CX云代理概述v2.0

目录

- 简介
- 背景信息
  - 先决条件
  - 关键域访问
    - 升级到CX云代理v2.0的先决条件
  - Cisco DNA Center 认证版本
  - 支持的浏览器
- 部署CX云代理
- 将CX云代理连接到CX云
- 部署和网络配置
  - OVA 部署
    - 胖客户端 ESXi 5.5/6.0 安装
    - Web 客户端 ESXi 6.0 安装
    - Web 客户端 vCenter 安装
    - Oracle Virtual Box 5.2.30 安装
    - Microsoft Hyper-V 安装
  - 网络配置
  - 使用CLI生成配对代码的备用方法
- 配置Cisco DNA Center以将系统日志转发到CX云代理
  - 前提条件
  - 配置系统日志转发设置
  - 启用信息级别系统日志设置
- 安全
  - 物理安全
  - 用户访问权限
  - 账户安全
  - 网络安全
  - 身份验证
  - 强化
  - 数据安全
  - 数据传输
  - 日志和监控
  - 安全汇总
- 常见问题解答
  - CX Cloud Agent
    - 部署
    - 版本和补丁
    - 身份验证和代理配置
    - Secure Shell (SSH)
    - 端口和服务

- CX Cloud Agent 与 Cisco DNA Center 的连接
- CX Cloud Agent 使用的诊断扫描
- CX Cloud Agent 系统日志

故障排除

- 收集失败响应
- 诊断扫描失败响应

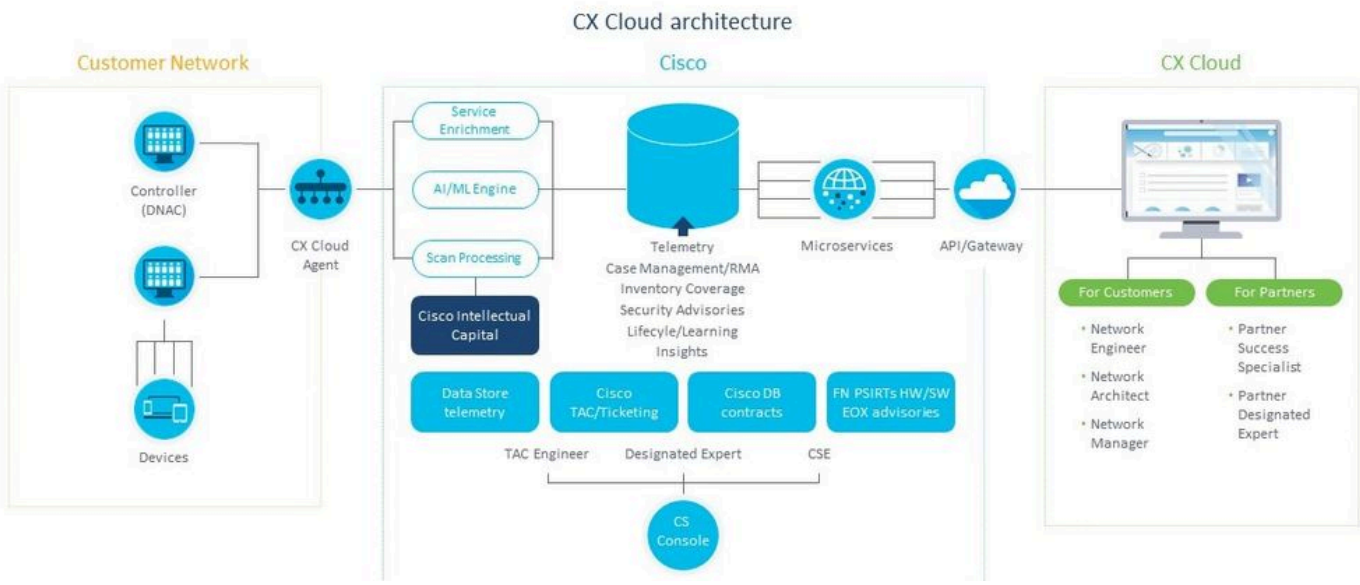
简介

本文档介绍Cisco CX云代理；一个模块化内部软件平台，可托管轻型容器化微服务功能。

背景信息

Cisco Customer Experience(CX)Cloud Agent功能可在客户现场通过云进行安装、配置和管理。CX云代理加速新产品的货币化，扩展功能，并帮助开发由大数据、分析、自动化、机器学习/人工智能(ML/AI)和流驱动的新一代服务。

> 注意：本指南面向CX云代理v2.0用户。有关其他相关信息，请参阅Cisco CX云代理。



CX Cloud Agent 架构

CX Cloud Agent 架构

> 注意：本指南中的图像（及其中的内容）仅供参考。实际内容可能有所不同。

先决条件

CX Cloud Agent 作为虚拟机 (VM) 运行，可以开放式虚拟设备 (OVA) 或虚拟硬盘 (VHD) 的形式进行下载。

部署要求：

- 以下虚拟机监控程序之一：
  - VMWare ESXi版本5.5或更高版本
  - Oracle Virtual Box 5.2.30
  - Windows虚拟机监控程序版本2012到2016
- 虚拟机监控程序可以托管需要以下内容的虚拟机：
  - 8 核心 CPU
  - 16 GB 内存/RAM
  - 200 GB 磁盘空间
- 对于使用指定的思科美国数据中心作为主要数据区域来存储CX云数据的客户：
  CX云代理必须能够连接到此处显示的服务器，使用FQDN并在TCP端口443上使用HTTPS:
  FQDN：agent.us.csco.cloud
  FQDN：ng.acs.agent.us.csco.cloud
  FQDN：cloudsso.cisco.com
  FQDN：api-cx.cisco.com
- 对于使用指定的思科欧洲数据中心作为主要数据区域来存储CX云数据的客户：
  CX云代理必须能够使用FQDN和TCP端口443上的HTTPS连接到此处所示的两个服务器：
  FQDN：agent.us.csco.cloud
  FQDN：agent.emea.csco.cloud
  FQDN：ng.acs.agent.emea.csco.cloud
  FQDN：cloudsso.cisco.com
  FQDN：api-cx.cisco.com
- 对于使用指定的思科亚太地区数据中心作为主要数据区域来存储CX云数据的客户：
  CX云代理必须能够使用FQDN和TCP端口443上的HTTPS连接到此处所示的两个服务器：
  FQDN：agent.us.csco.cloud
  FQDN：agent.apjc.csco.cloud
  FQDN：ng.acs.agent.apjc.csco.cloud
  FQDN：cloudsso.cisco.com
  FQDN：api-cx.cisco.com

- 对于使用指定的思科欧洲和思科亚太地区数据中心作为其主要数据区域的客户，FQDN连接：仅在初始设置期间向CX云注册CX云代理时需要agent.us.csco.cloud。在CX云代理成功注册到CX云后，不再需要此连接。
- 对于CX云代理的本地管理，必须能够访问端口22。

有关 CX Cloud Agent 的其他说明：

- 如果在VM环境中启用了动态主机配置协议(DHCP)，则自动检测到IP。否则，必须有一个可用的IPv4地址、子网掩码、默认网关IP地址和DNS服务器IP地址。
- 仅支持IPv4，不支持IPv6。
- 需要从1.2.8到1.3.3.9以及2.1.2.0到2.2.3.5的认证单节点和高可用性(HA)集群思科数字网络架构(DNA)中心版本。
- 如果网络具有SSL拦截，则允许列表CX云代理IP地址。

关键域访问

要开始CX云之旅，用户需要访问这些域。

主要域	其他域
cisco.com	mixpanel.com
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

特定于区域的域:

美洲地区	欧洲、中东和非洲	亚太地区
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

升级到CX云代理v2.0的先决条件

升级到CX Cloud Agent v2.0之前必须满足本部分列出的必备条件。

1. 确保在开始升级之前必须安装CX云代理v1.12.x及更高版本。
2. 如果尚未配置域名服务器，请执行以下步骤配置该服务器：
    1. 登录到CX云代理虚拟机的命令行界面(CLI)控制台。

2. 执行cxcli agent configureDNS命令。
3. 输入DNS IP地址。
4. 单击。Exit

3. 确保客户的网络允许关键域访问中的域名在迁移期间完成云代理重新注册。CX云代理必须能够访问这些域，并且这些域必须可以从DNS服务器进行解析。 如果有任何域无法访问，请与网络团队联系。
4. 在启动v2.0升级之前拍摄云代理VM快照（需要正确访问）。

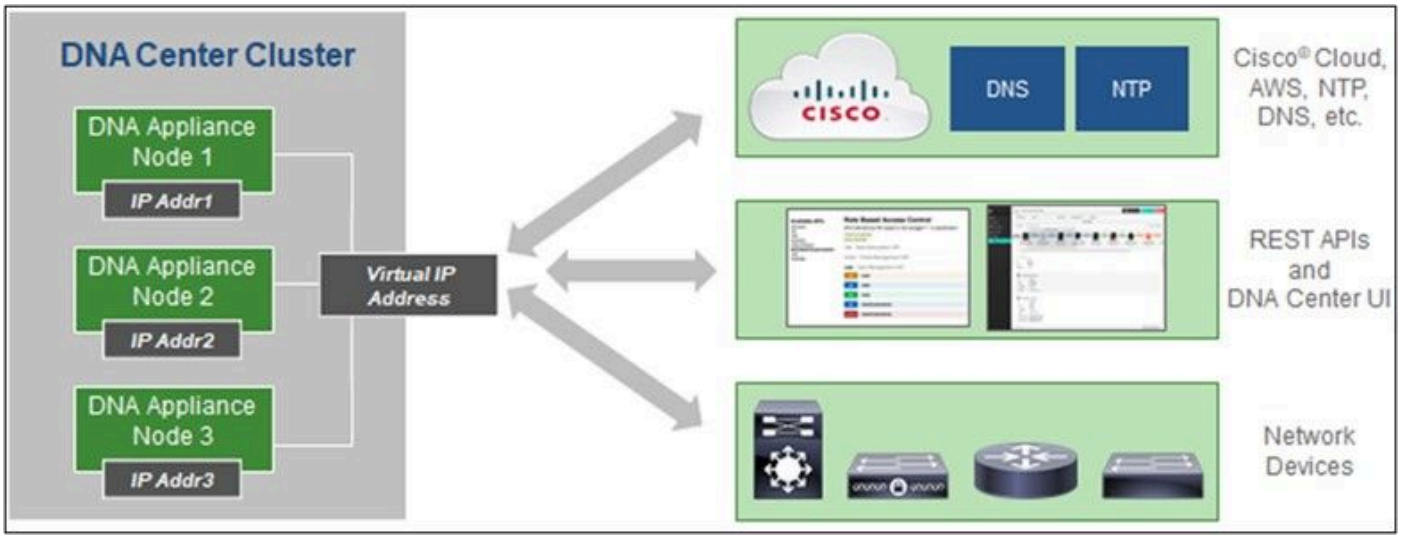
注意：1.10之前的版本必须首先升级到v1.10，然后逐步升级到v1.12.x，再升级到v2.0。用户可以在CX云门户中从“管理员设置”>“数据源”进行升级。单击View Update，完成升级。

要成功安装，必须满足以下条件：

1. DNAC及其凭证列表
2. 具有管理员或观察者角色访问的DNAC用户
3. DNAC群集的虚拟IP地址或独立/物理IP地址
4. 云代理和DNAC之间的成功可达性
5. DNAC必须至少有一台受管设备

Cisco DNA Center 认证版本

认证单节点和 HA 集群 Cisco DNA Center 版本为 1.2.8 至1.3.3.9 和 2.1.2.0 至 2.2.3.5。



多节点 HA 集群 Cisco DNA Center

多节点 HA 集群 Cisco DNA Center

支持的浏览器

要获得Cisco.com上的最佳体验，我们建议使用以下浏览器的最新正式版本：

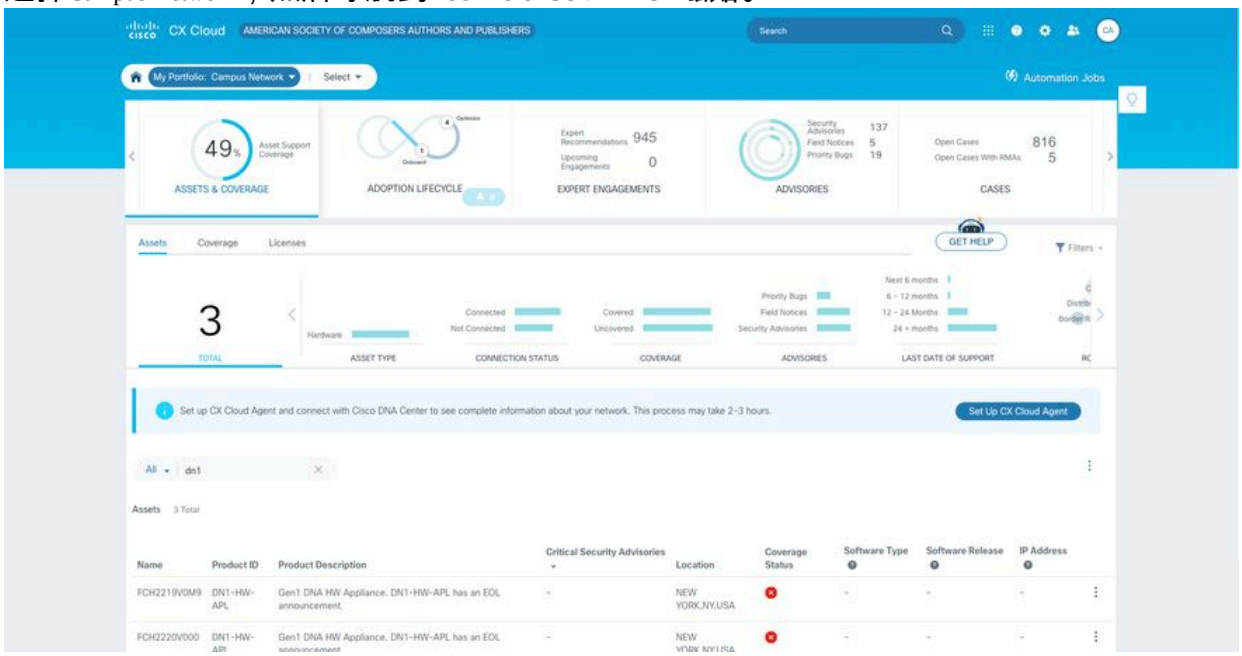
- Google Chrome
- Microsoft Edge

- Mozilla Firefox

部署CX云代理

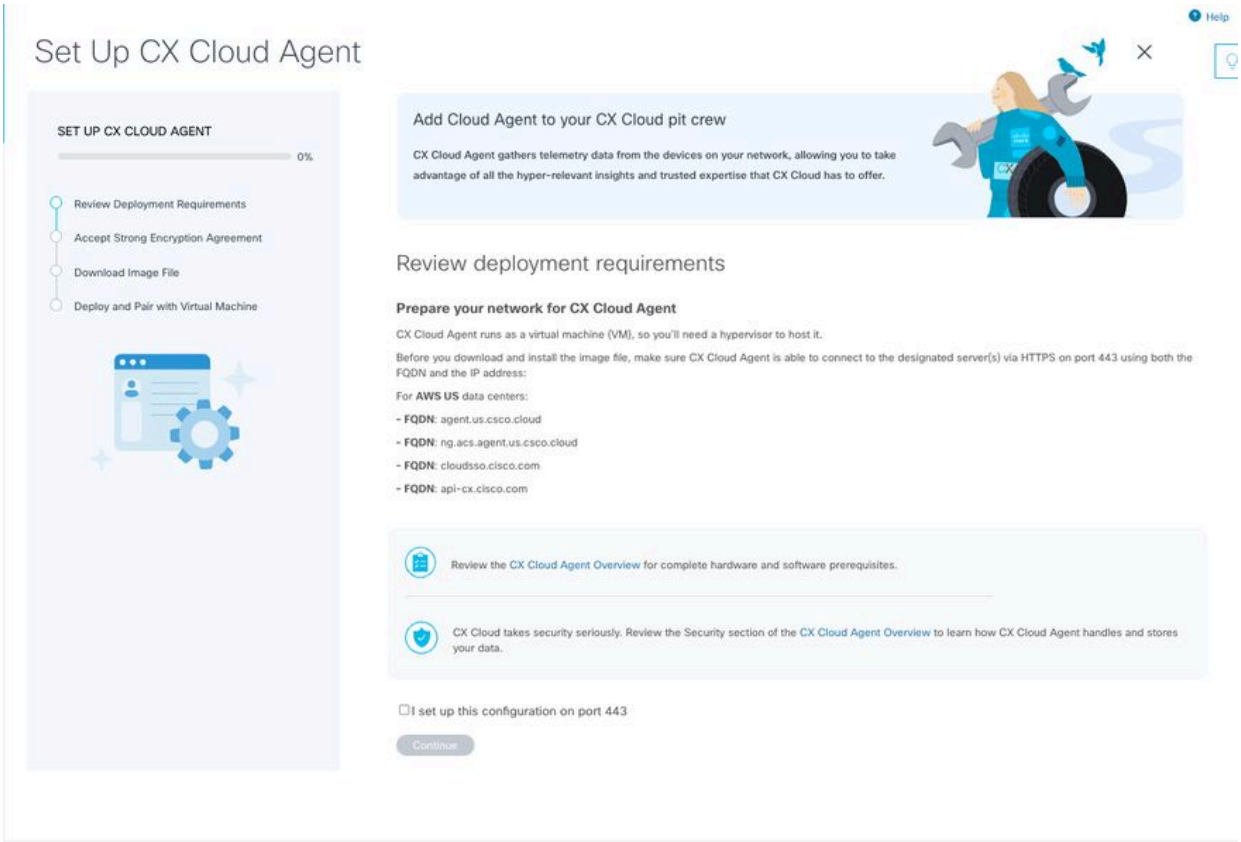
要部署 CX Cloud Agent，请执行以下操作：

1. 点击 cx.cisco.com以登录到 CX Cloud。
2. 选择Campus Network ，然后导航到ASSETS & COVERAGE磁贴。



主页

3. 在横幅中单击Set Up CX Cloud Agent。Set Up CX Cloud Agent - Review deployment requirements 窗口打开。

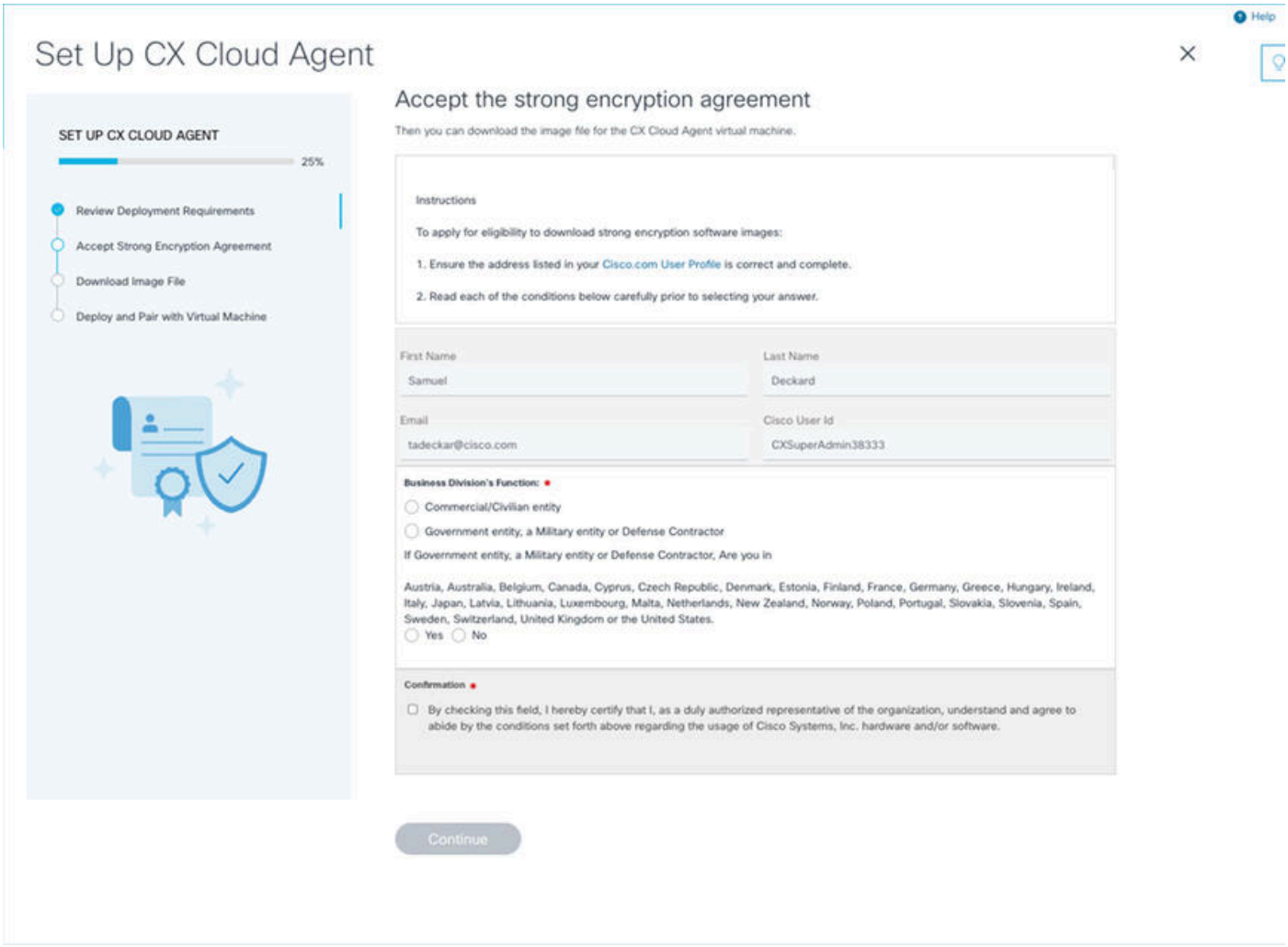


审核部署要求

4. 阅读查看部署要求中的必备条件，并选中I set up this configuration on port 443复选框。

注意：本指南中的图像（及其中的内容）仅供参考。实际内容可能有所不同。

5.单击继续。Set Up CX Cloud Agent - Accept the strong encryption agreement窗口打开。



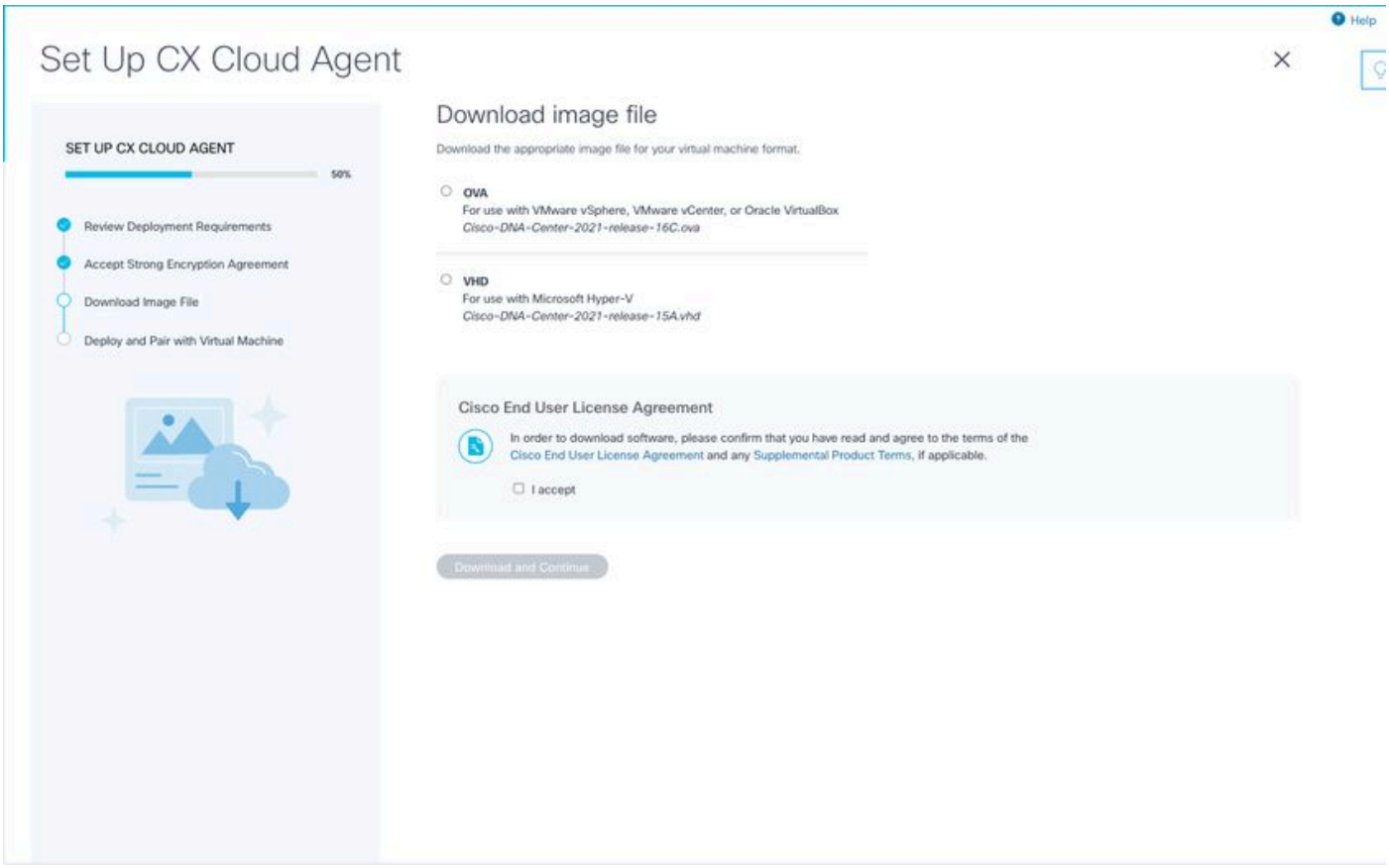
加密协议

6.验证First Name、Last Name、E-mail和CCO User Id字段中的预填信息。

7.选择适当的 Business division’s function.

8.选中此Confirmation复选框以同意使用条件。

9.单击继续。Set Up CX Cloud Agent - Download image file窗口打开。



下载映像

10.选择适当的文件格式下载安装所需的映像文件。

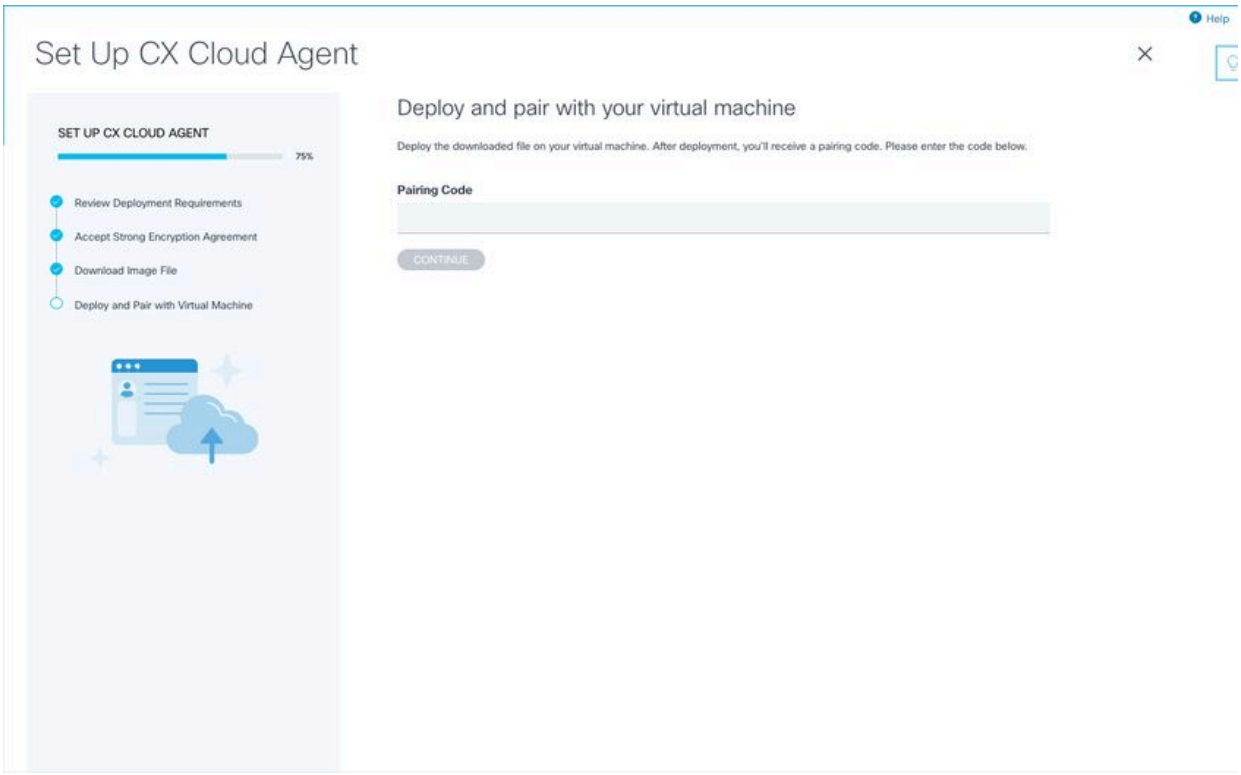
11.选中I accept复选框以同意思科最终用户许可协议。

12.单击Download and Continue。Set Up CX Cloud Agent - Deploy and pair with your virtual machine窗口打开。

13.请参阅OVA安装的网络配置，然后继续下一节以安装CX云代理。

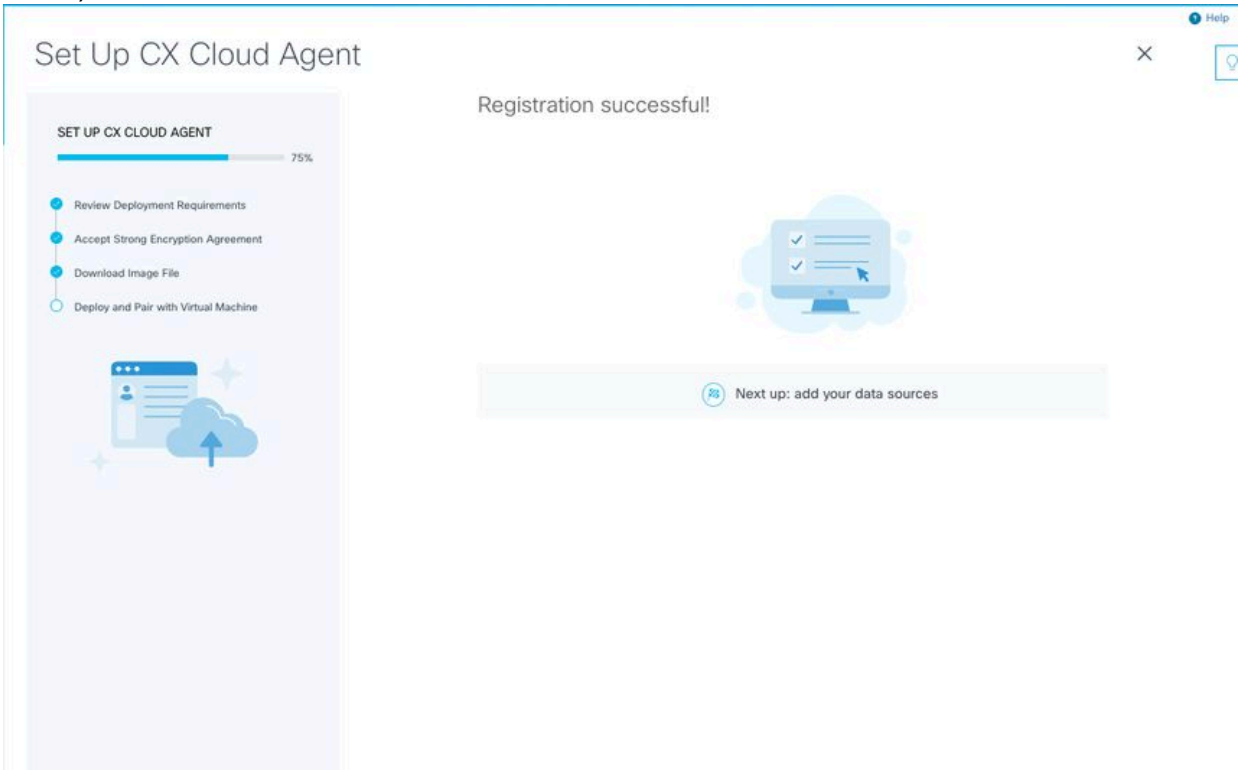
将CX云代理连接到CX云

1. 输入控制台对话框或命令行界面(CLI)中提供的配对代码。

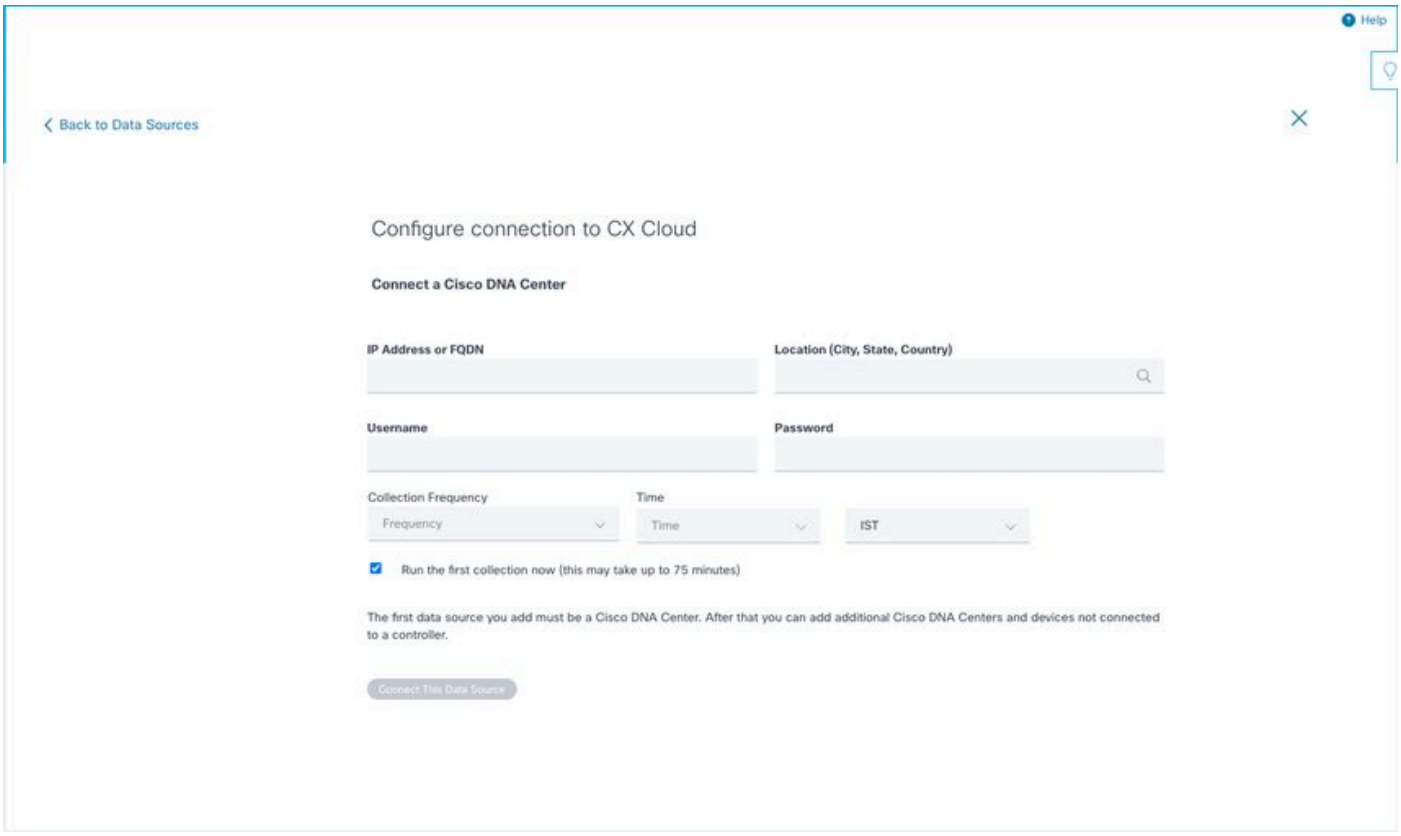


配对代码

2. 单击Continue注册CX云代理。在自动导航到Configure Connection to CX Cloud窗口之前，将显示Set Up CX Cloud Agent - Registration successful（设置CX云代理 — 注册成功）窗口。

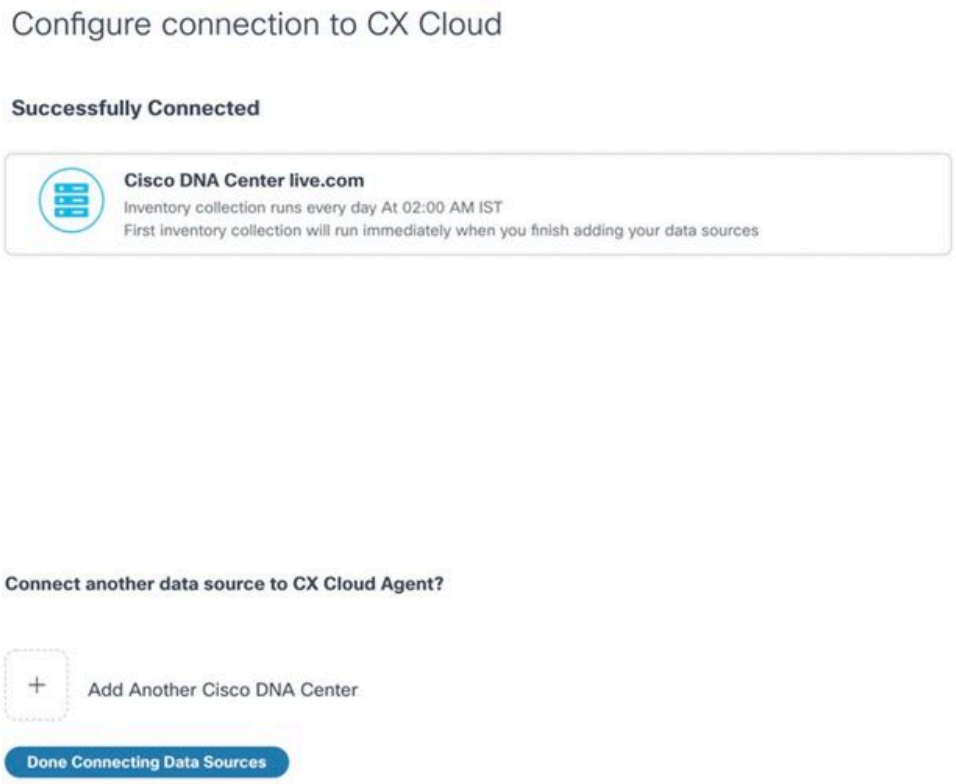


注册成功



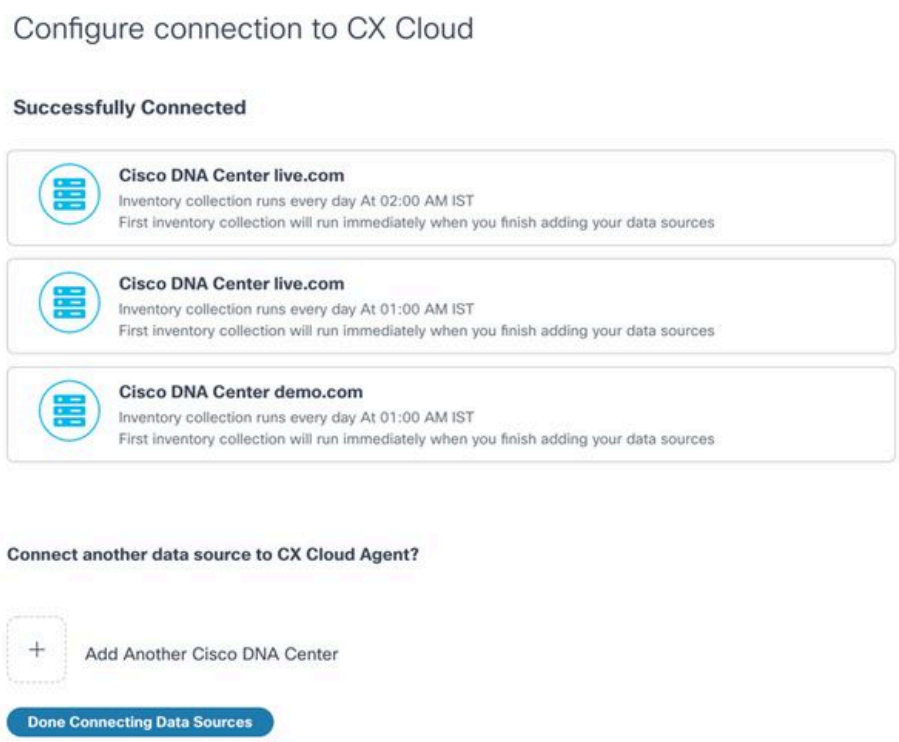
配置连接

3.输入数据，然后单击连接此数据源。系统将显示确认消息“成功连接”。



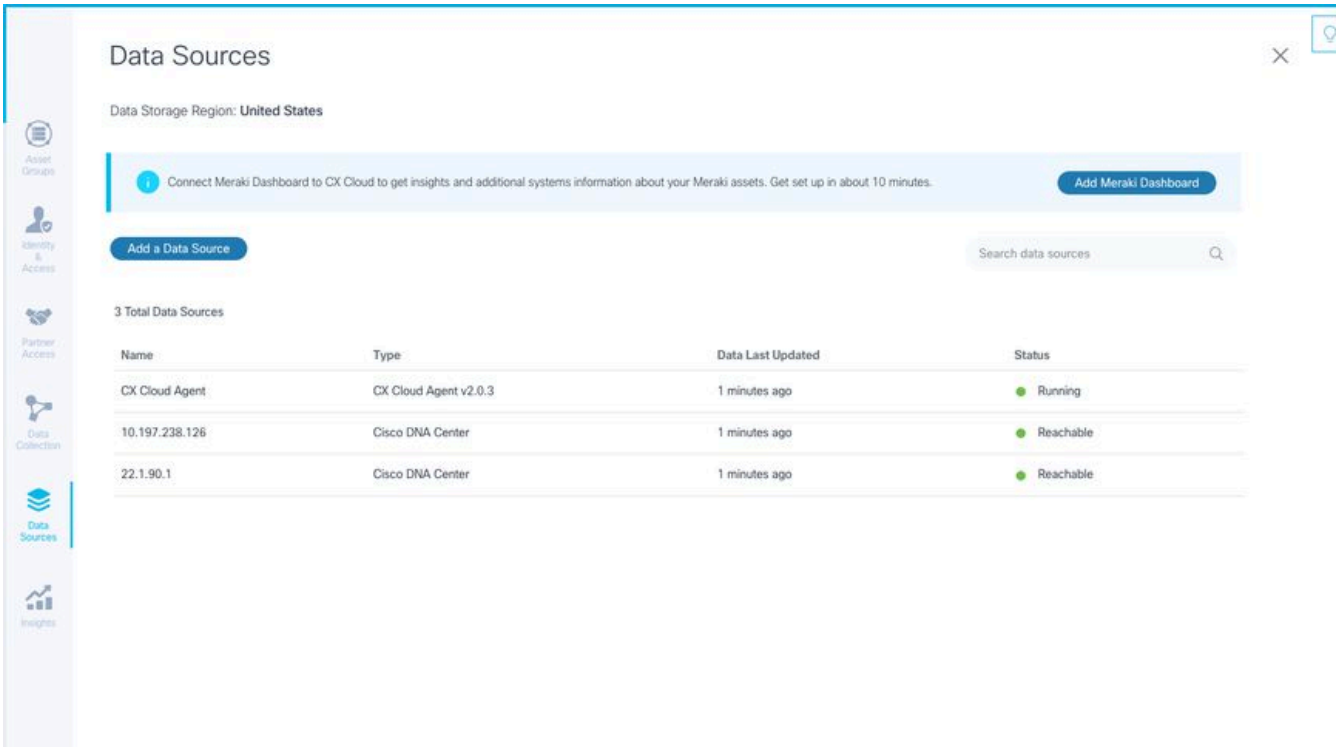
已成功添加DNAC

注意：单击Add Another Cisco DNA Center以添加多个DNAC。



已添加多个DNAC

4.单击完成连接数据源。Data Sources窗口打开。



部署和网络配置

可以选择以下任一选项来部署CX云代理：

- 如果选择 VMware vSphere/vCenter 胖客户端 ESXi 5.5/6.0，请转至胖客户端
- 如果选择 VMware vSphere/vCenter Web 客户端 ESXi 6.0，请转至 Web 客户端 vSphere 或中心
- 如果选择 Oracle Virtual Box 5.2.30，请转至 Oracle VM
- 如果选择 Microsoft Hyper-V，请转至 Hyper-V

OVA 部署

胖客户端 ESXi 5.5/6.0 安装

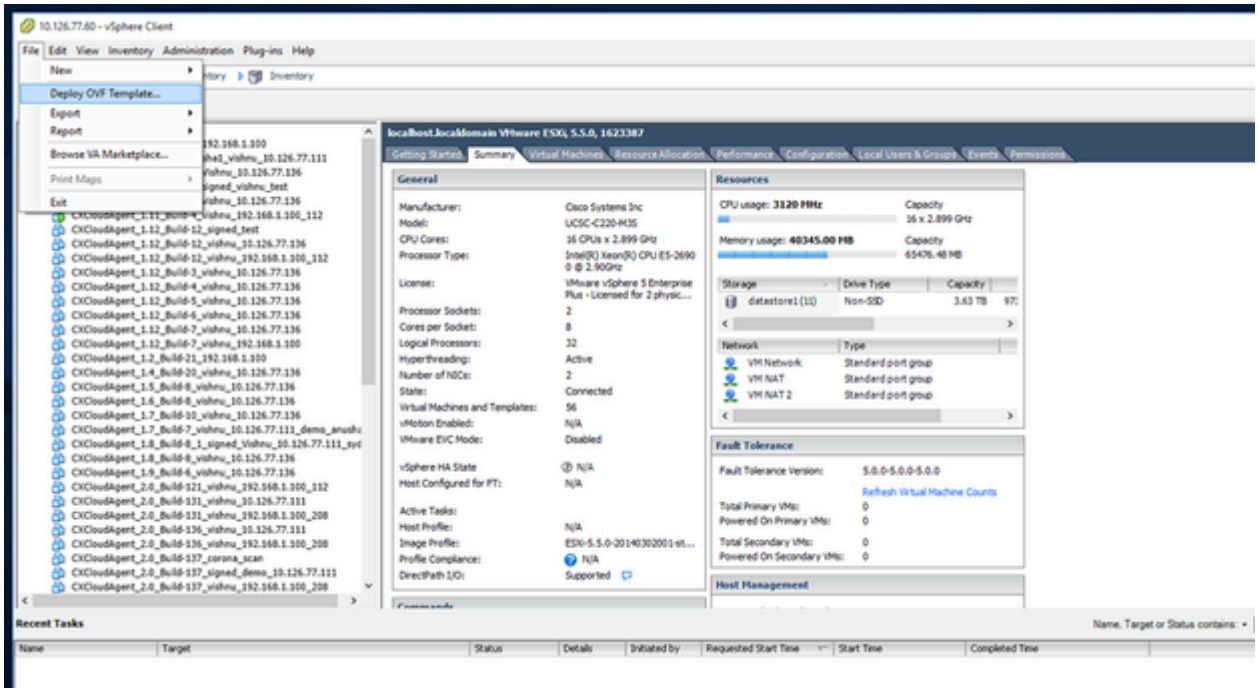
此客户端允许使用vSphere胖客户端部署CX云代理OVA。

1. 下载映像后，启动VMware vSphere客户端并登录。



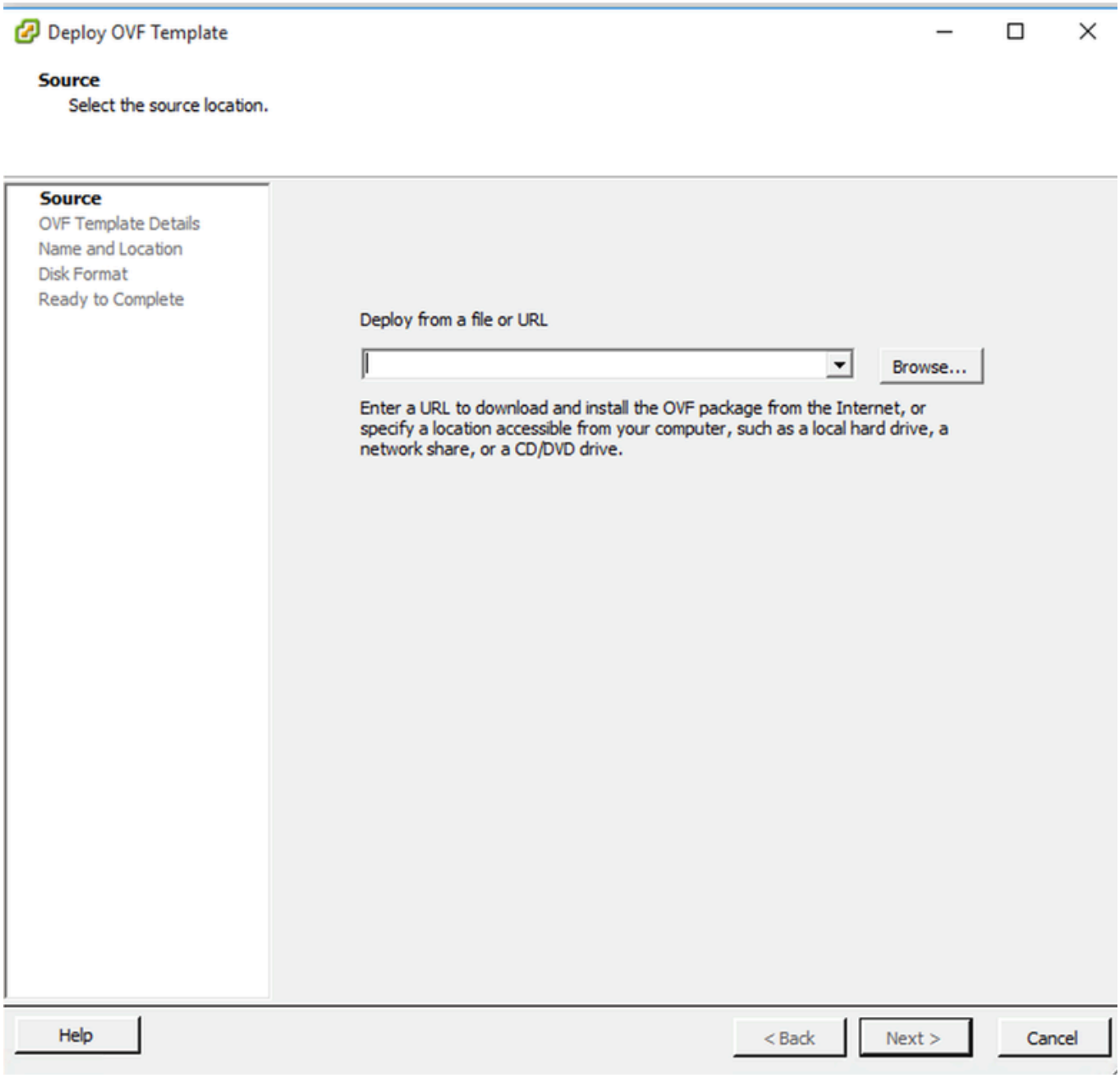
登录

2. 导航至 File > Deploy OVF Template.



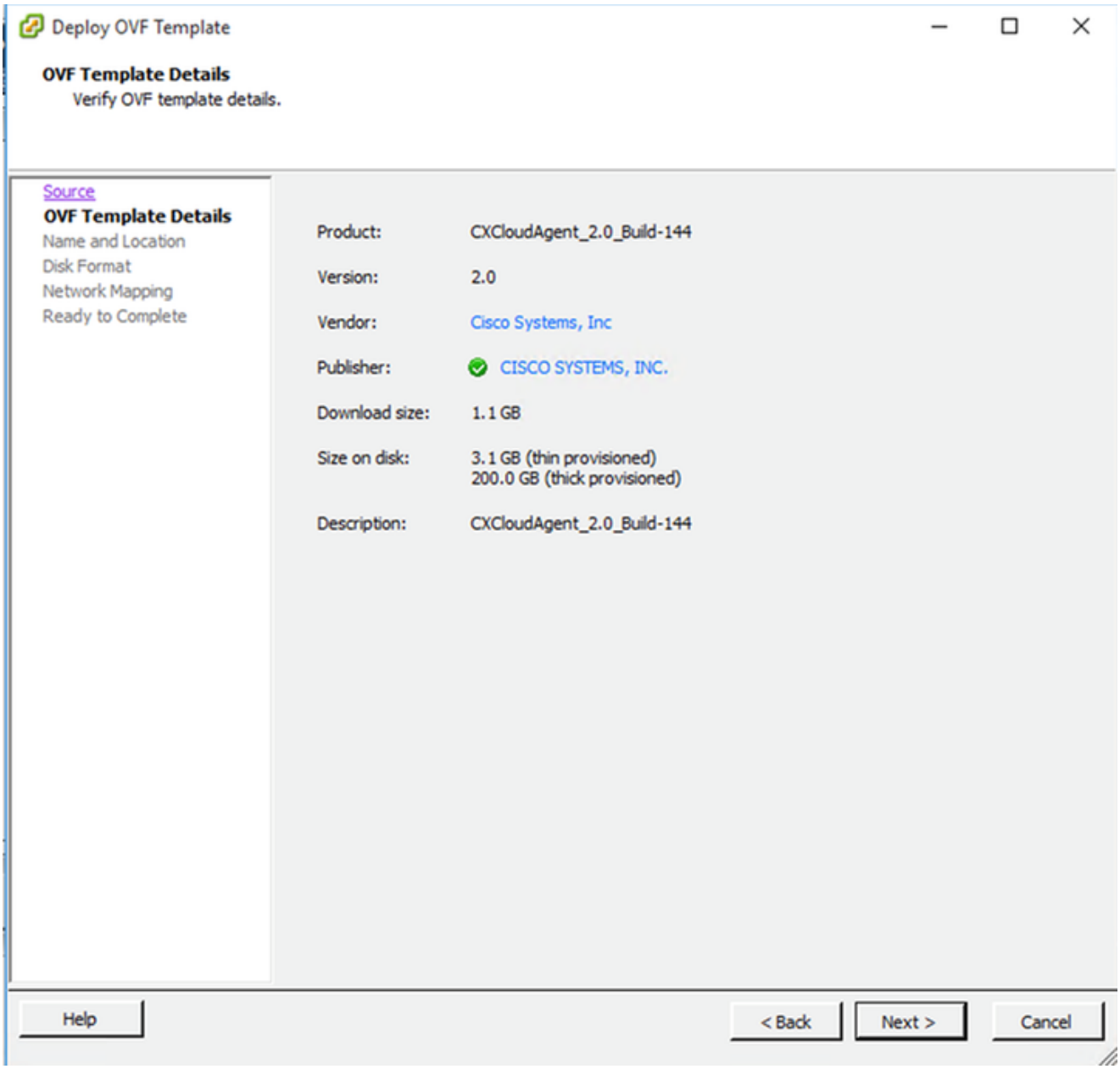
vSphere 客户端

3. 浏览以选择OVA文件，然后点击Next。



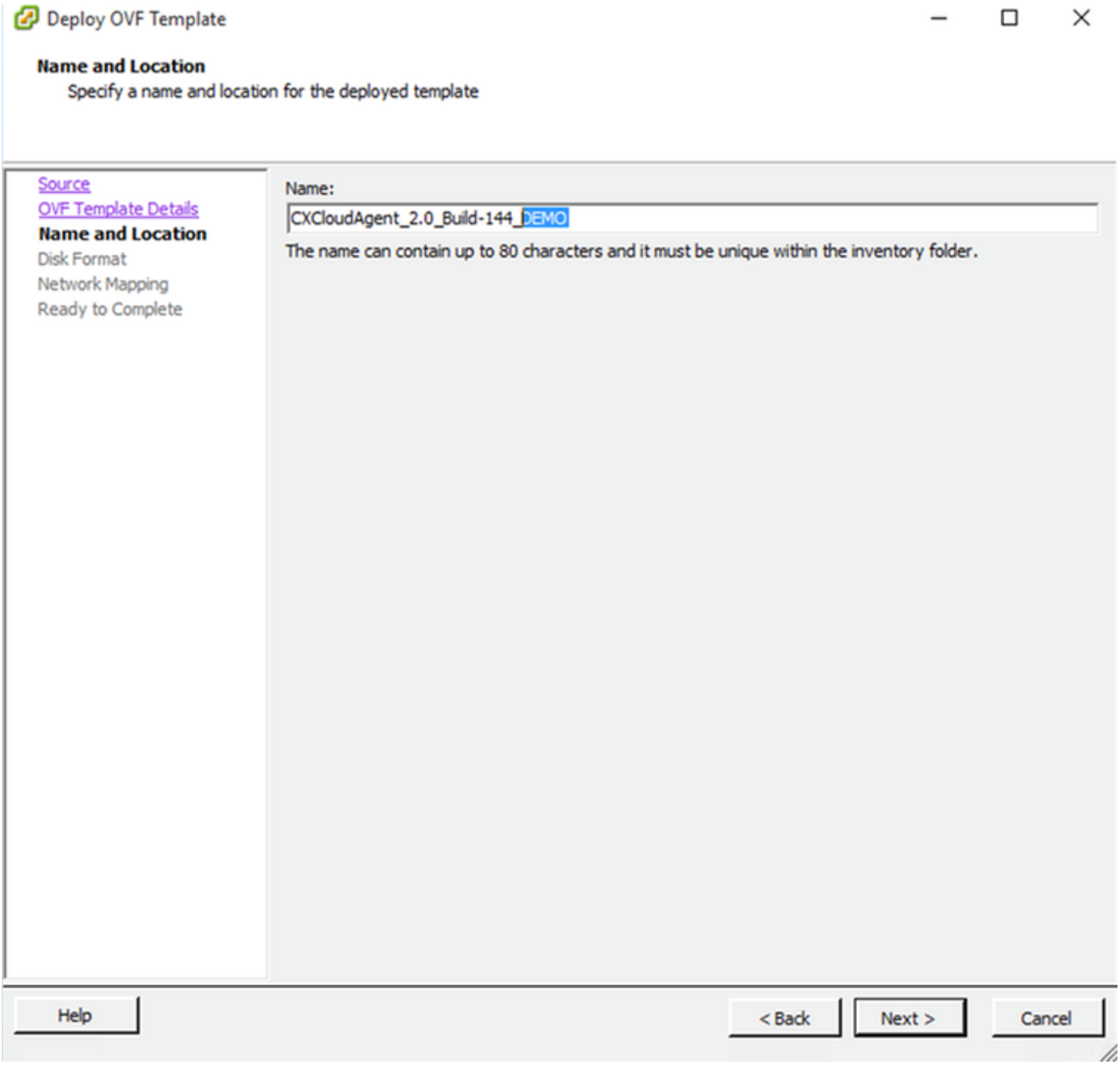
OVA 路径

4. 验证并OVF Details单击Next。



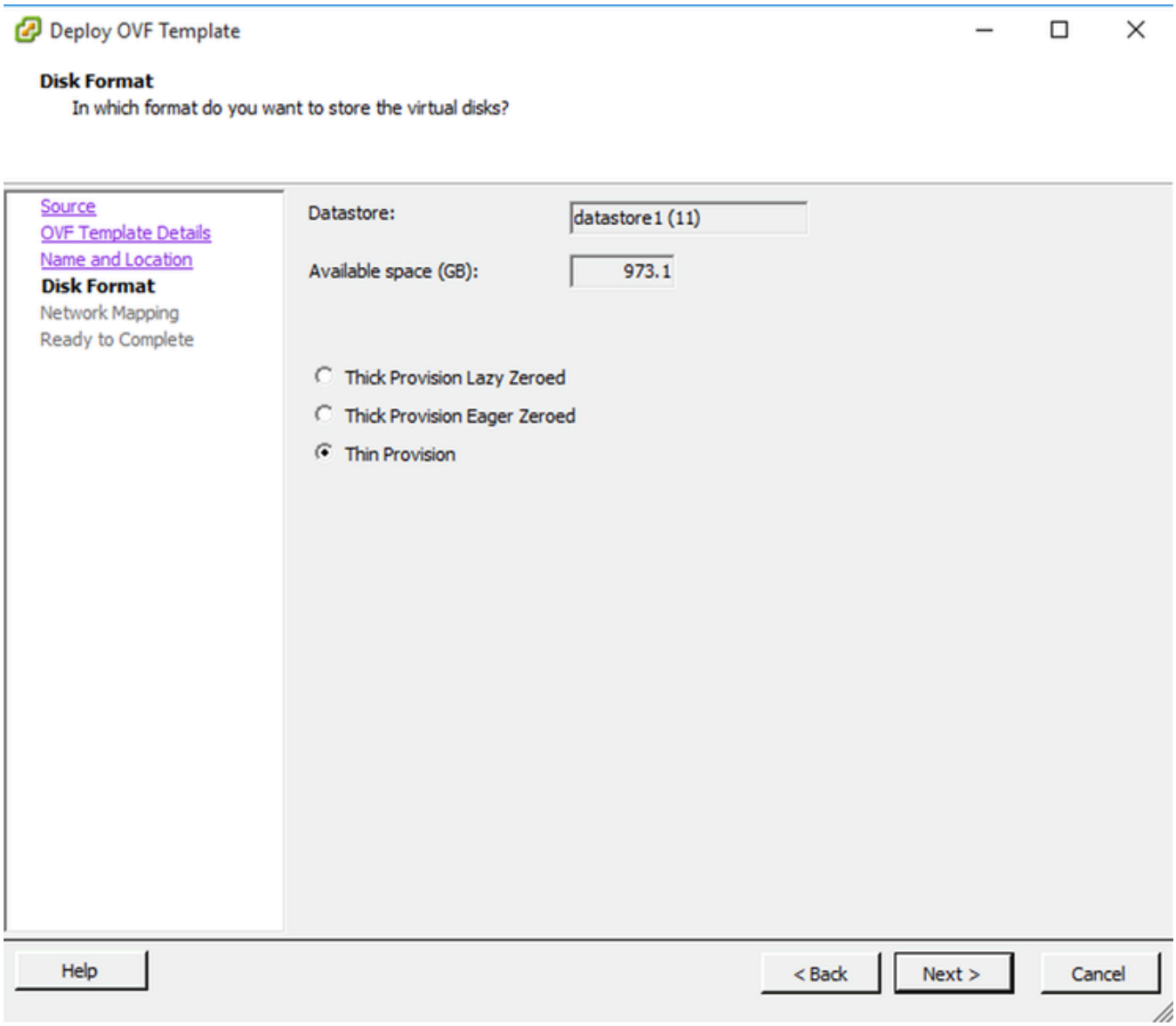
模板详细信息

5. 输入并点击Unique NameNext。



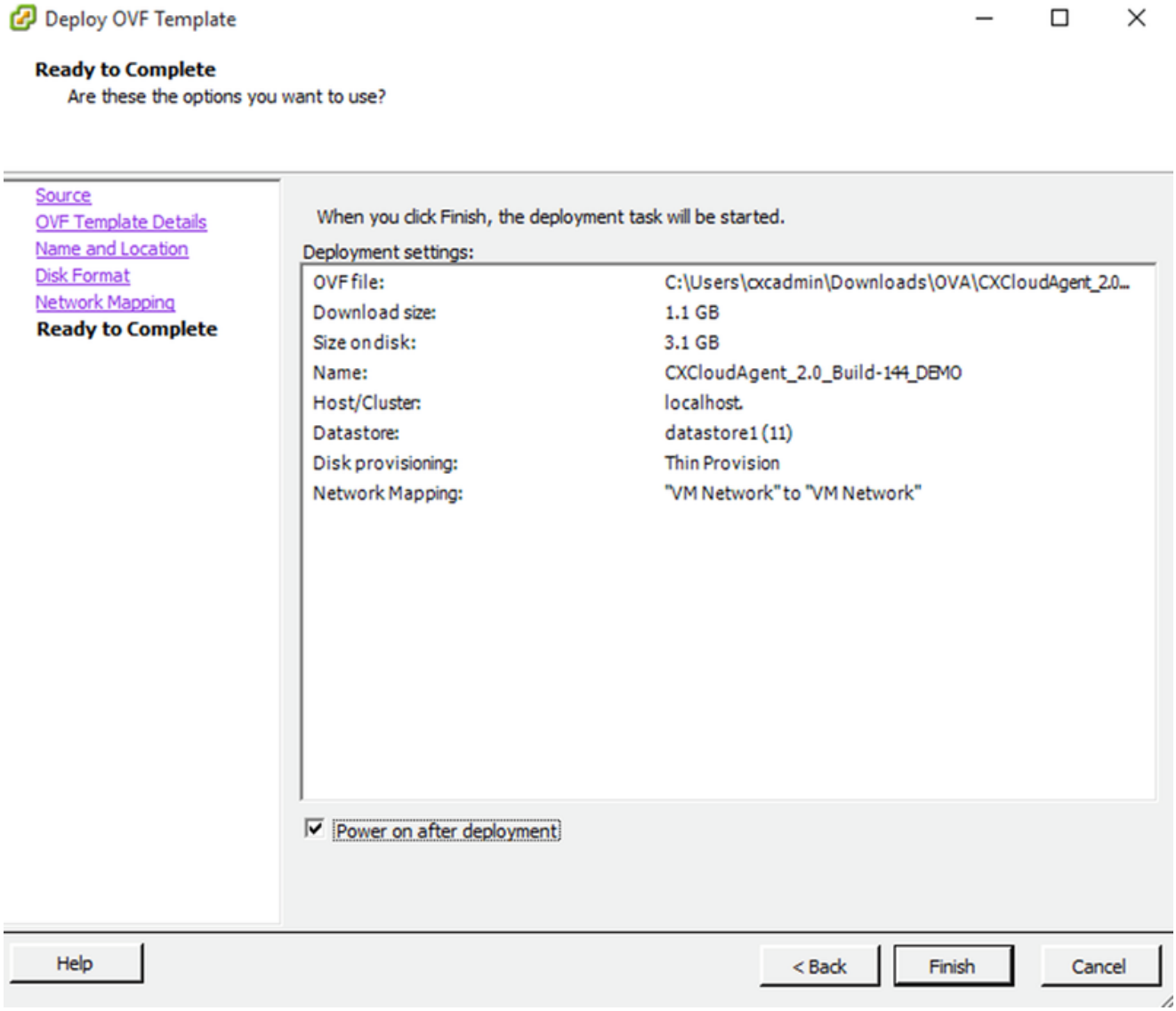
名称和位置

6. 选择一个Disk Format，然后点Next 击（建议使用精简调配）。



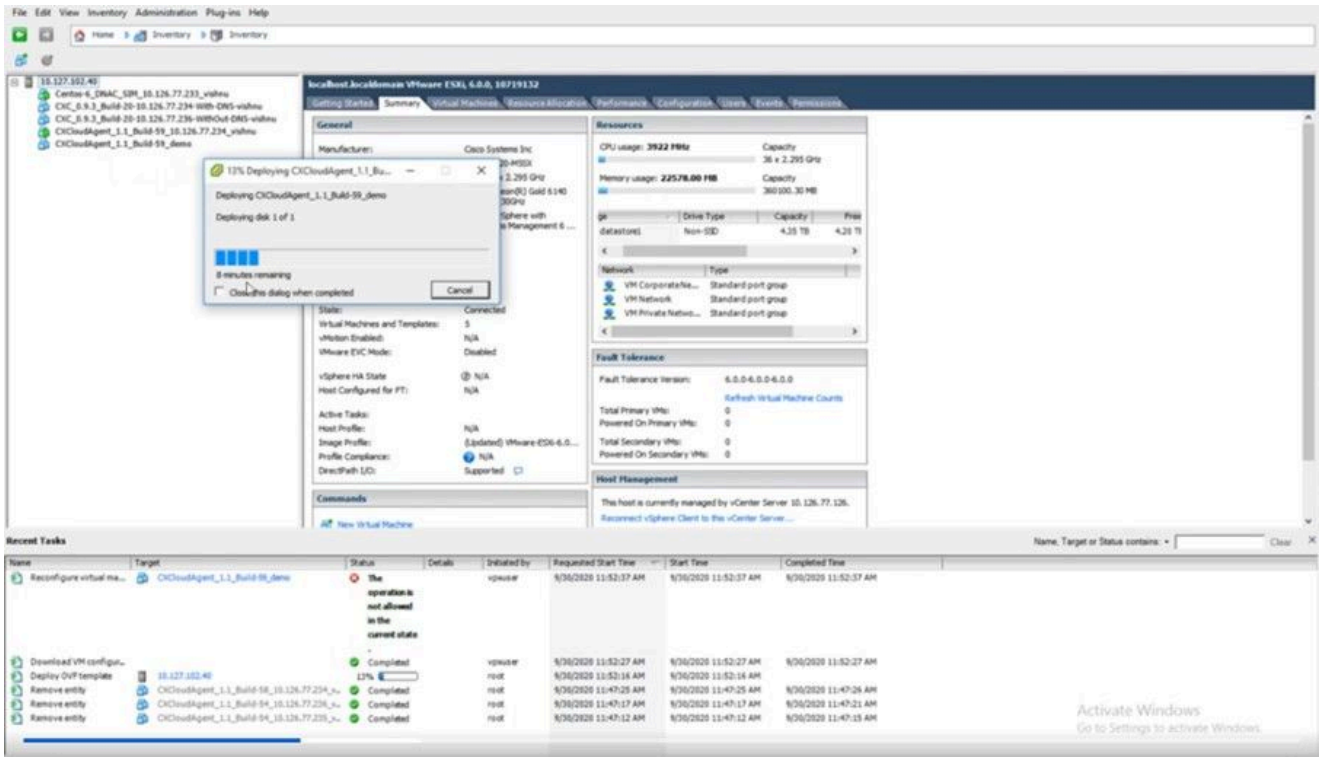
磁盘格式化

7. 选中复选Power on after deployment框，然后点击Finish。

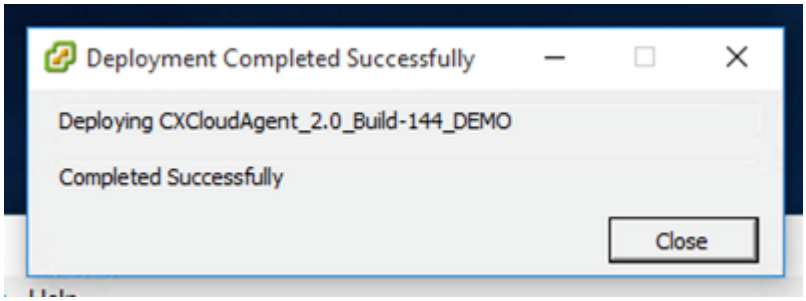


准备完成

部署可能需要几分钟。请等待，直到收到部署成功的消息。



正在部署



已完成部署

8. 选择刚部署的VM，打开控制台并转至Network Configuration。

Web 客户端 ESXi 6.0 安装

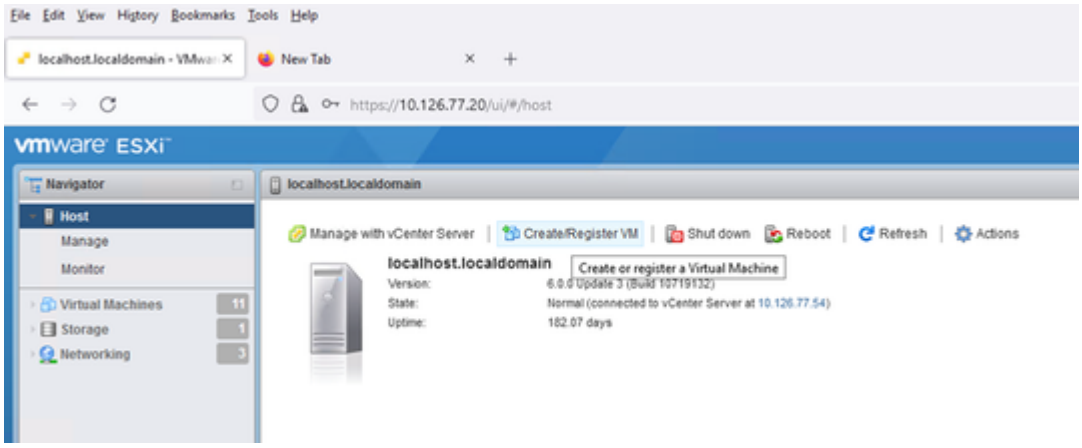
此客户端使用vSphere Web部署CX云代理OVA。

1. 使用用于部署VM的ESXi/虚拟机监控程序凭证登录到VMWare UI。

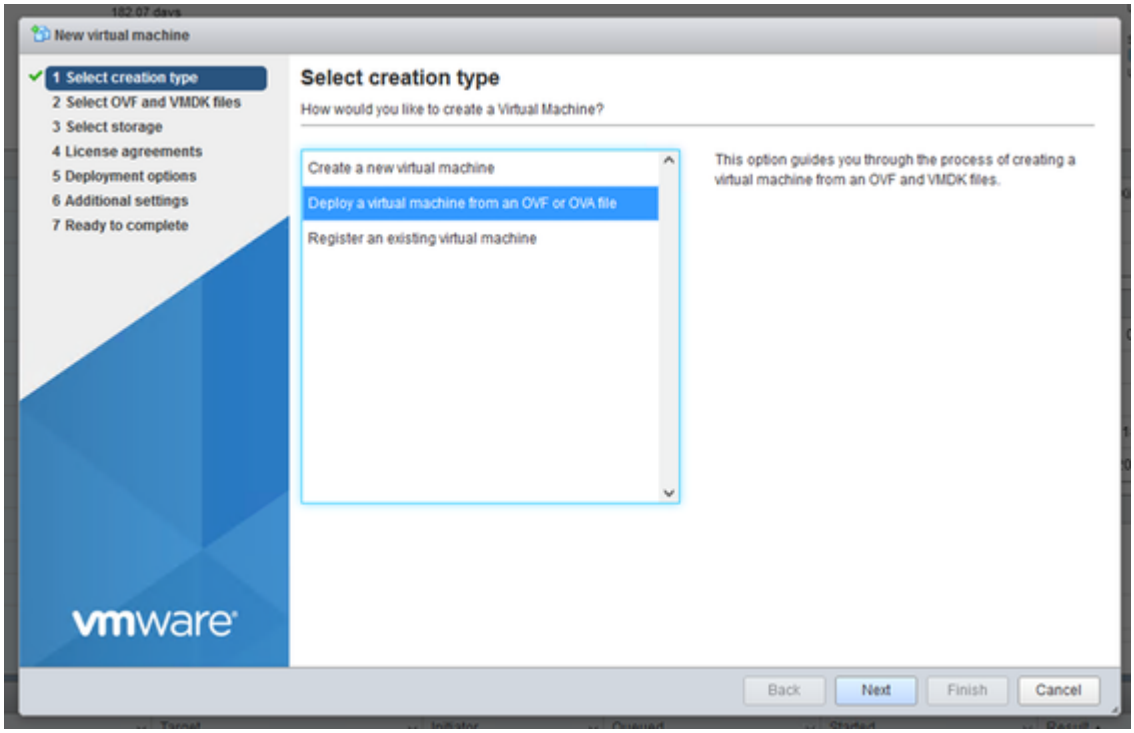


VMware ESXi 登录

2. 选择.Virtual Machine > Create / Register VM

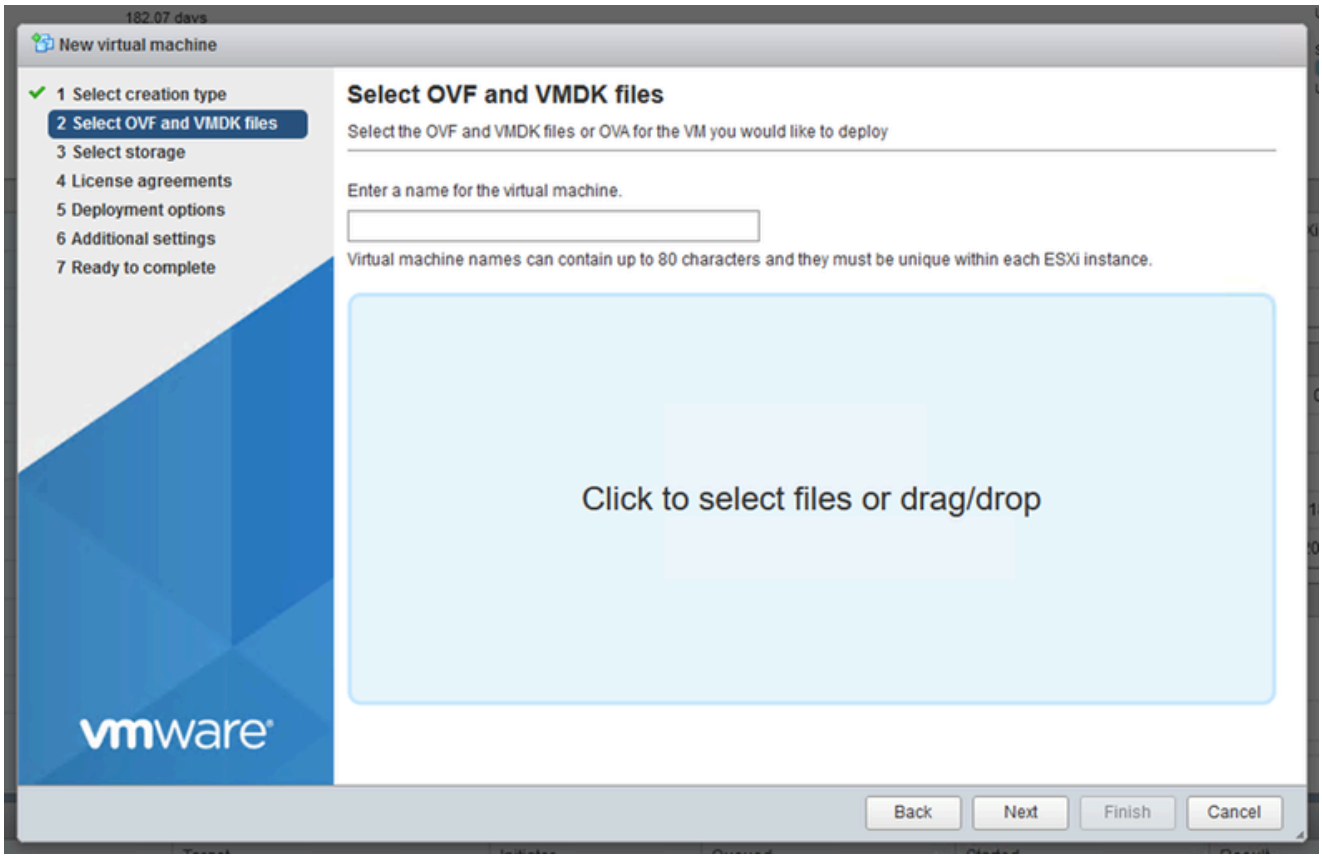


创建 VM



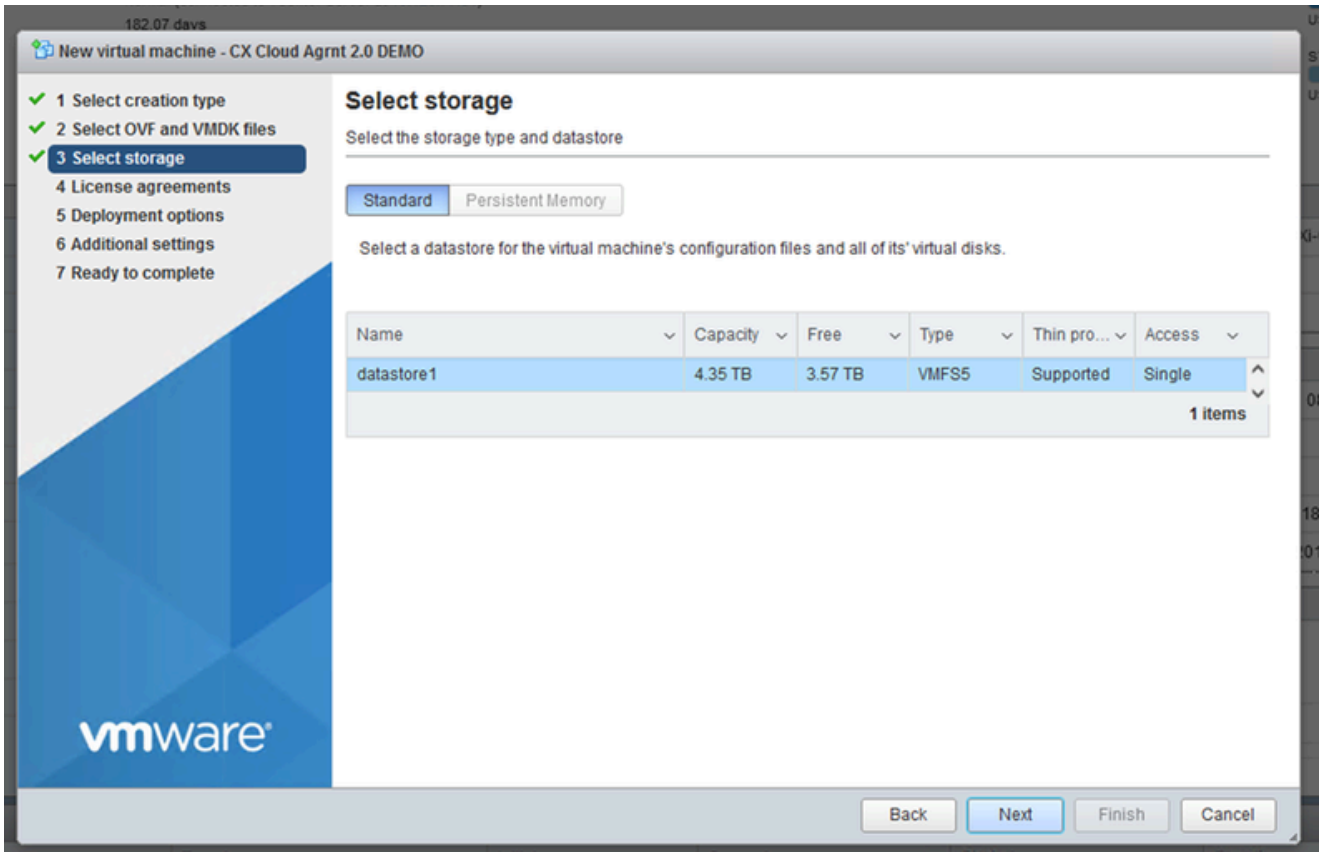
OVA 部署

3. 选择Deploy a virtual machine from an OVF or OVA file ，然后单击Next。
4. 输入虚拟机的名称，浏览以选择文件，或者拖放下载的OVA文件。
5. 单击。Next

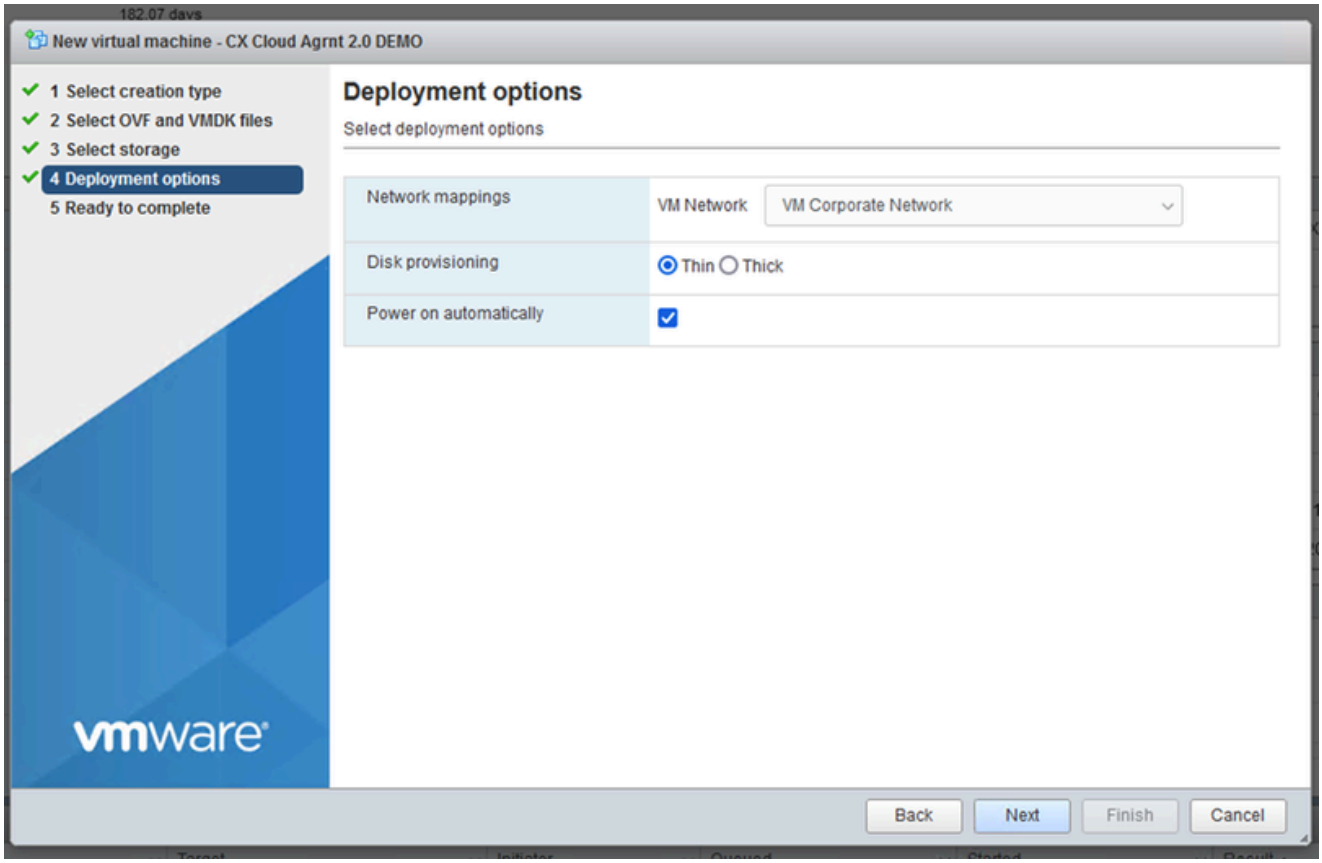


OVA 选择

6. 选择Standard Storage ，然后单击Next。

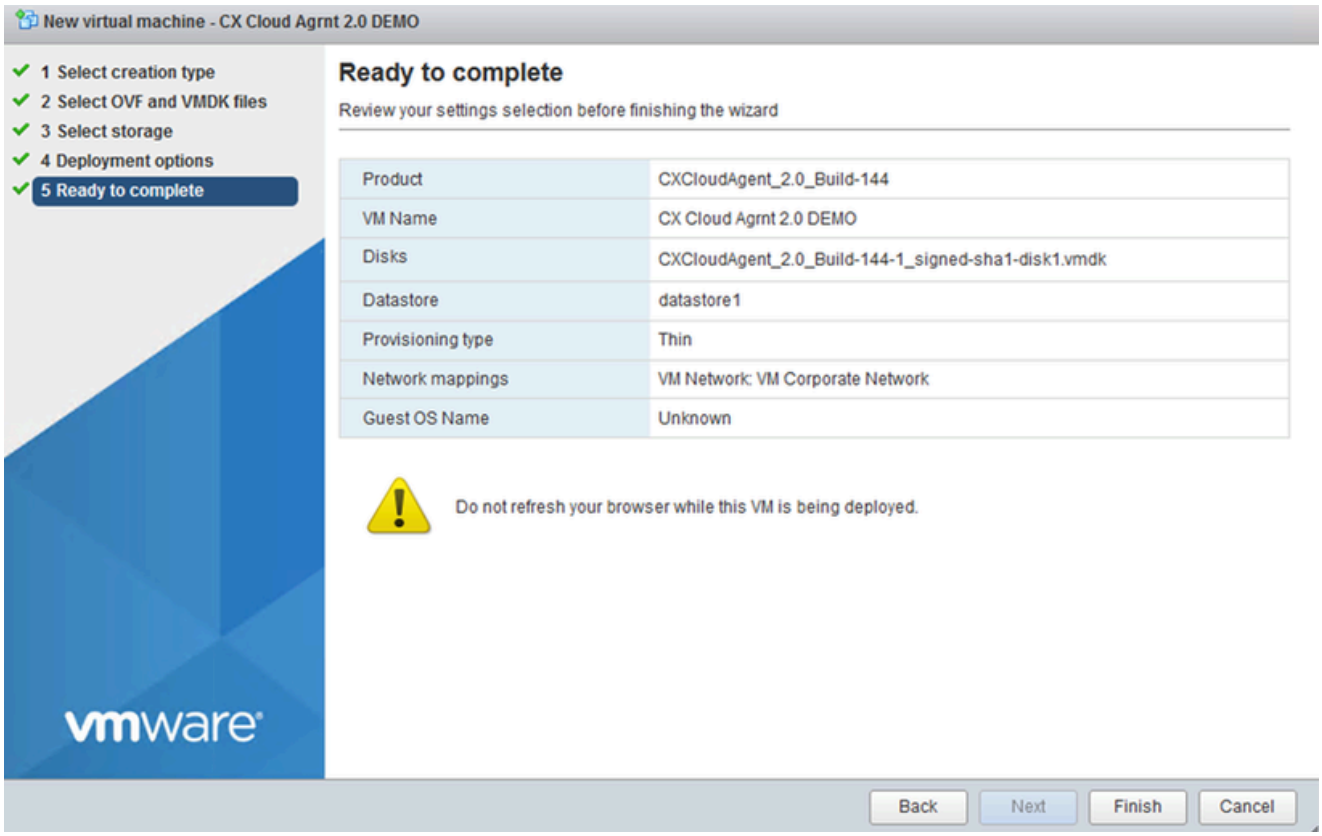


选择存储

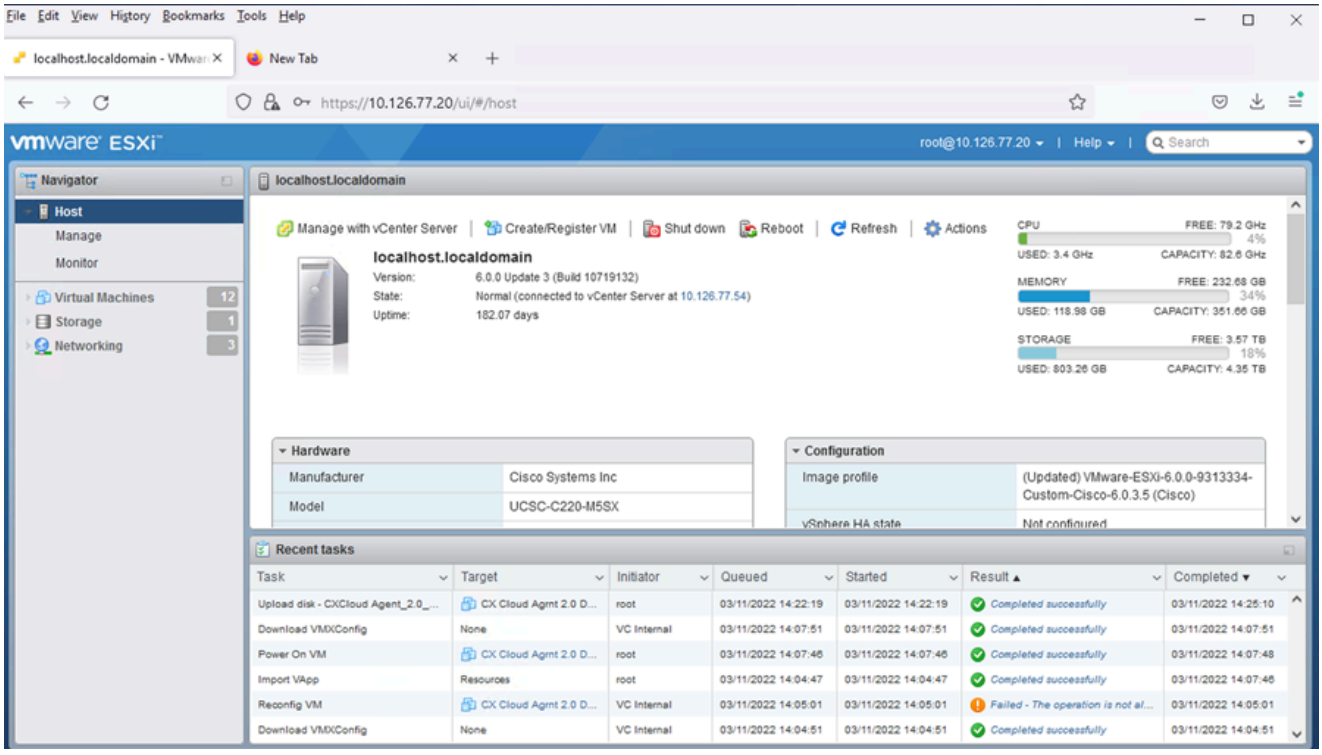


部署选项

7. 选择适当的部署选项并点击Next。

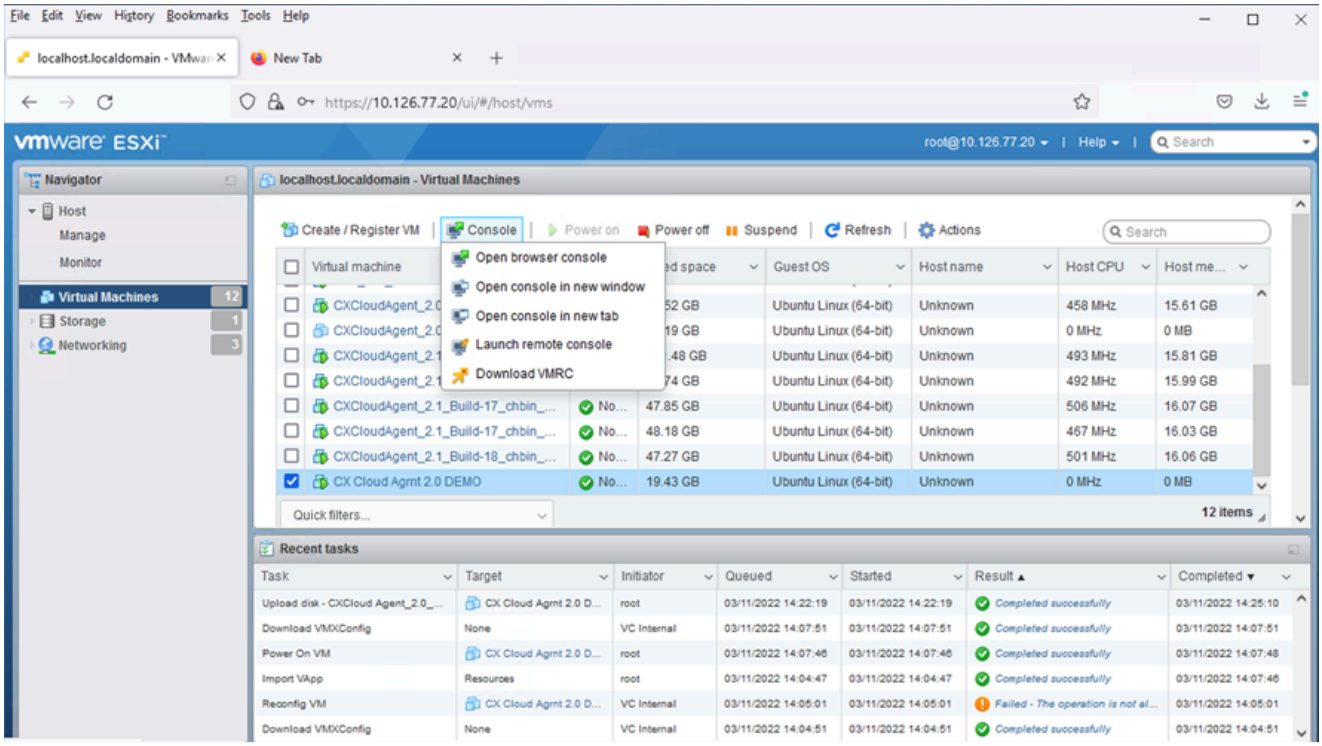


准备完成



成功完成

8. 检查设置并单击Finish。
9. 选择刚部署的VM并选择Console > Open browser console。



打开控制台

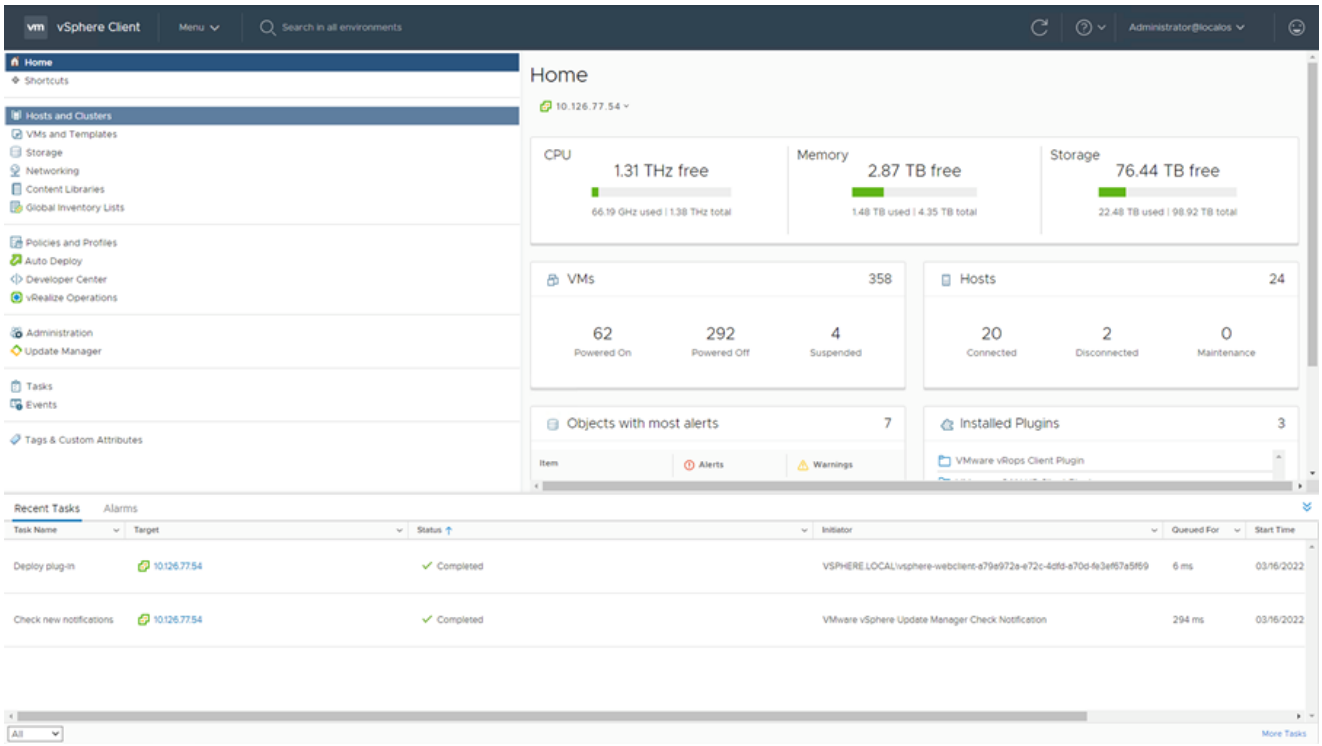
10. 导航至网络配置。

Web 客户端 vCenter 安装

1. 使用ESXi/虚拟机监控程序凭证登录vCenter客户端。

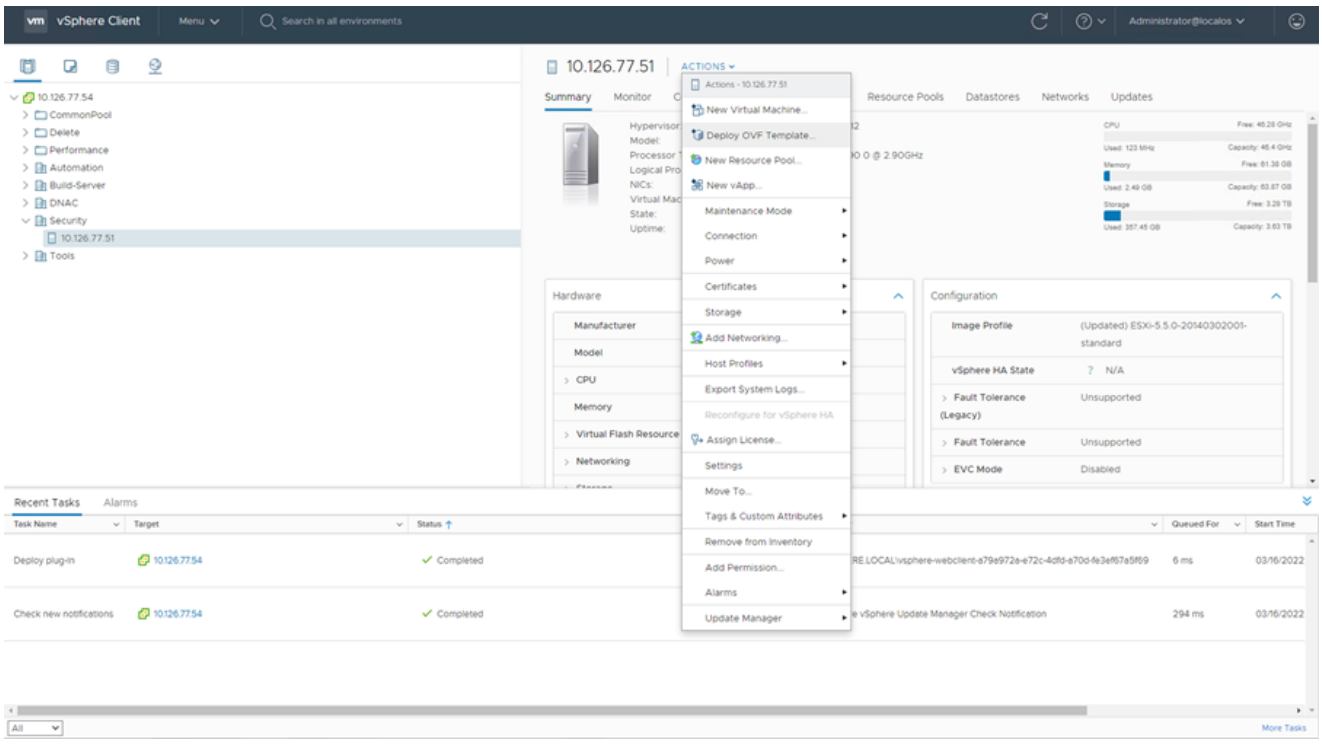


登录

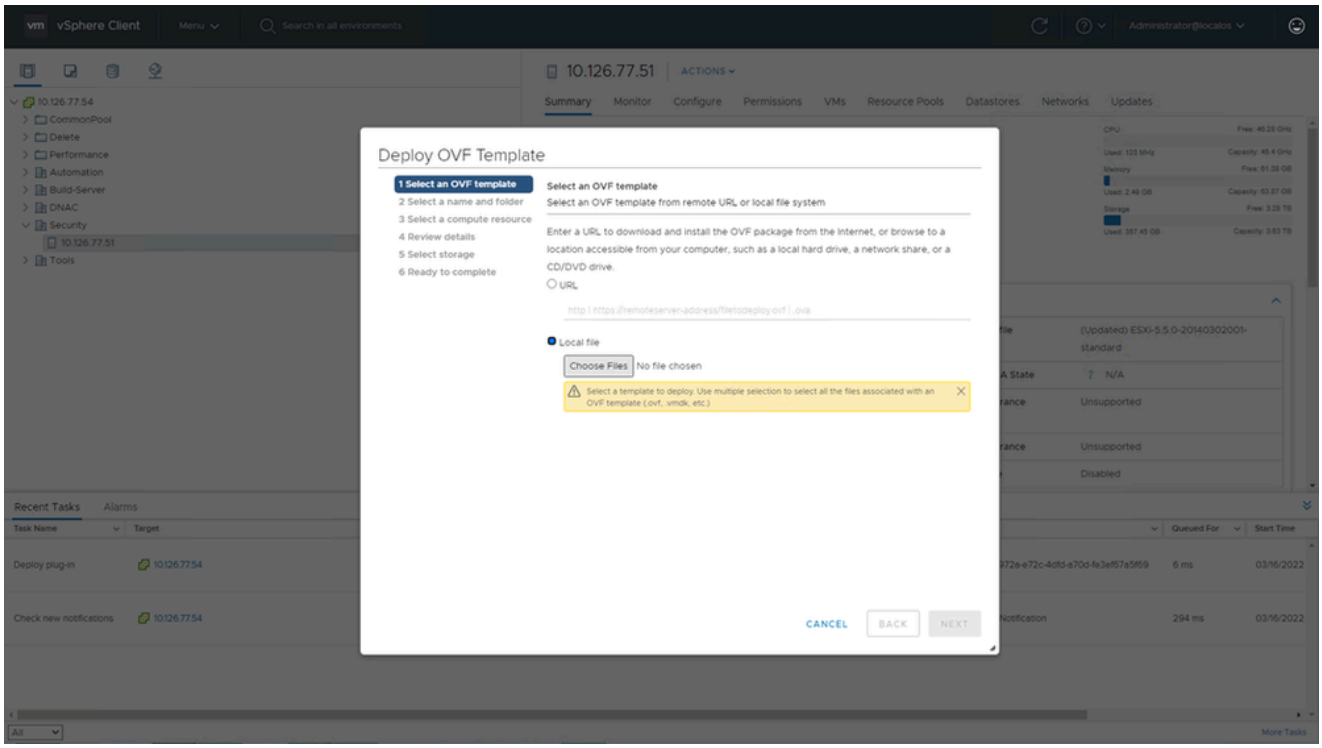


主页屏幕

2. 在主页上单击Hosts and Clusters。
3. 选择VM并点击Action > Deploy OVF Template。

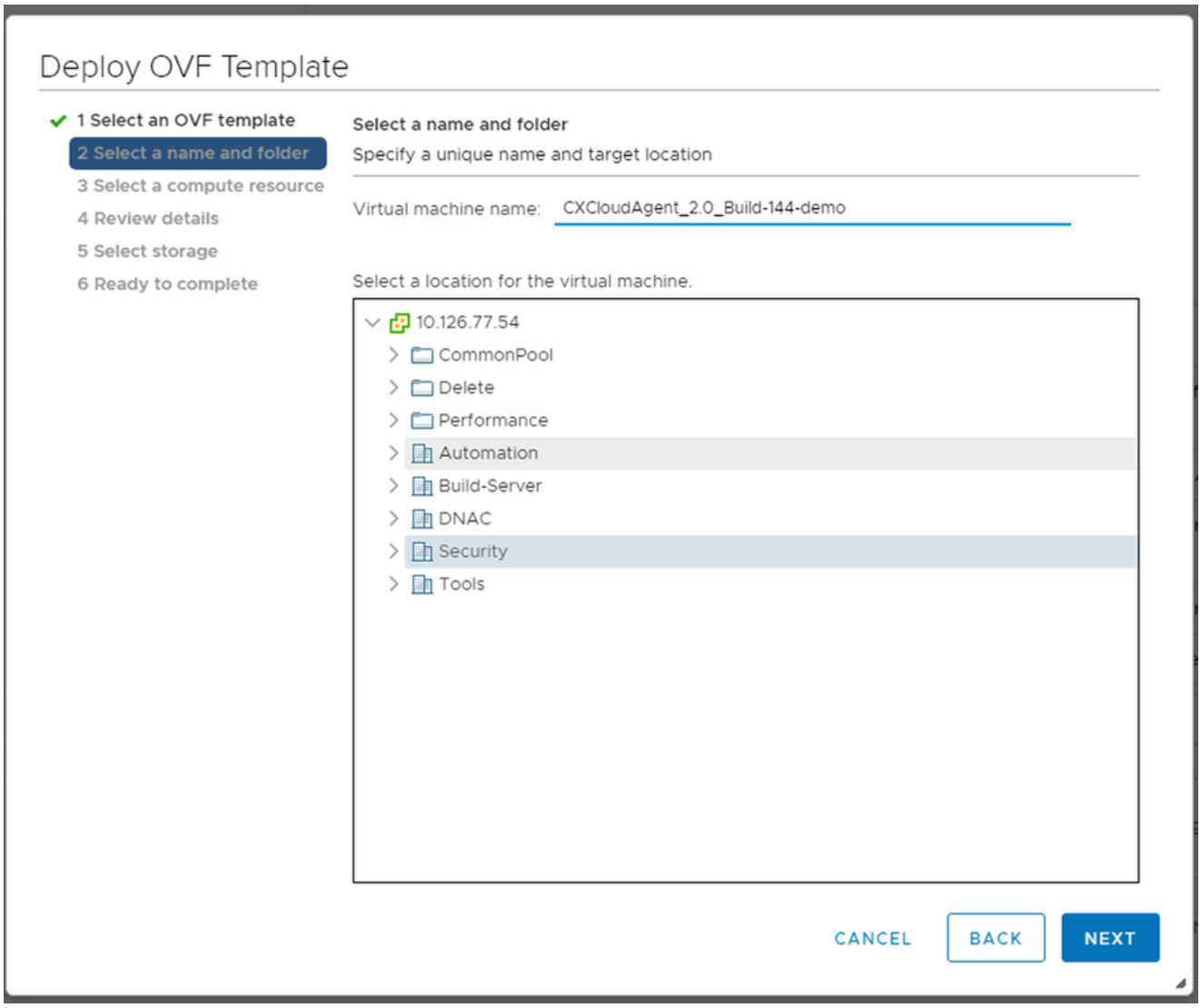


操作



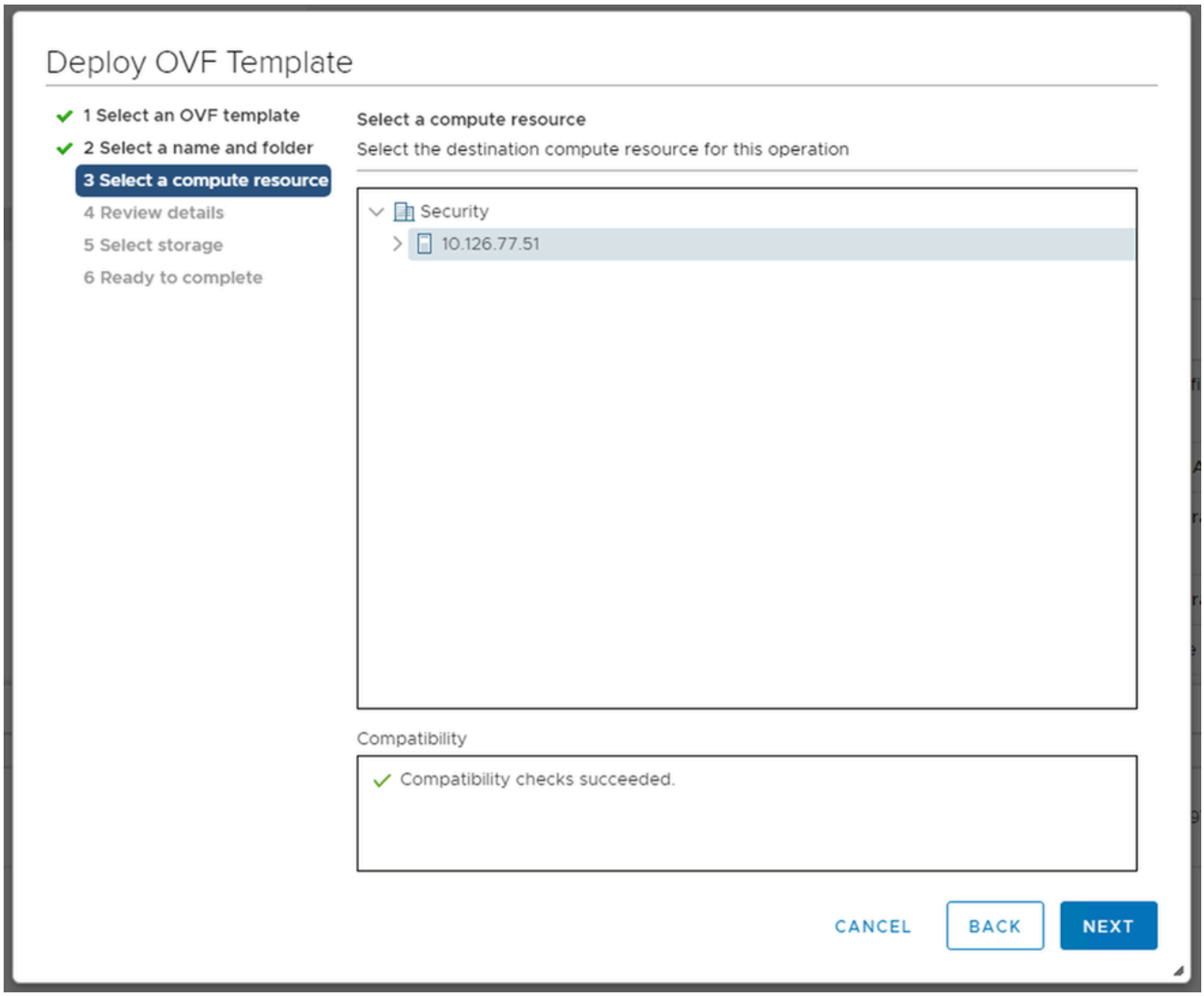
选择模板

4. 直接添加URL或浏览以选择OVA文件并点击Next。
5. 输入唯一的名称，并在需要时浏览到该位置。
6. 单击。Next



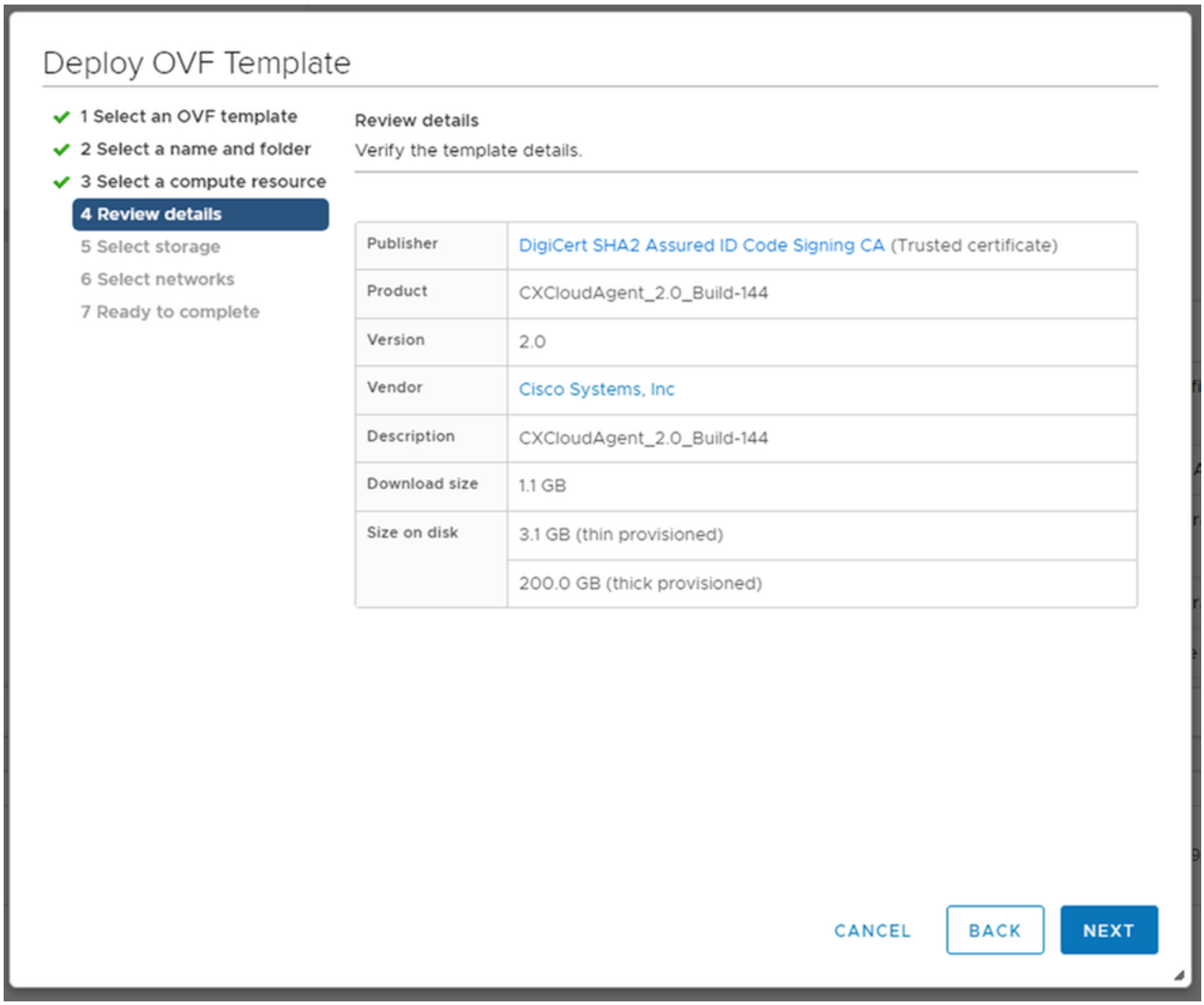
名称和文件夹

7. 选择计算资源并单击Next。



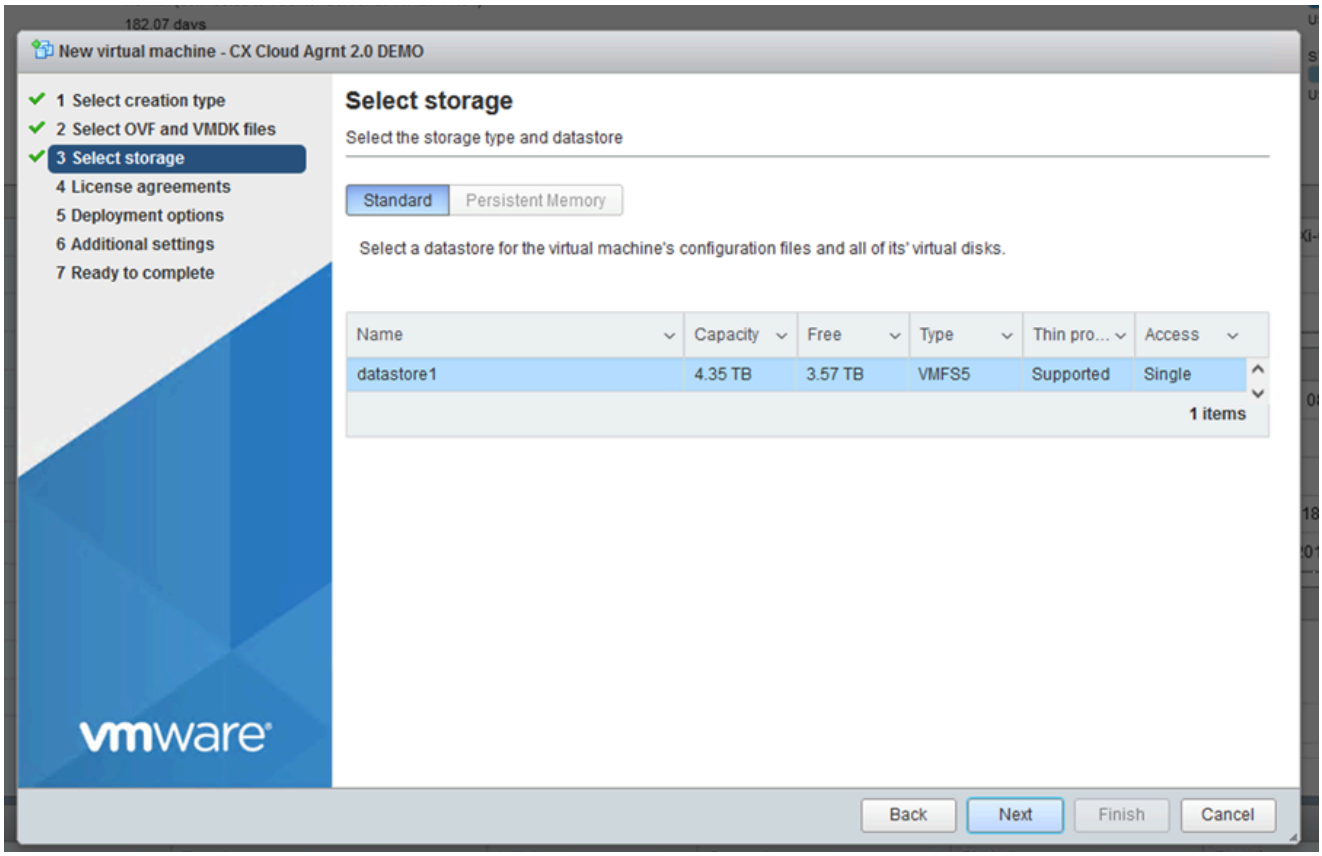
选择计算资源

8. 查看详细信息并点击Next。



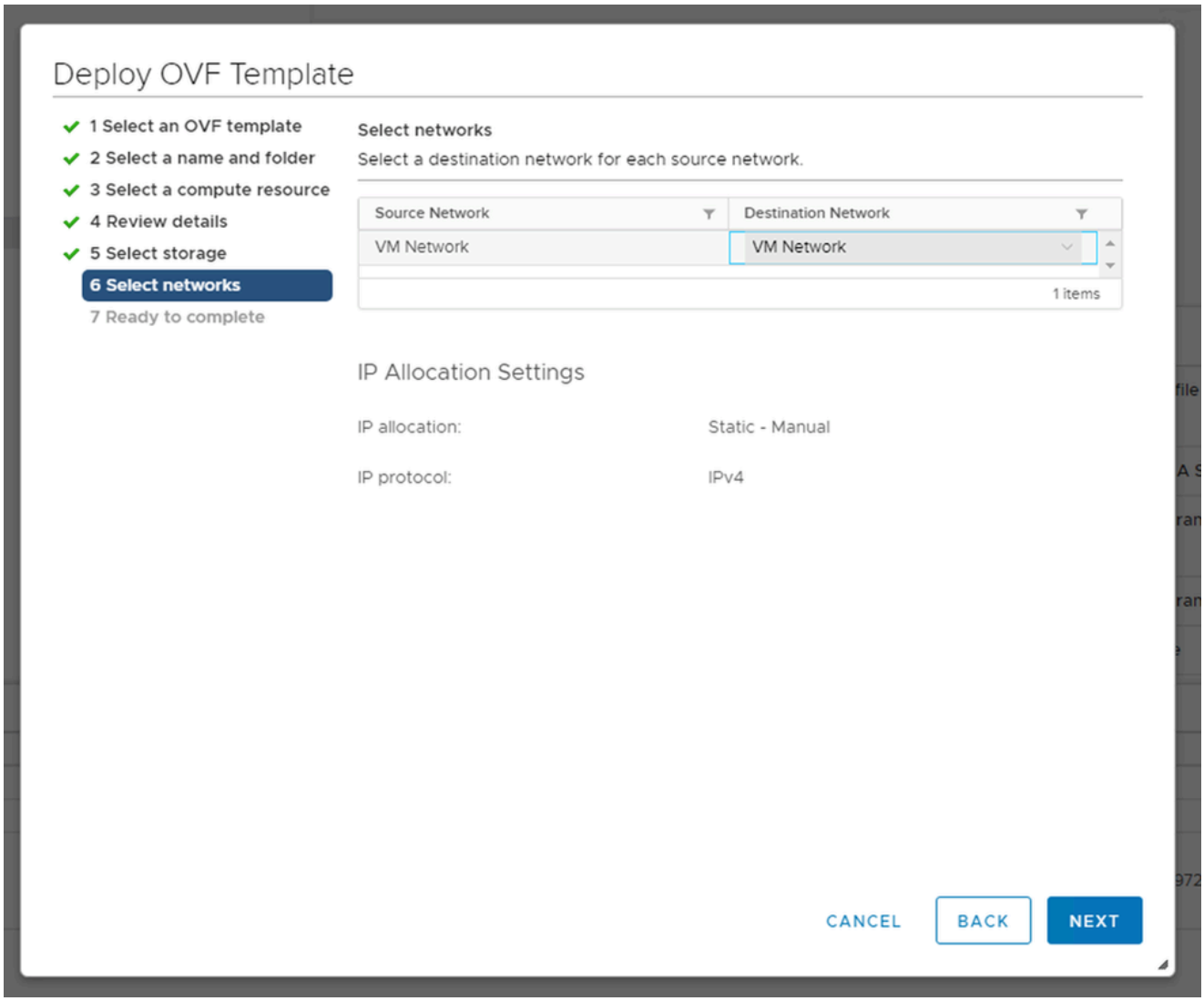
检查详细信息

9. 选择虚拟磁盘格式并单击Next。



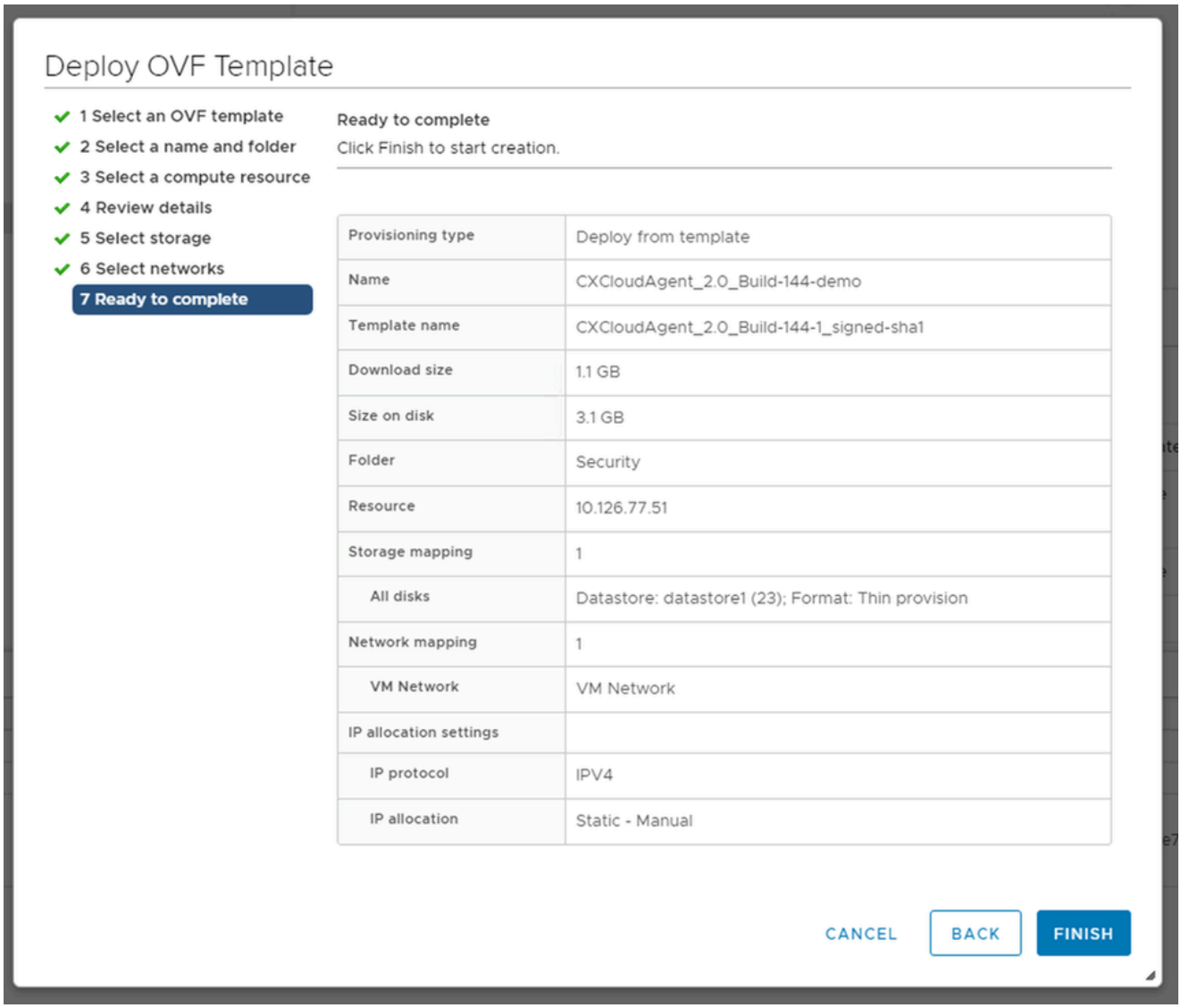
选择存储

10. 单击。Next



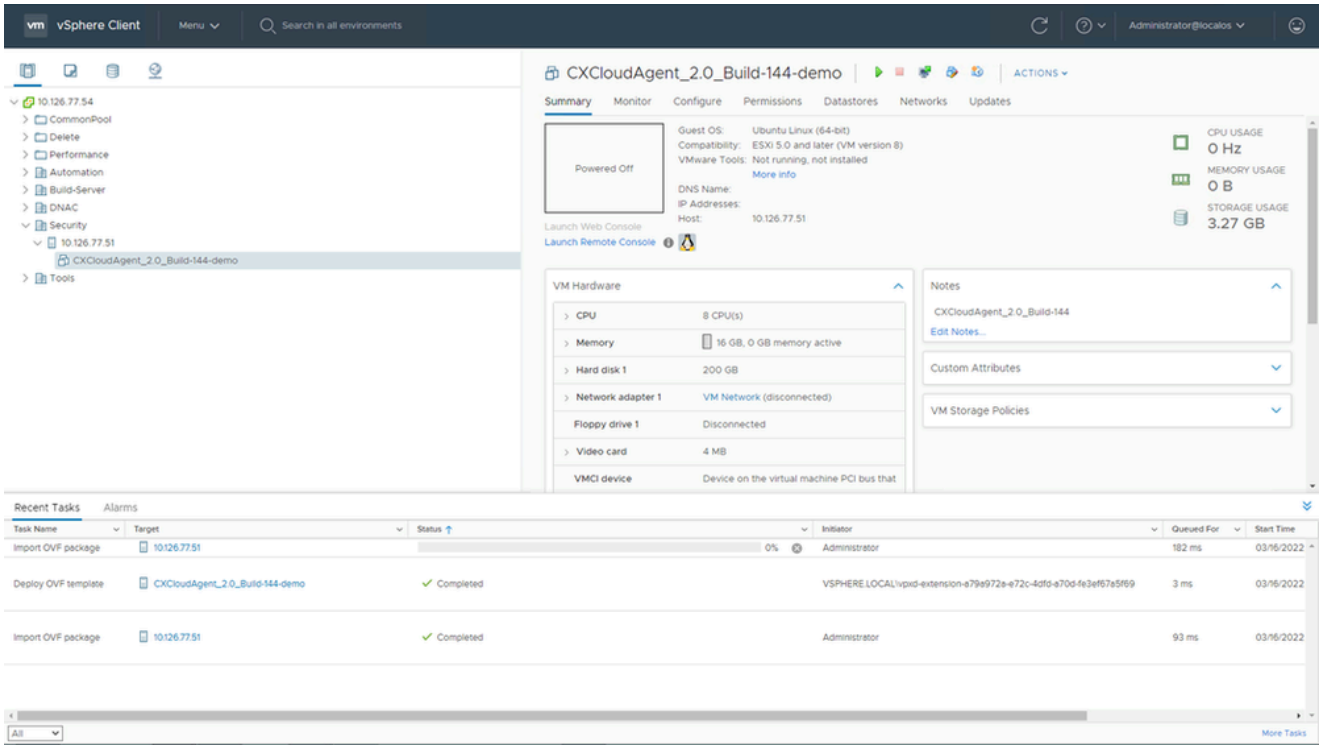
选择网络

11. 单击。Finish



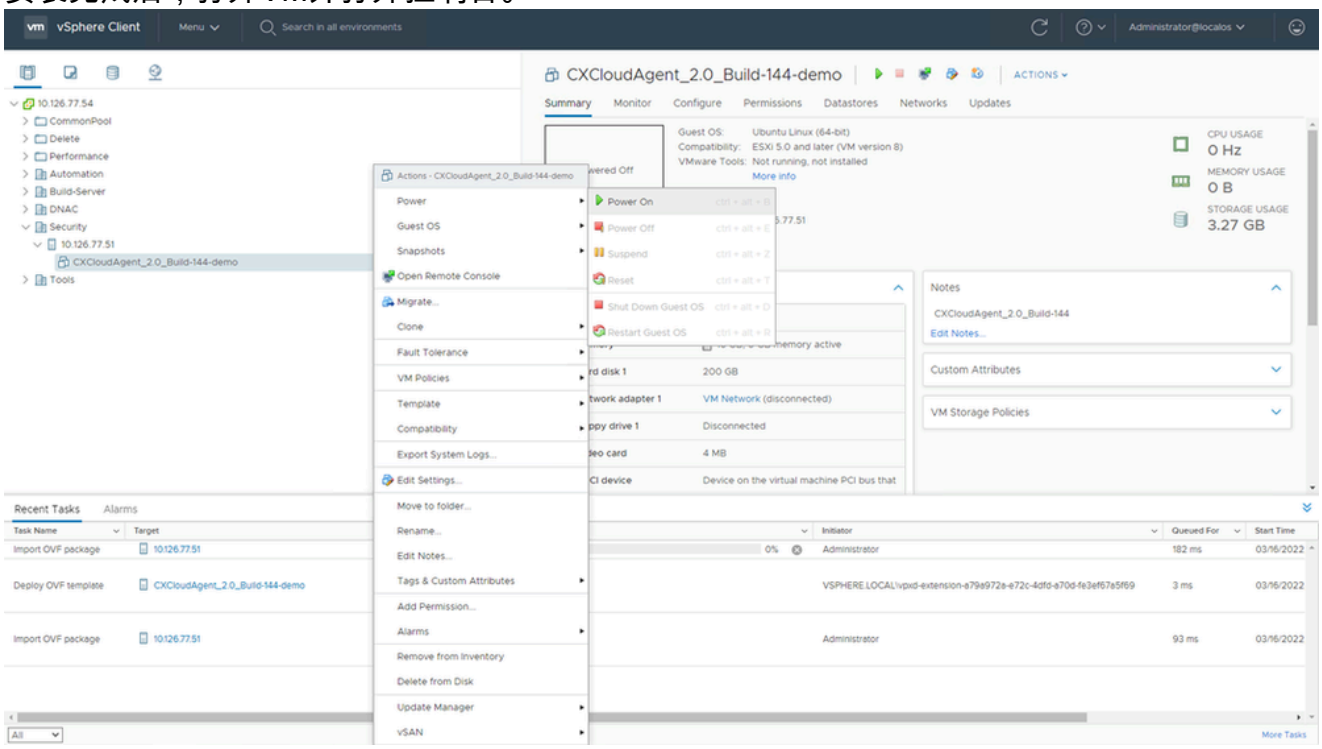
准备完成

12. 添加了一个新VM。单击其名称查看状态。



已添加VM

13. 安装完成后，打开VM并打开控制台。



打开控制台

14. 导航至网络配置。

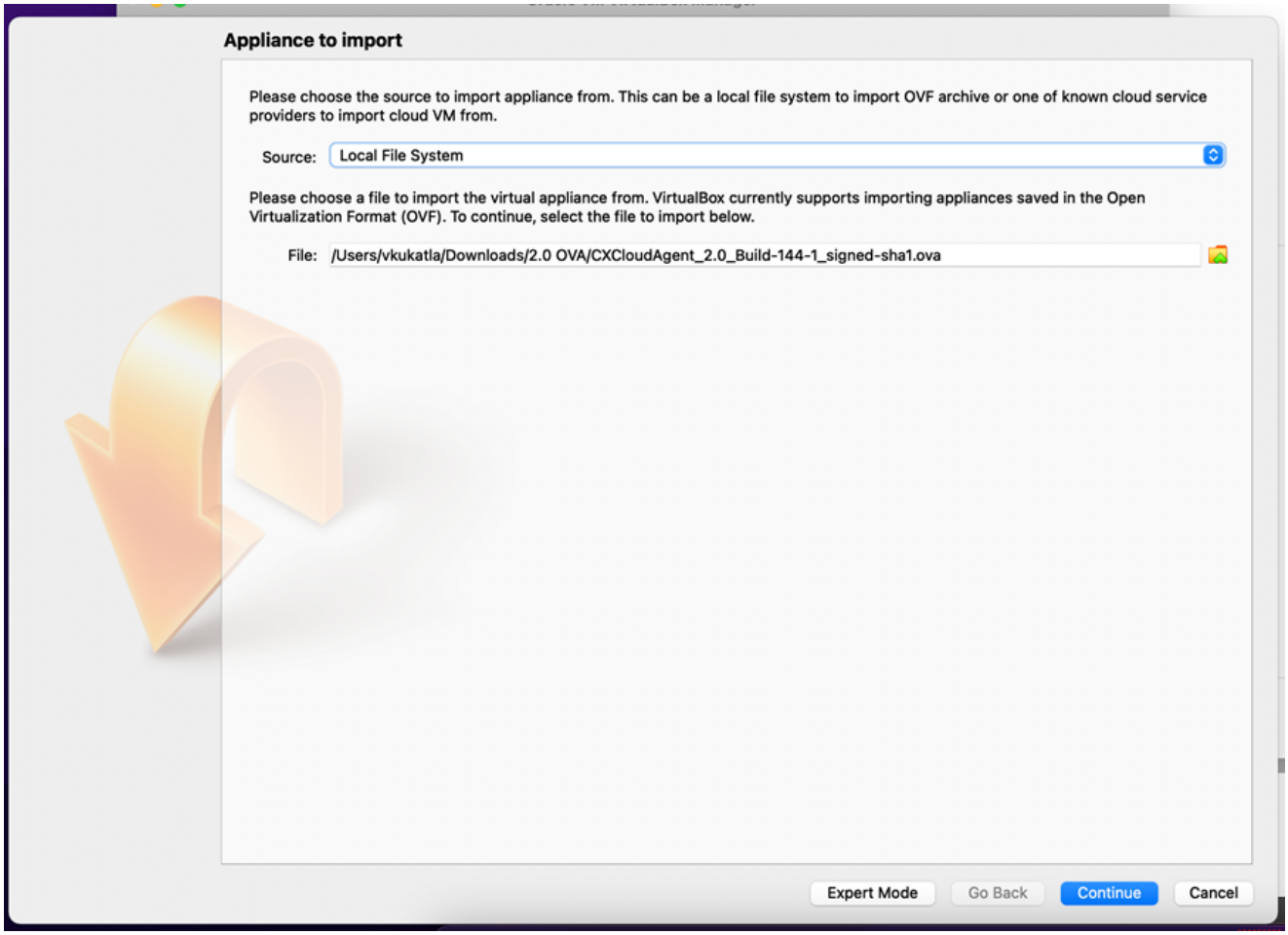
Oracle Virtual Box 5.2.30 安装

此客户端通过Oracle虚拟盒部署CX云代理OVA。



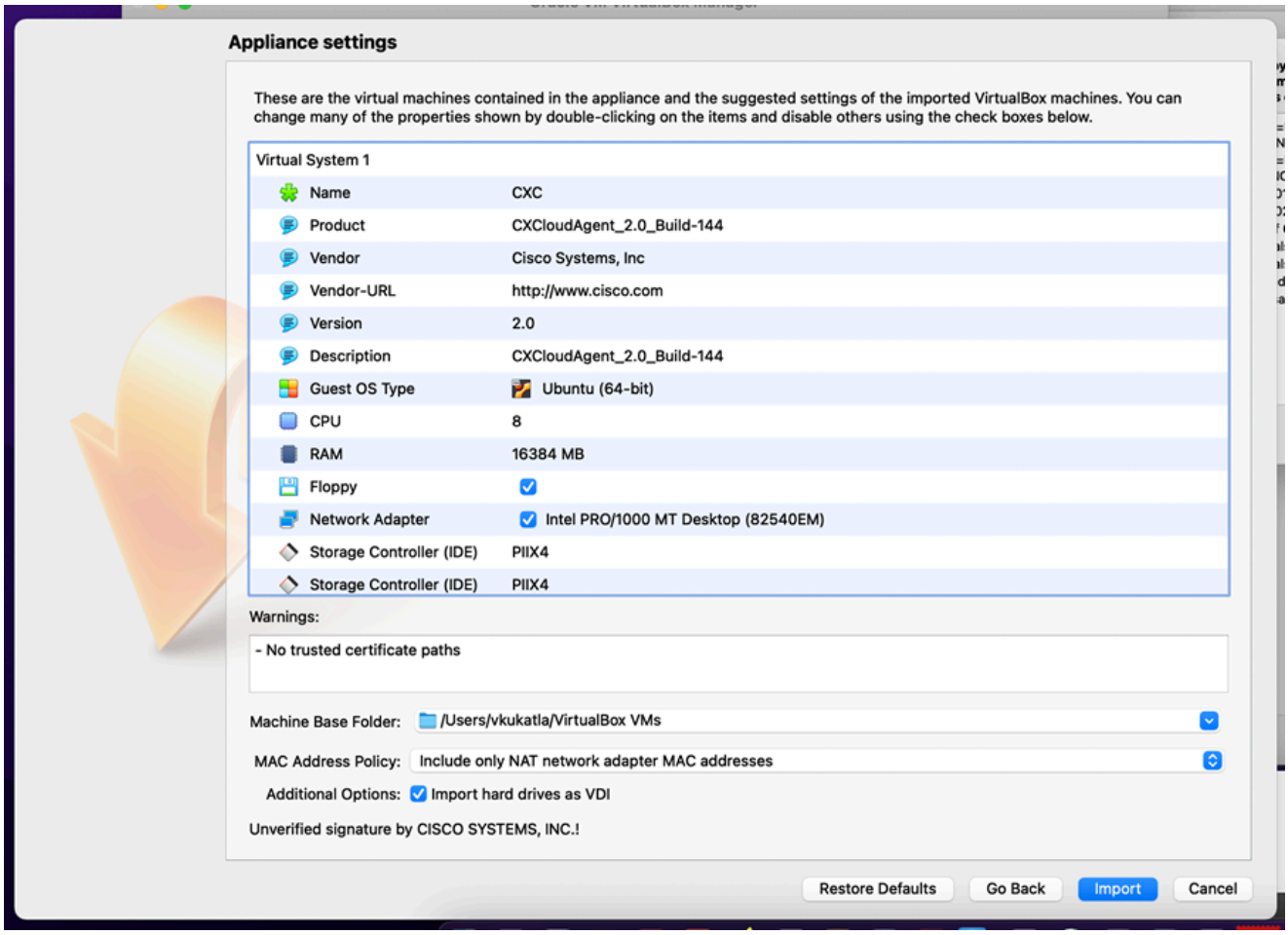
Oracle VM

1. 打开Oracle VM UI并选择File > Import Appliance。
2. 浏览以导入 OVA 文件。



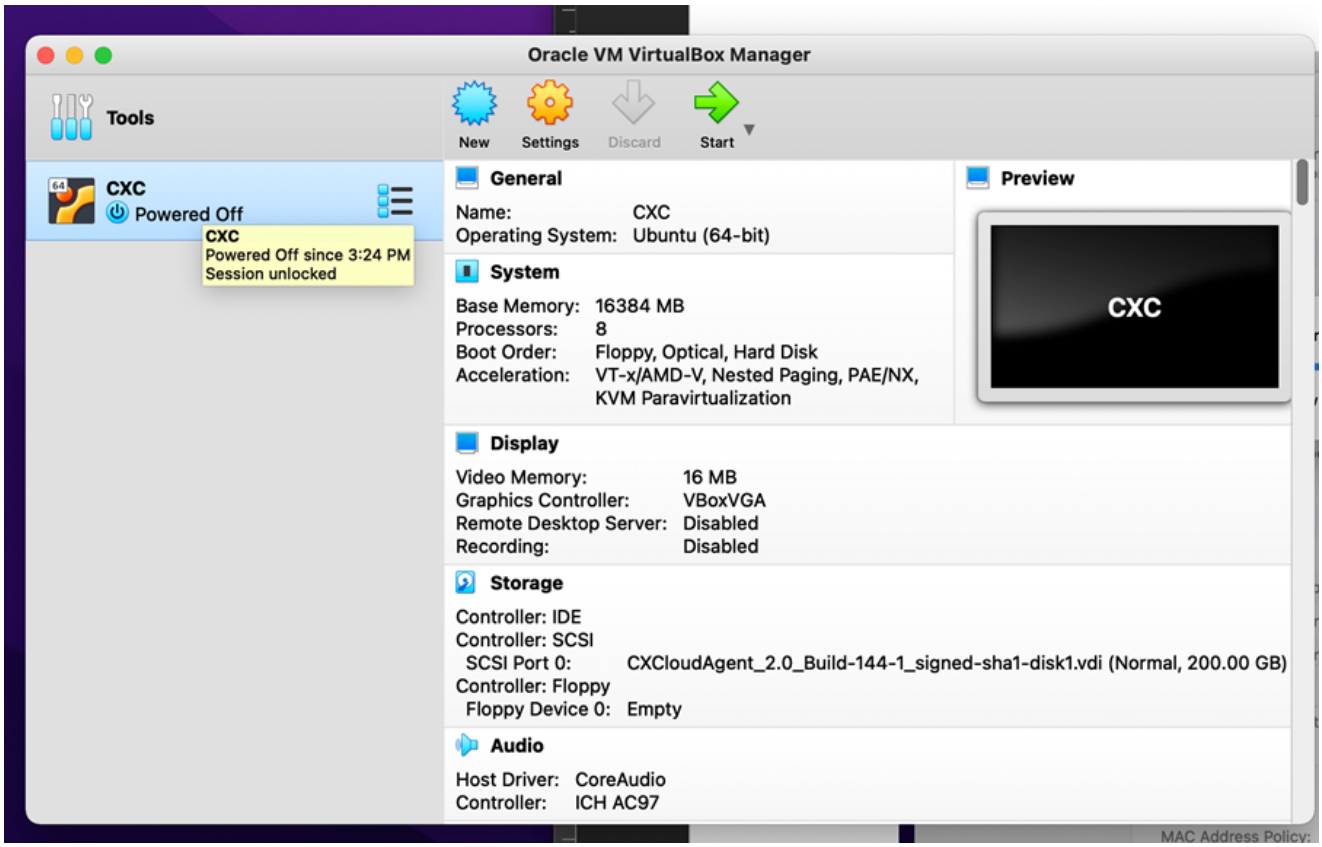
选择文件

3. 单击。Import

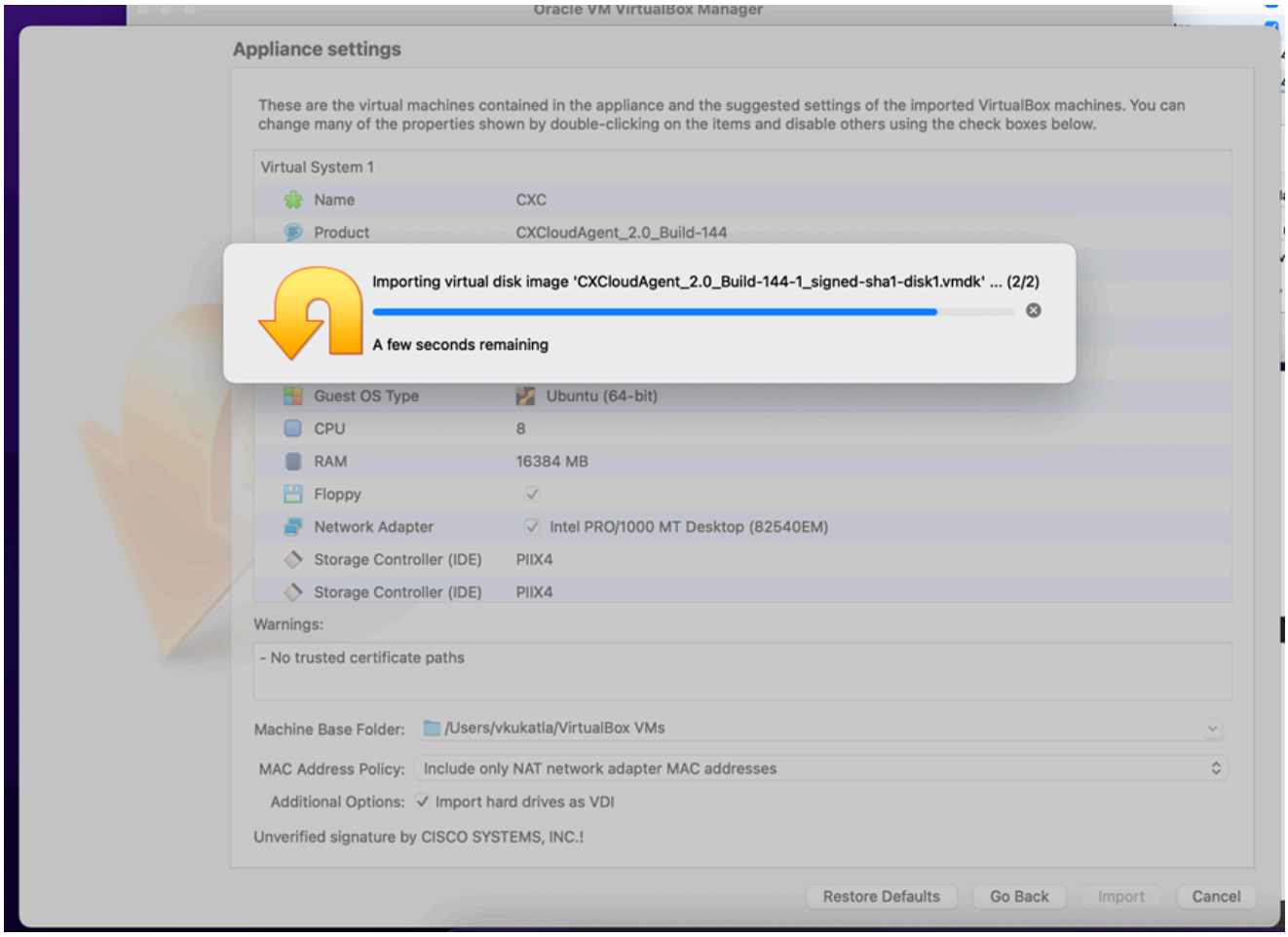


导入文件

4. 选择刚部署的VM，然后点击Start。

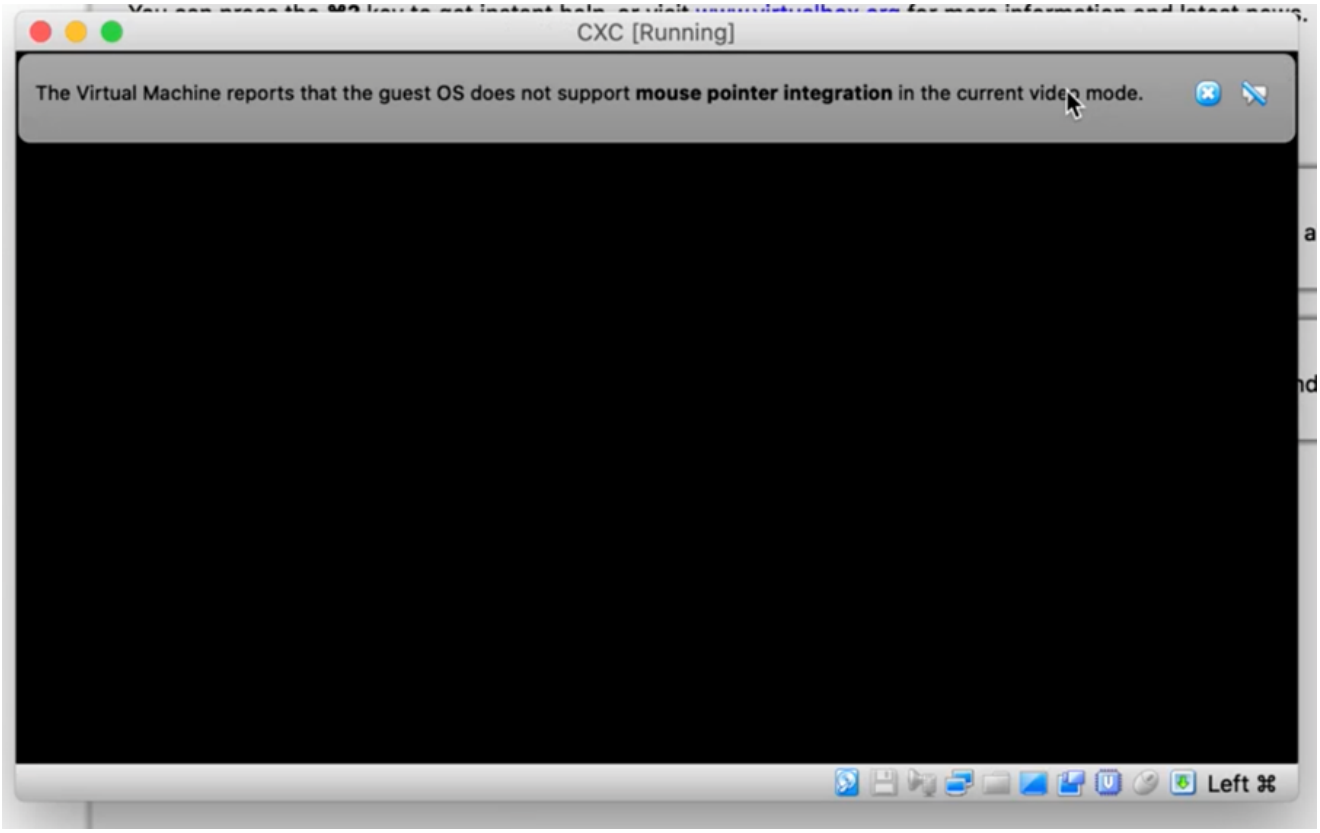


VM 控制台启动



正在导入

5. 打开VM电源。系统随即会显示控制台。

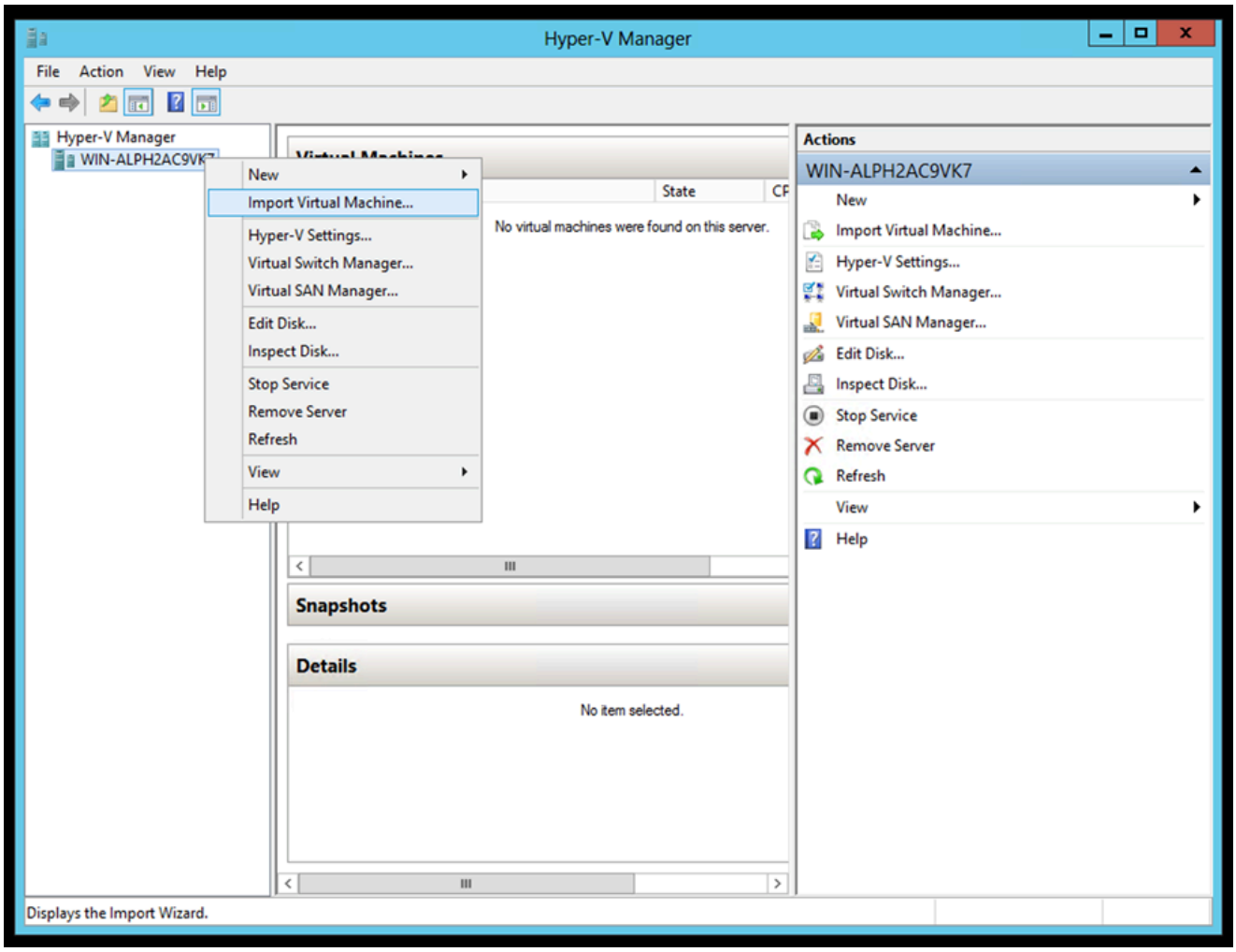


打开控制台

6. 导航至网络配置。

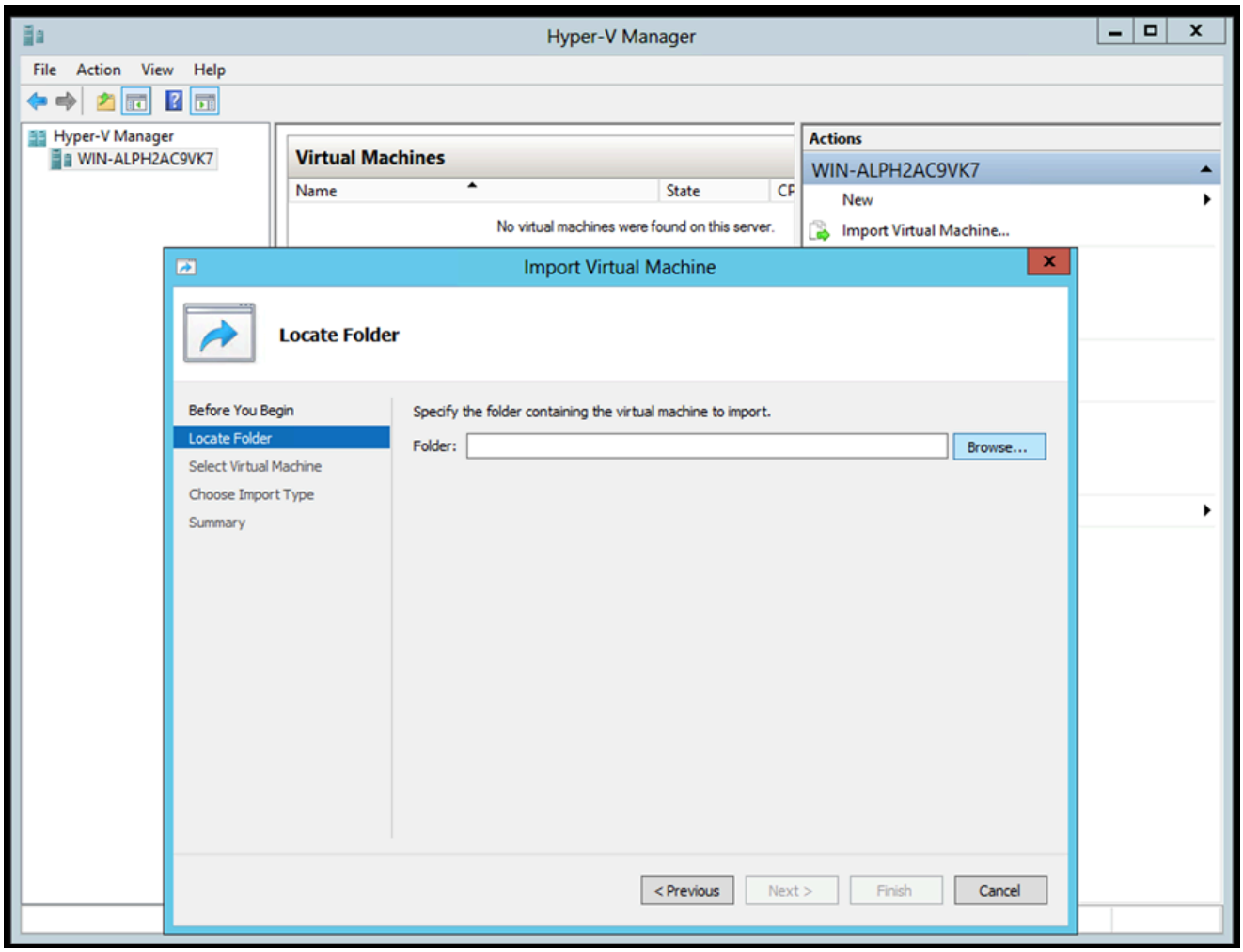
Microsoft Hyper-V 安装

1. 选择.Import Virtual Machine



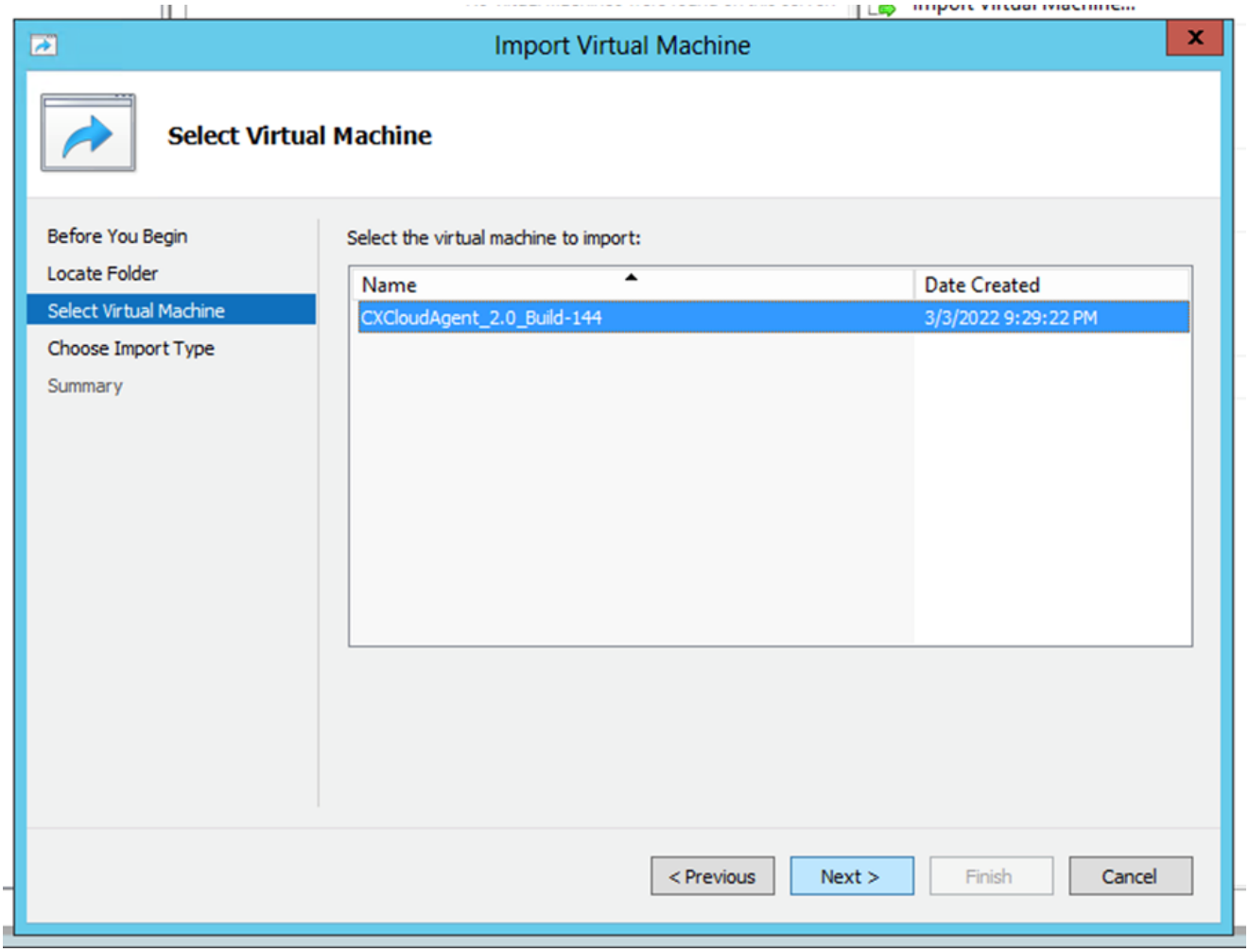
Hyper-V 管理器

2. 浏览并选择下载文件夹。
3. 单击。Next



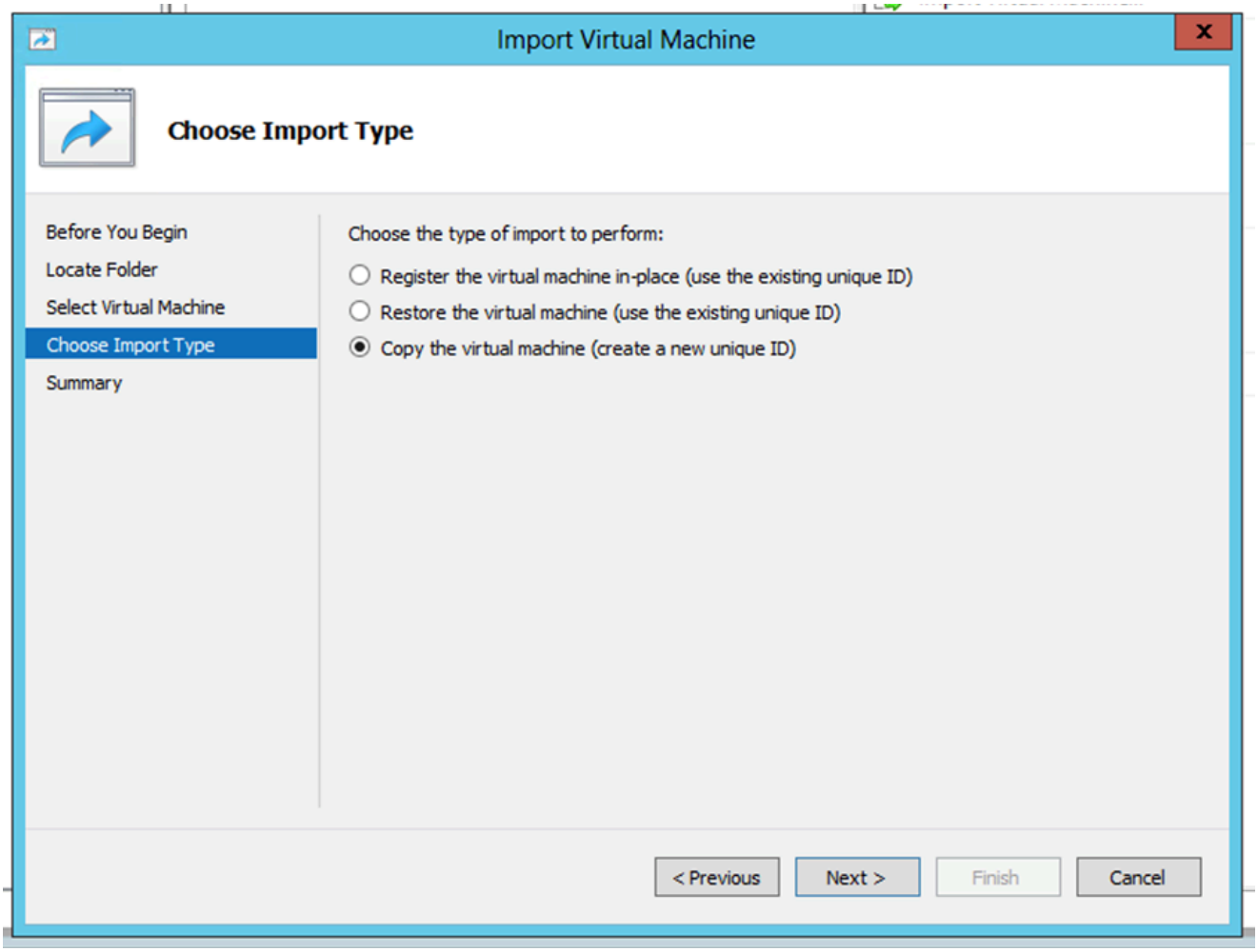
要导入的文件夹

4. 选择VM并点击Next。



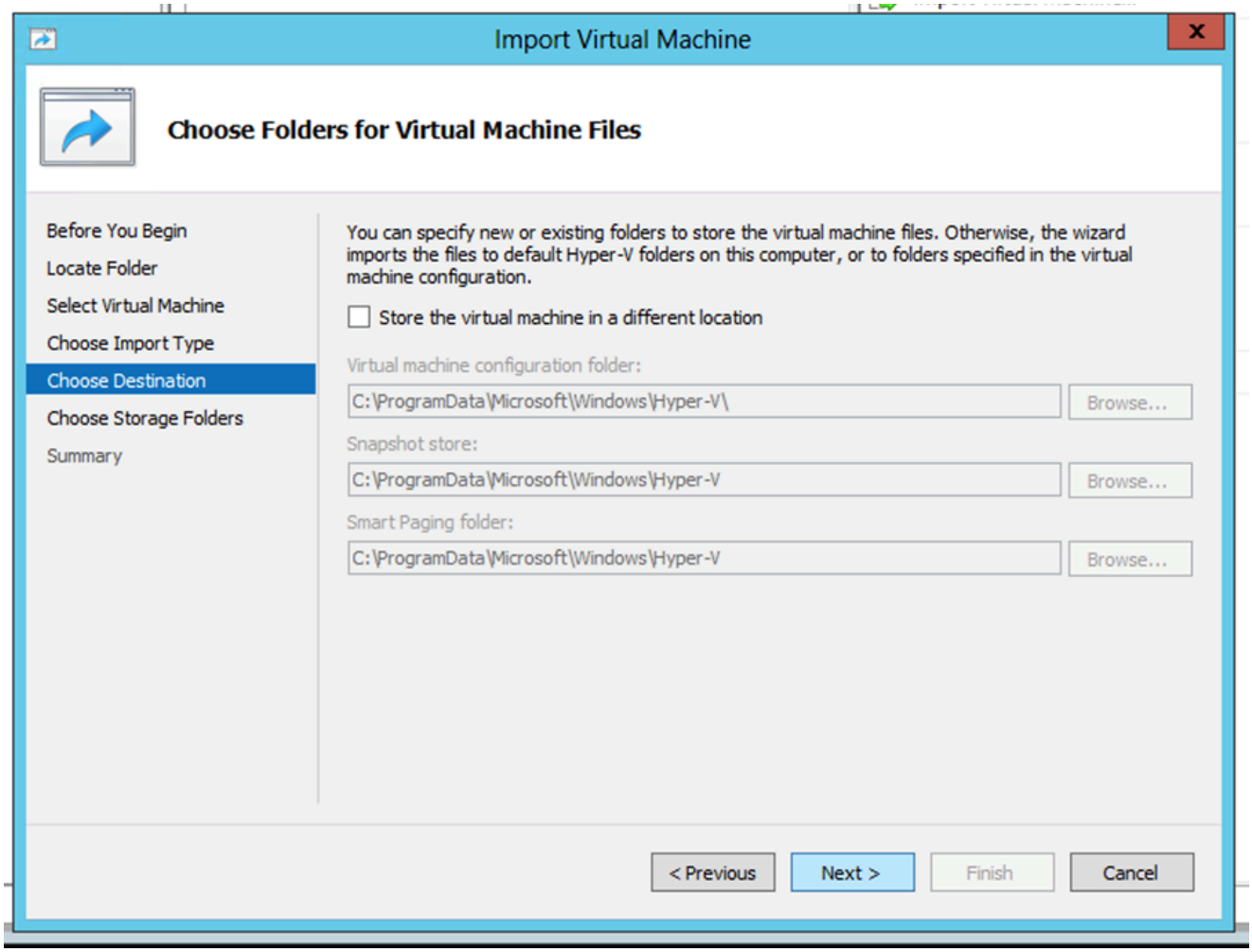
选择 VM

5. 选择单Copy the virtual machine (create a new unique ID) 选按钮并单击Next。



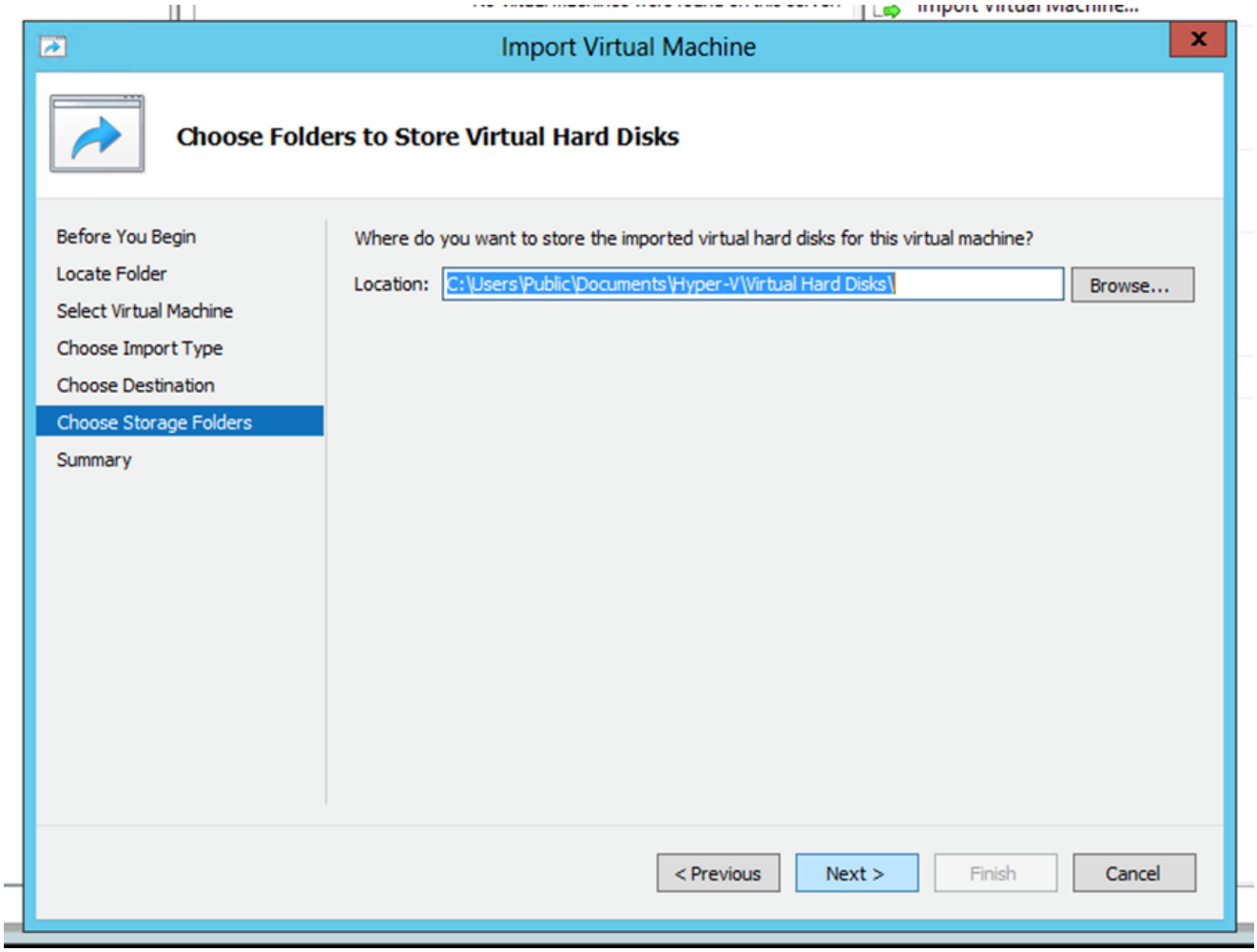
导入类型

6. 浏览以选择 VM 文件的文件夹。建议使用默认路径。
7. 单击。Next



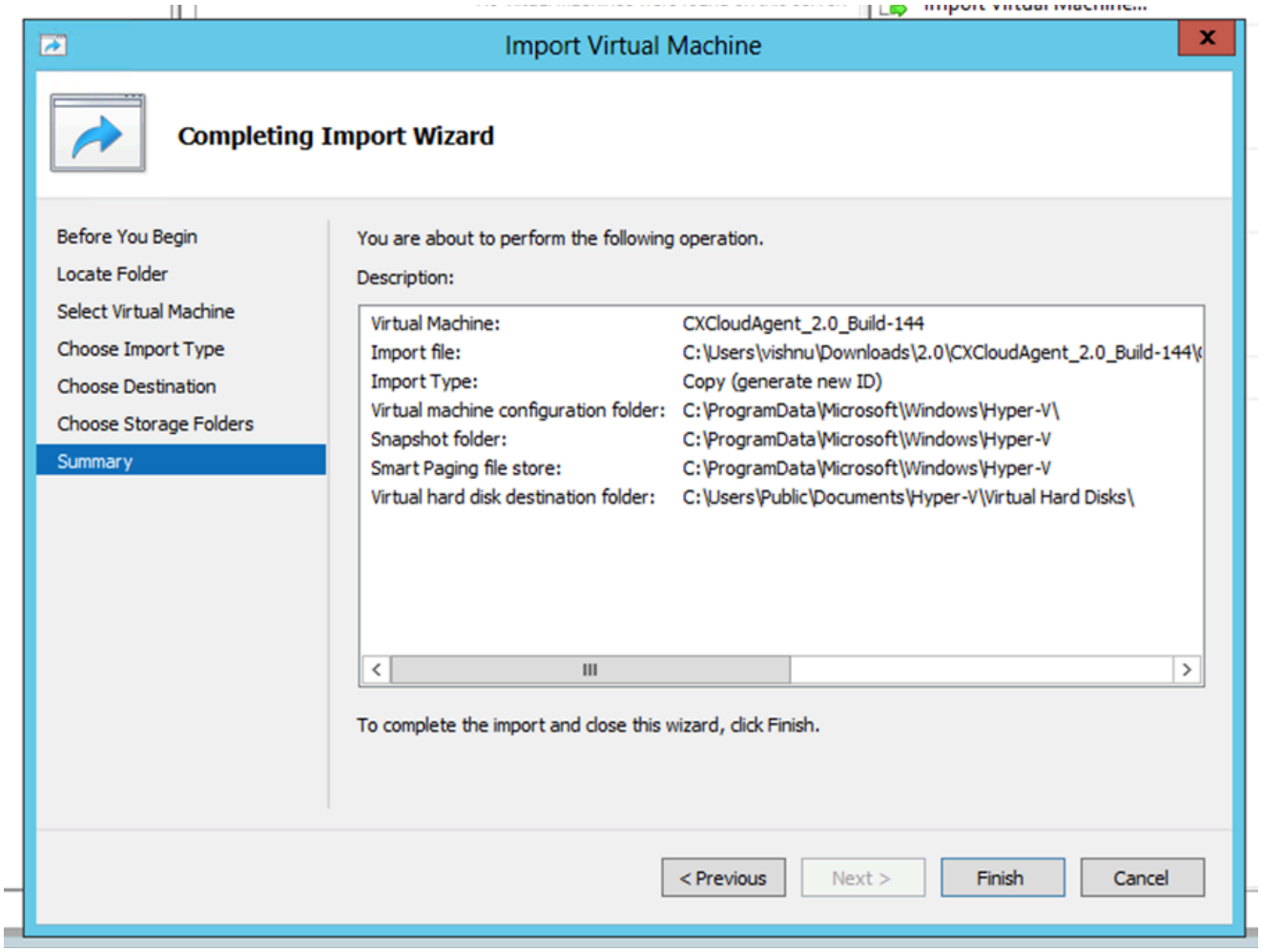
选择文件夹

8. 浏览并选择要存储 VM 硬盘的文件夹。建议使用默认路径。
9. 单击。Next



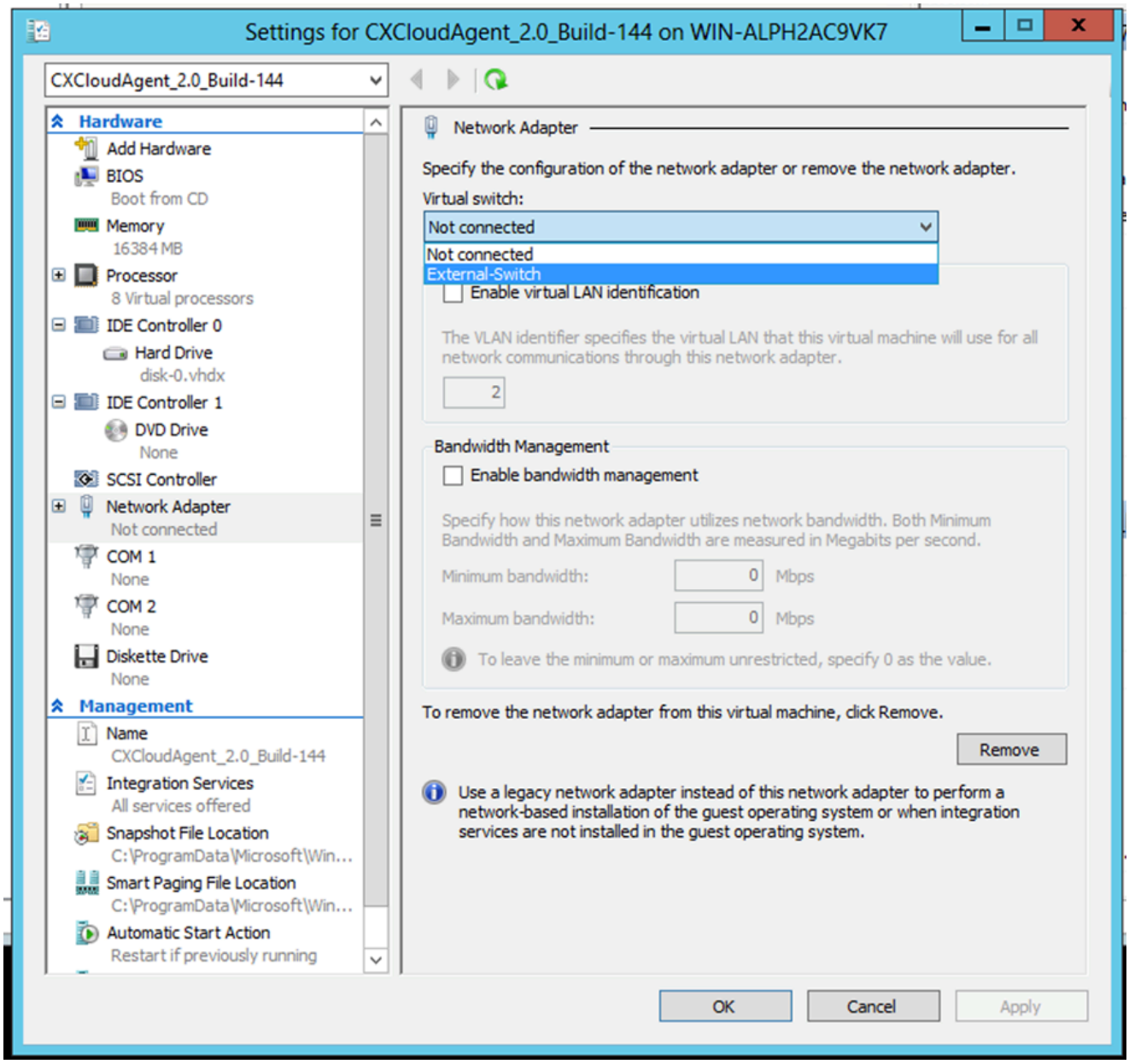
用于存储虚拟硬盘的文件夹

10. 系统随即会显示VM摘要。检验所有输入并点击Finish。



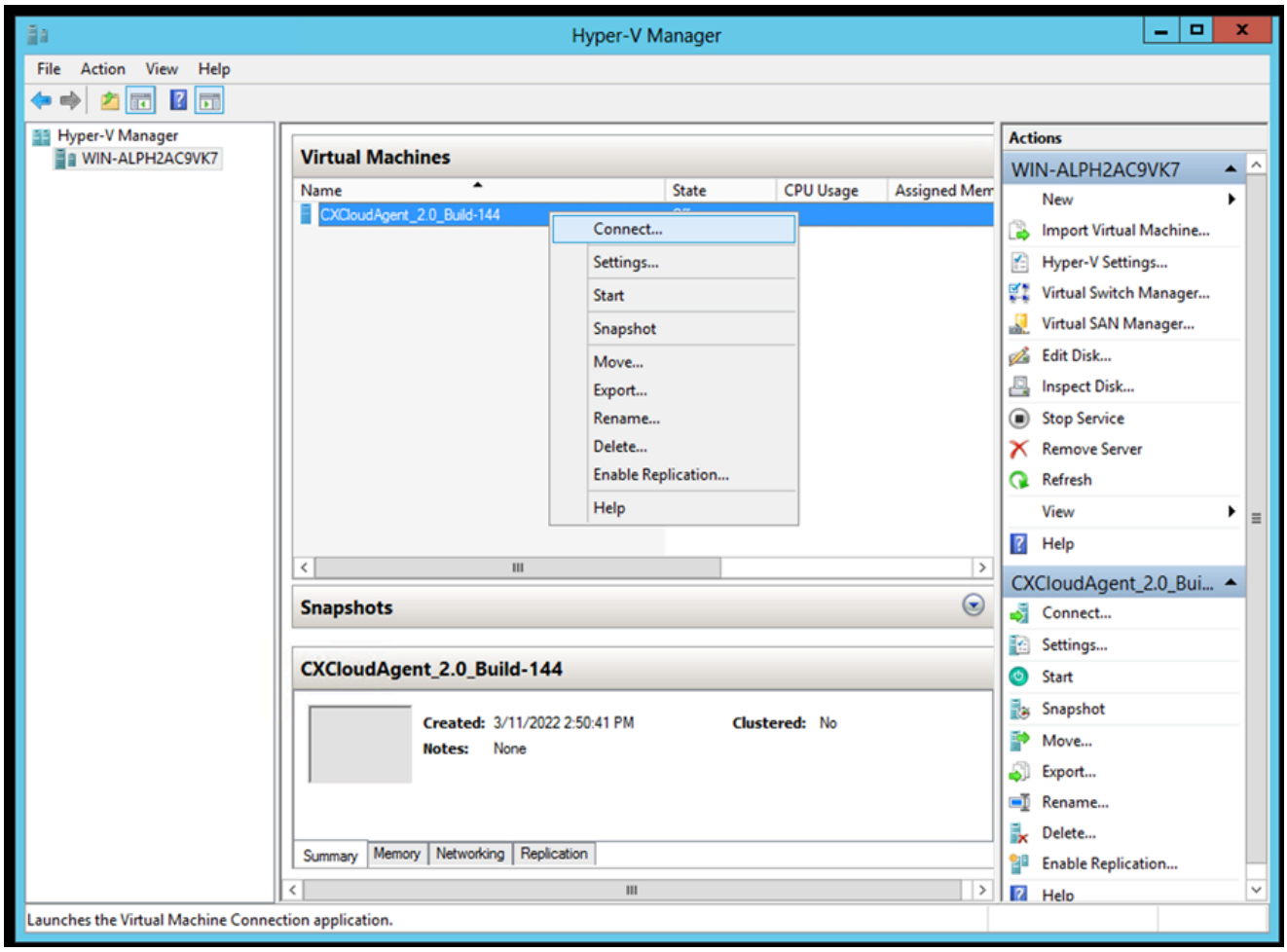
摘要

11. 成功完成导入后，将在Hyper-V上创建新的VM。打开VM设置。
12. 在左侧窗格中选择网络适配器，然后从下拉列Virtual Switch表中选择可用的网络适配器。



虚拟交换机

13. 选择Connect，启动VM。



启动 VM

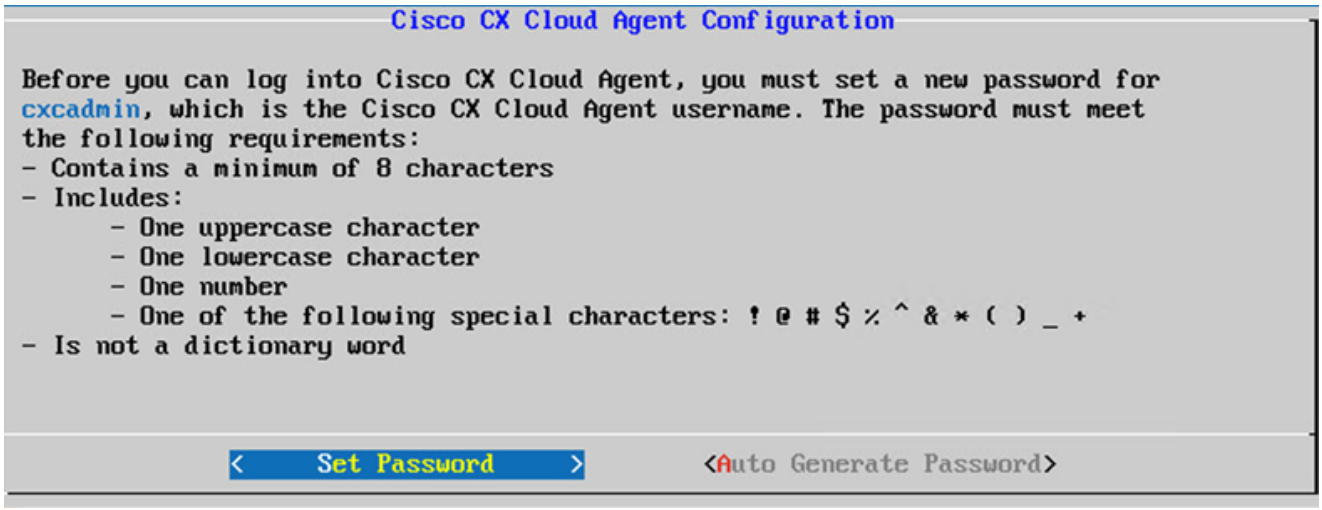
14. 导航至网络配置。

网络配置



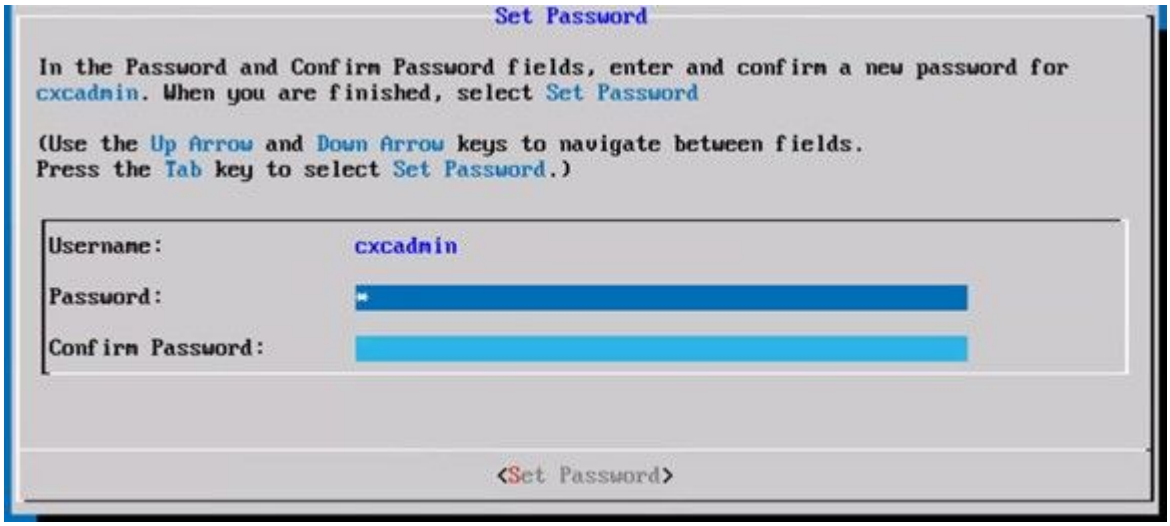
VM 控制台

1. 点击Set Password，为cxcadmin添加新密码；或者点击Auto Generate Password，获取新密码。



设置密码

2. 如果Set Password，请输入cxcadmin的密码并确认。单击Set Password，然后转至步骤3。



新密码

或者，如Auto Generate Password果选中了此项，请复制生成的密码并将其存储起来以供将来使用。单击Save Password，然后转至步骤4。



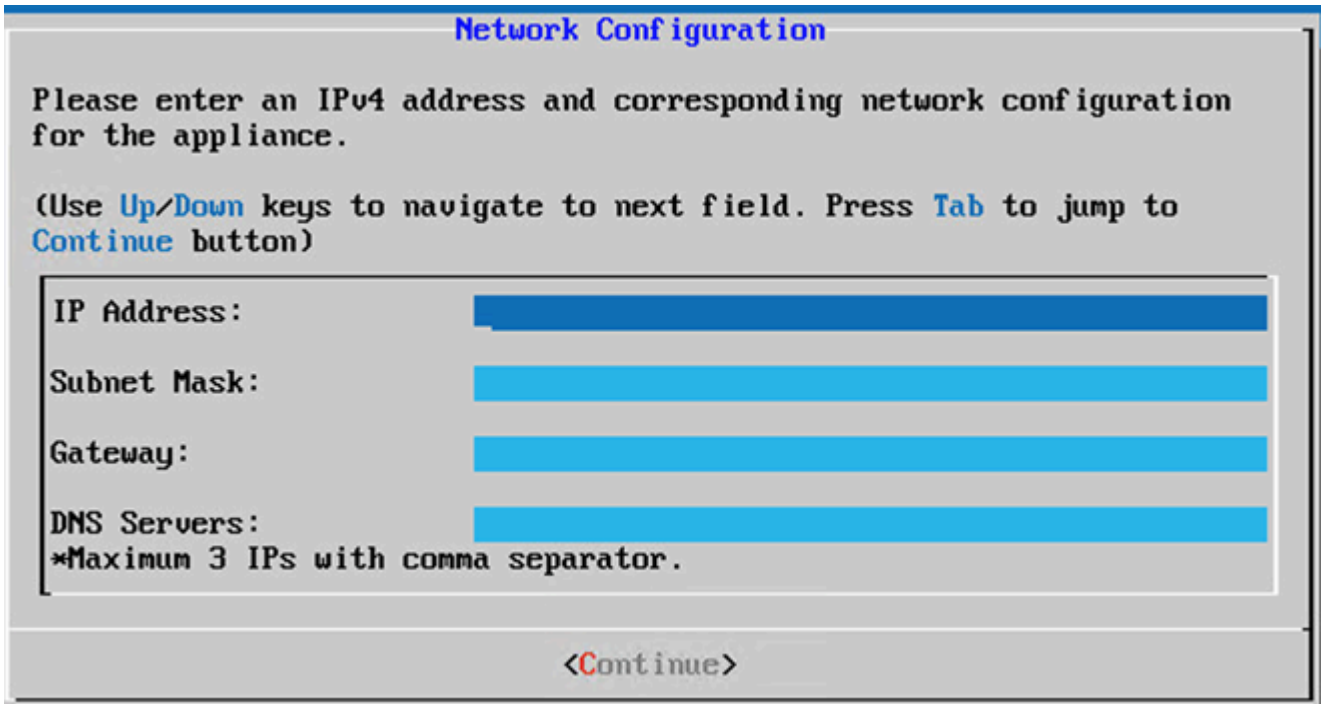
自动生成的密码

3. 单击Save Password，将其用于身份验证。



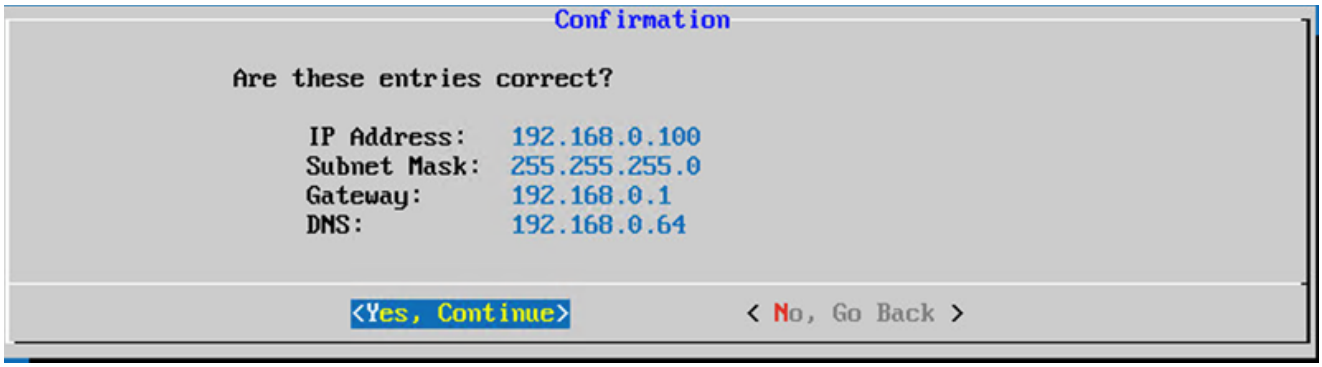
保存密码

4. 输入IP Address、 Subnet Mask、 Gateway ，然DNS Server 后单Continue。



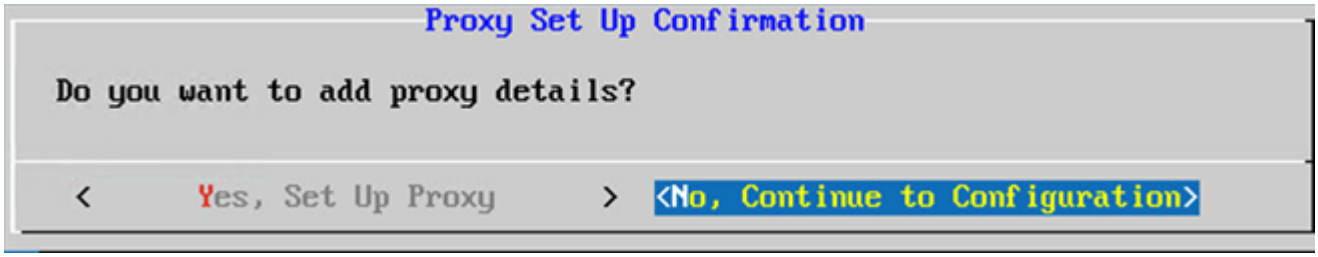
网络配置

5. 确认条目并点击Yes,Continue。



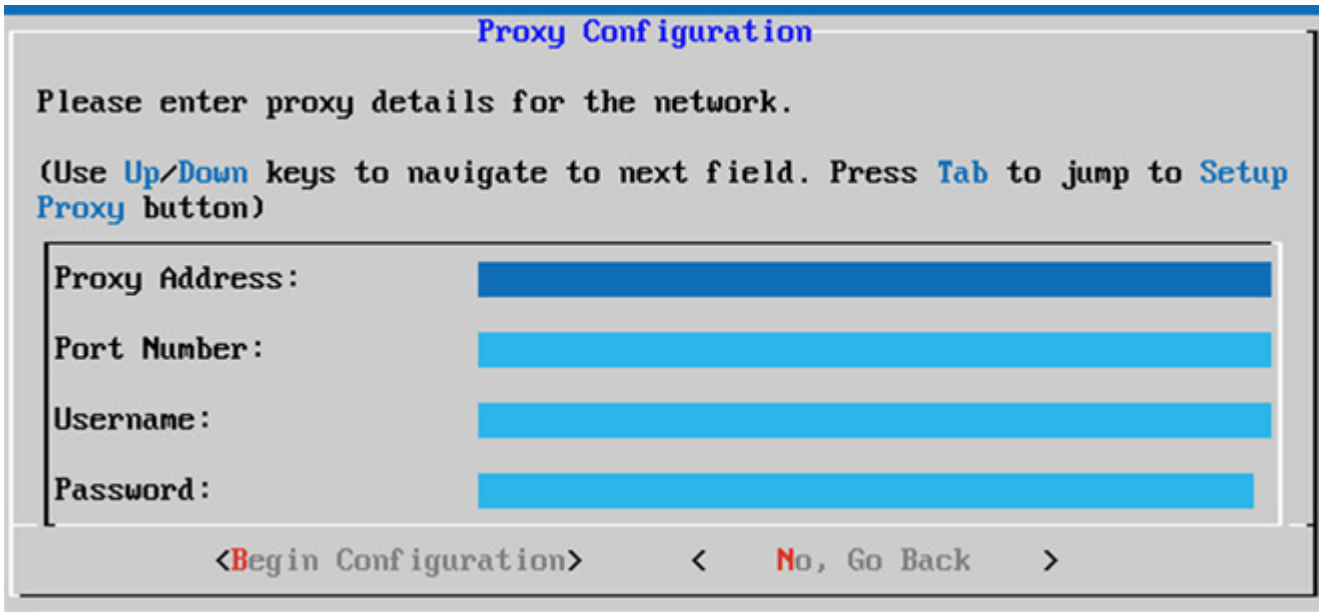
确认

6. 要设置代理详细信息，请点Yes,击Set Up Proxy 或点击No, Continue to Configuration ，完成配置并转到步骤8。



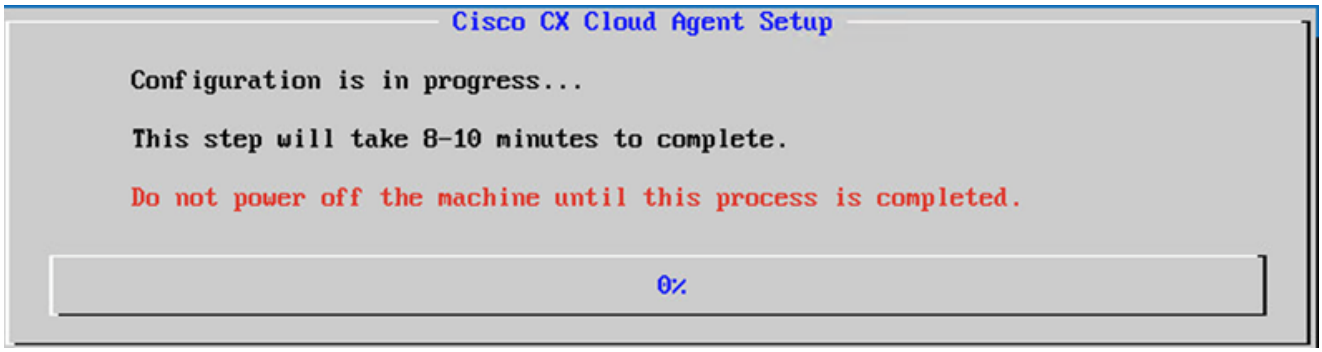
代理设置

7. 输入Proxy Address、 Port Number、 Username和Password。



代理配置

8. 单击。Begin Configuration完成配置可能需要几分钟。



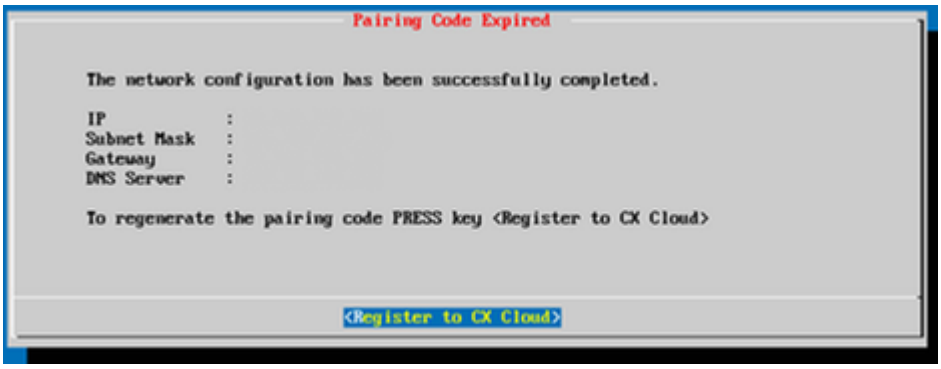
正在配置

9. 复制Pairing Code，然后返回到CX云以继续设置。



配对代码

10.如果“配对代码”过期，请单击Register to CX Cloud，再次获取该代码。



代码已过期

11.单击OK。



注册成功

12.返回将CX云代理连接到CX云部分，并执行列出的步骤。

使用CLI生成配对代码的备用方法

用户还可以使用CLI选项生成配对代码。

要使用CLI生成配对代码，请执行以下操作：

1. 使用cxcadmin用户凭证通过SSH登录云代理。
2. 使用命令 cxcli agent generatePairingCode 生成配对代码。



生成配对代码 CLI

3. 复制Pairing Code，然后返回到CX云以继续设置。有关详细信息，请参阅连接到客户门户。

配置Cisco DNA Center以将系统日志转发到CX云代理

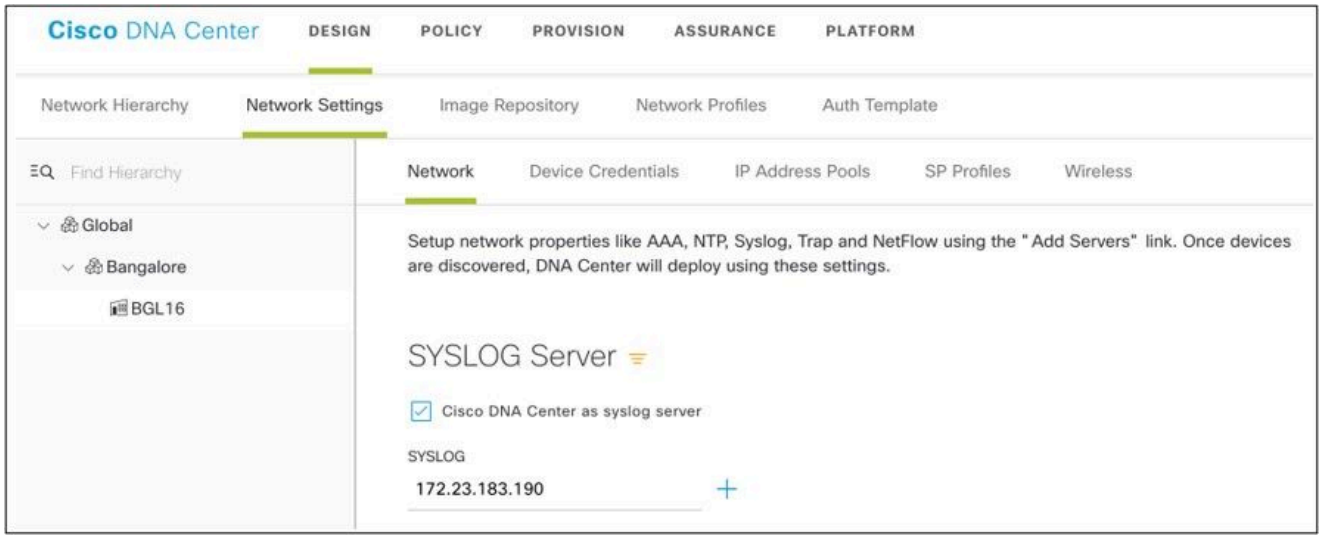
前提条件

支持的Cisco DNA Center版本为1.2.8到1.3.3.9和2.1.2.0到2.2.3.5。

配置系统日志转发设置

要使用UI在Cisco DNA Center中配置到CX云代理的系统日志转发，请执行以下步骤：

1. 启动 Cisco DNA Center。
2. 转到Design > Network Settings > Network。
3. 对于每个站点，将 CX Cloud Agent IP 添加为系统日志服务器。



syslog 服务器

> 注意：
> — 配置后，所有与该站点关联的设备都将配置为向CX云代理发送级别为“关键”的系统日志。
> — 设备必须关联到站点，才能启用从设备到CX云代理的系统日志转发。
> — 更新系统日志服务器设置时，与该站点关联的所有设备都会自动设置为默认严重级别。

启用信息级别系统日志设置

要使系统日志信息级别可见，请执行以下步骤：

1. 导航至Tools> Telemetry。



工具菜单

2.选择并展开站点,Site View 然后从站点层次结构中选择站点。



站点视图

3.选择所需地点并使用复选框选择所有Device name设备。

4.从下拉Actions ，选择Optimal Visibility。



操作

安全

CX云代理可确保客户获得端到端安全性。CX云和CX云代理之间的连接已加密。CX云代理的安全套接字外壳(SSH)支持11个不同的密码。

物理安全

在安全的VMware服务器公司中部署CX云代理OVA映像。OVA 通过思科软件下载中心安全共享。引导加载程序（单用户模式）密码设置为随机唯一密码。用户必须参阅常见问题解答才能设置此引导加载程序（单用户模式）密码。

用户访问权限

CX云用户只能获得身份验证并访问云代理API。

账户安全

在部署时，会创建cxcadmin用户帐户。用户在初始配置期间必须设置密码。cxcadmin 用户/凭证用于访问 CX Cloud Agent API 和通过 SSH 连接设备。

cxcadmin用户具有权限最低的限制访问权限。cxcadmin密码符合安全策略，是单向散列密码，有效期为90天。cxcadmin用户可以使用名为remoteaccount的实用程序创建cxcroot用户。cxcroot 用户可以获取 root 权限。密码将在两天后过期。

网络安全

CX云代理VM可使用带有cxcadmin用户凭证的ssh进行访问。传入端口限制为 22 (SSH)、514（系统日志）。

身份验证

基于密码的身份验证：设备会维护一个单用户的 - ‘cxcadmin’，使用户能够进行身份验证并与 CX Cloud Agent 通信。

- 使用 SSH 在设备上执行 root 特权操作

  cxcadmin用户可以使用名为remoteaccount的实用程序创建cxcroot用户。此实用程序显示RSA/ECB/PKCS1v1_5加密密码，该密码只能从SWIM门户(https://swims.cisco.com/abraxas/decrypt)解密。 只有授权人员才能访问此门户。cxcroot 用户可以使用此解密密码获取 root 权限。密码有效期仅为两天。密码过期后，cxcadmin 用户需要重新创建账户并从 SWIM 门户获取密码。

强化

CX云代理设备符合CIS强化标准。

数据安全

CX Cloud Agent 设备不存储任何客户个人信息。

设备凭证应用（作为其中一个 Pod 运行）将加密的 Cisco DNA Center 服务器凭证存储在安全数据库中。Cisco DNA Center 收集的数据不会以任何形式存储在设备中。收集完成后，收集的数据会立即上传到支持的数据中心，并从代理中清除数据。

数据传输

注册包包含所需的唯一X.509设备证书和密钥，用于与Iot核心建立安全连接。使用该代理通过TLS v1.2使用MQTT建立安全连接

日志和监控

日志不包含任何形式的敏感信息。审核日志会捕获在CX云代理设备上执行的所有安全敏感型操作。

安全汇总

安全特性	描述
引导加载程序密码	引导加载程序（单用户模式）密码设置为随机唯一密码。用户必须参考常见问题解答才能设置其引导加载程序（单用户模式）密码。
用户访问权限	SSH： • 使用 cxcadmin 用户访问设备需要使用安装期间创建的凭证。 • 使用cxcroot用户访问设备需要授权人员使用SWIM门户解密凭证。
用户帐户	• cxcadmin：这是创建的默认用户账户。用户可以使用 cxcli 执行 CX Cloud Agent 应用命令，并且在设备上具有最低权限。使用 cxcadmin 用户创建 cxcroot 用户及其加密密码 • cxcroot：cxcadmin 可以使用实用程序“remoteaccount”创建此用户。用户可以使用此账户获得 root 权限。
cxcadmin 密码政策	• 密码使用 SHA-256 进行单向散列处理并安全存储。 • 至少八(8)个字符，包含下列三个类别：大写字母、小写字母、数字和特殊字符。
cxcroot 密码政策	• cxcroot 密码已经过 RSA/ECB/ PKCS1v1_5 加密。 • 生成的密码需要在 SWIM 门户中解密。 • cxcroot 用户和密码的有效期最长为两天，可以使用 cxcadmin 用户重新生成。
SSH 登录密码政策	• 至少八(8)个字符，包含下列三个类别：大写字母、小写字母、数字和特殊字符。 • 5次失败的登录尝试锁定该盒30分钟。密码有效期为 90 天。

端口	开放传入端口 – 514（系统日志）和 22 (SSH)
数据安全	未存储任何客户信息。 未存储设备数据。 Cisco DNA Center 服务器凭证已加密并存储在数据库中。

常见问题解答

CX Cloud Agent

部署

问 - 通过“重新安装”选项，用户能否使用新的 IP 地址部署新的 Cloud Agent？

答 - 可以

问：安装可用的文件格式有哪些？

答 - OVA 和 VHD

问 - 在什么环境中能够部署此可安装程序？

答 - OVA

VMWare ESXi版本5.5或更高版本

Oracle Virtual Box 5.2.30或更高版本

VHD

Windows虚拟机监控程序2012到2016

问 - CX Cloud Agent 能否在 DHCP 环境中检测 IP 地址？

答 - 能，在 DHCP 环境中，系统会处理 IP 配置期间的 IP 地址分配。但是，不支持未来任何时候对 CX Cloud Agent 进行 IP 地址更改。此外，建议客户在其 DHCP 环境中为 Cloud Agent 保留 IP。

问 - CX Cloud Agent 是否同时支持 IPv4 和 IPv6 配置？

答 - 否，仅支持 IPv4。

问 - 在 IP 配置期间，是否验证了 IP 地址？

A — 是，IP地址语法和重复的IP地址分配已验证。

问 - OVA 部署和 IP 配置大约需要多少时间？

答 - OVA 部署取决于复制数据的网络速度。IP 配置大约需要 8-10 分钟，包括创建 Kubernetes 和容器。

问 - 是否对任何硬件类型有任何限制？

答：部署OVA的主机必须满足作为CX门户设置的一部分提供的要求。CX Cloud Agent是在运行在Intel Xeon E5处理器硬件上的VMware/Virtual机箱上测试的，Intel Xeon E5处理器的vCPU比设置为2:1。如果使用的处理器CPU比功能更弱或更大，性能可能会下降。

问 - 我们能否随时生成配对代码？

答 - 否，仅当 Cloud Agent 未注册时，才能生成配对代码。

问：- DNAC(对于最多10个集群或20个非集群)与代理之间的带宽要求是什么？

A — 当座席和DNAC位于客户环境中的同一个LAN/WAN网络时，带宽不是限制。对于5000台设备的资产收集，所需的最低网络带宽为2.7 Mb/秒，对于代理程序到DNAC连接则需要13000个接入点。如果为L2分析收集系统日志，则最低所需带宽为3.5 Mbits/sec，用于5000台设备+13000个用于库存的无线接入点、5000台设备syslogs和2000台用于扫描的设备 — 所有设备均从代理并行运行。

版本和补丁

问 - CX Cloud Agent 升级列出了哪些不同类型的版本？

答 — 此处显示的是列出的CX云代理的已发布版本集：

- A.x.0（其中 x 是最新的生产主功能版本，示例：1.3.0）
- A.x.y(其中A.x.0是强制升级和要启动的增量升级，x是最新生产主要功能版本，y是最新升级补丁程序，例如：1.3.1）。
- A.x.y-z(其中A.x.0是必须启动的增量升级，x是最新生产主要功能版本，y是最新实时升级补丁，z是即时修复的即时补丁，时间跨度非常短，例如：1.3.1-1）

其中，A 是跨 3-5 年的长期版本.

问：在哪里可以找到最新发布的CX云代理版本，以及如何升级现有的CX云代理？

A — 转到Admin Settings>Data Sources。单击并View Update，执行屏幕上共享的指令。

身份验证和代理配置

问 - CX Cloud Agent 应用的默认用户是什么？

答 - cxcadmin

问：如何为默认用户设置密码？

答 - 在网络配置期间设置密码。

问 - 在 Day-0 之后是否有任何选项可用于重置密码？

答 - 代理未提供用于重置密码的特定选项，但您可以使用 linux 命令重置 cxcadmin 的密码。

问 - 配置 CX Cloud Agent 的密码策略是什么？

答 - 密码策略包括：

- 密码最长期限（长度）设置为 90 天
- 密码最小期限（长度）设置为 8
- 密码最大长度为 127 个字符。
- 必须至少提供一个上箱和一个下箱。
- 必须至少包含一个特殊字符(例如，!$%^&*()_+|~-=\'{}[]:";'<>?,/)。
- 不允许使用这些字符
  - 特殊的 8 位字符（例如，¬£、√Å √´、√¥、√ë、¬ø、√ü）
  - 空格
- 密码不能是最近使用的10个密码。
- 不得包含正则表达式，即
- 不得包含以下词或其衍生物：cisco、sanjose和sanfran

问 - 如何设置 Grub 密码？

A — 要设置Grub密码，请执行以下步骤：

1. 以 cxcroot 身份运行 ssh 并提供令牌 [联系支持团队以获取 cxcroot 令牌]
2. 执行 sudo su，提供相同的令牌
3. 执行命令 grub-mkpasswd-pbkdf2 并设置 GRUB 密码。打印所提供密码的散列值，复制内容。
4. vi 到文件 /etc/grub.d/00_header。导航到文件末尾，将内容password_pbkdf2根目录之前的哈希输出替换为步骤3中获取的密码的已获取哈希*****
5. 使用 :wq! 命令保存文件。
6. 执行命令 update-grub

问：密码的到期时间是多长cxcadmin?

答 - 90天后密码到期。

问 - 连续登录尝试失败后，系统是否会禁用帐户？

答 - 是，帐户在连续 5 次失败尝试后被禁用。锁定时间为 30 分钟。

问 - 如何生成密码？

A — 执行这些步骤，

1. 以 cxcadmin 用户身份运行 ssh 并登录
2. 执行命令remoteaccount cleanup -f
3. 执行命令remoteaccount create

问 - 代理主机是否支持主机名和 IP？

答 — 是，但是要使用主机名，用户必须在网络配置期间提供DNS IP。

Secure Shell (SSH)

问 - SSH Shell 支持哪些密码？

答 - chacha20-poly1305@openssh.com、aes256-gcm@openssh.com、aes128-gcm@openssh.com、aes256-ctr、aes192-ctr、aes128-ctr

问 - 如何登录控制台？

答 — 使用以下步骤登录：

1. 以 cxcadmin 用户身份登录。
2. 提供cxcadmin密码。

问 - 是否记录 SSH 登录？

A — 是，它们作为var/logs/audit/audit.log目录的一部分进行记录。

问 - 空闲会话超时时间是多少？

A — 如果云代理空闲五(5)分钟，则会发生SSH会话超时。

端口和服务

问 - 默认情况下，CX Cloud Agent 上的哪些端口保持打开状态？

A — 这些端口可用：

- Outbound port:部署的CX云代理可以连接到HTTPS端口443上的表中所示的思科后端，也可以通过代理将数据发送到思科。部署的 CX Cloud Agent 可以通过 HTTPS 端口 443 连接到 Cisco DNA Center.

.

美洲地区	欧洲、中东和非洲	亚太地区
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

注意：除了列出的域外，当EMEA或APJC客户重新安装云代理时，客户防火墙中必须允许域agent.us.csco.cloud。

成功重新安装后不再需要域agent.us.csco.cloud。

注意：确保在端口443上必须允许返回流量。

- Inbound port:对于CX云代理的本地管理，必须可以访问514(Syslog)和22(ssh)。客户必须允许其防火墙中的端口443从CX云接收数据。

CX Cloud Agent 与 Cisco DNA Center 的连接

问 - Cisco DNA Center与 CX Cloud Agent 的用途和关系是什么？

答 — Cisco DNA Center是管理客户驻地网络设备的云代理。CX Cloud Agent 从已配置的 Cisco DNA Center 收集设备的资产信息，并上传在 CX Cloud 中作为“资产视图”提供的资产信息。

问 - 用户何时可以提供 CX Cloud Agent 上的 Cisco DNA Center 详细信息？

答 — 在第0天 — CX云代理设置期间，用户可以从CX云门户添加Cisco DNA Center详细信息。此外，在第N天操作期间，用户可以从添加额外的DNA中心Admin Settings > Data source。

问 - 可以添加多少个 Cisco DNA Center？

A - 10个Cisco DNAC集群或20个DNAC非集群。

问：Cisco DNA Center用户可以扮演什么角色？

A — 用户角色可以是admin 或observer。

问：如何反映由于连接的DNA Center凭证发生变化而对CX代理进行的修改？

A — 从CX云代理控制台执行以下命令：

cxcli agent modifyController

在DNAC凭证更新期间出现任何问题，请与支持部门联系。

问 - Cisco DNA Center 详细信息如何存储在 CX Cloud Agent 中？

答 - Cisco DNA Center 凭证使用 AES-256 加密并存储在 CX Cloud Agent 数据库中。CX Cloud Agent 数据库使用受保护的用户 ID 和密码进行保护。

问：从CX云代理访问Cisco DNA Center API时使用哪种加密？

答 - Cisco DNA Center 和 CX Cloud Agent 之间使用 HTTPS over TLS 1.2 进行通信。

问 - CX Cloud Agent 在集成的 Cisco DNA Center Cloud Agent 上执行了哪些操作？

答 — CX云代理收集Cisco DNA Center有关网络设备的数据，并使用Cisco DNA Center命令运行器界面与终端设备通信并执行CLI命令（show命令）。 不执行任何配置更改命令

问 - 从 Cisco DNA Center 收集并上传到后端的默认数据是什么？

A-

- 网络实体
- 模块
- show version
- config
- 设备映像信息
- 标签

问 - 从 Cisco DNA Center 收集并上传到思科后端的其他数据是什么？

答 - 您可以从此处获取所有信息。

问 - 如何将资产数据上传到后端？

答 - CX Cloud Agent 通过 TLS 1.2 协议将数据上传到思科后端服务器。

问 - 资产上传的频率是多少？

答 — 收集根据用户定义的计划触发，并上传到思科后端。

问 - 用户能否重新计划资产？

A — 是，有一个选项可用于修改中的计划信息Admin Settings> Data Sources。

问 - Cisco DNA Center 和 Cloud Agent 之间的连接超时何时发生？

A — 超时按以下方式分类：

- 对于初始连接，超时最大为 300 秒。如果在最多 5 分钟内未在 Cisco DNA Center 和 Cloud Agent 之间建立连接，则连接会终止。
- 对于周期性的典型连接或更新：响应超时为 1800 秒。如果在 30 分钟内未收到响应或无法读取数据，则连接会终止。

CX Cloud Agent 使用的诊断扫描

问 - 在设备上执行的扫描命令有哪些？

A — 在扫描过程中，动态确定需要在扫描设备上执行的命令。该组命令可以随时间而更改，即使对于同一设备也是如此（并且不能控制诊断扫描）。

问 - 扫描结果在哪里存储和分析？

答 - 扫描结果在思科后端存储和分析。

问 - 插入 Cisco DNA Center 源后，是否将 Cisco DNA Center 中的重复项（按主机名或 IP）添加到

诊断扫描？

答 — 否，过滤重复项，仅提取唯一设备。

问 - 当其中一个命令扫描失败时会发生什么情况？

答 — 设备扫描已完全停止并标记为不成功。

CX Cloud Agent 系统日志

问：哪些运行状况信息会发送到CX云？

答 - 应用日志、Pod 状态、Cisco DNA Center 详细信息、审核日志、系统详细信息和硬件详细信息。

问 - 会收集哪些系统详细信息和硬件详细信息？

答 - 示例输出：

system_details":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"内核版本":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
"操作系统":"linux",
"osImage":"Ubuntu 20.04.1 LTS",
"systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
},
"hardware_details":{
"total_cpu":"8",
"cpu_utilization":"12.5%",
"total_memory":"16007MB",
"free_memory":"9994MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}

问 - 运行状况数据如何发送到后端？

答 — 使用CX云代理，运行状况服务（可服务性）将数据流传输到思科后端。

问 - 后端中 CX Cloud Agent 的运行状况数据日志保留策略是什么？

答 - 后端中的 CX Cloud Agent 的运行状况数据日志保留策略为 120 天。

问 - 可用的上传类型有哪些？

A — 三种上传类型，

1. 库存上传
2. 系统日志上传
3. 代理运行状况上传：3项作为健康上传的内容
    1. 服务运行状况 — 每5分钟
    2. Podlog — 每1小时
    3. 审核日志 — 每1小时

故障排除

问题：无法访问已配置的 IP。

解决方案：使用配置的 IP 执行 ssh。如果连接超时，可能原因是IP配置错误。在这种情况下，请通过配置有效的 IP 重新安装。可通过门户使用页面中提供的重新安装选项完成此Admin Setting项。

问题：如何在注册后验证服务是否正常运行？

解决方案：执行此处所示的命令，验证Pod是否已启动并正在运行。

1. 以 cxcadmin身份使用 ssh 连接到配置的 IP 地址。
2. 提供密码。
3. 执行命令kubectl get pod。

Pod可以处于任何状态，例如运行、初始化或容器创建，但在20分钟后，Pod必须处于运行状态。

如果状态未运行或Pod初始化，请使用此处显示的命令检查Pod描述

kubectl describe pod <podname>

输出中提供了Pod状态信息。

问题：如何验证客户代理是否禁用了SSL拦截器？
解决方案：执行此处显示的curl命令以验证服务器证书部分。响应包含concsoweb服务器的证书详细信息。

curl -v —header '授权：Basic xxxxxx' https://concsoweb-prd.cisco.com/

*服务器证书：

*主题：C =美国；ST=加利福尼亚；L=圣荷西；O=思科系统公司；CN=concsoweb-prd.cisco.com

*开始日期：2月16日11:55:11 2021格林尼治标准时

*到期日期：2月16日12:05:00 2022格林尼治标准时

* subjectAltName:主机“concsoweb-prd.cisco.com”匹配证书“concsoweb-prd.cisco.com”

*颁发者：C =美国；O=HydrantID(Avalanche Cloud Corporation);CN=HydrantID SSL CA G3

* SSL证书验证正常。

> GET / HTTP/1.1

问题：kubectl命令失败，错误显示为“The connection to the server X.X.X.X:6443 was refused - do you specify the right host or port”
解决方案：

- 请验证资源的可用性。[示例：CPU、内存]
- 等待 Kubernetes 服务启动

问题：如何获取命令/设备收集失败的详细信息

解决方案：

- 执行kubectl get pods并获取集合Pod名称。
- 执行kubectl logs
  以获取命令/设备特定的详细信息。

问题：kubectl 命令未执行，并提示错误“[authentication.go:64] 无法对请求进行身份验证，错误：[x509：证书已过期或无效，x509：证书已过期或无效]”

解决方案：以cxcroot用户身份运行此处显示的命令

rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3
kubectl —insecure-skip-tls-verify=true delete secret -n kube-system k3s-serving
systemctl restart k3

收集失败响应

收集失败原因可能是控制器中添加的控制器或设备出现了任何限制或问题。

此处显示的表包含收集过程中在“收集微服务”(Collection Microservice)下看到的使用案例的错误代码段。

使用案例	收集微服务中的日志片段

如果在 Cisco DNA Center 未找到请求的设备	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a
	"
	}

如果无法从 Cisco DNA Center 访问请求的设备	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occurred while executing command: show version\nError connecting to device [Host: 172.21.137.221:22]No route to host : No route to host "
	}

如果无法从 Cisco DNA Center 访问请求的设备	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nError connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connection timed out: /X.X.X.X:22"
	}

如果请求的命令在设备中不可用	{
	"command": "show run-config",
	"status": "Success",
	"commandResponse": " Error occured while executing command : show run-config\n\nshow run-config\n ^\n% Invalid input detected at \u0027^\u0027 marker.\n\nXXCT5760#",
	"errorMessage": ""
	}

如果所请求的设备没有SSHv2，思科DNA中心会尝试使用SSHv2连接设备	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nSSH2 channel closed : Remote party uses incompatible protocol, it is not SSH-2 compatible."
	}

使用案例	收集微服务中的日志片段

如果在收集微服务中禁用了命令	{
	"command": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "Command collection is disabled",
	"errorMessage": ""
	}

如果命令运行器任务失败且 Cisco DNA Center 未返回任务 URL	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s. Task URL is empty."
	}

如果无法在 Cisco DNA Center 创建命令运行器任务	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s. No task details."
	}

如果收集微服务在 Cisco DNA Center 发出命令运行器请求时未收到任何响应	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s."
	}

如果 Cisco DNA Center 未在配置的超时（收集微服务中每个命令为 5 分钟）内完成任务	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Operation Timedout. The command runner task failed for device %s, RequestURL: %s. No progress details."
	}

如果命令执行器任务失败且 Cisco DNA Center 提交的任务的文件 ID 为空	{ "command": "show version", "status": "Failed",

使用案例	收集微服务中的日志片段
	"commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: %s. File id is empty." }

如果命令运行器任务失败且 Cisco DNA Center 未返回文件 ID 标记	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s. No file id details."
	}

如果设备不符合执行命令运行器的条件	{
	"command": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Requested devices are not in inventory,try with other devices available in inventory"
	}

如果为用户禁用了命令运行器	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"Role does not have valid permissions to access the API\"}\n"
	}

诊断扫描失败响应

扫描失败，原因可能来自任何列出的组件

当用户从门户发起扫描时，偶尔会显示为“失败：内部服务器错误”

问题的原因可能是列出的任何组件

- 控制点
- 网络数据网关
- 连接器
- 诊断扫描
- CX Cloud Agent 微服务 [devicemanager, collection]

- Cisco DNA Center
- APIX
- Mashery
- Ping 访问
- IRONBANK
- IRONBANK GW
- 大数据代理(BDB)

要查看日志，请执行以下操作：

1. 登录到CX云代理控制台
2. 使用 ssh 登录到 cxcadmin 并提供密码
3. 执行 kubectl get pods
4. 获取集合、连接器及可维护性的Pod名称。
5. 验证收集、连接器和可维护性微服务日志

- 执行 kubectl logs
- 执行 kubectl logs
- 执行 kubectl logs

此处显示的表格显示在收集微服务和可服务性微服务日志下看到的错误片段，该错误片段是由于组件出现的问题/限制而发生的。

使用案例	收集微服务中的日志片段

可以访问和支持设备，但在该设备上执行的命令在收集微服务上以块形式列出	{
	"command": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "Command collection is disabled",
	}

如果尝试扫描的设备不可用。 在组件（例如门户、诊断扫描、CX 组件和 Cisco DNA Center 等）之间存在同步问题时发生该问题	No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a
如果尝试进行扫描的设备繁忙，且（在某个场景中）同一设备属于其他作业的一部分，同时 Cisco DNA Center 不会处理该设备的并行请求。	All requested devices are already being queried by command runner in another session. Please try other devices".
如果不支持对设备进行扫描	Requested devices are not in inventory, try with other devices available in inventory

使用案例	收集微服务中的日志片段
如果尝试进行扫描的设备无法访问	"Error occurred while executing command: show udi\nError connecting to device [Host: x.x.x.x:22] No route to host : No route to host

如果无法从 Cloud Agent 访问 Cisco DNA Center，或者 Cloud Agent 的收集微服务在 Cisco DNA Center 发出命令运行器请求时未收到任何响应	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s."
	}

使用案例	控制点代理微服务中的日志片段
如果扫描请求缺少计划详细信息	Failed to execute request {"message":"23502: null value in column \"schedule\" violates not-null constraint"}
如果扫描请求缺少设备详细信息	Failed to create scan policy. No valid devices in the request
如果与 CPA 之间的连接断开	Failed to execute request.
如果请求的扫描设备在诊断扫描中不可用	Failed to submit the request to scan. Reason = {\"message\":\"Device with Hostname=x.x.x.x' was not found\"}

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。