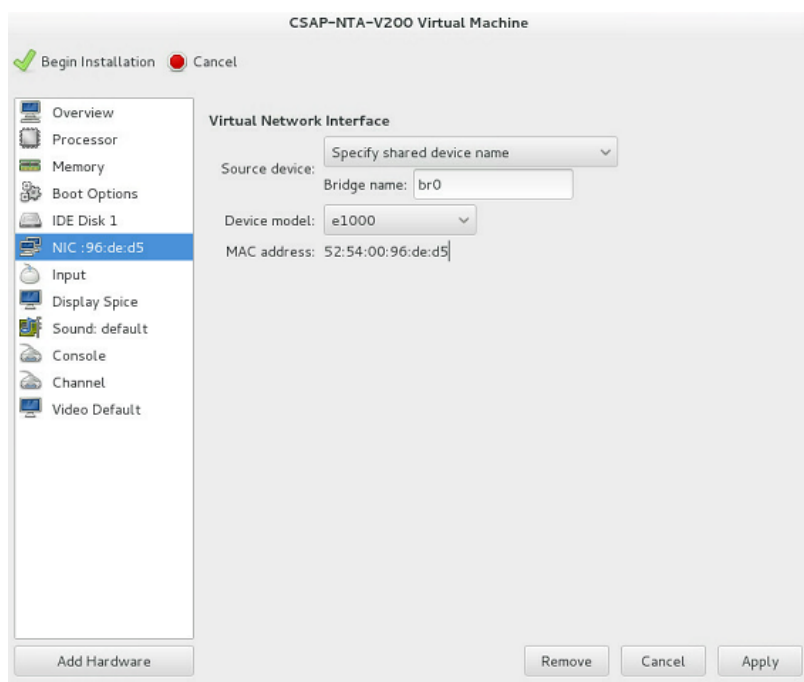
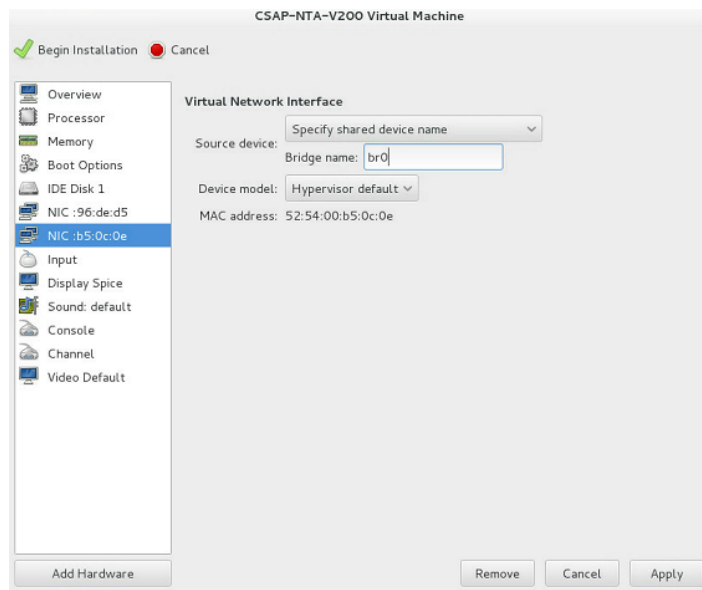


图3-26 配置网卡方式二



- (10) 要正常运行 CSAP-NTA-V200，至少需要按照两个虚拟网卡来配置，而虚拟机基本配置中只有一块网卡。要添加新网卡，可以在客户化配置界面左下角点击<Add Hardware>，进入添加新硬件配置界面，然后选择网络设备，并配置网卡的属性，如图 3-27 所示。

图3-27 添加新网卡



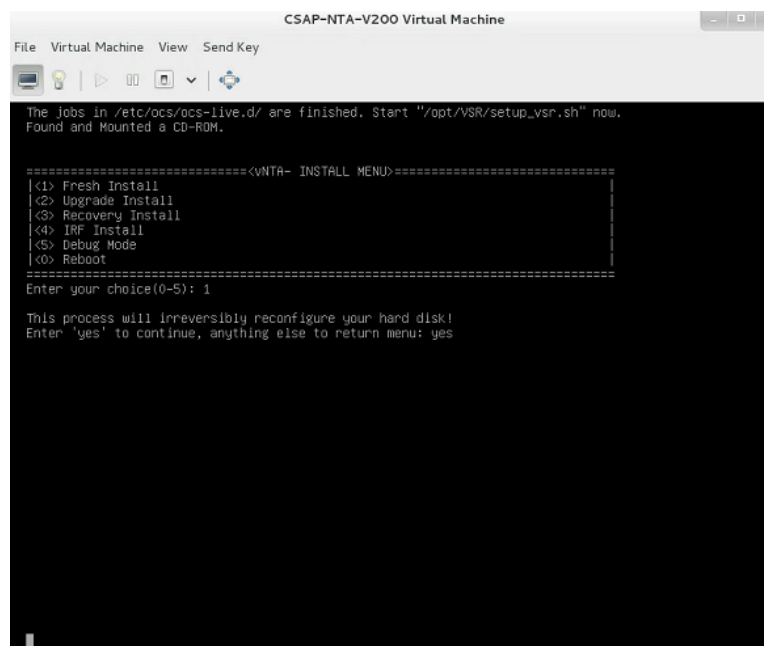
(11) 点击<Begin Installation>, 完成虚拟机的创建。新创建的虚拟机会自动运行, 并进入 CSAP-NTA-V200 的安装过程。

(12) 添加 10G 网卡。KVM 添加 10G 网卡与 CAS 平台方法相同, 详情请参考附录 9

2. 安装 CSAP-NTA-V200

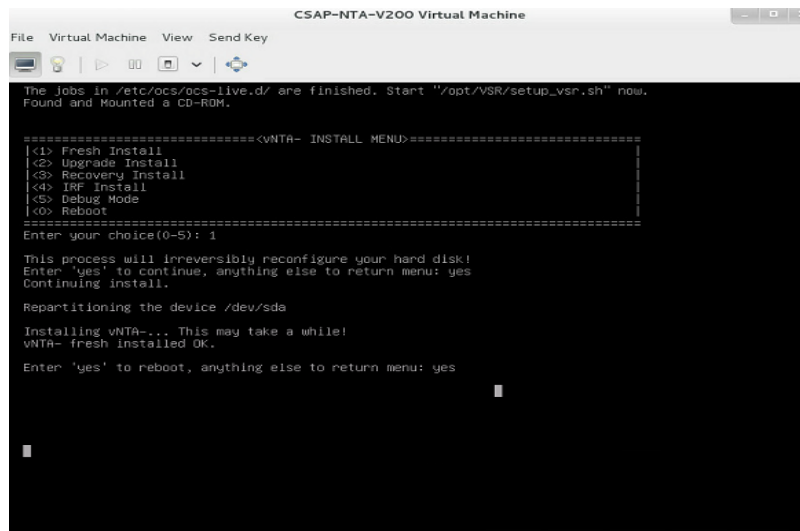
(1) 虚拟机系统从 ISO 启动, 并直接进入安装界面, 安装界面如图 3-28 所示。选择<1>进行安装, 并输入“yes”确认后, 系统将会自动完成安装。

图3-28 安装启动界面



(2) 输入“yes”重启系统, 完成 CSAP-NTA-V200 的安装, 如图 3-29 所示。

图3-29 完成 CSAP-NTA-V200 的安装



(3) 进入探针用户名和密码：admin/admin。

3.3.2 通过 PXE 安装 CSAP-NTA-V200



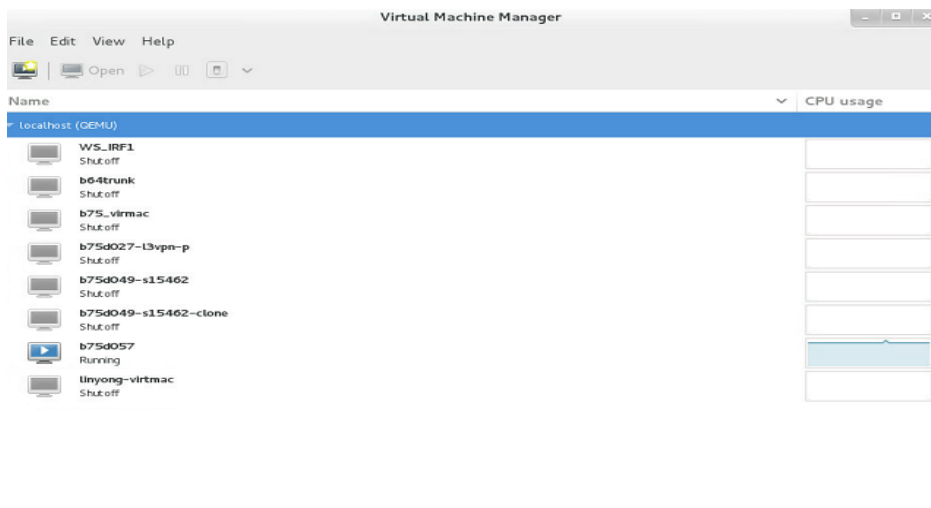
提示

本章节只给出 PXE Client 的安装方法，PXE Server 的搭建方法请参见“9 附录 D: PXE Server 搭建”或者自行网络查找。

1. 新建虚拟机

(1) 运行 Virtual Machine Manager 软件。运行成功之后会出现管理界面，如图 3-30 所示。

图3-30 Virtual Machine Manager 管理界面



 说明

Virtual Machine Manager 是图形化的管理软件且为 Linux 操作系统的选装软件。请在安装宿主机 Linux 操作系统的时候启用图形化管理界面，并选择安装 Virtual Machine Manager 软件。


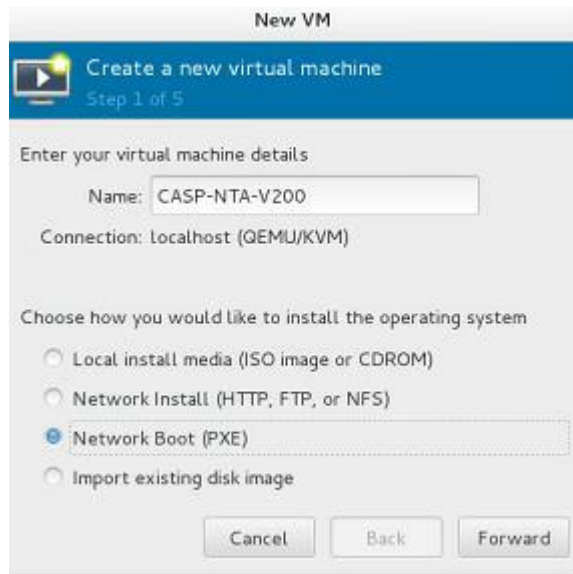
- (2) 点击  图标，开始新建一个虚拟机。在图 3-31 所示的配置界面，为新建的虚拟机创建设备名，然后选择网络引导（PXE），点击<Forward>。

图3-31 创建一个新的虚拟机



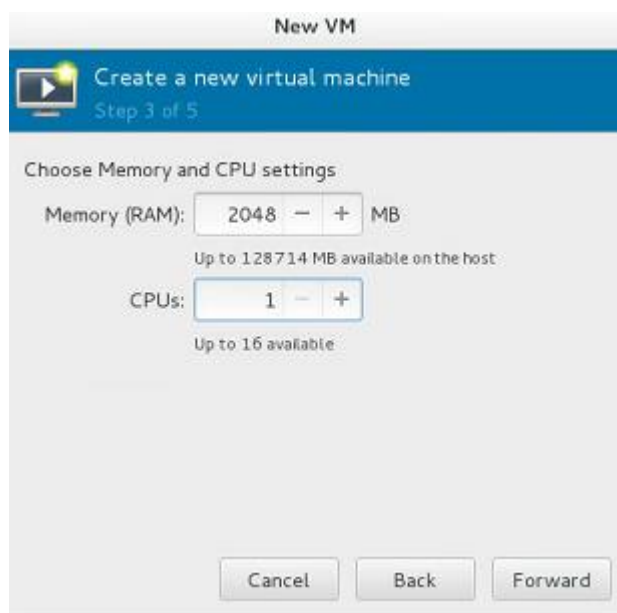
- (3) 在图 3-32 所示界面中选择操作系统和版本后，点击<Forward>。

图3-32 选择操作系统和版本



- (4) 选择虚拟机 CPU 和内存的分配数量，然后点击<Forward>，如[图 3-33](#)所示。CPU 至少需要配置 1 个 vCPU（主频不小于 2.0GHz），内存至少需要配置 2GB。

图3-33 指定虚拟机 CPU 和内存的分配数量



- (5) 选择虚拟机的硬盘空间分配数量，然后点击<Forward>，如[图 3-3434](#)所示。至少需要配置 1 个 vHD，8GB。

图3-34 指定虚拟机硬盘空间的分配数量



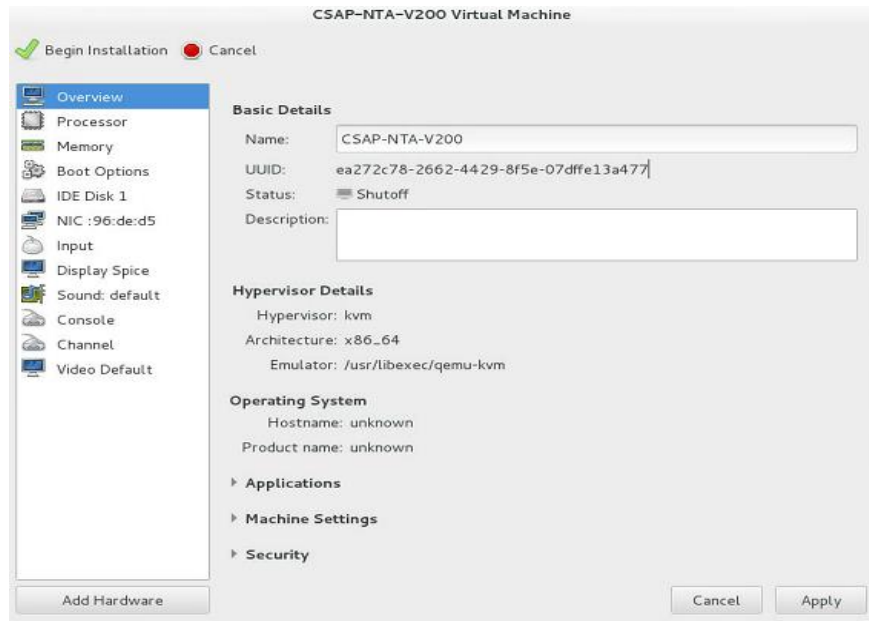
- (6) 其它高级选项的配置，勾选“Customize configuration before install”选项，然后点击<完成>，如图3-35所示。

图3-35 其它高级选项配置



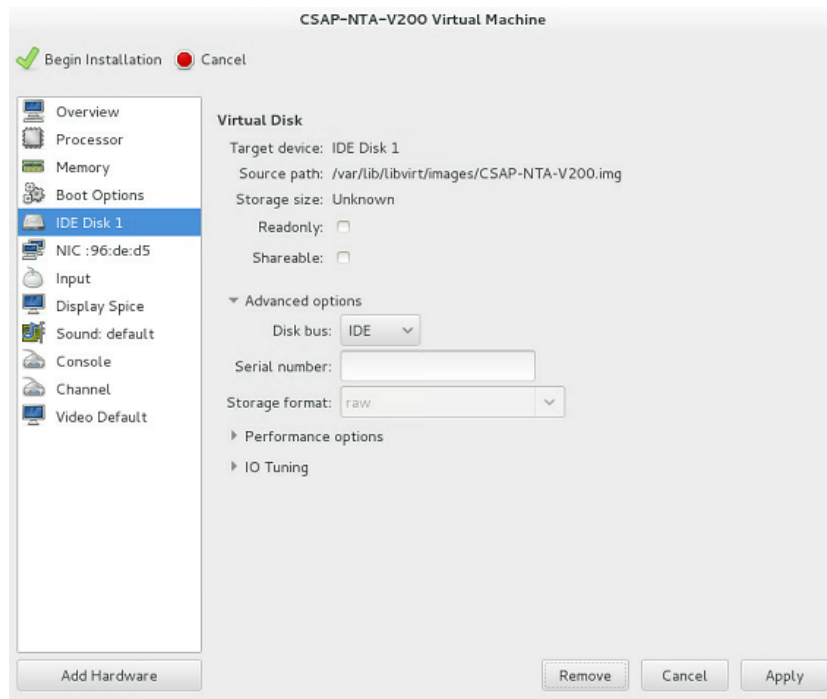
- (7) 由于勾选了“Customize configuration before install”在安装前自定义配置，完成虚拟机的基本配置后，会出现自定义配置界面，如图3-36所示。

图3-36 自定义配置界面



- (8) 在自定义配置界面左侧的列表框中选择<Disk 1>，进入磁盘配置界面。将磁盘总线（Disk bus）指定成 IDE，并点击<Apply>，如图 3-37 所示。

图3-37 配置磁盘总线



- (9) 在自定义配置界面左侧的列表框中选择<NIC>，进入网卡配置界面。有两种配置方式，如图 3-38 或图 3-39 所示。建议使用方式二设置网卡。其中 br0 的创建方法可参见[错误!未找到引用源。错误!未找到引用源。](#)。配置好后点击<Apply>。

图3-38 配置网卡方式一

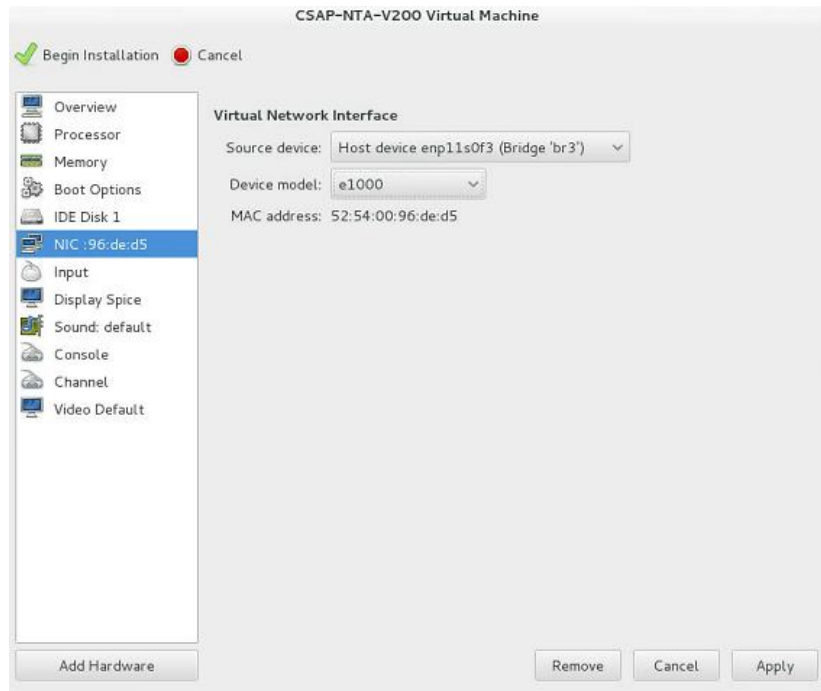
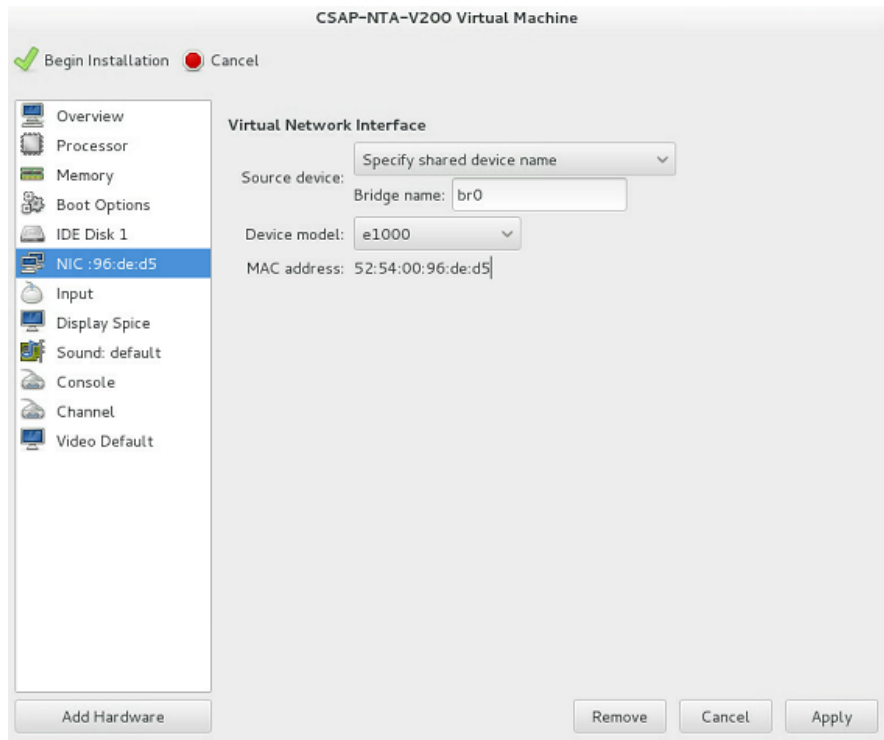
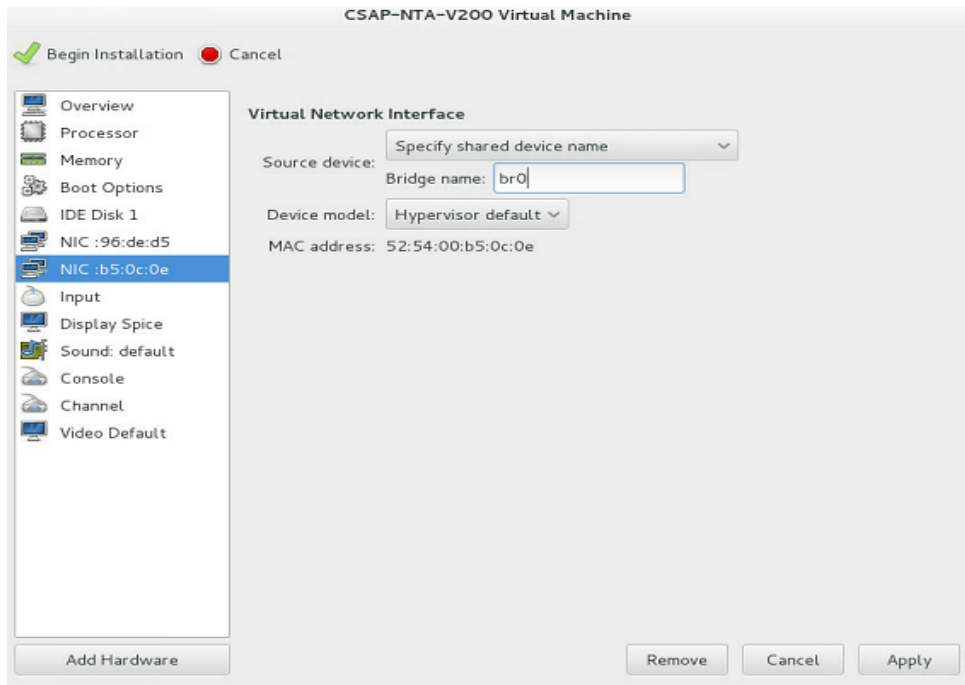


图3-39 配置网卡方式二



(10) 要正常运行 CSAP-NTA-V200，至少需要按照两个虚拟网卡来配置，而虚拟机基本配置中只有一块网卡。要添加新网卡，可以在客户化配置界面左下角点击<Add Hardware>，进入添加新硬件配置界面，然后选择网络设备，并配置网卡的属性，如[图 3-40](#)所示。

图3-40 添加新网卡

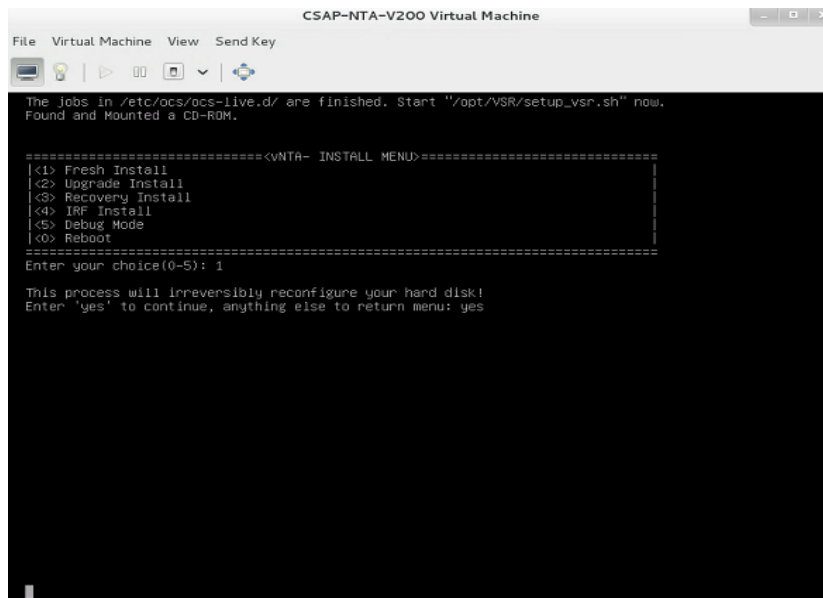


(11) 点击<Begin Installation>, 完成虚拟机的创建。新创建的虚拟机会自动运行, 并进入 CSAP-NTA-V200 的安装过程。

2. 安装 CSAP-NTA-V200

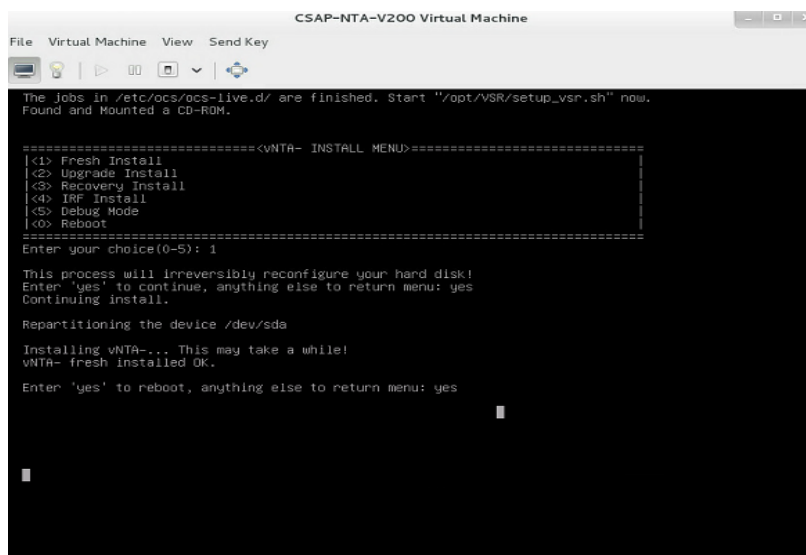
(1) 虚拟机自动从 PXE Server 下载所需文件, 并直接进入安装界面, 安装界面如图 3-41 所示。选择<1>进行安装, 并输入“yes”确认后, 系统将会自动完成安装。

图3-41 安装启动界面



(2) 输入“yes”重启系统, 完成 CSAP-NTA-V200 的安装, 如图 3-42 所示。

图3-42 完成 CSAP-NTA-V200 的安装



(3) 进入系统默认用户名和密码：admin/admin。

3.3.3 通过 PXE 无人值守方式安装 CSAP-NTA-V200



提示

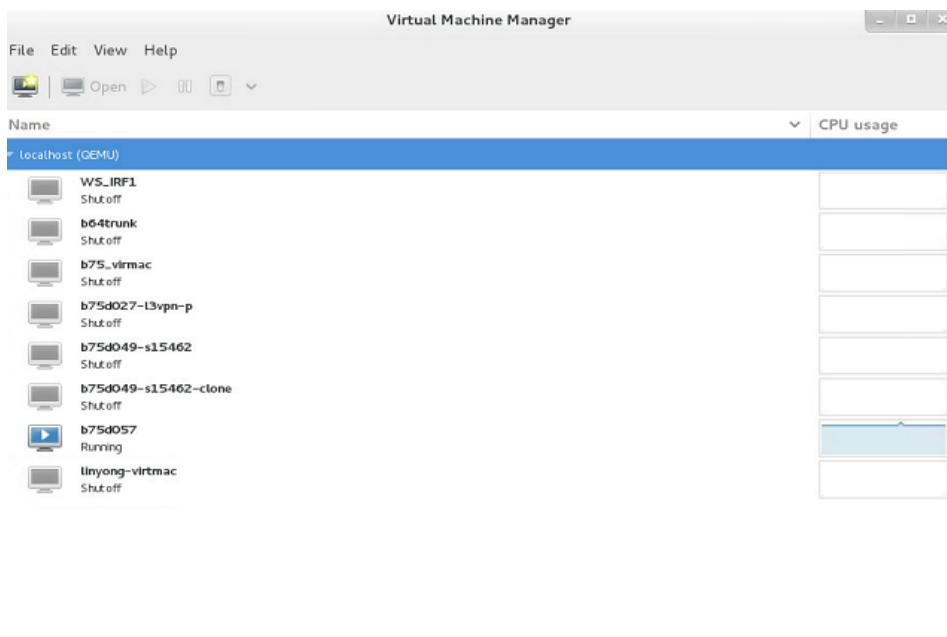
本章节只给出 PXE Client 的安装方法

PXE Server 搭建时，修改 syslinux 配置参数 `ocs_live_run="/opt/VSR/setup_vsr_pxe.sh unattended fresh "`。

1. 新建虚拟机

(1) 运行 Virtual Machine Manager 软件。运行成功之后会出现管理界面，如[图 3-30](#)所示。

图3-43 Virtual Machine Manager 管理界面



 说明

Virtual Machine Manager 是图形化的管理软件且为 Linux 操作系统的选装软件。请在安装宿主机 Linux 操作系统的时候启用图形化管理界面，并选择安装 Virtual Machine Manager 软件。


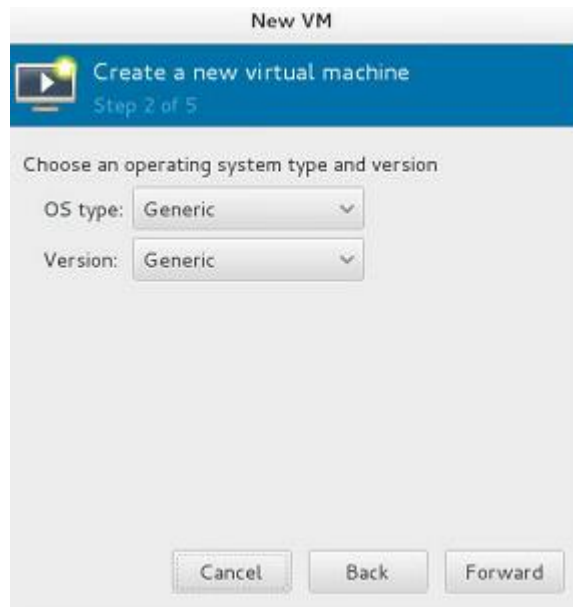
- (2) 点击  图标，开始新建一个虚拟机。在图 3-31 所示的配置界面，为新建的虚拟机创建设备名，然后选择网络引导（PXE），点击<Forward>。

图3-44 创建一个新的虚拟机



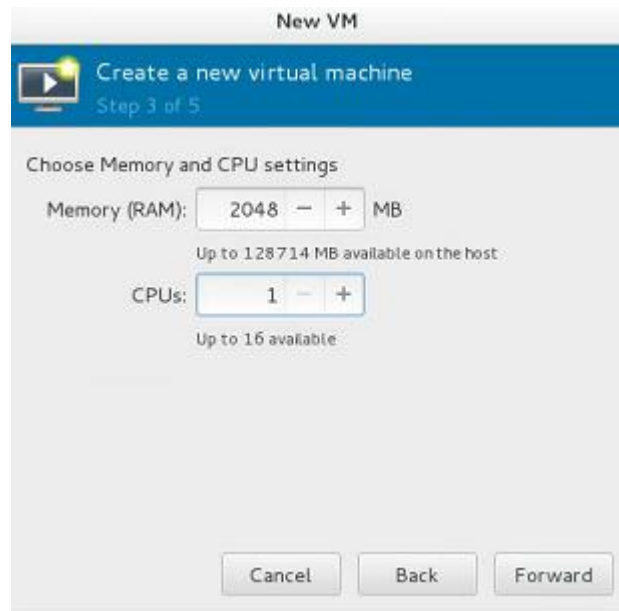
(3) 在图 3-32 所示界面中选择操作系统和版本后，点击<Forward>。

图3-45 选择操作系统和版本



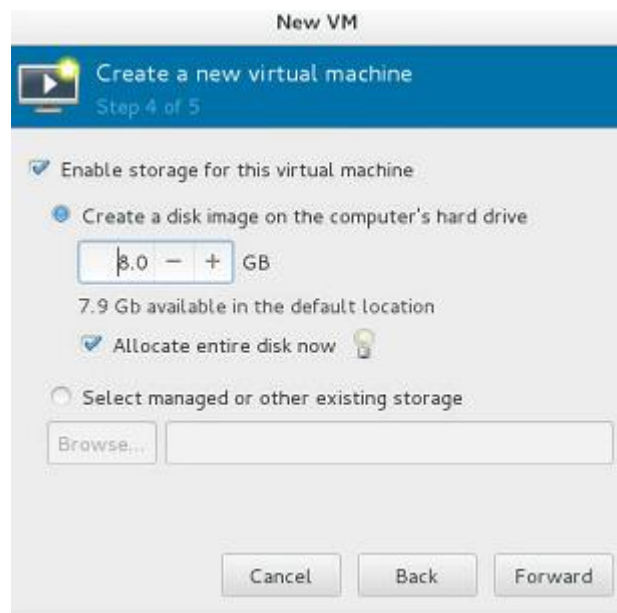
(4) 选择虚拟机 CPU 和内存的分配数量，然后点击<Forward>，如图 3-33 所示。CPU 至少需要配置 1 个 vCPU（主频不小于 2.0GHz），内存至少需要配置 2GB。

图3-46 指定虚拟机 CPU 和内存的分配数量



(5) 选择虚拟机的硬盘空间分配数量，然后点击<Forward>，如图 3-34 所示。至少需要配置 1 个 vHD，8GB。

图3-47 指定虚拟机硬盘空间的分配数量



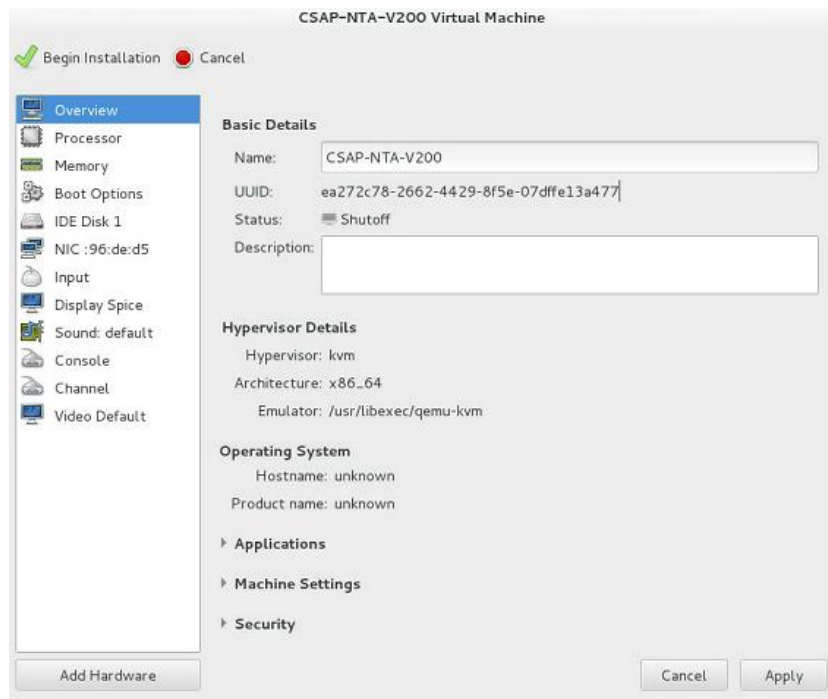
- (6) 其它高级选项的配置，勾选“Customize configuration before install”选项，然后点击<完成>，如图 3-35 所示。

图3-48 其它高级选项配置



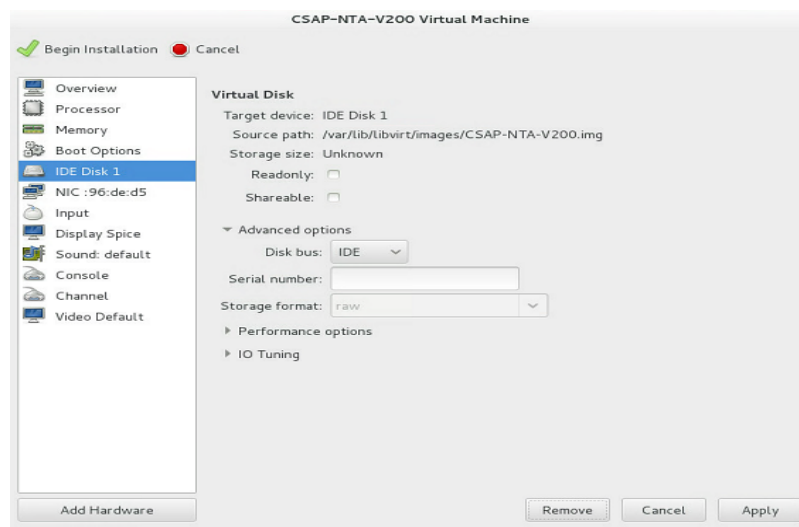
- (7) 由于勾选了“Customize configuration before install”在安装前自定义配置，完成虚拟机的基本配置后，会出现自定义配置界面，如图 3-36 所示。

图3-49 自定义配置界面



- (8) 在自定义配置界面左侧的列表框中选择<Disk 1>，进入磁盘配置界面。将磁盘总线（Disk bus）指定成 IDE，并点击<Apply>，如[图 3-37](#)所示。

图3-50 配置磁盘总线



- (9) 在自定义配置界面左侧的列表框中选择<NIC>，进入网卡配置界面。有两种配置方式，如[图 3-38](#)或[图 3-39](#)所示。建议使用方式二设置网卡。其中 br0 的创建方法可参见[错误!未找到引用源。错误!未找到引用源。](#)。配置好后点击<Apply>。**注意：网卡模式需要设置混杂模式。方法参考 3.2.1**

图3-51 配置网卡方式一

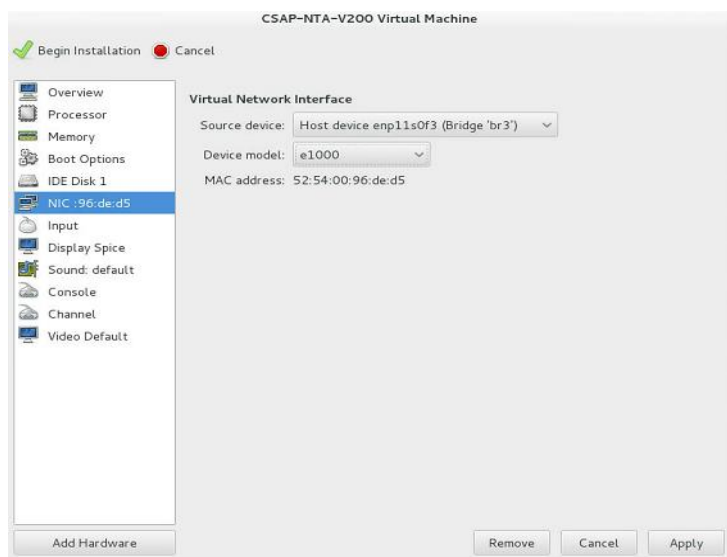
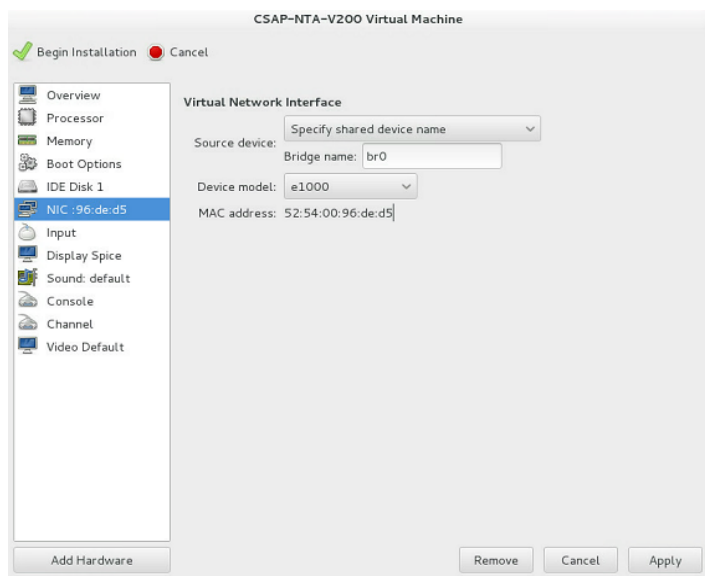
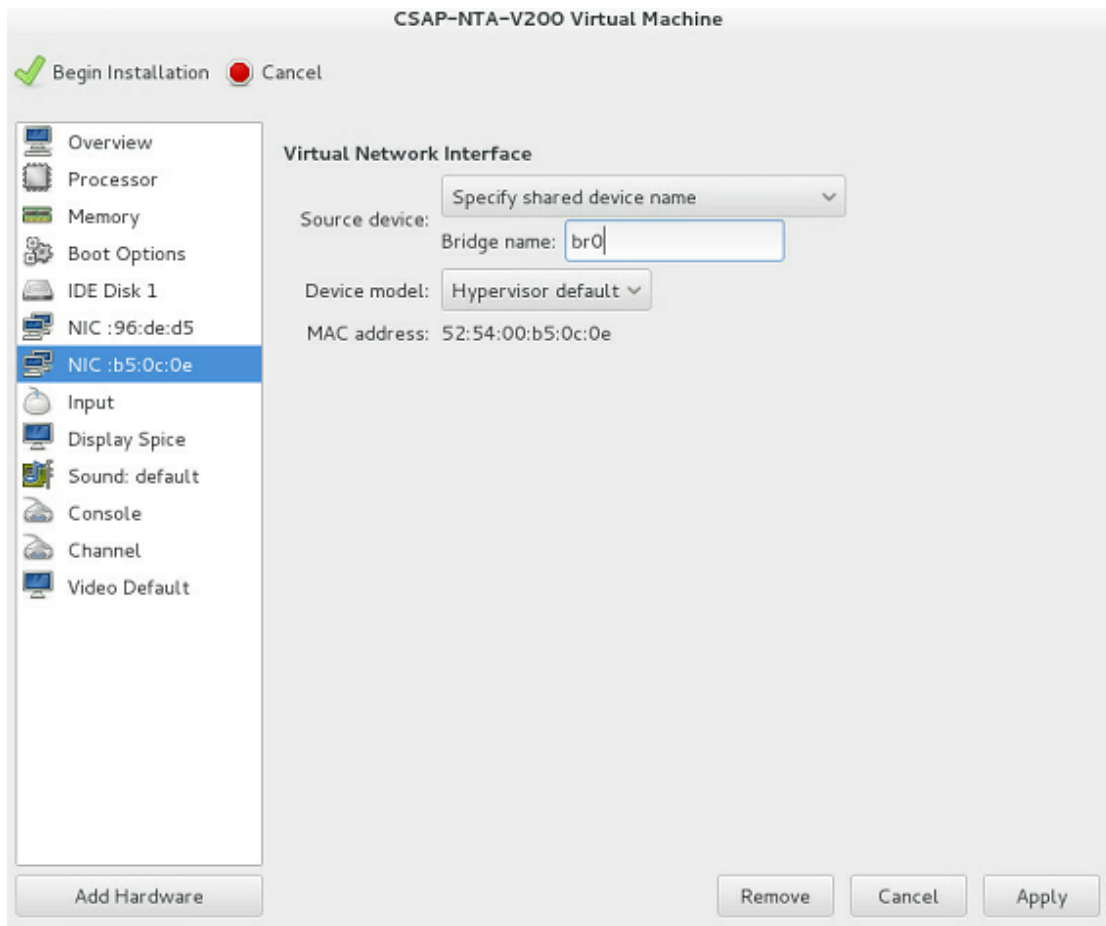


图3-52 配置网卡方式二



(10) 要正常运行 CSAP-NTA-V200，至少需要按照两个虚拟网卡来配置，而虚拟机基本配置中只有一块网卡。要添加新网卡，可以在客户化配置界面左下角点击<Add Hardware>，进入添加新硬件配置界面，然后选择网络设备，并配置网卡的属性，如[图 3-40](#) 所示。

图3-53 添加新网卡



(11) 点击<Begin Installation>，完成虚拟机的创建。新创建的虚拟机会自动运行，并进入 CSAP-NTA-V200 的安装过程。

2. 安装 CSAP-NTA-V200

虚拟机自动从 PXE Server 下载所需文件，并将会自动完成安装。
进入探针默认用户名和密码：**admin/admin**。

3.4 在CAS平台安装CSAP-NTA-V200



说明

在 CAS 平台安装 NTA 产品的方式相同，下面将以 CSAP-NTA-V200 为例进行介绍。

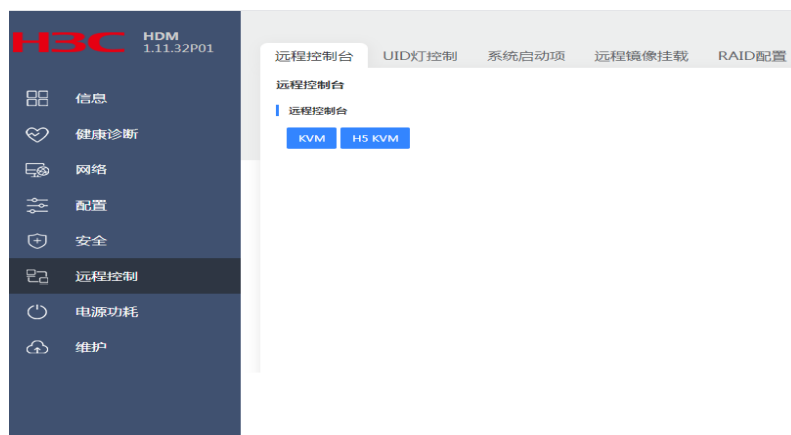
在 CAS 平台上，H3C CSAP-NTA-V200 只可通过以 ISO 进行安装。

3.4.1 CAS 平台

1. 利用 HDM 访问裸金属服务器

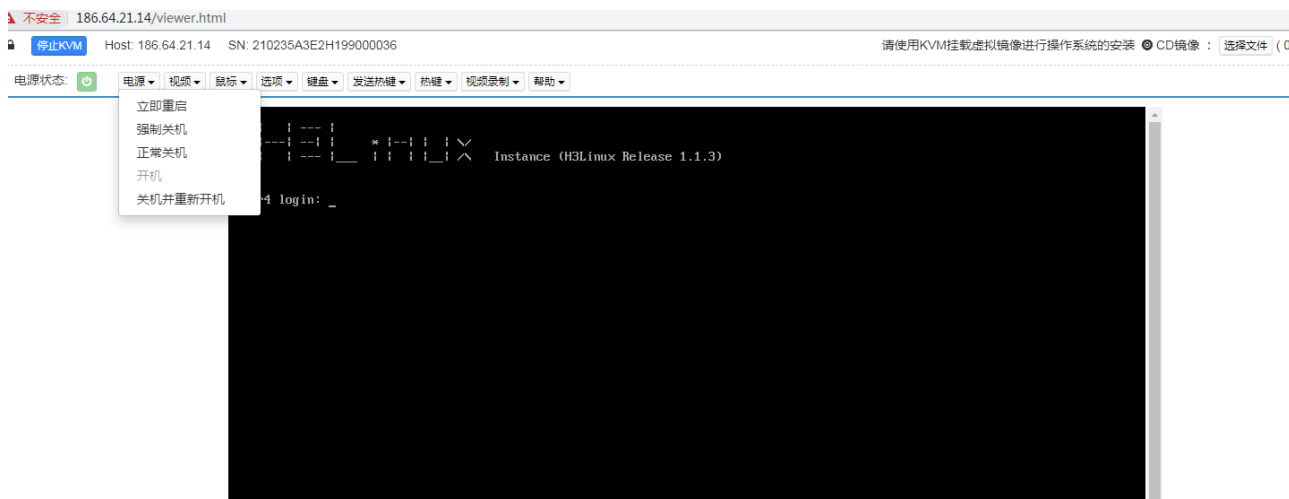
(1) 交换机的网线需要先链接到服务器的 HDM 口上。

- (2) 在浏览器中输入服务器的 HDM 地址，例如：<https://192.168.100.179/index.html>。默认密码：`admin/Password@_`
- (3) 打开网页后，会出现[如下图](#)所示界面，选择[远程控制台->远程控制台-> H5 KVM]，利用 HDM 口登录裸金属服务器。



- (4) 登录成功后，打开 H5 kvm 会出现[错误!未找到引用源。](#)所示界面,点击立即重启。

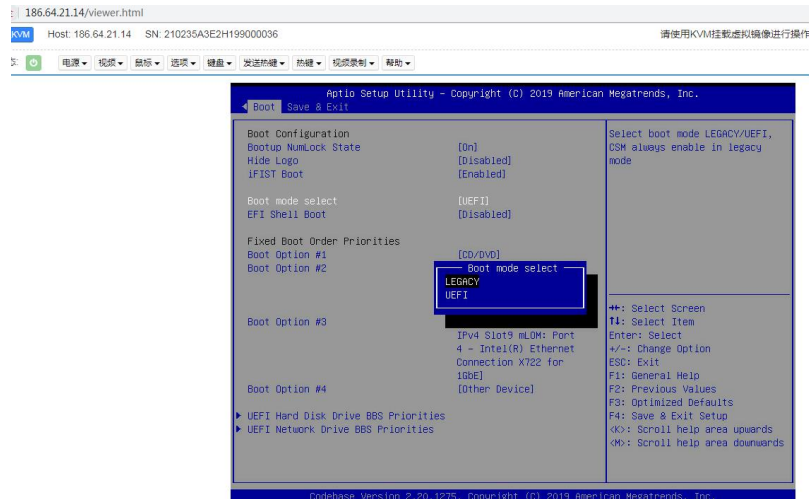
图3-54 成功登录服务器



在下图界面，点按“Esc”按键进入 BIOS 界面，如下图：



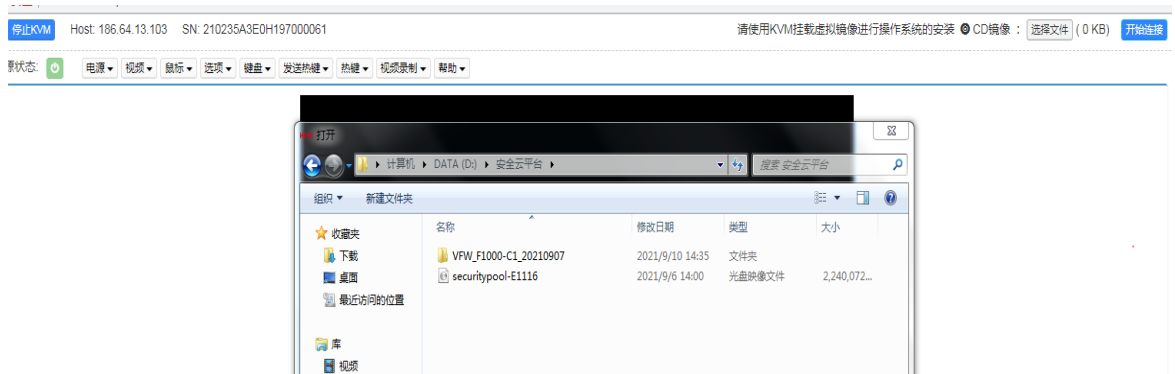
(5) 进入 BIOS 界面后，选择 boot 界面，该界面 boot mode select 更改为'legacy',如下图



(6) 如下图 第一启动项更改为 CD/DVD，第二启动项更改为硬盘启动，最后保存配置

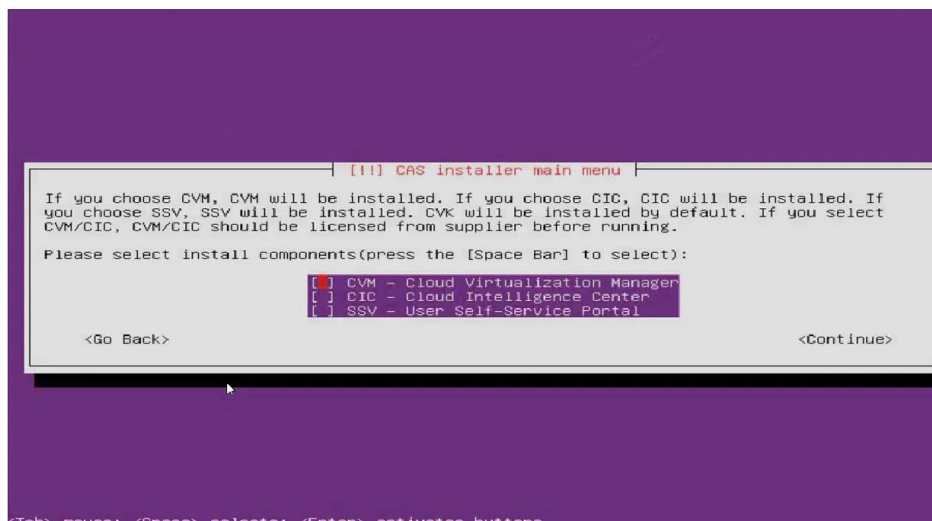


(7) 点击左上角选择文件--选中需要安装的 ISO 文件—开始连接，连接虚拟机的 CD 设备到 securitypool-E1116 的安装 ISO 文件上，等待虚拟机自动读取安装映像，如下图



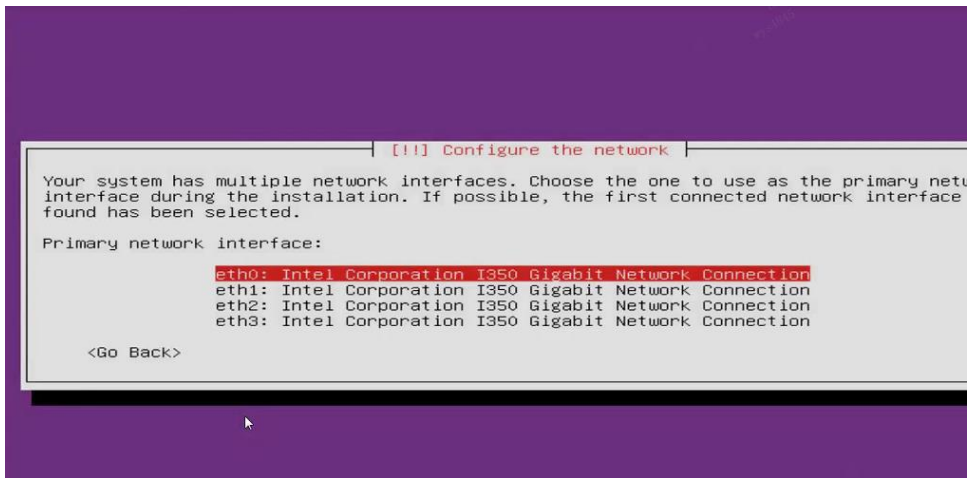
2. 安装 cas 平台

(1) 弹出以下界面时，选择 CVM-contion，继续下一步安装。

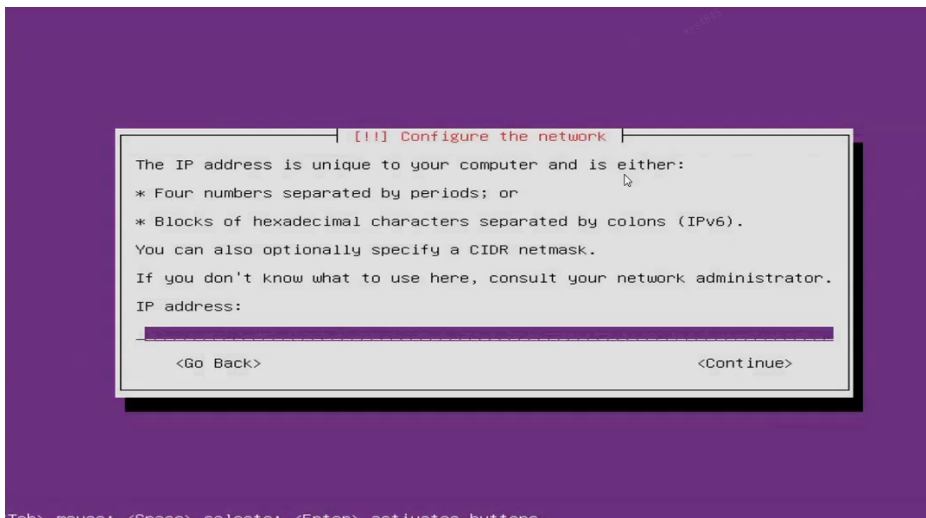


注意：光标停在 CVM 栏后，先按空格键选中 CVM，光标上出现“*”则表示选中。

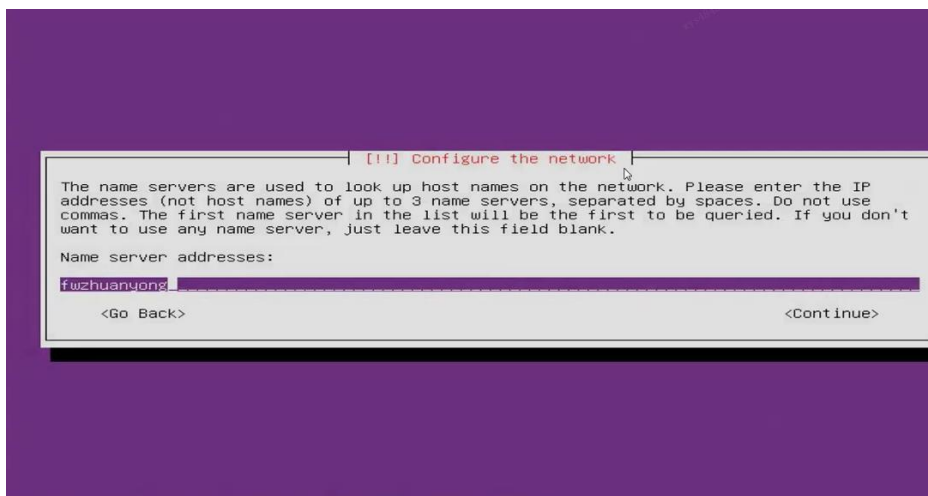
(2) 选择物理网卡作为管理口的物理网卡。



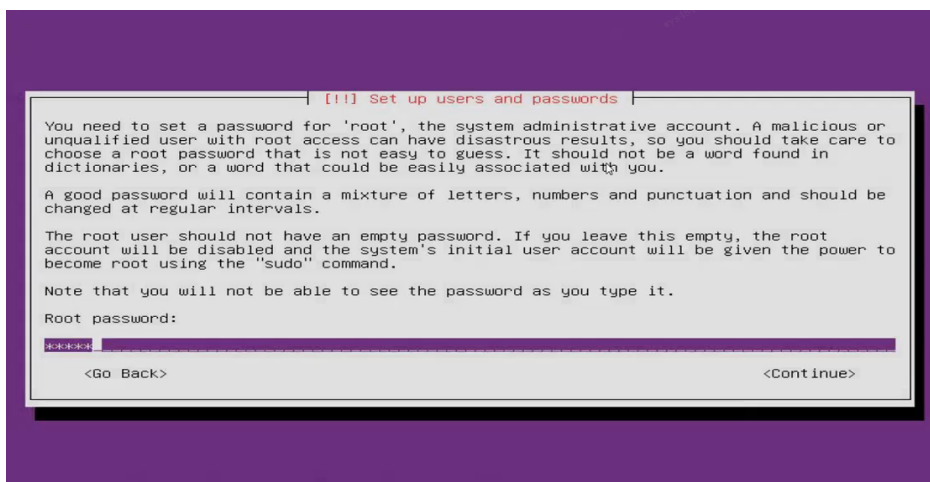
(3) 输入 IP 地址，此 IP 地址作为 CAS 平台的登录地址。



(4) 再输入 mac 和网关，name server address 可以任意输入如下图

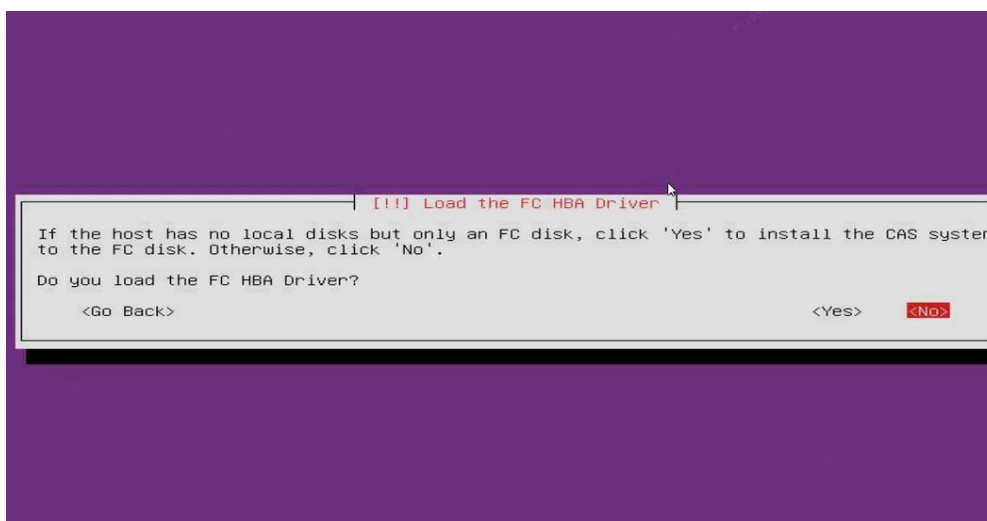


(5) Host name 界面和 domain name 直接选择默认，root password 界面直接输入密码，弹出一个界面后再重新一遍密码。

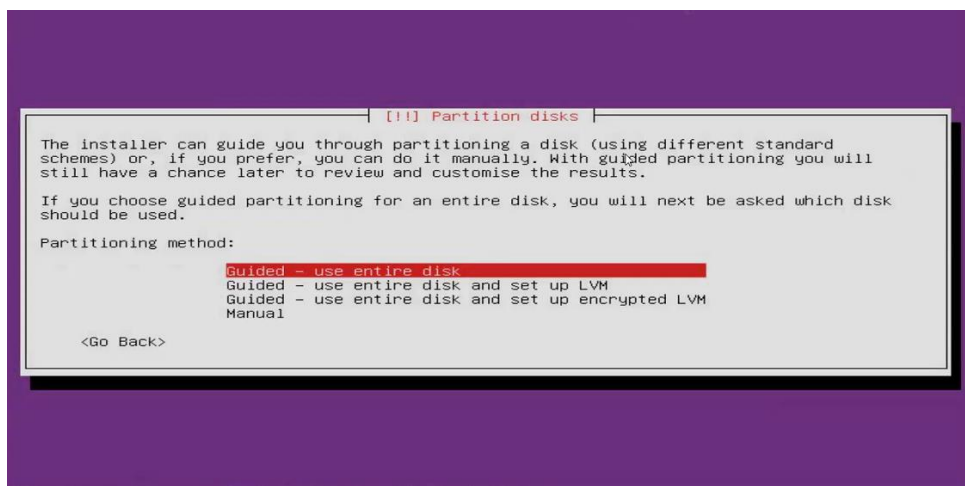


注意：此处密码 CAS 平台新建集群和修改 CAS 平台网页地址需要用到。

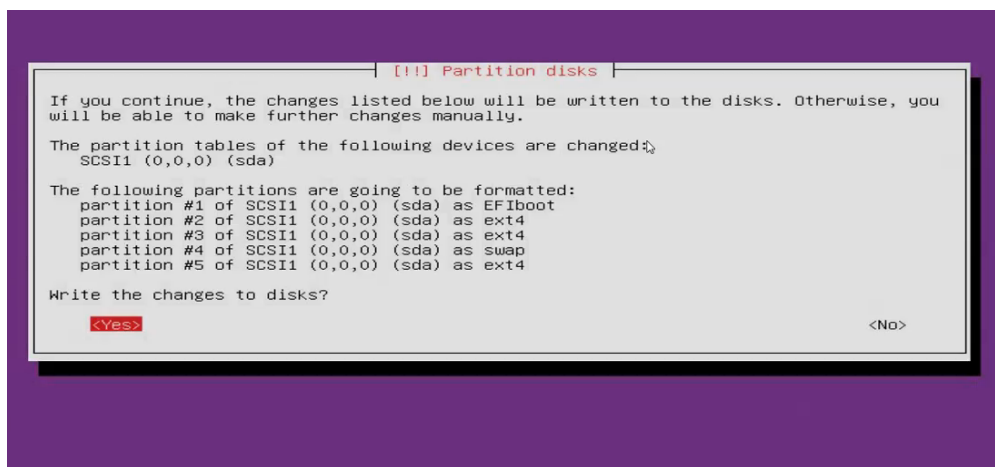
(6) 弹出是否安装 FC 界面，选择“NO”。



选择 use entire disk，进入下个界面



选择“yes”，等待安装完成，时间较长，大约需要四五十分钟。



3.4.2 通过 ISO 安装 CSAP-vNTA-200

1. 新建主机

- (1) 使用浏览器打开 CAS 云计算管理平台登录界面，如图 3-55 所示。输入登录的用户名、密码，点击<登录>按钮。登录默认密码：admin/admin，CAS 平台登录地址为安装 CAS 平台时输入的 IP 地址，如：http://186.8.0.248:8080/cas/login

图3-55 登录 CAS 云计算管理平台



说明

CAS 云计算管理平台的登录用户名及密码请联系该管理平台管理员获取。

登录成功后，会出现图 3-56 所示界面。

图3-56 CAS 云计算管理平台主界面



- (2) 在界面左侧的导航树中选中“云资源”，然后点击<增加主机池>按钮，开始新建一个主机池。在 [3-57](#) 所示增加主机池窗口中输入主机池名称，然后点击<确定>。

图3-57 新建主机池

增加主机池

名称*

确定 取消

- (3) 选中新建的主机池，点击<增加主机>按钮，开始新建一个主机。在 [图 3-58](#) 所示增加主机窗口，输入要管理的 CVK 主机 IP 地址、用户名和密码，然后点击<确定>。

图3-58 新建主机



增加主机

IP地址* 192.168.100.40

用户名* admin

密码*

确定 取消

 说明

CVK 主机的登录用户名及密码请联系该服务器管理员获取。

- (4) 主机新建成功后，点击<更多操作>中的<连接主机>按钮，然后在弹出窗口点击<确定>，使 CVM 可以与主机建立连接，如[图 3-59](#)所示。

图3-59 连接主机



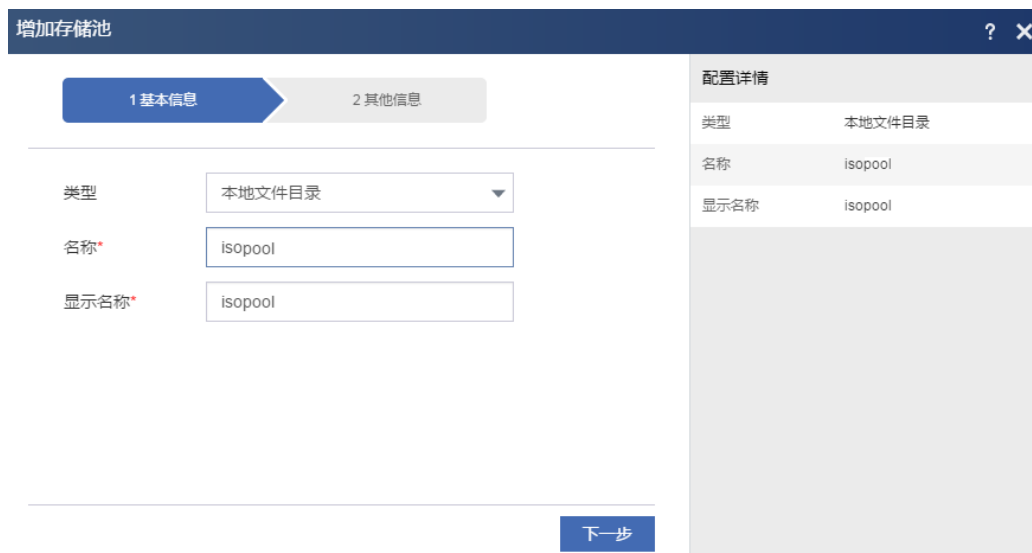
- (5) 在界面左侧的导航树中选中刚刚新建的主机，然后点击“存储”页签，进入[图 3-60](#)所示配置界面，开始为主机新建存储池。

图3-60 存储管理界面



(6) 点击<增加>按钮，创建用于存放 CSAP-NTA-V200 ISO 文件的存储池。在图 3-61 所示配置界面，输入存储池的名称，然后点击<下一步>。

图3-61 新建存储池



(7) 点击<完成>按钮，并启动存储池，完成存储池的创建，如图 3-62 所示。

图3-62 完成存储池的创建



(8) 选中新建的存储池，点击<上传文件>按钮，开始上传 CSAP-NTA-V200 ISO 文件到 CVK 主机，如图 3-63 所示。

图3-63 文件上传管理界面



(9) 可以直接把文件拖拽到文件上传区，然后点击<开始上传>，如图 3-64 所示。

图3-64 上传文件



上传完毕后，关闭此窗口，回到 CAS 云计算管理平台主界面。

2. 新建虚拟机

- (1) 选择新建的主机，点击<增加虚拟机>按钮，开始新建一个虚拟机。输入虚拟机的基本信息如名称和描述，虚拟机的操作系统选择“Linux”，版本选择“Other Linux(64 位)”，然后点击<下一步>，如图 3-65 所示。

图3-65 输入虚拟机名称及操作系统



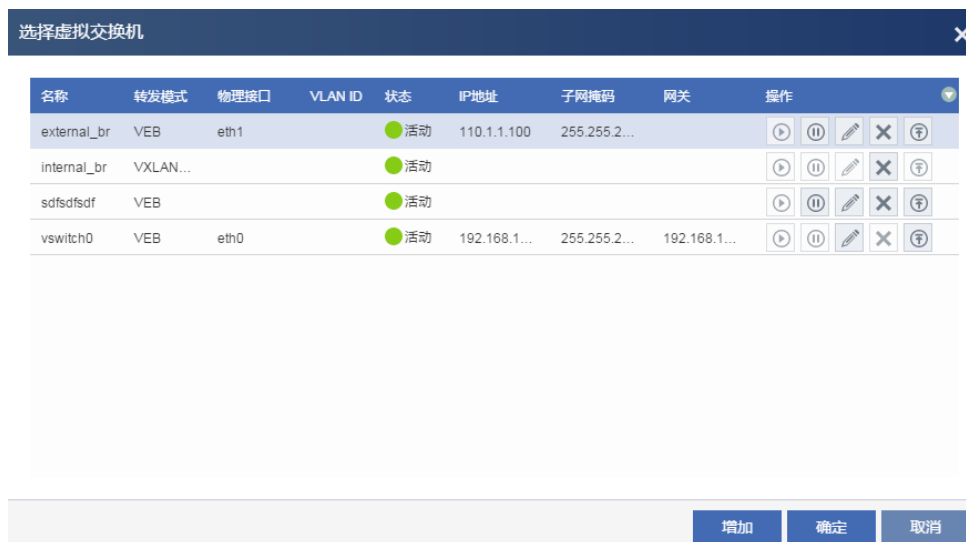
- (2) 进入硬件信息输入界面，硬件的配置需要满足[表 3-1](#)最低配置要求。如果要添加新网卡，可点击<增加硬件>，进入添加新硬件配置界面，然后选择增加网卡，如[图 3-66](#)所示。

图3-66 配置硬件



- (3) 点击网络栏的 图标，在弹出的窗口中为 CSAP-NTA-V200 选择虚拟交换机，然后点击<确定>，如[图 3-67](#)所示。虚拟交换机的创建过程及参数设置请参考 CAS 云计算管理平台在线帮助。说明：此方法作千兆网卡做管理口用，一般不做镜像流量用。

图3-67 选择虚拟交换机



提示

- 安装 1G 网口，可直接添加物理接口，如要安装 10G 网口，应先虚出 vf 口，操作方法如 3。

- (4) 点击磁盘选项 图标，显示虚拟机磁盘高级设置，如[图 3-68](#)所示。

图3-68 选择存储




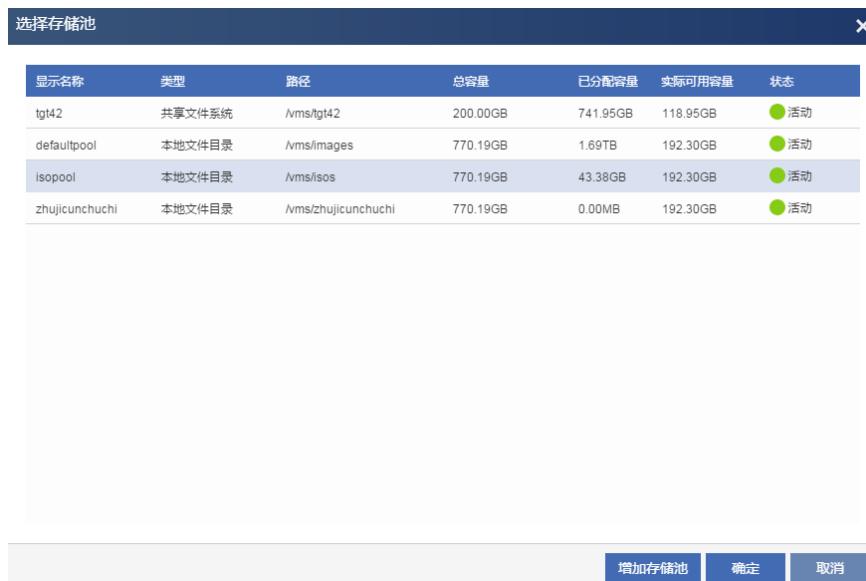
- (5) 点击存储池对应的  图标，弹出选择存储池对话框，选择新建主机时创建的存储池作为虚拟机磁盘，如 [图 3-69](#)

图3-69 选择存储池




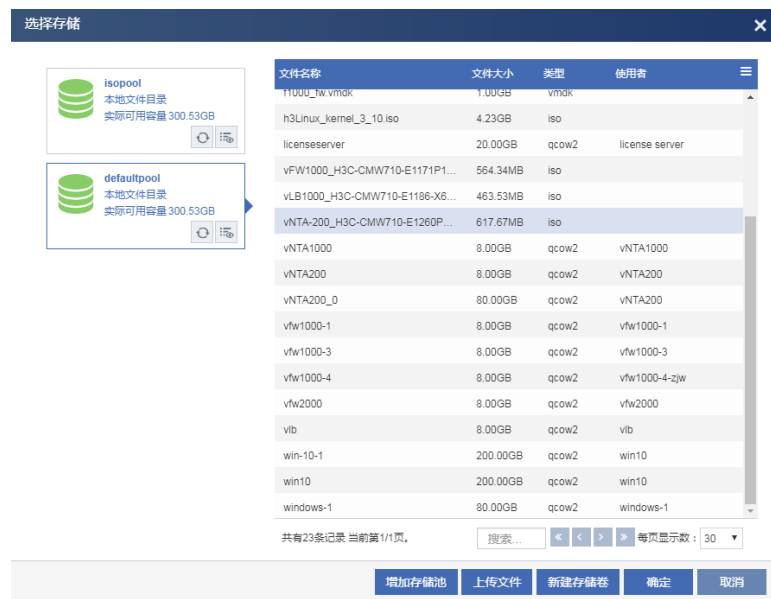
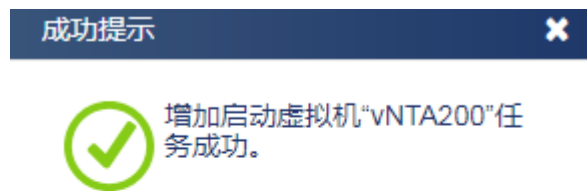
- (6) 点击光驱栏的  图标，选择要安装的 CSAP-NTA-V200 ISO 文件。如 [3-70](#) 所示，选择新建主机过程中上传到 CVK 主机上的 CSAP-NTA-V200 ISO 文件，点击<确定>回到“增加虚拟机”界面。

图3-70 选择 CSAP-NTA-V200 ISO 文件



(7) 点击<完成>按钮，完成虚拟机的创建，如图 3-71 所示。刚创建的虚拟机会列在导航树中。

图3-71 完成虚拟机的创建

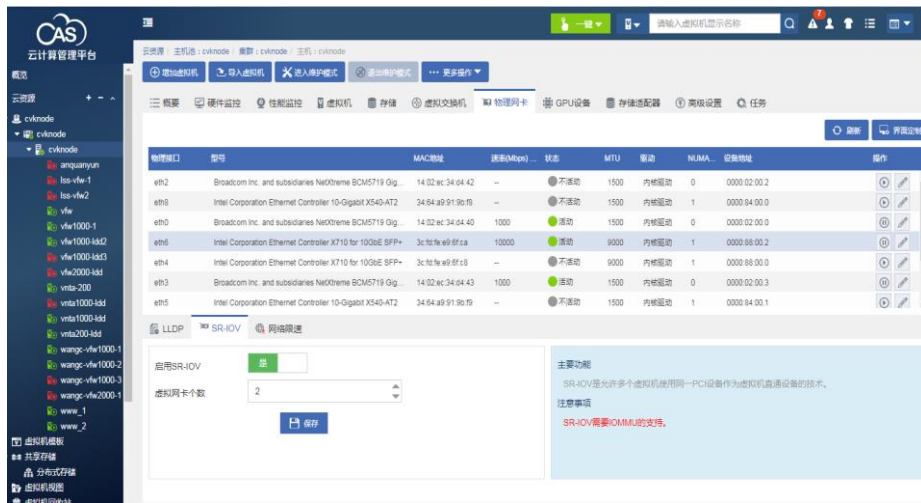


3. 安装 10G 网卡

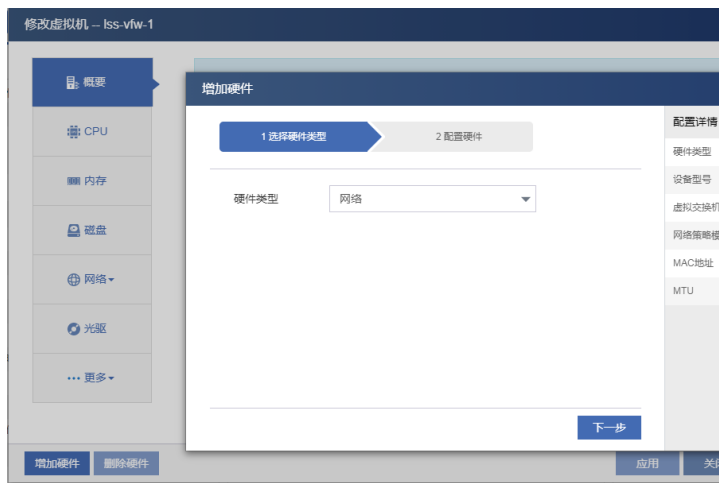
(1) 添加 10G 网口前需要把 IOMMU 开启，选择 cvknode 主机—高级设置---启动项配置---IOMMU 配置，需重启服务器配置才会生效。



(2) 在物理网卡界面选择对应的 10G 口物理接口，在 SR-IOV 虚出网卡个数，cvknode 主机-物理网卡-选中 10G 物理接口—SR-IOV—开启



(3) 选择新建的虚拟机---修改虚拟机---增加硬件，硬件类型选择网络



(4) 设备型号选择 SR-IOV 直通网卡，在点击  图标选择对应的 10G 口物理接口，如下图：



注意：虚拟机开机时，使修改虚拟机生效需要重启虚拟机。

4. 安装 CSAP-NTA-V200

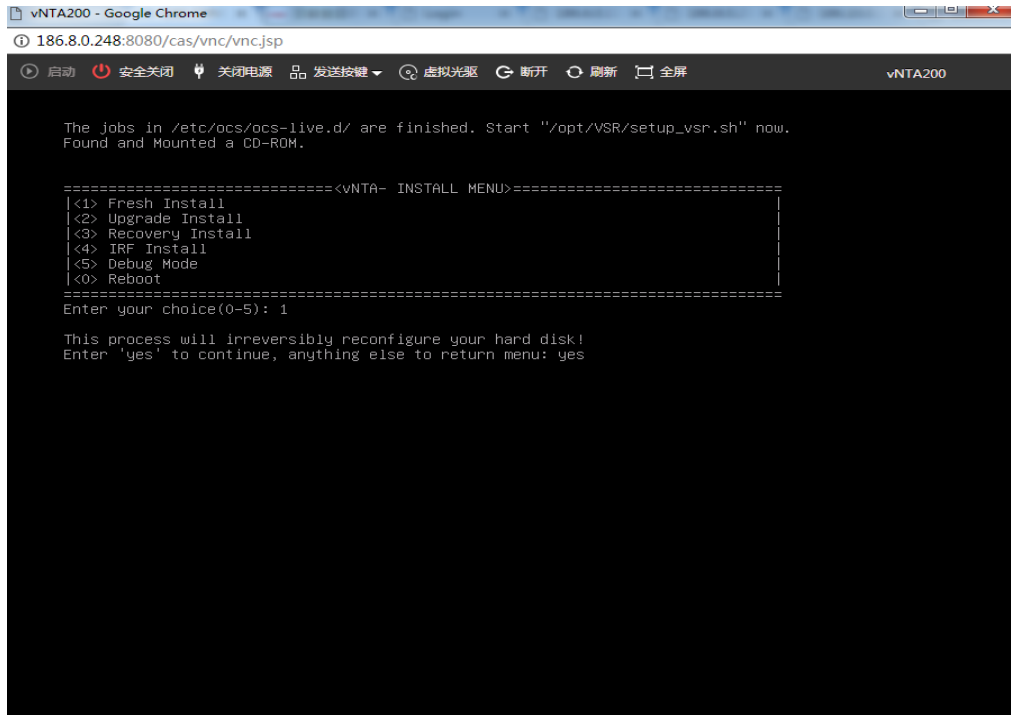
- (1) 在导航树中选中新建的虚拟机，然后点击<启动>按钮，启动虚拟机，并在弹出的提示窗口中选择<是>。
- (2) 点击“控制台”页签，然后点击<打开 Java 控制台>或<打开网页控制台>，启动虚拟机的控制台。

提示

- 运行 CAS 的虚拟机 Java 控制台需要 JRE 环境，请先安装 JRE 软件包再打开控制台。
- 在 CSAP-NTA-V200 安装完毕之后，应该进入 CAS 中“修改虚拟机”的界面。

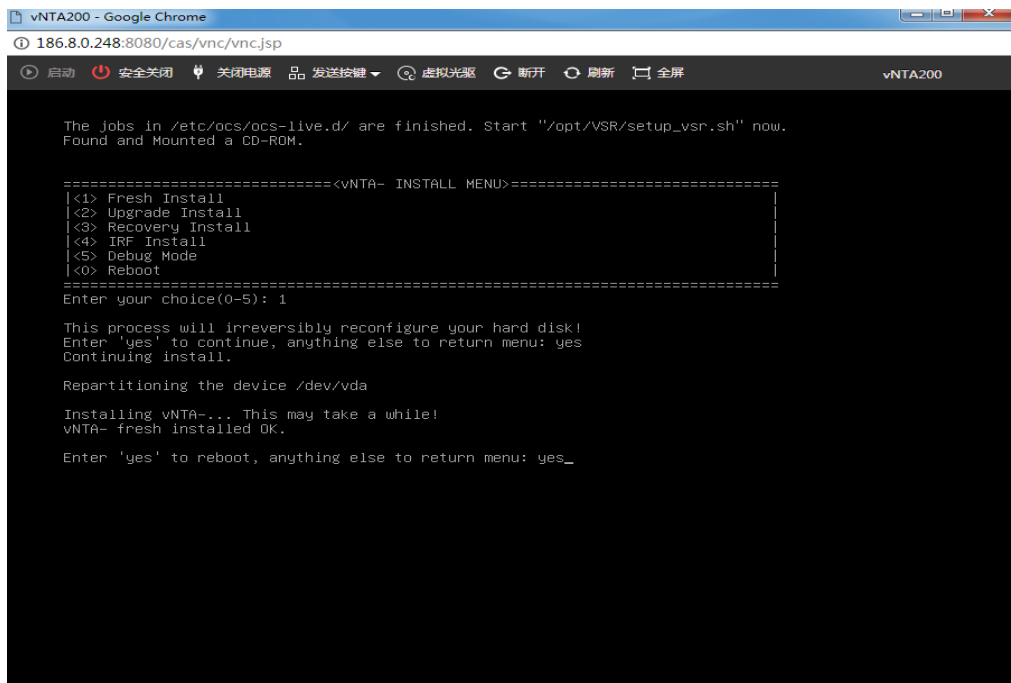
- (3) 虚拟机系统加载 ISO 文件，进入安装界面，安装界面如[图 3-72](#)所示。选择安装类型<1>，并输入“yes”确认后，系统将会自动完成安装。

图3-72 安装启动界面



(4) 输入“yes”重启系统，完成 CSAP-NTA-V200 的安装，如图 3-73 所示。

图3-73 完成 CSAP-NTA-V200 的安装



弹出下个界面后，直接按“Enter”键。重启系统后，完成 vNTA-200 安装。

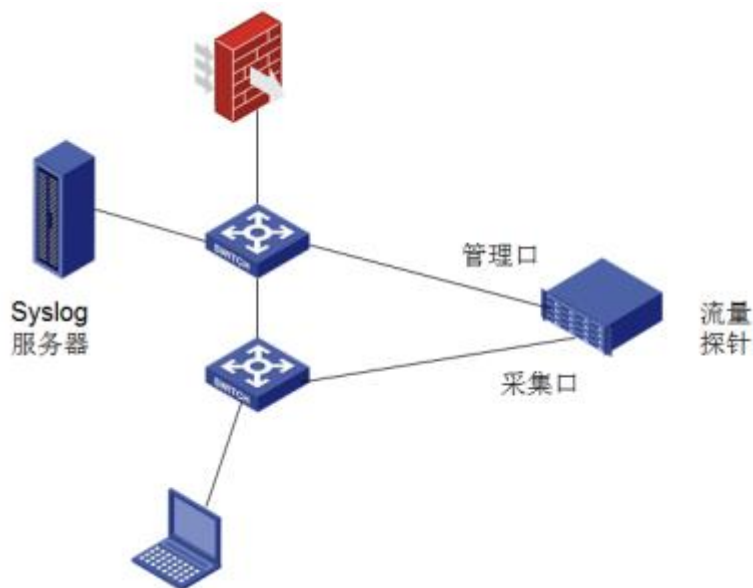
(5) 进入探针默认用户名和密码：admin/admin。

4 业务配置

4.1 组网说明

流量探针版本，只支持旁路部署，与 syslog 服务器之间网络可达，将数据包从交换机镜像到流量探针，实现对网络中的一台或者多台设备的数据采集。常规组网场景如下图所示。

图4-1 流量探针组网图



4.2 License

4.2.1 License 基本介绍

(1) 用户需要为设备购买授权码、安装 License，才能使用设备上的指定特性。哪些特性需要安装 License 可通过 License 授权信息页面中的信息和设备实际支持的特性共同决定。

(2) 设备的部分特性需要获取 License 授权后才能使用，如：

- IPS (Intrusion Prevention System, 入侵防御系统)
- WAF (Web Application Firewall, Web 应用防火墙)
- URL 过滤
- ARP 应用识别
- AV 防病毒
- 威胁情报

H3C 网站提供了 License 的激活申请功能，根据申请的授权序列号等信息，激活并生成相应的 License 激活文件。只有将 License 激活文件导入到设备，完成 License 激活文件的安装，才能保证相关特性功能的正常使用和特征库的及时升级。

License 针对不同的授权分为如下几种类型：

- 基础授权：软件产品正常运行需要安装基础授权 License；当 License 失效后，设备大幅度丢包无法使用，如需继续使用该功能请重新安装基础授权 License。
- 特征库升级授权：设备需要对某功能的特征库进行升级时，需要安装有效的 License；License 失效后，此类功能可以采用设备中已有的特征库正常工作，但无法继续升级特征库。如防病毒特征库升级授权。

vNTA200 产品软件功能授权描述：

描述	License 安装方式	预授权	正式授权	正式授权启用时间
H3C SecCenter CSAP-N TA-V200 网络全流量威胁分析探针功能授权函（3130A50U 基础特征库）	本地授权 远程授权	支持(有效期 180 天)	永久	授权码首次激活时启用
H3C SecCenter CSAP-N TA-V1 特征库升级授权函，1 年（3130A50P 六合一特征库）	本地授权 远程授权	支持(有效期 180 天)	1 年	授权码首次激活时启用（在 License 管理平台上获取到激活文件时即开始计算启用时间）

vNTA1000 产品软件功能授权描述：

描述	License 安装方式	预授权	正式授权	正式授权启用时间
H3C SecCenter CSAP-N TA-V1000 网络全流量威胁分析探针功能授权函（3130A50S 基础特征库）	本地授权 远程授权	支持(有效期 180 天)	永久	授权码首次激活时启用
H3C SecCenter CSAP-N TA-V2 特征库升级授权函，1 年（3130A50Y 六合一特征库）	本地授权 远程授权	支持(有效期 180 天)	1 年	授权码首次激活时启用（在 License 管理平台上获取到激活文件时即开始计算启用时间）

申请 license 正式网站：<https://lmp.h3c.com/Default.aspx?go=%2fdefault.aspx>



说明

探针自带试用授权，过期后建议购买正式授权，避免因 license 过期影响功能使用。

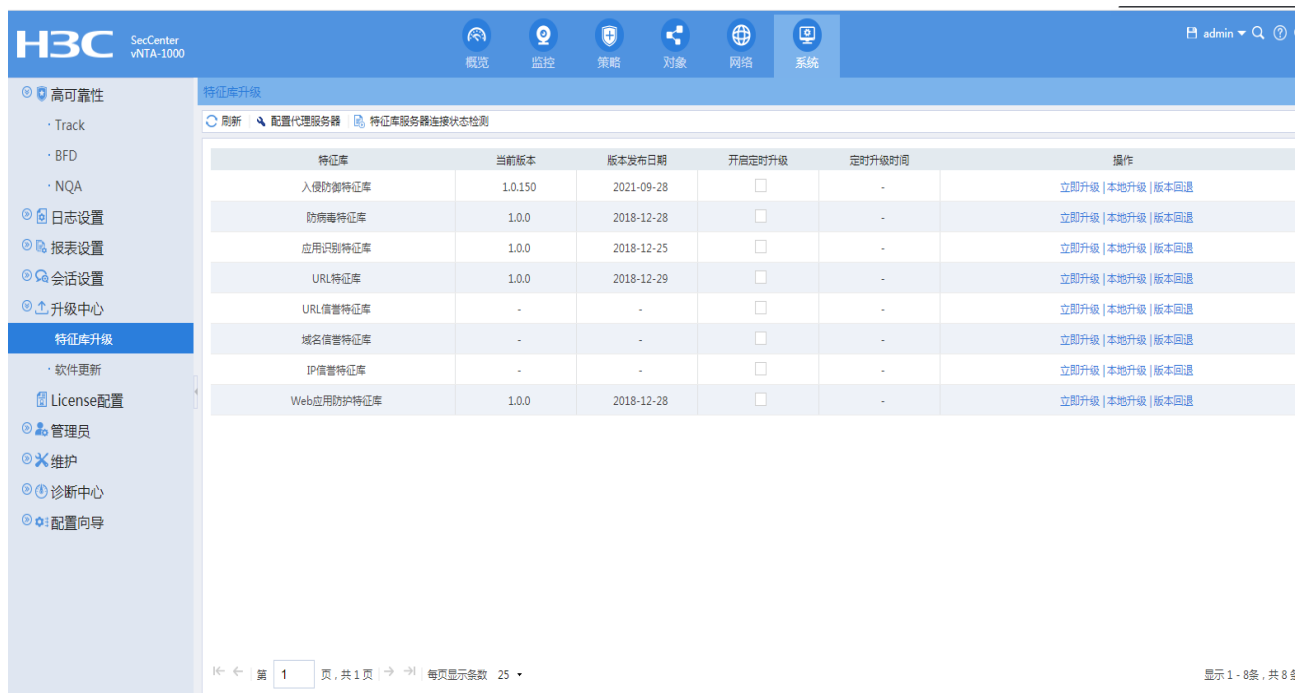
4.2.2 特征库升级

（1）特征库是用来对经过设备的应用层流量进行应用识别、URL 过滤、病毒检测、入侵防御和 Web 应用防护等的资源库。随着网络攻击不断的变化和发展，需要及时升级设备中的特征库。设备也支持特征库版本回退功能。目前，设备中存在入侵防御特征库、防病毒特征库、应用识别特征库、URL 特征库、Web 应用防护特征库、IP 信誉特征库、URL 信誉特征库和域名信誉特征库。

(2) 在官网地址

https://www.h3c.com/cn/Products_Technology/Products/IP_Security/Characteristic_Service_Area/ 找到特征库下载到本地

(3) 登录 web 界面，升级特征库，web 登录网址就是探针设备管理口的地址和密码。点击系统--升级中心--特征库升级--本地升级，找到需要升级的特征库，如下图



特征库对应关系如下：

入侵防御特征库——v7-IPS

防病毒特征库——v7-AV

应用识别特征库——v7-APR

域名信誉特征库——TI-HOSTNAME-V7

URL 特征库——v7-URL

Web 应用防护特征库——v7-WAF

URL 信誉特征库——TI-URL-V7

IP 信誉特征库——TI-IP-V7

4.3 web配置流量探针服务器

说明：登录 web 用户名和密码就是登录探针的用户名和密码，默认用户名和密码：**admin/admin**
探针有默认开局配置，如需把探针日志上传到日志平台可进行以下配置（此处以态势感知平台为例）。
探针默认配置有：

1. 接口加入黑洞模式，如需修改接口模式可参考 4.3.1 章节的（2）修改工作模式
2. 接口会话日志进出日志使能
3. 以开放用户权限为管理员，安全域、安全策略默认已配置，如需修改安全域可参考 4.3.1 章节的（4）修改
4. 配送会话/信誉/dns/防病毒/URL/IPS 日志发生到服务器，如需修改或增加请参考 4.3.1 章节的（7）、（6）修改
5. URL/防病毒/IPS 审计策略/IPS 抓包上传，如需修改或增加请参考 4.3.1 章节的（3）、（5）修改
需手动配置管理口 IP 地址，配置方法请参考 2.2.2 章节的配置网络。

4.3.1 探针日志上传到态势感知平台 web 配置过程

本举例中流量探针设备以旁路模式部署在网络中，用于监控用户流量。配置步骤如下：

- (1) 修改管理口。在 web 管理界面，进入“网络-接口 -接口”，点击编辑，把需要更改的管理口加入 Management 安全域。此处以 GE1/0 为例，如下图：



- (2) 把接口加入黑洞。登录设备的 Web 管理界面，进入“网络-接口 -接口对”，根据实际组网环境，选择旁路部署接口，加入接口对模式为黑洞模式。

注意：流量通过的接口需要加入黑洞，管理口不要加入黑洞模式。配置旁路部署



- (3) 配置审计策略

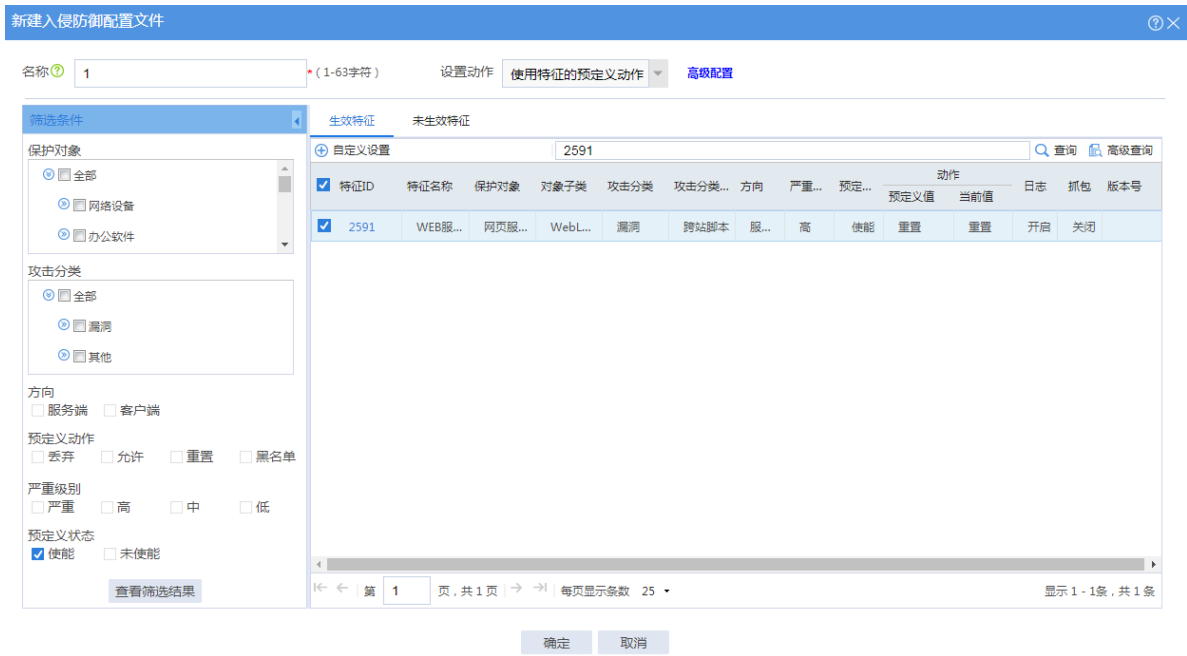
在导航栏中选择“对象-应用安全”，更具实际需求，新建审计策略（如 URL 过滤、入侵防御策略、防病毒、web 应用防护策略、数据过滤、应用识别、APT 防御）。

- ① URL 策略举例。选择对象--应用安全—URL 过滤，单击新建，根据实际需求，新建策略，如下图所示。

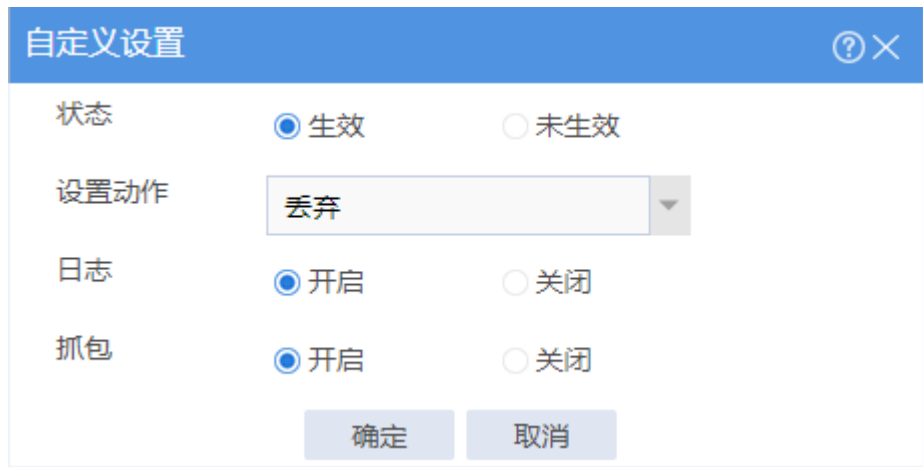
图4-2 配置 URL 检测策略



② 配置 IPS 抓包上传, 选择对象--应用安全--入侵防御--配置文件--新建—搜索需要上传的规则开启规则, 如下图:



选择自定义设置, 如下图



点击 对象--应用安全--安全动作--捕获--编辑，把捕获的规则上传到日志平台。如下图：



③配置防病毒策略。对象--应用安全—防病毒—配置文件。选择新建，如下图：



④ web 应用防护。对象--应用安全—web 应用防护—配置文件。点击新建，如下图：

新建Web应用防护配置文件

名称 * (1-63字符)

CC攻击防护配置文件

筛选特征

通过筛选特征，对Web应用防护配置文件需要匹配的特征进行筛选，如果不配置任何筛选条件，则此配置文件将对所有缺省处于启用状态的特征进行匹配。

保护对象

- 全部

攻击分类

- 全部
- 漏洞
- 其他

方向

- 服务端
- 客户端

⑤数据过滤。对象--应用安全—数据过滤—配置文件。点击新建，添加对应的过滤规则，如下图：

新建数据过滤配置文件

名称 * (1-31字符)

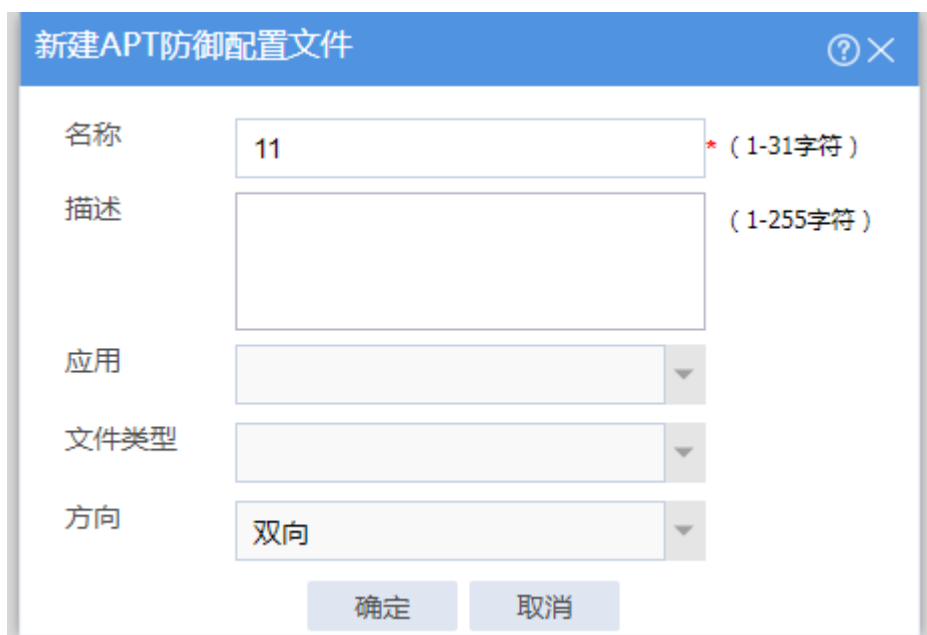
描述 (1-255字符)

数据过滤规则

<input type="checkbox"/>	名称	关键字组	应用	方向	动作	日志	编辑
<input type="checkbox"/>	11			上传	允许	打开	<input type="button" value="编辑"/>

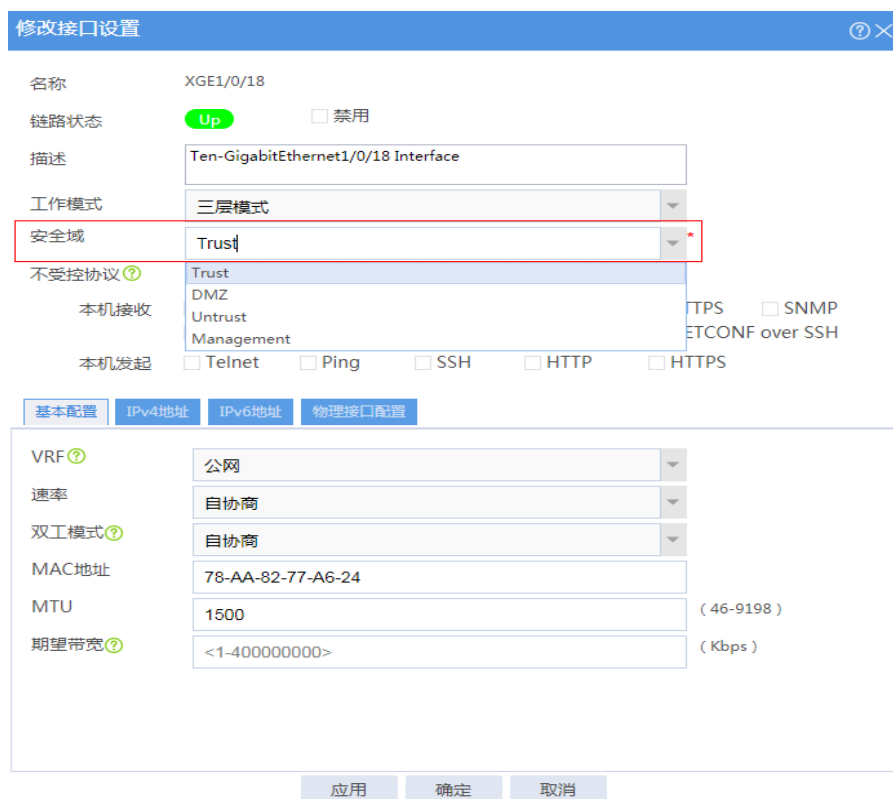
共1条

⑥ATP 防御策略。对象--应用安全—ATP 防御—配置文件，选择新建，如下图：



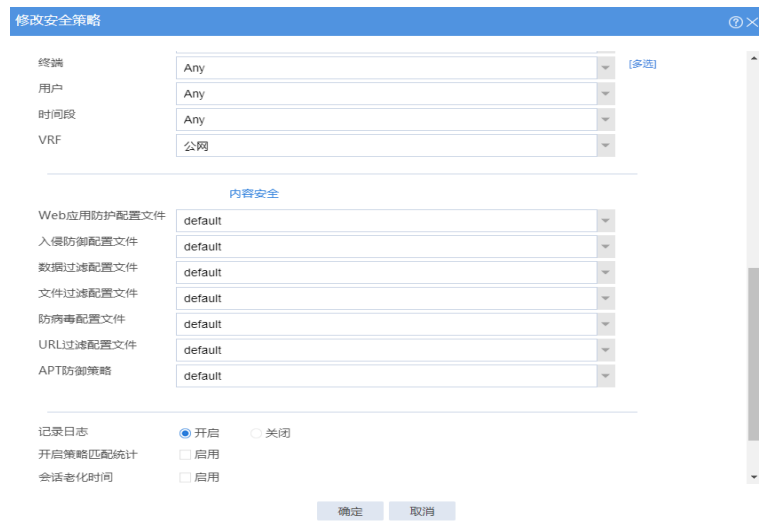
(4) 进入“网络-接口”将业务口加入相应安全域内。

图4-3 配置接口加入安全域



(5) 进入“策略-安全策略-编辑”安全策略，内容安全应用建立的审计策略。此处配置的 ips/url/dns 等策略放行。

图4-4 配置安全策略，应用审计内容



(6) 配置日志输出类型

在导航栏中选择“系统-日志设置-威胁日志”，日志类型选择快速日志，输出中文日志，如下图所示。

图4-5 配置日志输出类型



“系统-日志设置-URL 过滤日志”，日志类型选择快速日志，开启 URL 过滤日志，如下图所示。

图4-6 配置日志输出类型



“系统-日志设置-会话日志”，日志类型选择快速日志—勾选记录新建/删除会话-应用，开启会话日志，如下图所示



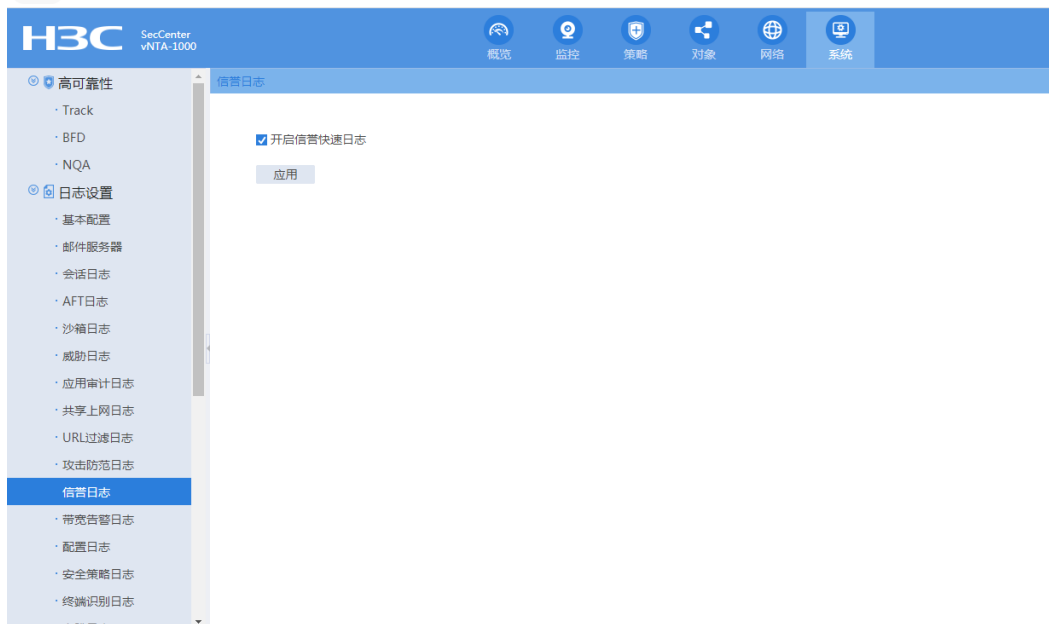
在当前页面点击生成日志的接口列表—添加接口，接口选择流量经过的接口，配置如下图：



开启信誉日志前需开启信誉情报，在策略—威胁情报—IP 信誉/域名信誉，启用该功能，如下图



然后再选择“系统-日志设置-信誉日志”，点击开启信誉日志，如下图所示



(7) 配置发送日志发送服务器

导航栏中选择“系统管理-日志设置-快速日志”，单击新建，配置日志服务器 IP 地址及服务器端口，选择输出的会话、入侵防御等日志，如下图所示。

注意：1.会话等日志上传到日志主机上，如果日志主机的态势感知平台，日志主机为态势平台的 IP 地址。2.设备时间需要同步网络时间，可在系统—维护—系统设置—日期和时间，把设备时间设置为当前网络时间。

图4-7 配置日志服务器





说明

单独配置 DNS 快速日志配置时，可能覆盖此处配置，建议统一一步用命令行配置，命令行配置如下：

```
customlog format dns
```

```
customlog host 192.169.1.2 export session dpi url-filter ips anti-virus reputation dns
```

配置 dns 日志时 customlog host 192.169.1.2 export 命令后需加上已经设置的，如 ips 命令

4.3.2 命令行参考

命令行配置如下：

```
#
bridge 1 blackhole
  add interface GigabitEthernet1/0/1    (把除管理口的接口加入黑洞模式)
#
bridge 2 blackhole
  add interface GigabitEthernet1/0/2
#
bridge 3 blackhole
  add interface GigabitEthernet1/0/3
#
bridge 4 blackhole
  add interface GigabitEthernet1/0/4
#
interface GigabitEthernet1/0/0
  port link-mode route
  ip address 192.169.1.1 255.255.255.0    (设置管理口的 IP)
#
interface GigabitEthernet1/0/1
  port link-mode route
  session log enable ipv4 inbound
  session log enable ipv4 outbound    (开启会话日志)
#
interface GigabitEthernet1/0/2
  port link-mode route
  session log enable ipv4 inbound
  session log enable ipv4 outbound
#
interface GigabitEthernet1/0/3
```

```

port link-mode route
session log enable ipv4 inbound
session log enable ipv4 outbound
#
interface GigabitEthernet1/0/4
port link-mode route
session log enable ipv4 inbound
session log enable ipv4 outbound
#
security-zone name Local
#
security-zone name Trust
import interface GigabitEthernet1/0/1
import interface GigabitEthernet1/0/2
import interface GigabitEthernet1/0/3
import interface GigabitEthernet1/0/4
import interface Ten-GigabitEthernet1/0/5
import interface Ten-GigabitEthernet1/0/6
import interface Ten-GigabitEthernet1/0/7
import interface Ten-GigabitEthernet1/0/8    (接口加入安全域)
#
security-zone name Management
import interface GigabitEthernet1/0/0    (管理口加入 management 安全域)
#
line vty 0 63
authentication-mode scheme
user-role network-admin
user-role network-operator    (设置用户操作权限)
#
customlog format session
customlog format dpi url-filter
customlog format dpi ips
customlog format dpi anti-virus
customlog format dpi reputation
customlog format dns            开启 dns/ips/会话/url/放病毒日志
customlog host 192.169.1.2 export session dpi url-filter ips anti-virus reputation dns (如需上传到
态势感知平台，此处地址为态势感知平台地址)
customlog timestamp localtime

```

```

#
local-user admin class manage
password simple admin
service-type ssh terminal https
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator （设置管理权限）
#
session statistics enable （开启会话统计）
session log flow-end
#
netconf soap https enable
netconf ssh server enable （开启服务）
#
ip https enable
ip http enable
#
app-profile 0_IPv4 （ips/url/防病毒策略放行）
ips apply policy ips_default mode protect
url-filter apply policy url_default
anti-virus apply policy av_default mode protect
#
inspect capture parameter-profile ips_capture_default_parameter （ips 抓包上传到 192.169.1.2 平台）
capture-limit 0
export url tftp://192.169.1.2
#
inspect logging parameter-profile av_logging_default_parameter （av 策略设置）
undo log syslog
#
inspect logging parameter-profile ips_logging_default_parameter （ips 日志默认设置）
undo log syslog
log language chinese
#
ip-reputation （开启 ip 信誉日志）
global enable
attack-category 1 action permit logging enable
attack-category 2 action permit logging enable

```

```
attack-category 3 action permit logging enable
attack-category 4 action permit logging enable
attack-category 5 action permit logging enable
attack-category 6 action permit logging enable
attack-category 7 action permit logging enable
attack-category 8 action permit logging enable
attack-category 9 action permit logging enable
attack-category 10 action permit logging enable
attack-category 11 action permit logging enable
attack-category 12 action permit logging enable
attack-category 15 action permit logging enable
attack-category 16 action permit logging enable
attack-category 17 action permit logging enable
attack-category 18 action permit logging enable
attack-category 19 action permit logging enable
attack-category 20 action permit logging enable
attack-category 21 action permit logging enable
attack-category 22 action permit logging enable
attack-category 23 action permit logging enable
#
security-policy ip    (放行 0_IPv4 安全策略)
rule 0 name security_policy
    action pass
    profile 0_IPv4
#
ips policy ips_default (ips 默认策略)
severity-level medium high critical
status enabled
signature override all permit logging capture
#
anti-virus policy av_default (av 默认策略)
inspect ftp direction both action alert
inspect http direction both action alert
inspect smb direction both action alert
inspect nfs direction both action alert
#
anti-virus logging parameter-profile av_logging_default_parameter
#
```

```

domain-reputation (开启域名信誉日志)
global enable
attack-category 1 action permit logging enable
attack-category 2 action permit logging enable
attack-category 3 action permit logging enable
attack-category 4 action permit logging enable
attack-category 5 action permit logging enable
attack-category 6 action permit logging enable
attack-category 7 action permit logging enable
attack-category 8 action permit logging enable
attack-category 9 action permit logging enable
attack-category 10 action permit logging enable
attack-category 11 action permit logging enable
attack-category 12 action permit logging enable
attack-category 15 action permit logging enable
attack-category 16 action permit logging enable
attack-category 17 action permit logging enable
attack-category 18 action permit logging enable
attack-category 19 action permit logging enable
attack-category 20 action permit logging enable
attack-category 21 action permit logging enable
attack-category 22 action permit logging enable
attack-category 23 action permit logging enable
#
return

```

5 升级 NTA 产品软件版本

5.1 启动文件简介

启动软件包是用于引导设备启动的程序文件，按其功能可以分为四类：**Boot** 软件包、**System** 软件包、**Feature** 软件包和 **Patch** 软件包。设备必须具有 **Boot** 软件包和 **System** 软件包才能正常运行，**Feature** 软件包可以根据需要选择安装。**Patch** 软件包只在需要修复设备软件缺陷时安装。

表5-1 启动软件包分类

启动软件包	说明
Boot软件包	包含Linux内核程序，提供进程管理、内存管理、文件系统管理、应急Shell等功能。

启动软件包	说明
System软件包	包含Comware内核和基本功能模块的程序，如设备管理、接口管理、配置管理和路由模块等。
Feature软件包	用于业务定制的程序，能够提供更丰富的业务。一个Feature包可能包含一种或多种业务。是否支持Feature包以及支持哪些Feature包与设备的型号有关，请以设备的实际情况为准。
Patch软件包	用来修复设备软件缺陷的程序文件。补丁包与软件版本一一对应，补丁包只能修复与其对应的启动软件包的缺陷，不涉及功能的添加和删除。

产品的启动文件支持以下三种发布形式：

- **BIN 文件：**后缀为.bin 的文件。一个 BIN 文件就是一个启动软件包。要升级的 BIN 文件之间版本必须兼容才能升级成功。
- **IPE（Image Package Envelope，复合软件包套件）文件：**后缀为.ipe 的文件。它是多个软件包的集合。产品通常会将同一个版本需要升级的所有类型的软件包都压缩到一个 IPE 文件中发布。用户将该 IPE 文件设置为加载文件时，设备会自动将它解压缩成一个个 BIN 文件。用户再使用这些 BIN 文件升级设备即可，从而能够减少启动软件包之间的版本管理问题。
- **ISO 文件：**后缀为.iso 的文件。它是多个软件包的集合。产品通常会将操作系统文件以及同一个版本需要升级的所有类型的软件包都压缩到一个 ISO 文件中发布。用户将该文件设置为加载文件时，设备会自动将它解压缩成一个个 IPE、BIN 文件。用户再使用这些 BIN 文件升级设备即可，从而能够减少启动软件包之间的版本管理问题。

通常情况下，启动文件是一个后缀名为.IPE 的文件。

5.2 升级方式简介

产品可以通过命令行进行升级，也可以使用 ISO 镜像文件进行升级，两种升级方式的说明如[表 5-2](#)所示。

表5-2 软件升级方式简介

升级方式	说明
通过Web升级产品	<ul style="list-style-type: none"> ● 需要重启设备来实现设备软件的升级 ● 使用该方式升级设备软件时会导致当前业务中断
通过命令行升级产品	
通过ISO升级产品	<ul style="list-style-type: none"> ● 设置 CSAP-NTA-V200、CSAP-NTA-V1000 使用 ISO 光盘引导启动并进行软件升级 ● 需要重启设备来实现设备软件的升级

5.3 通过Web升级产品

5.3.1 升级前的准备



- 产品的升级方式相同，下面将以 CSAP-NTA-V200 为例进行介绍。
 - 组网图中 Device 指代 CSAP-NTA-V200 设备。
-

在升级启动文件前，需要配置如下图所示的升级环境。升级前的准备工作如下：

- 配置 CSAP-NTA-V200 接口 IP、路由、安全域、安全策略，使之与 PC 之间路由可达。
- PC 上安装了 Chrome、IE 10 或 FireFox 浏览器。
- 通过 PC 登录到 CSAP-NTA-V200 的 Web 界面中。
- 将 CSAP-NTA-V200 的升级启动文件拷贝到 PC 上。

图5-1 产品升级组网环境示意图



5.3.2 通过 Web 升级 CSAP-NTA-V200 的启动文件

- (1) 在 PC 上启动浏览器，在地址栏中输入 CSAP-NTA-V200 的 IP 地址“1.1.1.1”后回车，进入设备的 Web 登录页面，输入设备缺省用户名 admin 和密码 admin，单击<登录>按钮即可登录。



输入缺省密码可能会提示密码强度弱，按页面提示修改缺省密码后重新登录即可。

- (2) 登录成功后，选择“系统 > 升级中心 > 软件更新”，进入如下图所示的页面。
- (3) 单击<立即升级>按钮，弹出立即升级配置页面，根据实际情况选择启动文件类型，如下图所示。

图5-2 软件升级页面

立即升级 ? ×

主用主控板总空间：2.99GB，剩余空间：781.22MB

如果ipe文件大于磁盘剩余空间，请选择bin文件方式进行升级。[如何使用?](#)

启动文件类型 ipe bin

主控板

自动删除当前所有启动文件

保存当前配置 ?

立即重启设备 ?

(4) 单击<确定>按钮开始进行软件升级。等待设备启动完成后，重新登录即可。

5.4 通过命令行升级产品

说明

- NTA 的升级方式相同，下面将以 CSAP-NTA-V200 为例进行介绍。
- 组网图中 Device 指代 CSAP-NTA-V200 设备。

5.4.1 升级前的准备

在升级 CSAP-NTA-V200 启动文件前，需要配置如下图所示的升级环境。升级前的准备工作如下：

- 配置 CSAP-NTA-V200 接口 IP、路由、安全域、安全策略，使之与 PC 之间路由可达。
- 开启文件服务器的 TFTP/FTP Server 功能。
- 通过配置终端登录到 CSAP-NTA-V200 的命令行配置界面中。
- 将 CSAP-NTA-V200 的升级启动文件拷贝到文件服务器上，并正确设置 TFTP/FTP Server 的访问路径。

图5-3 产品升级环境示意图



5.4.2 使用 TFTP 协议升级 CSAP-NTA-V200 的启动文件

CSAP-NTA-V200 作为 TFTP 客户端，访问 TFTP 文件服务器的指定路径，完成启动文件的备份及升级操作，具体操作步骤如下：

1. 备份当前启动文件和配置文件

(1) 执行 **save** 命令，保存当前配置信息：

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg) [flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait....
Configuration is saved to device successfully.
<Sysname>
```

(2) 执行 **dir** 命令查看当前的文件系统，确认启动文件及配置文件名，以及存储的剩余空间，保证有足够空间放入新的启动文件：

```
<Sysname> dir
Directory of flash: (VFAT)
 0 drw-      - Jun 30 2020 05:39:20  diagfile
 1 -rw-      47 Jun 30 2020 06:32:46  ifindex.dat
 2 drw-      - Jun 30 2020 05:47:24  license
 3 drw-      - Jun 30 2020 06:32:46  logfile
 4 -rw-      768 Jun 30 2020 06:33:27  reboot.log
 5 drw-      - Jun 30 2020 05:39:20  seclog
 6 -rw-     2268 Jun 30 2020 06:32:46  startup.cfg
 7 -rw-     31526 Jun 30 2020 06:32:46  startup.mdb
 8 -rw-    8772608 Jun 30 2020 06:32:30  CSAP-NTA-V200-CMW710-BOOT-E1260P10-X64.bin
 9 -rw-   163973120 Jun 30 2020 06:32:32  CSAP-NTA-V200-CMW710-SYSTEM-E1260P10-X64.bin
10 -rw-   172752896 Jun 30 2020 06:31:14  CSAP-NTA-V200_H3C-CMW710-E1260P11-X64.ipe
11 -rw-     21016 Jun 30 2020 06:33:33  version.log

7325704 KB total (6988168 KB free)
<Sysname>
```

(3) 执行 **tftp put** 命令将启动文件备份到 TFTP 文件服务器上：

```
<Sysname> tftp 2.2.2.2 put CSAP-NTA-V200_H3C-CMW710-E1260P11-X64.ipe

File will be transferred in binary mode
```

```
Sending file to remote TFTP server. Please wait... \  
TFTP: 31131648 bytes sent in 70 second(s).  
File uploaded successfully.
```

<Sysname>

(4) 执行 **tftp put** 命令将配置文件 **startup.cfg** 备份到 TFTP 文件服务器上:

```
<Sysname> tftp 2.2.2.2 put startup.cfg  
File will be transferred in binary mode  
Sending file to remote TFTP server. Please wait... \  
TFTP: 1694 bytes sent in 0 second(s).  
File uploaded successfully.
```

<Sysname>

2. 升级启动文件

(1) 执行 **tftp get** 命令将启动文件导入到 NTA 中:

```
<Sysname> tftp 2.2.2.2 get CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe  
File will be transferred in binary mode  
Downloading file from remote TFTP server, please wait...|  
TFTP: 31131648 bytes received in 70 second(s)  
File downloaded successfully.
```

<Sysname>

(2) 执行 **boot-loader** 命令设置 NTA 下次启动使用的启动文件，并指定启动文件类型为 **main**:

```
<Sysname> boot-loader file flash:/CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe main  
Verifying the file flash:/CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe on the device...Done.  
H3C SecPath CSAP-NTA-V200 images in IPE:  
CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin  
CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin  
This command will set the main startup software images. Please do not reboot the  
device during the upgrade. Continue? [Y/N]:y  
Add images to the device.  
Decompressing file CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin to flash:/CSAP-NTA-V200-  
CMW710-BO  
OT-E1185-X64.bin...Done.  
Decompressing file CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin to flash:/CSAP-NTA-V200-  
CMW710-  
SYSTEM-E1185-X64.bin.....Done.  
Verifying the file flash:/CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin on the device...Done  
.  
Verifying the file flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin on the device...Do  
ne.  
The images that have passed all examinations will be used as the main startup so  
ftware images at the next reboot on the device.  
Decompression completed.  
You are recommended to delete the .ipe file after you set startup software image  
s for all slots.  
Do you want to delete flash:/CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe now? [Y/N]:n
```

<Sysname>

(3) 执行 **display boot-loader** 命令查看设备的启动程序文件信息:

```
<Sysname> display boot-loader
Software images on the device:
Current software images:
  flash:/CSAP-NTA-V200-CMW710-BOOT-E1260P10-X64.bin
  flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1260P10-X64.bin
Main startup software images:
  flash:/CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin
  flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin
Backup startup software images:
  None
```

<Sysname>

如上显示信息，下一次启动的程序文件已经设置为 **CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe** 中包含的 **CSAP-NTA-V200-CMW710-BOOT-E1260P10-X64.bin** 和 **CSAP-NTA-V200-CMW710-SYSTEM-E1260P10-X64.bin**。

5.4.3 使用 FTP 协议升级 CSAP-NTA-V200 的启动文件

将 **CSAP-NTA-V200** 作为 FTP 客户端，访问 FTP 文件服务器的指定路径，完成启动文件的备份及升级操作，具体操作步骤如下:

1. 备份当前启动文件和配置文件

(1) 执行 **save** 命令保存当前配置信息:

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait....
Configuration is saved to device successfully.
```

<Sysname>

(2) 执行 **dir** 命令查看当前的文件系统，确认启动文件及配置文件名，以及存储剩余空间，保证有足够空间放入新的启动文件:

```
<Sysname> dir
Directory of flash: (VFAT)
 0 drw-      - Jun 30 2020 05:39:20  diagfile
 1 -rw-      47 Jun 30 2020 06:32:46  ifindex.dat
 2 drw-      - Jun 30 2020 05:47:24  license
 3 drw-      - Jun 30 2020 06:32:46  logfile
 4 -rw-     768 Jun 30 2020 06:33:27  reboot.log
 5 drw-      - Jun 30 2020 05:39:20  seclog
 6 -rw-     2268 Jun 30 2020 06:32:46  startup.cfg
 7 -rw-    31526 Jun 30 2020 06:32:46  startup.mdb
 8 -rw-   8772608 Jun 30 2020 06:32:30  CSAP-NTA-V200-CMW710-BOOT-E1260P10-X64.bin
 9 -rw-  163973120 Jun 30 2020 06:32:32  CSAP-NTA-V200-CMW710-SYSTEM-E1260P10-X64.bin
```

```
10 -rw- 172752896 Jun 30 2020 06:31:14 CSAP-NTA-V200_H3C-CMW710-E1260P11-X64.ipe
11 -rw- 21016 Jun 30 2020 06:33:33 version.log
```

7325704 KB total (6988168 KB free)

<Sysname>

(3) 执行 ftp 命令登录 FTP 文件服务器，根据系统提示输入登录用户名和密码：

```
<Sysname> ftp 2.2.2.2
Press CTRL+C to abort.
Connected to 2.2.2.2 (2.2.2.2).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (2.2.2.2:(none)): user001
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS
ftp>
```

(4) 执行 put 命令将启动文件备份到 FTP 文件服务器上：

```
ftp> put CSAP-NTA-V200_H3C-CMW710-E1260P11-X64.ipe
227 Entering passive mode (2,2,2,2,209,112)
125 Using existing data connection
.....
.....
.....
.....
.....
226 Closing data connection; File transfer successful.
172752896 bytes sent in 3.508 seconds (46.96 Mbytes/s)
```

ftp>

(5) 执行 put 命令将配置文件 startup.cfg 备份到 FTP 文件服务器上：

```
ftp> put startup.cfg
227 Entering passive mode (2,2,2,2,209,126)
125 Using existing data connection
.
226 Closing data connection; File transfer successful.
2268 bytes sent in 0.010 seconds (214.22 Kbytes/s)
```

ftp>

2. 升级启动文件

(1) 在 FTP 客户端视图下，执行 get 命令将启动文件导入到 NTA 中：

```
ftp> get CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe
227 Entering passive mode (2,2,2,2,209,150)
125 Using existing data connection
.....
.....
```

```
.....  
.....  
.....  
226 Closing data connection; File transfer successful.  
181030912 bytes received in 13.071 seconds (13.21 Mbytes/s)
```

```
ftp>
```

(2) 执行 quit 命令返回到命令行配置界面的用户视图:

```
ftp>quit  
221 Service closing control connection  
<Sysname>
```

(3) 执行 boot-loader 命令, 设置 NTA 下次启动使用的启动文件, 并指定启动文件类型为 main:

```
<Sysname> boot-loader file flash:/ CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe main  
Verifying the file flash:/CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe on the device...Done.  
H3C SecPath CSAP-NTA-V200 images in IPE:  
  CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin  
  CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin  
This command will set the main startup software images. Please do not reboot the  
device during the upgrade. Continue? [Y/N]:y  
Add images to the device.  
Decompressing file CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin to flash:/CSAP-NTA-V200-  
CMW710-BO  
OT-E1185-X64.bin...Done.  
Decompressing file CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin to flash:/CSAP-NTA-V200-  
CMW710-  
SYSTEM-E1185-X64.bin....Done.  
Verifying the file flash:/CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin on the device...Done  
.  
Verifying the file flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin on the device...Do  
ne.  
The images that have passed all examinations will be used as the main startup so  
ftware images at the next reboot on the device.  
Decompression completed.  
You are recommended to delete the .ipe file after you set startup software image  
s for all slots.  
Do you want to delete flash:/CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe now? [Y/N]:n
```

```
<Sysname>
```

(4) 执行 display boot-loader 命令查看设备的启动程序文件信息:

```
<Sysname> display boot-loader  
Software images on the device:  
Current software images:  
  flash:/CSAP-NTA-V200-CMW710-BOOT-E1260P10-X64.bin  
  flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1260P10-X64.bin  
Main startup software images:  
  flash:/CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin  
  flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin
```

Backup startup software images:

None

<Sysname>

如上显示信息中，下一次启动的程序文件已设置为 CSAP-NTA-V200_H3C-CMW710-E1185-X64.ipe 文件中的 CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin 和 CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin。

5.4.4 重启 CSAP-NTA-V200 设备

升级完启动文件后，需要重新启动设备来实现设备软件的升级。



注意

在重启过程完成前，设备的各项业务功能将不可用。

(1) 执行 `reboot` 命令重启 CSAP-NTA-V200:

```
<Sysname> reboot
```

```
Start to check configuration with next startup configuration file, please  
wait.....DONE!
```

```
This command will reboot the device. Continue? [Y/N]:y
```

```
Now rebooting, please wait...
```

(2) 通过 `display version` 命令查看 CSAP-NTA-V200 的启动文件版本信息是否与升级的启动文件一致:

```
<Sysname>display version
```

```
H3C Comware Software, Version 7.1.064, ESS 1185
```

```
Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights reserved.
```

```
H3C SecPath CSAP-NTA-V200 uptime is 0 weeks, 0 days, 0 hours, 1 minute
```

```
Last reboot reason : User reboot
```

```
Boot image: flash:/CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin
```

```
Boot image version: 7.1.064, ESS 1185
```

```
Compiled May 27 2020 15:00:00
```

```
System image: flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin
```

```
System image version: 7.1.064, ESS 1185
```

```
Compiled May 27 2020 15:00:00
```

```
CPU ID: 0x01000101, vCPUs: Total 1, Available 1
```

```
2.00G bytes RAM Memory
```

```
Basic BootWare Version: 1.11
```

```
Extended BootWare Version: 1.11
```

```
[SLOT 1]VNIC-E1000 (Driver)1.0<Sysname>
```

5.5 通过ISO升级产品



说明

产品的升级方式相同，下面将以 CSAP-NTA-V200 为例进行介绍。

- (1) 初始升级步骤和通过 ISO 安装 CSAP-NTA-V200 是相同的，请参见 [3.2 在 VMware 平台安装](#)、[3.3 在 KVM 平台安装](#)或 [3.4 在 CAS 平台安装](#)。
- (2) 在进入安装界面后，注意选择菜单<2> Upgrade Install，如下图所示，将 CSAP-NTA-V200 运行的版本升级到 ISO 光盘中的版本。

图5-4 通过 ISO 升级 CSAP-NTA-V200

```
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "/opt/USR/setup_usr.sh" now.
Found and Mounted a CD-ROM.

=====<uFW INSTALL MENU>=====
|<1> Fresh Install |
|<2> Upgrade Install |
|<3> Recovery Install |
|<4> IRF Install |
|<5> Debug Mode |
|<0> Reboot |
=====
Enter your choice(0-5): 2
```

- (3) 安装完成后，注意先断开 CD 连接，如[错误!未找到引用源。](#)、[错误!未找到引用源。](#)所示，然后重启系统。
- (4) 设备重启后，查看 NTA 的启动文件版本信息是否与升级的启动文件一致：

```
<Sysname>display version
H3C Comware Software, Version 7.1.064, ESS 1185
Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath CSAP-NTA-V200 uptime is 0 weeks, 0 days, 0 hours, 1 minute
Last reboot reason : User reboot
Boot image: flash:/CSAP-NTA-V200-CMW710-BOOT-E1185-X64.bin
Boot image version: 7.1.064, ESS 1185
  Compiled May 27 2020 15:00:00
System image: flash:/CSAP-NTA-V200-CMW710-SYSTEM-E1185-X64.bin
System image version: 7.1.064, ESS 1185
  Compiled May 27 2020 15:00:00

CPU ID: 0x01000101, vCPUs: Total 1, Available 1
2.00G bytes RAM Memory
Basic BootWare Version: 1.11
Extended BootWare Version: 1.11
[SLOT 1]VNIC-E1000 (Driver)1.0
<Sysname>
```

6 恢复产品



说明

产品的恢复方式相同，下面将以 CSAP-NTA-V200 为例进行介绍。

CSAP-NTA-V200 可以通过 ISO 进行恢复，步骤如下：

- (1) 初始恢复步骤和通过 ISO 安装 CSAP-NTA-V200 是相同的，请参见 [3.2 在 VMware 平台安装](#)、[3.3 在 KVM 平台安装](#)或 [3.4 在 CAS 平台安装](#)。
- (2) 进入安装界面后，注意选择菜单<3> Recovery Install，如下图所示，将 CSAP-NTA-V200 运行的版本恢复到 ISO 光盘中的版本。

图6-1 通过 ISO 恢复 CSAP-NTA-V200 的版本

```
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "/opt/USR/setup_usr.sh" now.
Found and Mounted a CD-ROM.

=====<uFW INSTALL MENU>=====
|<1> Fresh Install |
|<2> Upgrade Install |
|<3> Recovery Install |
|<4> IRF Install |
|<5> Debug Mode |
|<0> Reboot |
=====
Enter your choice(0-5): 3
```

- (3) 安装完成后，然后重启系统。

7 附录 B: OVS bridge

Linux bridge 产生的 bridge 无法提供 VLAN 隔离功能，如果需要使用 VLAN 隔离功能，可以使用 OVS bridge 来代替 Linux bridge。

配置 OVS bridge 前，请先安装 Openvswitch。Openvswitch 的安装方法请参见安装指导。

7.1 配置 OVS bridge

(1) OVS bridge 配置

将 toMarketToolsV1.x.zip 压缩包上传到 CentOS 7 服务器上，解压后，根据需要执行操作：

- 过滤支持 SR-IOV 的网卡

在路径 toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v1/ovs，执行 ./ovs-setup-deb.sh -i 命令完成 OVS bridge 的配置。

```
[root@localhost ~]# unzip toMarketToolsV1.x.zip
[root@localhost ~]# cd toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v1/ovs
[root@localhost ovs]# chmod 777 ./ovs-setup-deb.sh
[root@localhost ovs]# ./ovs-setup-deb.sh -i
Network default destroyed
```

```
Network default unmarked as autostarted
```

```
remove module bridge
openvswitch install complete.
network config ens160 to ovs-bridge br0 complete.
```

- 不过滤支持 SR-IOV 的网卡

在路径 toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v2/ovs，执行 ./ovs-setup-deb.sh -i 命令完成 OVS bridge 的配置。

```
[root@localhost ~]# unzip toMarketToolsV1.x.zip
[root@localhost ~]# cd toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v2/ovs
[root@localhost ovs]# chmod 777 ./ovs-setup-deb.sh
[root@localhost ovs]# ./ovs-setup-deb.sh -i
Network default destroyed
```

```
Network default unmarked as autostarted
```

```
remove module bridge
openvswitch install complete.
network config ens160 to ovs-bridge br0 complete.
```



说明

配置 OVS bridge 的脚本文件 `toMarketToolsV1.x.zip` 是和 CSAP-NTA-V200 的版本一起发布的，可在获取 CSAP-NTA-V200 版本时一同获取。

`chmod 777 ./ovs-setup-deb.sh` 命令用于更改命令权限。该命令为可选命令，如果执行 `./ovs-setup-deb.sh -i` 时提示 `permission denied`，需要使用该命令。

`Create_Bridge_shell_v1` 和 `Create_Bridge_shell_v2` 两个版本的差异：

- v1 版本创建桥时会过滤支持 SR-IOV 的网卡，v2 版本不会过滤支持 SR-IOV 的网卡。
- v1 版本创建 ovs 桥时会过滤掉支持 SR-IOV 的网卡，v2 版本不会过滤支持 SR-IOV 的网卡。

(2) 确认是否执行成功

执行完脚本后，通过下面的操作确认是否执行成功：

```
[root@localhost h3c]# ovs-vsctl show
2bc21194-95b8-48df-929f-a2fdc8842723

    Bridge "br0"
        Port "br0"
            Interface "br0"
                type: internal
        Port "eno1"
            Interface "eno1"
        .....
    Bridge "br6"
        Port "ens2f0"
            Interface "ens2f0"
        Port "br6"
            Interface "br6"
                type: internal
    ovs_version: "2.3.1"
```

如果看到每个 Bridge 中有一个 Port 口对应物理接口，说明创建 OVS 桥正常。

(3) 查看 network-scripts 配置文件

查看生成的 `network-scripts` 配置文件是否正确，以 `eno1`、`br0` 为例。

```
[root@localhost h3c]# cat /etc/sysconfig/network-scripts/ifcfg-br0
DEVICE=br0
HWADDR=c4:34:6b:b8:b1:0c
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.1.25
NETMASK=255.255.0.0

[root@localhost h3c]# cat /etc/sysconfig/network-scripts/ifcfg-eno1
DEVICE=eno1
HWADDR=c4:34:6b:b8:b1:0c
TYPE=Ethernet
```

```

BOOTPROTO=static
ONBOOT=yes
[root@localhost h3c]# ifconfig br0
br0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 2002:6200:101:b:c634:6bff:feb8:b10c prefixlen 64 scopeid 0x0<global>
    inet6 2002:6100:2f4:b:c634:6bff:feb8:b10c prefixlen 64 scopeid 0x0<global>
    inet6 fec0::b:c634:6bff:feb8:b10c prefixlen 64 scopeid 0x40<site>
    inet6 fec0::5:c634:6bff:feb8:b10c prefixlen 64 scopeid 0x40<site>
    inet6 2002:aca8:284d:5:c634:6bff:feb8:b10c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::c634:6bff:feb8:b10c prefixlen 64 scopeid 0x20<link>
    ether c4:34:6b:b8:b1:0c txqueuelen 0 (Ethernet)
    RX packets 59563399 bytes 14654045807 (13.6 GiB)
    RX errors 0 dropped 27785742 overruns 0 frame 0
    TX packets 954617 bytes 58597317 (55.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost h3c]# ifconfig eno1
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::c634:6bff:feb8:b10c prefixlen 64 scopeid 0x20<link>
    ether c4:34:6b:b8:b1:0c txqueuelen 1000 (Ethernet)
    RX packets 57371550 bytes 14237402755 (13.2 GiB)
    RX errors 0 dropped 430 overruns 0 frame 0
    TX packets 802515 bytes 56395122 (53.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16

```

参数说明:

- **DEVICE:** 接口名称, 需与 `ifconfig` 看到的一致。
- **TYPE:** 接口类型, OVS 桥、物理接口配置文件中取值均为 `Ethernet`。
- **BOOTPROTO:** `[none|dhcp|static]`, 表示引导时[不使用任何协议|; 使用 `dhcp` 协议获取地址|; 使用静态配置 IP]。OVS 桥、物理接口配置文件取值均为 `static`。
- **ONBOOT:** `[yes|no]`, 表示引导时[是|否]激活设备。此处值需为 `yes`。
- **IPADDR:** IP 地址, 物理接口上的 IP 转移到桥上, 配置文件中不存在该选项。OVS 桥配置文件中取值为原物理口配置的 IP 值, 与 `ifconfig` 中的 `inet` 值一致。
- **NETMASK:** IP 子网掩码, 同 `IPADDR`。
- **HWADDR:** MAC 地址, OVS 桥、物理接口配置文件中取值与 `ifconfig` 查看到 `ether` 一致。



提示

由于执行创建 OVS bridge 脚本的过程中会重启网络服务, 所以请通过服务器自带登录系统登录设备完成操作, 不要通过网络远程登录到服务器进行该操作。

7.2 配置OVS网卡的MTU

(1) 配置 OVS 网卡的 MTU，根据需要执行操作：

- 过滤支持 SR-IOV 的网卡

在路径 `toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v1/ovs` 下，执行 `./setMtu.sh phyNic mtuSize` 命令配置物理网卡和对应 vnet 的 MTU 值：

```
[root@localhost ovs]# chmod 777 ./setMtu.sh
[root@localhost ovs]# ./setMtu.sh eno2 3000
eno2 mtu set to 3000 complete.
```

- 不过滤支持 SR-IOV 的网卡

在路径 `toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v2/ovs` 下，执行 `./setMtu.sh phyNic mtuSize` 命令配置物理网卡和对应 vnet 的 MTU 值：

```
[root@localhost ovs]# chmod 777 ./setMtu.sh
[root@localhost ovs]# ./setMtu.sh eno2 3000
eno2 mtu set to 3000 complete.
```

(2) 以 `eno2`、`br1` 为例，通过命令查看是否配置成功：

```
[root@localhost ovs]# ifconfig eno2 | grep mtu
eno2: flags=4099<UP,BROADCAST,MULTICAST> mtu 3000
[root@localhost ovs]# ifconfig br1 | grep mtu
br1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 3000
[root@localhost ovs]# cat /etc/sysconfig/network-scripts/ifcfg-eno1 | grep -i mtu
MTU=1600
```

7.3 删除OVS bridge配置

- 过滤支持 SR-IOV 的网卡

在路径 `toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v1/ovs` 下，执行 `./ovs-setup-deb.sh -r` 命令删除 OVS bridge 配置。

```
[root@localhost ovs]# chmod 777 ./ovs-setup-deb.sh
[root@localhost ovs]# ./ovs-setup-deb.sh -r
network unconfig ovs-bridge br0 to ens160 complete.
Stopping openvswitch (via systemctl): [ OK ]
Network default started
```

```
Network default marked as autostarted
```

- 不过滤支持 SR-IOV 的网卡

在路径 `toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v2/ovs` 下，执行 `./ovs-setup-deb.sh -r` 命令删除 OVS bridge 配置。

```
[root@localhost ovs]# chmod 777 ./ovs-setup-deb.sh
[root@localhost ovs]# ./ovs-setup-deb.sh -r
network unconfig ovs-bridge br0 to ens160 complete.
```

```
Stopping openswitch (via systemctl): [ OK ]
Network default started

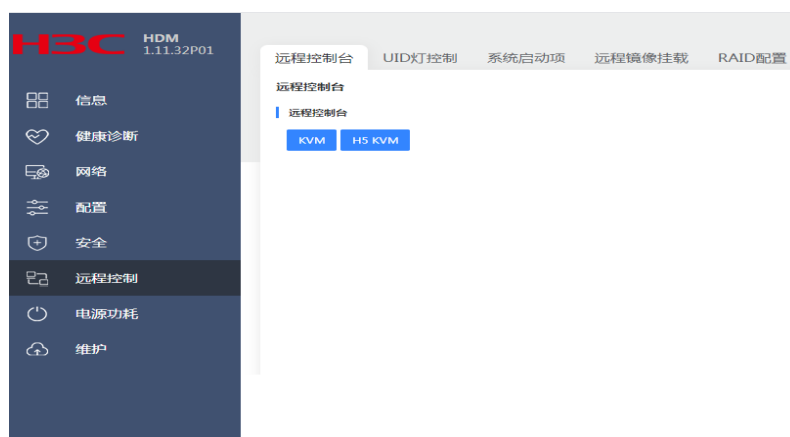
Network default marked as autostarted
```

8 KVM 和 VMware 平台安装

8.1 VMware平台安装

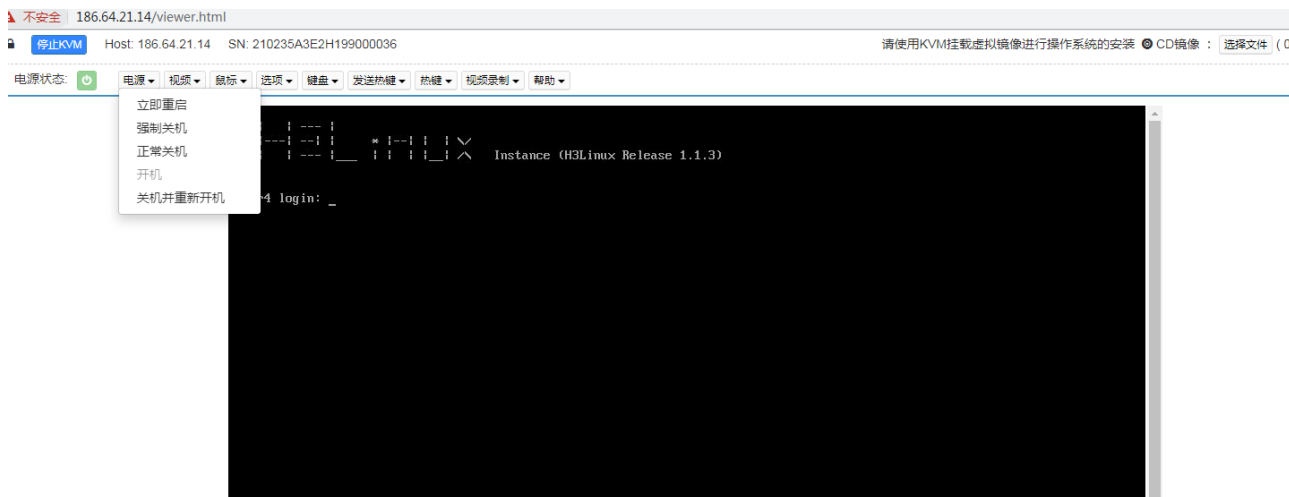
1. ISO 镜像加载

- (1) 交换机的网线需要先链接到服务器的 HDM 口上。
- (2) 在浏览器中输入服务器的 HDM 地址，例如：<https://192.168.100.179/index.html>。
- (3) 打开网页后，会出现如下图所示界面，选择[远程控制台->远程控制台-> H5 KVM]。默认密码：admin/Password@_

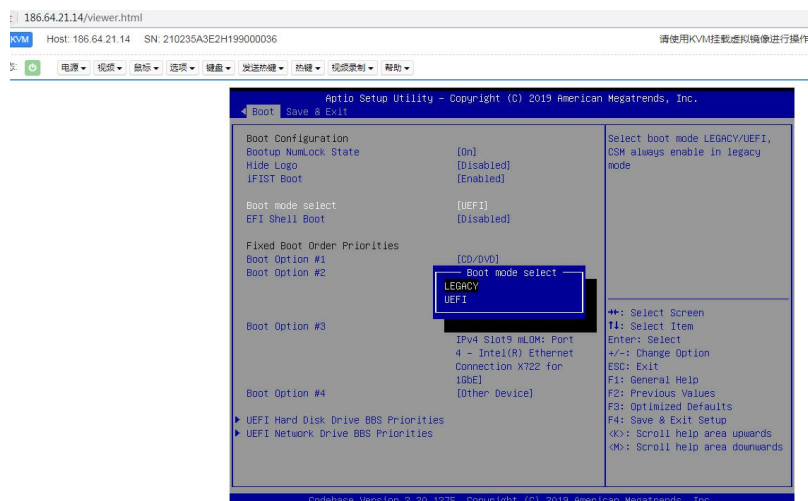


- (4) 登录成功后，打开 H5 kvm 会出现[错误!未找到引用源。](#)所示界面,点击立即重启。

图8-1 成功登录服务器



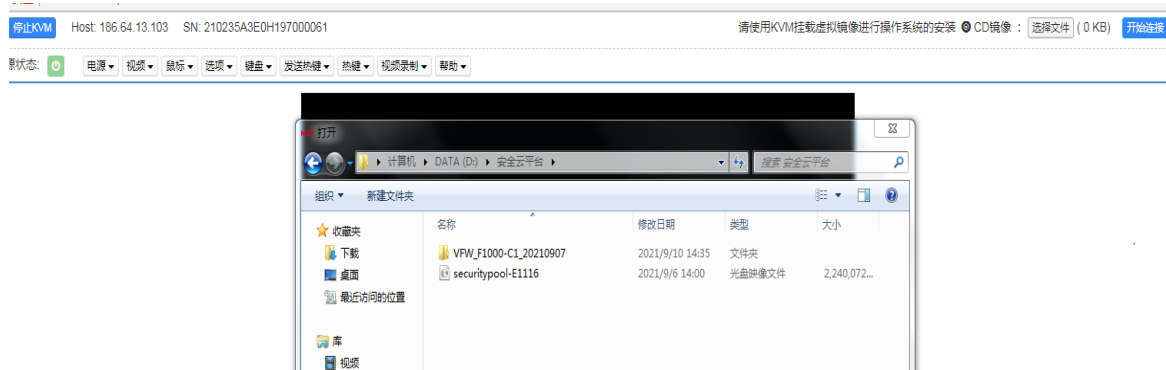
- (5) 在弹出的页面，点击电源—立即重启，开机的过程中，按 ‘Esc’进入 BIOS 界面，进入 boot 界面，boot mode select 更改为'legacy',如下图



- (6) 如下图 第一启动项更改为 CD/DVD，第二启动项更改为硬盘启动，最后保存配置

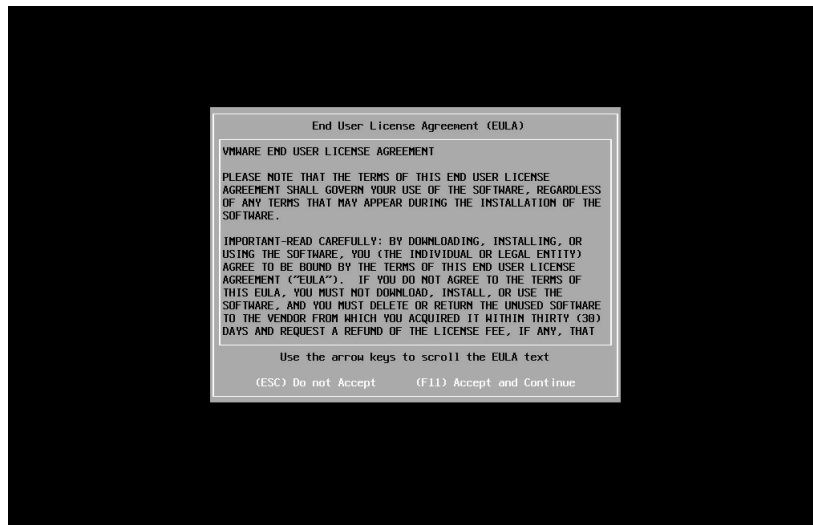


- (7) 点击左上角选择文件--选中需要安装的 ISO 文件—开始连接，连接虚拟机的 CD 设备到 ESXi-5.x-Custom 的安装 ISO 文件上，等待虚拟机自动读取安装映像，如下图

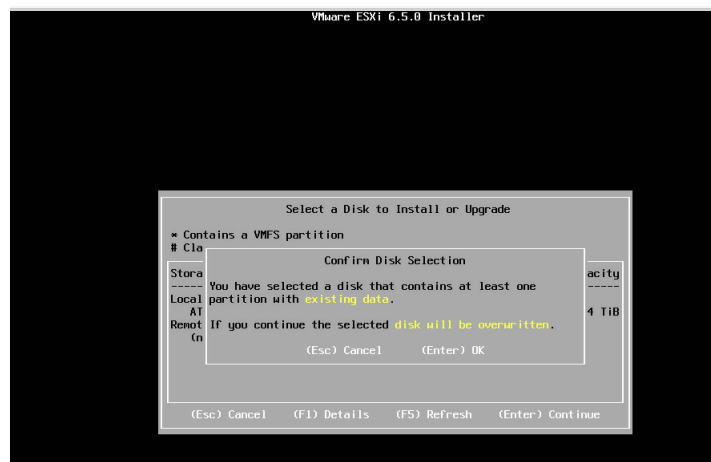


2. 安装 VMware 平台

- (1) 加载完镜像后，等待安装—按 “F11” 选择 Accept and contion.



(2) 在按“Enter”,弹出以下界面



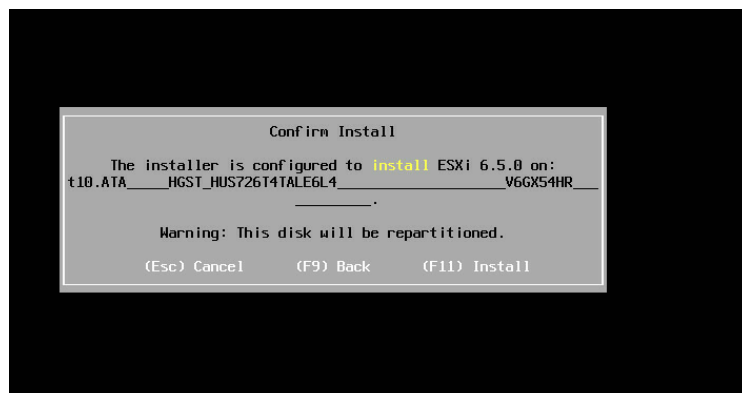
(3) 选择默认语言, 输入“Enter”



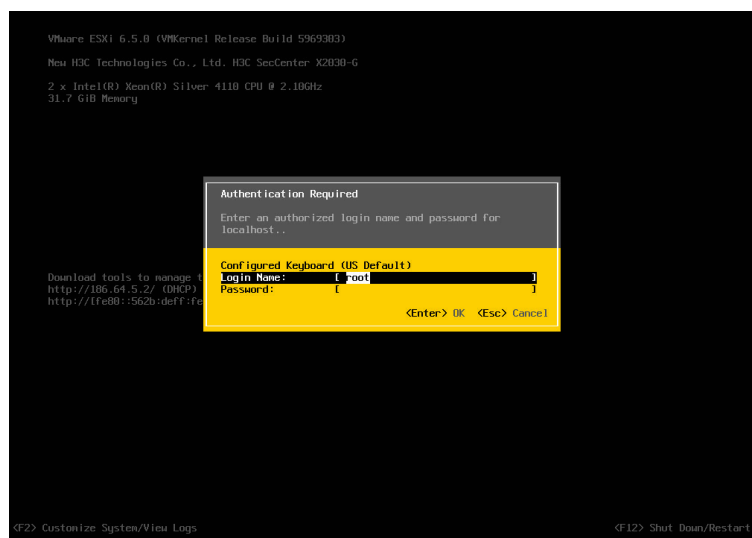
(4) 输入用户名和密码, 再输入“Enter”, 密码至少7位



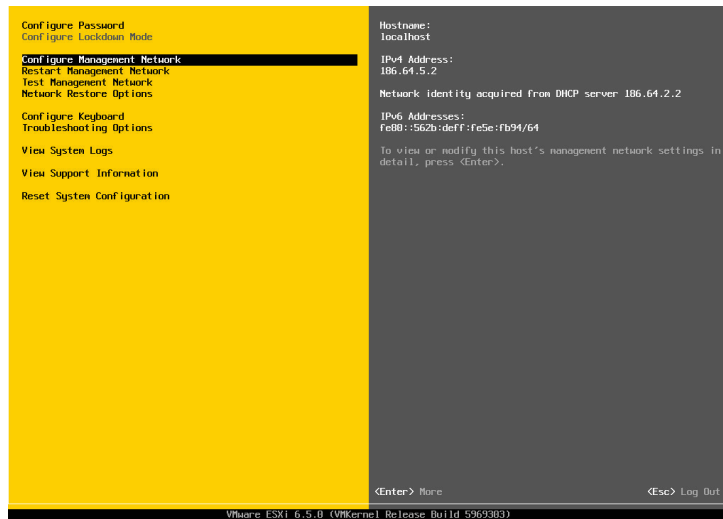
(5) 输入“F11”，开始安装。



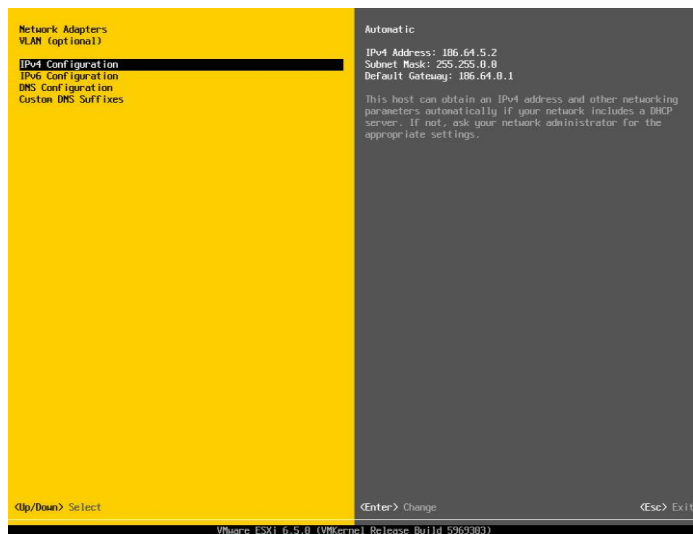
(6) 加载完系统，输入“F2”，弹出图 3-35 界面，输入密码，此处密码与刚才输入密码相同



(7) 输入密码后，弹出以下界面，选择“Configure Management Network”



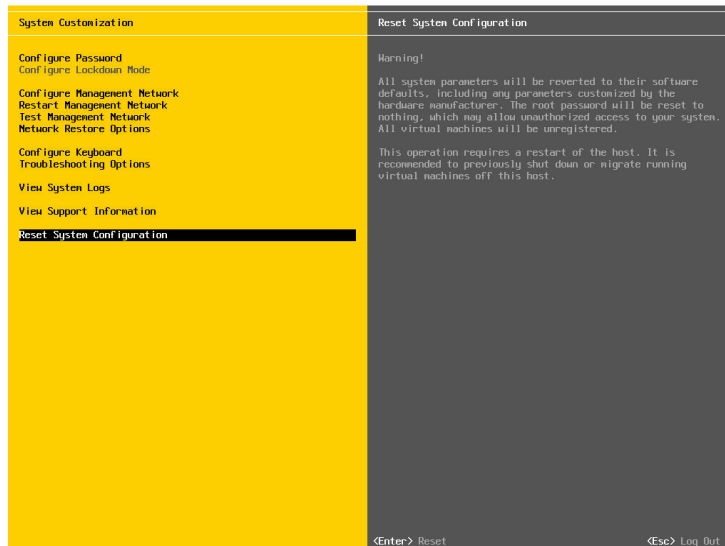
(8) 选择“IPv4 Configuration”编辑 IP 和网关。此处地址为 web 登录地址



(9) 编辑完 IP、网关后，保存，重启系统选择“reset system configure”



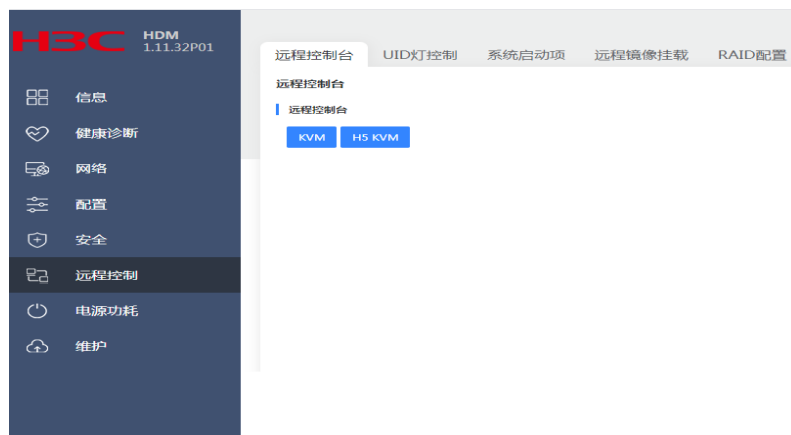
(10) 选择“reset system configure”，重启系统



8.2 KVM平台安装

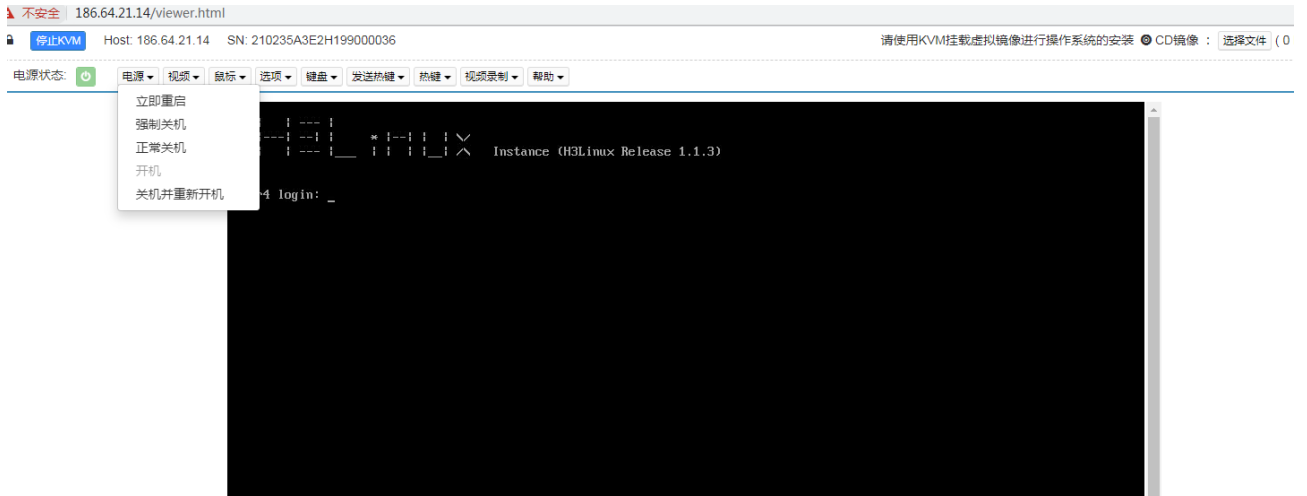
1. 利用 HDM 访问裸金属

- (1) 交换机的网线需要先链接到服务器的 HDM 口上。
- (2) 在浏览器中输入服务器的 HDM 地址，例如：<https://192.168.100.179/index.html>。
- (3) 打开网页后，会出现如下图所示界面，选择[远程控制台->远程控制台-> H5 KVM]。默认密码：admin/Password@_

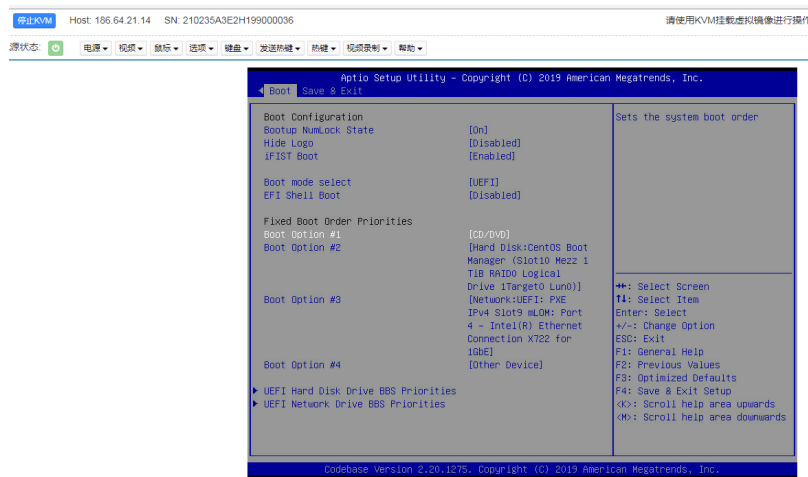


- (4) 登录成功后，打开 H5 kvm 会出现[错误!未找到引用源。](#)所示界面,点击立即重启。

图8-2 成功登录服务器

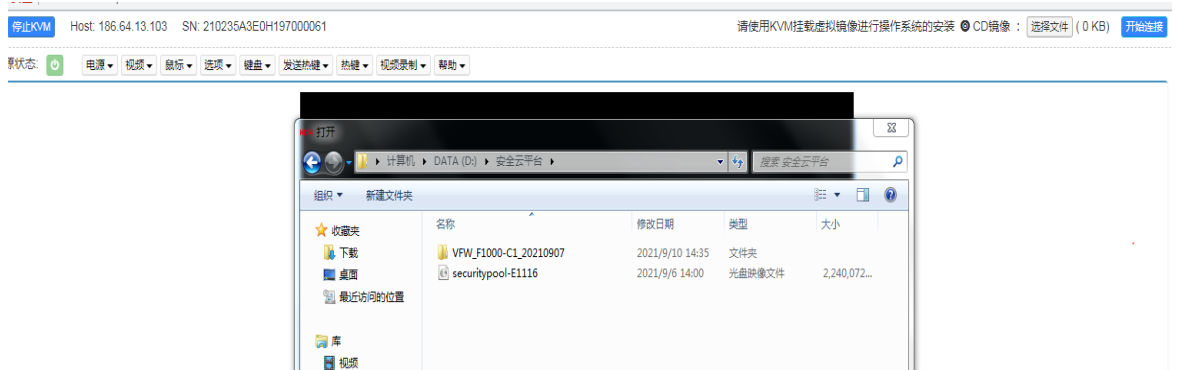


(5) 如下图 第一启动项更改为 CD/DVD, 第二启动项更改为硬盘启动, 最后保存配置



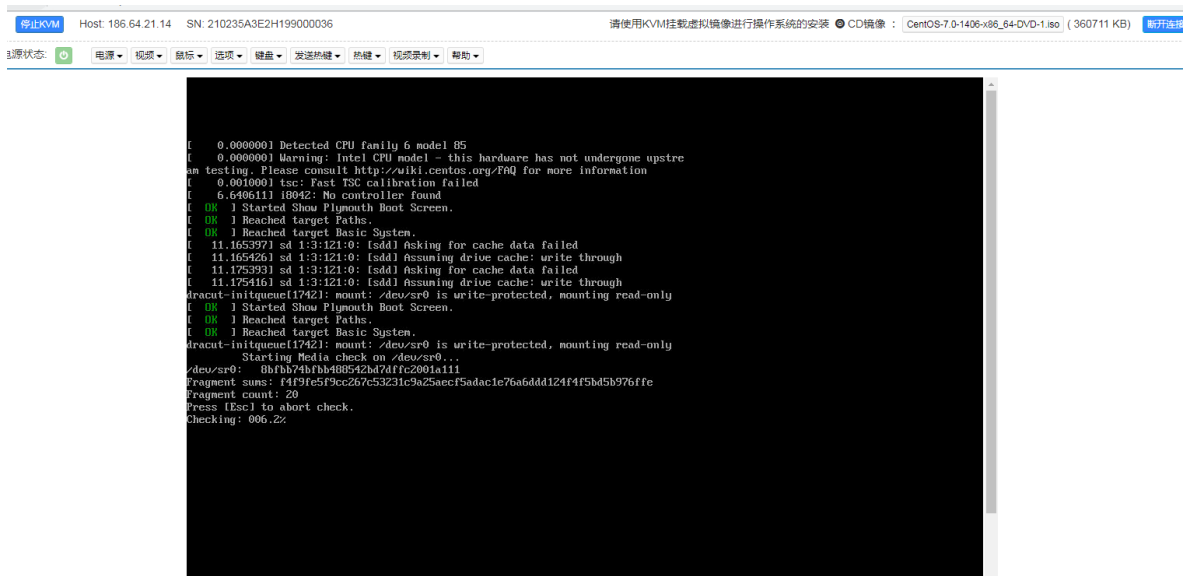
(6) 点击左上角选择文件--选中需要安装的 ISO 文件—开始连接, 连接虚拟机的 CD 设备到 CentOS-7.0-1406-x86_64-DVD-1 的安装 ISO 文件上, 等待虚拟机自动读取安装映像, 如下

图



2. 安装 KVM 平台

(1) 加载镜像后弹出以下界面, 等待自动安装



(2) 加载镜像后弹出以下界面，等待自动安装，安装完成后，选择中文



(3) 在安装信息摘要页面，点击<SOFTWARE SELECTION>，开始选择安装的软件，如图所示。



(4) 在选择安装软件界面，选择安装的虚拟化组件。为了方便虚拟机的管理以及确保虚拟化组件被正确安装，请按照选择图中红色框所示进行选择，然后点击<Done>。

SOFTWARE SELECTION CENTOS 7 INSTALLATION

Done us

Base Environment

- Minimal Install**
Basic functionality.
- Infrastructure Server**
Server for operating network infrastructure services.
- File and Print Server**
File, print, and storage server for enterprises.
- Basic Web Server**
Server for serving static and dynamic internet content.
- Virtualization Host**
Minimal virtualization host.
- Server with GUI**
Server for operating network infrastructure services, with a GUI.
- GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.
- KDE Plasma Workspaces**

Add-Ons for Selected Environment

- Remote Management for Linux**
Remote management interface for CentOS Linux, including OpenLMI and SNMP.
- Resilient Storage**
Clustered storage, including the GFS2 file system.
- Virtualization Client**
Clients for installing and managing virtualization instances.
- Virtualization Hypervisor**
Smallest possible virtualization host installation.
- Virtualization Tools**
Tools for offline virtual image management.
- Compatibility Libraries**
Compatibility libraries for applications built on previous versions of CentOS Linux.

SOFTWARE SELECTION CENTOS 7 INSTALLATION

Done us

Base Environment

- Minimal Install**
Basic functionality.
- Infrastructure Server**
Server for operating network infrastructure services.
- File and Print Server**
File, print, and storage server for enterprises.
- Basic Web Server**
Server for serving static and dynamic internet content.
- Virtualization Host**
Minimal virtualization host.
- Server with GUI**
Server for operating network infrastructure services, with a GUI.
- GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.
- KDE Plasma Workspaces**

Add-Ons for Selected Environment

- Machine and user identity servers.**
- E-mail Server**
Allows the system to act as a SMTP and/or IMAP e-mail server.
- FTP Server**
Allows the system to act as an FTP server.
- File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
- Hardware Monitoring Utilities**
A set of tools to monitor server hardware.
- High Availability**
Infrastructure for highly available services and/or shared storage.
- Identity Management Server**
Centralized management of users, servers and authentication policies.
- Infiniband Support**

SOFTWARE SELECTION CENTOS 7 INSTALLATION

Done us

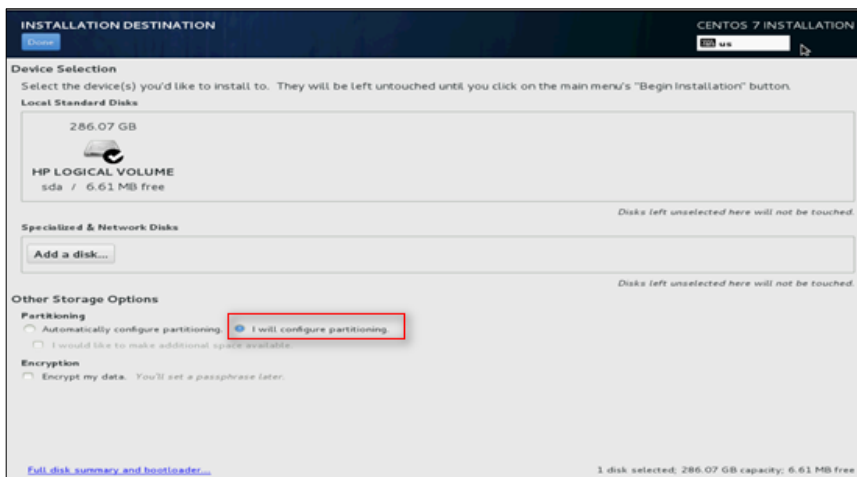
Base Environment

- Minimal Install**
Basic functionality.
- Infrastructure Server**
Server for operating network infrastructure services.
- File and Print Server**
File, print, and storage server for enterprises.
- Basic Web Server**
Server for serving static and dynamic internet content.
- Virtualization Host**
Minimal virtualization host.
- Server with GUI**
Server for operating network infrastructure services, with a GUI.
- GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.
- KDE Plasma Workspaces**

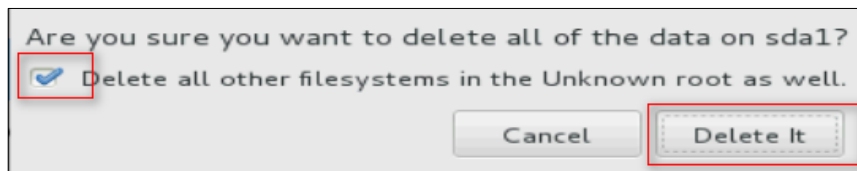
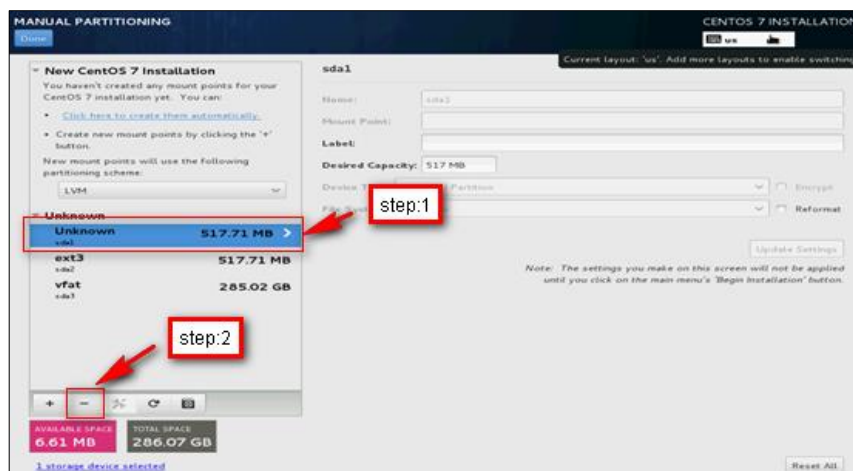
Add-Ons for Selected Environment

- High Availability**
Infrastructure for highly available services and/or shared storage.
- Identity Management Server**
Centralized management of users, servers and authentication policies.
- Infiniband Support**
Software designed for supporting clustering and grid connectivity using RDMA-based InfiniBand and iWARP fabrics.
- Java Platform**
Java support for the CentOS Linux Server and Desktop Platforms.
- KDE**
The KDE Plasma Workspaces, a highly-configurable graphical user interface which includes a panel, desktop, system icons and desktop widgets, and many powerful KDE applications.

- (5) 选择了待安装的虚拟化组件后，将自动返回的安装信息摘要界面，点击<INSTALLATION DESTINATION>进入下[错误!未找到引用源。](#)示选择系统安装路径界面。按照红框所示选择，自定义安装磁盘分区，然后点击<Done>按钮完成自定义安装路径设置。

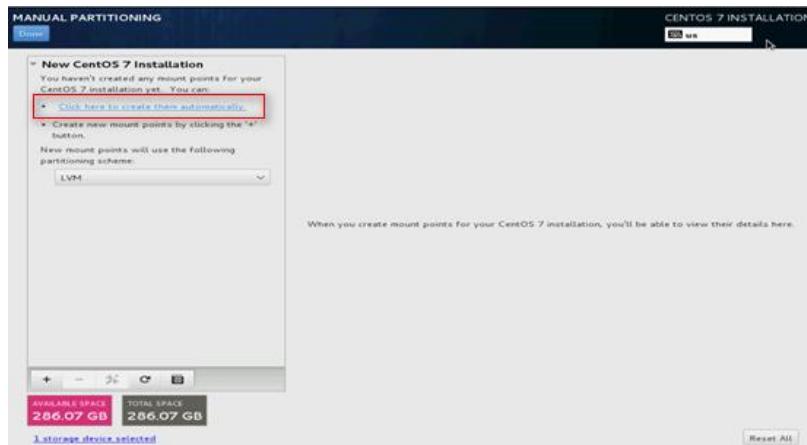


- (6) 进入自定义界面后，按照[错误!未找到引用源。](#)中红色框所示的步骤点击<Unknown>，然后点击 ‘-’ 释放 Unknown 空间。在弹出的提示框中，按照[错误!未找到引用源。](#)中红色框所示进行操作。



- (7) 删除 Unknown 空间后，请在图 8-33 所示的界面中，点击“Click here to create them automatically”，来自动创建磁盘分区。

图8-3 自动创建磁盘分区



(8) 由于虚拟机的镜像存放在/var 或者/opt 子目录下的，需要“/”分区比较大，而系统自动分配的 home 分区所占用的空间比较大，因此建议删除“/home”分区，并把其所占的空间添加到“/”分区。其他用来存放系统文件的分区可保持不变。删除“home”分区空间的步骤如图8-4所示，为“/”分区增加空间的步骤如图8-5所示。

图8-4 删除“/home”分区空间

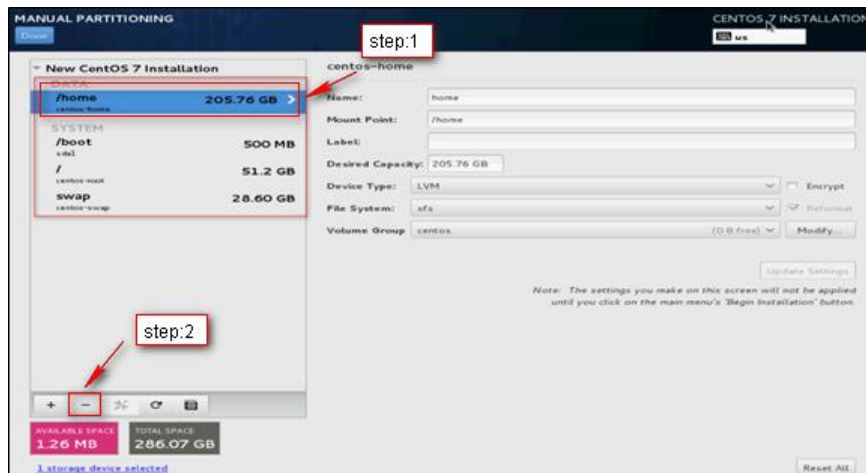
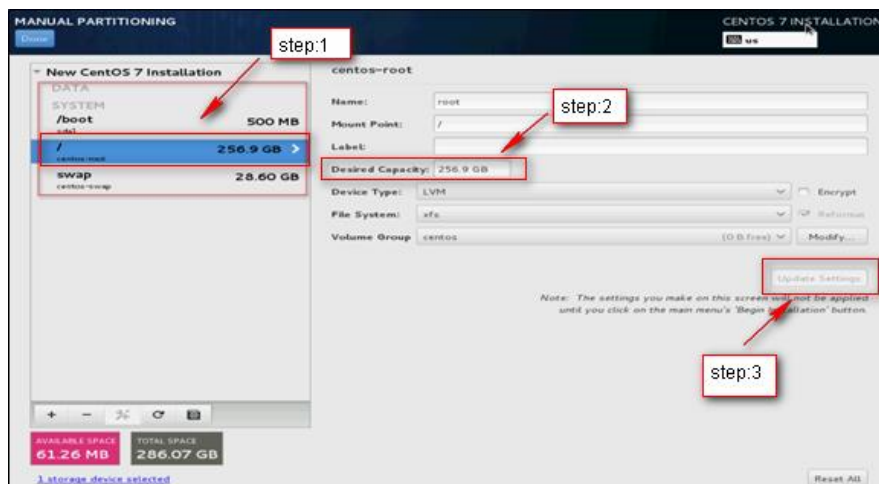


图8-5 为“/”分区添加空间



 说明

目前系统启动方式有 Legacy BIOS Mode 和 UEFI Mode 两种模式。在 UEFI Mode 模式下删除磁盘空间时，请不要删除“/boot/efi”分区，因为该分区是用于系统引导的。

- (9) 为了增加系统稳定性，降低服务器突然掉电时虚拟机镜像文件被写坏的概率，建议修改分区的“Device Type”以及 File System”配置。如图 8-6 中，更改了“/”分区的设备类型及文件系统配置。各分区请按照表 8-1 进行设置：

图8-6 更改“/”分区配置

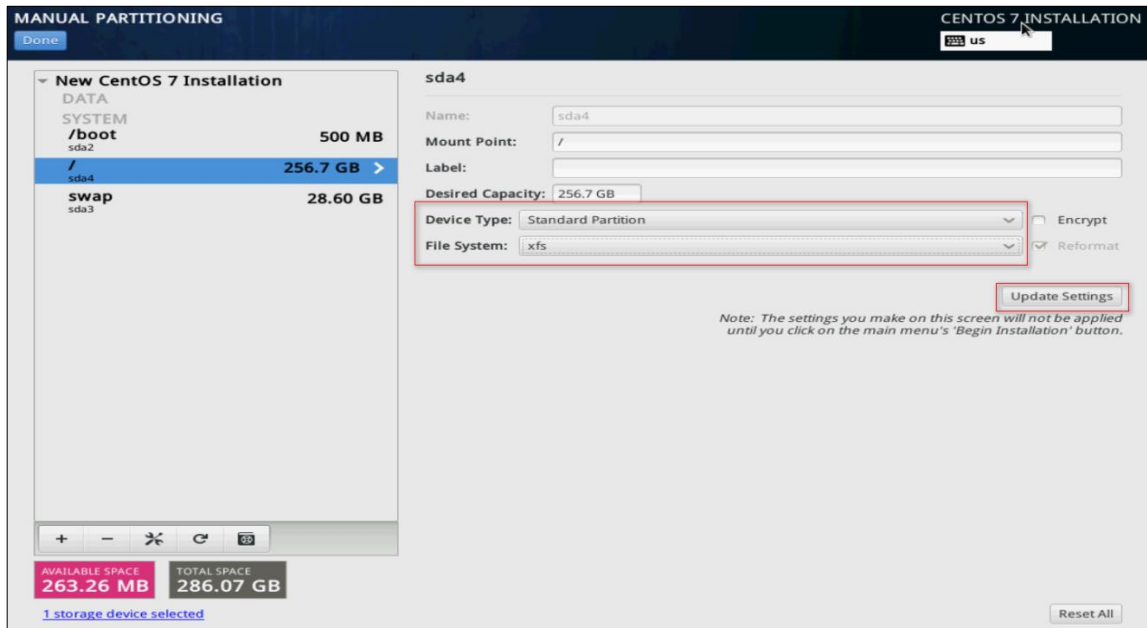


表8-1 更改分区配置

	分区名称	
/boot		标准分区
/boot/efi (只有UEFI模式才有)		标准分区
/		标准分区
swap		标准分区

- (10) 完成上述配置后，点击<Done>按钮，此时出现图 8-7 所示提示框，请点击“Accept Changes”，完成自定义安装磁盘分区类型和文件系统格式的设置。

图8-7 保存设置



SUMMARY OF CHANGES

Your customizations will result in the following changes taking effect on the disks you've selected:

Order	Action	Type	Device Name	Mountpoint
1	Destroy Format	vfat	sda3	
2	Destroy Device	partition	sda3	
3	Destroy Format	ext3	sda2	
4	Destroy Device	partition	sda2	
5	Destroy Device	partition	sda1	
6	Destroy Format	partition table (MSDOS)	sda	
7	Create Format	partition table (MSDOS)	sda	
8	Create Device	partition	sda1	
9	Create Device	partition	sda2	
10	Create Device	partition	sda3	
11	Create Format	swap	sda3	

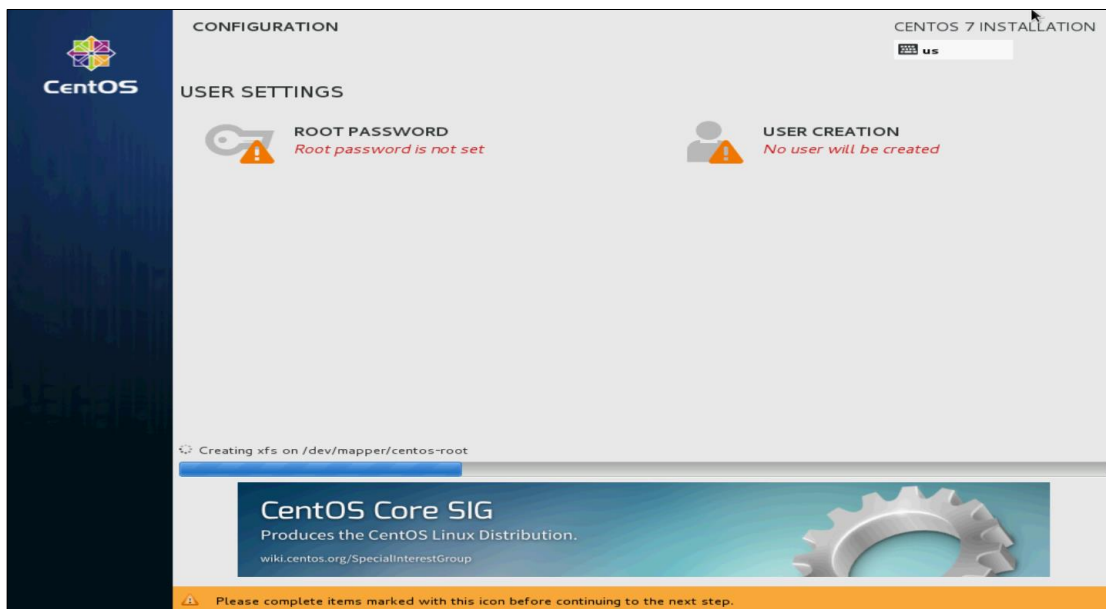
Buttons: Cancel & Return to Custom Partitioning, Accept Changes

 提示

添加设备文件时，请将 Device Type 设置成标准类型，文件系统设置成 xfs 类型，以便降低服务器异常掉电时对部分文件损坏的概率。

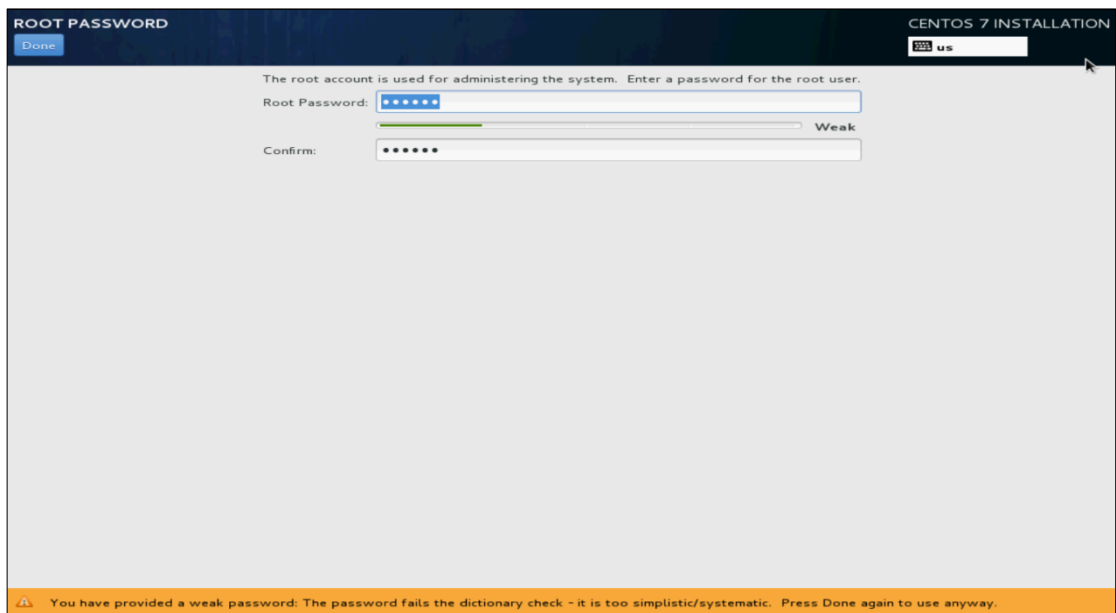
(11) 完成磁盘格式设置后，在返回的安装信息摘要界面中，点击<Begin Installation>，进入图 8-8 所示的安装过程界面。点击<ROOT PASSWORD>，开始设置 root 密码。

图8-8 安装过程界面



(12) 在图 8-9 所示界面设置 root 密码，然后点击<Done>按钮，完成密码设置。

图8-9 设置 root 密码

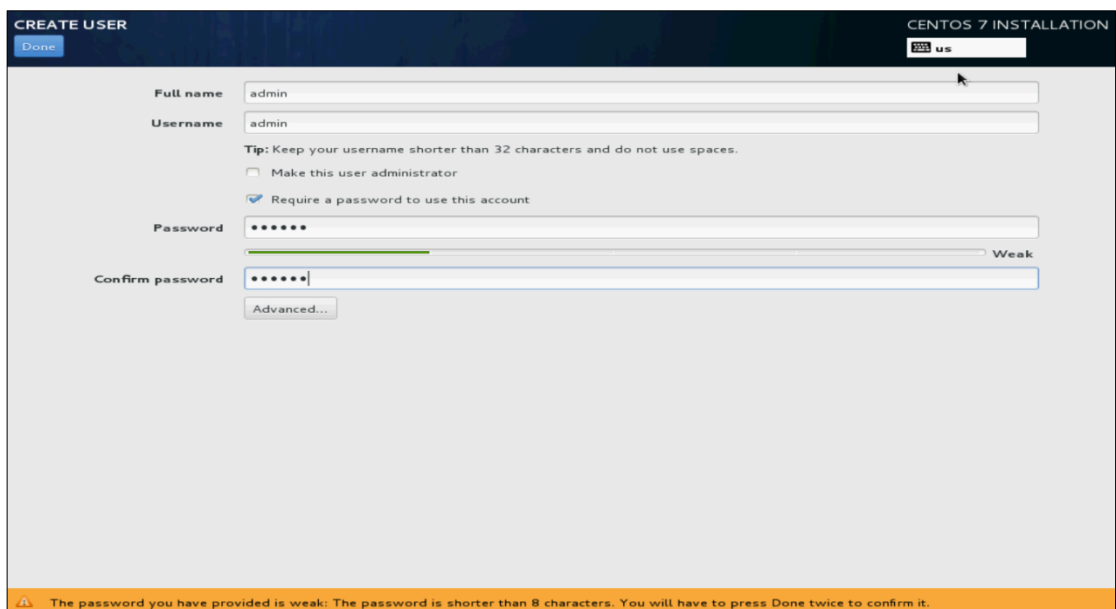


 提示

点击<Done>后，如果系统提示密码设置的太弱，可再次点击<Done>来确认用此弱密码。

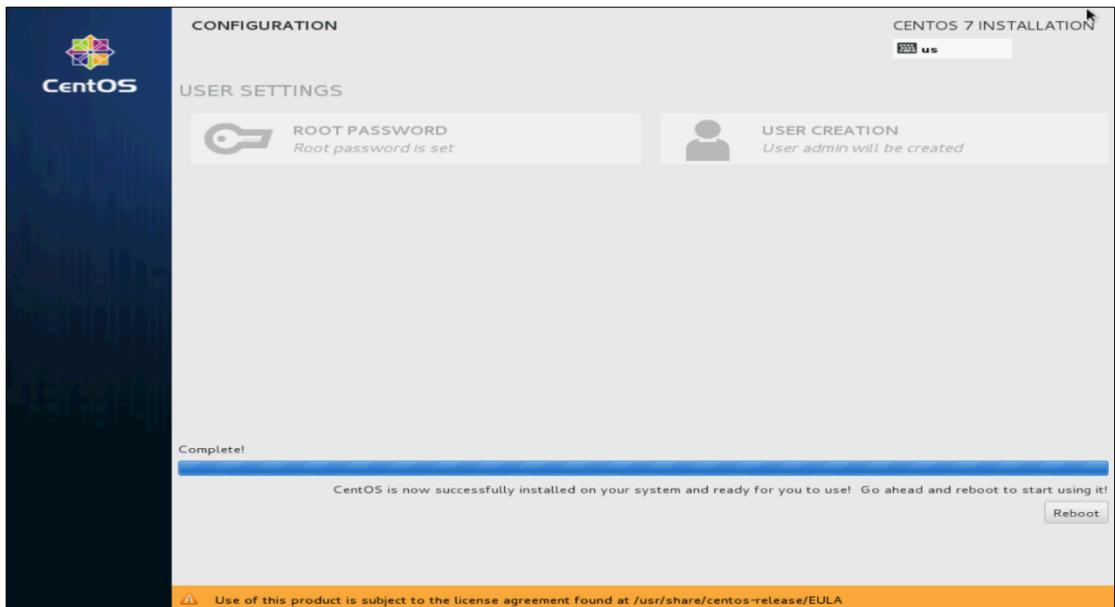
- (13) 完成 root 密码设置后，返回安装过程界面，点击<USER CREATION>，进入创建账户及密码界面，如图 8-10 所示。输入用户名和密码，然后点击<Done>，完成该项设置。在登录 Linux 系统时也可以选择用此处创建的非管理员账户及密码登录。

图8-10 创建账号及密码



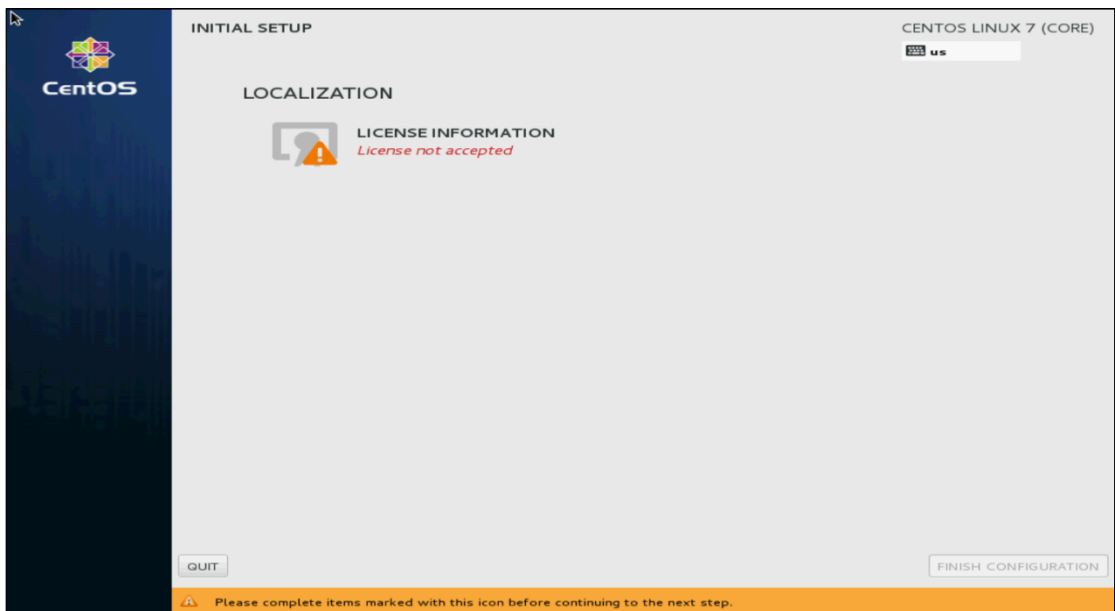
- (14) 创建用户后，进入系统的自动安装步骤。待系统安装完成后，点击<Reboot>进行系统重启，如[图 8-11](#)所示。如果是用光盘安装的，安装完成后，将光盘取出后再重新启动。

图8-11 安装完成



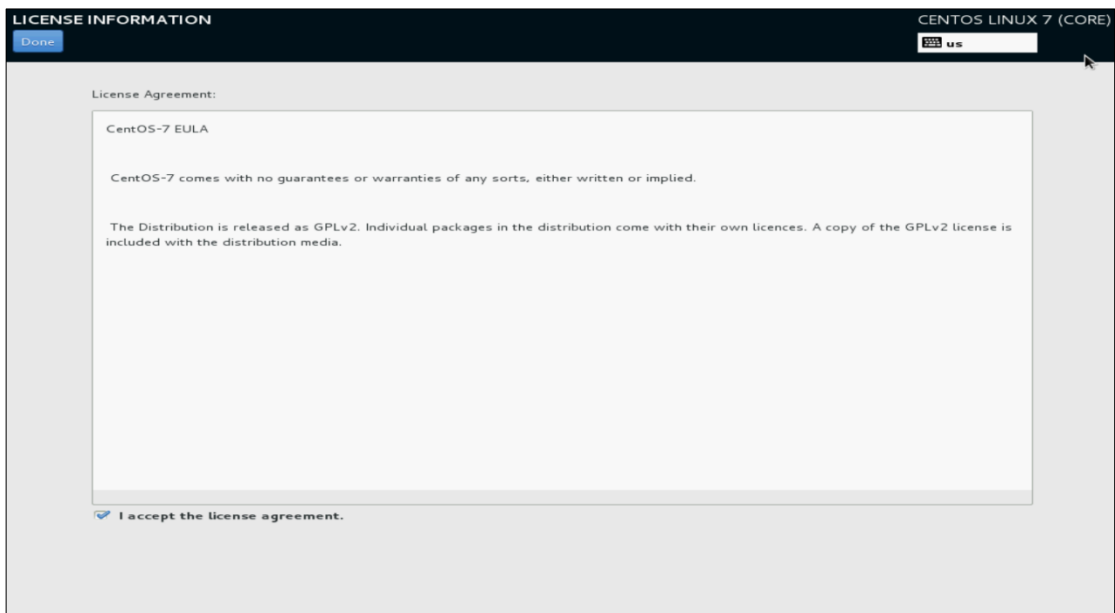
- (15) 重启系统后将自动进入 CentOS 主界面，如[图 8-12](#)所示。为了正常地使用所安装的系统，请点击<LICENSE INFORMATION>，进行一些必要的信息确认。

图8-12 CentOS 主界面



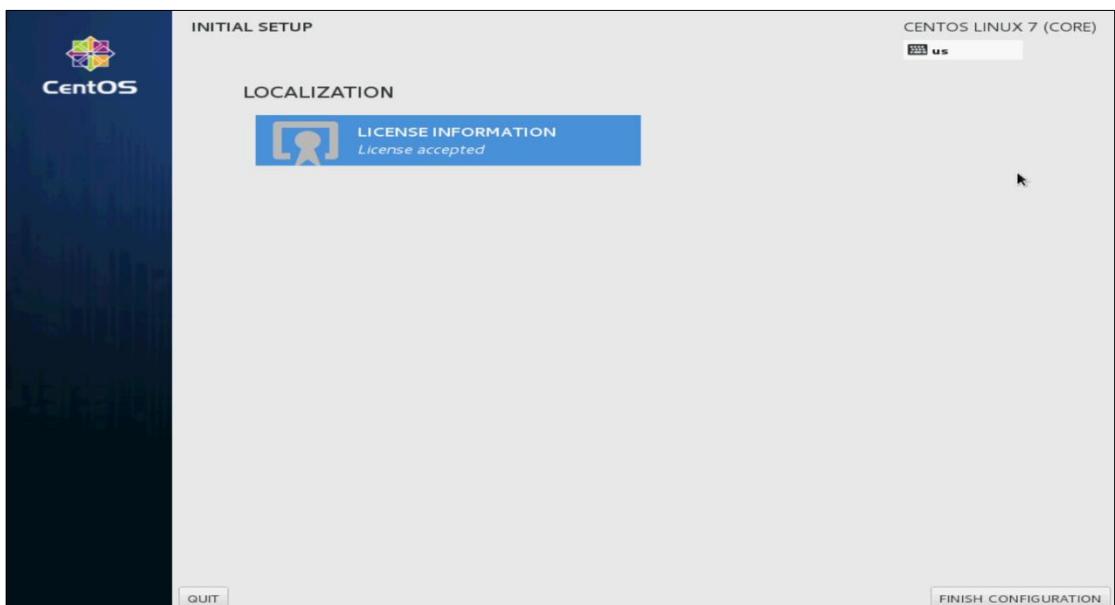
- (16) 勾选“*I accept the license agreement*”，确认系统授权信息，然后点击<Done>，如[图 8-13](#)所示。

图8-13 授权信息



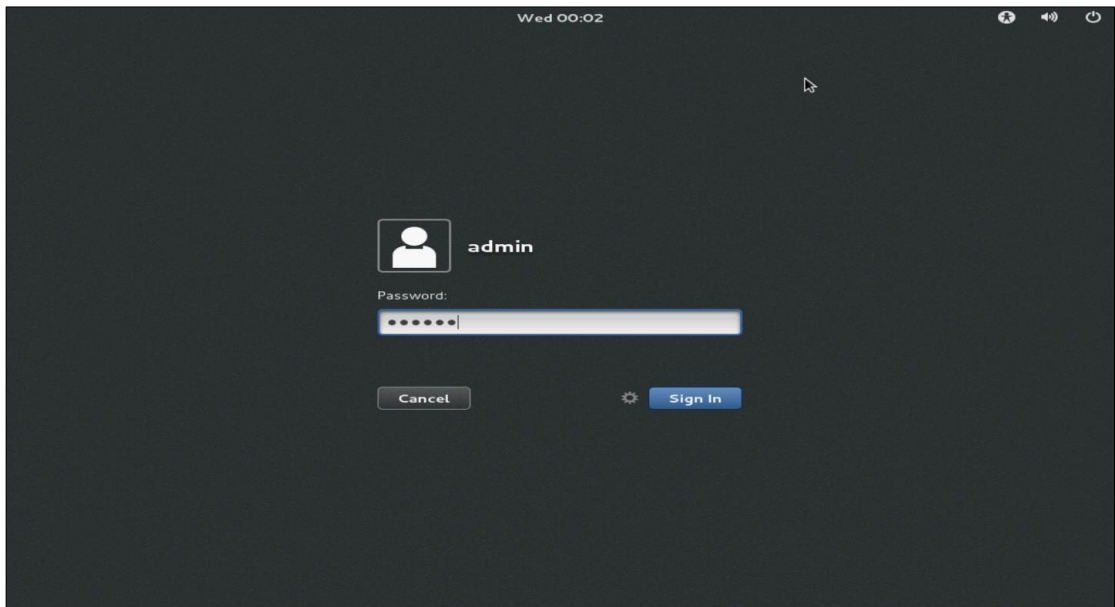
(17) 点击<FINISH CONFIGURATION>按钮，完成配置，如[图 8-14](#)所示。

图8-14 完成配置界面



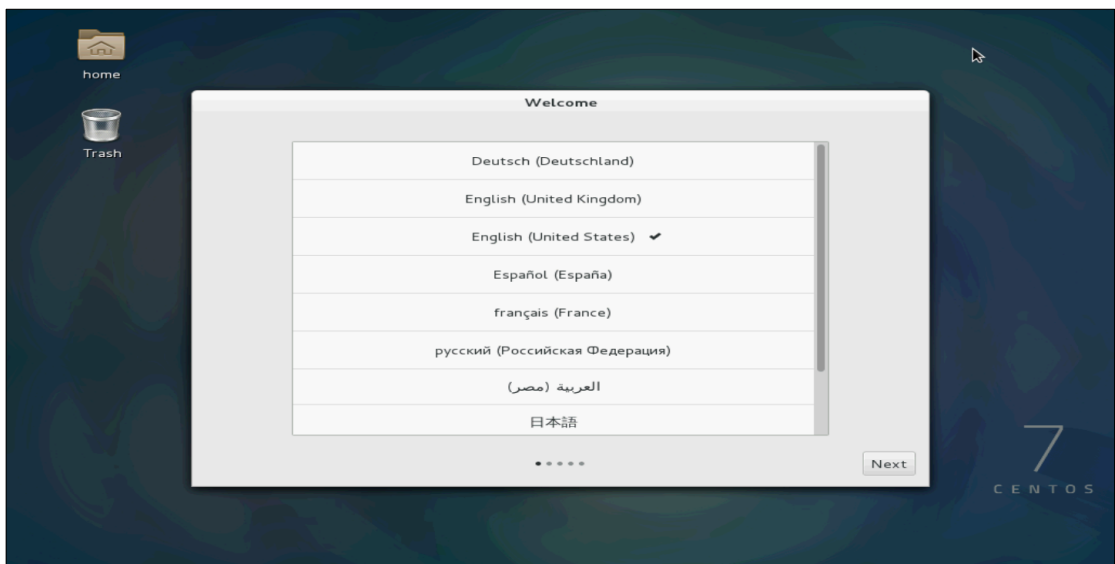
(18) 配置完成后，进入用户登录界面，如[图 8-15](#)所示。输入之前创建的账号和密码，点击<Sign In>，登录 CentOS 系统。

图8-15 登录界面



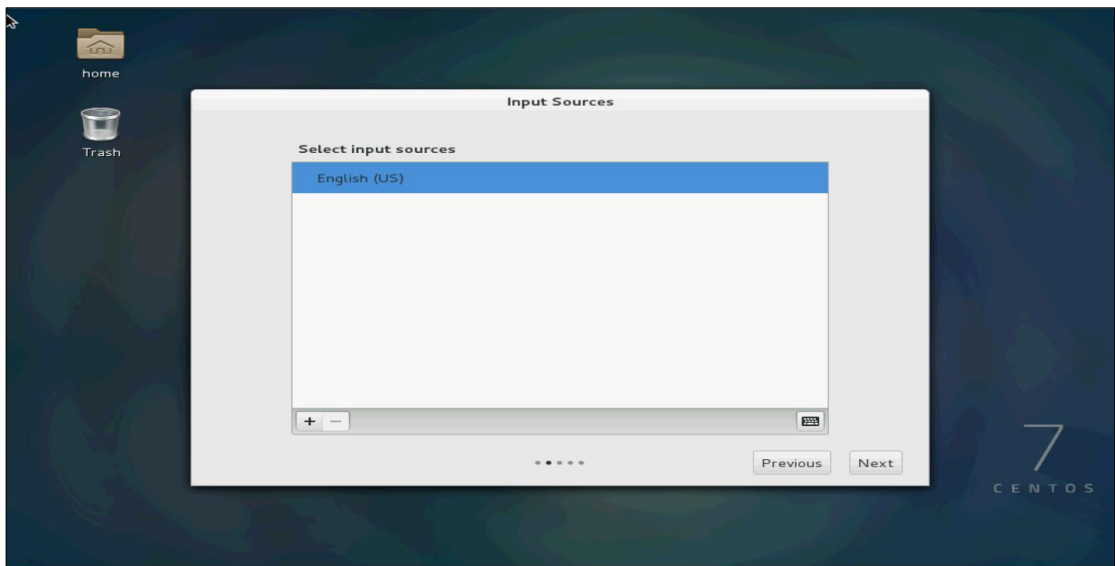
(19) 进入系统后，自动进入欢迎界面，如[图 8-16](#)所示。选择安装语言后点击<Next>。

图8-16 选择安装语言



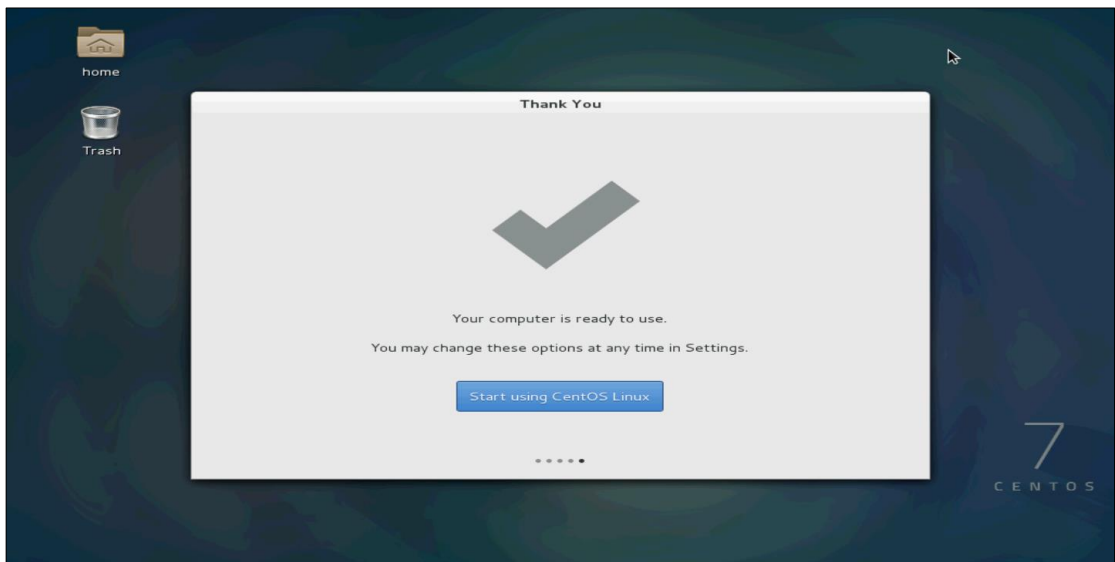
(20) 选择输入语言，如[图 8-17](#)所示，点击<Next>继续。

图8-17 选择输入语言



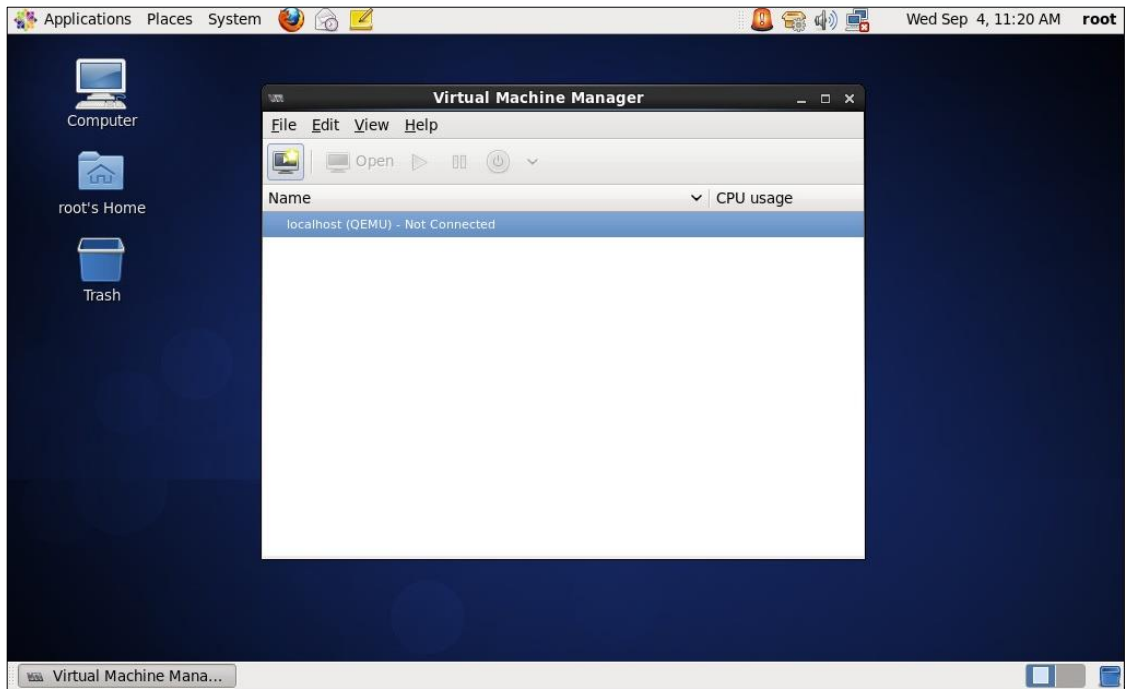
(21) 点击<Start using CentOS Linux>, 开始使用 linux 系统, 如[图 8-18](#)所示。

图8-18 完成欢迎配置界面



(22) 进入系统后, 选择菜单[Applications -> System Tools -> Virtual Machine Manager], 进入 KVM 管理工具界面, 如[图 8-19](#)所示。

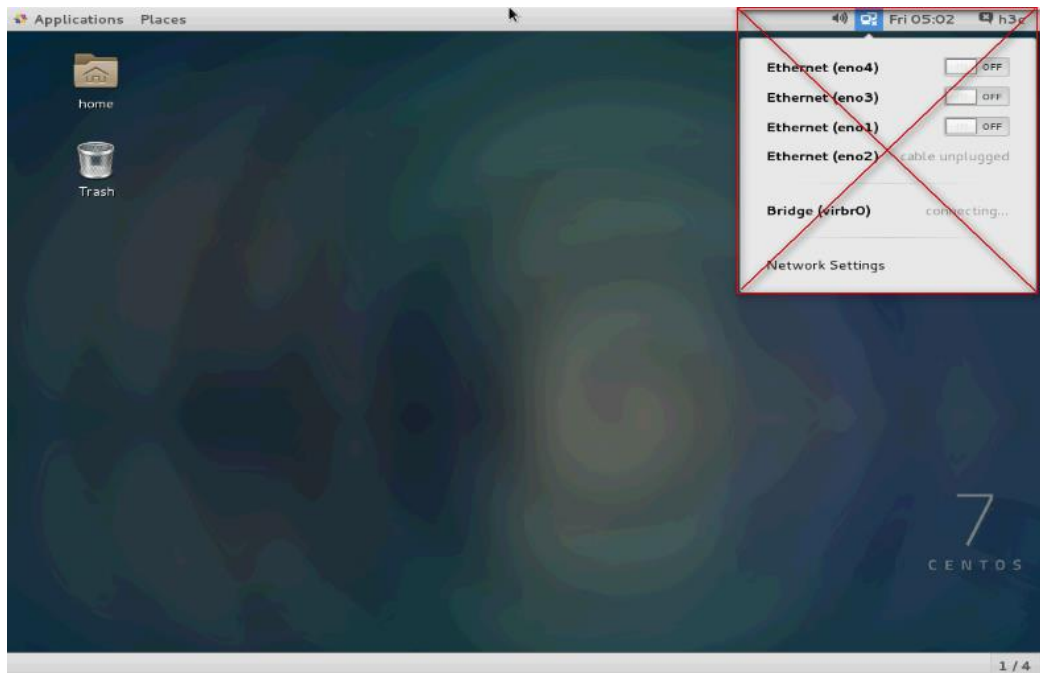
图8-19 Virtual Machine Manager 管理界面



8.2.2 配置网络参数

安装 CentOS 7 后，不能直接通过右上方的设置功能来配置网络参数，如下图所示。因为图形界面配置网络参数是通过 NetworkManager 服务进行管理的，但是后期创建 bridge 的时候需要关闭掉 NetworkManager 服务，这样就会使之前配置的网络参数失效，所以建议手动配置 IP。

图8-20 禁止使用图形界面配置网络参数



手动配置 IP 的方法包括临时配置和永久配置。

1. 临时配置

该方法配置的 IP 地址在系统重启之后会丢失。

#配置网络接口 eno1 的 IP 地址为 192.168.16.33，子网掩码为 16 位：

```
ifconfig eno1 192.168.16.33/16
```

2. 永久配置

在 `/etc/sysconfig/network-scripts/` 目录下，每一个网口对应一个配置文件，例如 eno1 对应 `ifcfg-eno1`，我们可以通过修改配置文件达到永久修改网口相关配置的目的。

(1) 修改配置文件中加黑部分的参数，如果找不到，直接在文件末尾处添加即可：

```
[root@localhost ~]# cd /etc/sysconfig/network-scripts/
[root@localhost network-scripts]# vim ifcfg-eno1
HWADDR=EC:B1:D7:80:50:54
TYPE=Ethernet
BOOTPROTO=static #初始是 dhcp, 修改为 static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno1
UUID=cbb80618-065f-4272-9fde-39ff9b06e474
ONBOOT=yes #初始为 no, 修改为 yes, 表示系统启动时激活此设备
IPADDR=192.168.16.33 #网口的 IP 地址
NETMASK=255.255.0.0 #网口 IP 地址的子网掩码
```

(2) 保存修改后的配置，重启网络服务：

```
[root@localhost network-scripts]# systemctl restart network.service
```

(3) 查看网口信息，已经更新为我们配置的信息：

```
[root@localhost network-scripts]# ifconfig eno1
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.16.33 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 2002:6f01:102:5:eeb1:d7ff:fe80:5054 prefixlen 64 scopeid 0x0<global>
    inet6 fec0::5:eeb1:d7ff:fe80:5054 prefixlen 64 scopeid 0x40<site>
    inet6 2002:8302:101:5:eeb1:d7ff:fe80:5054 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::eeb1:d7ff:fe80:5054 prefixlen 64 scopeid 0x20<link>
    inet6 2002:aca8:284d:5:eeb1:d7ff:fe80:5054 prefixlen 64 scopeid 0x0<global>
    ether ec:b1:d7:80:50:54 txqueuelen 1000 (Ethernet)
    RX packets 291341 bytes 126617361 (120.7 MiB)
    RX errors 0 dropped 178991 overruns 0 frame 0
    TX packets 332 bytes 46253 (45.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 1
```

8.2.3 关闭 SE Linuxfuwu

修改文件/etc/selinux/config，并手动关闭 SELinux 服务。

```
[root@CentOS home]# vim /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted. - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
[root@CentOS home]# /usr/sbin/setenforce 0
```

8.2.4 在 KVM 虚拟化平台配置 Linux bridge

如果服务器没有支持 SR-IOV 的网卡（如 82599 网卡），或者需要将支持 SR-IOV 的网卡和其他网卡配合使用，则需要通过 Linux bridge 技术完成网卡的虚拟化。

(1) 将压缩包 toMarketToolsV1.x.zip 上传到 KVM 虚拟化平台。解压后，根据需要执行操作：

- 过滤支持 SR-IOV 的网卡

在路径 toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v1/ovs 执行 ./bridge-setup.sh -i 命令配置 Linux bridge。

```
[root@localhost ~]# unzip toMarketToolsV1.x.zip
[root@localhost ~]# cd toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v1/bridge
[root@localhost bridge]# chmod 777 ./bridge-setup.sh
[root@localhost bridge]# ./bridge-setup.sh -i
Network default destroyed

Network default unmarked as autostarted

network config eno1 to bridge br0 complete.
network config eno2 to bridge br1 complete.
network config eno3 to bridge br2 complete.
network config eno4 to bridge br3 complete.
```

- 不过滤支持 SR-IOV 的网卡

在路径 toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v2/ovs 执行 ./bridge-setup.sh -i 命令配置 Linux bridge。

```
[root@localhost ~]# unzip toMarketToolsV1.x.zip
[root@localhost ~]# cd toMarketTools/Create_Bridge_shell/Create_Bridge_shell_v2/bridge
[root@localhost bridge]# chmod 777 ./bridge-setup.sh
[root@localhost bridge]# ./bridge-setup.sh -i
Network default destroyed

Network default unmarked as autostarted
```

```
network config eno1 to bridge br0 complete.
network config eno2 to bridge br1 complete.
network config eno3 to bridge br2 complete.
network config eno4 to bridge br3 complete.
```

 说明

配置 Linux bridge 的脚本文件 `toMarketToolsV1.x.zip` 是和 `CSAP-NTA-V200` 的版本一起发布的，可在获取 `CSAP-NTA-V200` 版本时一同获取。

`chmod 777 ./bridge-setup.sh` 命令用于更改命令权限。该命令为可选命令，如果执行 `./bridge-setup.sh -i` 时提示 `permission denied`，需要使用该命令。

`Create_Bridge_shell_v1` 和 `Create_Bridge_shell_v2` 两个版本的差异：

- v1 版本创建桥时会过滤支持 SR-IOV 的网卡，v2 版本不会过滤支持 SR-IOV 网卡。
 - v1 版本创建 ovs 桥时会过滤支持 SR-IOV 的网卡，v2 版本不会过滤支持 SR-IOV 的网卡。
-

(2) 执行完脚本后，通过下面的操作确认是否执行成功：

```
[root@localhost ~]# brctl show
bridge name      bridge id                STP enabled  interfaces
br0               8000.c4346bb8d138       no           eno1
br1               8000.c4346bb8d139       no           eno2
br2               8000.c4346bb8d13a       no           eno3
br3               8000.c4346bb8d13b       no           eno4
br4               8000.6cc217415ee0       no           ens1f0
br5               8000.6cc217415ee4       no           ens1f1
br6               8000.8cdcd4015950       no           ens2f0
br7               8000.8cdcd4015954       no           ens2f1
virbr0            8000.000000000000       yes
```

如果看到除了 `virbr0` 默认网桥外，其余网桥与物理网卡为一一对应的关系，说明创建网桥正常。

(3) 查看生成的 `network-scripts` 配置文件是否正确，以 `eno1`、`br0` 为例

```
[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-br0
DEVICE=br0
TYPE=Bridge
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.1.196
NETMASK=255.255.0.0
[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno1
DEVICE=eno1
HWADDR=c4:34:6b:b8:d1:38
BOOTPROTO=none
ONBOOT=yes
BRIDGE=br0
[root@localhost ~]# ifconfig br0
```

```
br0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2000
    inet 192.168.1.196 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 2002:6100:2f4:b:c634:6bff:feb8:d138 prefixlen 64 scopeid 0x0<global>
    inet6 fec0::5:c634:6bff:feb8:d138 prefixlen 64 scopeid 0x40<site>
    inet6 fec0::b:c634:6bff:feb8:d138 prefixlen 64 scopeid 0x40<site>
    inet6 fe80::c634:6bff:feb8:d138 prefixlen 64 scopeid 0x20<link>
    inet6 2002:aca8:284d:5:c634:6bff:feb8:d138 prefixlen 64 scopeid 0x0<global>
    inet6 2002:6200:101:b:c634:6bff:feb8:d138 prefixlen 64 scopeid 0x0<global>
    ether c4:34:6b:b8:d1:38 txqueuelen 0 (Ethernet)
    RX packets 29465349 bytes 7849790528 (7.3 GiB)
    RX errors 0 dropped 19149249 overruns 0 frame 0
    TX packets 4415 bytes 400662 (391.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
[root@localhost ~]# ifconfig eno1
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::c634:6bff:feb8:d138 prefixlen 64 scopeid 0x20<link>
    ether c4:34:6b:b8:d1:38 txqueuelen 1000 (Ethernet)
    RX packets 31576735 bytes 8896279718 (8.2 GiB)
    RX errors 0 dropped 7960 overruns 0 frame 0
    TX packets 4461 bytes 464952 (454.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16
```

参数说明:

- **DEVICE:** 接口名称, 需与 `ifconfig` 看到的一致。
- **TYPE:** 接口类型, 只有在网桥的配置文件中存在, 取值为 `Bridge`。
- **BOOTPROTO:** `[none|dhcp|static]`, 表示引导时[不使用任何协议]; 使用 `dhcp` 协议获取地址 |; 使用静态配置 `IP`。物理接口配置文件取值为 `none`, 网桥配置文件取值为 `static`。
- **ONBOOT:** `[yes|no]`, 表示引导时[是|否]激活设备。此处值需为 `yes`。
- **IPADDR:** `IP` 地址, 物理接口上的 `IP` 转移到桥上, 配置文件中不存在该选项。网桥配置文件中取值为原物理口配置的 `IP` 值, 与 `ifconfig` 看到的 `inet` 值一致。
- **NETMASK:** `IP` 子网掩码, 同 `IPADDR`。
- **HWADDR:** `MAC` 地址, 只有物理接口的配置文件中存在, 取值与 `ifconfig` 查看到 `ether` 一致。
- **BRIDGE:** 物理接口绑定到的网桥的名字, 只有物理接口配置文件中存在。

 提示

- 由于执行创建 `linux bridge` 脚本的过程中会重启网络服务, 所以请通过服务器自带登录系统登录设备完成操作, 不要通过网络远程登录到服务器进行该操作。
 - 使用 `Linux bridge` 时 `bridge` 上的虚拟接口无法实现 `VLAN` 隔离。如果需要使用 `VLAN` 隔离功能, 可以使用 `OVS bridge` 来代替 `Linux bridge`, 详细情况请参见附录。
-

9 附录 C: 10G 网卡在虚拟平台的加载 (Intel 82599 VF 为例)

9.1 Intel 82599 VF网卡概述

Intel 82599 网卡支持 SR-IOV 技术, 可以在 82599 网卡上通过硬件虚拟化, 虚拟出若干虚拟网卡 (Virtual Function, 简称 VF 网卡)。这些 VF 网卡可以作为 PCI 设备, 添加到虚拟机中。虚拟机使用基于硬件虚拟的 VF 网卡, 比传统的基于软件虚拟的网卡, 性能可以得到大幅提升。



提示

在虚拟 Intel 82599 VF 网卡之前, 请确认你的服务器支持 VT-d 和 SR-IOV 技术。

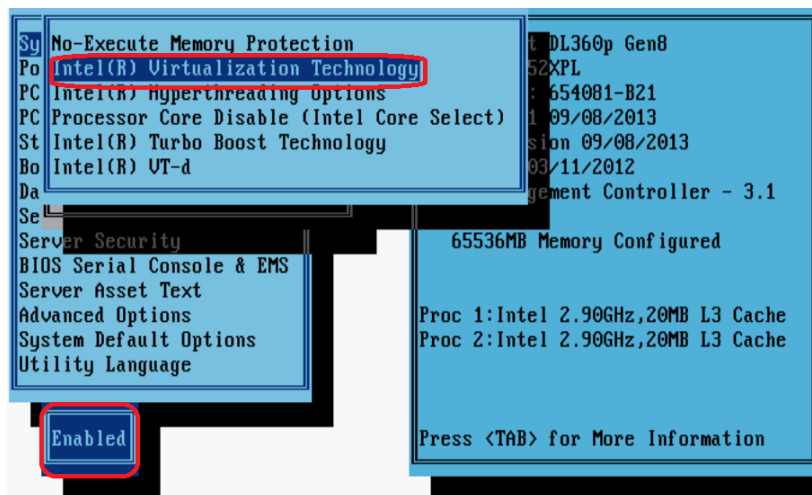
9.2 服务器BIOS设置

本节以硬件平台 HP 360Gen8 为例, 说明服务器 BIOS 中的配置项。

(1) 使能 CPU 的虚拟化技术

进入服务器的 BIOS, 然后选择[System Options -> Processor Options]菜单, 使能虚拟化技术。如下图所示。

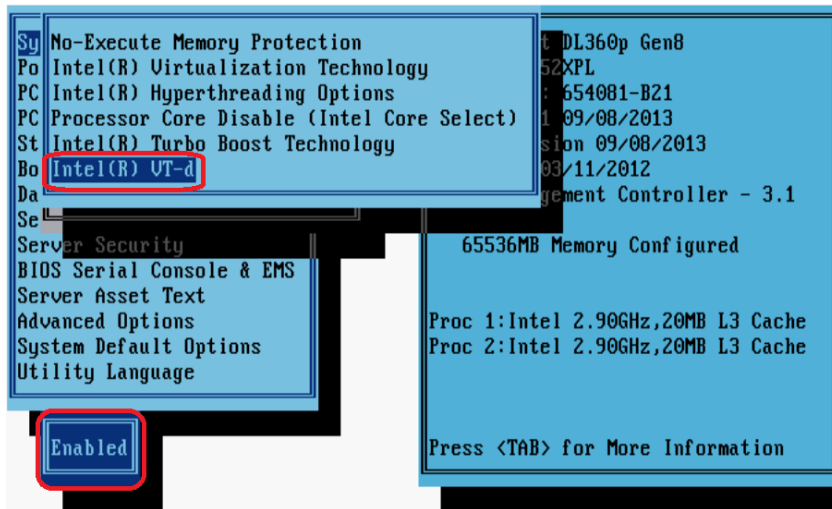
图9-1 使能 CPU 的虚拟化技术



(2) 使能 CPU 的 VT-d 技术

进入服务器的 BIOS 的[System Options -> Processor Options]菜单, 使能 VT-d 技术。如下图所示。

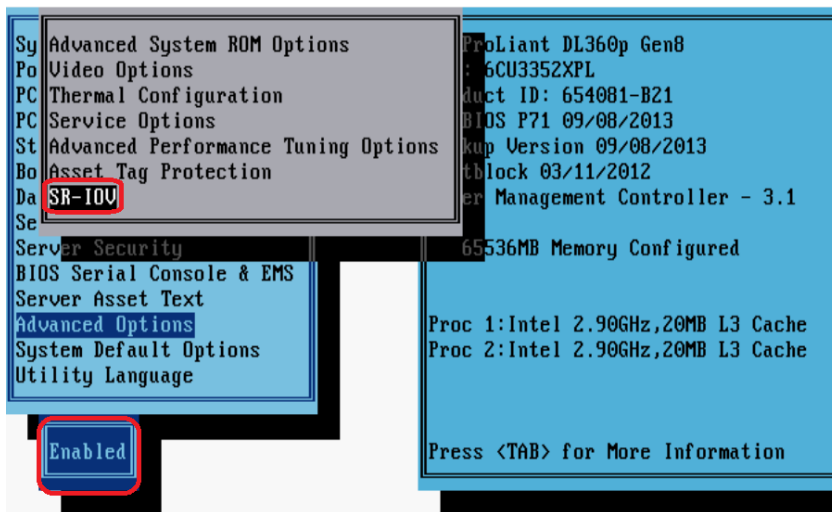
图9-2 使能 CPU 的虚拟化技术



(3) 使能 SR-IOV 技术

进入服务器的 BIOS 的 Advanced Options 菜单，使能 SR-IOV 技术。

图9-3 使能 SR-IOV 技术



9.3 服务器虚拟平台设置

9.3.1 VMWare 平台加载 Intel 82599 VF 网卡

本节以硬件平台 HP 360Gen8，Host 操作系统 VMware ESXI 5.1 版本为例，说明 VMWare 平台下加载 Intel 82599 VF 网卡的步骤。

1. 启动服务器并使能 ESXI Shell

在执行完[服务器 BIOS 设置](#)后，引导启动 VMware ESXI 5.1 系统。启动后，使能 ESXI Shell。关于 ESXI Shell 的配置，请参考 VMware 的相关文档。

2. 通过 EXSI Shell 登录，并查看系统内 Intel 82599 网卡的信息

登录后，使用如下命令查看 82599 网卡信息：

```
~ # lspci | grep -i intel | grep -i 'ethernet\|network'
```

- 当前服务器上有 1 块 Intel 82599 网卡，共 2 个物理端口，显示如下图所示。

图9-4 1 块 Intel 82599 网卡

```
~ # lspci | grep -i intel | grep -i 'ethernet\|network'
00:0e:00.0 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic6]
00:0e:00.1 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic7]
```

- 当前系统也可能有 2 块 Intel 82599 网卡，共 4 个物理端口，显示信息如下图所示。vmnic0 和 vmnic1 显示的编号为 00:03:00.0 和 00:03:00.1，所以这两个物理端口在一块 Intel 82599 网卡上。

图9-5 2 块 Intel 82599 网卡

```
00:03:00.0 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic0]
00:03:00.1 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic1]
00:04:00.0 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic6]
00:04:00.1 Network controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection [vmnic7]
```

3. 设置'max_vfs'参数，创建 VF 网卡

使用命令行创建 VF 网卡：

```
~ # esxcfg-module ixgbe -s max_vfs=X,Y
```

- max_vfs 是加载 ixgbe 模块时的参数，表示在每个物理端口上创建的 VF 的数量。等号后的 2 个值分别在图 9-4 系统内的 2 个物理端口上生效，生效的顺序与使用命令“lspci | grep -i intel | grep -i 'ethernet\|network'”看到的顺序相同。例如 max_vfs=7,8，则对应图 9-4 中 vmnic6 创建 7 个 VF 网卡，vmnic7 上创建 8 个 VF 网卡。
- 当系统内存在多个 Intel 82599 网卡时，例如图 9-5 的 2 块 82599 网卡，则 max_vfs=W,X,Y,Z，分别对应 2 块 Intel 82599 网卡的 4 个物理端口，生效的顺序与使用命令“lspci | grep -i intel | grep -i 'ethernet\|network'”看到的顺序相同。例如 max_vfs=0,10,0,10，则对应图 9-5 中 vmnic0 和 vmnic6 不创建 VF 网卡，vmnic1 和 vmnic7 各创建 10 个 VF 网卡。

4. 检查 82599 网卡的设置，并重启服务器

```
~ # esxcfg-module -g ixgbe
```

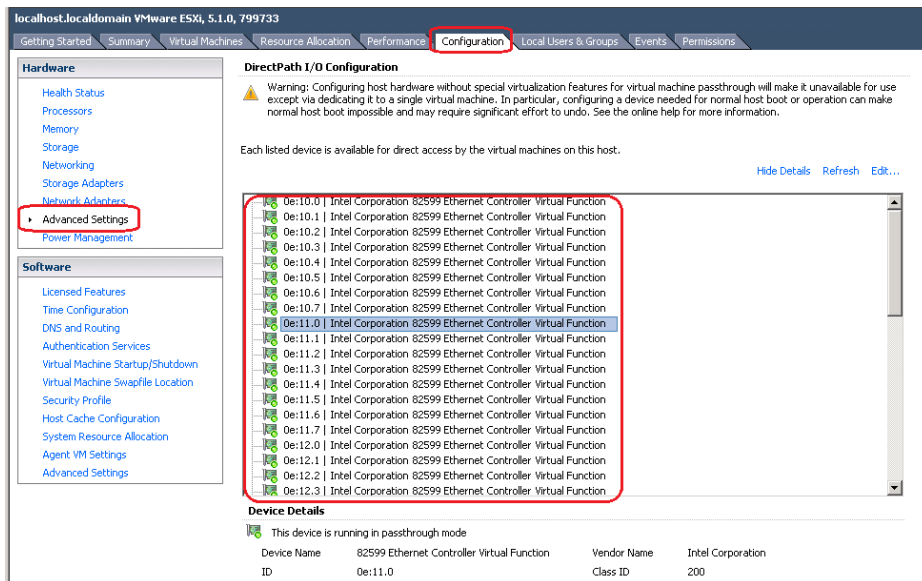
输出 ixgbe enabled = 1 options = 'max_vfs=X,Y'

如果输出的 max_vfs 的值与第(6)步设置的值相同，说明设置成功，重启服务器。

5. 确认 VF 网卡创建成功

使用 VMware vSphere Client 登录服务器，然后进入到[配置 -> 高级设置]中，可以看到 VF 网卡创建成功，如下图所示。

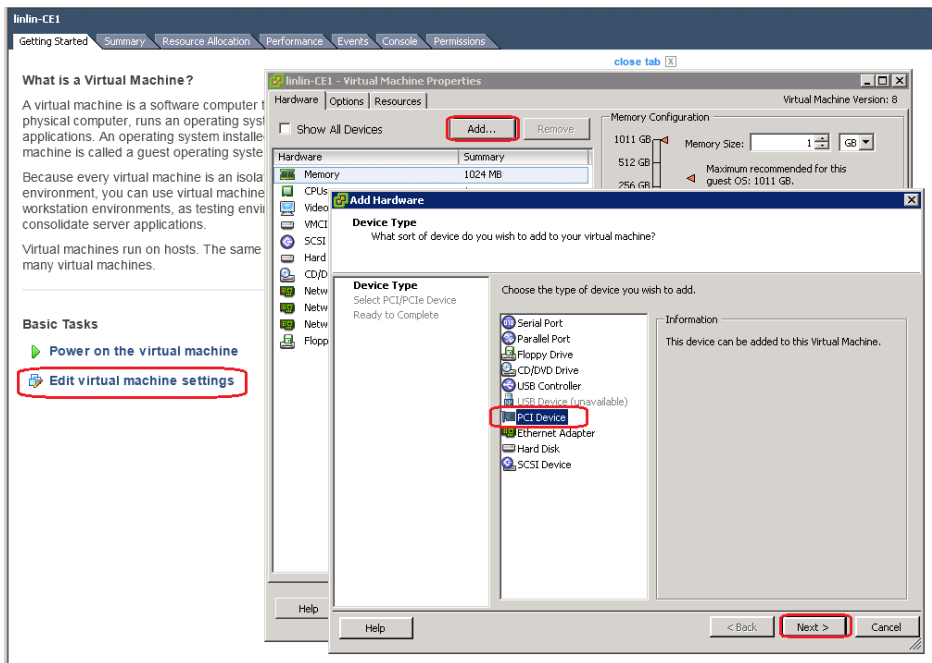
图9-6 VF 网卡创建成功



6. 为 CSAP-NTA-V200 添加 VF 网卡

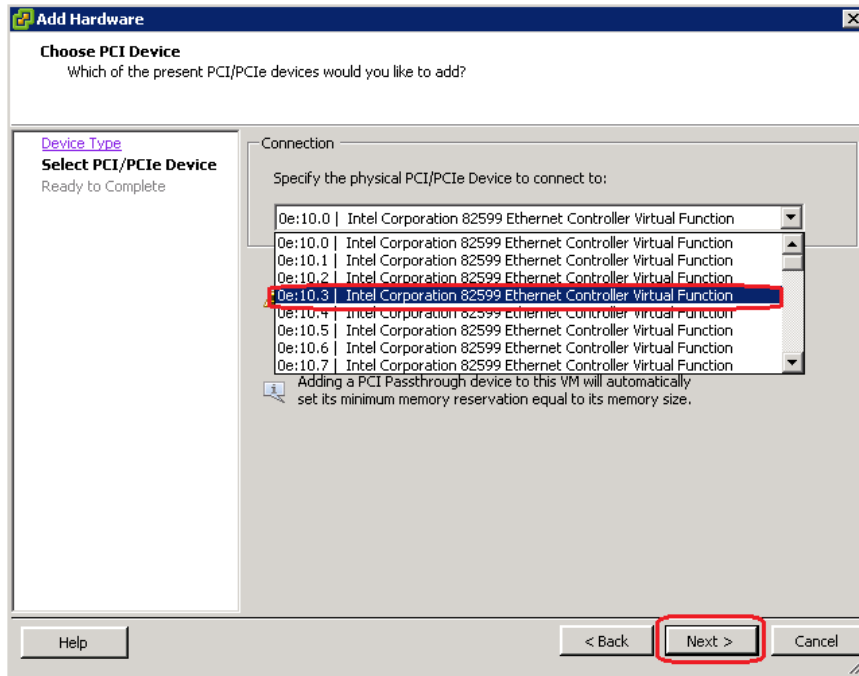
- (1) 在 VMware vSphere Client 登录服务器后，找到要添加 VF 网卡的 CSAP-NTA-V200，然后进入“编辑虚拟机设置”，点击<添加>按钮，在弹出的“添加硬件”窗口中选中 PCI 设备，然后点击<Next>，如下图所示。

图9-7 为虚拟机添加 PCI 设备



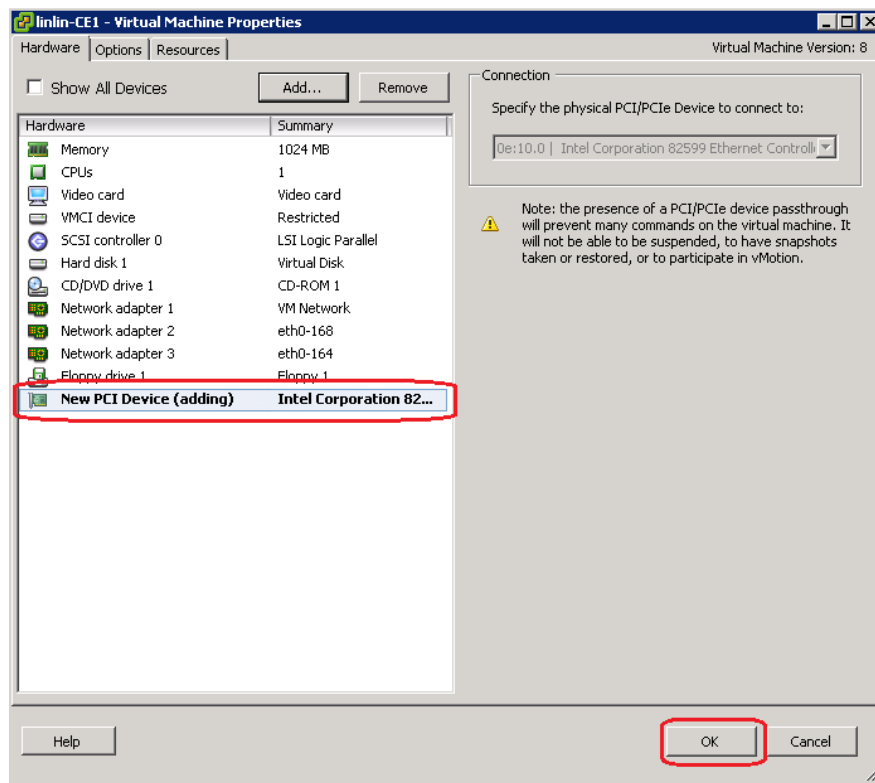
- (2) 选中要添加的 VF 网卡，点击<Next>按钮，如下图所示。再点击<完成>按钮，保存退出，为 CSAP-NTA-V200 添加 VF 网卡成功。

图9-8 添加 VF 网卡



- (3) 添加 VF 网卡成功之后，返回到“虚拟机属性”界面，然后单击“确定”按钮保存虚拟机配置，如下图所示。

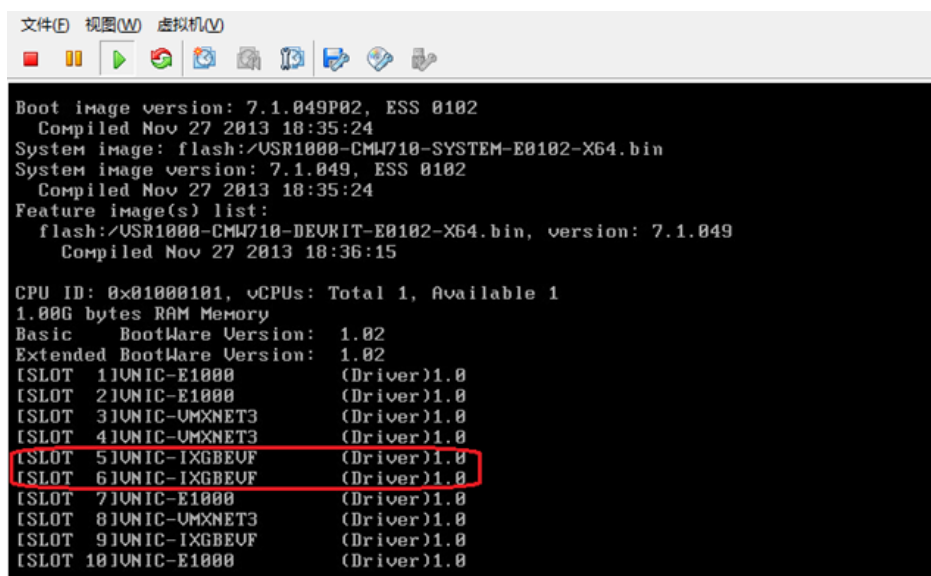
图9-9 保存虚拟机配置



7. 启动 CSAP-NTA-V200，查看 VF 网卡

启动 CSAP-NTA-V200 之后，使用 `display version` 命令查看系统信息，可以看到 VF 网卡已经加载，如下图所示。

图9-10 `display version` 输出



9.3.2 KVM 平台加载 Intel 82599 VF 网卡

1. 执行脚本配置 VF 网卡

当服务器的网卡支持 SR-IOV 技术时,可以通过 SR-IOV 技术完成网卡虚拟化。进行网卡虚拟化时,请将 toMarketToolsV1.x.zip 压缩包上传到 CentOS 7 服务器并解压,解压后进入目录 toMarketTools/Create_VF_shell 下,根据表 9-1 选择脚本合适的参数进行配置。

表9-1 脚本使用介绍

脚本名	使用介绍
-s,--status	显示我们脚本支持的所有SR-IOV网卡的状态,包括pci号、接口名称、使用的驱动类型等信息
-h,--help	显示脚本使用帮助信息
-i,--install	指定创建VF动作,需要与后面的-t、--pci、--ifname参数配合使用
-t,--type	通过使用的驱动类型来指定要创建VF的网卡
--pci	通过pci号来指定要创建VF的网卡
--ifname	通过接口名来指定要创建VF的网卡
-d	指定使用系统原生的PF驱动,默认是安装我们提供的驱动包, toMarketToolsV1.x.zip中的*.rpm
-n,--number	指定每个网卡要创建的VF的数量,不指定默认为8个



说明

网卡虚拟化时用的脚本文件在 toMarketToolsV1.x.zip 内和 CSAP-NTA-V200 的版本一起发布,可在获取 CSAP-NTA-V200 版本时一同获取。

举例如下:

(2) 上传并解压工作包

```
[root@CentOS-254 ~]# unzip toMarketToolsV1.x.zip
[root@CentOS-254 ~]# cd toMarketTools/Create_VF_shell
```

(3) 显示脚本支持的网卡信息

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -s
Network devices supported by this script
=====
0000:08:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:08:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
```

```

0000:05:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:04:00.0 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno49 mtu=1500
numvfs=0 totalvfs=63 driver=ixgbe
0000:04:00.1 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno50 mtu=1500
numvfs=0 totalvfs=63 driver=ixgbe

```

(4) 进行配置

可以通过-t 参数, 或者--pci 参数, 或者--ifname 参数来指定要创建 VF 的网卡。如配置每个 82599 网卡创建 32 个 VF, 下面的三种方式可以达到同样的效果:

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -i -t ixgbe -n 32
```

或者

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -i --pci 0000:04:00.0 --pci
0000:04:00.1 -n 32
```

或者

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -i --ifname eno49 --ifname eno50 -n 32
```

(5) 再次显示当前网卡信息

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -s
```

Network devices supported by this script

=====

```

0000:08:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:08:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:04:00.0 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno49 mtu=1500
numvfs=32 totalvfs=63 driver=ixgbe
0000:04:00.1 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno50 mtu=1500
numvfs=32 totalvfs=63 driver=ixgbe

```

可以看到 ixgbe 网卡当前的 VF 个数为 32。

(6) 通过下面的命令进一步确认是否执行成功

```
[root@localhost h3c]# lspci | grep 82599
```

```
03:00.0 Ethernet controller: Intel Corporation 82599 10 Gigabit Dual Port Network
Connection (rev 01)
```

```
03:00.1 Ethernet controller: Intel Corporation 82599 10 Gigabit Dual Port Network
Connection (rev 01)
```

```
03:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual
Function (rev 01)
```

```
03:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual
Function (rev 01)
```

.....

```
03:1f.4 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual
Function (rev 01)
```

```
03:1f.5 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual
Function (rev 01)
```

如果查看到只有物理网卡 PCI 信息而没有 VF 信息则说明配置失败。

```
[root@localhost h3c]# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
4: eno1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 3000 qdisc mq state UP mode
DEFAULT qlen 1000
    link/ether 38:ea:a7:8b:89:00 brd ff:ff:ff:ff:ff:ff
    vf 0 MAC 74:25:8a:e4:1b:c9, spoof checking on, link-state auto
    vf 1 MAC 74:25:8a:e4:1b:ca, spoof checking on, link-state auto
.....
5: eno2: <NO-CARRIER,BROADCAST,MULTICAST,PROMISC,UP> mtu 1500 qdisc mq state DOWN mode
DEFAULT qlen 1000
    link/ether 38:ea:a7:8b:89:01 brd ff:ff:ff:ff:ff:ff
    vf 0 MAC 74:25:8a:e4:21:db, spoof checking on, link-state auto
    vf 1 MAC 74:25:8a:e4:21:dc, spoof checking on, link-state auto
.....
```

请关注 VF 口的 MAC 信息是否正确。



注意

使用 SR-IOV 技术对网卡进行虚拟化后，除 Intel 82599 网卡之外的其他网卡将无法使用。因此如需同时使用 Intel 82599 网卡和其他网卡，请通过 Linux bridge 或 OVS bridge 技术完成网卡的虚拟化，避免出现问題。

2. 配置 Intel 82599 网卡的 MTU

在实际 Apply 的组网中可能会遇到需要给指定的物理网口配置 MTU 的需求，比如：组网中使用到 VXLAN 技术，由于是把原始二层数据帧封装在 UDP 里，所以会多出外层的 8 字节 VXLAN 头+8 字节 UDP 头+20 字节 IP 头，原来默认的 1500 的 MTU 不再满足需求。

(1) 查看当前网卡 mtu

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -s
Network devices supported by this script
=====
0000:08:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:08:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:04:00.0 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno49 mtu=1500
numvfs=0 totalvfs=63 driver=ixgbe
0000:04:00.1 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno50 mtu=1500
numvfs=0 totalvfs=63 driver=ixgbe
```

(2) 配置 mtu

在路径 toMarketTools/Create_VF_shell 下执行 `. /setMtu.sh phyNic mtuSize` 命令配置物理网卡的 MTU 值。

```
[root@CentOS-254 Create_VF_shell]# ./setMtu.sh eno49 1600
eno49 mtu set to 1600 complete.
```

(3) 再次查看网卡 mtu

```
[root@CentOS-254 Create_VF_shell]# ./createVf.sh -s
Network devices supported by this script
=====
0000:08:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:08:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens1f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.1 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f1 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:05:00.0 'Ethernet Controller XXV710 for 25GbE SFP28 [158b]' if=ens2f0 mtu=1500
numvfs=0 totalvfs=64 driver=i40e
0000:04:00.0 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno49 mtu=1600
numvfs=0 totalvfs=63 driver=ixgbe
0000:04:00.1 '82599 10 Gigabit Dual Port Network Connection [10fb]' if=eno50 mtu=1500
numvfs=0 totalvfs=63 driver=ixgbe
```

(4) 通过下面命令进一步确认是否配置成功:

```
[root@CentOS-254 Create_VF_shell]# ifconfig eno49 | grep mtu
Eno49: flags=4355<UP,BROADCAST,PROMISC,MULTICAST> mtu 1600
[root@CentOS-254 sr-ioV-82599]# cat /etc/sysconfig/network-scripts/ifcfg-eno49 | grep -i
mtu
MTU=1600
```

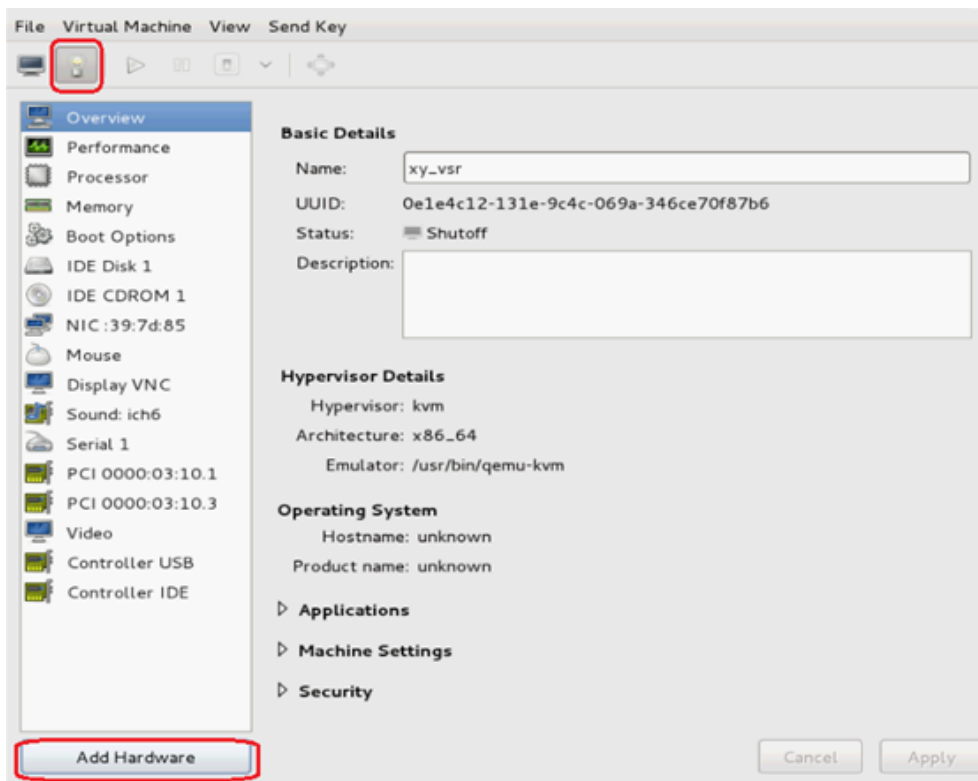


请勿使用 `setMtu.sh` 为 `./createVF.sh -s` 显示之外的网卡设置 MTU，可能存在问题。

3. 为 CSAP-NTA-V200 添加 VF 网卡

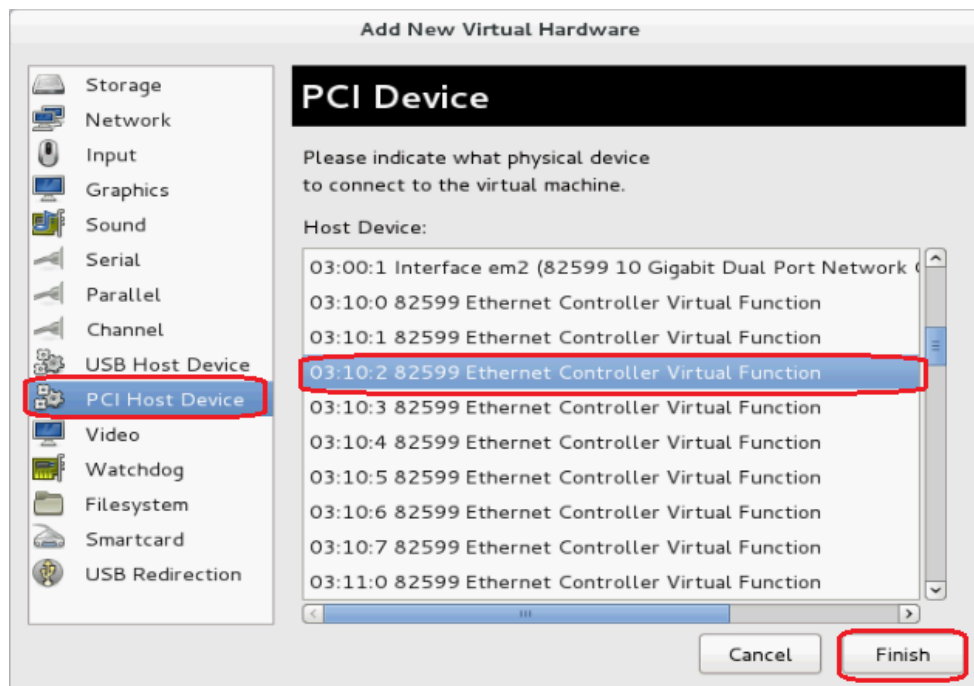
- (1) 在 CentOS 7 上使用“Virtual Machine Manager”，找到要添加 VF 网卡的 CSAP-NTA-V200，然后进入“Show virtual hardware details”界面，点击“Add Hardware”按钮，如下图所示。

图9-11 为虚拟机添加硬件



(2) 在弹出的新对话框中，选中 PCI 设备，并在右侧的对话框中选中 VF 网卡，然后点击“Finish”按钮完成添加 VF 网卡，如下图所示。

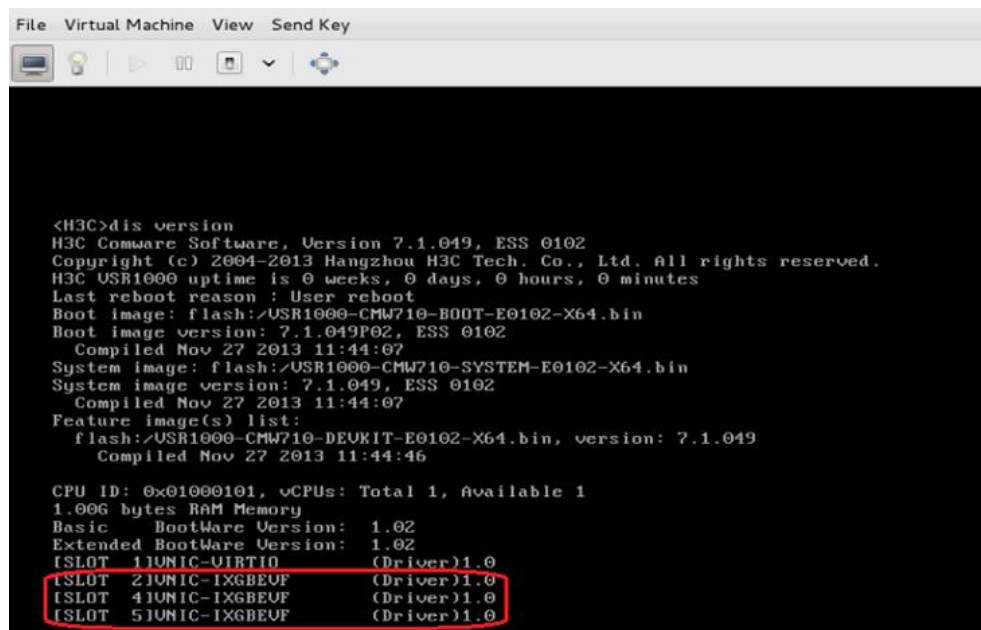
图9-12 添加 VF 网卡



4. 启动 CSAP-NTA-V200, 查看 VF 网卡

启动 CSAP-NTA-V200 之后, 使用 `display version` 命令查看系统信息, 可以看到 VF 网卡已经加载, 如下图所示。

图9-13 `display version` 命令输出



9.3.3 CAS 平台加载 Intel 82599 VF 网卡

1. 启用主机的 Intel 82599 网卡设置

(1) 在主机的高级设置选项中, 将 IOMMU 当前状态修改为启用状态, 并点击<修改>确定设置, 如下图所示。

图9-14 启用 IOMMU 配置

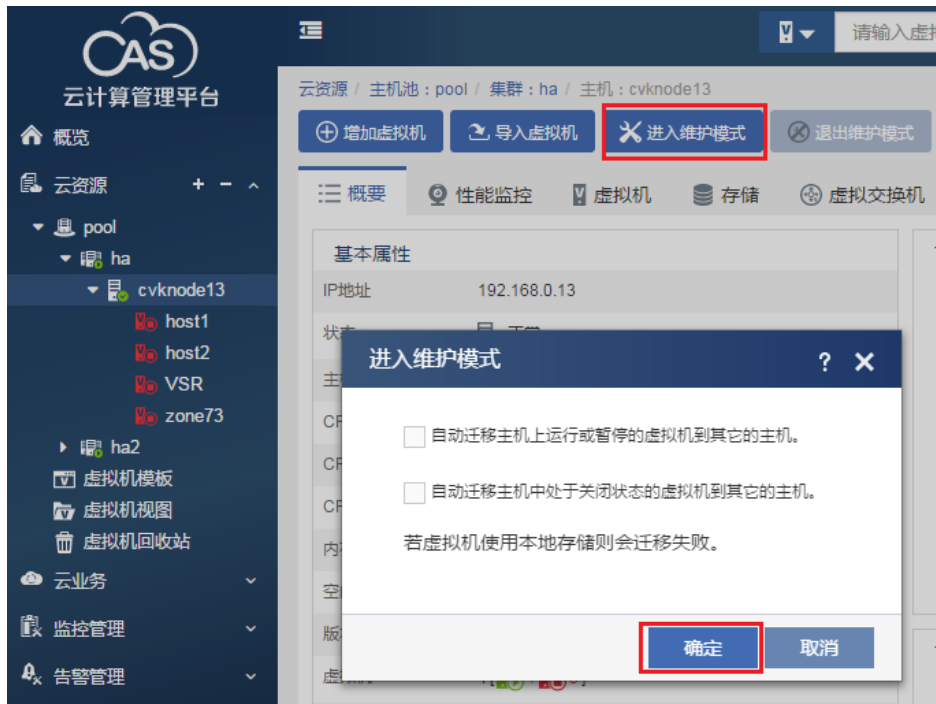


(2) 点击<进入维护模式>按钮, 使主机进入维护模式, 如下图。

说明

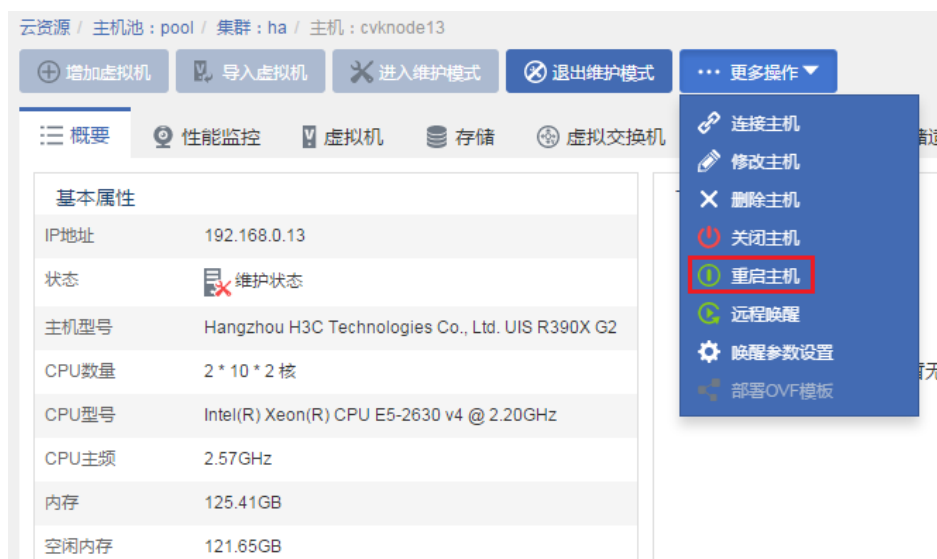
- 修改主机 IOMMU 配置状态后需要重启主机才能生效。只有在维护模式下才能执行重启主机的操作。
- 如果主机中有处于开启或暂停的状态下的虚拟机，需要先关闭虚拟机或勾选“自动迁移处于运行或暂停状态的虚拟机”选项才能进入维护模式。

图9-15 主机进入维护模式



(3) 点击<更多操作>中的“重启主机”选项，将主机重启，如下图。

图9-16 重启主机



(4) 重启后再次进入到高级设置页查看，此时 IOMMU 配置经变成启用状态，如下图。

图9-17 主机进入 IOMMU 启用状态



2. 启用网卡 SR-IOV 并创建 VF 网卡

(1) 选择主机的“物理网卡”选项，选中要进行 SR-IOV 配置的网卡，在下方的 SR-IOV 页签中，启用 SR-IOV，并输入虚拟网卡个数。如下图中将物理网卡虚拟为两个 VF 网卡。配置好后点击<保存>按钮。

⚠ 注意

- 请选择活动状态的非管理网卡能进行 SR-IOV 配置。
- 管理网卡已经被虚拟交换机使用，则无法进行 SR-IOV 配置。
- 非活动状态的物理网卡无法进行 SR-IOV 配置。

图9-18 创建 VF 网卡



(2) 点击<确定>，确认网卡的 SR-IOV 设置。

图9-19 确认网 SR-IOV 设置



3. 为 CSAP-NTA-V200 添加 VF 网卡

(1) 选择要添加 VF 网卡的 CSAP-NTA-V200，点击<修改虚拟机>按钮，如下图。

图9-20 修改虚拟机



(2) 点击<增加硬件>按钮，选择增加网络，点击<下一步>添加网络，如下图。

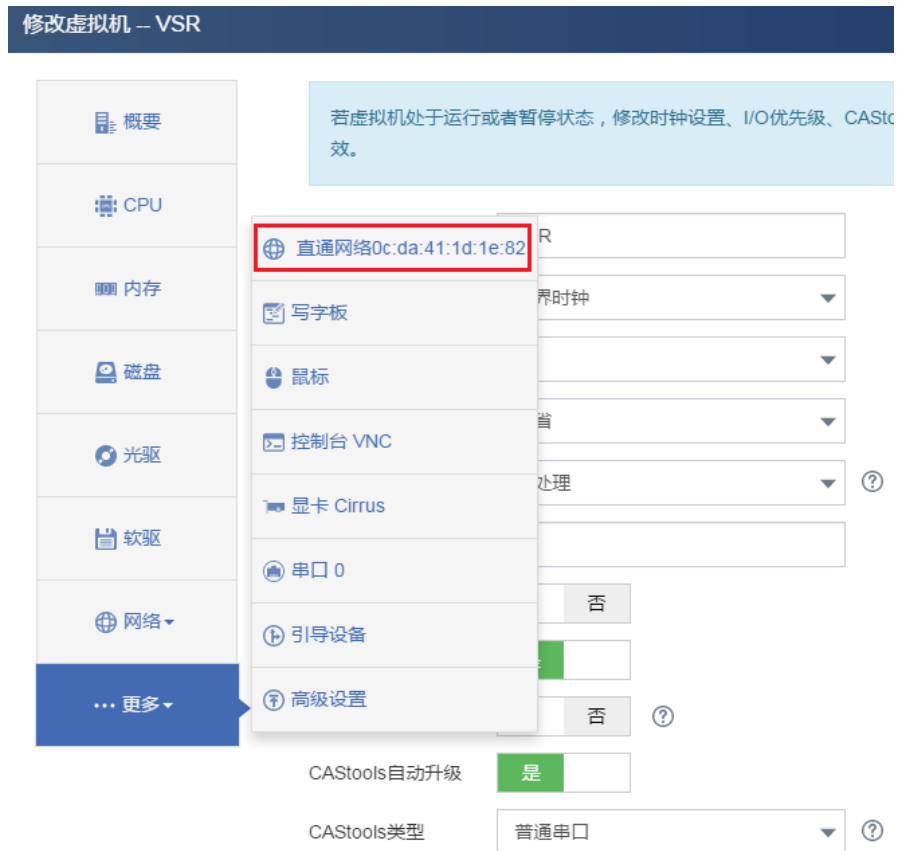
图9-21 添加网络

(3) 设备型号选择 SR-IOV 直通网卡，驱动类型选择 VFIO，物理网卡选择配置 VF 网卡时进行 SRV-IOV 配置的网卡，点击<完成>，如下图。

图9-22 添加 VF 网卡

5、配置成功后，在虚拟机的“更多”选项中会出现添加的直通网络，如下图。

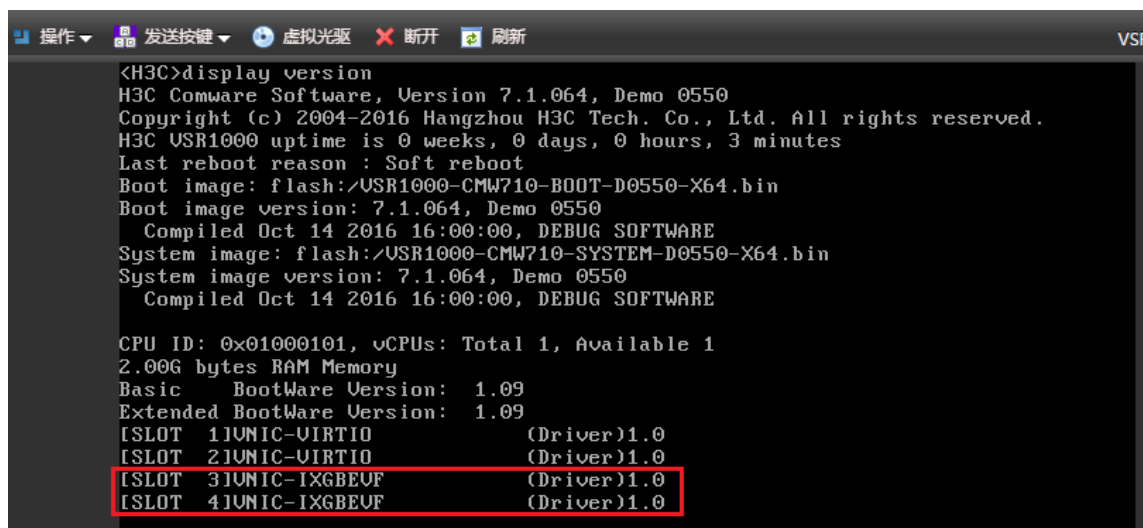
图9-23 查看直通网络



4. 启动 CSAP-NTA-V200，查看 VF 网卡

启动 CSAP-NTA-V200 之后，使用 `display version` 命令查看系统信息，可以看到 VF 网卡已经加载，如下图所示。

图9-24 display version 命令输出



```
<H3C>display version
H3C Comware Software, Version 7.1.064, Demo 0550
Copyright (c) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C USR1000 uptime is 0 weeks, 0 days, 0 hours, 3 minutes
Last reboot reason : Soft reboot
Boot image: flash:/USR1000-CMW710-BOOT-D0550-X64.bin
Boot image version: 7.1.064, Demo 0550
  Compiled Oct 14 2016 16:00:00, DEBUG SOFTWARE
System image: flash:/USR1000-CMW710-SYSTEM-D0550-X64.bin
System image version: 7.1.064, Demo 0550
  Compiled Oct 14 2016 16:00:00, DEBUG SOFTWARE

CPU ID: 0x01000101, vCPUs: Total 1, Available 1
2.00G bytes RAM Memory
Basic   BootWare Version: 1.09
Extended BootWare Version: 1.09
[SL0T 1]UNIC-VIRTIO           (Driver)1.0
[SL0T 2]UNIC-VIRTIO           (Driver)1.0
[SL0T 3]UNIC-IXGBEVF          (Driver)1.0
[SL0T 4]UNIC-IXGBEVF          (Driver)1.0
```

10 附录 D: PXE Server 搭建

10.1 CentOS系统下环境搭建

本节以 CentOS Linux release 7.1.1503 (Core)的 minimal 版本为例进行说明,其他 CentOS 版本可能会有些微差别。

本文统一使用 yum 工具进行安装,如果环境中可以正常连接外网,则直接使用下文中提到的 yum 命令安装即可;如果无法连接外网,则可以使用系统对应的 ISO 作为本地镜像源进行安装。

配置本地镜像源的方法如下:

- (1) 上传镜像文件到系统(或者通过 CDROM 挂载进设备)。
- (2) mount ISO 文件到本地:

```
[root@localhost ~]# mount /dev/sr0 /media/
```

```
mount: /dev/sr0 is write-protected, mounting read-only
```

这里使用 CDROM 的方式挂载的镜像文件,所以会多出一个/dev/sr0 设备。

- (3) 修改/etc/yum.repos.d/下的配置文件。

备份默认的 repo 文件。

```
[root@localhost yum.repos.d]# mkdir bak
```

```
[root@localhost yum.repos.d]# mv *.repo bak
```

新增 myself.repo 文件。

```
[root@localhost yum.repos.d]# vi myself.repo
```

修改文件内容如下:

```
[base]
```

```
name=CentOS-$releasever - Base
```

```
baseurl=file:///media/
enabled=1
gpgcheck=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
# 清空 cache。
[root@localhost yum.repos.d]# yum clean all
[root@localhost yum.repos.d]# yum makecache
```

10.1.2 安装并配置 DHCP

配置过程中可能会由于书写错误等遇到一些问题，需根据具体问题定位。

(1) 安装 DHCP。

```
[root@localhost ~]# yum -y install dhcp
```

(2) 修改配置文件。

vim /etc/dhcp/dhcpd.conf, 其中 next-server 信息为 tftp 服务器地址（一般 tftp 也搭建在同一 host 上，如果 tftp 也在同一 host 上则为本 host 接口 ip）。

```
[root@localhost ~]# vi /etc/dhcp/dhcpd.conf
```

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
subnet 192.168.1.0 netmask 255.255.255.0{
    range 192.168.1.100 192.168.1.200;
    default-lease-time 600;
    max-lease-time 7200;
    next-server 192.168.1.87;
    filename "pxelinux.0";
}
```

(3) 启动/重启 DHCP 服务。

```
[root@localhost ~]# systemctl restart dhcpd
```

查看 dhcp 服务状态。

```
[root@localhost ~]# systemctl status dhcpd
```

```
dhcpd.service - DHCPv4 Server Daemon
```

```
Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; disabled)
```

```
Active: active (running) since Fri 2019-08-16 04:31:33 EDT; 40s ago
```

注意，DHCP 配置的网段要和接口地址在同一网段，否则 DHCP 无法分配地址

10.1.3 安装并配置 TFTP

配置过程中可能会由于书写错误等遇到一些问题，需根据具体问题定位。

(1) 安装 TFTP。

```
[root@localhost ~]# yum -y install tftp-server
```

(2) 修改配置文件。

```
[root@localhost ~]# vi /etc/xinetd.d/tftp
```

```
# default: off
```

```
# description: The tftp server serves files using the trivial file transfer \
```

```
# protocol. The tftp protocol is often used to boot diskless \
```

```
# workstations, download configuration files to network-aware printers, \
```

```
# and to start the installation process for some operating systems.
```

```
service tftp
```

```
{
```

```
    socket_type          = dgram
```

```
    protocol             = udp
```

```
    wait                 = yes
```

```
    user                 = root
```

```
    server               = /usr/sbin/in.tftpd
```

```
    server_args          = -s /var/lib/tftpboot -C #修改
```

```
    disable              = no                #修改
```

```
    per_source           = 11
```

```
    cps                  = 100 2
```

```
    flags                = IPv4
```

```
}
```

(3) 启动/重启 TFTP 服务。

```
[root@localhost ~]# systemctl restart xinetd
```

查看状态。

```
[root@localhost ~]# systemctl status xinetd
```

```
xinetd.service - Xinetd A Powerful Replacement For Inetd
```

```
Loaded: loaded (/usr/lib/systemd/system/xinetd.service; enabled)
```

```
Active: active (running) since Fri 2019-08-16 04:40:22 EDT; 8s ago
```

10.1.4 安装并配置 http

配置过程中可能会由于书写错误等遇到一些问题，需根据具体问题定位。

(1) 安装 HTTP。

```
[root@localhost ~]# yum -y install httpd
```

(2) 配置文件。

http 配置文件位置为/etc/httpd/conf/httpd.conf，其中 DocumentRoot 定义的路径为 http 访问的根路径，缺省为/var/www/html。

```
[root@localhost ~]# cat /etc/httpd/conf/httpd.conf | grep DocumentRoot
```

```
# DocumentRoot: The directory out of which you will serve your
DocumentRoot "/var/www/html"
```

(3) 启动/重启 HTTP 服务。

```
[root@localhost ~]# systemctl restart httpd
```

查看状态。

```
[root@localhost ~]# systemctl status httpd
```

```
httpd.service - The Apache HTTP Server
```

```
Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
```

```
Active: active (running) since Fri 2019-08-16 04:49:51 EDT; 37s ago
```

10.1.5 安装并配置 NFS

(1) 安装 nfs。

```
[root@localhost ~]# yum -y install nfs-utils rpcbind
```

(2) 启动 rpcbind、nfs 服务

```
[root@localhost ~]# systemctl start rpcbind
```

```
[root@localhost ~]# systemctl start nfs
```

查看状态。

```
[root@localhost ~]# systemctl status rpcbind
```

```
rpcbind.service - RPC bind service
```

```
Loaded: loaded (/usr/lib/systemd/system/rpcbind.service; static)
```

```
Active: active (running) since Fri 2019-08-16 05:08:31 EDT; 35s ago
```

```
[root@localhost ~]# systemctl status nfs
```

```
nfs-server.service - NFS server and services
```

```
Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled)
```

```
Active: active (exited) since Fri 2019-08-16 05:08:38 EDT; 33s ago
```

10.1.6 关闭防火墙

```
[root@localhost ~]# systemctl stop firewalld
```

查看状态。

```
[root@localhost ~]# systemctl status firewalld
```

```
firewalld.service - firewalld - dynamic firewall daemon
```

```
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
```

```
Active: inactive (dead) since Fri 2019-08-16 05:11:13 EDT; 23s ago
```

不关闭防火墙可能会导致 client 无法访问 TFTP 服务，如果环境对安全有要求，可以通过配置 iptable 策略解决（具体方法这里不给出，请自行网上查找）。

```
[root@localhost ~]# setenforce 0    #关闭 SELinux
```

10.1.7 安装并配置 syslinux

(1) 安装 syslinux。

```
[root@localhost ~]# yum -y install syslinux
```

(2) 拷贝引导文件及版本文件。

找到 host 上 syslinux 的 pxelinux0 文件，拷贝到 tftp server 的工作路径下（tftp 配置文件中 server_args 指定的路径）/var/lib/tftpboot。

```
[root@localhost ~]# cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/
```

将 ISO 镜像中的 initrd.img 和 vmlinuz 拷贝到/var/lib/tftpboot 路径下，把 ISO 镜像上传到 PXE server，先挂载镜像，然后从镜像中找到这两个文件。

```
[root@localhost ~]# mount /home/h3c/CSAP-NTA-V200_H3C-CMW710-E1260P11-X64.iso /mnt/
mount: /dev/loop0 is write-protected, mounting read-only #iso 名称以实际版本为准
```

```
[root@localhost ~]# cp /mnt/pxeboot/{initrd.img,vmlinuz} /var/lib/tftpboot
```

拷贝版本到 nfs 共享目录下。

```
[root@localhost ~]# mkdir /var/www/html/CSAP-NTA-V200 #CSAP-NTA-V200 为自定义名称，可根据需求更改
```

```
[root@localhost ~]# cp -a /mnt/* /var/www/html/fw1000
```

(3) 配置 nfs 共享目录。

修改/etc/exports 文件，内容如下：

```
[root@localhost ~]# vi /etc/exports
```

```
/var/www/html/CSAP-NTA-V200 192.168.0.0/16(rw,async)
```

注意：

x.x.x.x/x 为 nfs client 的网段，这里应该就是 dhcpd.conf 中配置分配给 client 的网段。

(rw,async)为访问权限。

通过执行 exportfs -r 命令生效。

重启 rpcbind 和 nfs 服务。

```
[root@localhost ~]# systemctl restart rpcbind
```

```
[root@localhost ~]# systemctl restart nfs
```

(4) 配置文件。

创建 pxelinux.cfg 文件夹

```
[root@localhost ~]# mkdir /var/lib/tftpboot/pxelinux.cfg
```

拷贝引导文件。

```
[root@localhost ~]# cp /mnt/pxeboot/pxelinux.cfg /var/lib/tftpboot/pxelinux.cfg/default
```

修改 default 文件。

```
[root@localhost ~]# chmod u+w /var/lib/tftpboot/pxelinux.cfg/default
```

```
[root@localhost ~]# vi /var/lib/tftpboot/pxelinux.cfg/default
```

```
default Live
```

Since no network setting in the squashfs image, therefore if ip=, the network is disabled. That's what we want.

label Live

kernel vmlinuz

```
append initrd=initrd.img boot=live union=overlay username=user config components quiet
noswap edd=on nomodeset locales=en_US.UTF-8 keyboard-layouts=NONE
ocs_live_run="/opt/VSR/setup_vsr_pxe.sh" ocs_live_extra_param="" ocs_live_batch="no"
ocs_final_action="reboot" vga=788 ip= net.ifnames=0 nosplash i915.blacklist=yes
radeonhd.blacklist=yes nouveau.blacklist=yes vmwgfx.enable_fbdev=1
fetch=http://192.168.1.87/CSAP-NTA-V200/live/filesystem.squashfs ocs_prerun="mkdir
/mnt/cdrom" ocs_prerun1="mount -t nfs 192.168.1.87:/var/www/html/CSAP-NTA-V200
/mnt/cdrom/"
```

TEXT HELP

* Boot menu for BIOS machine

* Disclaimer: Live system comes with ABSOLUTELY NO WARRANTY

ENDTEXT

修改以下配置:

fetch 后面的路径为 filesystem.squashfs 在 PXE Server 上存放的路径。

ocs_prerun1 的动作为挂载 nfs 文件系统, 路径需为 nfs server 实际共享的路径。

如果安装模式为 PXE 无人值守方式, 同时修改以下配置:

ocs_live_run 执行脚本增加无人值守参数, 修改为 ocs_live_run="/opt/VSR/setup_vsr_pxe.sh unattended fresh "。

10.2 Ubuntu系统下环境搭建

本节以 Ubuntu 5.4.0-6ubuntu1~16.04.10 的 server 版本为例进行说明, 其他 Ubuntu 版本可能会有些微差别。

本文统一使用 apt-get 工具进行安装, 如果环境中可以正常连接外网, 则直接使用下文中提到的 apt-get 命令安装即可; 如果无法连接外网, 则可以使用系统对应的 ISO 作为本地镜像源进行安装。

配置本地镜像源的方法如下:

(1) 上传镜像文件到系统 (或者通过 CDROM 挂载进设备)。

(2) mount ISO 文件到本地。

```
h3c@ubuntu:~$ sudo mount /dev/sr0 /media/cdrom/
```

```
mount: /dev/sr0 is write-protected, mounting read-only
```

这里使用 CDROM 的方式挂载的镜像文件, 所以会多出一个/dev/sr0 设备。

(3) 修改/etc/apt/下的配置文件。

备份默认的 repo 文件。

```
h3c@ubuntu:/etc/apt$ sudo mkdir bak
```

```
h3c@ubuntu:/etc/apt$ sudo mv sources.list bak/
```

```
# 重新编写 source.list 文件。
h3c@ubuntu:/etc/apt$ sudo vi sources.list
# 修改文件内容如下：
[deb file:///media/cdrom/ubuntu xenial main #xenial 为 ubuntu 发行版昵称，main 代表源类型为支持的开源软件
#刷新源
h3c@ubuntu:/etc/apt$ sudo apt-get update
```

10.2.2 安装并配置 DHCP

配置过程中可能会由于书写错误等遇到一些问题，需根据具体问题定位。

(1) 安装 DHCP。

```
h3c@ubuntu:/etc/apt$ sudo apt-get -y install isc-dhcp-server
```

(2) 修改配置文件。

```
# 修改/etc/default/isc-dhcp-server 配置文件，指定提供 DHCP 服务的接口。
```

```
h3c@ubuntu:~$ sudo vi /etc/default/isc-dhcp-server
```

```
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
```

```
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
```

```
INTERFACES="ens3" #根据实际环境修改
```

```
# 修改/etc/dhcp/dhcpd.conf 配置文件。
```

```
h3c@ubuntu:~$ sudo vi /etc/dhcp/dhcpd.conf
```

```
# option definitions common to all supported networks...
```

```
# option domain-name "example.org";
```

```
# option domain-name-servers ns1.example.org, ns2.example.org; #注释掉这两项
```

```
# A slightly different configuration for an internal subnet.
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
    range 192.168.1.100 192.168.1.200; #取消注释，根据实际分配的网段修改。
```

```
# option domain-name-servers ns1.internal.example.org;
```

```
# option domain-name "internal.example.org";
```

```
# option subnet-mask 255.255.255.224;
```

```
# option routers 10.5.5.1;
```

```
# option broadcast-address 10.5.5.31;
```

```
# default-lease-time 600;
```

```
# max-lease-time 7200;
```

```
    next-server 192.168.1.88;
```

```
    filename "pxelinux.0";
```

```
    allow booting;
```

```
    allow bootp; #增加这几项配置。
```

```
}
```

注意：dhcpd.conf 中的配置只修改文中的部分，其他保持默认即可。

(3) 启动/重启 DHCP 服务。

```
h3c@ubuntu:~$ sudo systemctl restart isc-dhcp-server
```

查看服务状态。

```
h3c@ubuntu:~$ sudo systemctl status isc-dhcp-server
```

```
isc-dhcp-server.service - ISC DHCP IPv4 server
```

```
Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
```

```
Active: active (running) since Sat 2019-08-17 00:04:30 MST; 20s ago
```

注意，DHCP 配置的网段要和接口地址在同一网段，否则 DHCP 无法分配地址。

10.2.3 安装并配置 TFTP

(1) 安装 TFTP。

```
h3c@ubuntu:~$ sudo apt-get -y install tftpd-hpa
```

(2) 修改配置文件。

```
h3c@ubuntu:~$ sudo vi /etc/default/tftpd-hpa
```

```
# /etc/default/tftpd-hpa
```

```
TFTP_USERNAME="tftp"
```

```
TFTP_DIRECTORY="/var/lib/tftpboot"
```

```
TFTP_ADDRESS=":69"
```

```
TFTP_OPTIONS="--secure"
```

注意：TFTP_DIRECTORY 根据需要进行修改，这里使用默认目录。

(3) 启动/重启 TFTP 服务。

```
h3c@ubuntu:~$ sudo systemctl restart tftpd-hpa
```

查看服务状态。

```
h3c@ubuntu:~$ sudo systemctl status tftpd-hpa
```

```
tftpd-hpa.service - LSB: HPA's tftp server
```

```
Loaded: loaded (/etc/init.d/tftpd-hpa; bad; vendor preset: enabled)
```

```
Active: active (running) since Sat 2019-08-17 00:10:51 MST; 28s ago
```

10.2.4 安装并配置 http

配置过程中可能会由于书写错误等遇到一些问题，需根据具体问题定位。

(1) 安装 HTTP。

```
h3c@ubuntu:~$ sudo apt-get -y install apache2
```

(2) 配置文件。

Apache2 对应的配置文件位置为 /etc/apache2/sites-available/000-default.conf，其中 DocumentRoot 定义的路径为 http 访问的根路径，缺省为 /var/www/html。

```
h3c@ubuntu:~$ sudo cat /etc/apache2/sites-available/000-default.conf | grep DocumentRoot
    DocumentRoot /var/www/html
```

(3) 启动/重启 HTTP 服务。

```
h3c@ubuntu:~$ sudo systemctl restart apache2
```

查看服务状态。

```
h3c@ubuntu:~$ sudo systemctl status apache2
```

```
apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: active (running) since Sat 2019-08-17 00:17:36 MST; 49s ago
```

10.2.5 安装并配置 NFS

(1) 安装 nfs。

由于 iso 镜像中没有 nfs-kernel-server 的 deb 包，可以从 <https://pkgs.org> 网站上下载对应版本的 deb 包并上传到 server 上。

```
h3c@ubuntu:~$ ls
```

```
nfs-kernel-server_1.2.8-9ubuntu12_amd64.deb
```

(2) 安装 nfs-server 依赖文件。

```
h3c@ubuntu:~$ sudo apt-get -y install nfs-common
```

使用 dpkg 命令安装 nfs-kernel-server。

```
h3c@ubuntu:~$ sudo dpkg --force-depends-version -i nfs-kernel-server_1.2.8-9ubuntu12_amd64.deb
```

注意：由于后下载的 nfs-kernel-server 需要 nfs-common (= 1:1.2.8-9ubuntu12)，而 iso 中自带的版本为 1:1.2.8-9ubuntu12.1，故这里使用选项--force-depends-version，应该不影响功能。

10.2.6 配置 server

(1) 拷贝引导文件及版本文件。

找到 ubuntu 镜像文件中的 pxelinux.0、ldlinux.c32 文件，拷贝到 tftp server 的工作路径下（tftp 配置文件中 server_args 指定的路径）/var/lib/tftpboot/。

```
h3c@ubuntu:~$ sudo cp /media/cdrom/install/netboot/ubuntu-installer/amd64/pxelinux.0 /var/lib/tftpboot/
```

```
h3c@ubuntu:~$ sudo cp /media/cdrom/install/netboot/ubuntu-installer/amd64/boot-screens/ldlinux.c32 /var/lib/tftpboot/
```

将 ISO 镜像中的 initrd.img 和 vmlinuz 拷贝到/var/lib/tftpboot 路径下，把 ISO 镜像上传到 PXE server，先挂载镜像，然后从镜像中找到这两个文件。

```
h3c@ubuntu:~$ sudo mount CSAP-NTA-V200_H3C-CMW710-E1260P10-X64.iso /mnt/
```

mount: /dev/loop0 is write-protected, mounting read-only #iso 名称以实际版本为准

```
h3c@ubuntu:~$ sudo cp /mnt/pxeboot/{initrd.img,vmlinuz} /var/lib/tftpboot
```

```

# 拷贝版本到 nfs 共享目录下。
h3c@ubuntu:~$ sudo mkdir /var/www/html/CSAP-NTA-V200 #CSAP-NTA-V200 为自定义名称,
可根据需求更改
h3c@ubuntu:~$ sudo cp -a /mnt/* /var/www/html/CSAP-NTA-V200/
(2) 配置 nfs 共享目录。
# 修改/etc/exports 文件, 内容如下:
h3c@ubuntu:~$ sudo vi /etc/exports
/var/www/html/CSAP-NTA-V200 *(ro,async,no_subtree_check)
# 注意: *表示不限制客户端。(ro,async,no_subtree_check)为访问权限。
# 重启 nfs-kernel-server 服务。
h3c@ubuntu:~$ sudo systemctl restart nfs-kernel-server
# 查看服务状态。
h3c@ubuntu:~$ sudo systemctl status nfs-kernel-server
nfs-server.service - NFS server and services
   Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2019-08-17 01:24:54 MST; 11s ago
(3) 配置文件。
# 创建 pxelinux.cfg 文件夹。
h3c@ubuntu:~$ sudo mkdir /var/lib/tftpboot/pxelinux.cfg
# 拷贝引导文件。
h3c@ubuntu:~$ sudo cp /mnt/pxeboot/pxelinux.cfg /var/lib/tftpboot/pxelinux.cfg/default
# 修改 default 文件。
h3c@ubuntu:~$ sudo chmod u+w /var/lib/tftpboot/pxelinux.cfg/default
h3c@ubuntu:~$ sudo vi /var/lib/tftpboot/pxelinux.cfg/default
default Live

# Since no network setting in the squashfs image, therefore if ip=, the network is disabled. That's
what we want.
label Live
   kernel vmlinuz
   append initrd=initrd.img boot=live union=overlay username=user config components quiet
noswap   edd=on   nomodeset   locales=en_US.UTF-8   keyboard-layouts=NONE
ocs_live_run="/opt/VSR/setup_vsr_pxe.sh"   ocs_live_extra_param=""   ocs_live_batch="no"
ocs_final_action="reboot"   vga=788   ip=   net.ifnames=0   nosplash   i915.blacklist=yes
radeonhd.blacklist=yes   nouveau.blacklist=yes   vmwgfx.enable_fbdev=1
fetch=http://192.168.1.87/CSAP-NTA-V200/live/filesystem.squashfs   ocs_prerun="mkdir
/mnt/cdrom"   ocs_prerun1="mount -t nfs 192.168.1.87:/var/www/html/CSAP-NTA-V200
/mnt/cdrom/"
   TEXT HELP

```

* Boot menu for BIOS machine

* Disclaimer: Live system comes with ABSOLUTELY NO WARRANTY

ENDTEXT

修改以下配置:

fetch 后面的路径为 filesystem.squashfs 在 PXE Server 上存放的路径, ocs_prerun1 的动作为挂载 nfs 文件系统, 路径需为 nfs server 实际共享的路径。

如果安装模式为 PXE 无人值守方式, 同时修改以下配置:

ocs_live_run 执行脚本增加无人值守参数, 修改为 ocs_live_run="/opt/VSR/setup_vsr_pxe.sh unmanned fresh "。