**技术文档**

**分布式虚拟化防火墙TopVSP-N**

**用户使用手册**

编制： 杨杰 日期：2017-02-20

审核： 日期：2017-02-20

批准： 日期：2017-02-20

变更记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 修订时间 | 修订人 | 修订类型 | 修订章节 | 修订内容 |
| 1.0 | 2017-02-20 | 杨杰 | A | 所有 | 编写所有章节 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

\*修订类型分为 **A** - ADDED **M** - MODIFIED **D** – DELETED

**目录**

[1 引言 4](#_Toc475627398)

[1.1 目的 4](#_Toc475627399)

[1.2 范围 4](#_Toc475627400)

[1.3 名词解释 4](#_Toc475627401)

[2 前提条件 4](#_Toc475627402)

[2.1 搭建vCenter server 4](#_Toc475627403)

[2.2 配置vCenter server 5](#_Toc475627404)

[3 VMware NSX基础环境部署 5](#_Toc475627405)

[3.1 NSX Manager管理平面部署 5](#_Toc475627406)

[3.1.1 获取与部署NSX Manager 6](#_Toc475627407)

[3.1.2 登录与配置NSX Manager 11](#_Toc475627408)

[3.1.3 将NSX Manager注册到vCenter 14](#_Toc475627409)

[3.1.4 备份NSX Manager 15](#_Toc475627410)

[3.2 NSX Controller控制平面部署 16](#_Toc475627411)

[3.2.1 NSX Controller安装部署 16](#_Toc475627412)

[3.3 VIB内核组件部署 18](#_Toc475627413)

[3.3.1 添加许可证 18](#_Toc475627414)

[3.3.1 ESXi主机安装VIB内核组件 20](#_Toc475627415)

[4 vSeccenter-N部署和应用 21](#_Toc475627416)

[4.1 部署vSeccenter-N 21](#_Toc475627417)

[4.2 配置vSeccenter-N 25](#_Toc475627418)

[4.3 登录和注册NSX服务 26](#_Toc475627419)

[4.4 部署和配置vFW 28](#_Toc475627420)

[4.5 配置安全组和重定向 35](#_Toc475627421)

[4.6 流量重定向结果验证 40](#_Toc475627422)

[5 参考书籍 42](#_Toc475627423)

# 引言

## 目的

本文档主要介绍了虚拟化桌面TVS基础环境部署、TVS-vCenter系统部署和应用及注意事项，旨在为初次接触TVS桌面虚拟化系统的技术人员提供帮助和指导。

## 范围

适用于对 TVS桌面虚拟化系统感兴趣的技术支持以及其他人员。

## 名词解释

**TVS：**是业界领先且最可靠的虚拟化平台。vSphere将[应用程序](http://baike.baidu.com/view/330120.htm)和[操作系统](http://baike.baidu.com/view/880.htm)从底层硬件分离出来，应用程序不再受底层操作系统的限制。vSphere允许一台物理服务器可以同时允许多个不同操作系统，同时也可以运行多个不同的应用程序，这样就跳出了一台服务器只能同时运行一个操作系统的框架，将单个服务器作为[资源池](http://baike.baidu.com/view/2385937.htm)进行管理，大大提高了硬件服务器的利用率。

**VMware NSX：**NSX是VMware软件定义数据中心的一部分，是一个虚拟化的网络和安全软件产品，NSX是一个独立的hypervisor云管理网络虚拟化平台，NSX可以提供完整的2-7层网络虚拟化服务。

# 前提条件

## 搭建vCenter server

VMware NSX需要提供搭建好的vCenter server环境，包括AD域服务器和DNS服务器，具体环境部署请参见《技术文档\_桌面虚拟化VMware vCenter Server6.0环境部署》。



## 配置vCenter server

搭建好vCenter server环境后，需要对其进行必要的配置，包括：添加许可、创建数据中心、创建集群、添加ESXi主机以及角色和权限分配等，如果集群下添加了多个ESXi主机，那么需要提前配置添加好共享存储和分布式虚拟交换机（vDS），如图1所示。

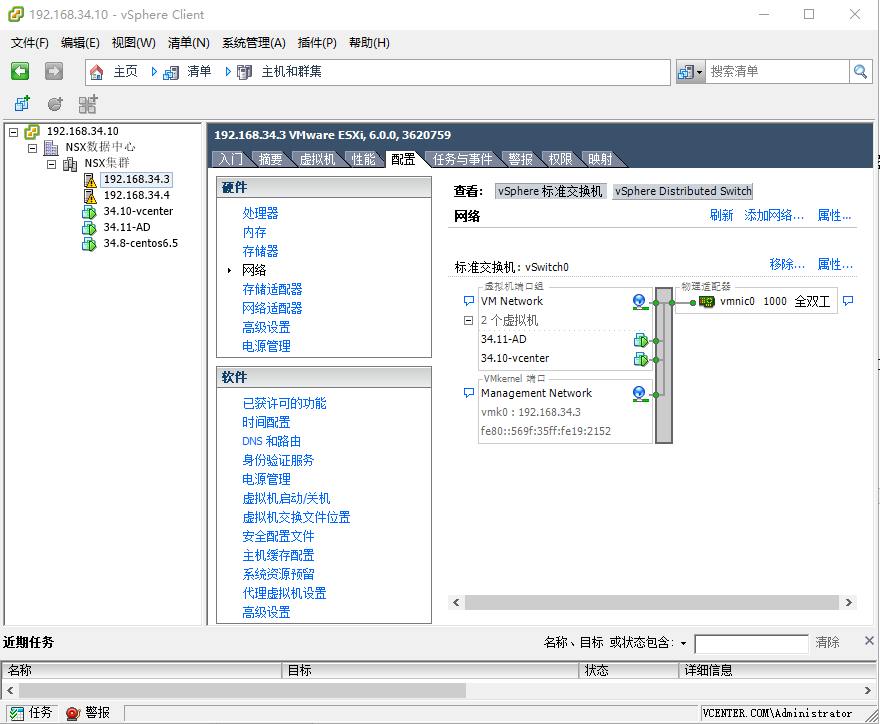


图1

# VMware NSX基础环境部署

## NSX Manager管理平面部署

NSX Manager是VMware NSX中的管理平面组件，只有当NSX Manager安装完成后，才能安装和部署VMware NSX的其他组件。NSX Manager的主要职责如下：

* 配置NSX Controller集群；
* 在ESXi主机的Hypervisor之上安装vSphere Installation Bundles（BIVs），已开启VXLAN、分布式路由器、分布式防火功能，并与NSX Controller集群进行信令信息交互。
* 配置NSX Edge服务网关，以关联负载均衡、VPN、NAT等网络服务。
* 为各种网络服务创建模板、快照等功能，实现快速和自动化部署逻辑网络。
* 为NSX Controller创建自签名证书，以允许ESXi主机加入NSX域，增强NSX控制平面的安全性。
* 提供网络流量的采集和监控功能。

### 获取与部署NSX Manager

NSX Manager通常是以打包OVA模板方式提供的，并允许用户使用vSphere Web Client将NSX Manager以虚拟机的形式进行安装部署。要获取这个文件，需要到VMware官方网站进行下载，或由用户对口的VMware原厂或代理商提供。

安装NSX Manager虚拟机的具体步骤如下：

1. 通过vSphere Web Client登录到vCenter主页，按照常规部署OVA模板的方式进行安装，右键单击需要部署的ESXi主机，选择从OVF模板进行部署，如图2所示。

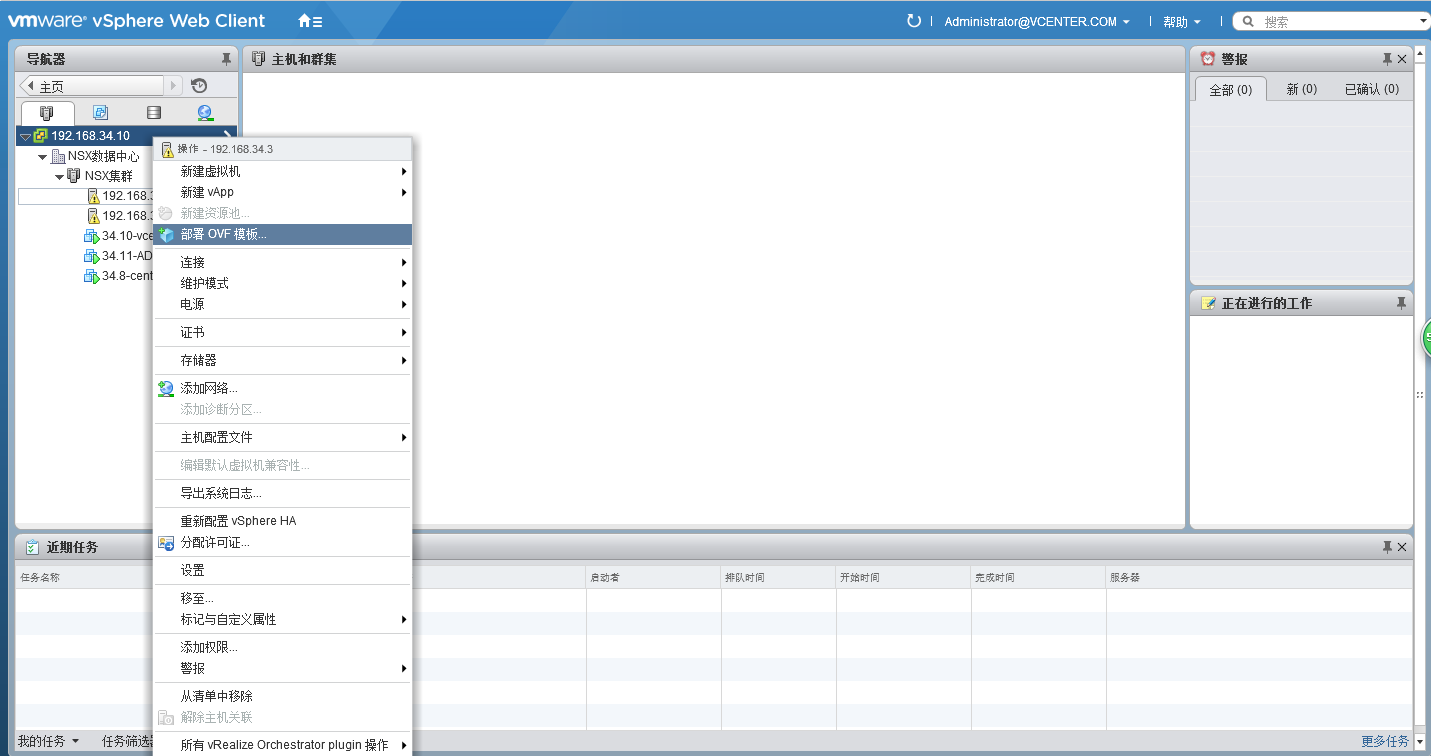


图2

1. 从本地文件夹选择NSX Manager的OVA文件，并点击“下一步”按钮，如图3所示。

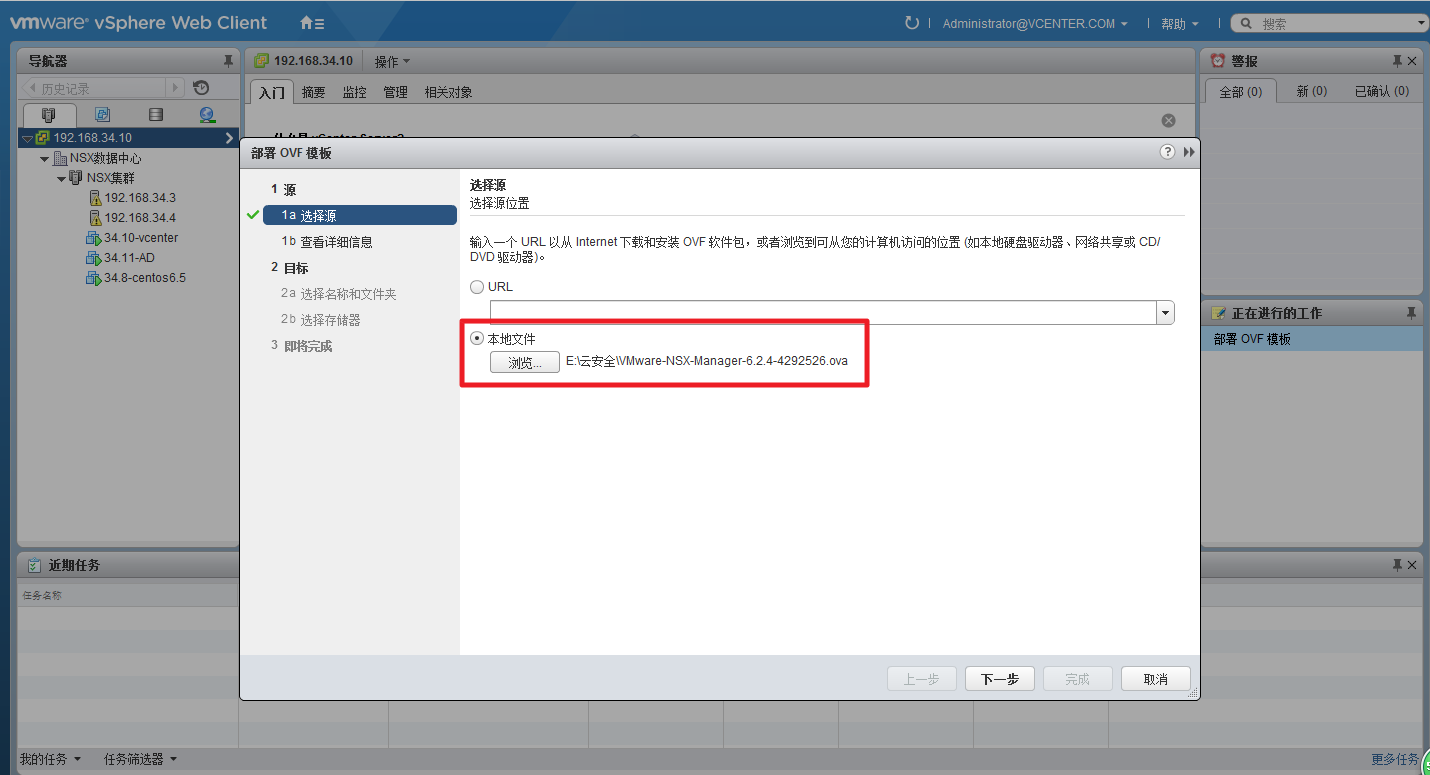


图3

1. 检查OVA模板的详细信息，并单击“下一步”按钮（需要勾选“接受额外配置选项”），如图4所示。

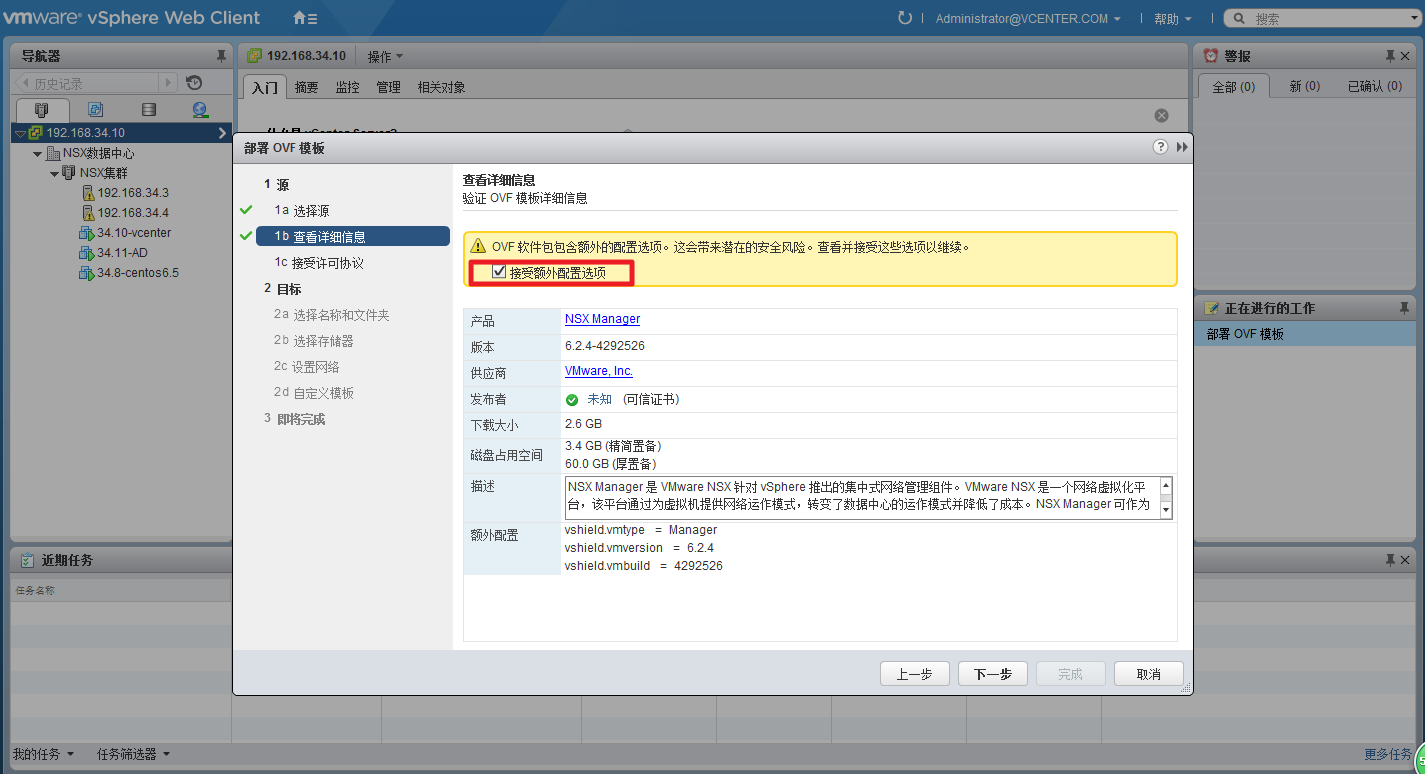


图4

1. 接受VMware的license协议，然后点击“下一步”按钮，如图5所示。

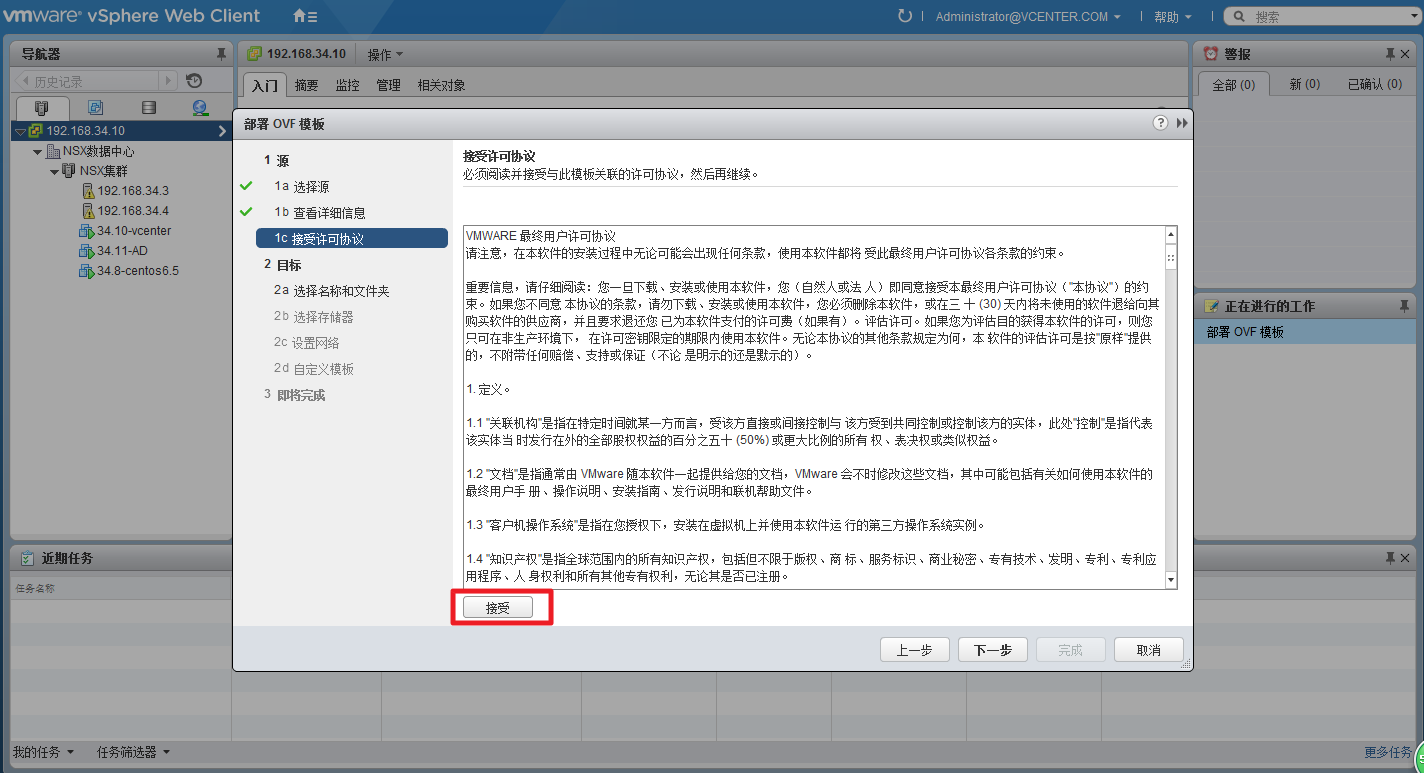


图5

1. 输入NSX Manager的名字，选择NSX Manager的安装位置，然后单击“下一步”按钮，如图6所示。

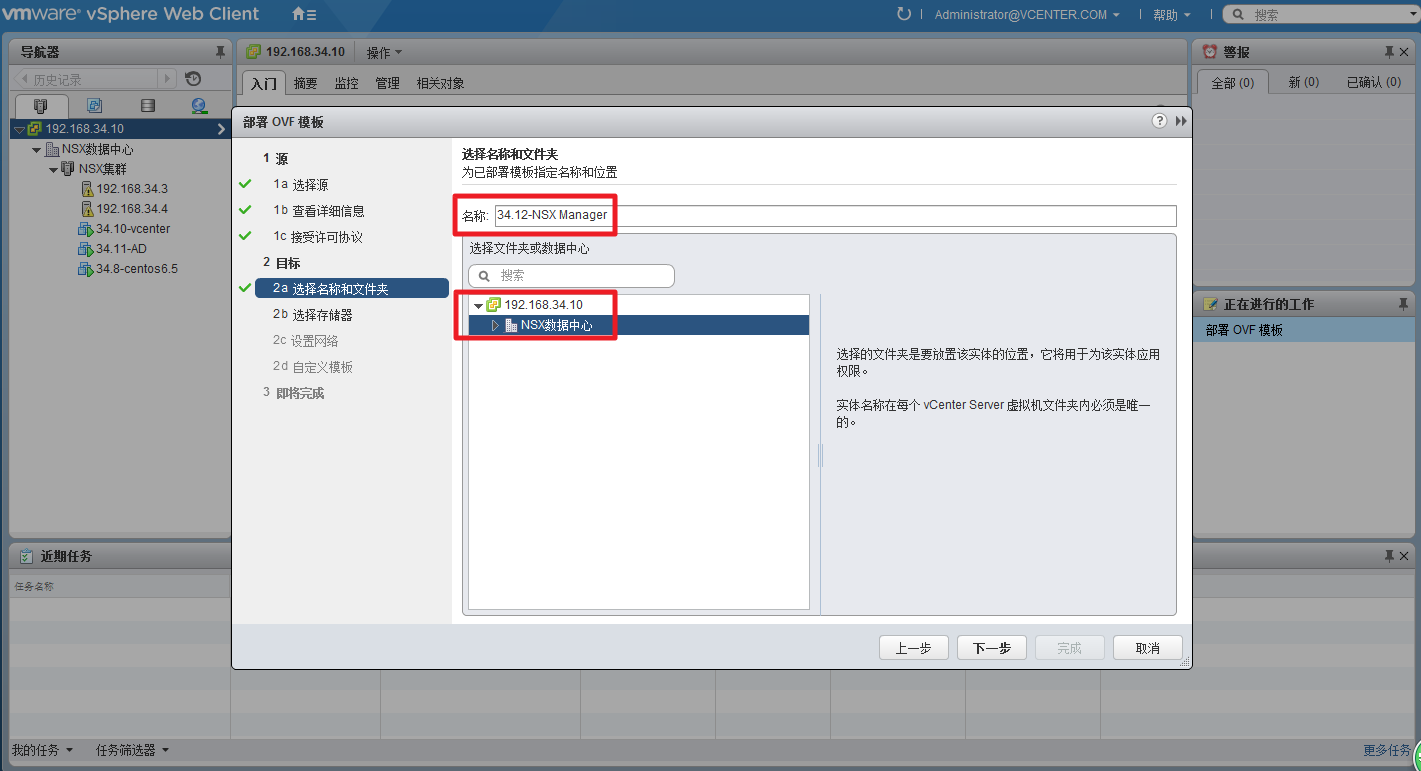


图6

1. 选择磁盘部署方式，选择磁盘位置，点击“下一步”按钮，如图7所示。

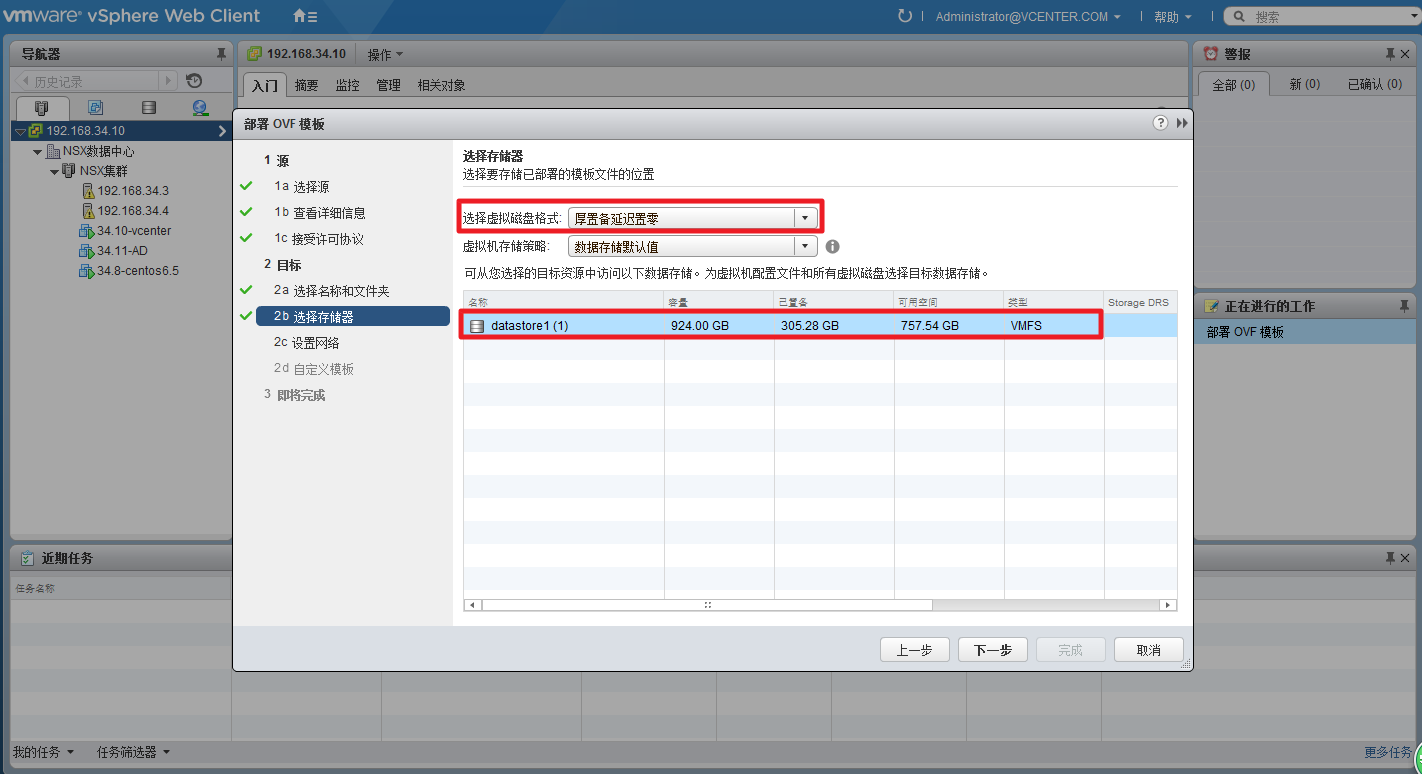


图7

1. 设置NSX Manager网络，单击“下一步”按钮，如图8所示。

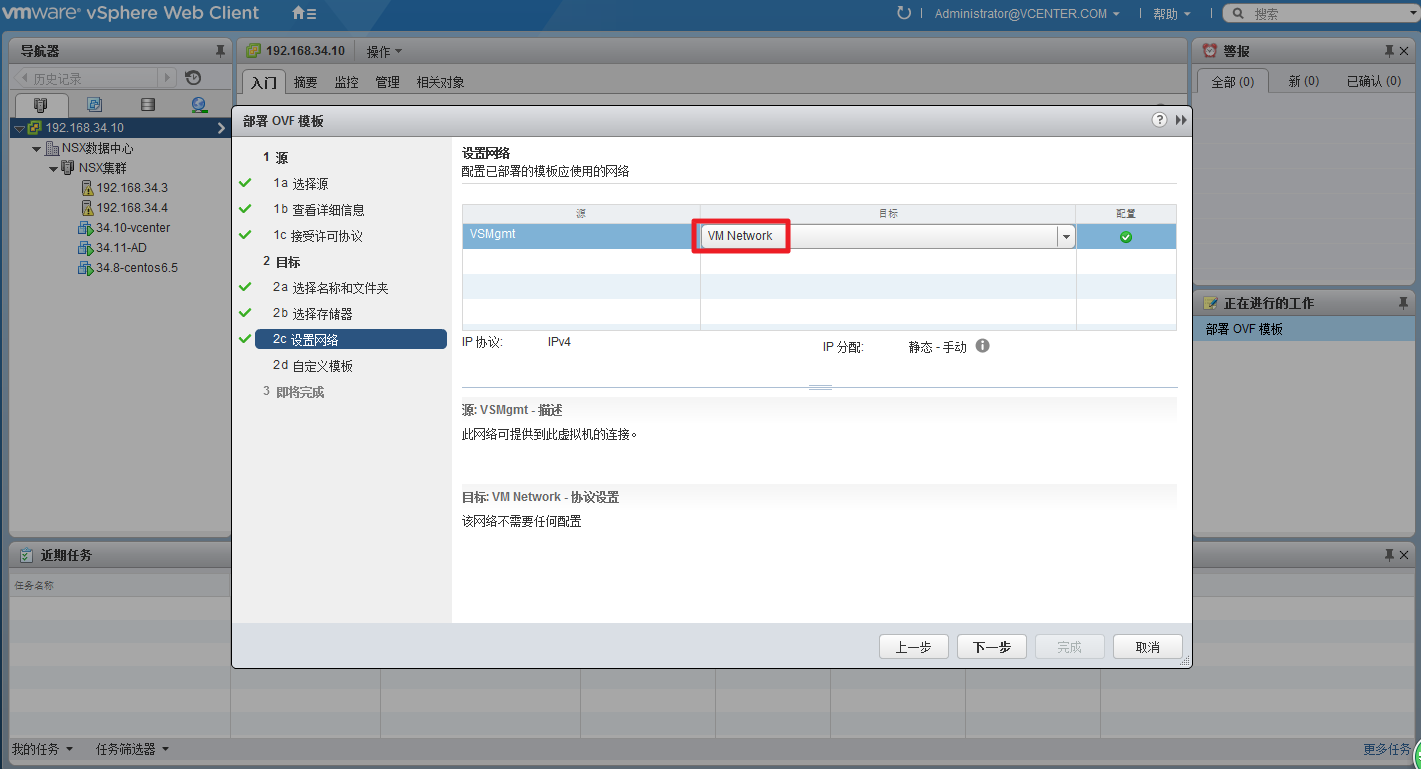


图8

1. 进入定制化模板页面，可进行以下设置，设置完成点击“下一步”按钮，如图9、10、11所示。

* CLI的密码。
* CLI的特权模式密码。
* NSX Manager虚拟机的主机名。
* IPv4的地址、掩码、网关。
* DNS地址、域和其他相关信息。
* NTP服务器。
* 开启SSH功能。

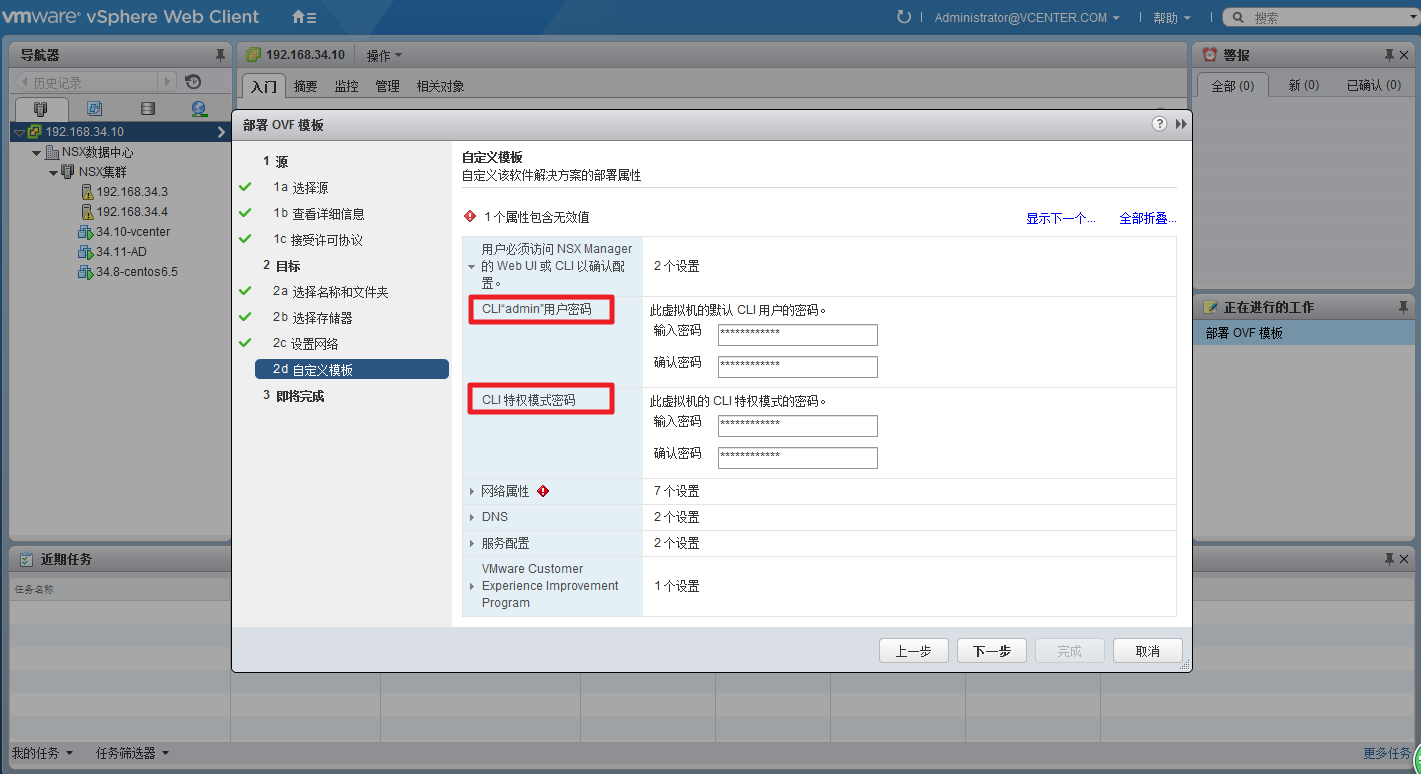


图9

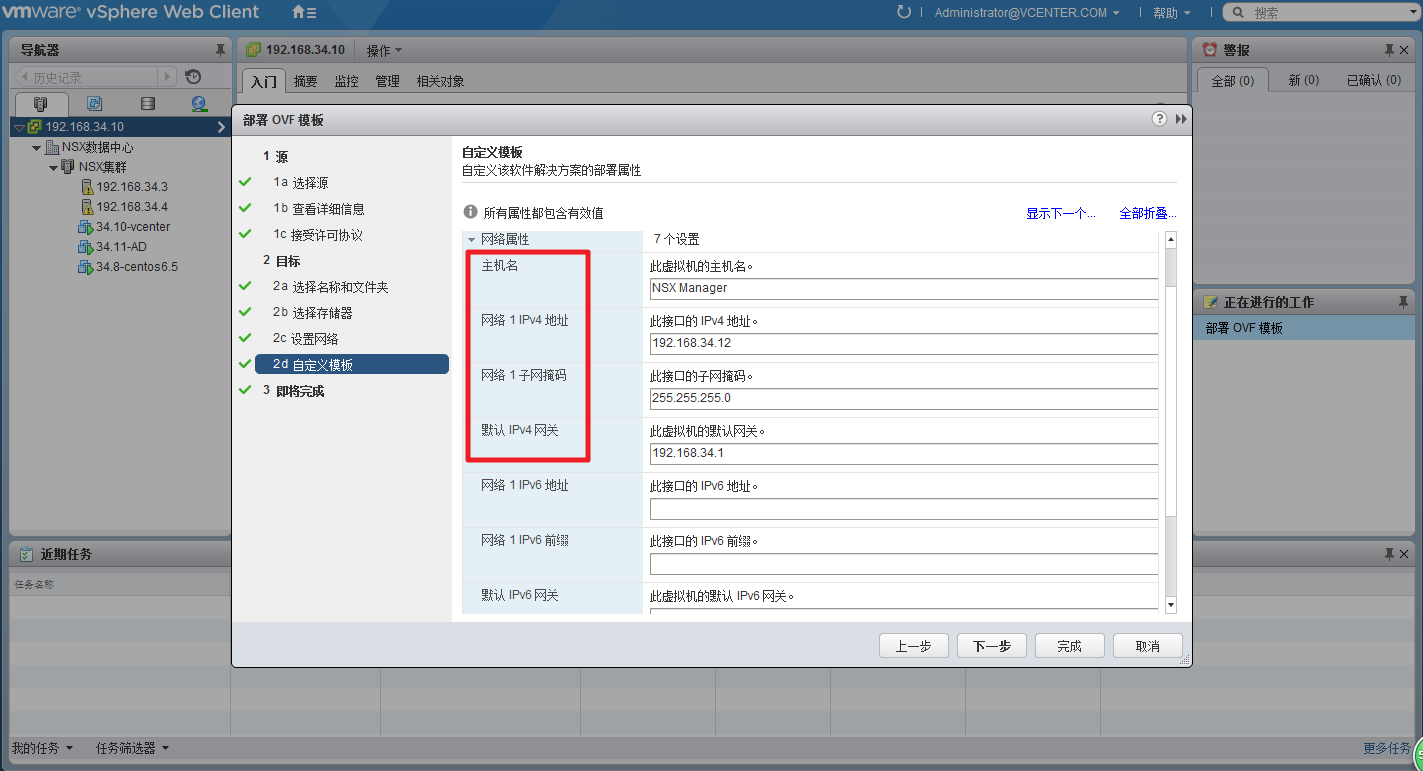


图10

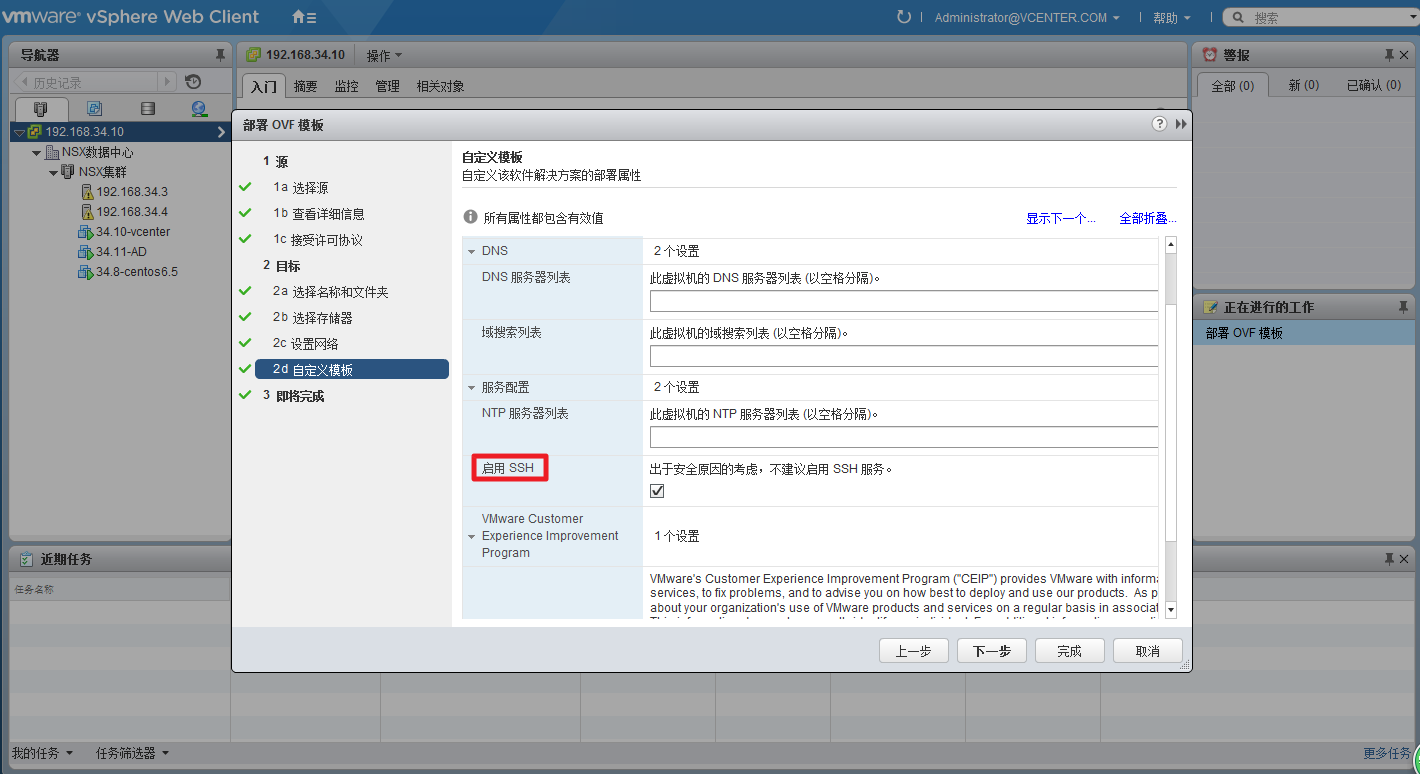


图11

1. 勾选“部署后打开电源”，点击“完成”按钮，至此NSX Manager安装完成，等待加电后并初始化完成，如图12所示。

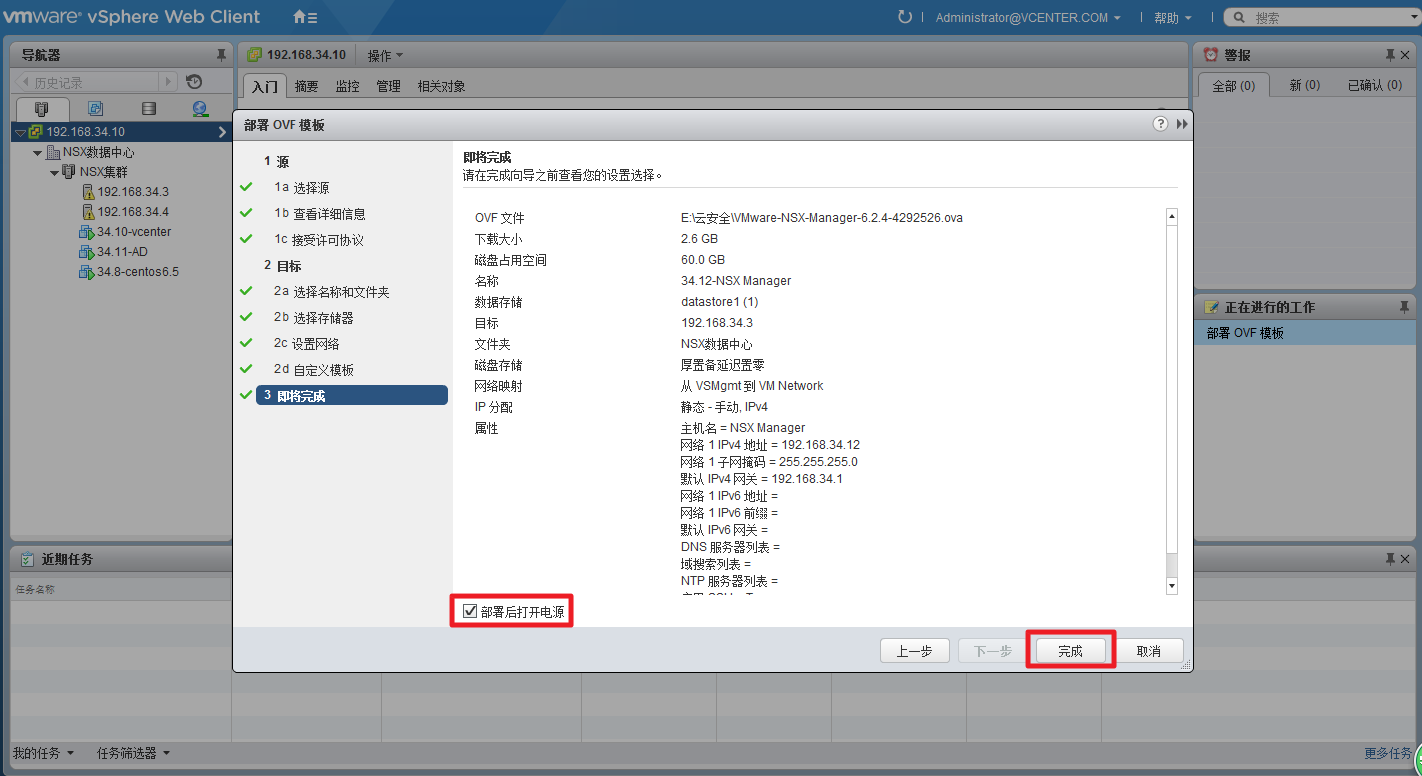


图12

### 登录与配置NSX Manager

安装完NSX Manager并确认已开启虚拟机后，就可以登录到NSX Manager，具体步骤如下：

1. 打开浏览器，建议使用Firefox或者IE11，输入NSX Manager的IP地址：<https://192.168.34.12>，用户名是admin，密码使用安装时设置的密码，如图13所示。

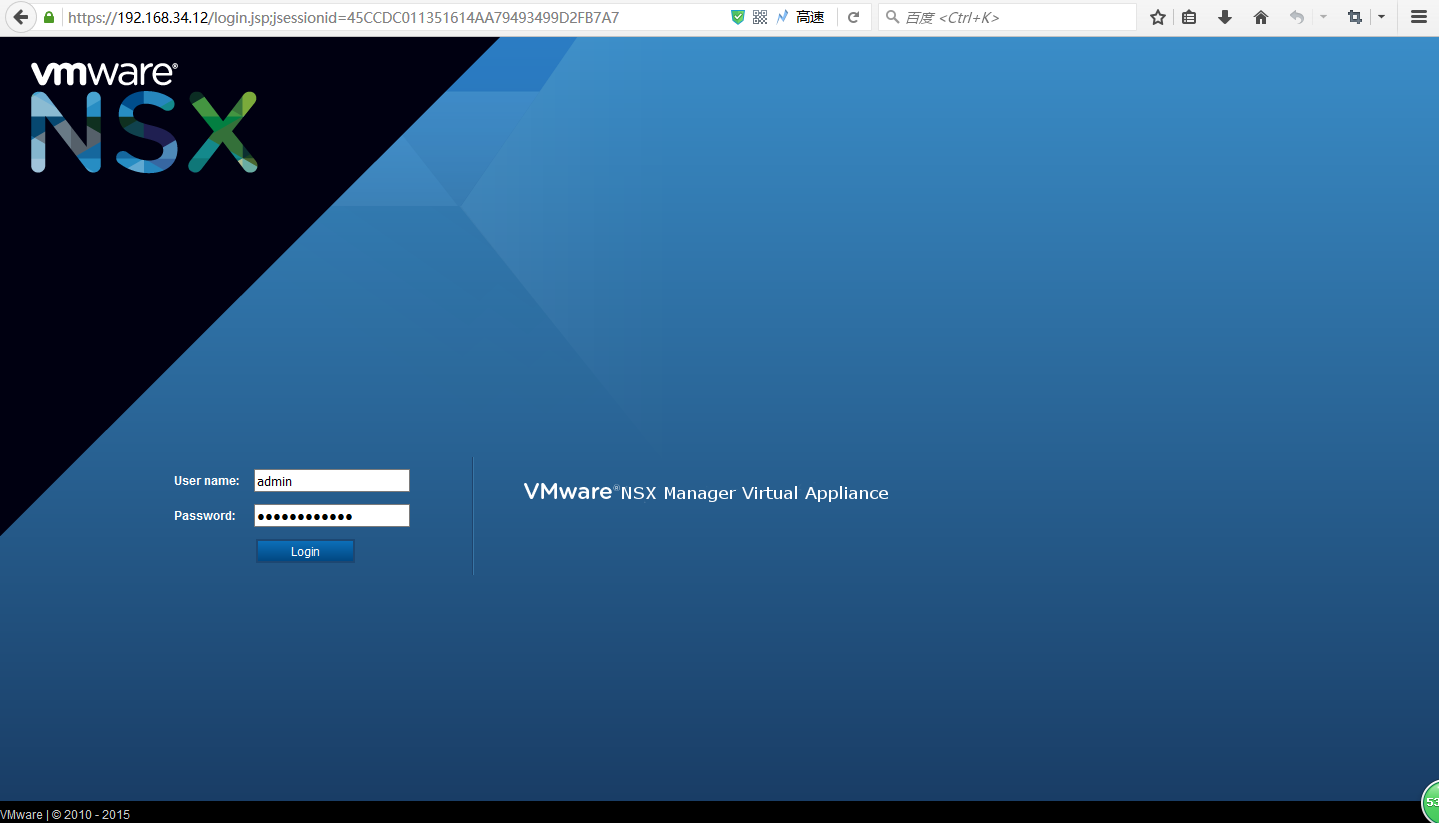


图13

1. 登录之后，可以点击View Summary对之前的安装情况进行检查，确认NSX Manager服务是否正常运行，如图14、15所示。

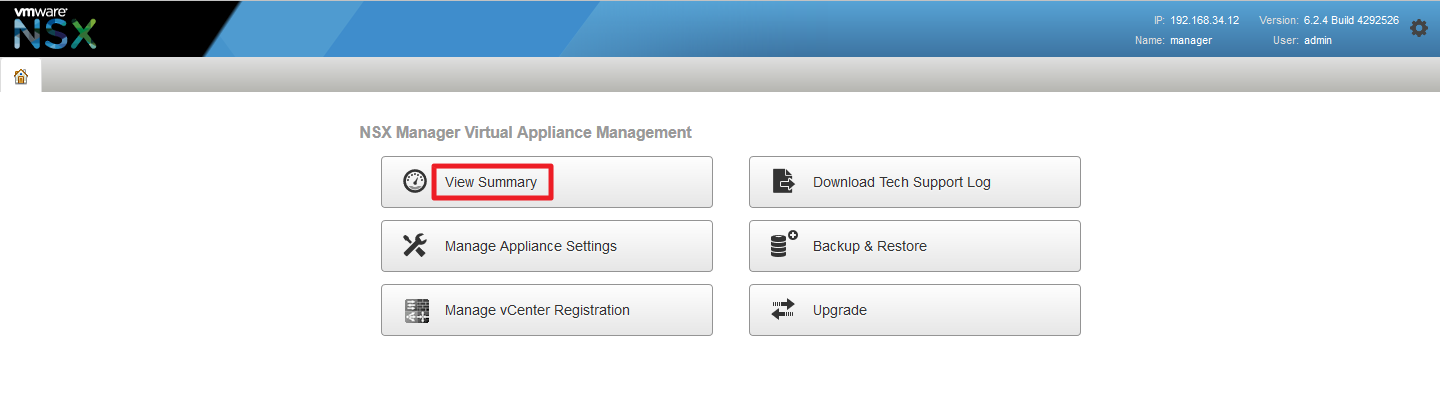


图14

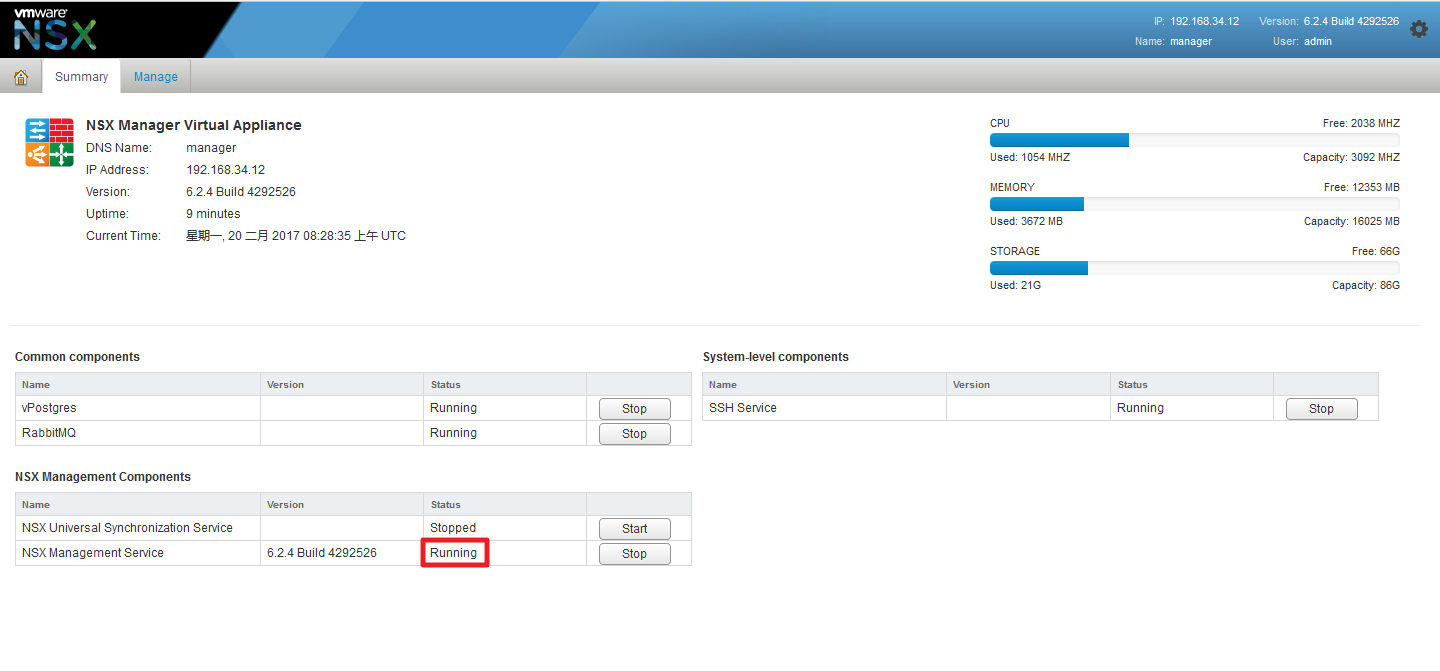


图15

1. 切换至Manager选项卡，这里可以查看和设置NTP服务、Syslog服务器、网络参数，如图16、17所示。

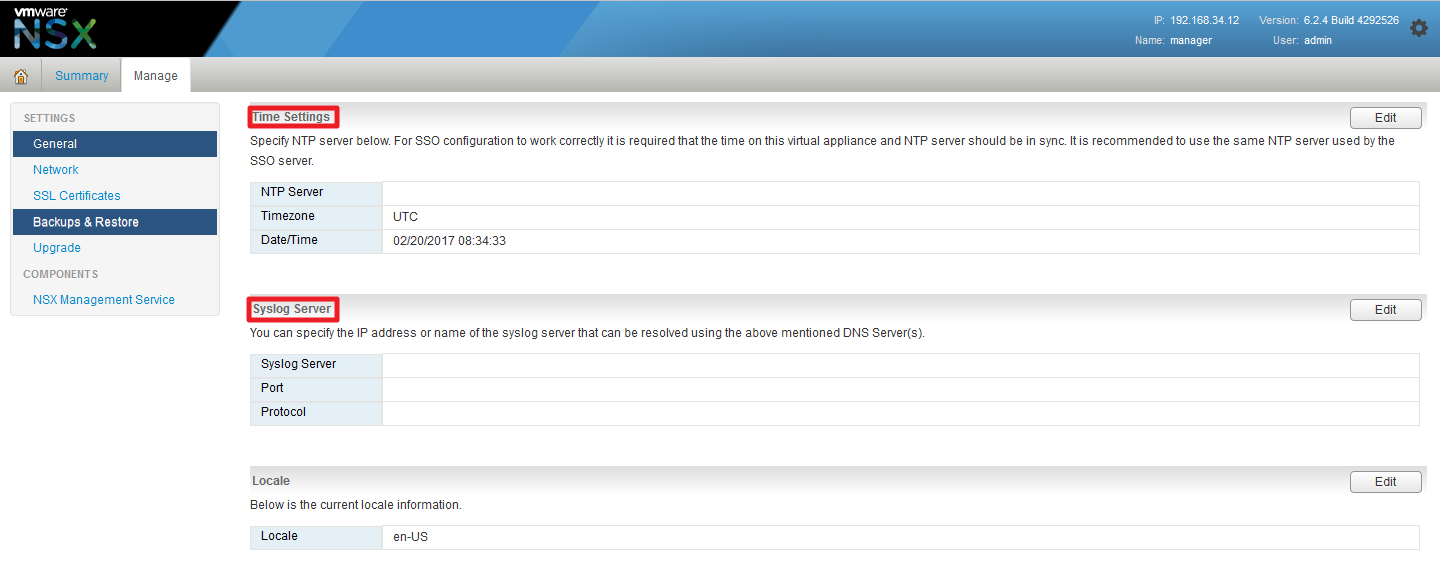


图16

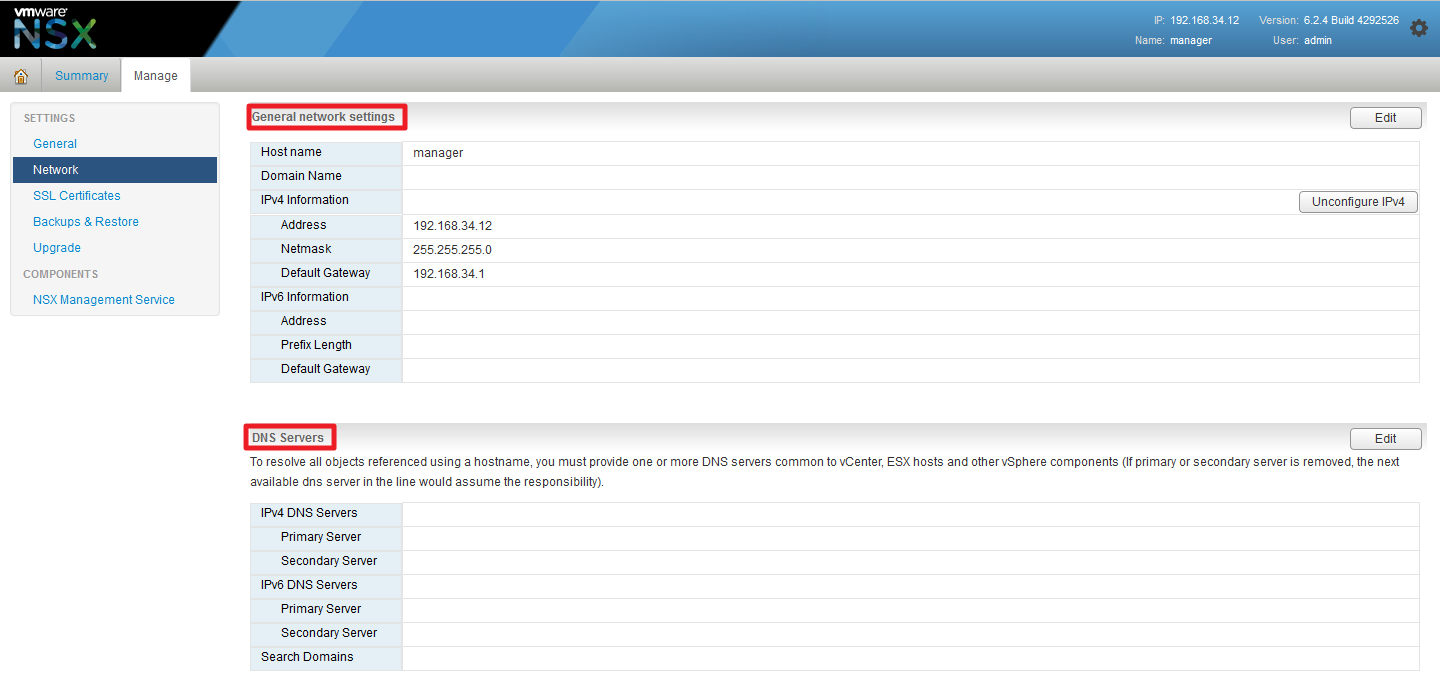


图17

1. 在NSX Manager中生成SSL证书（点击Generate CSR，会自动生成证书），如图18所示。

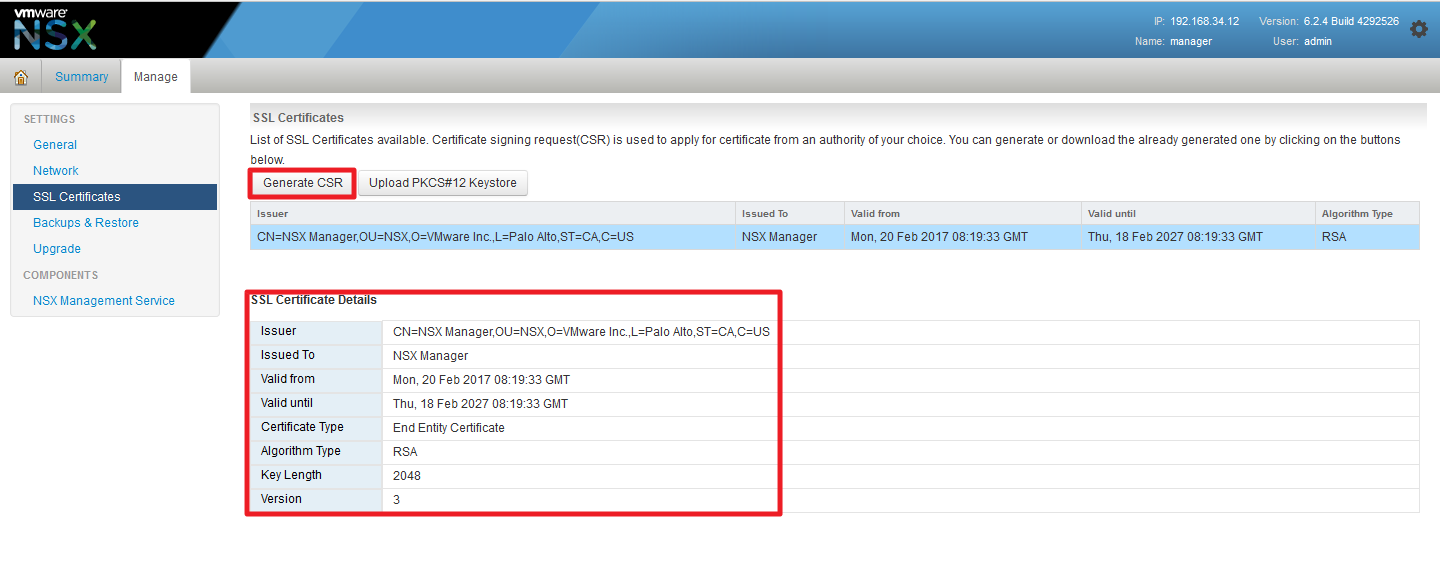


图18

### 将NSX Manager注册到vCenter

由于NSX Manager必须与vCenter进行关联，因此在安装完成NSX Manager之后，必须将其注册到vCenter，具体步骤如下：

1. 继续之前的步骤，点击“NSX Management Service”选项，点击vCenter Server编辑按钮，输入vCenter相关信息——IP地址、用户名、密码，点击“OK”按钮，如图19所示。

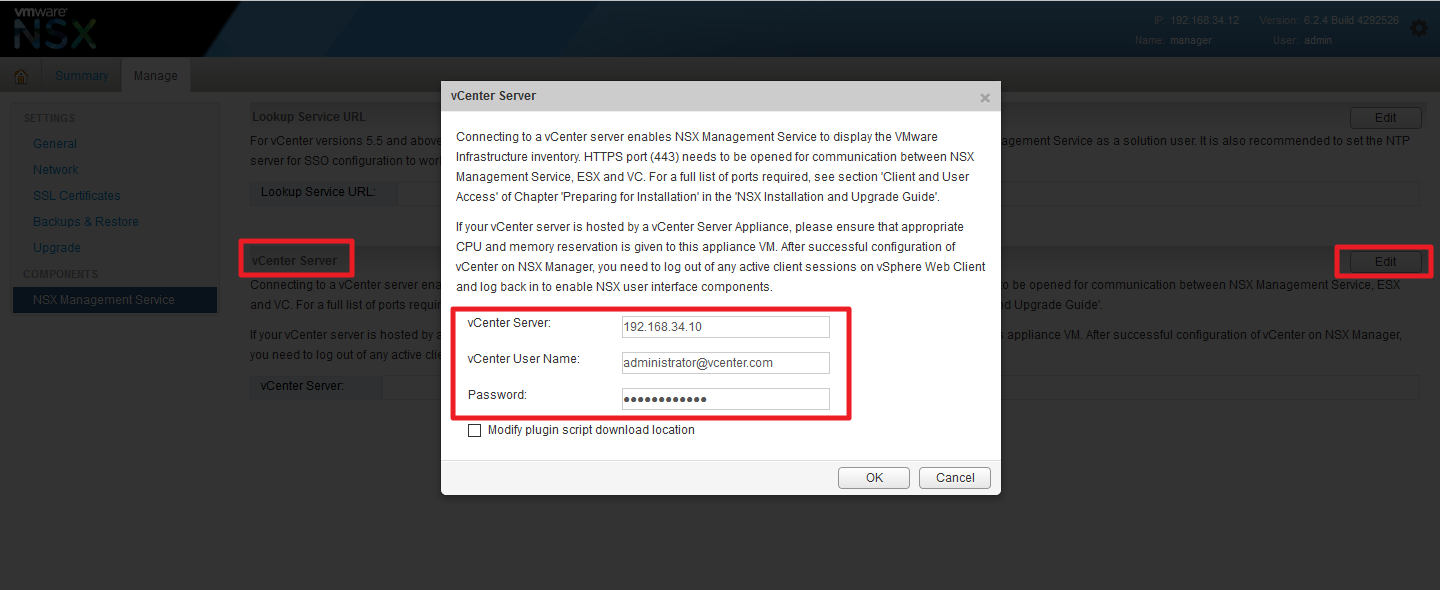


图19

1. 确认证书，并点击“Yes”按钮，如图20所示。

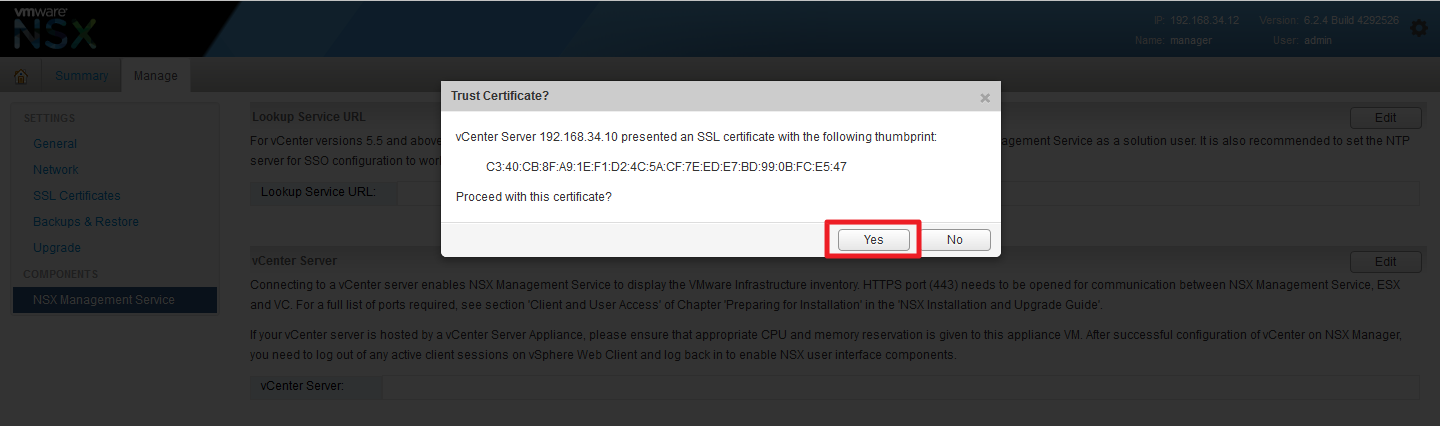


图20

1. 返回到vCenter Server界面，确认NSX Manager与vCenter是Connected（已连接）状态，如图21所示。

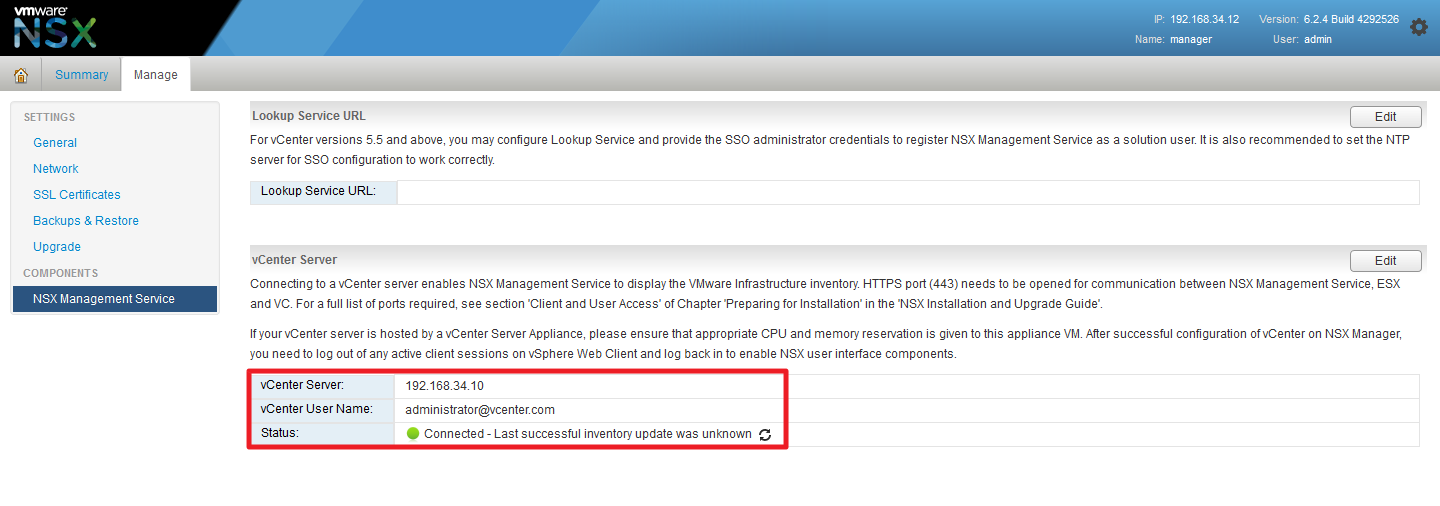


图21

1. 为了确认NSX Manager已经和vCenter关联成功，请重新登录一次vSphere Web Client，在主界面中可以看到“网络和安全”图标已存在，如图22所示。

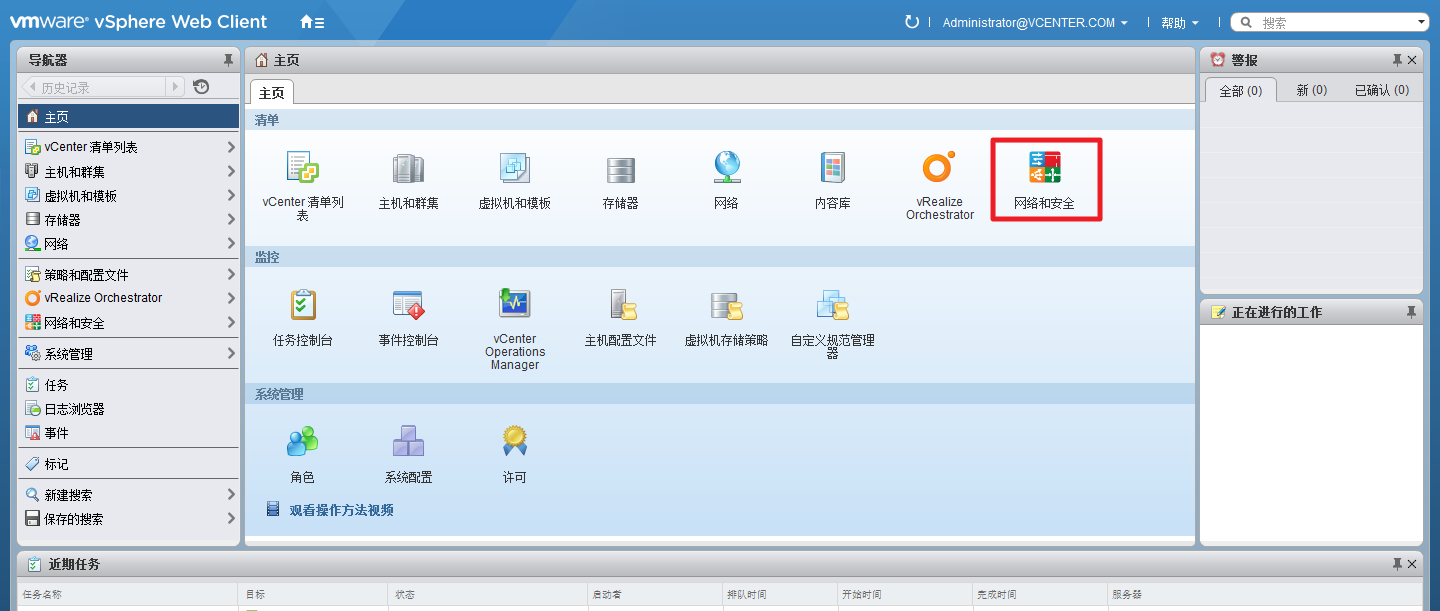


图22

### 备份NSX Manager

配置和部署过程中，可以自主选择是否备份NSX Manager，具体步骤如下：

1. 在NSX的Manager选项卡中，点击“Backup&Restore”选项，如图23所示。



图23

1. 选择备份服务器的地址、传输方式、端口、用户名、密码等，即可完成与备份服务器的同步，如图24所示。

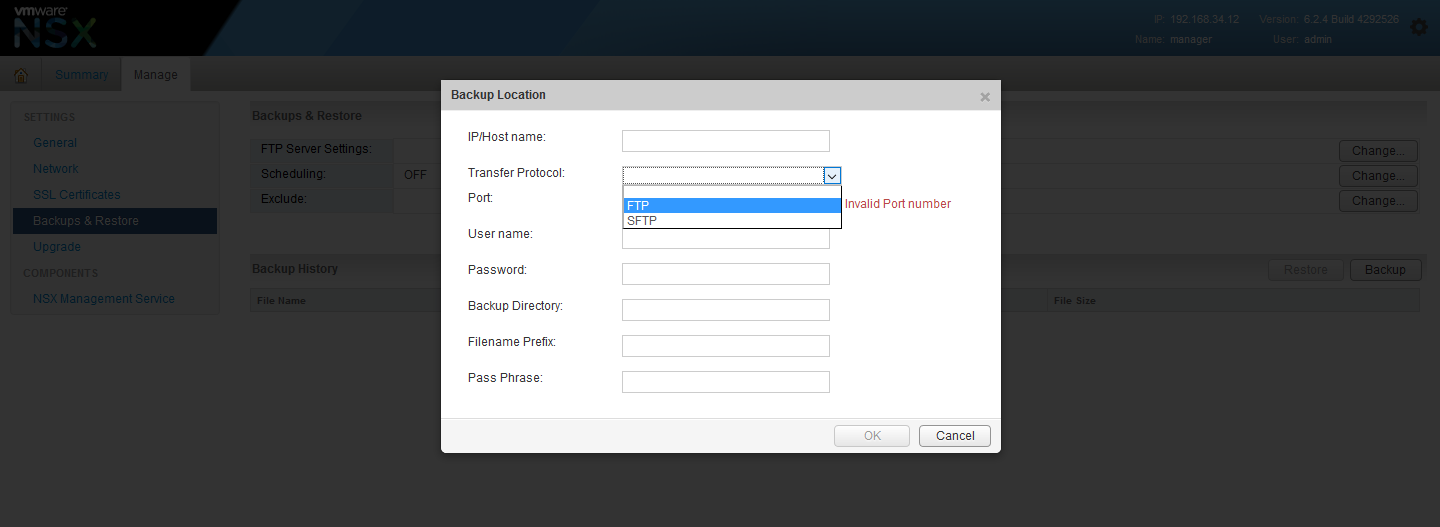


图24

## NSX Controller控制平面部署

只有当NSX Manager安装完成后，才可以安装和部署NSX的控制平面组件——NSX Controller集群。NSX Controller是负责VMware NSX最终提供的各种服务的控制平台，非常重要，一般将其部署为集群模式，保证其冗余和负载均衡。

NSX Controller部署流程需要遵循以下步骤：

* 确认NSX Manager安装完成。
* 确认NSX Manager与vCenter集成完毕。
* 使用vSphere Web Client登录到vCenter，进行NSX Controller的部署。

### NSX Controller安装部署

1. 使用vSphere Web Client登录到vCenter，点击“网络和安全”选项，左侧工具栏中点击“安装”选项，用于安装和部署NSX Controller。在NSX Controller节点处点击“+”，开始创建NSX Controller节点，如图25所示。

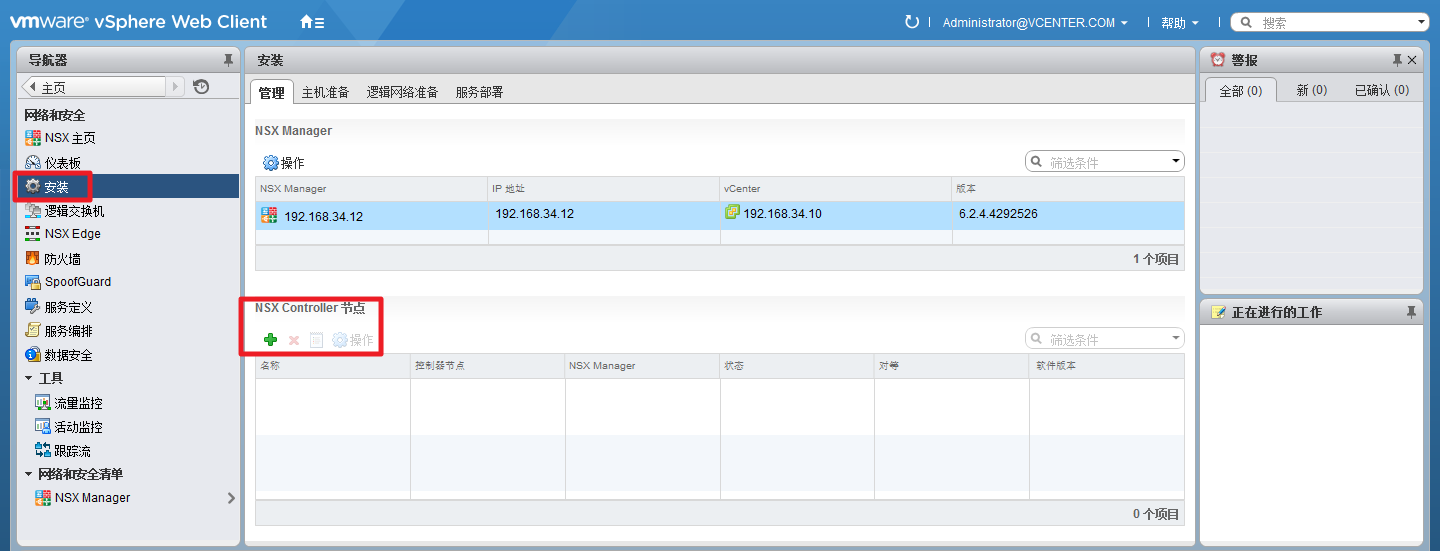


图25

1. 在添加控制器界面输入和选择NSX Controller的名称、NSX Manager、数据中心、集群、数据存储、主机、文件夹、“已连接到”点击选择可用网络、IP池选择并创建可用IP范围、密码和确认密码，如图26、27所示。

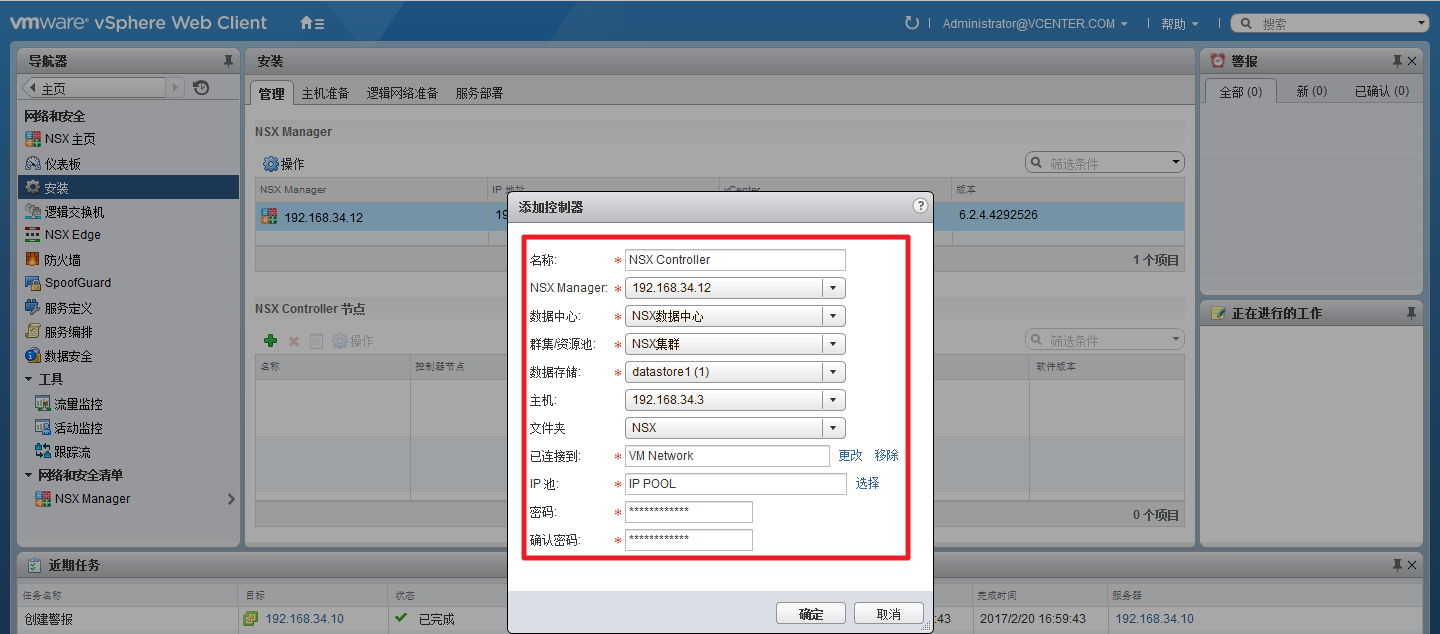


图26



图27

1. 创建完一个Controller节点后，可以添加另外的Controller节点，添加其他节点时，不需要设置用户名和密码，因为创建第一个节点时设置的用户名和密码是集群的用户名和密码，会同步到其他节点。Controller节点配置完成后，如果状态显示为，那么节点部署就成功了，如图28所示。

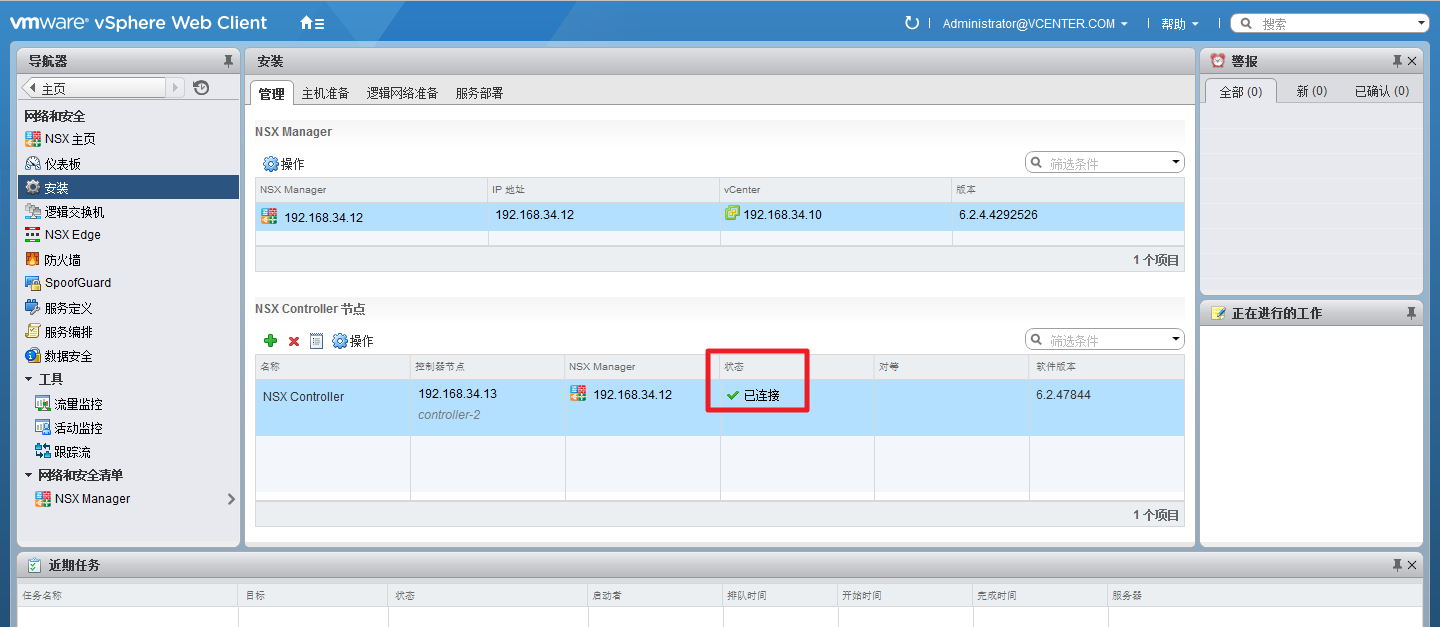


图28

## VIB内核组件部署

vSphere Installation Bundles（VIBs）安装在ESXi主机的Hypervisor之上，用以开启VXLAN、分布式路由器、分布式防火功能，并与NSX Controller集群进行信令信息的交互。

### 添加许可证

安装VIB内核组件之前，首先需要添加符合NSX for vSphere解决方案的许可证，具体步骤如下：

1. 使用vSphere Web Client登录到vCenter主页，点击“许可”选项，如图29所示：

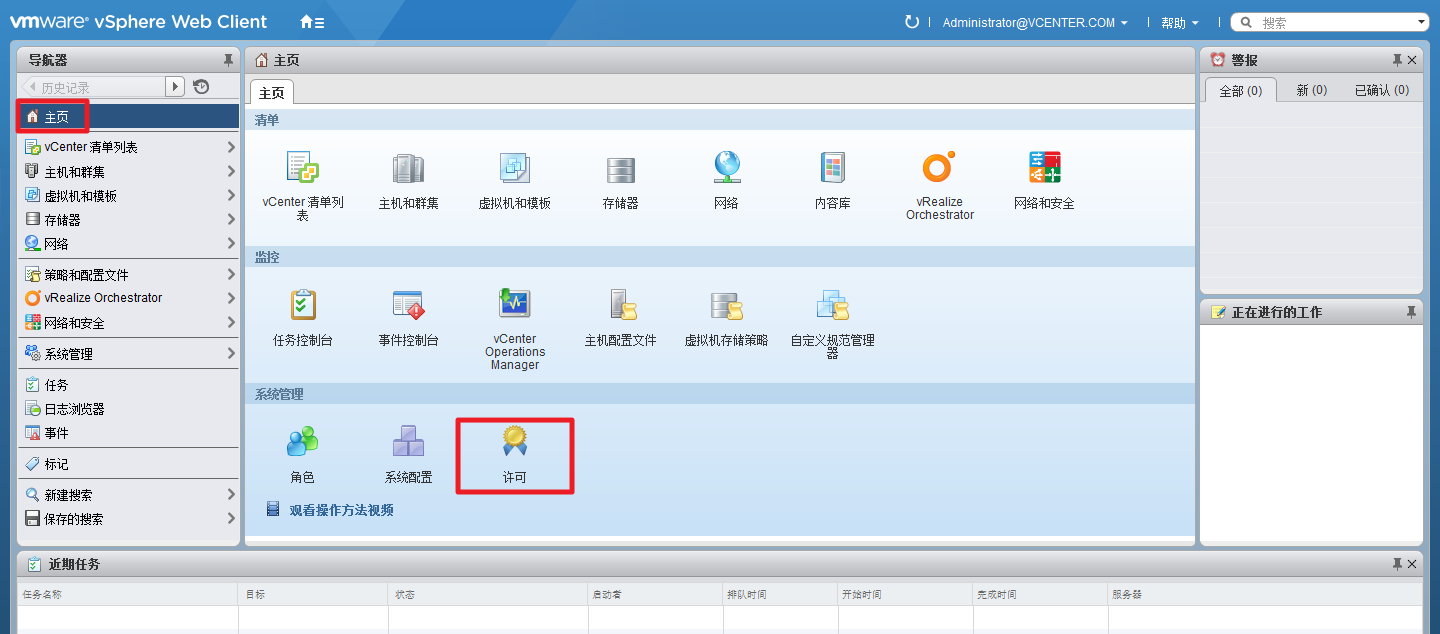


图29

1. 选择“许可证”选项卡，点击“+”按钮，在新许可证界面输入正确的许可证，点击“下一步”按钮直至完成，如图30所示：

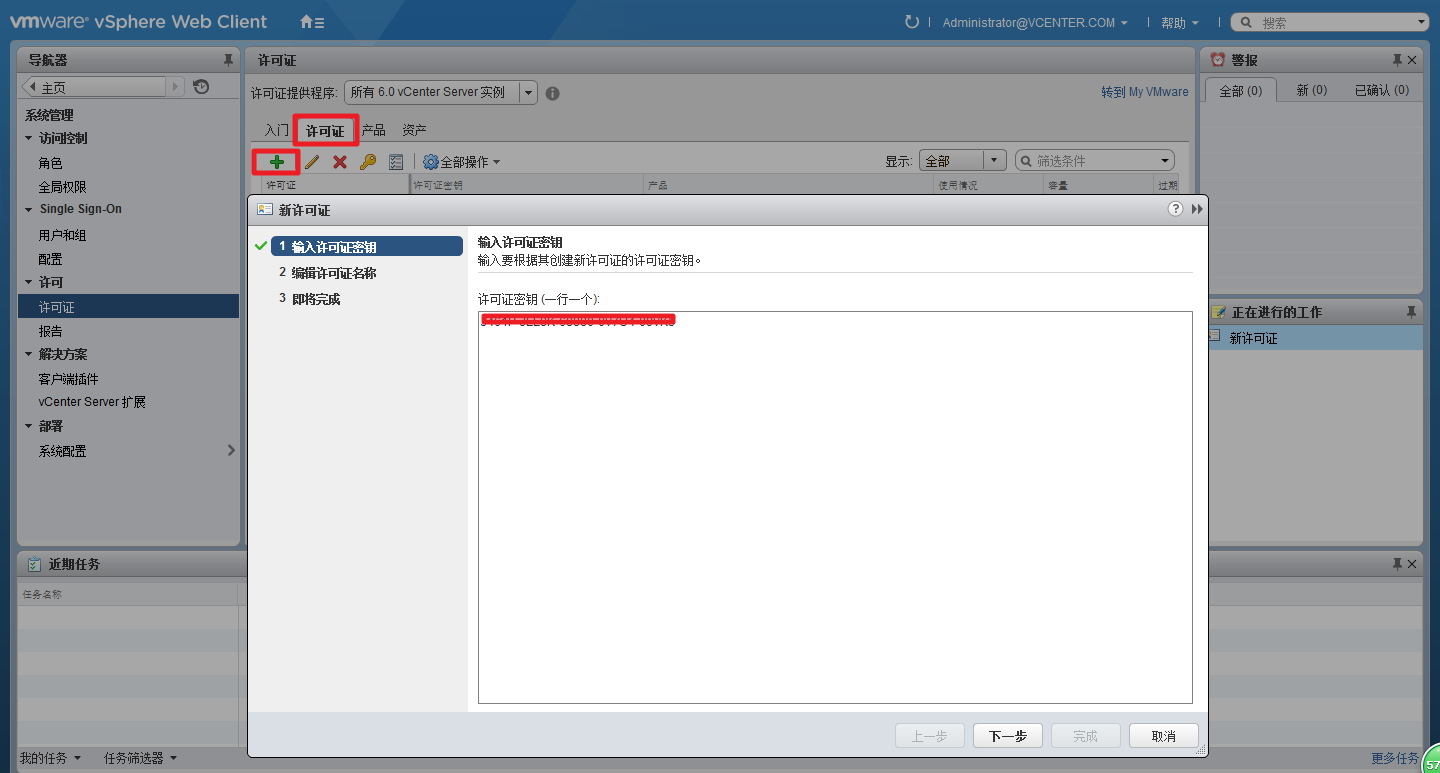


图30

1. 切换到“资产”选项卡，点击“解决方案”选项，选中资产“NSX for vSphere”后点击“分配许可证”按钮，如图31所示：

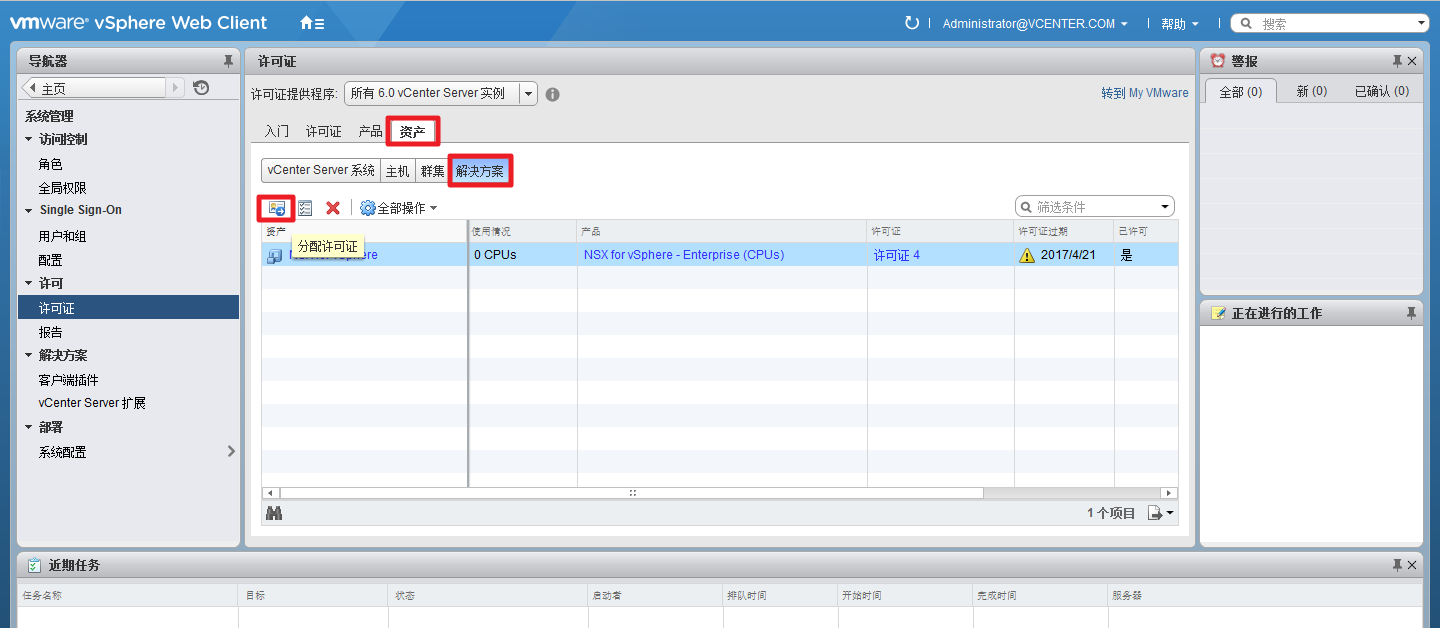


图31

1. 选中之前添加的许可证，点击“确定”按钮，如图32所示：

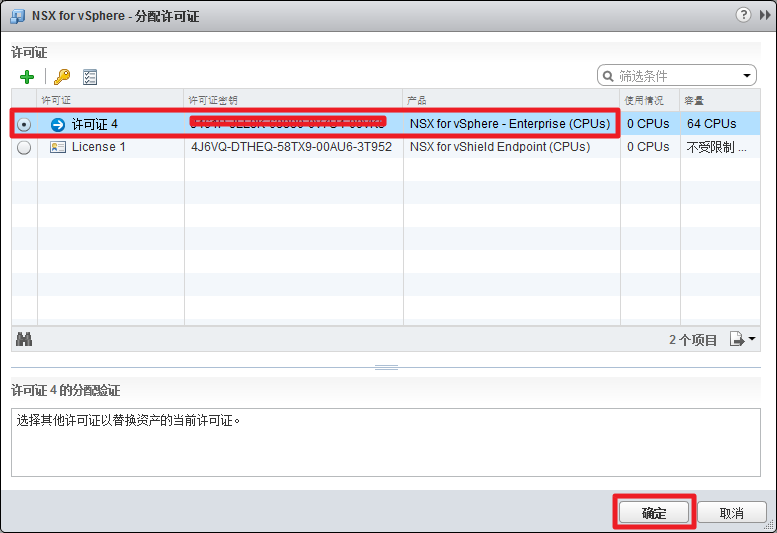


图32

### ESXi主机安装VIB内核组件

添加完成许可证后，即可进行VIB内核组件的安装，具体步骤如下：

1. 使用vSphere Web Client登录到vCenter主页，点击“网络和安全”选项，左侧工具栏中点击“安装”选项，切换到“主机准备”选项卡，点击集群上面的“安装”选项进行VIB内核组件安装，如图33所示：

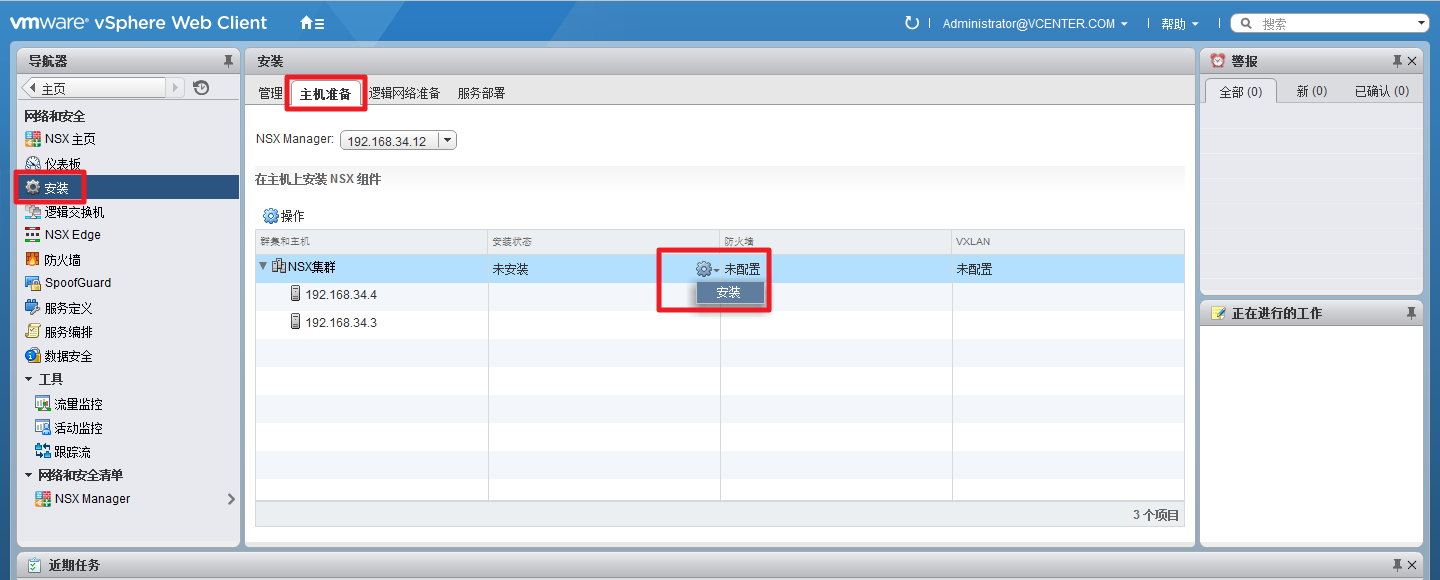


图33

1. 耐心等待安装完成后，安装状态显示为正常，如图34所示：

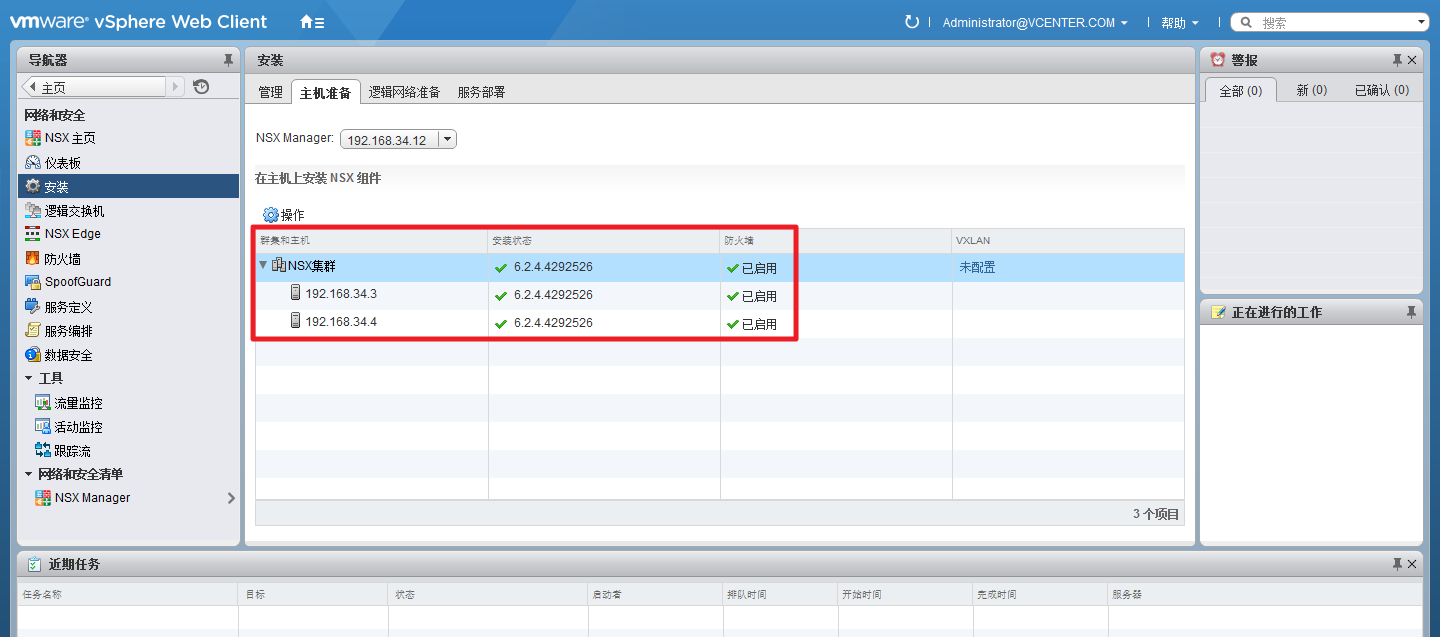


图34

# vSeccenter-N部署和应用

## 部署vSeccenter-N

vSeccenter-N是天融信公司针对VMware NSX提供的一套集访问控制、流量监控、入侵防御、基于流的病毒防护和安全迁移感知等功能于一体的云安全防护系统，通常是以打包OVA模板方式提供的，并允许用户使用vSphere Web Client将vSeccenter-N以虚拟机的形式进行安装部署。要获取这个文件，请联系北京天融信公司相关人员提供。

安装vSeccenter-N虚拟机的具体步骤如下：

1. 通过vSphere Web Client登录到vCenter主页，按照常规部署OVA模板的方式进行安装，右键单击需要部署的ESXi主机，选择从OVF模板进行部署，如图35所示：

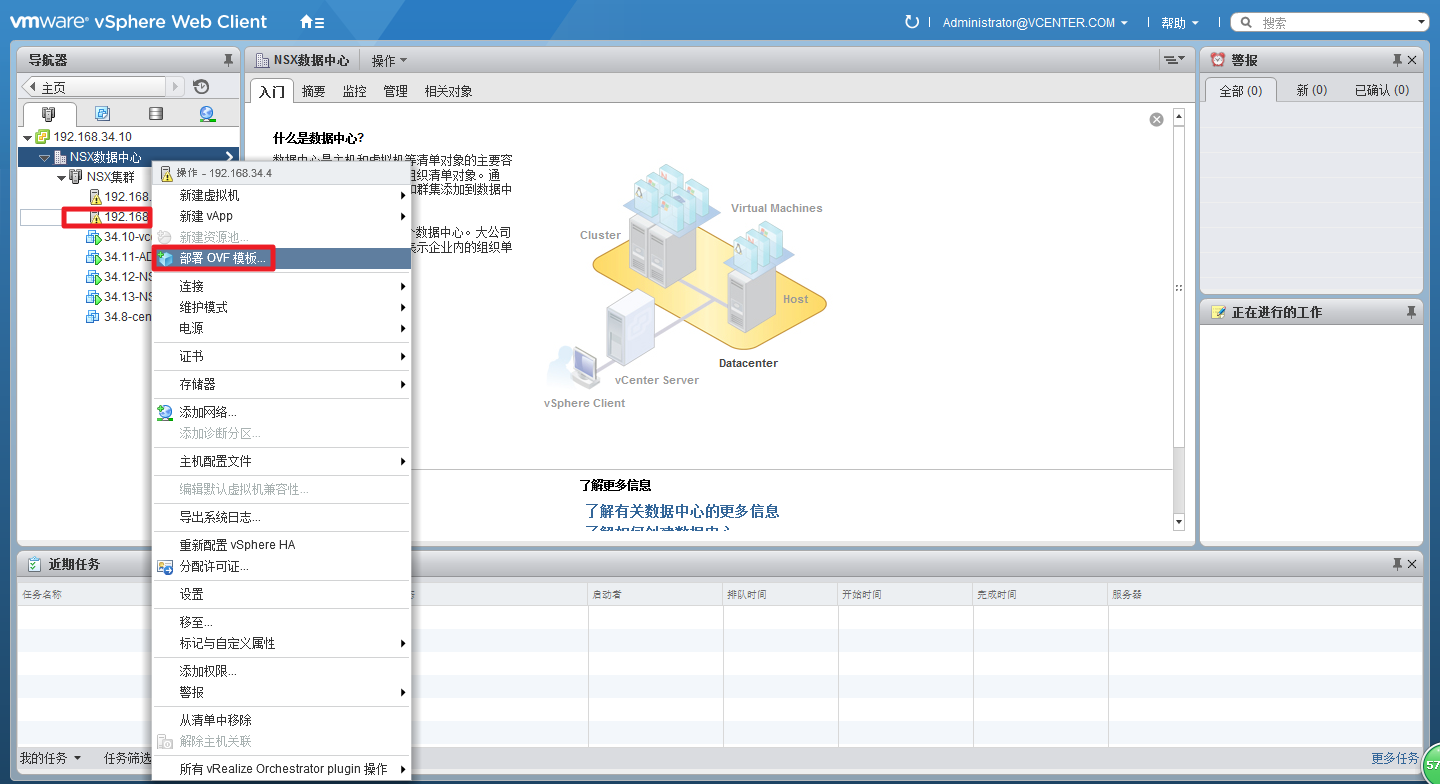


图35

1. 从本地文件夹选择vSeccenter-N的OVA文件，并点击“下一步”按钮，如图36所示。

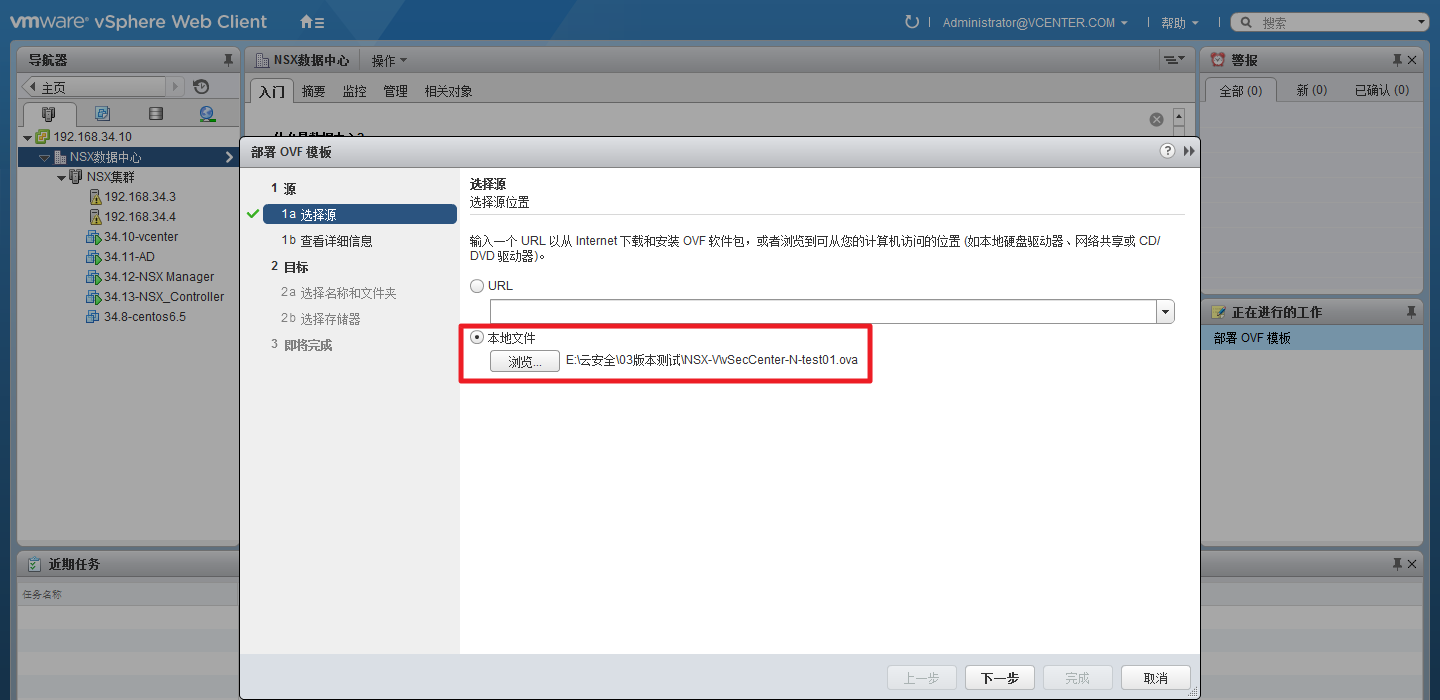


图36

1. 检查OVA模板的详细信息，并单击“下一步”按钮，如图37所示。

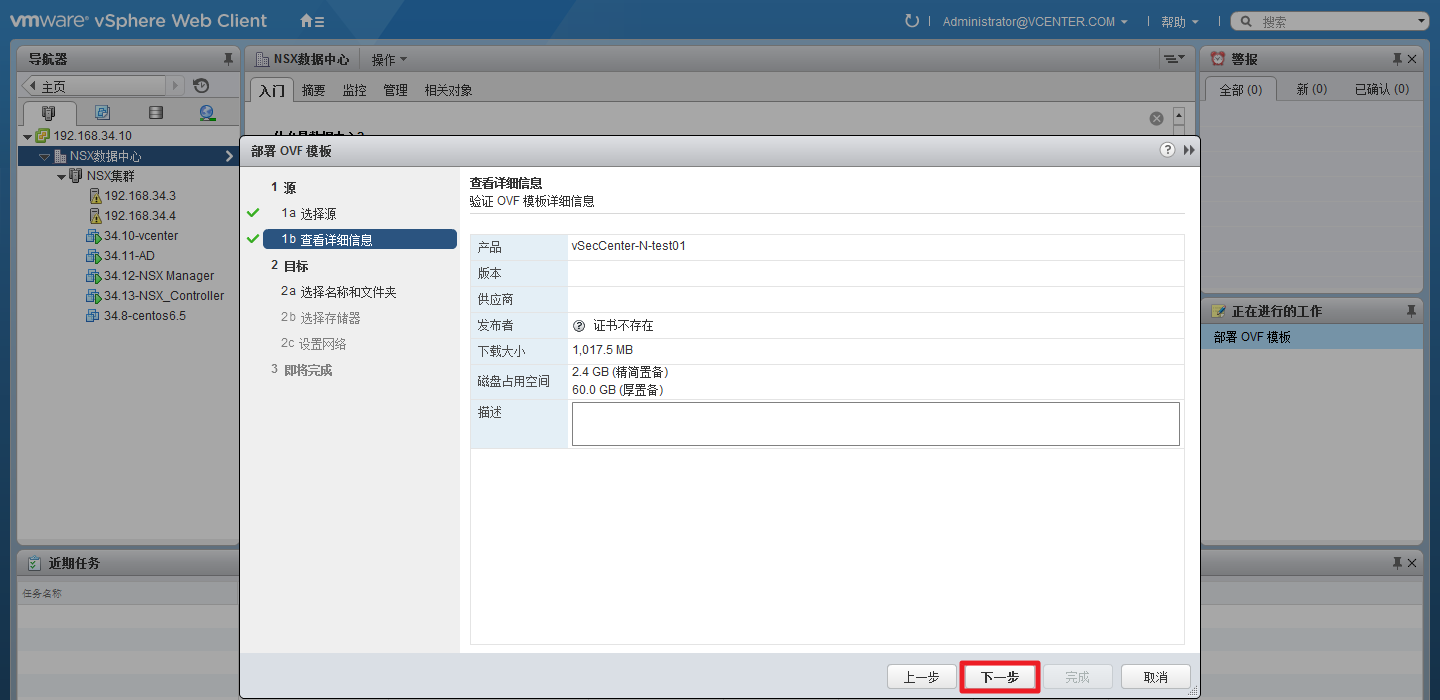


图37

1. 选择vSeccenter-N的安装位置，然后单击“下一步”按钮，如图38所示。

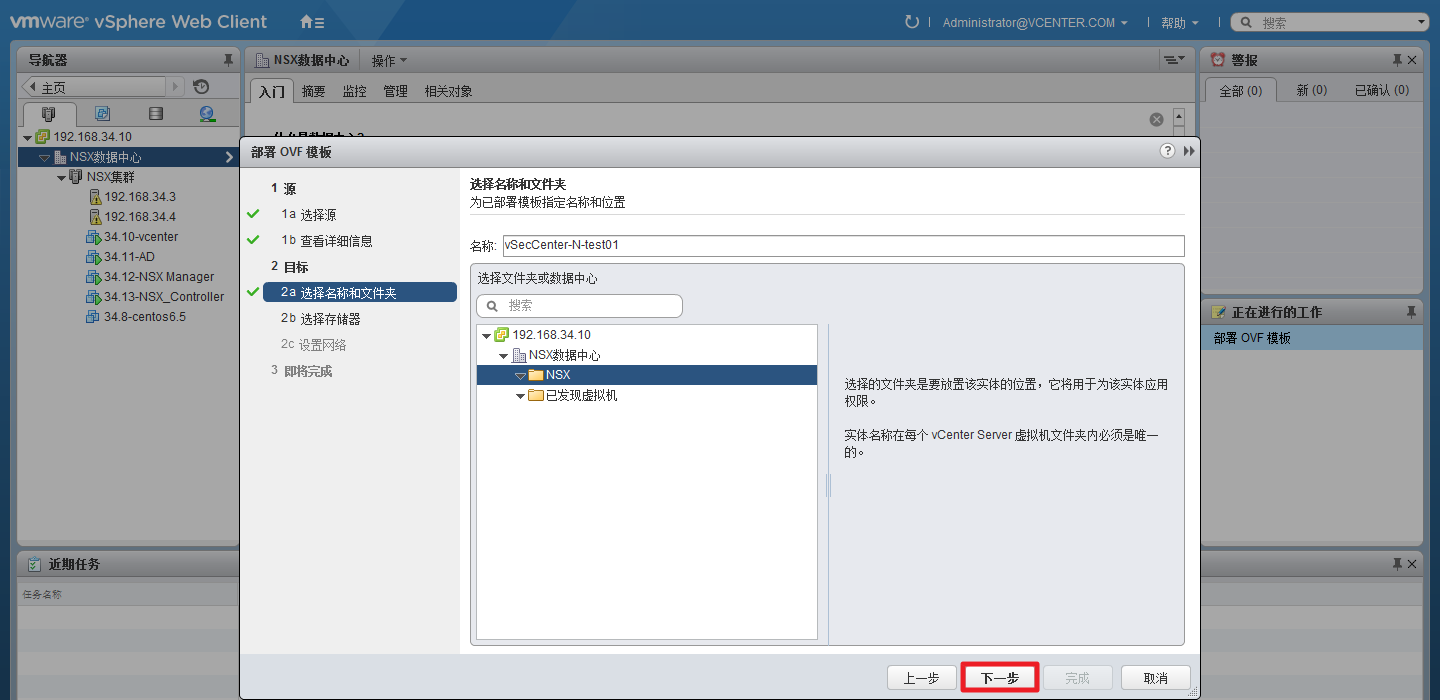


图38

1. 选择磁盘部署方式，选择磁盘位置，点击“下一步”按钮，如图39所示。

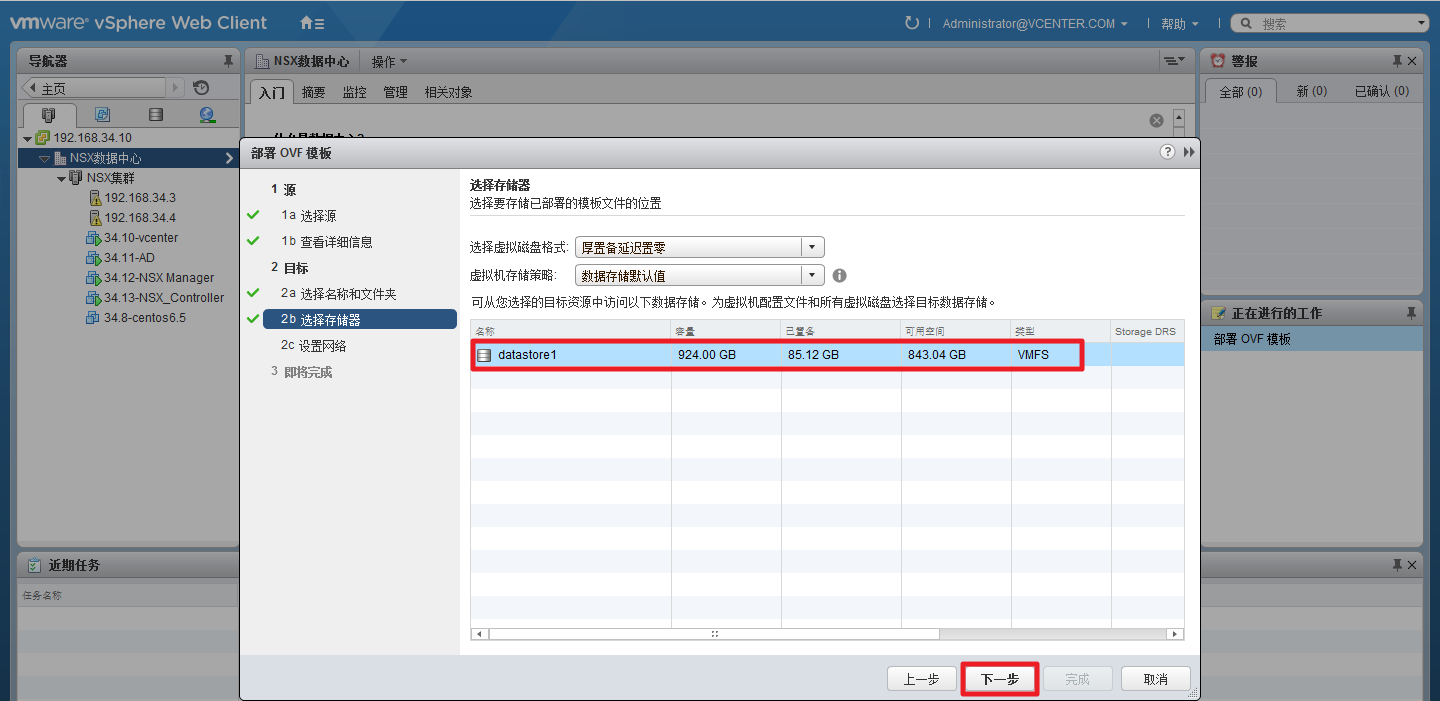


图39

1. 设置vSeccenter-N的网络，单击“下一步”按钮，如图40所示。

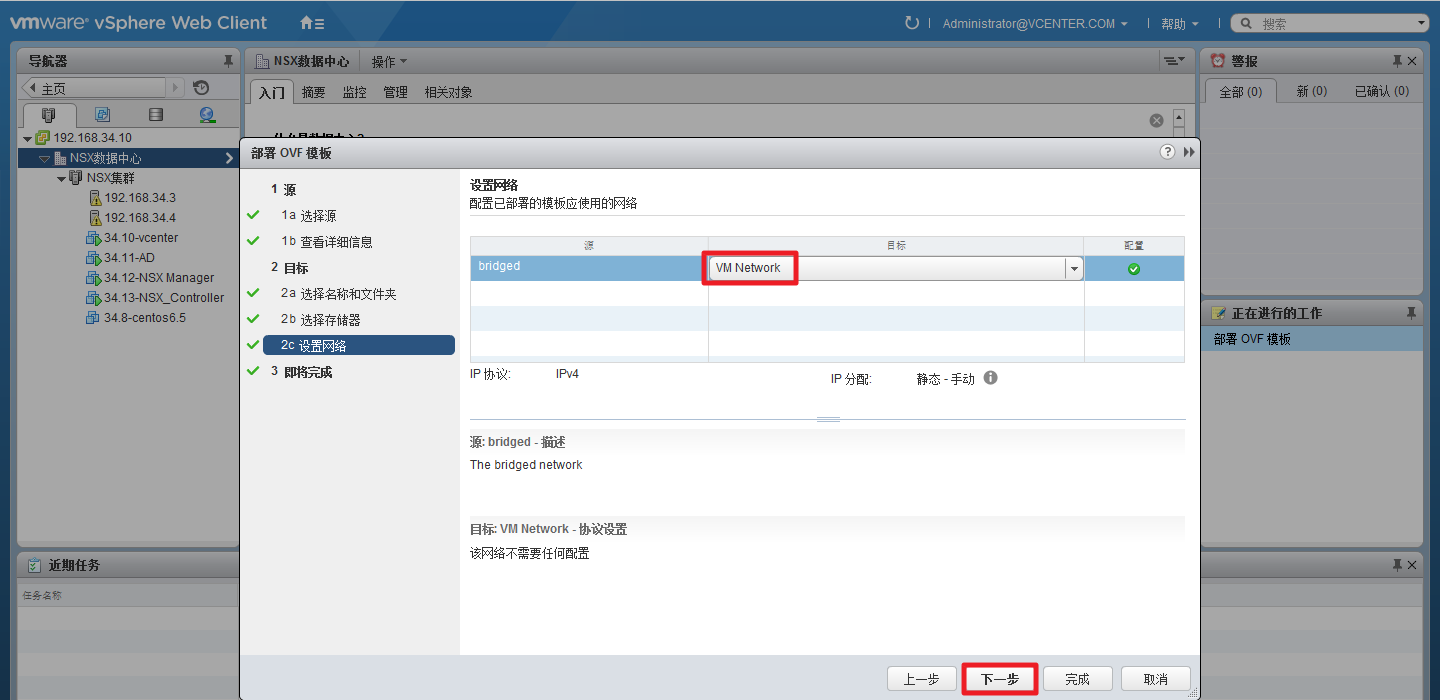


图40

1. 勾选“部署后打开电源”，点击“完成”按钮，至此vSeccenter-N安装完成，等待加电后并初始化完成，如图41所示。

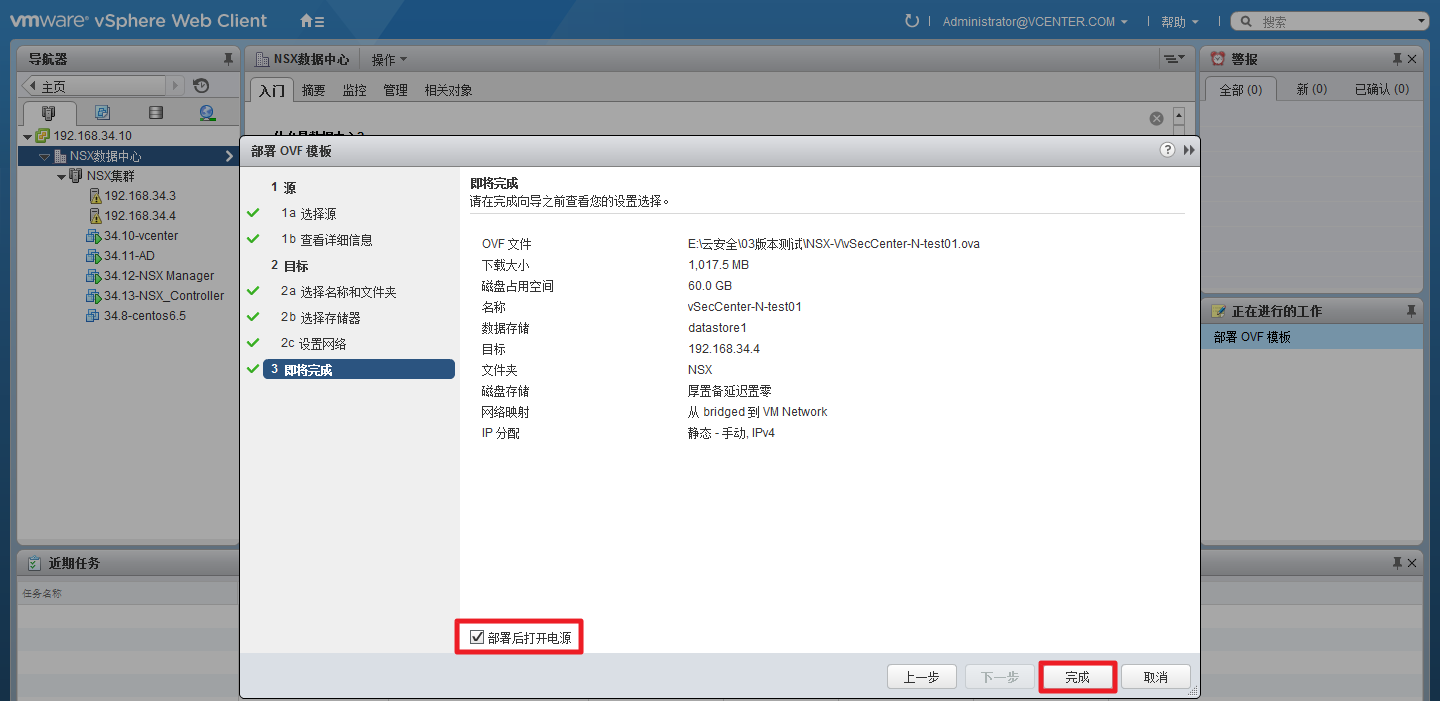


图41

## 配置vSeccenter-N

部署完成vSeccenter-N虚拟机后需要对其进行基础配置，包括修改服务器IP地址、开启服务自启动、开启主服务，具体步骤如下：

1. 打开vSeccenter-N虚拟机控制台或者使用工具SSH连接后台，登录后使用vi /etc/sysconfig/network-scripts/ifcfg-ens33对服务器IP地址进行修改和保存，如图42所示。

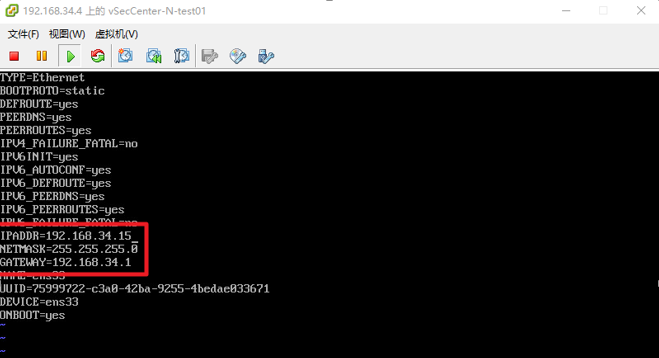


图42

1. 修改和保存服务器IP地址后，需要手动重启网卡服务，如图43所示。



图43

1. 后台使用vseccenter.sh autostart配置服务自启动，使用vseccenter.sh start启动系统主服务，如图44所示。

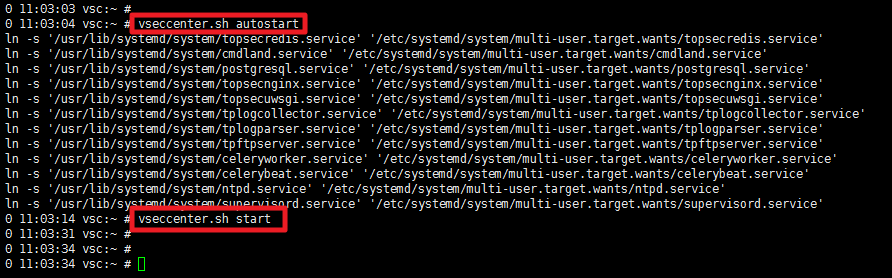


图44

## 登录和注册NSX服务

部署和配置完成vSeccenter-N后，即可登录vSeccenter-N系统进行相关配置，主要包括：添加虚拟化平台和注册NSX服务，具体步骤如下：

1. 打开浏览器，建议使用Firefox或者Chrome，输入vSeccenter-N的IP地址：<https://192.168.34.15:9443>，用户名密码是admin/admin，如图45所示。

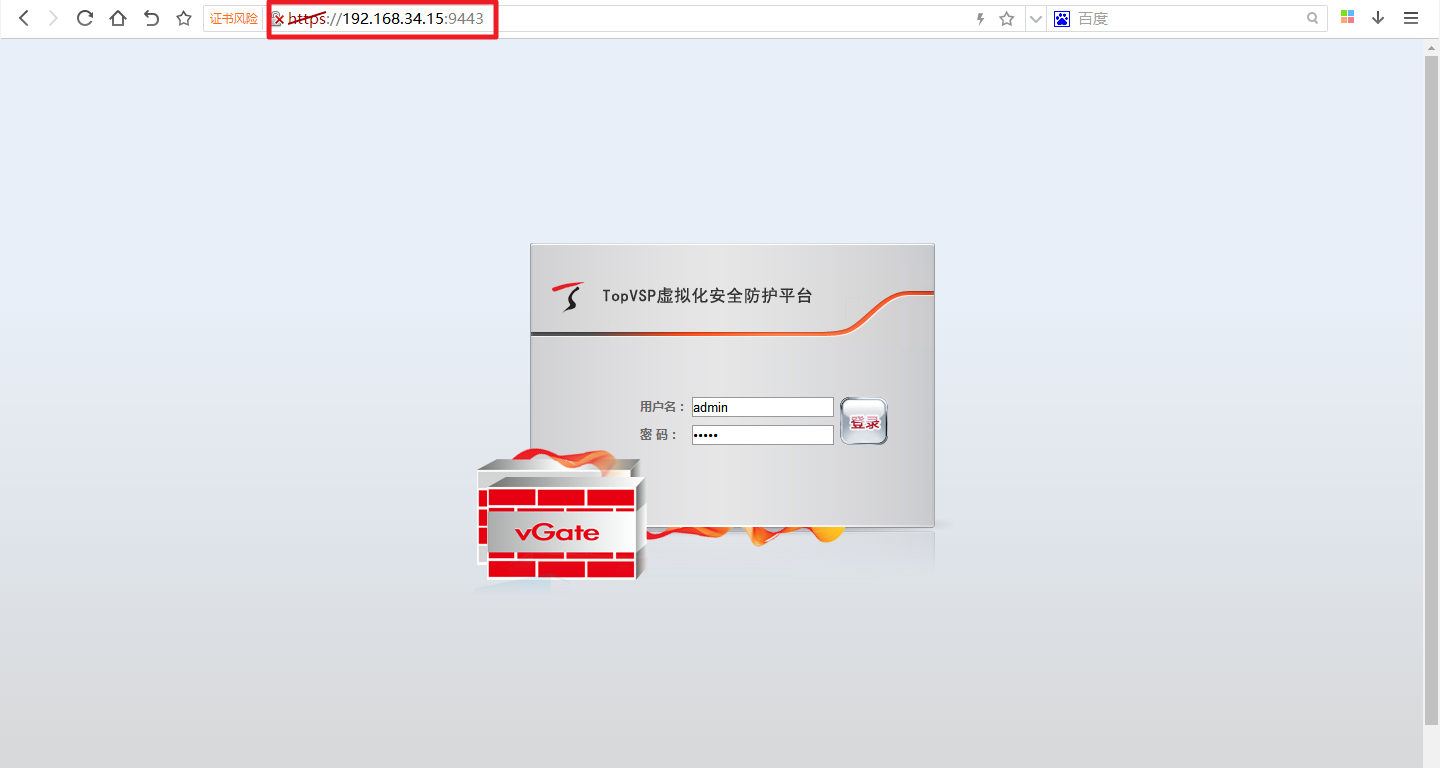


图45

1. 登录成功后，左侧菜单栏中点击**虚拟化平台>>平台管理中心**，然后点击“添加”按钮，在添加虚拟化平台界面分别输入正确的vCenter和NSX Manager平台相关信息，然后点击“保存”按钮，如图46所示。

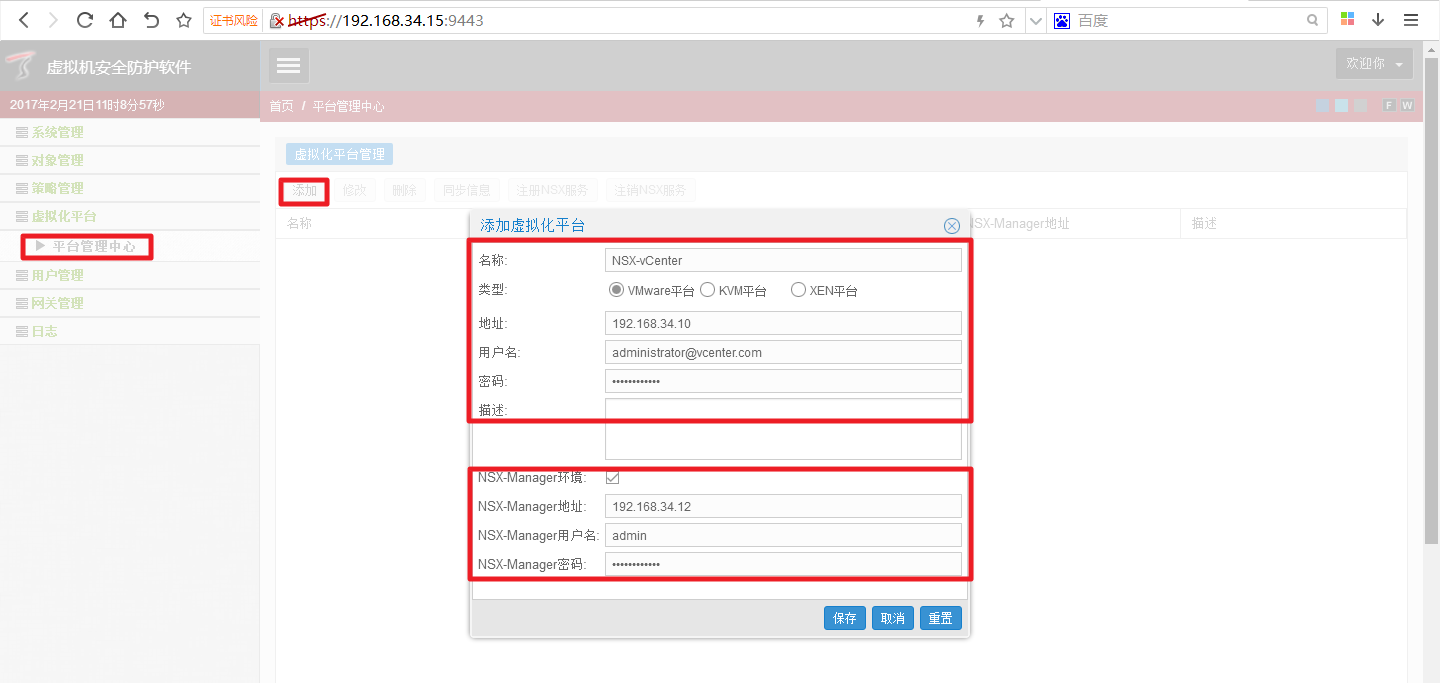


图46

1. 虚拟化平台添加完成后，点击“同步信息”按钮，如图47所示。

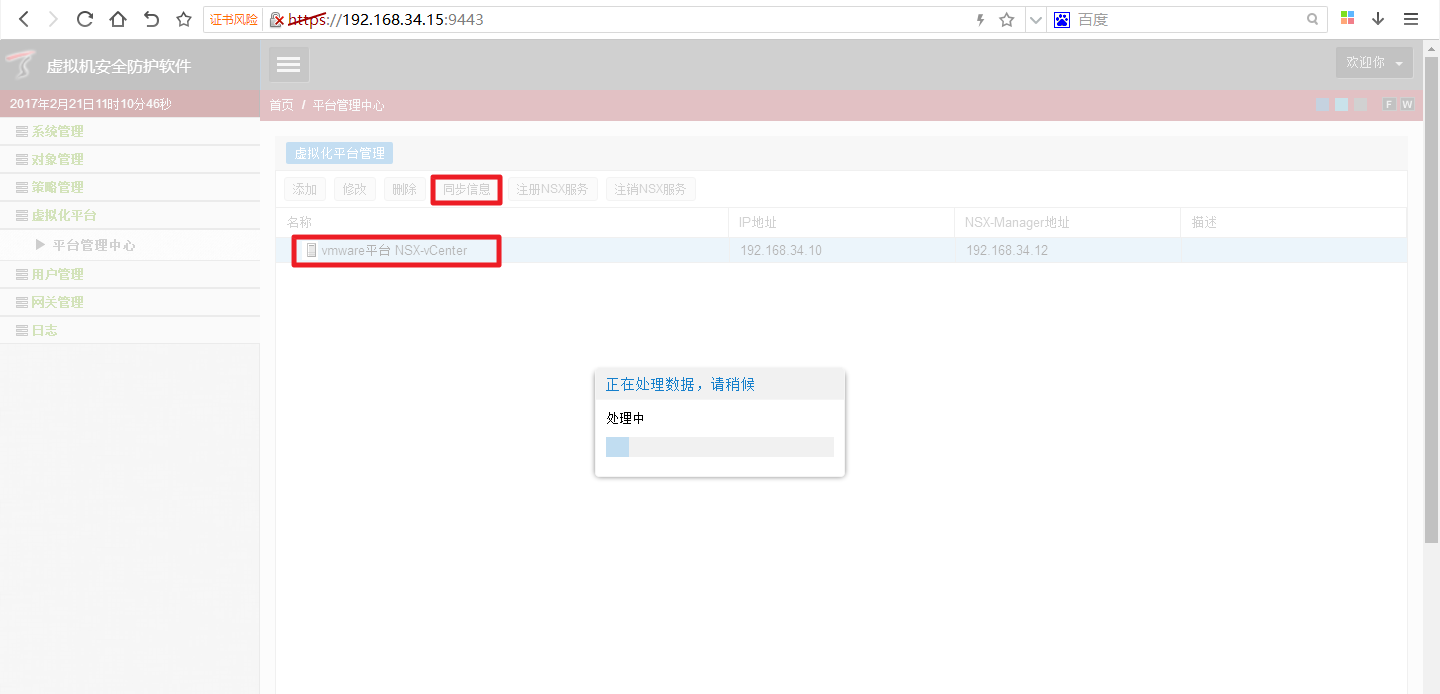


图47

1. 同步信息成功后，点击“注册NSX服务”按钮进行NSX服务注册，如图48所示。

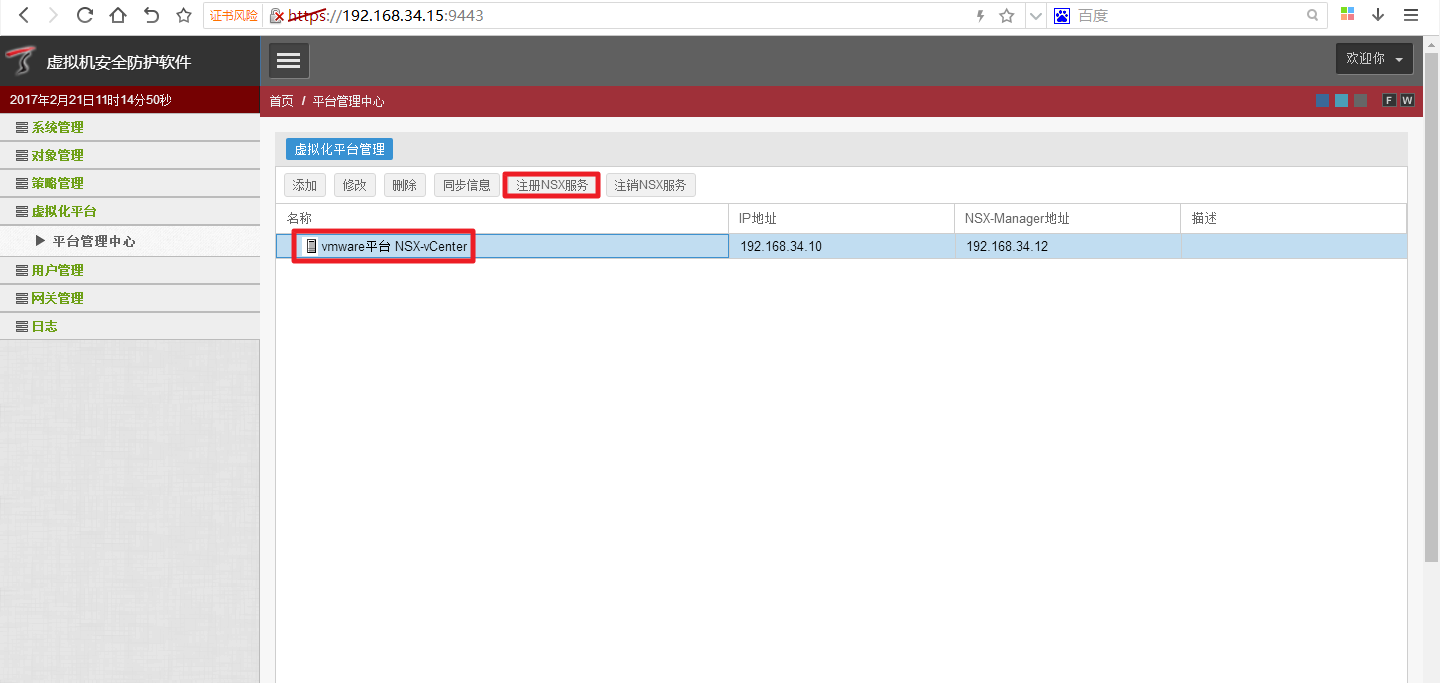


图48

1. 注册NSX服务成功后，通过vSphere Web Client登录到vCenter主页，点击“网络和安全”选项，左侧工具栏中点击“服务定义”选项，切换“服务”选项卡，确认NSX服务注册成功，如图49所示。

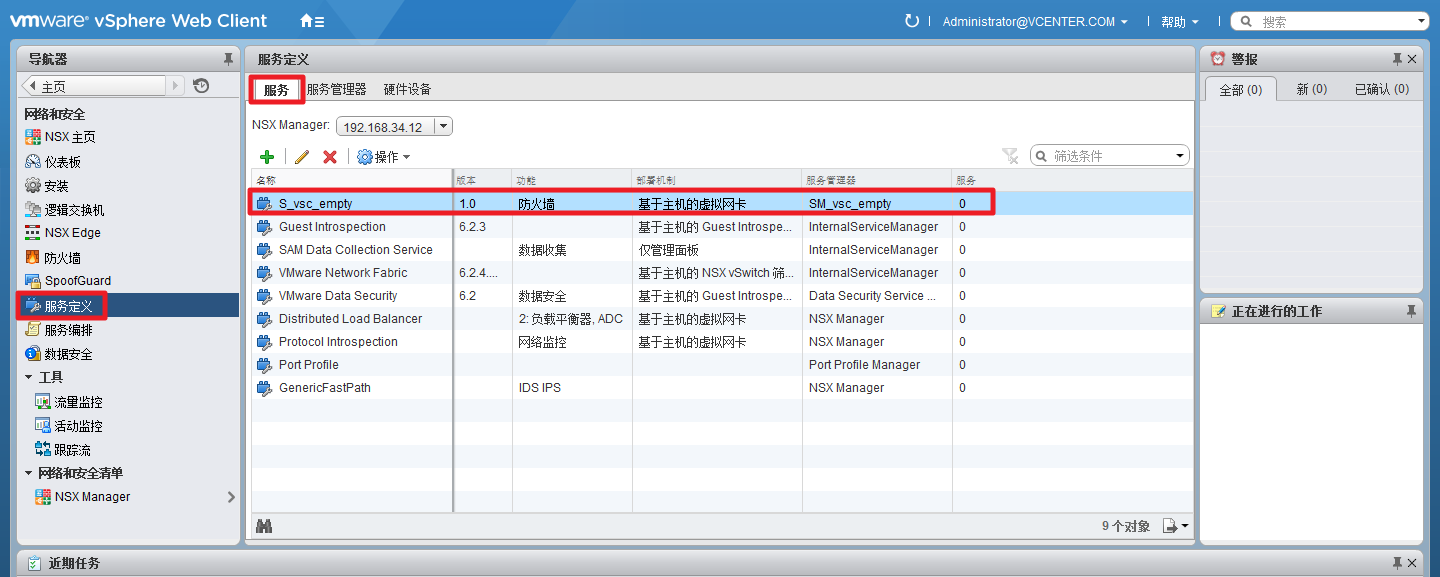


图49

## 部署和配置vFW

注册服务后，接下来进行部署vFW操作，但是目前版本vFW对应的模板还未集成到vSeccenter-N中，所以在此之前需要手动修改一下OVF URL，具体步骤如下：

1. 通过vSphere Web Client登录到vCenter主页，点击“网络和安全”选项，左侧工具栏中点击“服务定义”选项，切换“服务”选项卡，选中之前注册的NSX服务“S\_vsc\_empty”点击操作中的“编辑设置”选项，如图50所示。

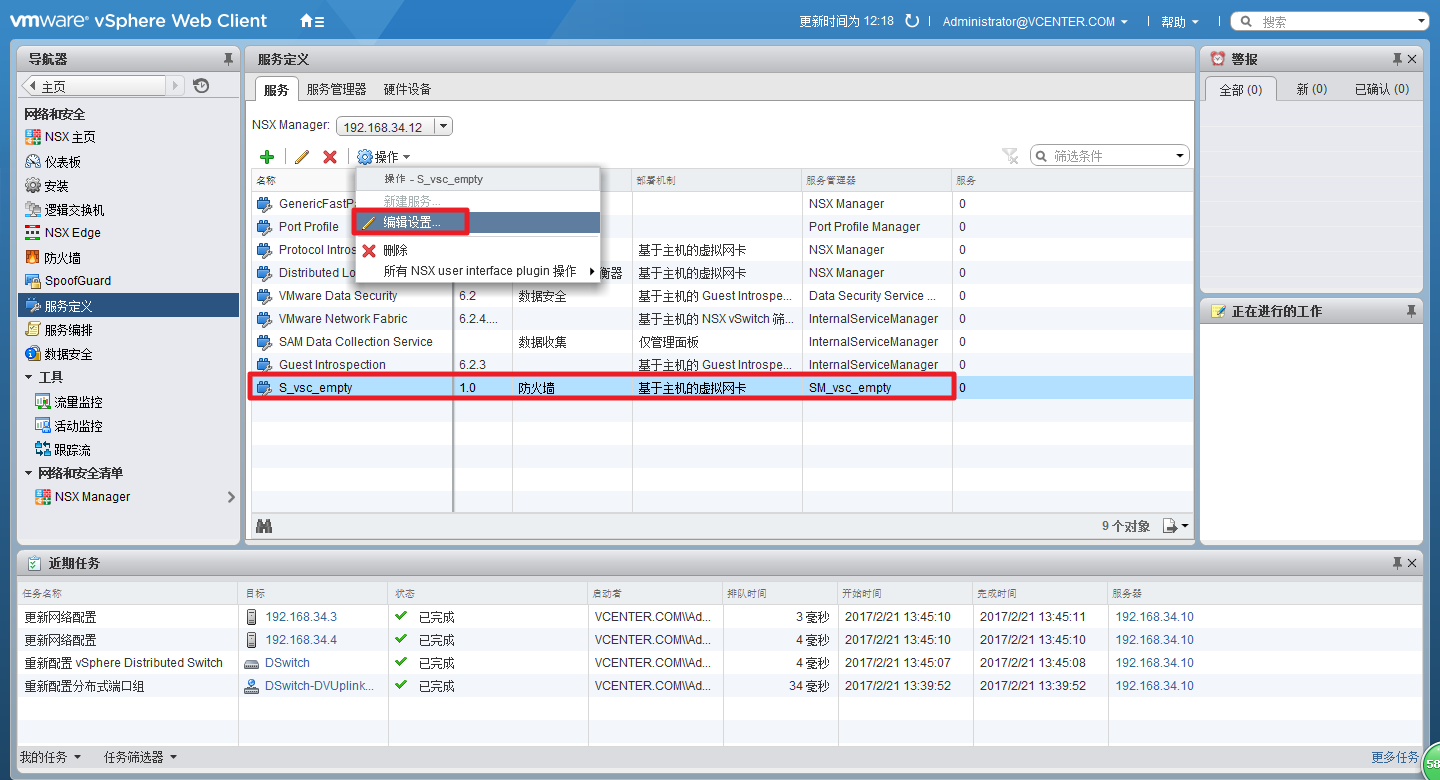


图50

1. 切换“管理”选项卡，再点击“部署”选项，修改OVF URL为可用的URL，例如：<http://172.19.15.155:8080/vNGFW_100G_tmpl.ovf，如图51>所示。

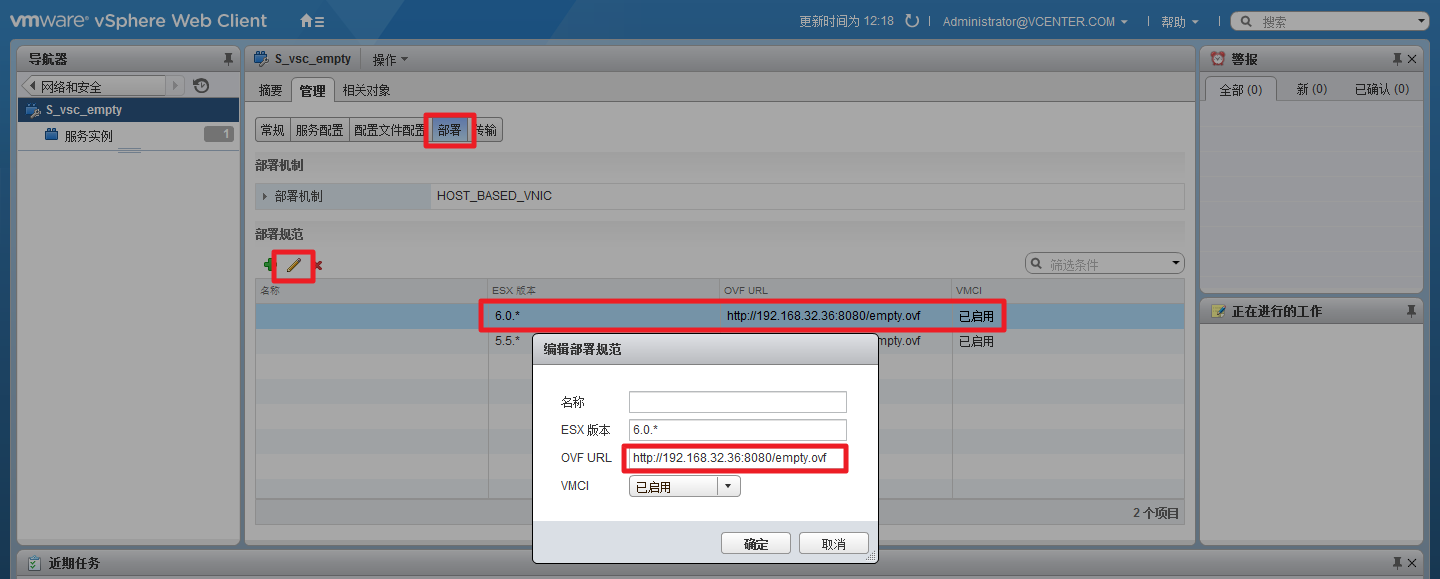


图51

1. 接下来即可进行vFW部署操作了，返回到vCenter主页，点击“网络和安全”选项，左侧工具栏中点击“安装”选项，切换“服务部署”选项卡，点击“+”按钮，在“部署网络和安全服务”界面选择之前注册的NSX服务“S\_vsc\_empty”，点击“下一步”按钮，如图52所示。



图52

1. 选择对应的数据中心和集群，点击“下一步”按钮，如图53所示。

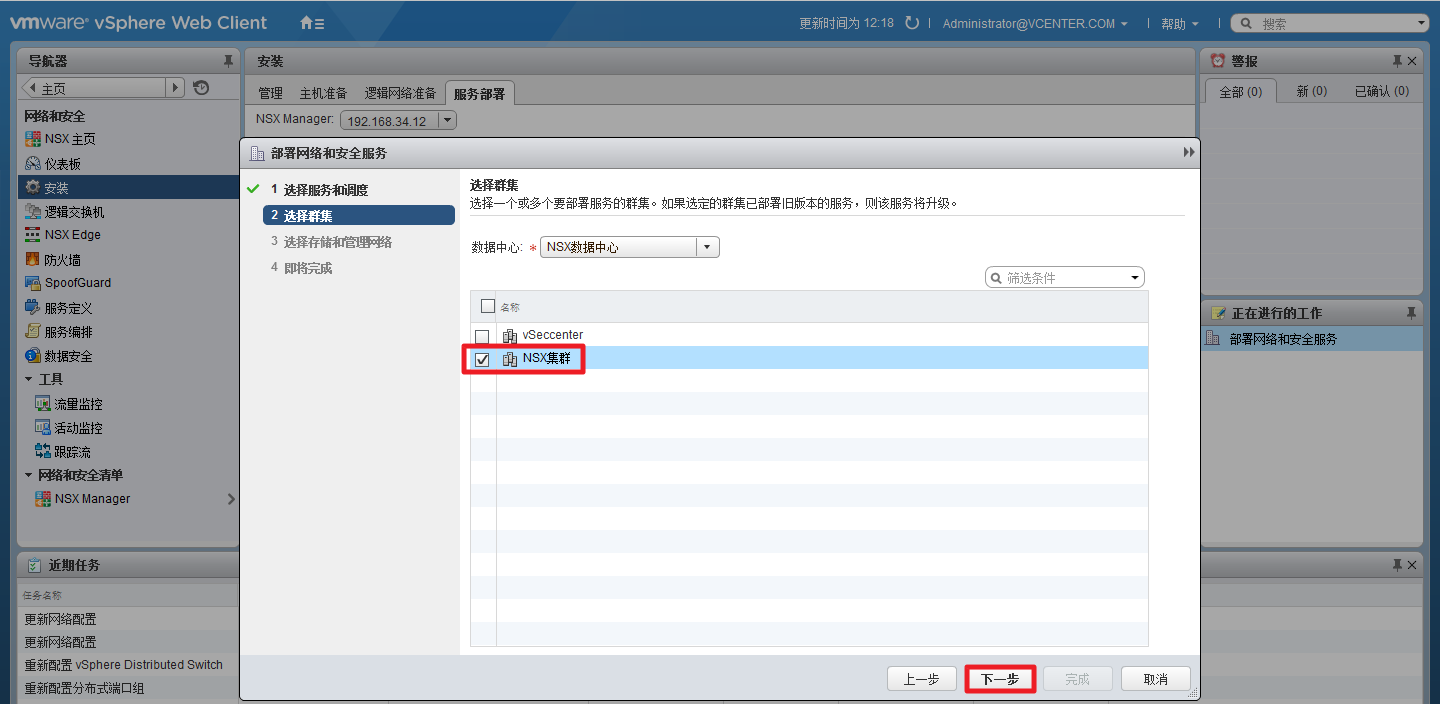


图53

1. 接下来选择数据存储、网络以及更改IP分配模式，这里需要注意两方面：一方面，选择网络时只能选择分布式虚拟交换机，故需要提前进行添加配置；另一方面，如果选择的集群中包含多个ESXi主机，那么数据存储需要选择共享存储，同样需要提前进行添加配置。然后点击“下一步”按钮，如图54所示。

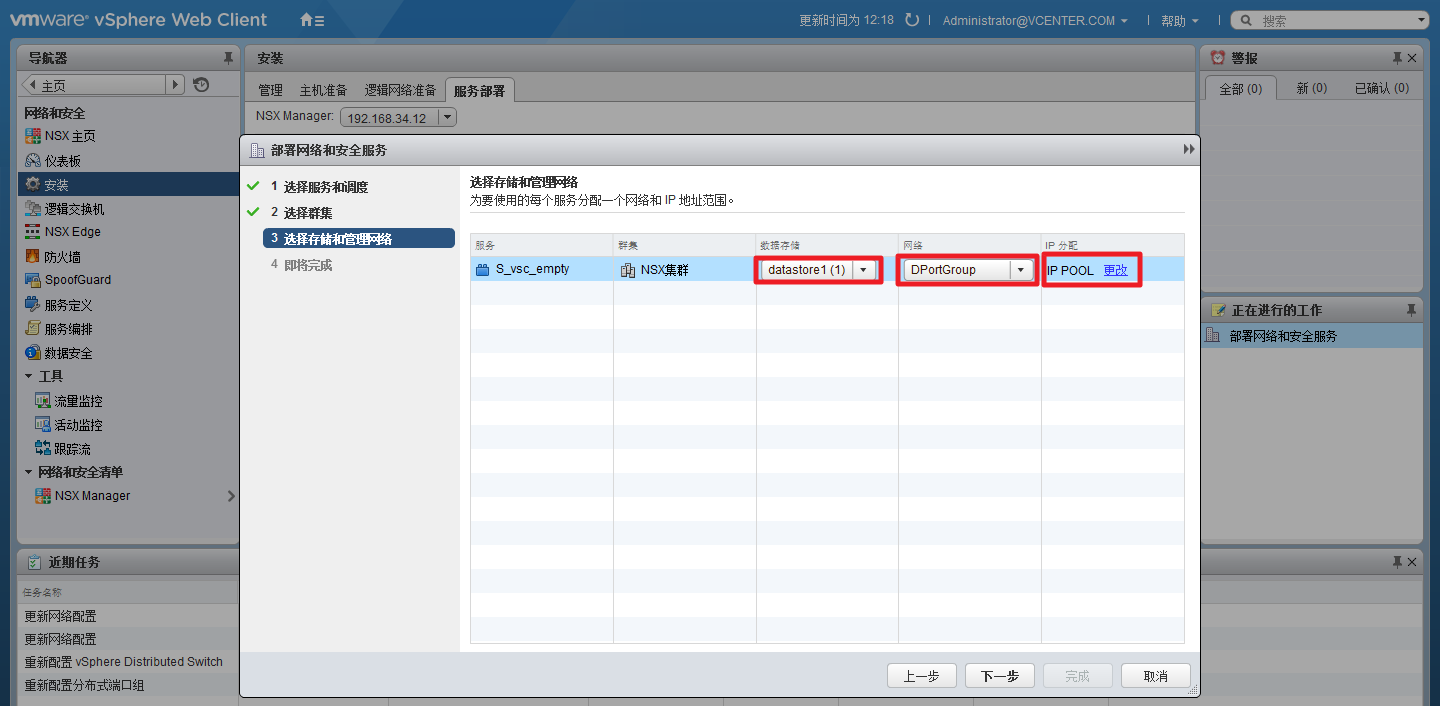


图54

1. 成功加载后请检查设置是否正确无误，点击“完成”按钮，如图55所示。

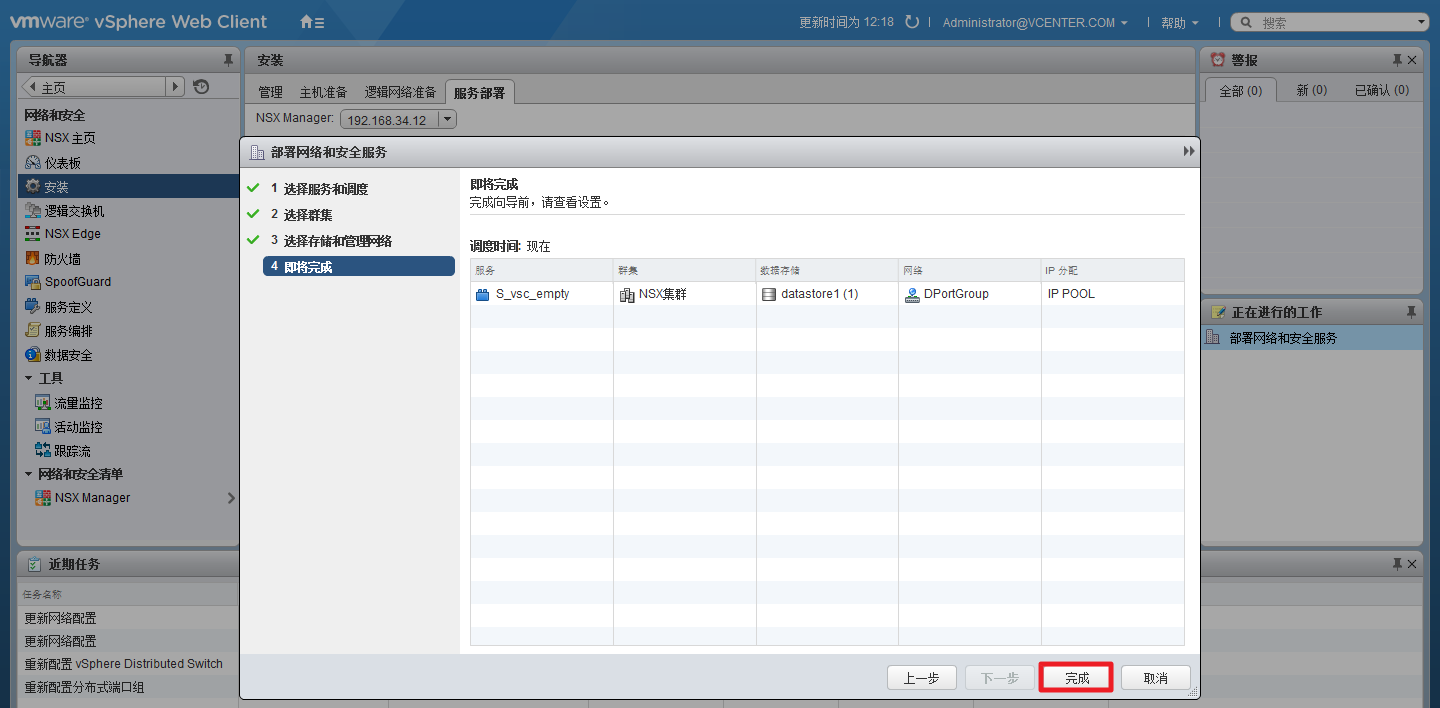


图55

1. 耐心等待部署vFW完成，安装状态显示为成功，如图56所示。

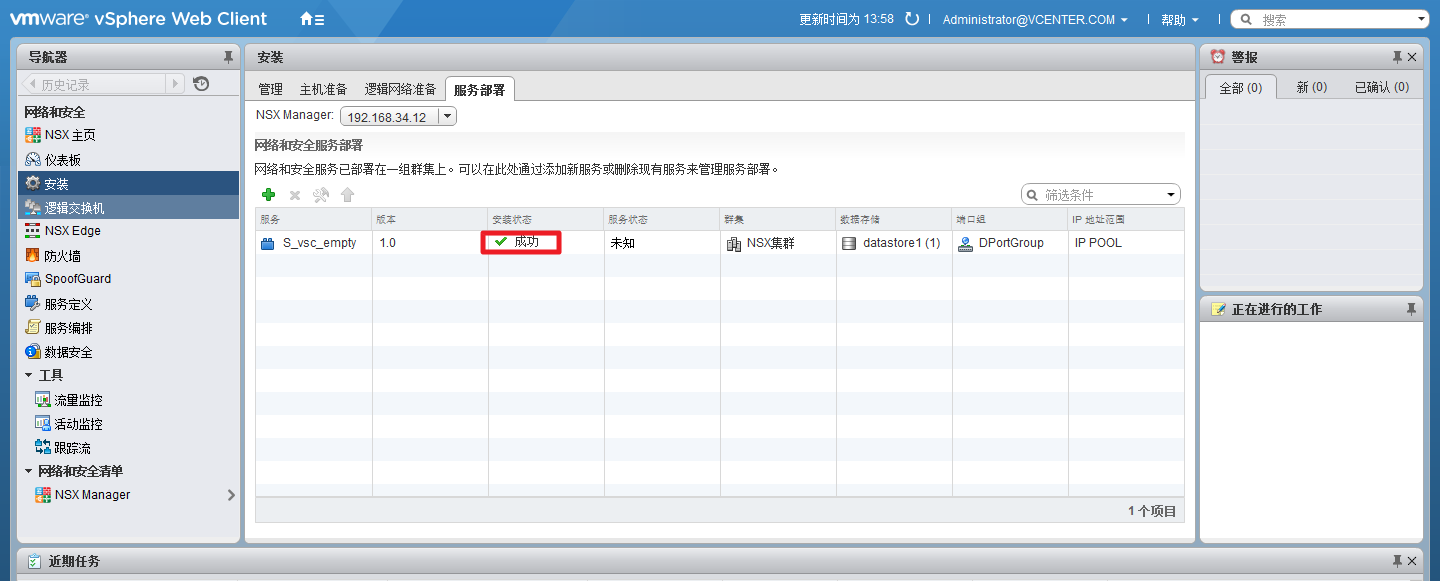


图56

1. 部署完成后需要手动修改vFW虚拟机网络为可用网络，打开控制台进行网络修改，如图57、58所示。

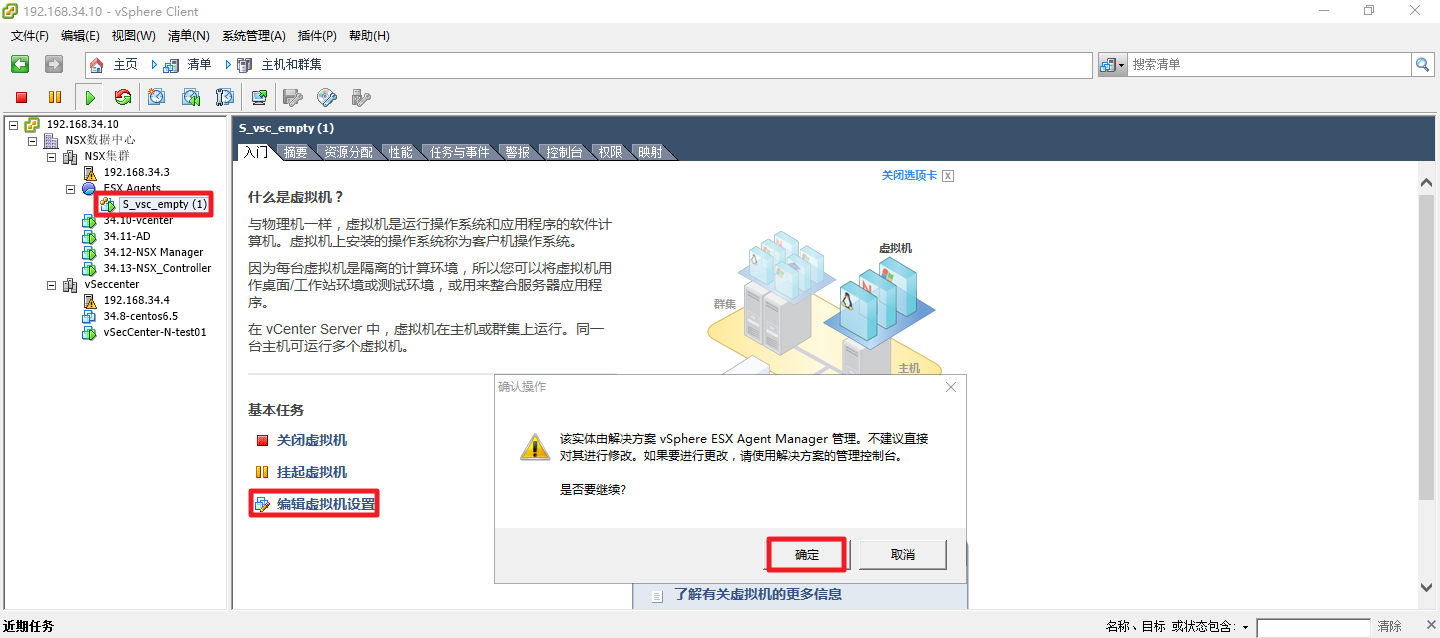


图57

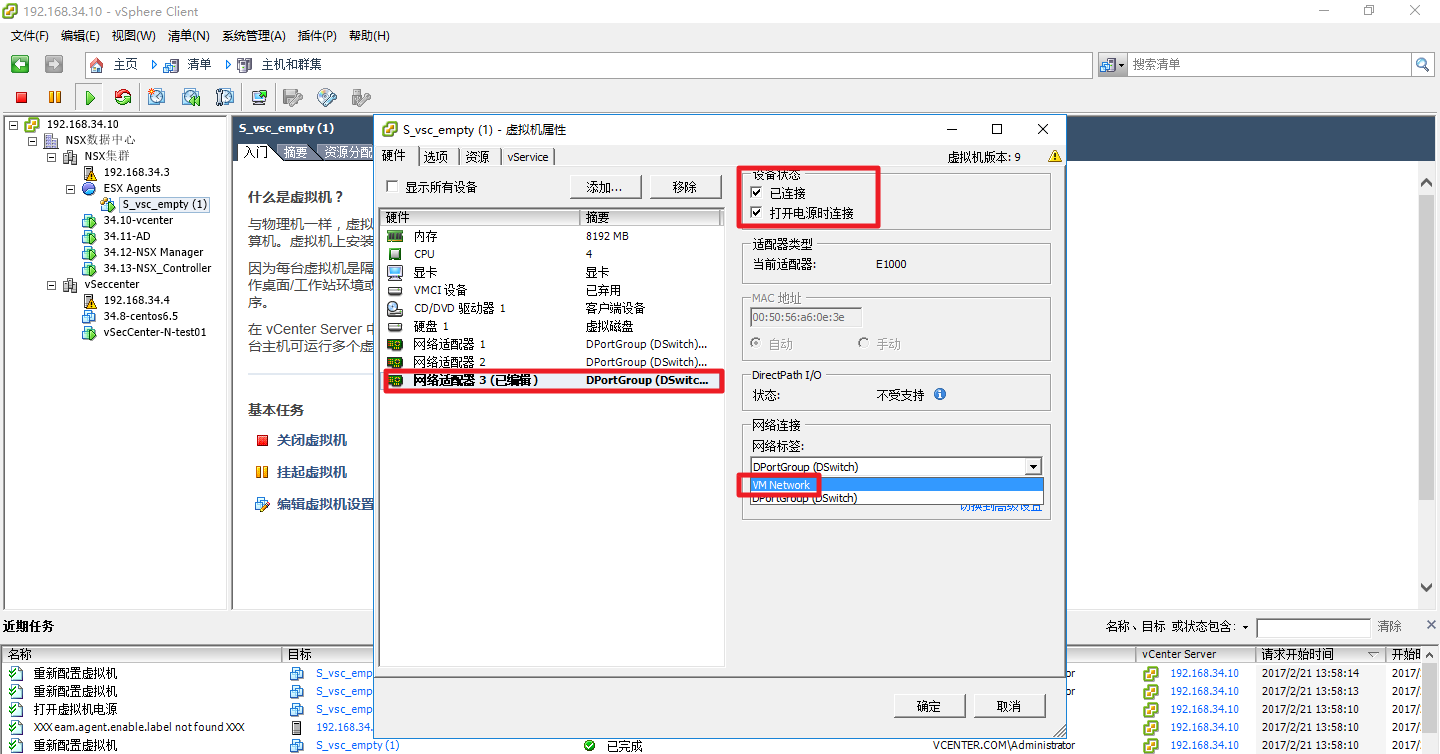


图58

1. 此时可以登录到vSeccenter-N查看对应的vFW，此时vFW并不能成功上线，仍需要继续进行相关配置，如图59所示。



图59

1. 目前版本每次启动vFW需要SSH登录到ngtos（用户密码：root/1）进行如下操作，如图60、61、62所示。

* 加载模块

# cd /root/data-plane/sample

# ./start-filter-nsx

* 启动cmdl\_agent

# cd /root/cmdl\_agent

# python main.py -d

* 启动ngfw

# ngtos start

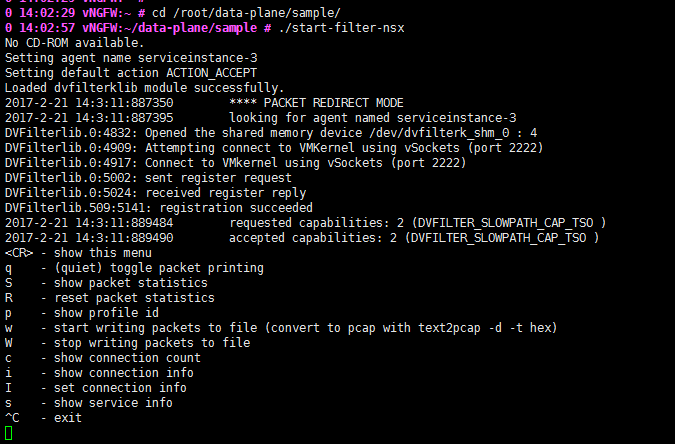


图60

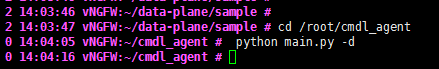


图61



图62

1. 目前版本第一次启动vFW时，需要SSH登录到ngtos（用户密码：root/1）手动修改cmdl\_ip对应的地址，需要SSH登录到vFW（用户密码：superman/talent）手动修改feth998网络接口，如图63、64所示。

* 修改cmdl\_ip为当前vSeccenter-N的地址

vNGFW:~# vi /root/cmdl\_agent/cmdl\_config.py

* 启动接口feth998并配置虚拟线

TopsecOS# network interface feth998 no shutdown

TopsecOS# network virtual-line add dev1 feth998 dev2 feth998

TopsecOS# save

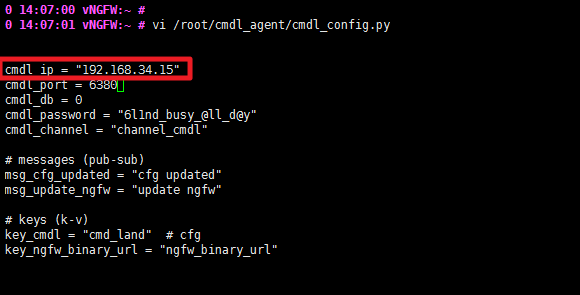


图63



图64

1. 此时再次登录到vSeccenter-N，查看对应的vFW，此时vFW的在线状态和CMDL连接状态均为在线状态，如图65所示。



图65

## 配置安全组和重定向

完成部署和配置vFW后，将进行安全组和流量重定向的相关配置，具体步骤如下：

1. 通过vSphere Web Client登录到vCenter主页，点击“网络和安全”选项，左侧工具栏中点击“服务编排”选项，切换“安全组”选项卡，点击“新建安全组”选项，输入安全组名称“安全组TEST”，点击“下一步”按钮，如图66所示。

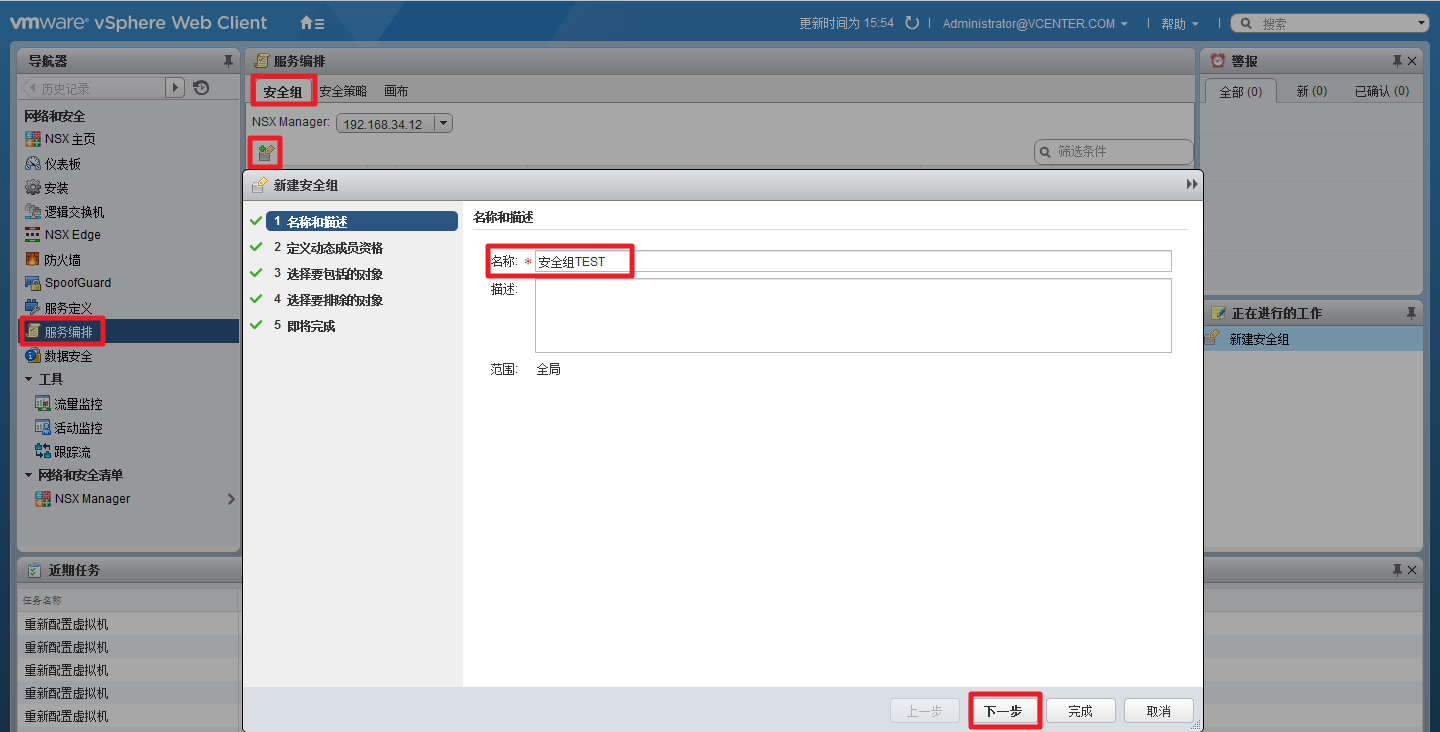


图66

1. 定义动态成员资格可以为对象指定要成为该安全组成员所必须满足的动态成员资格条件，这里可以灵活选择判断实体、满足条件以及成员资格条件之间的与或关系，如图67所示。

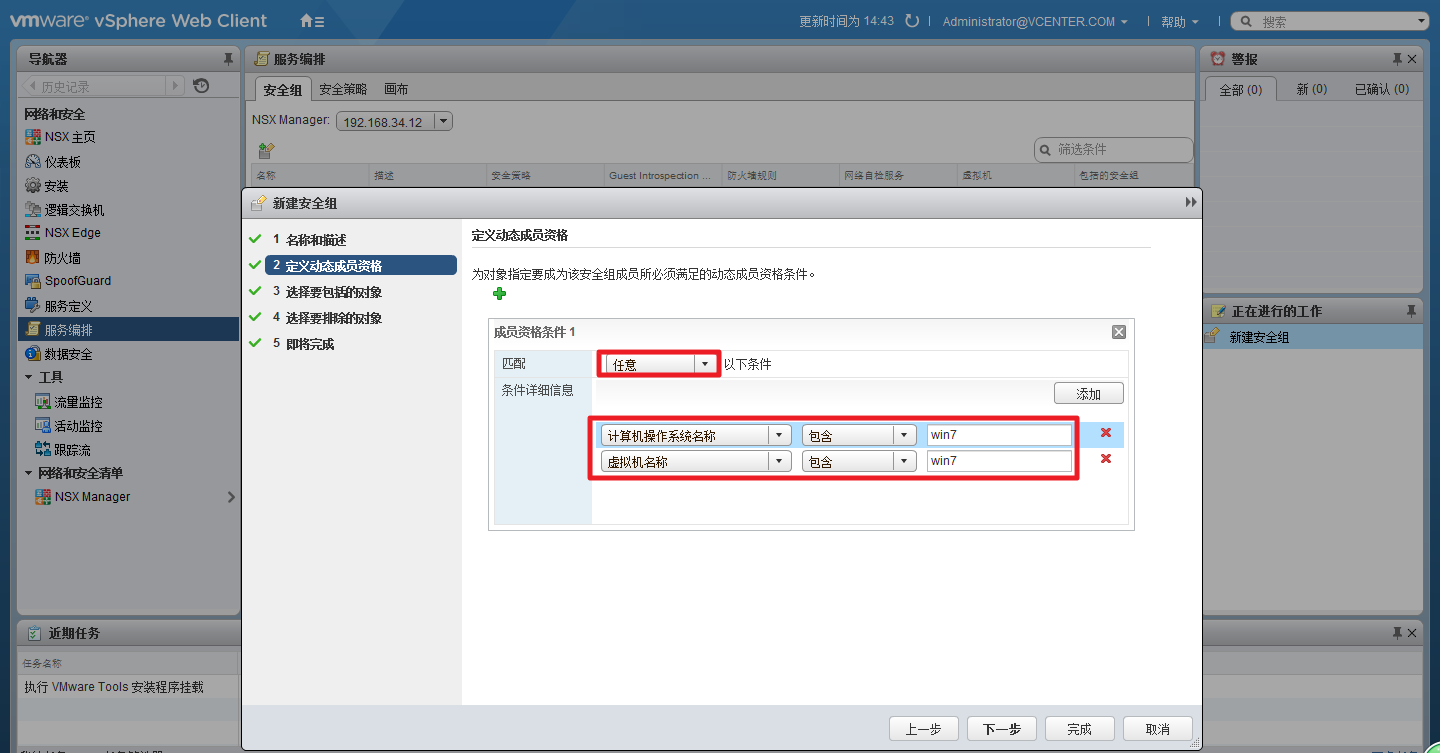


图67

1. 选择要包括的对象后，将会始终包括在该策略中，不论其是否满足成员资格条件，如图68所示。

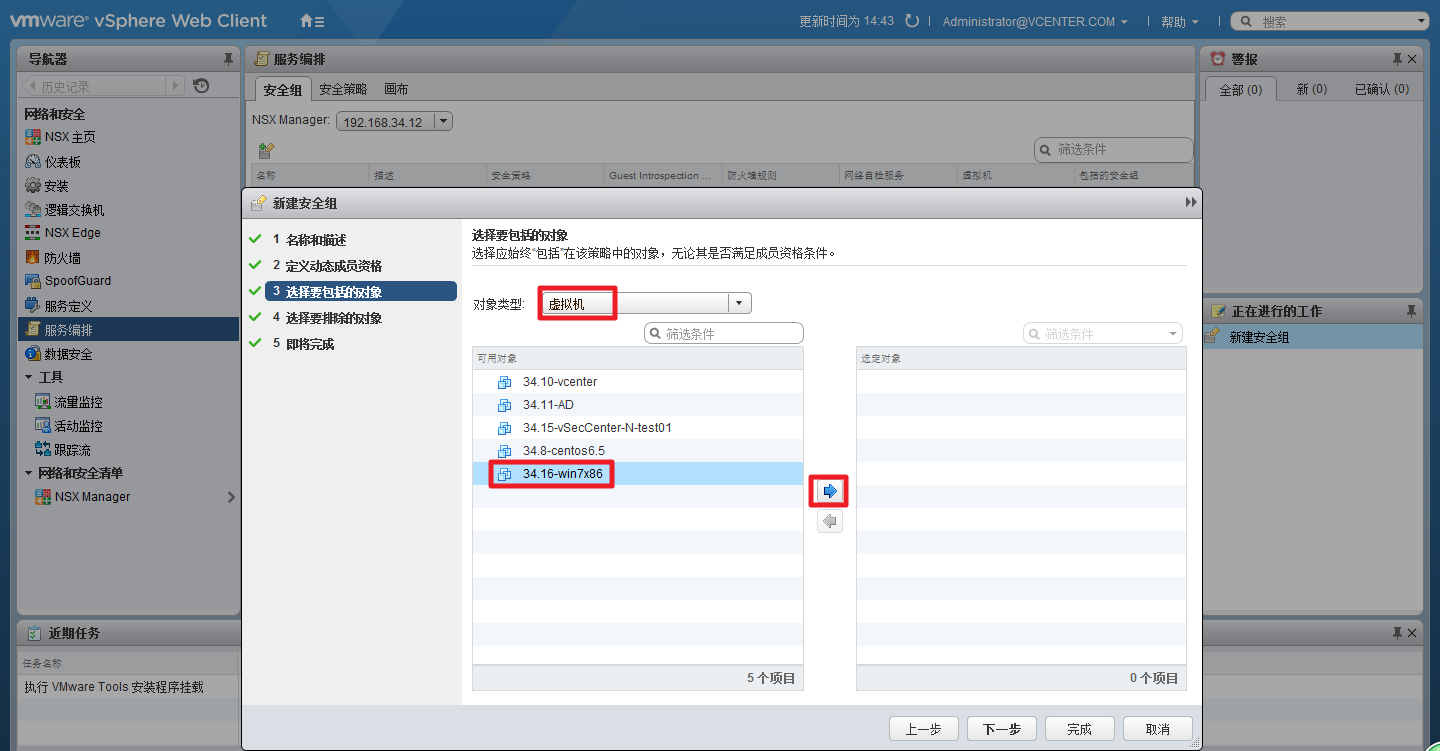


图68

1. 选择要排除的对象后，将会始终在该策略中排除，不论其是否满足成员资格条件，如图69所示。

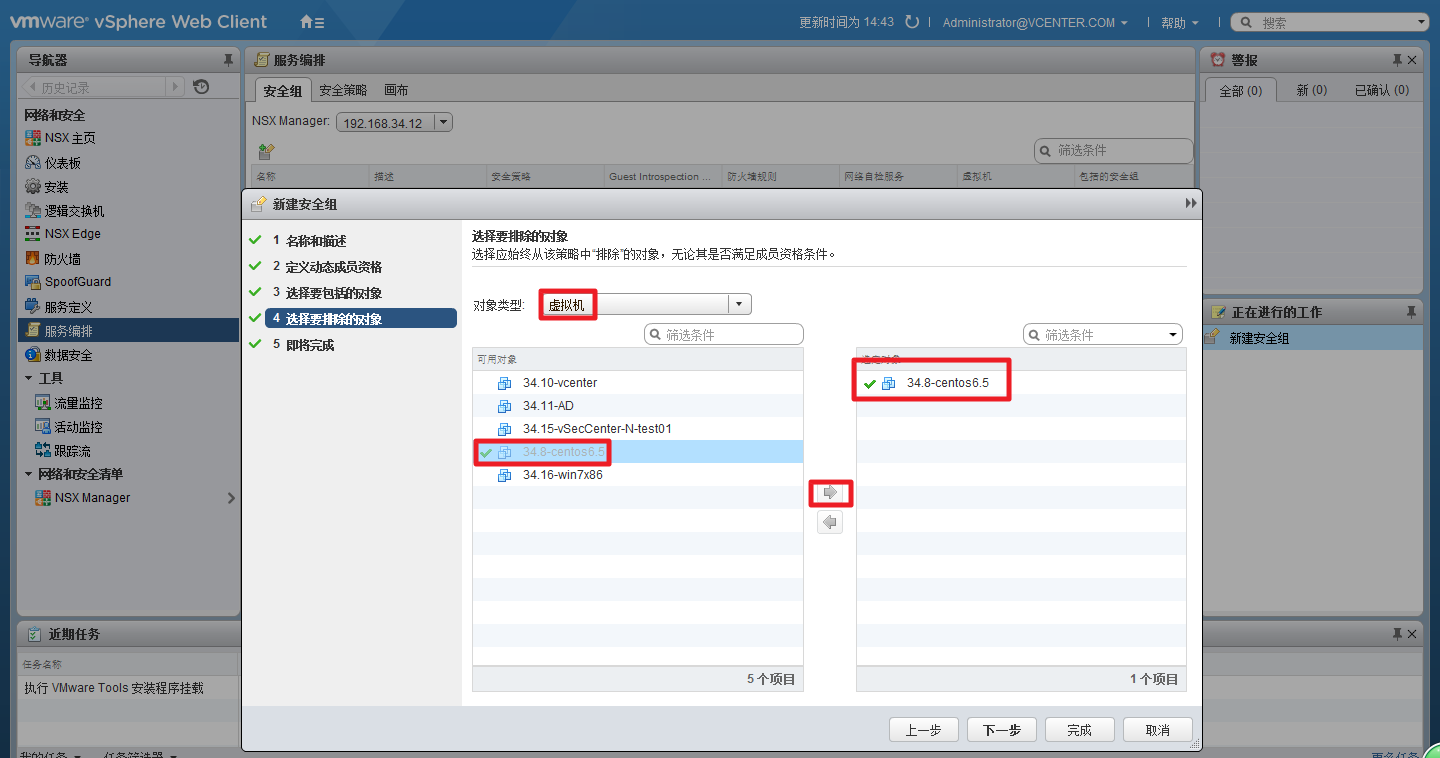


图69

1. 检查新建安全组配置是否正确无误，点击“完成”按钮，如图70所示。

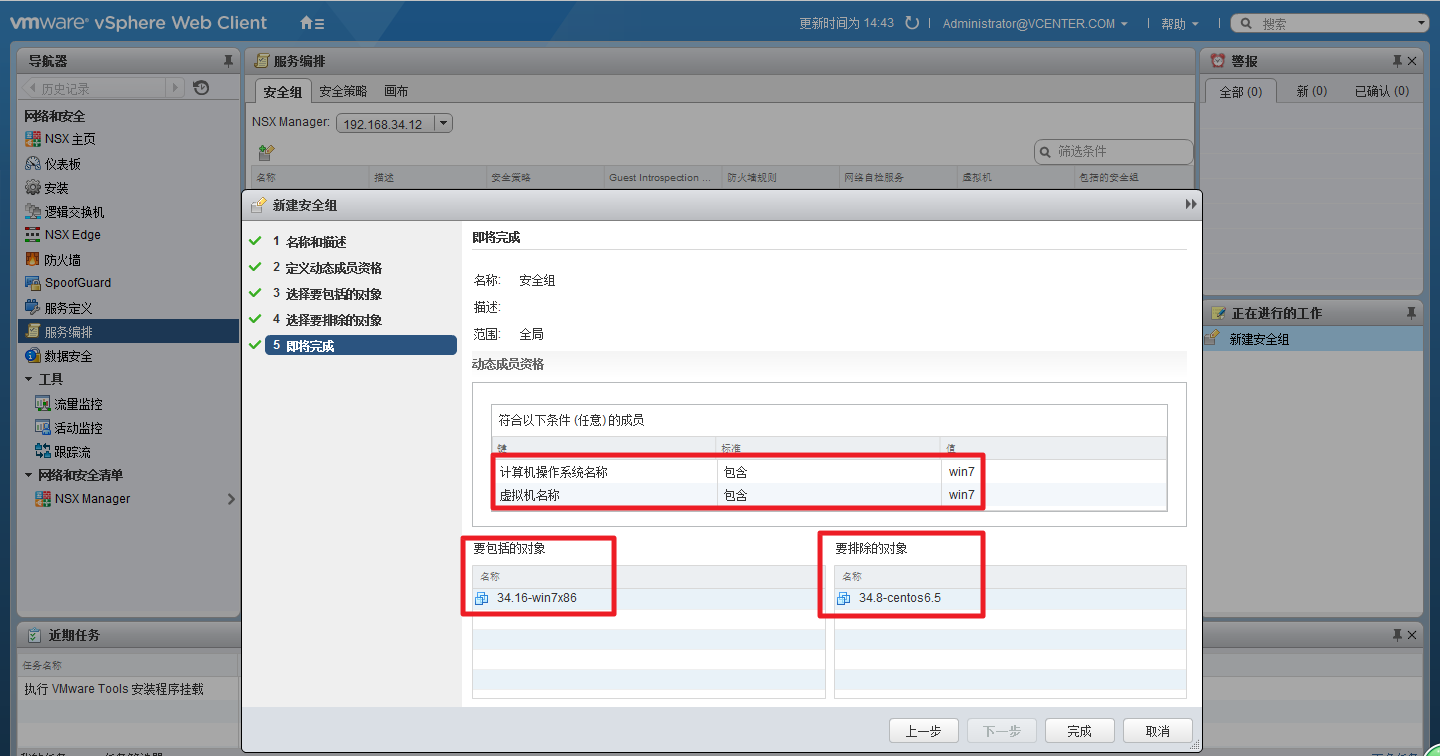


图70

1. 创建完成安全组后可以查看该安全组内符合资格的对象，如图71所示。

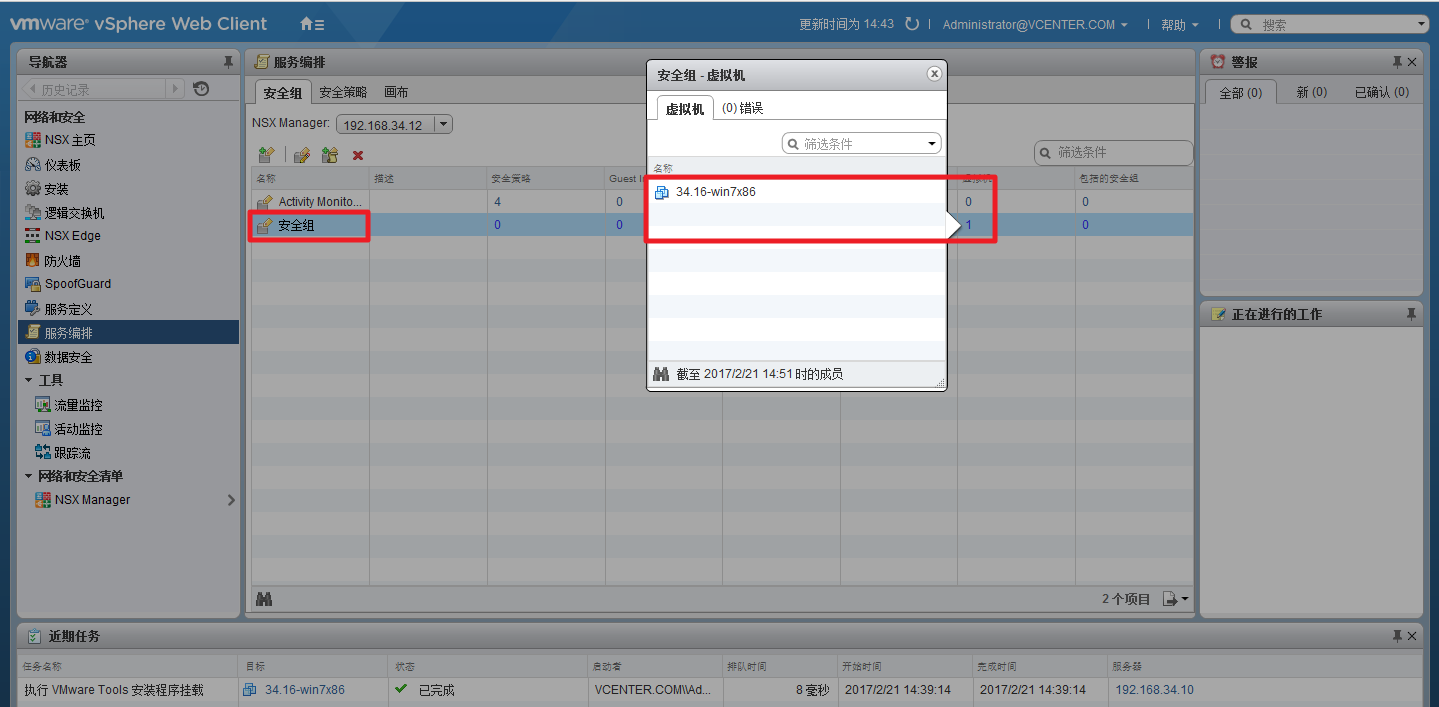


图71

1. 接下来我们进行流量重定向的配置，左侧工具栏切换到“防火墙”选项，点击“配置”选项卡，再切换到“合作伙伴安全服务”选项卡，点击“添加规则”按钮，如图72所示。

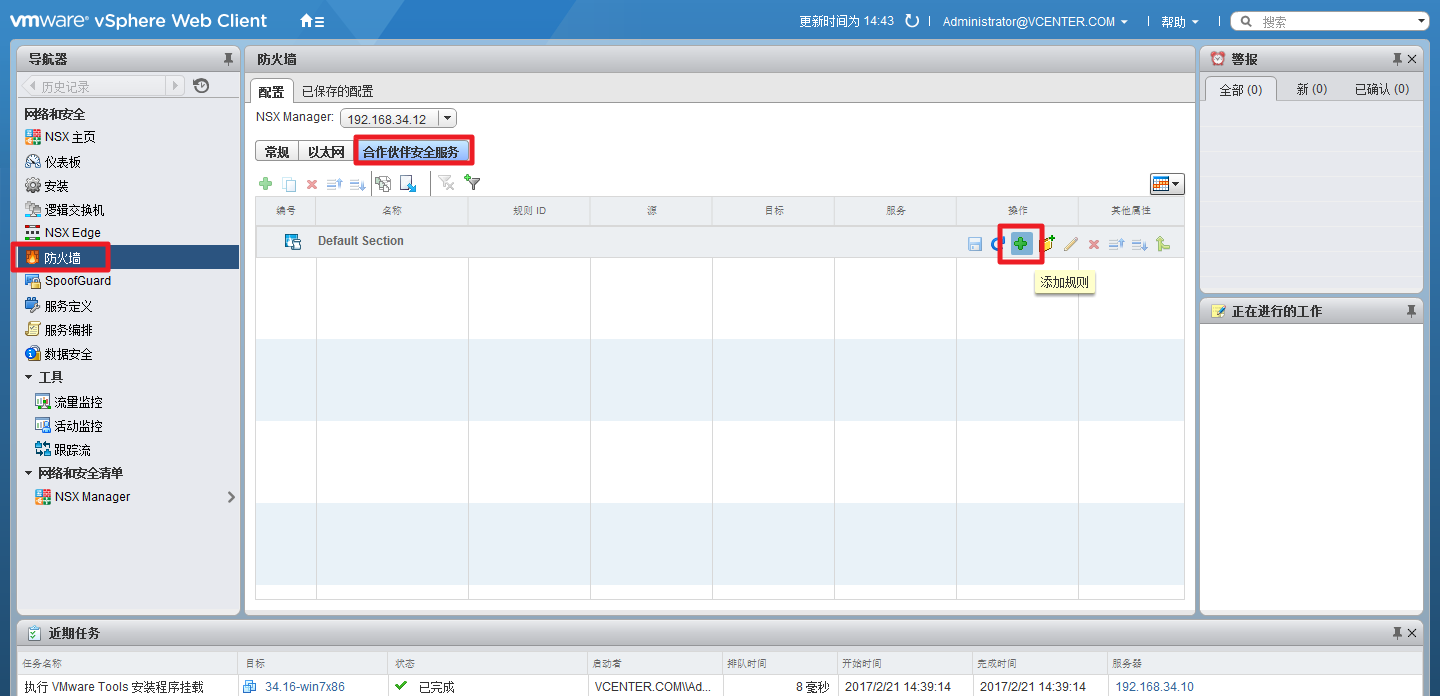


图72

1. 在新建规则上点击修改，如图73所示。



图73

1. 在规则编辑操作界面，【服务】选择之前注册的NSX服务“S\_vsc\_empty”，【服务配置文件】选择“S\_vsc\_empty\_VendorTem…..”，【操作】选择“重定向”，【方向】选择“入站/出站”，【数据包类型】选择“IPV4”，然后点击“保存”按钮，如图74所示。

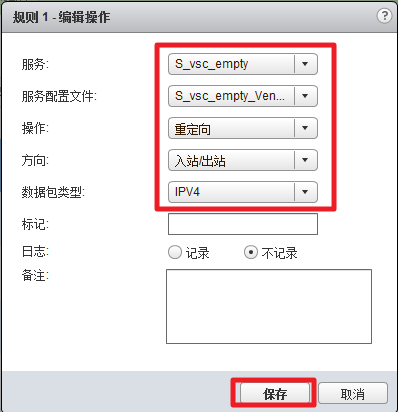


图74

1. 返回之前页面，在刚添加的规则之上点击“S\_vsc\_empty\_VendorTemplate for service-9”，在弹出的“指定服务配置文件绑定”界面选中并添加之前配置的安全组“安全组TEST”，点击“确定”按钮，如图75所示。

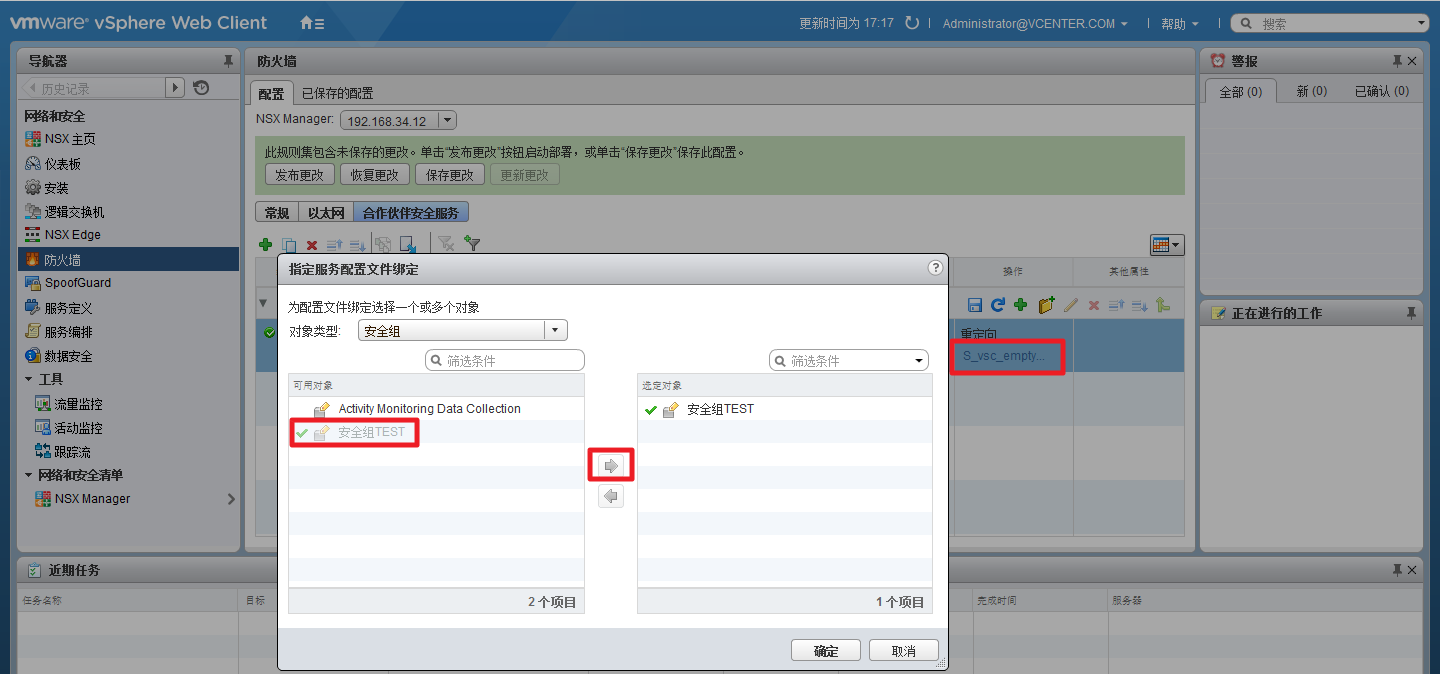


图75

1. 点击“发布更改”按钮，完成规则发布，如图76、77所示。

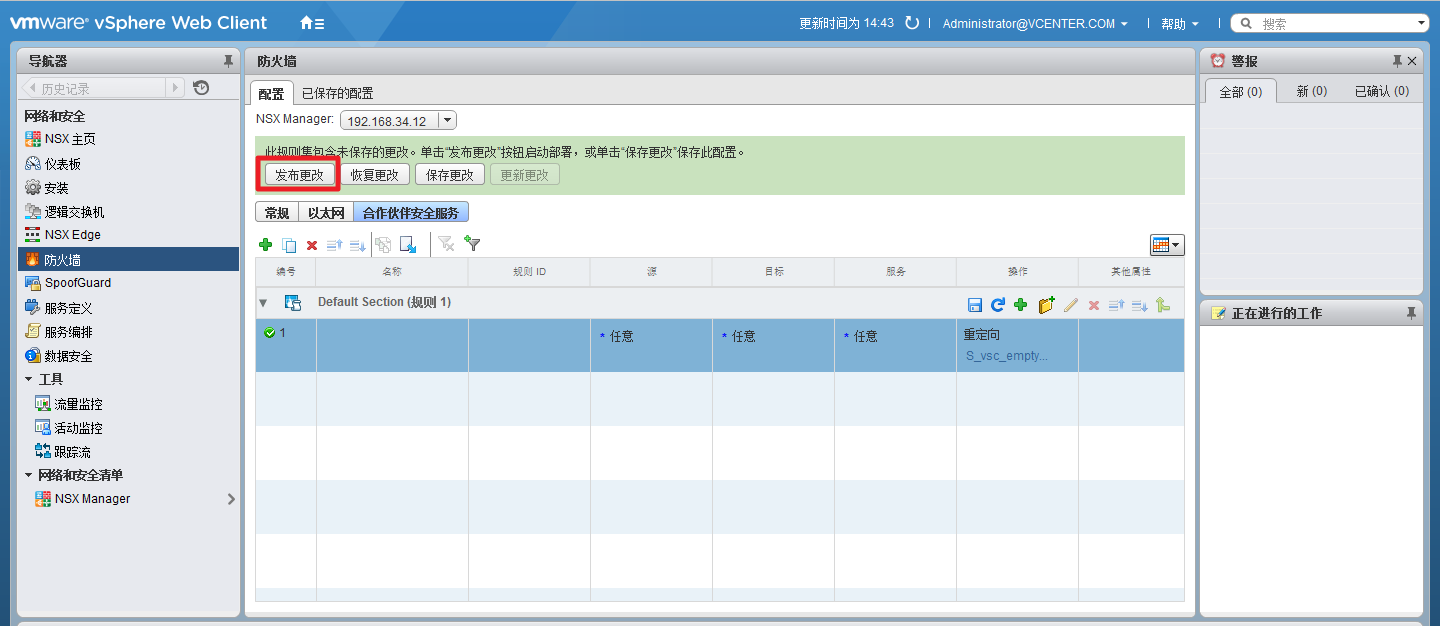


图76

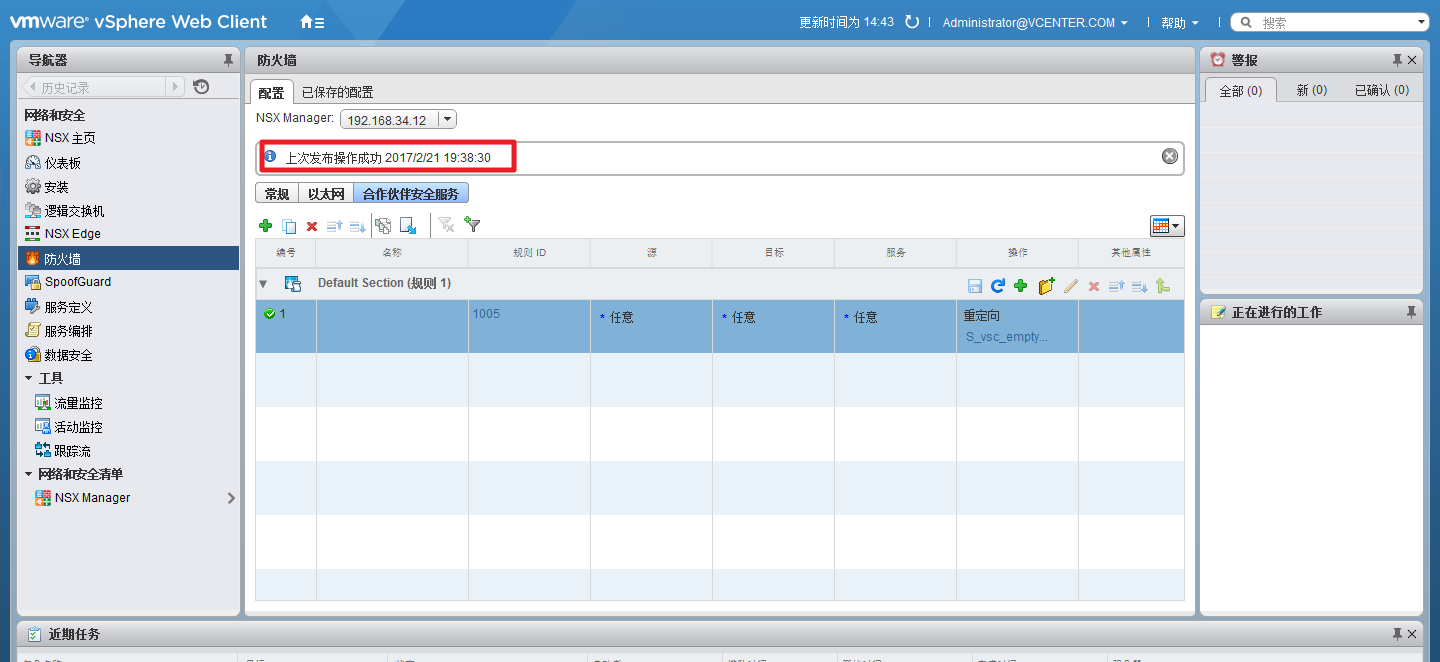
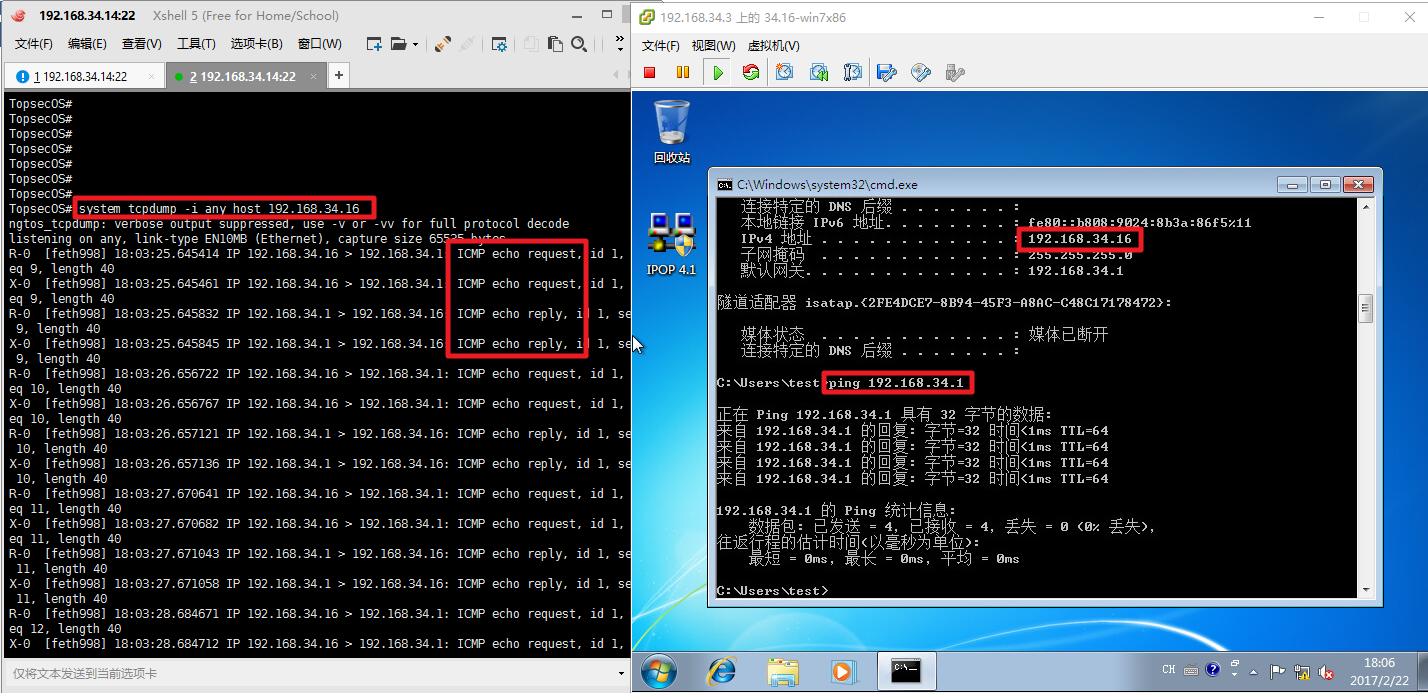


图77

## 流量重定向结果验证

至此，我们完成了VMware NSX基础环境和vSeccenter-N的部署和配置，现在提供两种验证流量重定向是否成功的简单方法，具体如下：

方法一：SSH登录vFW后（superman/talent），使用tcpdump针对测试机进行抓包，然后使用测试机进行ping操作，在vFW上可以抓到ICMP echo request和ICMP echo reply的数据包证明流量重定向成功，如图78所示。



方法二：登录到vSeccenter-N，添加测试机IP地址为主机地址对象，配置这样的访问控制策略：【动作】选择“拒绝”，【源地址】选择主机地址“34.16”，【服务】选择预定义服务“ICMP”，【高级选项】选择日志“记录日志”，并成功下发策略到vFW，然后使用测试机进行ping操作，发现无法ping通，且在vFW上只能抓到ICMP echo request的数据包证明流量重定向成功，如图79、80所示。



图79

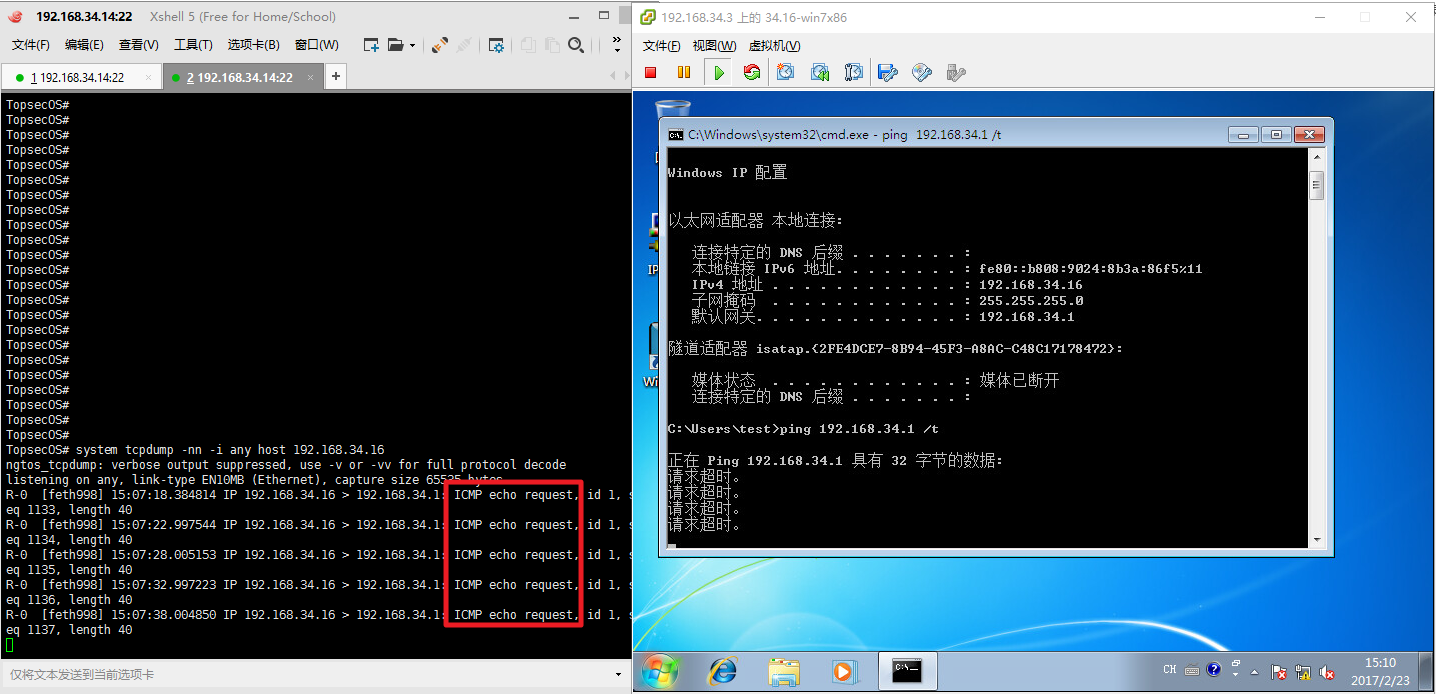


图80

# 参考书籍

《新一代SDN-VMware NSX网络原理与实践》