

AnaTraf Virtual 安装指南 (VMWareESXi)

- 介绍 2**
- 1.创建存储 2**
- 2.创建虚拟交换机..... 3**
- 3.创建端口组 4**
- 4.创建虚拟机 5**
- 5.修改虚拟机配置..... 7**
- 6.配置管理口 IP 8**
- 7.配置硬盘 10**

介绍

最低配置要求：

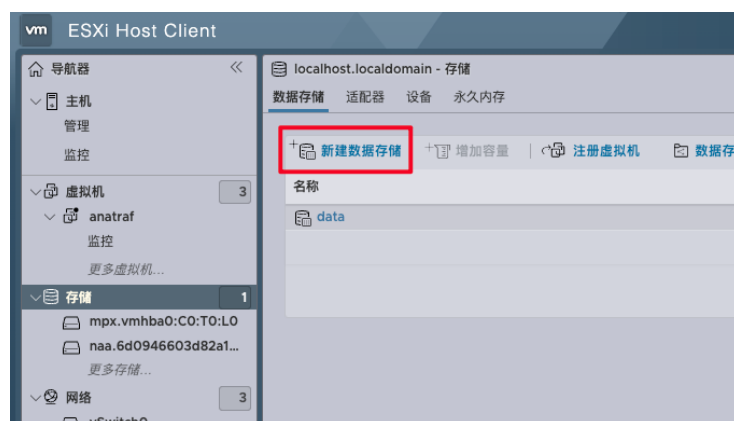
- 网卡数量 ≥ 2
- CPU 核心 ≥ 4
- 内存 ≥ 8 GB
- 硬盘大小 ≥ 50 GB

性能：

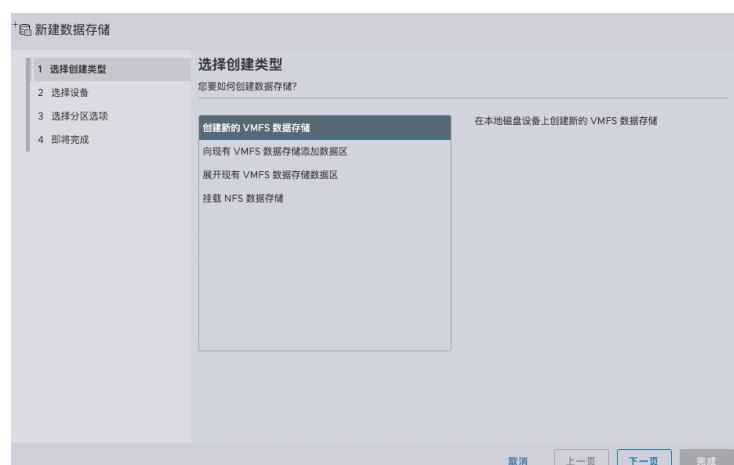
- 带宽 100M
- 分析数据存储 7 天
- PCAP 存储 512G

1.创建存储

登录 ESXi Host Client，点击左侧导航栏的“存储”，再点击“新建数据存储”：



选择创建新的 VMFS 数据存储：



选择分区选项：



2.创建虚拟交换机

登录 ESXi Host Client，点击左侧导航栏的“网络”，点击“虚拟交换机”标签，再点击“添加标准虚拟交换机”：



填写配置项, 添加所需的上行链路 (待分析的流量), 安全选项中的混杂模式选择“接受”:

添加标准虚拟交换机 - 新建交换机

vSwitch 名称: 新建交换机

MTU: 1500

上行链路 1: vmnic1 - 关机

上行链路 2: vmnic2 - 关机

链路发现: 单击以展开

安全

混杂模式: ☒ 接受 ☐ 拒绝

MAC 地址更改: ☐ 接受 ☒ 拒绝

伪传输: ☐ 接受 ☒ 拒绝

取消 添加

3.创建端口组

登录 ESXi Host Client, 点击左侧导航栏的“网络”, 点击“端口组”标签, 再点击“添加端口组”:



配置管理口端口组, 选择相应的虚拟交换机:

添加端口组 - 新建端口组

名称: 新建端口组

VLAN ID: 0

虚拟交换机: vSwitch0

安全: 单击以展开

取消 添加

配置业务口端口组，选择第 3 步中创建的虚拟交换机：

添加端口组 - 新建端口组

名称	新建端口组
VLAN ID	0
虚拟交换机	镜像交换机
> 安全	单击以展开

取消

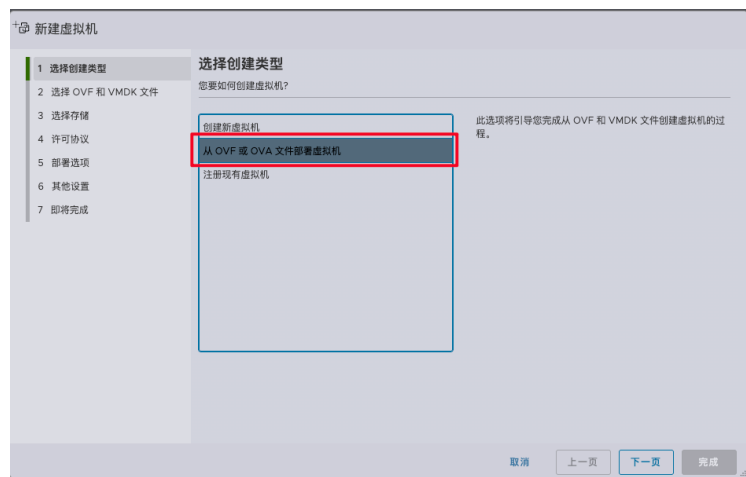
添加

4.创建虚拟机

登录 ESXi Host Client，点击左侧导航栏的“虚拟机”，再点击“创建虚拟机”：



选择“从 OVF 或 OVA 文件部署虚拟机”：



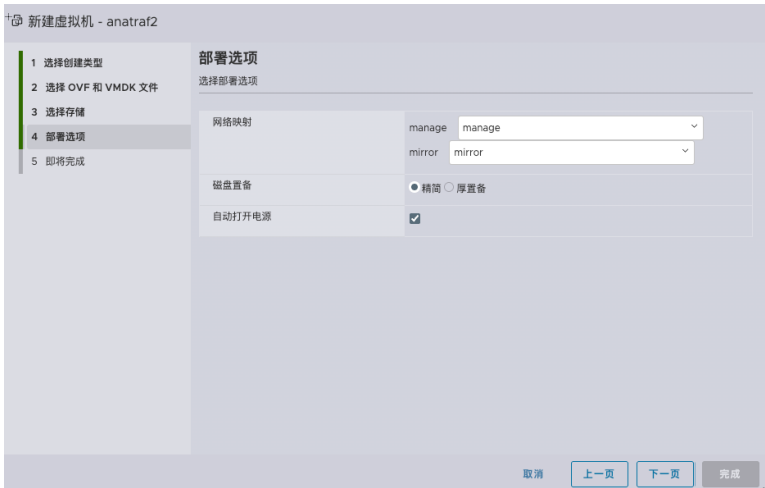
输入虚拟机名称，选择相应的 OVF 和 VMDK 文件：



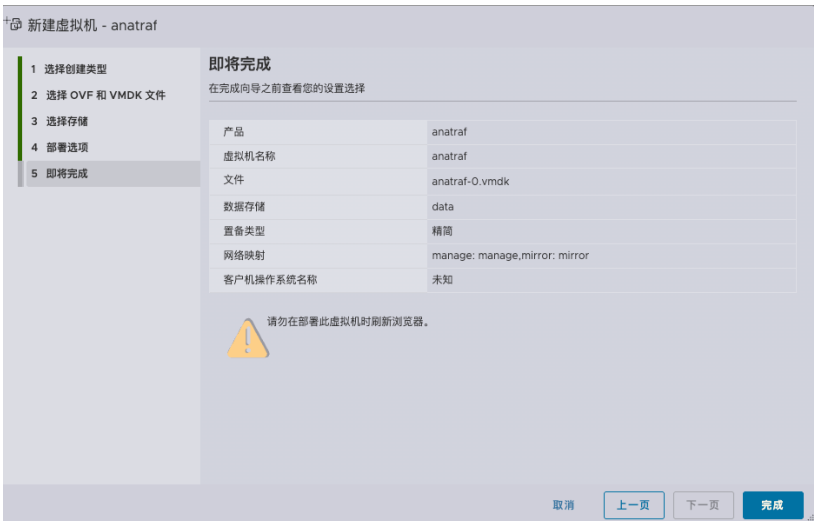
为虚拟机选择一个数据存储：



配置网络映射，其中 manage 为管理网口，mirror 为业务口：



完成创建虚拟机：

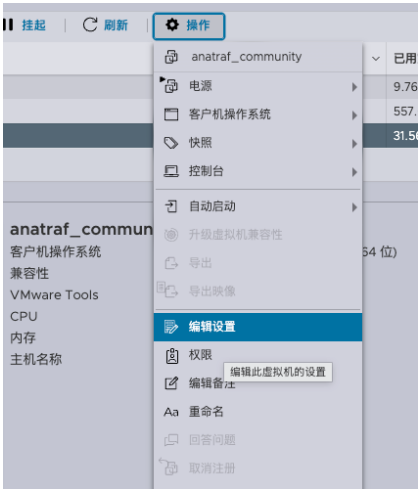


等待近期任务中创建虚拟机的任务完成：

近期任务		
任务	对象	启动者
Import VApp	Resources	root
上传磁盘 - anatraf-0.vmdk (1 of 1)	anatraf2	root

5.修改虚拟机配置

在虚拟机列表中，选中新创建的虚拟机，点击“操作”菜单栏中的“编辑设置”：

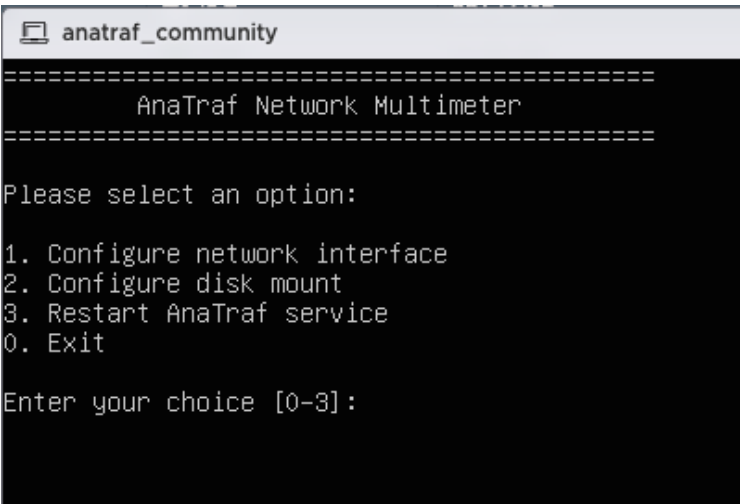


可以调整 CPU 数，内存大小，硬盘大小，网络适配器数量（至少 2 个）。其中的“硬盘 2”用于存储 pcap 文件。



6.配置管理口 IP

开启创建好的 anatraf 虚拟机，登录用户和密码都是 anatraf，选择第 1 项配置管理口 IP：



选择一个网口作为管理口，其余的网口将自动设置成业务口。界面显示的网卡顺序与配置虚拟机网卡时，在虚拟机硬件详情中的网卡顺序一致：

```
anatraf
=====
          AnaTraf Network Multimeter
=====

AnaTraf Control Interface IP Configuration (Netplan)

Available interfaces:

1. ens34
2. ens35
0. Return to main menu

Please select the interface to modify control IP [0-2]:
1_
```

输入静态 IP，掩码和网关后完成配置：

```
anatraf
=====
          AnaTraf Network Multimeter
=====

AnaTraf Control Interface IP Configuration (Netplan)

Available interfaces:

1. ens34
2. ens35
0. Return to main menu

Please select the interface to modify control IP [0-2]:
1
Please enter the control IP for ens34 (CIDR format, e.g. 192.168.1.10/24) [192.168.1.210/24]:
192.168.1.210
Please enter default gateway (can be left empty to skip) [192.168.1.1]:
192.168.1.1
Applying Netplan configuration...
Netplan application failed, rolling back from backup: /etc/netplan/00-installer-config.yaml.bak
Netplan write or application failed, please check permissions or configuration.
Press any key to return to the main menu...
```

7.配置硬盘

开启创建好的 anatraf 虚拟机，登录用户和密码都是 anatraf，选择第 2 项配置硬盘：

```
anatraf_community
=====
AnaTraf Network Multimeter
=====

Please select an option:

1. Configure network interface
2. Configure disk mount
3. Restart AnaTraf service
0. Exit

Enter your choice [0-3]:
```

输入相应的硬盘序号：

```
anatraf_community
=====
AnaTraf Network Multimeter
=====

Disk Mount Configuration

Available non-system disk(s):

1. /dev/sdb Size: 25G Type: ext4

Select disk to mount [1-1]:
1_
```

配置完成后选择第 3 项重启 AnaTraf 服务，重启后，即可通过浏览器访问上述设置的管理口 IP，访问 AnaTraf 的 WEB 界面。

```
anatraf_community
=====
AnaTraf Network Multimeter
=====

Please select an option:

1. Configure network interface
2. Configure disk mount
3. Restart AnaTraf service
0. Exit

Enter your choice [0-3]:
```

AnaTraf 的 WEB 界面登录用户名为：admin，登录密码为：anatraf。

欢迎登录

登录