CX代理概述指南3.1版

目录

- 简介
  - 先决条件
  - 访问关键域
  - 特定于CX云门户的域
  - 特定于CX代理VM的域
  - Catalyst Center支持的版本
  - 支持的浏览器
  - 支持的产品列表
  - 升级/安装CX Agent v3.1.5
  - 将现有VM升级到大中型配置
- 升级到CX Agent v3.1.5
  - 自动升级
  - 手动升级
- 添加CX代理
- 配置用于BCS/LCS的CX代理
  - 先决条件
  - 配置CX代理
- 配置RADKit功能
  - 通过CLI集成RADKit客户端
- 为现有CX代理配置保管库
  - 通过CLI将CX代理与HashiCorp Vault集成
    - 先决条件
    - 与HashiCorp Vault集成
  - 启用HashiCorp Vault集成
  - 禁用HashiCorp Vault集成
  - HashiCorp保管库设备凭证方案
  - 在HashiCorp Vault中配置设备凭证（第一次）
  - 向HashiCorp Vault添加更多凭证
  - 具有默认凭证的CX云种子文件
- 添加Catalyst Center作为数据源
- 添加BCS/LCS数据源
  - 添加SolarWinds®
  - 添加EPNM
  - 添加APIC
- 添加其他资产作为数据源
  - 发现协议
  - 连接协议
  - 设备的遥测处理限制

使用种子文件添加其他资产
- 使用新的种子文件添加其他资产
- 使用已修改的种子文件添加其他资产
- 种子文件的默认凭据

使用IP范围添加其他资产
- 按IP范围添加其他资产
- 编辑IP范围
- 删除IP范围
- 关于从多个控制器中发现的设备

使用CDP或LLDP添加其他资产
- 编辑CDP或LLDP详细信息

安排诊断扫描

将CX Agent VM升级到大中型配置
- 使用VMware vSphere胖客户端重新配置
- 使用Web客户端ESXi v6.0重新配置
- 使用Web客户端vCenter重新配置

部署和网络配置
- OVA 部署
  - ThickClient ESXi 5.5/6.0安装
  - WebClient ESXi 6.0安装
  - WebClient vCenter安装
  - OracleVirtual Box 7.0.12安装
  - MicrosoftHyper-V安装
  - 处理器设置
  - Microsoft Hyper-V映像签名验证
- 网络配置
- 使用CLI生成配对代码的备用方法
- 配置设备以将系统日志转发到CX云代理
  - 先决条件
  - 配置系统日志转发设置
- 配置其他资产（直接设备收集）以将系统日志转发到CX代理
  - 具有转发功能的现有系统日志服务器
  - 没有转发功能的现有系统日志服务器或没有系统日志服务器
- 启用Cisco Catalyst Center的信息级别系统日志设置

备份和恢复CX云虚拟机
- 备份CX云虚拟机
- 恢复CX云虚拟机

安全
- 物理安全
- 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

简介

本文档介绍思科的客户体验(CX)代理。思科的CX代理是一个高度可扩展的平台，可从客户网络设备收集遥测数据，为客户提供切实可行的见解。CX代理支持将人工智能(AI)/机器学习(ML)将活动运行配置数据转换为CX云中显示的主动预测性见解(包括成功跟踪、智能网络支持服务(SNTC)和业务关键型服务(BCS)或生命周期服务(LCS)产品)。

本指南仅适用于CX云和合作伙伴管理员。具有超级用户管理员(SUA)和管理员角色的用户拥有执行本指南中所述操作所需的权限。

本指南特定于CX Agent v3.1.5请参阅Cisco CX Agent页面以访问以前的版本。

注：本指南中的图像仅供参考。实际内容可能有所不同。

先决条件

CX代理作为虚拟机(VM)运行，可作为开放式虚拟设备(OVA)或虚拟硬盘(VHD)下载。

部署需求

- 新安装需要以下虚拟机监控程序之一：
  - VMware ESXi v5.5或更高版本
  - Oracle Virtual Box v5.2.30或更高版本
  - Windows虚拟机监控程序版本2012到2022和版本2025
- 部署VM需要下表中的配置：

CX代理部署类型	CPU核心数	RAM	硬盘	*直接资产的最大数量已连接到CX代理	支持的虚拟机监控程序
小型OVA	8核	16GB	200GB	10,000	VMware ESXi、Oracle VirtualBox和Windows Hyper-V
中型OVA	16摄氏度	32GB	600GB	20,000	VMware ESXi、Windows Hyper-V
大型OVA	32摄氏度	64GB	1200GB	50,000	VMware ESXi、Windows Hyper-V

*除连接每个CX云代理实例的20个Cisco Catalyst Center(Catalyst Center)非集群或10个Catalyst

Center集群外，

- 对于使用指定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代理必须能够连接到此处所示的服务器，使用完全限定域名(FQDN)，并在TCP端口443上使用HTTPS:
  - FQDN：agent.us.csco.cloud
  - FQDN：ng.acs.agent.us.csco.cloud
- 对于将指定的欧洲数据中心用作存储CX云数据的主要数据区域的客户：cx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
- 对于将指定的亚太地区数据中心用作存储CX云数据的主要数据区域的客户：cx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
- 对于使用指定的欧洲和亚太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。
- 对于使用RADKit（使用FQDN）和HTTPS（在TCP端口443上）的客户：
  - 美国FQDN:radkit.us.csco.cloud
  - EMEA FQDN:radkit.emea.csco.cloud
  - APJC FQDN:radkit.apjc.csco.cloud
- 要启用RADKit以将输出附加到服务请求，CX代理必须可以访问FQDN cxd.cisco.com。
- 下表汇总了必须打开并启用CX云代理才能正常运行的端口和协议：

来源	目的地	协议	端口	目的	类型
CX Cloud Agent	所有地区： ◦ agent.us.csco.cloud ◦ Catalyst中心 AMER地区： ◦ ng.acs.agent.us.csco.cloud ◦ radkit.us.csco.cloud* EMEA地区： ◦ agent.emea.csco.cloud ◦ ng.acs.agent.emea.csco.cloud ◦ radkit.emea.csco.cloud* APJC地区：	HTTPS	TCP/443	◦ 初始配置 ◦ 升级 ◦ 库存和遥测传输 ◦ 访问RADKit云	出站到Cisco AWS区域数据中心和Catalyst Center

	◦ agent.apjc.csco.cloud ◦ ng.acs.agent.apjc.csco.cloud ◦ radkit.apjc.csco.cloud*				
CX Cloud Agent	网络设备	SNMP	UDP/161	◦ 初始发现 ◦ 持续资产收集	出站到LAN
CX Cloud Agent	网络设备	SSH	TCP/22	从CLI命令收集遥测数据	出站到LAN
CX Cloud Agent	网络设备	Telnet	TCP/23	从CLI命令收集遥测	出站到LAN
网络设备	CX Cloud Agent	系统日志	UDP/514	用于警报故障管理的传输系统日志	从LAN入站
工作站	CX Cloud Agent	SSH	TCP/22	CX云代理维护	从LAN入站

*除非使用RADKit，否则非强制性。

注意：
— 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，必须提供可用的IPv4地址、子网掩码、默认网关IP地址和域名服务(DNS)服务器IP地址。
— 仅支持IPv4。
— 经认证的单节点和高可用性(HA)Cluster Catalyst Center版本为2.1.2.x到2.2.3.x、2.3.3.x、2.3.5.x、2.3.7.x和Catalyst Center虚拟设备。
— 如果网络具有SSL拦截，则允许列表CX代理的IP地址。
— 对于所有直接连接的资产，需要SSH权限级别15。
— 仅使用提供的主机名；不应使用静态IP地址。

访问关键域

要开始 CX Cloud 之旅，用户需要以下域的访问权限。仅使用提供的主机名；请勿使用静态IP地址。

特定于CX云门户的域

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

特定于CX代理VM的域

美洲地区	欧洲、中东和非洲	亚太地区
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

注意：必须在端口443上为指定FQDN启用重定向的情况下允许出站访问。

Catalyst Center支持的版本

支持的单节点和高可用性集群Catalyst Center版本为2.1.2.x到2.2.3.x、2.3.3.x、2.3.5.x、2.3.7.x以及Catalyst Center虚拟设备和Catalyst Center虚拟设备。

支持的浏览器

为在Cisco.com上获得最佳体验，建议使用以下浏览器的最新正式版本：

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

支持的产品列表

要查看CX代理支持的产品列表，请参阅支持的产品列表。

升级/安装CX Agent v3.1.5

- 升级到新版本的现有客户应参阅升级CX代理v3.1.5
- 实施全新灵活的OVA v3.1安装的新客户应参阅添加CX代理。

将现有VM升级到大中型配置

客户可以根据自己的网络规模和复杂性，使用灵活的OVA选项将其现有的VM配置升级为中或大型。

要将现有VM配置从小型升级到中型或大型，请参阅将CX代理VM升级到中型和大型配置部分。

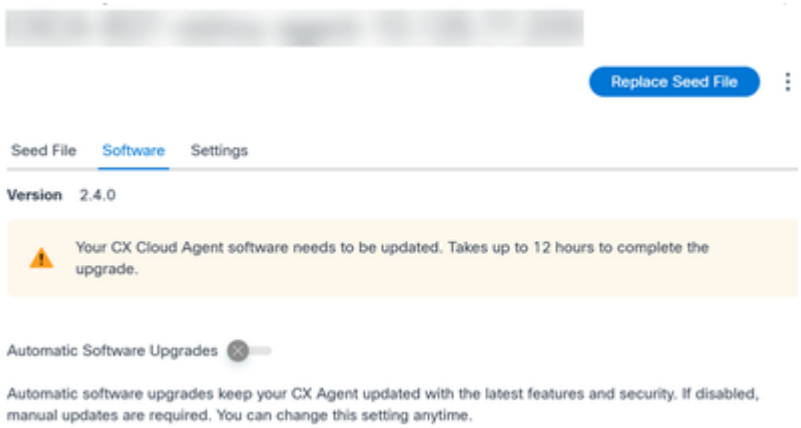
升级到CX Agent v3.1.5

现有客户可以通过启用自动升级或选择从现有版本手动升级来升级到最新版本。

注意：本指南中的图像仅供参考。实际内容可能有所不同。

自动升级

客户可以启用Automatic Software Upgrades切换以确保其系统在发布新版本时得到更新。默认情况下，此选项为新安装启用，但可随时修改以与公司策略保持一致，或在计划的维护时段内安排升级。



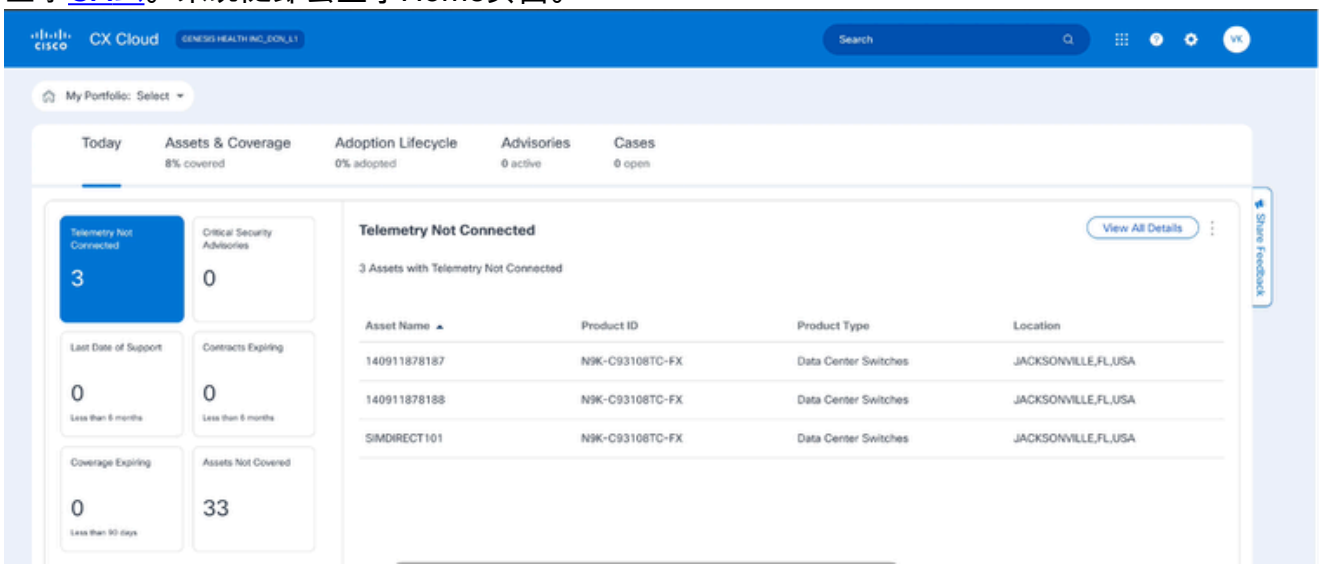
注意：默认情况下，现有CX代理实例禁用自动升级，但用户可以随时启用它们。

手动升级

如果客户不希望使用自动升级且未启用自动软件升级，则可以选择手动升级。CX代理支持直接升级到v3.1.5。

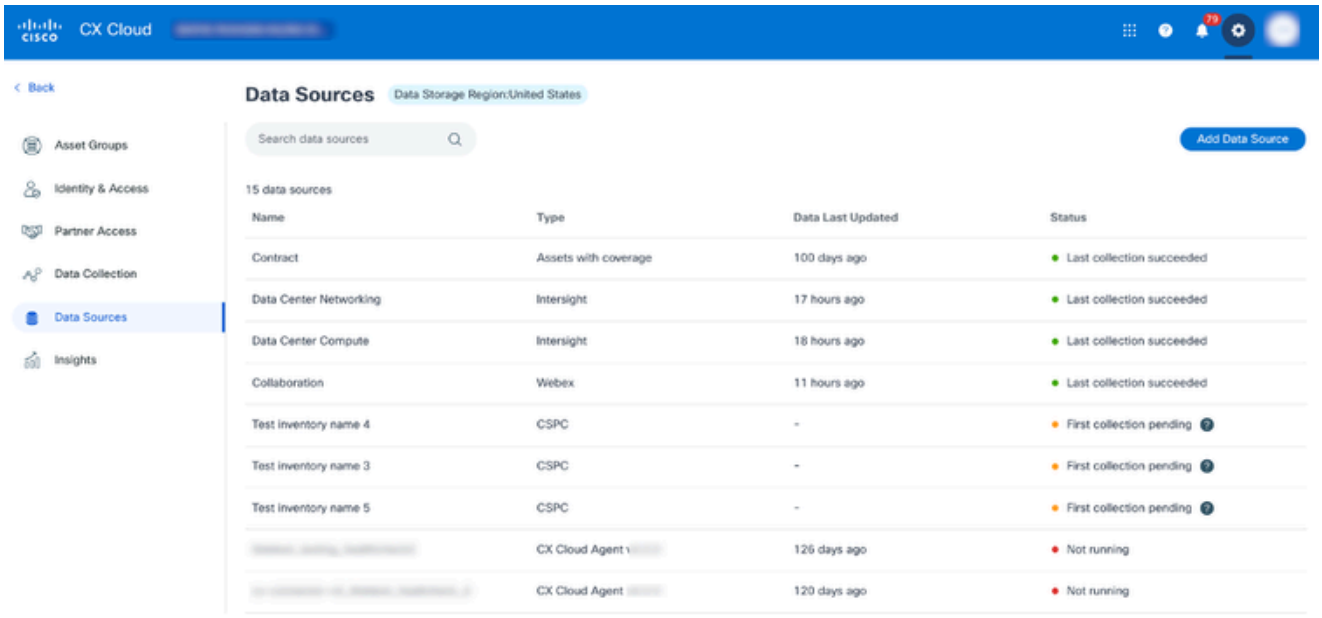
从CX云安装CX代理升级v3.1.5的步骤：

1. 登录CX云。系统随即会显示Home页面。



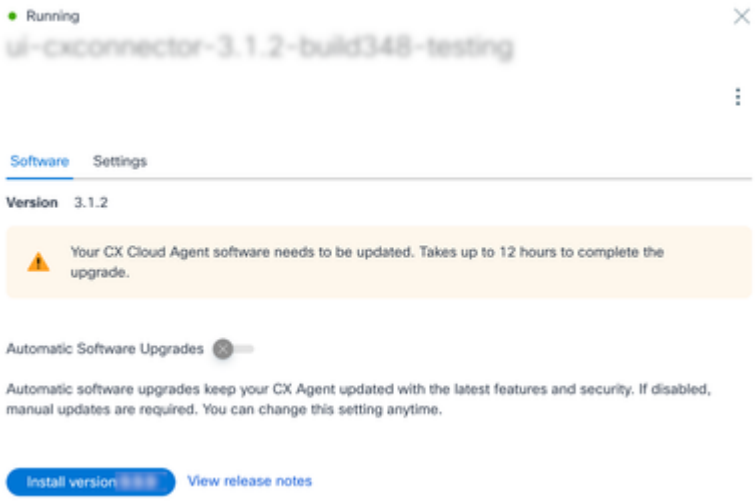
CX云主页

2. 选择Admin Center图标。Data Sources窗口打开。



数据源

3. 单击CX Agent Data Source。CX Agent详细信息窗口打开。



安装版本

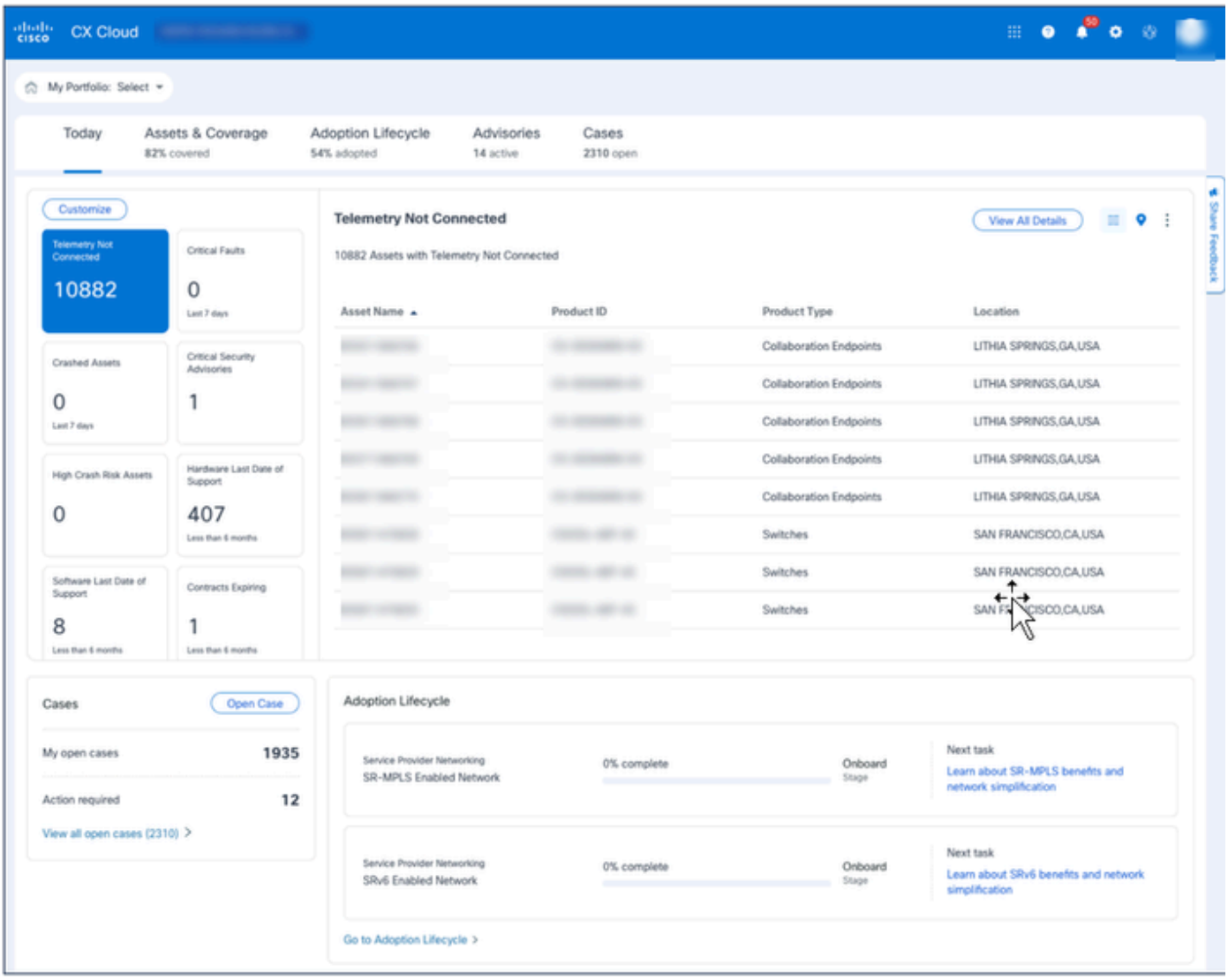
4. 单击Software选项卡。
5. 单击Install version。

添加CX代理

在CX云中，客户最多可添加20个CX代理实例。

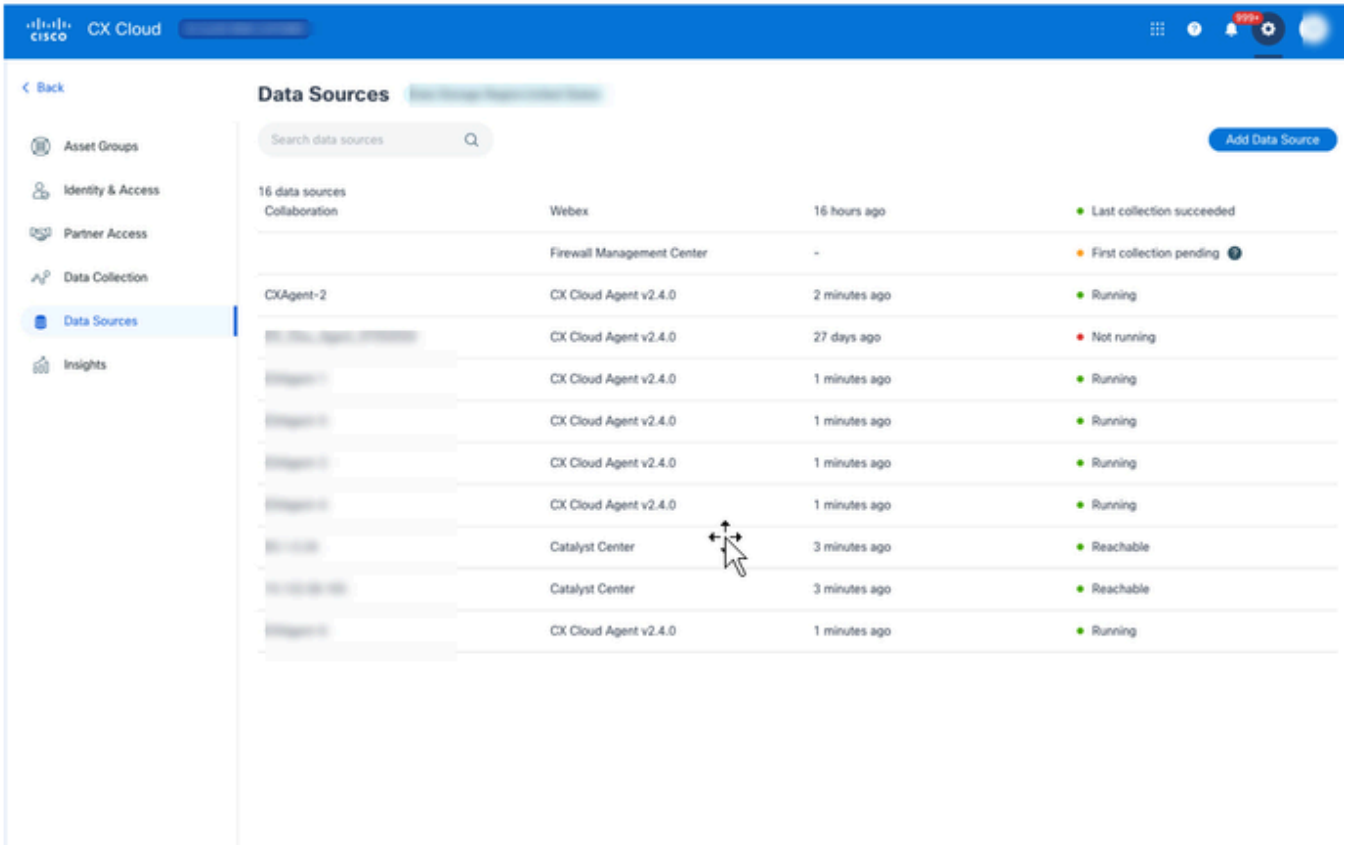
添加CX代理的步骤：

1. 登录到CX云。系统随即会显示Home页面。



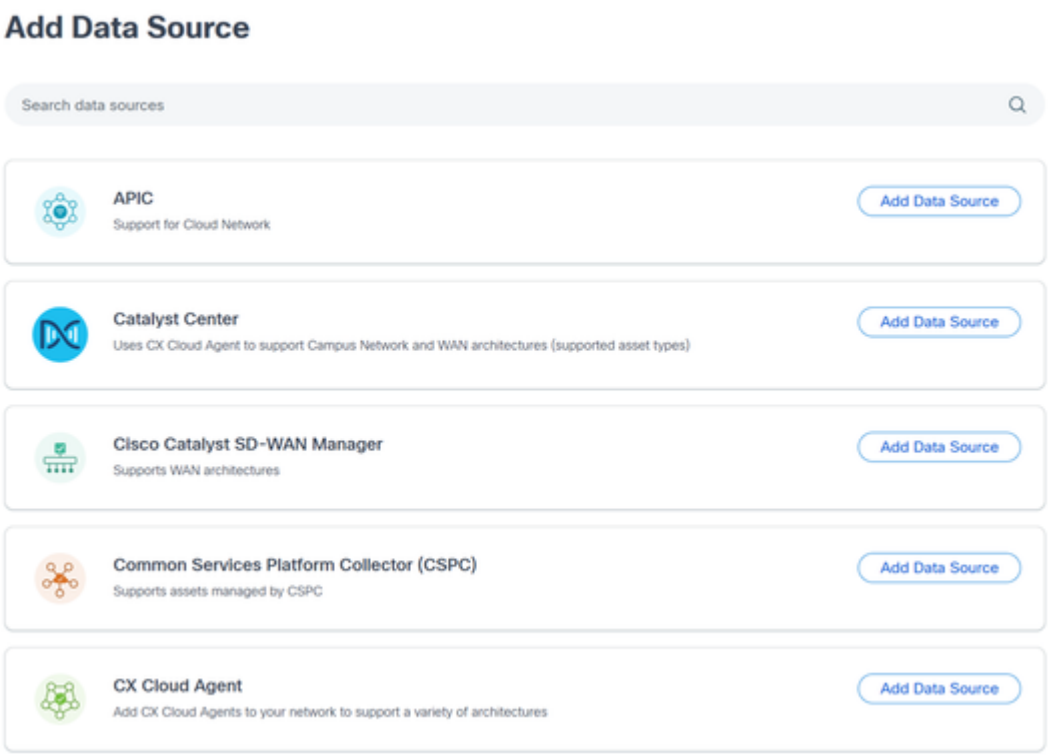
CX云主页

2. 选择Admin Center图标。Data Sources窗口打开。

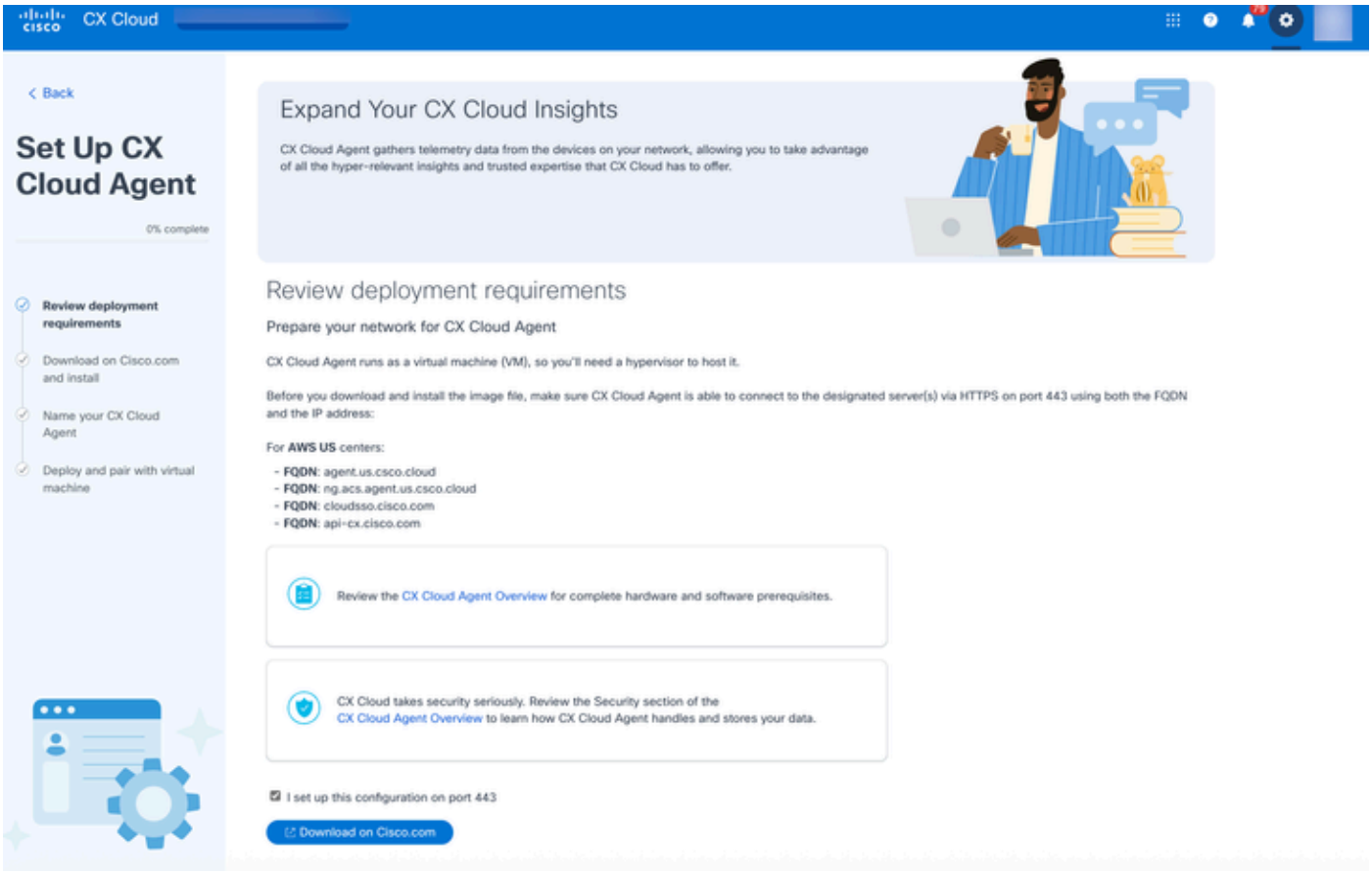


数据源

3. 单击添加数据源。将打开添加数据源页。



4. 单击CX Cloud Agent选项中的添加数据源。设置CX代理窗口打开。



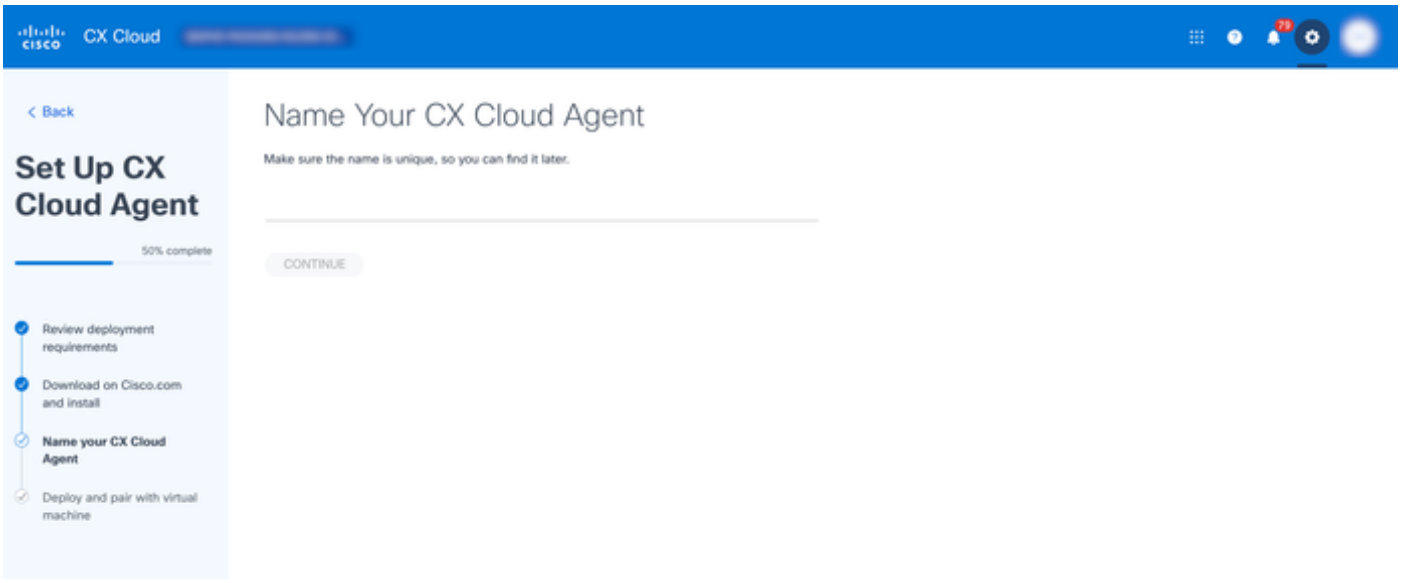
添加CX代理

5. 查看Review deployment requirements部分并选择I set up this configuration on port 443复选框。
6. 单击Cisco.com上的下载。软件下载窗口将在另一个选项卡中打开。
7. 下载“CX Agent v3.1.5 OVA”文件。

注意：在部署虚拟机后生成完成CX代理设置所需的配对代码。

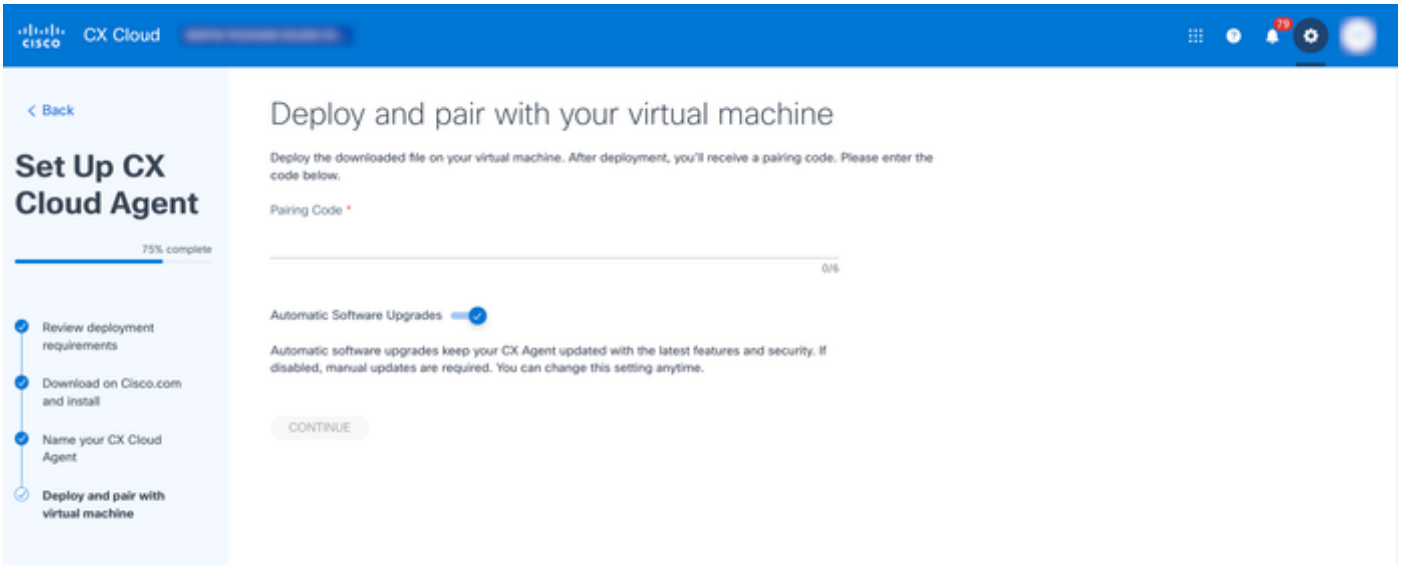
---

8. 在Name Your CX Cloud Agent字段中输入CX代理名称。



名称CX代理

9.单击继续。Deploy and pair with your virtual machine窗口打开。



配对代码

10.输入VM部署后收到的配对代码。

11.单击Continue。系统将显示注册进度，然后显示确认消息。

注意：重复上述步骤，添加其他CX代理实例作为数据源。

配置用于BCS/LCS的CX代理

思科新的融合收集功能简化了用于BCS/LCS的CX Agent v3.1配置，简化了客户体验。

BCS/LCS客户可以访问CX云社区，了解有关用户自注册及其他相关信息的更多信息。

注意：此配置特定于负责为BCS/LCS客户设置收集器的思科支持工程师。

先决条件

具有超级用户管理员(SUA)和管理员访问权限的支持工程师只能为BCS/LCS执行CX代理配置。

配置CX代理

要配置适用于BCS/LCS的CX代理，请与您指派的BCS/LCS技术咨询工程师联系。

配置RADKit功能

CX Agent v3.1.5提供可选的RADKit配置，旨在增强CX云中思科设备的远程管理和故障排除。启用

后，授权用户可以安全地远程执行数据捕获、配置和软件升级等操作。可根据客户的运行要求随时启用或禁用这些设置。

有关RADKit的详细信息，请参阅Cisco RADKit。

通过CLI集成RADKit客户端

要集成RADKit客户端服务，请创建管理员帐户并通过完成以下步骤注册该服务：

注意：以下步骤需要对CX代理VM进行root访问。

---

1. 使用适当的凭证将终端和安全外壳(SSH)打开到VM，例如：

```
ssh your_username@your_vm_ip
```

2. 运行以下命令以启用网络连接：

```
kubectl get netpol deny-from-other-namespaces -o yaml >
/home/cxcadmin/deny-from-other-namespaces.yaml

kubectl delete netpol deny-from-other-namespaces
```

3. 在本地计算机上，向管理器终结点发送POST请求以创建管理员帐户。请求正文应包括：

- admin_name（必填）：管理员帐户的用户名
- 电子邮件（可选）：管理员帐户的邮件地址
- full_name（可选）：管理员的全名
- 说明（可选）：管理员帐户的说明

以下示例展示如何使用cURL发送此请求：

```
卷曲 — X POST \

  http://<your_vm_ip>:30100/radkitmanager/v1/createAdmin \

  -H "内容类型：application/json" \

  -d '{

        "admin_name":"admin_user123",

        "电子邮件":"admin@example.com",

        "full_name":"管理员用户",

        "说明":"用于管理系统的管理员帐户"

      }'
```

成功创建管理员帐户后，服务器会以确认消息进行响应，指示已成功创建管理员帐户。此响应还包

括一个临时密码，首次登录时必须更改该密码。但是，如果管理员帐户已存在，服务器将返回400状态代码，并显示消息“Admin already created”。

4. 打开Web浏览器并导航至RADKit Web UI:https://<your_vm_ip>:30101/。
5. 使用管理员用户名(admin_name)和响应中提供的临时密码登录。

注意：首次登录时，系统会提示用户更改密码。按照屏幕上的说明设置新密码。

---

6. 在本地计算机上运行RADKit客户端以注册服务。
7. 身份验证后，通过运行以下命令生成一次性密码：

```
grant_service_otp()
```

8. 在本地计算机上，向管理器终端发送POST请求以注册服务。请求正文应包括：

- OTP（必填）：一次性密码字符串

以下示例展示如何使用cURL发送此请求：

```
卷曲 — X POST \

  http://<your_vm_ip>:30100/radkitmanager/v1/enrollService \

  -H "内容类型：application/json" \

  -d '{

        "one_time_password":"PROD:1234-1234-1234"

      }'
```

成功注册后，系统会显示确认消息，用户可以使用管理员帐户管理RADKit服务。

要禁用网络连接，请运行以下命令：

```
kubectl apply -f /home/cxcadmin/deny-from-other-namespaces.yaml
```

为现有CX代理配置保管库

可选的Vault配置功能使CX云能够安全地连接到保险存储服务，以使用最新凭证访问敏感数据（如令牌和资产列表）。启用后，CX云会自动使用配置的地址和令牌。可以随时启用或禁用此设置。目前，仅支持HashiCorp的Vault配置。

可以通过CLI配置电子仓库。

通过CLI将CX代理与HashiCorp Vault集成

本节概述配置Cisco CX代理和HashiCorp Vault实例之间的连接的过程。此集成允许安全存储和检索设备凭证，从而增强整体安全状态。

先决条件

- cxcroot访问CX代理VM



注意：必须打开支持案例才能访问cxroot和root用户。

- 运行且可访问的保管库实例

与HashiCorp Vault集成

- 要启用电子仓库集成，请运行以下命令：

```
cxcli agent vault on
```

- 要禁用保管库集成，请运行以下命令：

```
cxcli agent vault off
```

- 要检查当前电子仓库集成状态，请运行以下命令：

```
cxcli agent vault status
```

启用HashiCorp Vault集成

要启用保险存储集成，请执行以下操作：

1. 使用cxcroot用户帐户通过SSH登录到CX代理以访问CX代理。
2. 切换到根用户以通过运行以下命令提升权限：

须藤市

3.运行以下命令以检查当前电子仓库集成状态：

```
root@cxcloudagent:/home/cxcroot# cxcli agent vault status
```

已禁用保管库集成

4.运行以下命令以启用电子仓库集成：

```
cxcli agent vault on
```

5.更新以下字段：

- 保管库地址
- 保管库根令牌

6.要验证，请检查与Vault的集成状态。响应消息应确认集成已启用：

```
root@cxcloudagent:/home/cxcroot# cxcli agent vault on
```

输入HashiCorp Vault地址：

输入HashiCorp Vault令牌：

已启用存储库集成root@cxcloudagent:/home/cxcroot#

禁用HashiCorp Vault集成

要访问CX代理，请执行以下操作：

1. 使用cxcroot用户帐户通过SSH登录到CX代理。
2. 切换到根用户以通过运行以下命令提升权限：

须藤市

3.运行以下命令以禁用HashiCorp Vault集成：

```
root@cxcloudagent:/home/cxcroot# cxcli agent vault off
```

已禁用保管库集成

```
root@cxcloudagent:/home/cxcroot# |
```

HashiCorp保管库设备凭证方案

保管库凭据方案:有关设备凭据的可用选项和支持字段的详细信息，请参阅“保管库凭据方案”文件。

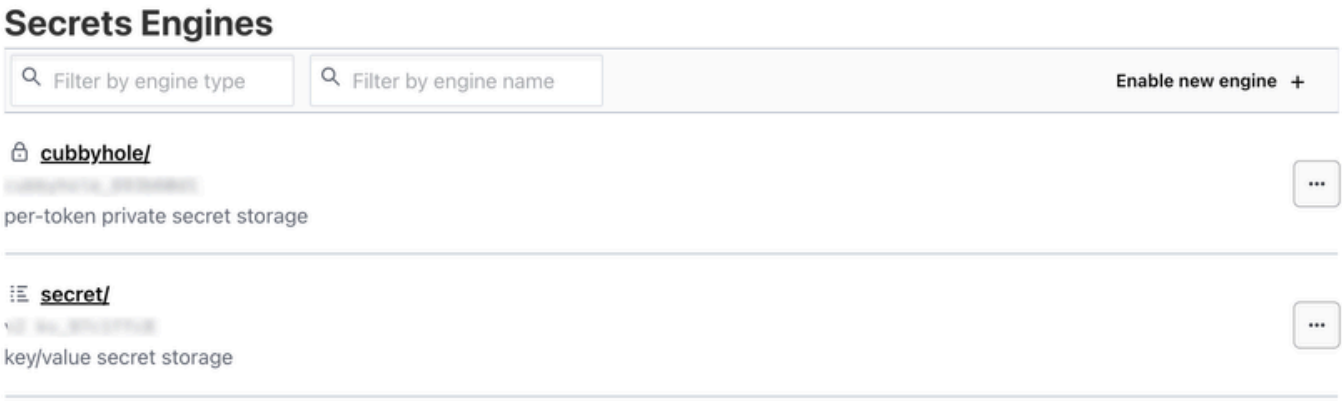
示例：以下是基于架构的JSON凭据的示例：

```
{
"targetIp": "5.0.1.*",
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
"password": "*******",
"enableUser": "cisco",
"enablePassword": "*******"
}
}
}
```

注意：用户可以在单个凭证JSON文件中指定多个协议。但是，应避免包含同一系列的重复协议（例如，不要在同一凭证文件中同时包含SNMPv2c和SNMPv3）。

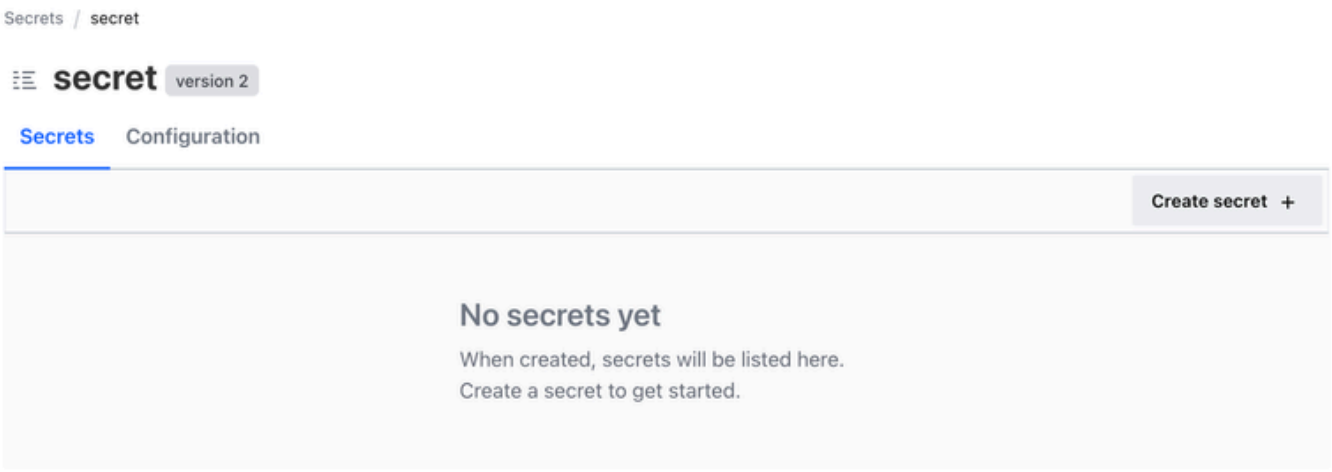
在HashiCorp Vault中配置设备凭证(第一次)

1. 登录到Vault实例。



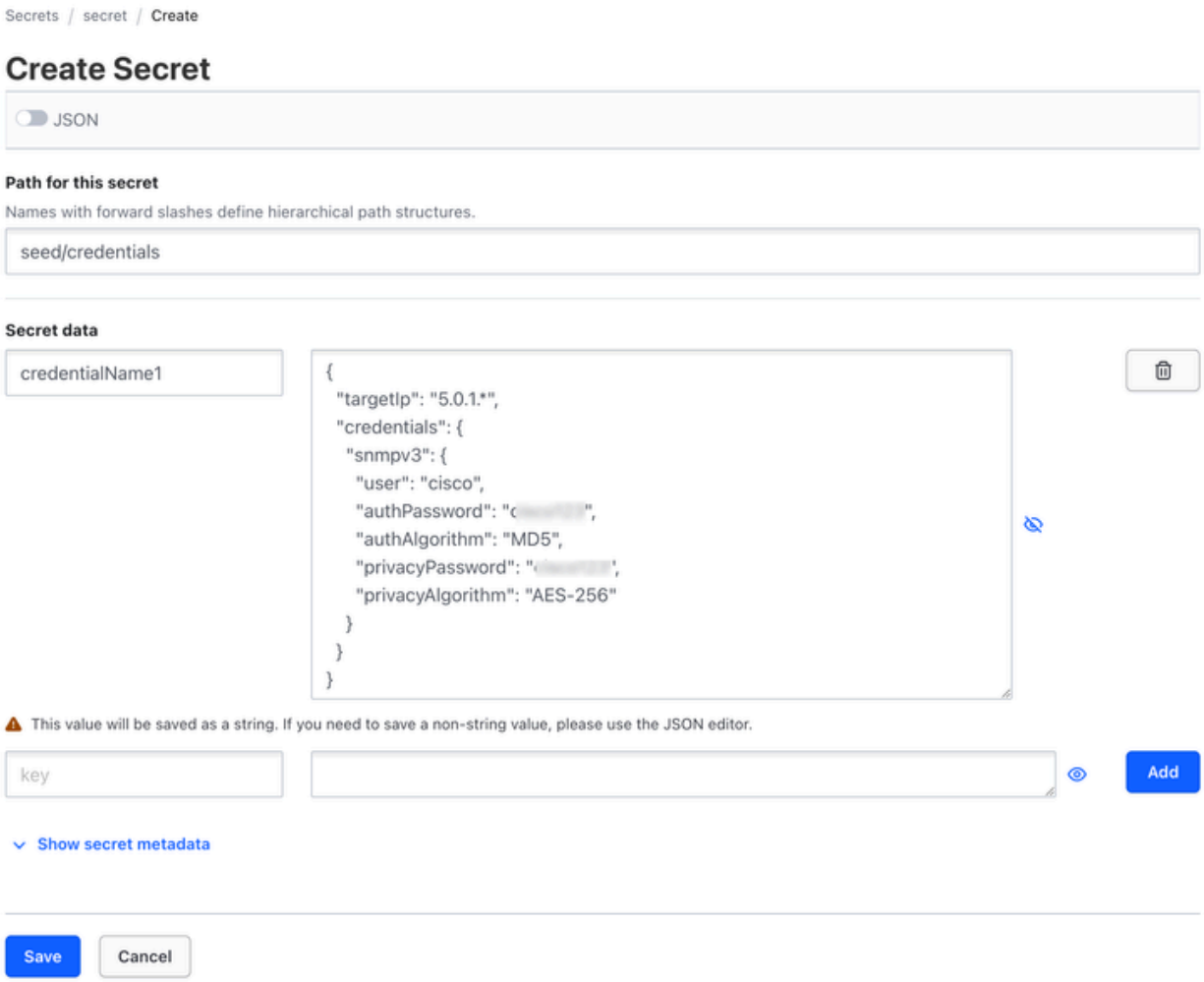
Secret

2. 使用以下路径创建新的密钥值密钥：secret/seed/credentials。
3. 选择key-value secret storage engine(secret/)。



密钥值密钥

4. 单击创建密钥。Create Secret窗口打开。

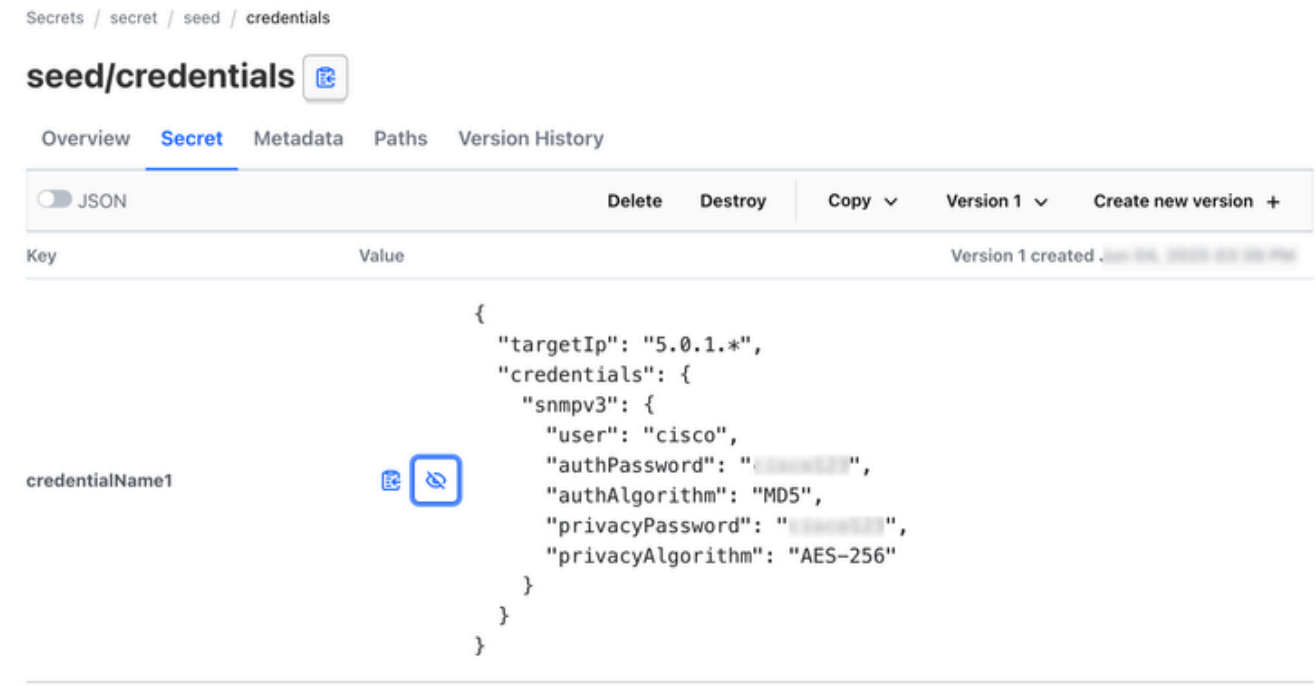


客户端密码

5.更新以下字段：

- 加密路径:种子/凭证
- 加密数据:密钥收集 — 价值机密
- 密钥:自定义唯一凭证名称
- 值：凭证JSON

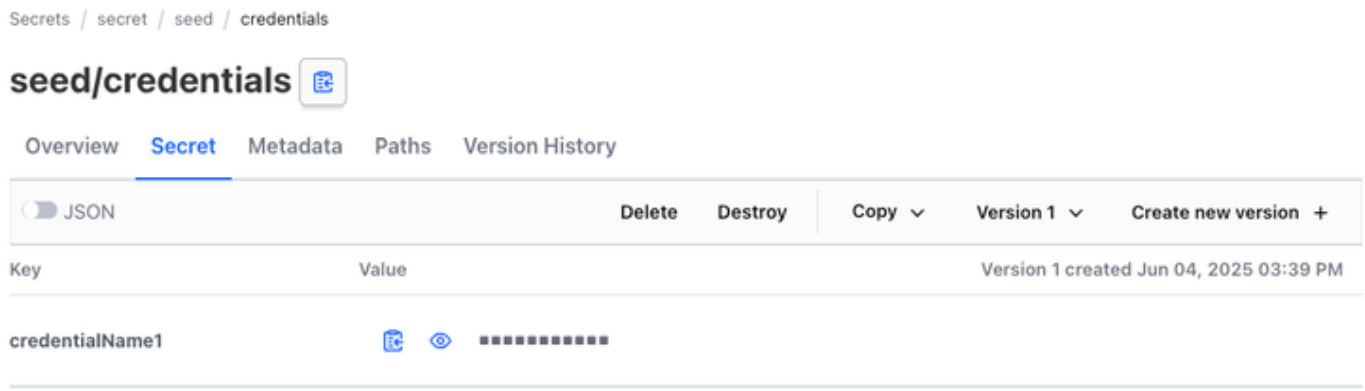
6.单击保存。机密现在应该储存在HashiCorp Vault中。



凭证

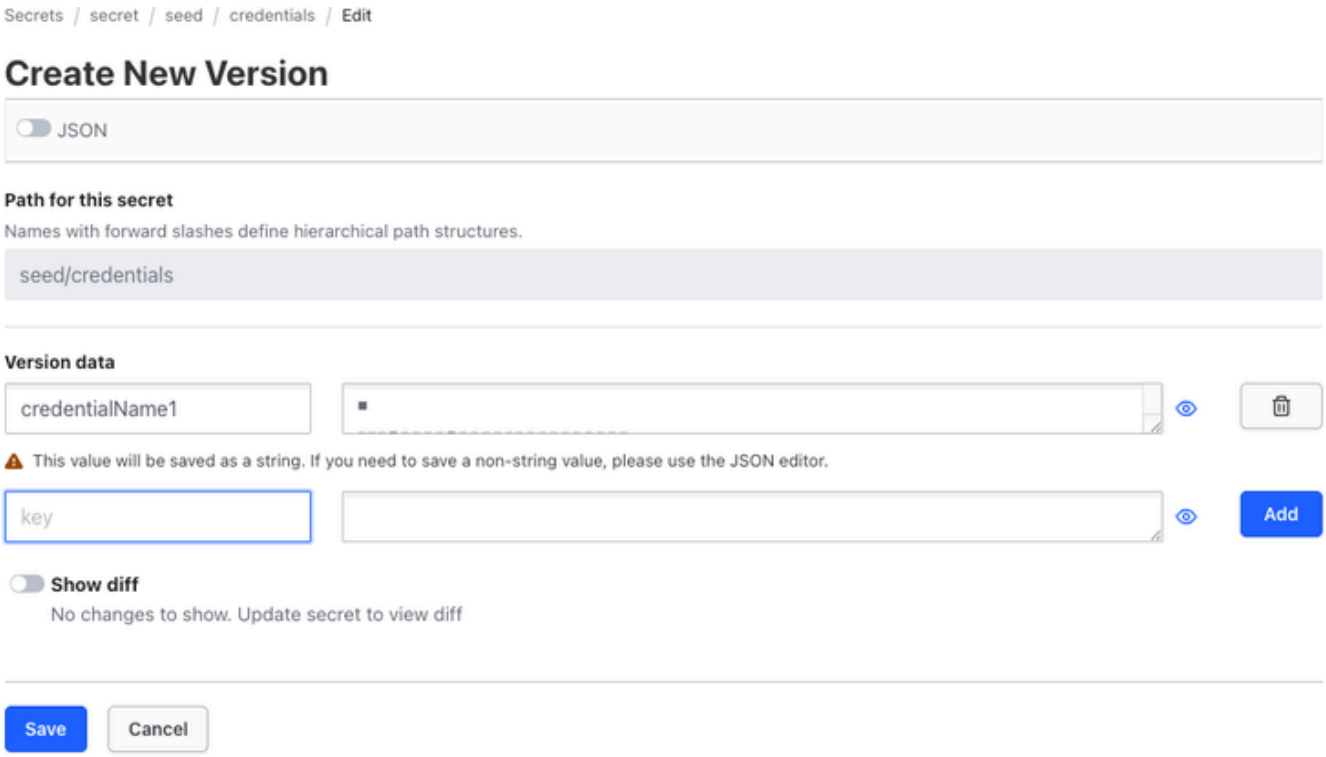
向HashiCorp Vault添加更多凭证

1. 登录到HashiCorp保管库实例。



添加凭证

2. 导航到已创建的密钥“密钥/种子/凭据”。



创建版本

3.单击创建新版本。

4.根据需要提供任意数量的密钥值对来添加新的密钥。

5.单击保存。

具有默认凭证的CX云种子文件

- 简化种子文件:使用通过Hashicorp保管库配置的凭证时，通过忽略敏感信息来简化种子文件
- 仅指定IP地址或主机名:用户只能传递种子文件中的IP地址或主机名，而将其他字段留空

```
5.0.1.2,,,,,,,,,,,,,,,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

IP或主机名

- 使用HashiCorp保管库和种子文件凭证:在种子文件中为某些设备提供凭证，同时依赖保管库管理其他设备的凭证

```
5.0.1.1,snmpv3,,username,,,,,,,cliUser,cliPassword,,enablePassword,,,
25.0.1.2,snmpv2c,readOnlyPassword,,,,,,,sshv2,,cliUser,cliPassword,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

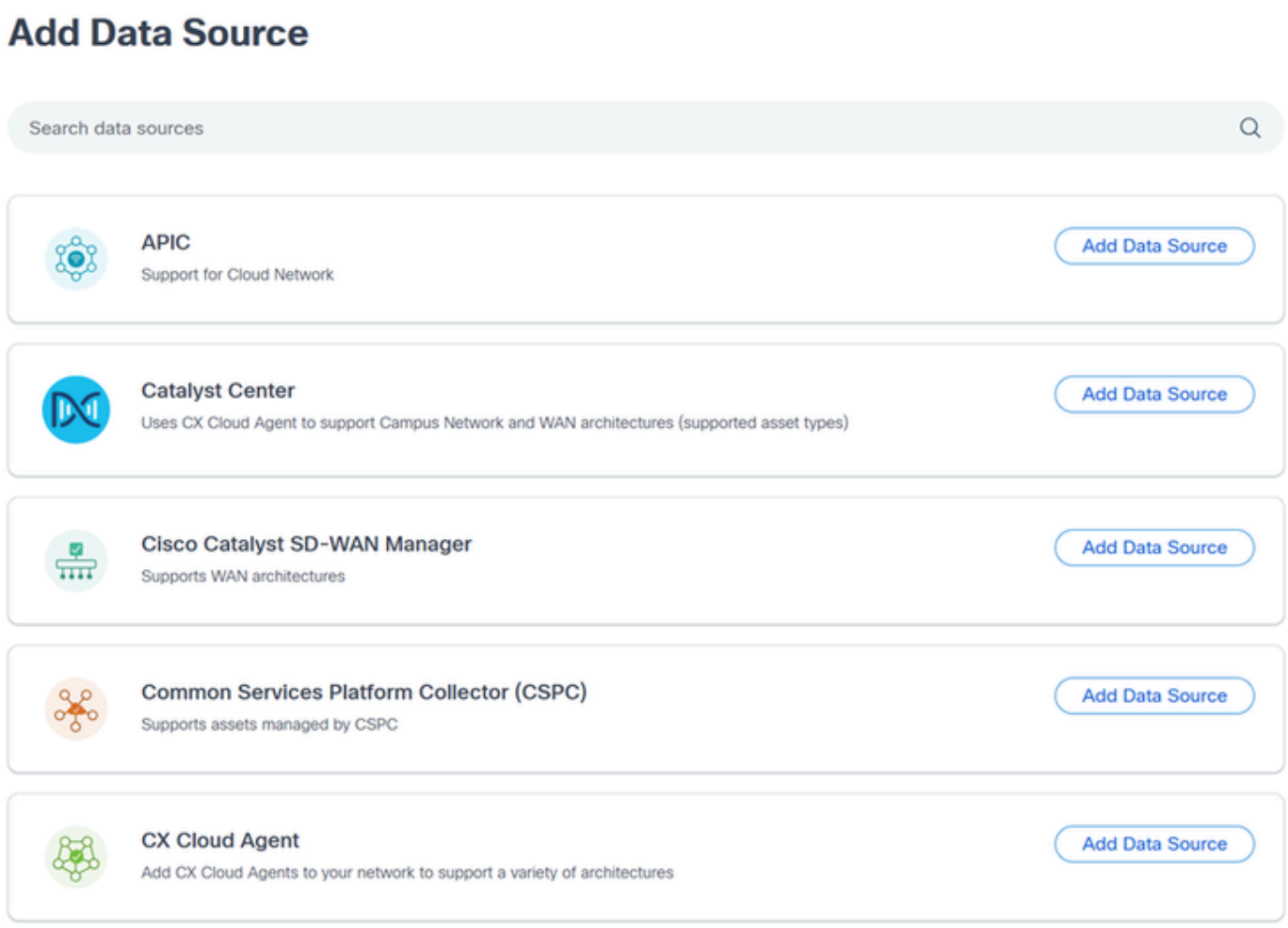
IP或主机名

添加Catalyst Center作为数据源

具有超级管理员用户角色的用户可以添加Catalyst Center数据源。

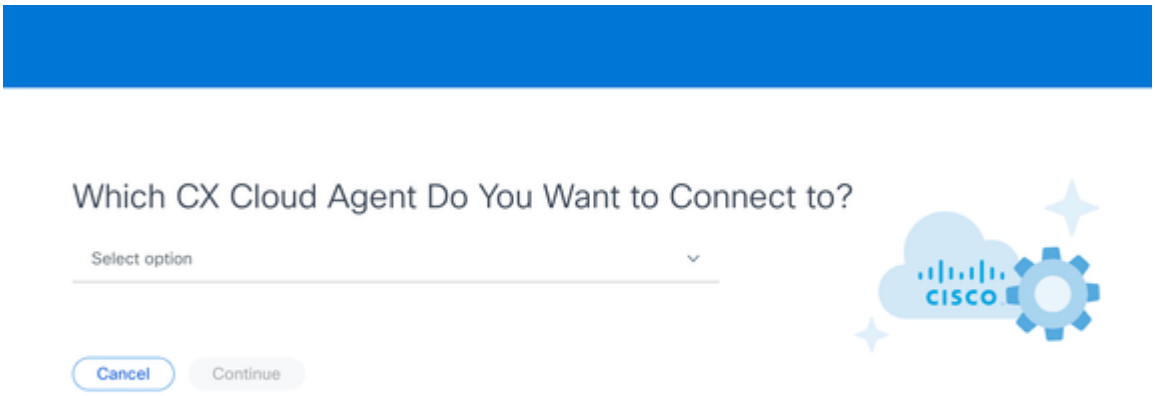
添加Catalyst Center作为数据源的步骤：

1. 选择管理中心图标。Data Sources窗口打开。
2. 单击添加数据源。系统随即会显示添加数据源页。



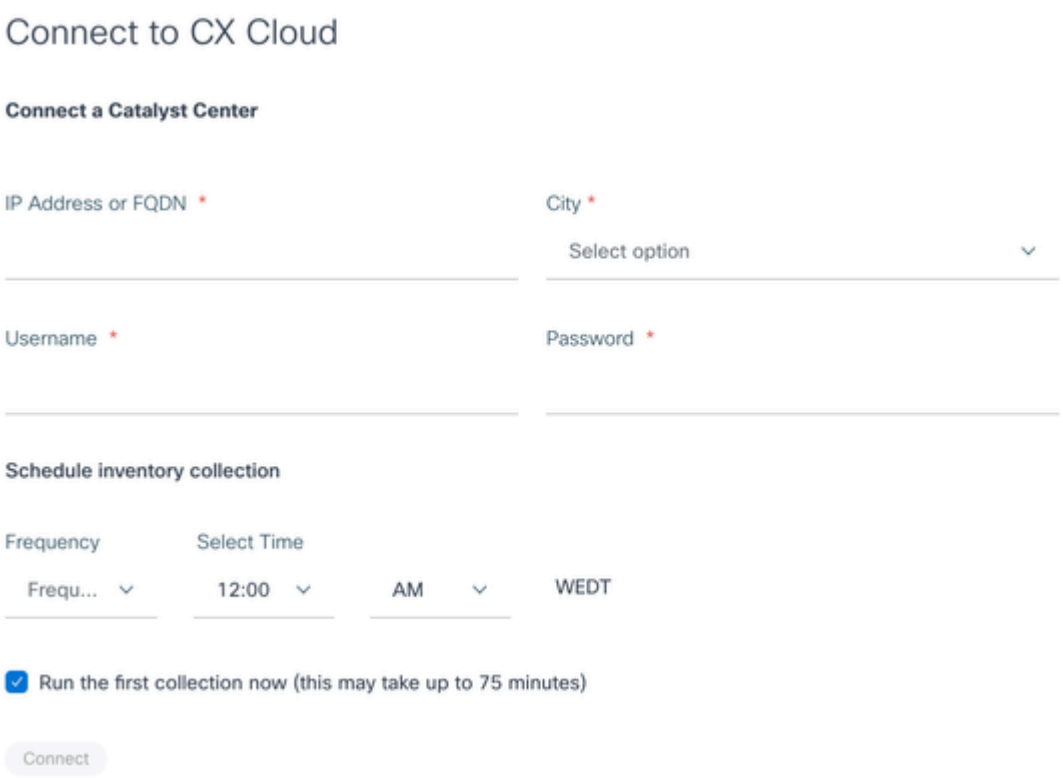
Catalyst中心

3. 单击Catalyst Center选项中的添加数据源。



选择CX代理

4. 从Which CX Agent Do You Want to Connect to下拉列表中选择CX代理。
5. 单击 Continue。连接到CX云窗口打开。



频率

6. 输入以下详细信息:

- 虚拟IP地址或FQDN（即，Catalyst Center IP地址）
- 城市（即Catalyst中心的位置）
- 用户名
- 密码
- 频率和选择时间以指示CX代理程序在“计划资产收集”部分中执行网络扫描的频率

注意：选中Run the first collection now复选框以立即运行收集。

7. 单击 Connect。系统随即会显示Catalyst Center IP地址的确认信息。

添加BCS/LCS数据源

警告：以下数据源仅适用于BCS转发资产。

添加SolarWinds®

注意：如果需要添加SolarWinds®数据源，请与思科支持联系以获得帮助。

BCS/LCS客户现在可以使用CX Agent功能与SolarWinds®进行外部集成，通过提高自动化程度提供更高的透明度、改进的可管理性和增强的用户体验。CX代理收集资产和其他所需数据，以生成各种报告，这些报告的格式、数据完整性和数据准确性与Operational Insights收集器生成的当前报告一致。CX代理支持SolarWinds®集成，方法是：允许BCS/LCS客户使用CX代理替换OIC，以便从Solarwinds®收集数据。

注意：此功能(包括Solarwinds®数据源)仅向BCS/LCS客户提供。

在第一次收集之前，必须在BCS转发中配置CX代理；否则，文件将保持未处理状态。有关BCS转发配置的详细信息，请参阅为BCS或LCS配置CX代理部分。

注意：
— 来自同一SolarWinds®实例的多个集合覆盖以前的文件（以后上传优先）。
— 支持多个源，但每个SolarWinds®实例必须具有唯一的IP和设备ID。

添加EPNM

BCS/LCS客户现在可以使用CX代理功能从外部与演进可编程网络管理器(EPNM)集成。 CX代理收集清单和其他所需数据以生成各种报告，这些报告在格式、数据完整性和数据准确性方面与OIC生成的当前报告一致。

添加APIC

BCS/LCS客户现在可以使用CX代理功能从外部与应用策略基础设施控制器(APIC)集成。 CX代理收集清单和其他所需数据以生成各种报告，这些报告在格式、数据完整性和数据准确性方面与OIC生成的当前报告一致。

添加其他资产作为数据源

遥测收集已扩展至非由Catalyst Center管理的设备，使用户能够查看遥测衍生的见解，并与针对更广泛设备的分析进行交互。在初始CX代理设置后，用户可以选择配置CX代理以连接到CX云监控的基础设施中的20个其他Catalyst中心。

用户可以通过使用种子文件唯一标识要合并到CX云中的设备，或通过指定IP范围（应由CX代理进行扫描）来标识这些设备。两种方法都依赖简单网络管理协议(SNMP)进行发现以及安全外壳(SSH)进行连接。这些必须正确配置才能成功收集遥感勘测数据。

要添加其他资产作为数据源，请使用以下任一选项：

- 使用种子文件模板上传种子文件
- 提供IP地址范围

发现协议

基于种子文件的直接设备发现和基于IP范围的发现都依赖SNMP作为发现协议。存在不同版本的SNMP，但CX代理支持SNMPv2c和SNMPv3，并且可配置任一或两种版本。用户必须提供相同的信息（如下面完整详述）才能完成配置并启用SNMP管理的设备与SNMP服务管理器之间的连接。

SNMPv2c和SNMPv3在安全性和远程配置模型方面有所不同。SNMPV3使用支持SHA加密的增强型加密安全系统来验证消息并确保其隐私。建议在所有公有网络和面向Internet的网络中使用SNMPv3，以防御安全风险和威胁。在CX云上，最好配置SNMPv3而不是SNMPv2c，但缺少内置支持SNMPv3的旧版设备除外。如果两个版本的SNMP均由用户配置，则CX代理会默认尝试使用SNMPv3与各个设备通信，并在无法成功协商通信时恢复为SNMPv2c。

连接协议

作为直接设备连接设置的一部分，用户必须指定设备连接协议的详细信息：SSH（或者Telnet）。应使用SSHv2，但个别传统资产缺乏相应内置支持的情况除外。请注意，SSHv1协议包含基本漏洞。当依赖SSHv1时，如果没有额外的安全性，遥测数据和底层资产可能会因这些漏洞而受到危害。Telnet也不安全。通过telnet提交的凭证信息（例如，用户名和密码）不加密，因此很容易受到危害，并且没有额外的安全性。

设备的遥测处理限制

以下是处理设备的遥测数据时的限制：

- 某些设备在收集摘要中可能显示为可访问，但在CX云资产页中不可见。
- 如果种子文件或IP范围集合中的设备也是Catalyst Center资产的一部分，则仅针对Catalyst Center条目报告一次该设备。种子文件或IP范围条目中的相应设备被跳过，以避免重复。
- CX云中不支持Cisco IP电话来进行CX代理的数据收集。因此，思科IP电话不会显示在资源列表中。

使用种子文件添加其他资产

种子文件是.csv文件，其中每一行代表系统数据记录。在种子文件中，每个种子文件记录都对应于CX代理应从中收集遥测的唯一设备。将从要导入的种子文件中捕获每个设备条目的所有错误或信息

消息，作为作业日志详细信息的一部分。种子文件中的所有设备都被视为受管设备，即使设备在初始配置时无法访问。如果上传新的种子文件来替换以前的种子文件，上次上传的日期会显示在CX云中。

CX代理将尝试连接到设备，但是如果无法确定PID或序列号，可能无法处理每个设备以在资产页面中显示。

种子文件中以分号开头的任何行都会被忽略。种子文件中的标题行以分号开头，可在创建客户种子文件时保留为（推荐选项）或删除该标题行。

用户可以采用与标准CX云种子文件相同的方式上传公共服务平台收集器(CSPC)种子文件，并且在CX云中管理任何所需的重新格式化。

对于CX代理v3.1.5及更高版本，客户可以以CSPC或CX格式上传种子文件；早期的CX代理版本仅支持CX格式种子文件。

示例种子文件（包括列标题）的格式不得以任何方式更改，这一点非常重要。

下表列出了所有必需的种子文件列以及必须包含在每个列中的数据。

种子文件列	列标题/标识符	列的用途
A	IP 地址或主机名	提供设备的有效、唯一的IP地址或主机名。
B	SNMP协议版本	SNMP协议是CX代理所必需的，用于客户网络中的设备发现。值可以是snmpv2c或snmpv3，但出于安全考虑，建议使用snmpv3。
C	snmpRo :如果col#=3被选为“snmpv2c”，则为必填项	如果为特定设备选择SNMPv2的旧变体，则必须指定设备SNMP集合的snmpRO（只读）凭证。否则，条目可以为空。
D	snmpv3用户名：如果col#=3被选为“snmpv3”，则为必填项	如果选择SNMPv3与特定设备进行通信，则必须提供各自的登录用户名。
E	snmpv3AuthAlgorithm:值可以是MD5或SHA	SNMPv3协议允许通过消息摘要(MD5)或安全散列算法(SHA)进行身份验证。 如果设备配置了安全身份验证，则必须提供相应的身份验证算法。 注意：MD5被视为不安全，SHA可在

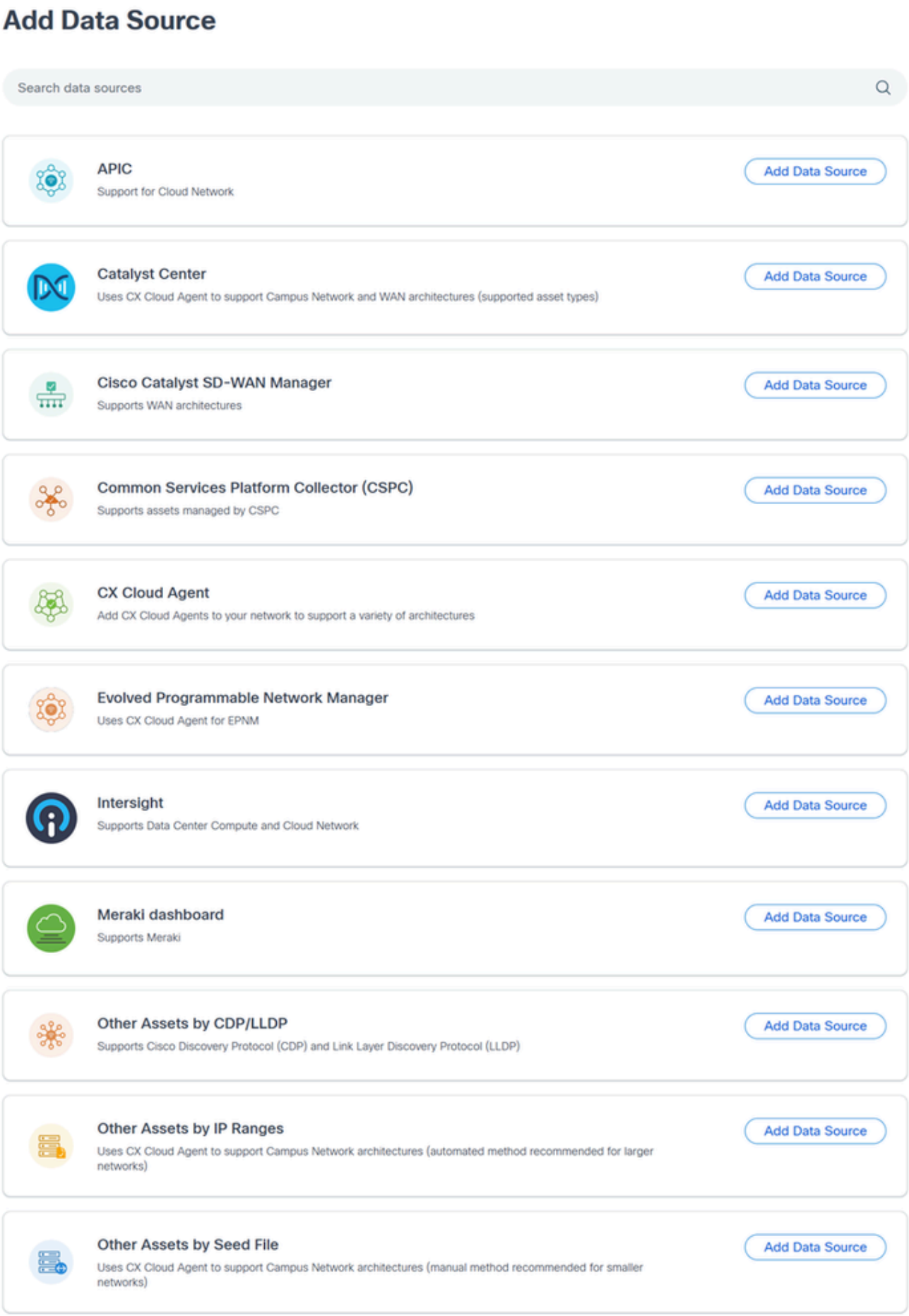
种子文件列	列标题/标识符	列的用途
		支持它的所有设备上使用。
F	snmpv3AuthPassword :密码	如果在设备上配置了MD5或SHA加密算法，则需要为设备访问提供相关身份验证密码。
G	snmpv3PrivAlgorithm:值可以是DES、3DES、AES-128、AES-192、AES-256	如果设备配置了SNMPv3隐私算法（此算法用于加密响应），则需要提供相应的算法。  注意：数据加密标准(DES)使用的56位密钥太短，无法提供加密安全性，并且三重数据加密标准(3DES)可用于支持它的所有设备。
H	snmpv3PrivPassword :密码	如果在设备上配置了SNMPv3隐私算法，则需要为设备连接提供其各自的隐私密码。
I	snmpv3EngineId:engineID，表示设备的唯一ID，如果手动在设备上配置，请指定引擎ID	SNMPv3 EngineID是代表每个设备的唯一ID。在收集CX代理的SNMP数据集时，会发送此引擎ID作为参考。如果客户手动配置EngineID，则需要提供相应的EngineID。
J	cliProtocol:值可以是'telnet'、'sshv1'、'sshv2'。 如果空值默认可设置为“sshv2”	命令行界面(CLI)用于直接与设备交互。CX代理将此协议用于特定设备的CLI收集。此CLI收集数据用于CX云中的资产和其他见解报告。建议使用SSHv2;如果没有其他网络安全措施，SSHv1和Telnet协议本身无法提供足够的传输安全性。
K	cliPort :CLI协议端口号	如果选择了任何CLI协议，则需要提供其各自的端口号。例如，22表示SSH，23表示telnet。
L	cliUser :CLI用户名(可以提供CLI用户名/密码或两者，但两列（col#=12和col#=13）不能为空。)	需要提供设备的相应CLI用户名。CX云代理在CLI收集期间连接到设备时使用此功能。

种子文件列	列标题/标识符	列的用途
M	cliPassword :CLI用户密码(可以提供CLI用户名/密码或两者，但两列（col#=12和col#=13）不能为空。)	需要提供设备的相应CLI密码。CX代理在CLI收集期间连接到设备时使用此功能。
n	cliEnableUser	如果在设备上配置了enable，则需要提供设备的enableUsername值。
O	cliEnablePassword	如果在设备上配置了enable，则需要提供设备的enablePassword值。
P	未来支持（无需输入）	留作将来使用
问	未来支持（无需输入）	留作将来使用
R	未来支持（无需输入）	留作将来使用
S	未来支持（无需输入）	留作将来使用

使用新的种子文件添加其他资产

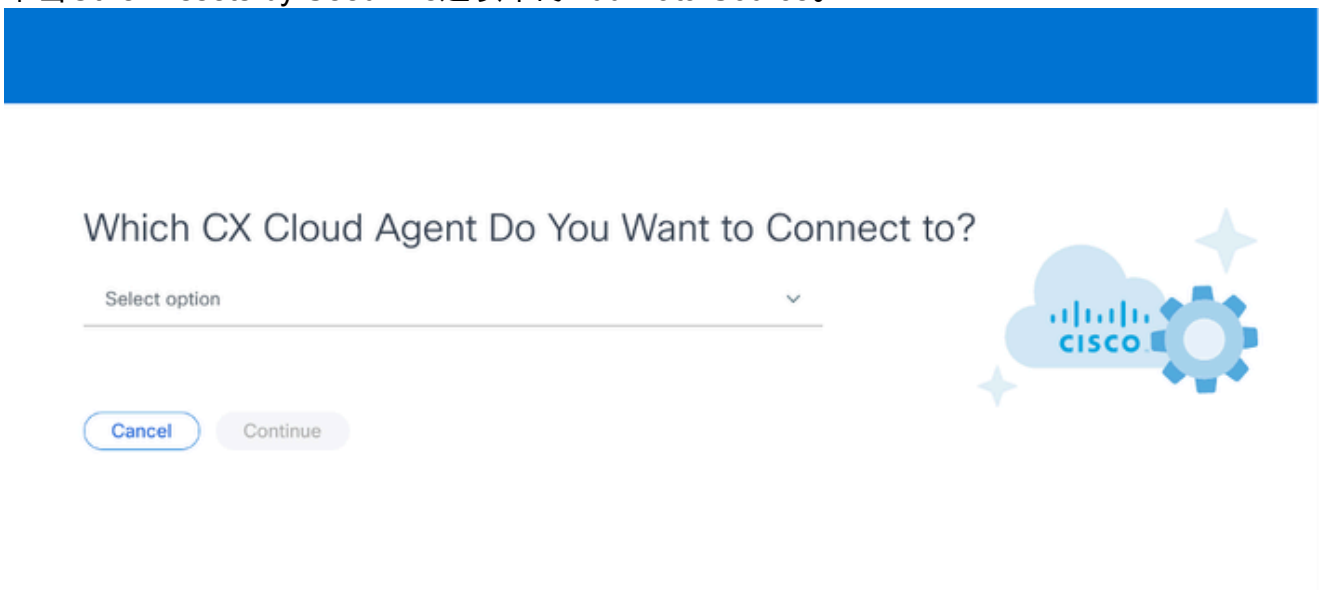
要使用新的种子文件添加其他资产，请执行以下操作：

1. 在Admin Center > Data Sources窗口中单击Add Data Source。



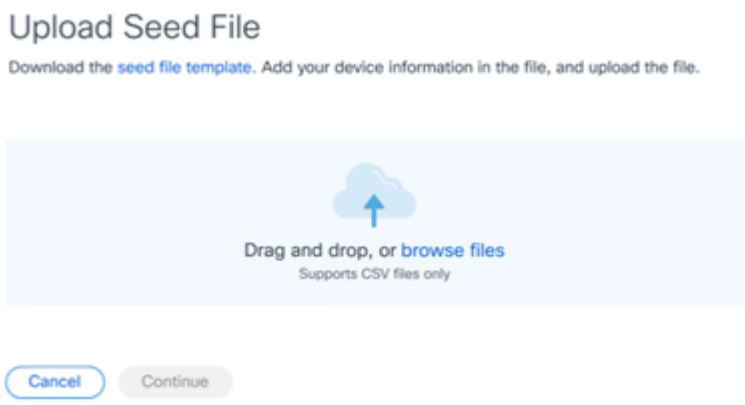
按种子文件分类的其他资产

2. 单击Other Assets by Seed File选项中的Add Data Source。



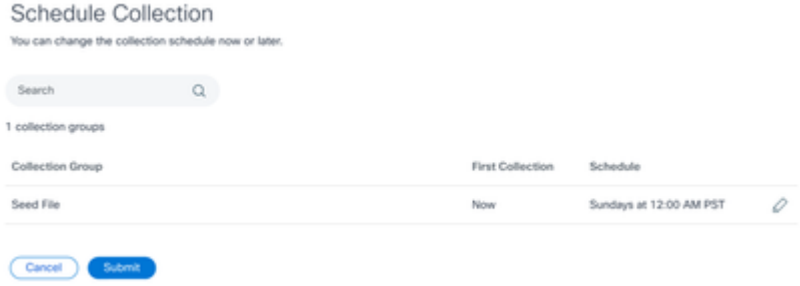
选择CX代理

3. 从Which CX Cloud Agent Do You Want to Connect to下拉列表中选择CX代理。
4. 单击 Continue。系统将显示Upload Seed File页面。



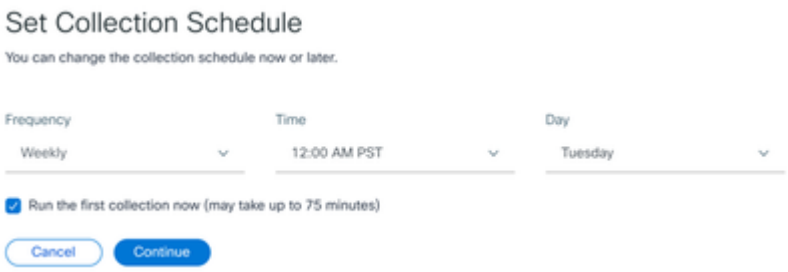
上传种子文件

5. 点击超链接种子文件模板下载模板。
6. 手动输入数据或将数据导入到文件中。完成后，将模板另存为.csv文件以将该文件导入CX代理。
7. 拖放或点击browse文件上传.csv文件。
8. 上传文件后，单击Continue。系统随即会显示计划收集页面。



计划收集

9. 单击Edit图标。系统随即会显示设置收集计划页面。



设置收集计划

10. 从以下下拉列表中选择一个选项：
    - 频率
    - 时间
    - 日
11. 选中Run the first collection now复选框以运行收集。

> 注意：在完成CX云的初始配置之前，CX云代理必须通过处理种子文件并与所有确定的设备建立连接来执行第一次遥测收集。可以按需启动收集，也可以根据此处定义的计划运行收集。用户可以通过选中Run the first collection now复选框执行第一个遥测连接。根据种子文件中指定的条目数量和其他因素，此过程可能需要相当长的时间。

12. 单击 Continue。系统将重新显示Schedule Collection页面。
13. 单击 submit。将打开数据源窗口，显示一条确认消息。

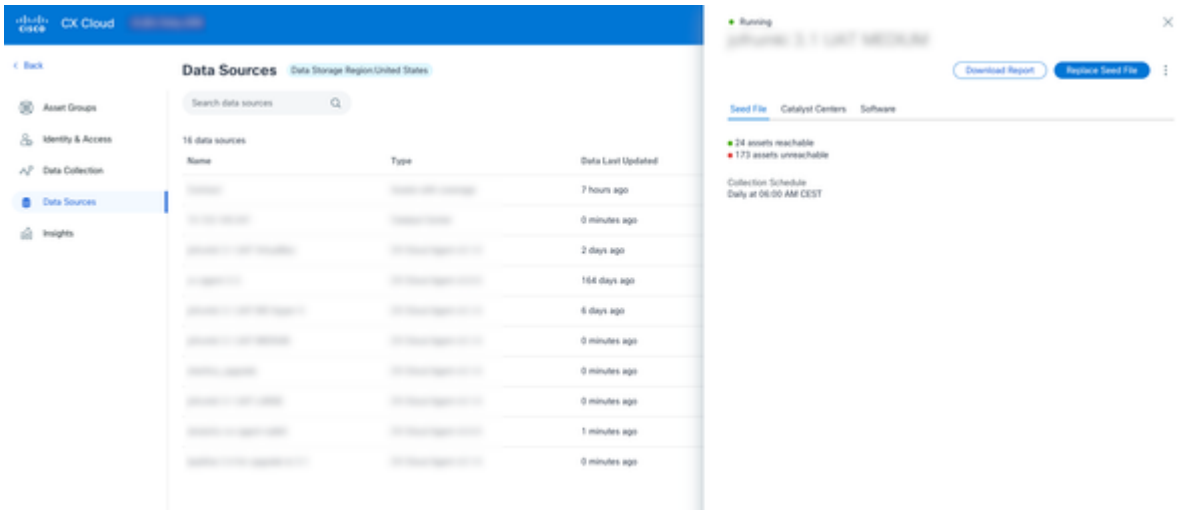
使用已修改的种子文件添加其他资产

要使用当前种子文件添加、修改或删除设备，请执行以下操作：

1. 打开先前创建的种子文件，进行所需的更改，然后保存文件。

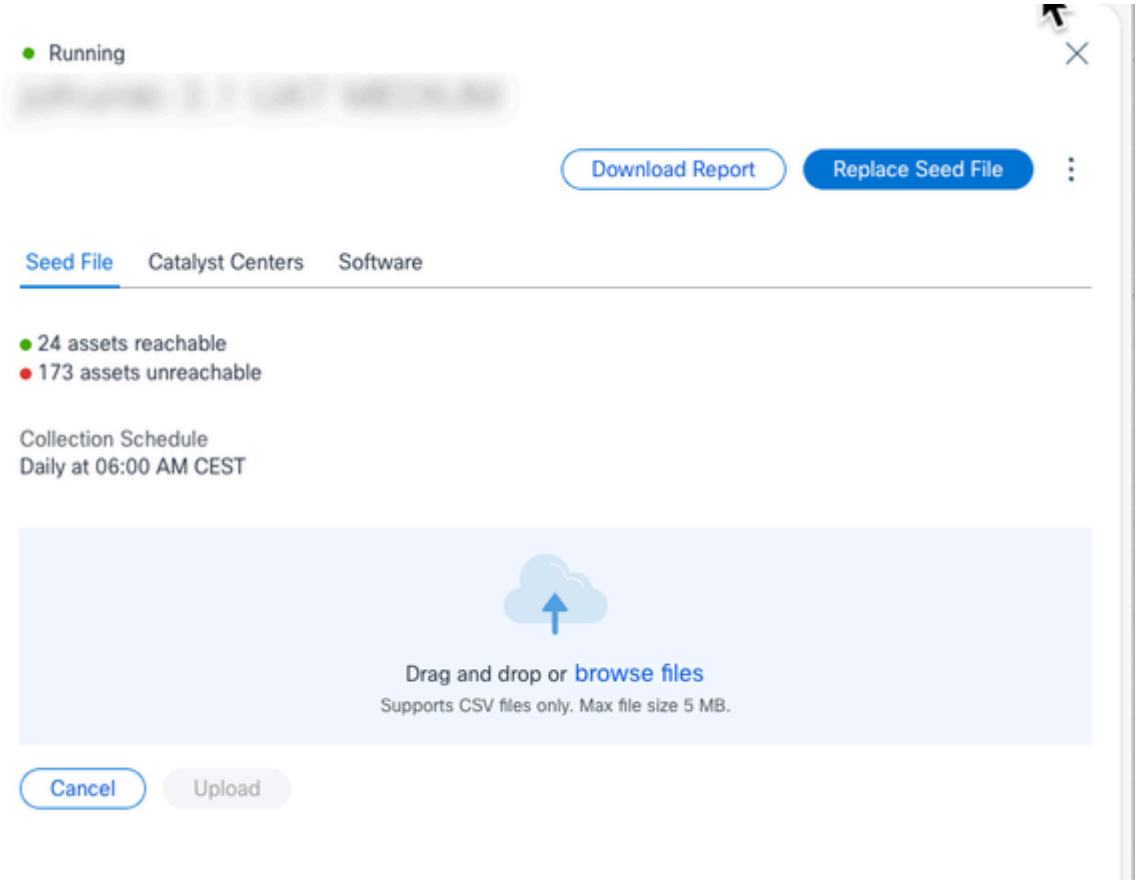
> 注意：要将资源添加到种子文件，请将这些资源附加到以前创建的种子文件，然后重新加载文件。这是必要的，因为上传新的种子文件会替换当前的种子文件。仅最新上传的种子文件用于发现和收集。

2. 在数据源页中，单击需要更新种子文件的CX代理数据源。CX Agent详细信息窗口打开。



种子文件

3. 单击替换种子文件。



替换种子文件

4. 拖放或单击浏览文件上传已修改的种子文件。
5. 单击Upload。

种子文件的默认凭据

CX代理不需要在种子文件中直接包含敏感密码。这通过减少机密信息的泄露提高了安全性，解决了客户关心的关键问题。有关启用此功能的信息，请参阅为现有CX代理配置Vault。

使用IP范围添加其他资产

IP范围允许用户识别硬件资产，然后根据IP地址从这些设备收集遥感勘测数据。通过指定单个网络级IP范围（CX代理可使用SNMP协议对其进行扫描），可以唯一标识遥测收集的设备。如果选择IP范围来标识直连设备，则所引用的IP地址可能受到尽可能严格的限制，同时允许覆盖所有需要的资产。

- 可以提供特定IP，也可以使用通配符替换IP的八位组以创建范围。
- 如果特定IP地址未包含在设置期间识别的IP范围内，CX代理不会尝试与具有此类IP地址的设备通信，也不会从此类设备收集遥测数据。
- 输入*.*.*.*允许CX代理将用户提供的凭据用于任何IP。例如：172.16.*.*允许将凭证用于172.16.0.0/16子网中的所有设备。
- 如果网络或客户群(IB)有任何变更，则可以修改IP范围。请参阅编辑IP范围

CX代理将尝试连接到设备，但是如果无法确定PID或序列号，则可能无法处理每个设备以在资产视图中显示。

注意：
单击Edit IP Address Range启动按需设备发现。将任何新设备（在指定IP范围之内或之外）添加或删除时，客户必须始终单击Edit IP Address Range(参阅Editing IP Ranges部分)，并完成启动按需设备发现所需的步骤，以将任何新添加的设备包含到CX代理程序收集清单中。

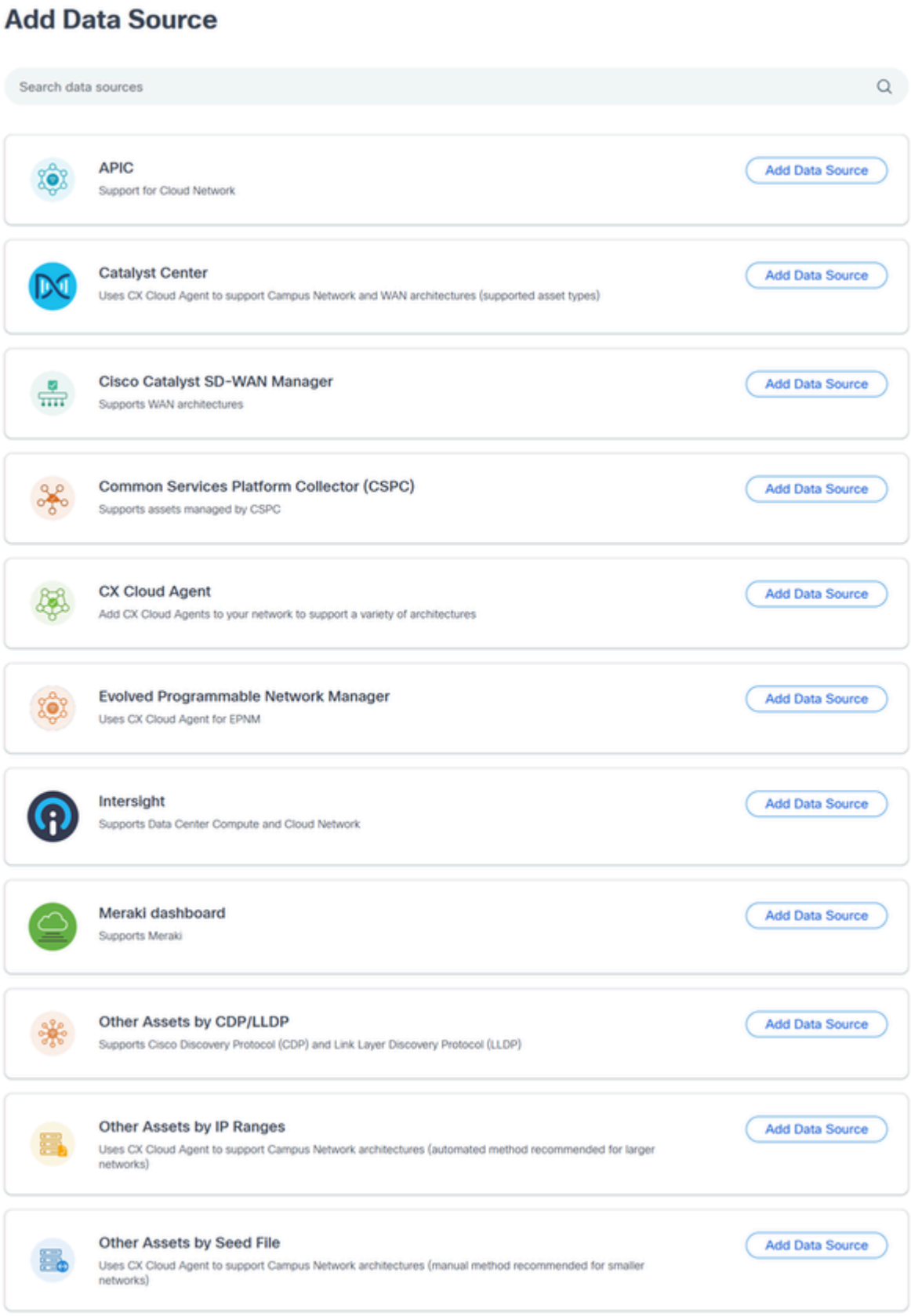
使用IP范围添加设备要求用户通过配置UI指定所有适用的凭证。显示的字段因在上一个窗口中选择的协议而异。如果为同一协议选择了多个选项（例如，同时选择SNMPv2c和SNMPv3或同时选择SSHv2和SSHv1），则CX代理将根据各个设备功能自动协商协议选择。

当使用IP地址连接设备时，客户应确保IP范围内所有相关协议以及SSH版本和Telnet凭证有效，否则连接将失败。

按IP范围添加其他资产

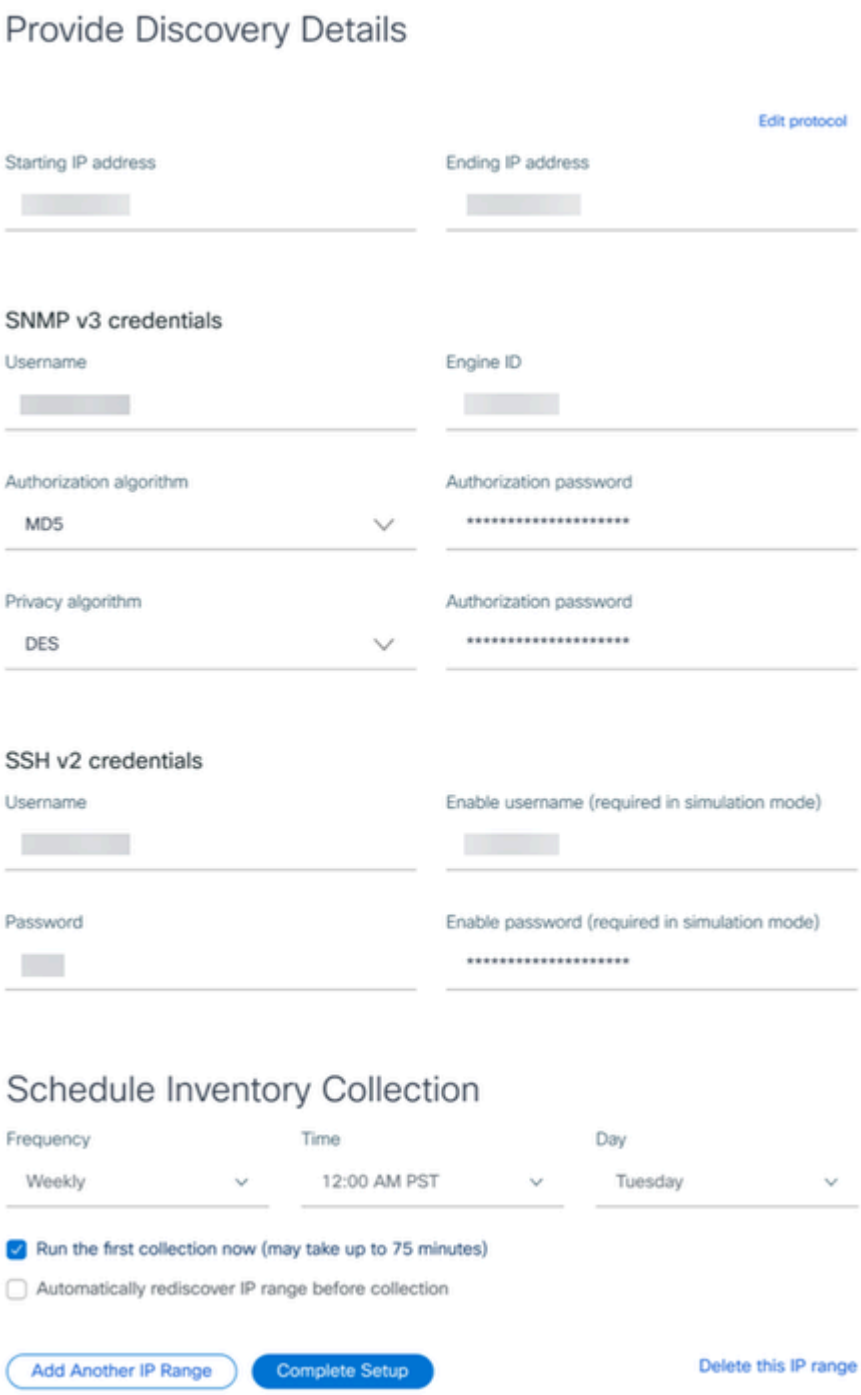
要使用IP范围添加设备，请执行以下操作：

1. 选择Admin Center图标。此时将打开Data Sources窗口。
2. 在Admin Center > Data Sources窗口中单击Add Data Source。



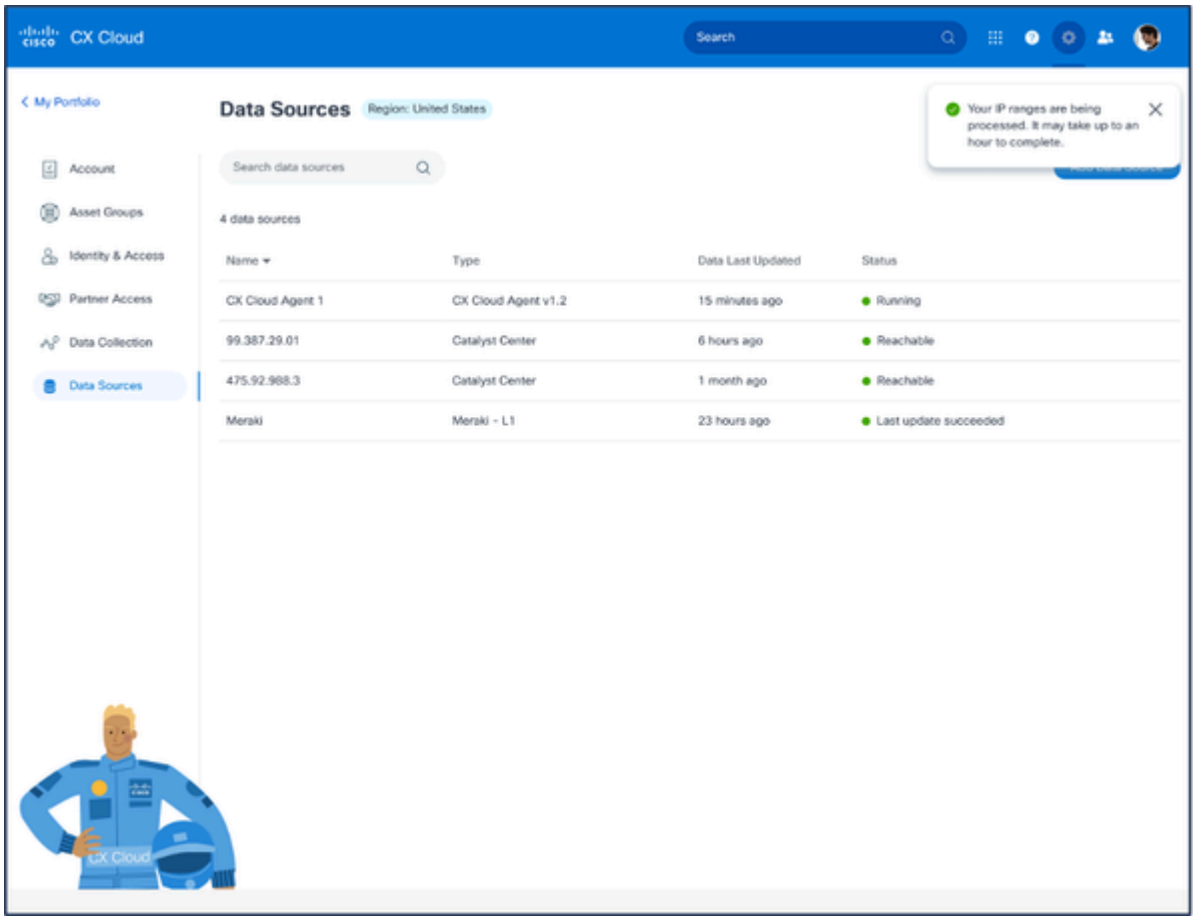
按IP范围划分的其他资产

3. 单击Other Assets by IP Range选项中的Add Data Source。将显示Provide Discovery Details页。



提供发现详细信息

4. 输入起始IP地址和结束IP地址。
5. 在SNMP和CLI凭证部分输入所需的详细信息。
6. 在Schedule Inventory Collection部分，从以下下拉列表中选择选项。
   - 频率
   - 时间
   - 日
7. 选中Run the first collection now复选框以运行收集。
8. 或者，选择Automatically rediscover IP range before collection复选框以启用IP范围的自动重新发现。
9. 单击完成设置。成功部署后会显示确认。

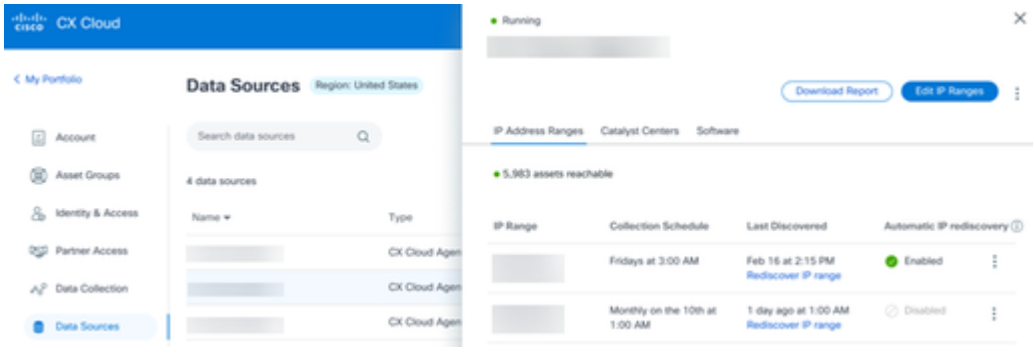


确认消息

编辑IP范围

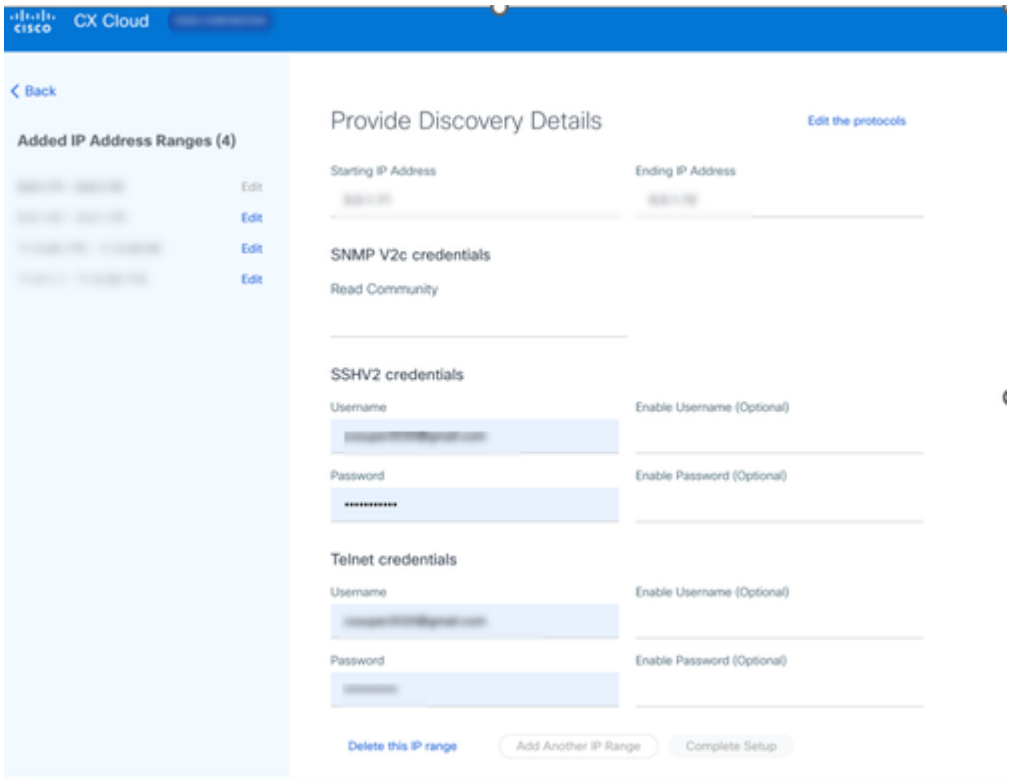
要编辑IP范围，请执行以下操作：

1. 定位至“数据源”窗口。
2. 单击Data Sources中需要IP范围编辑的CX代理。详细信息窗口打开。

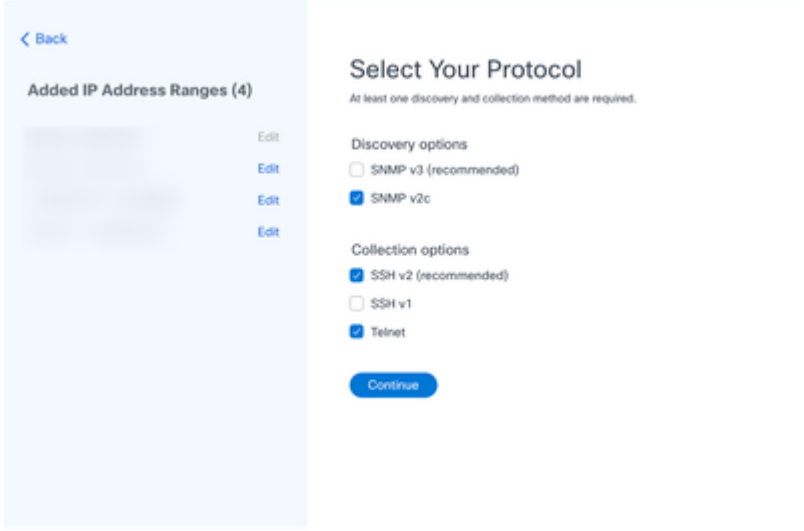


IP范围详细信息窗口

3. 单击Edit IP Address Range。

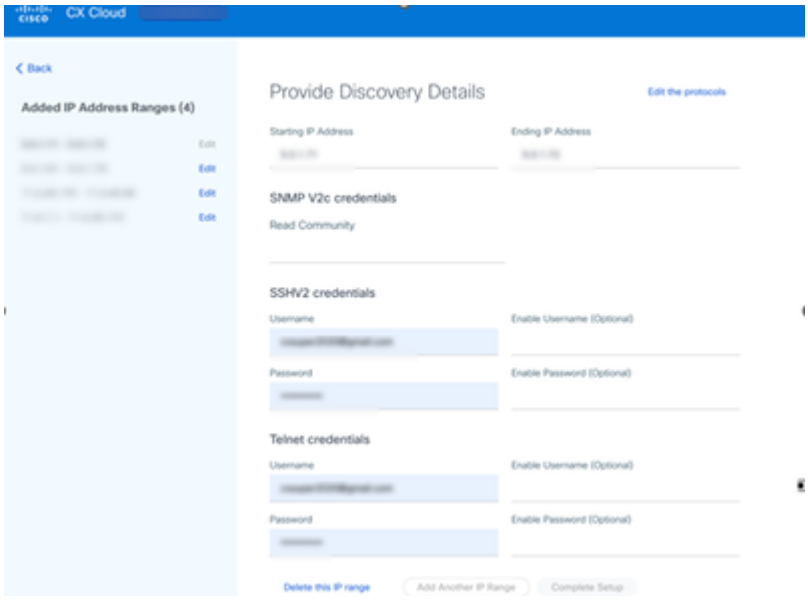


4. 单击Edit the protocols。Select Your Protocol窗口打开。



选择您的协议

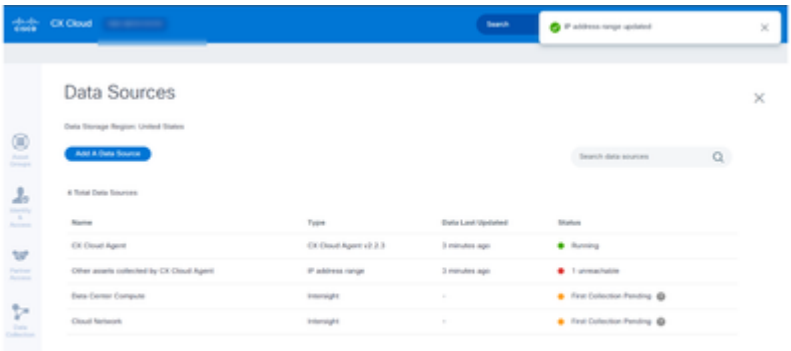
5. 选择适当的复选框以选择适用的协议，然后单击Continue以导航回Provide Discovery Details窗口。



提供发现详细信息

6.根据需要编辑详细信息，然后单击完成设置。Data Sources窗口打开，显示一条消息，确认新添加的IP地址范围已添加。

注意：此确认消息不会验证修改后的范围内的设备是否可访问，或者其凭证是否被接受。此确认发生在客户启动发现过程时。

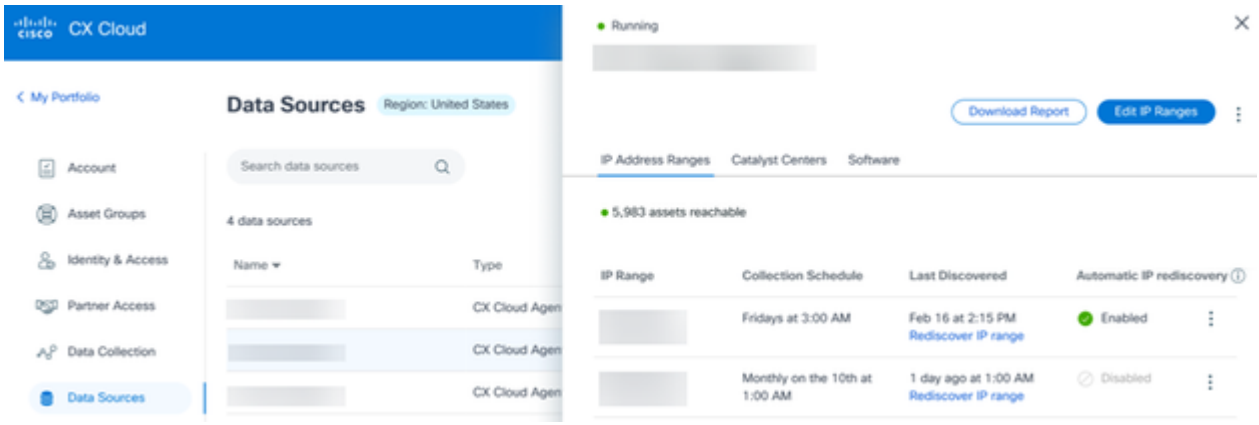


确认

删除IP范围

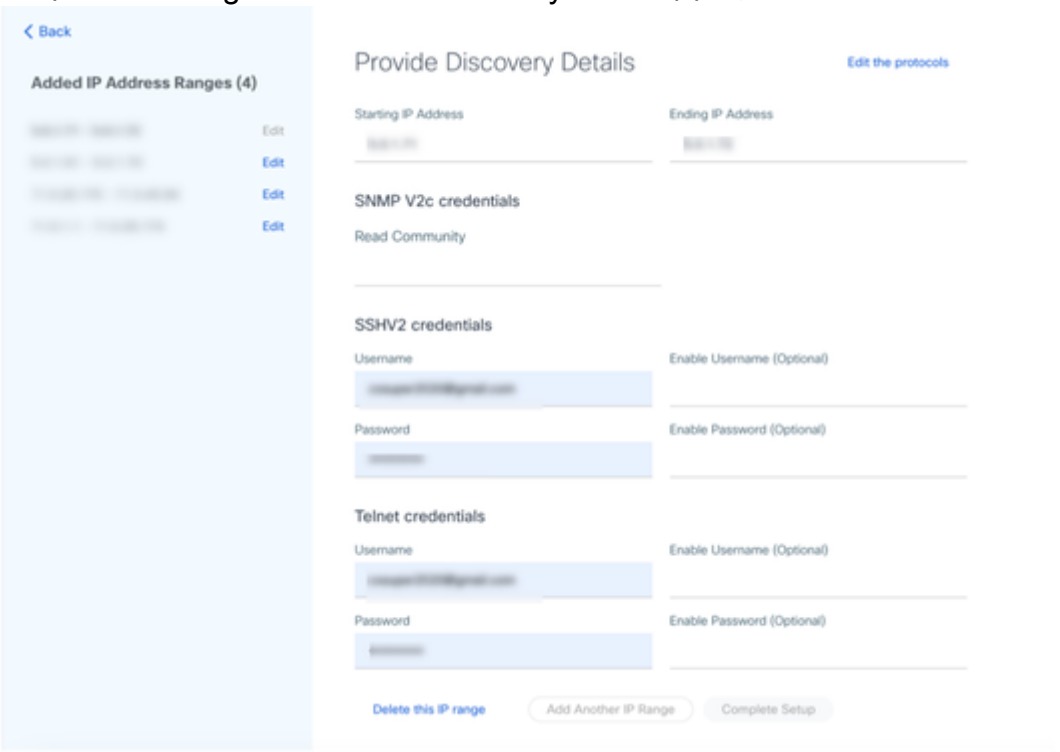
删除IP范围的步骤：

1. 定位至“数据源”窗口。
2. 选择具有需要删除的IP范围的相应CX代理。详细信息窗口打开。



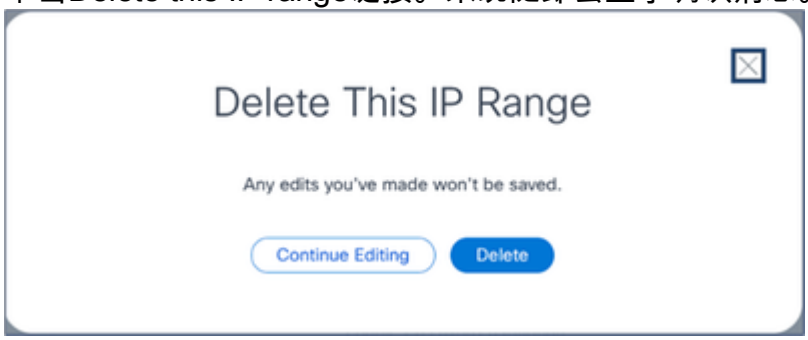
编辑IP范围

3. 单击Edit IP Ranges。Provide Discovery Details窗口打开。



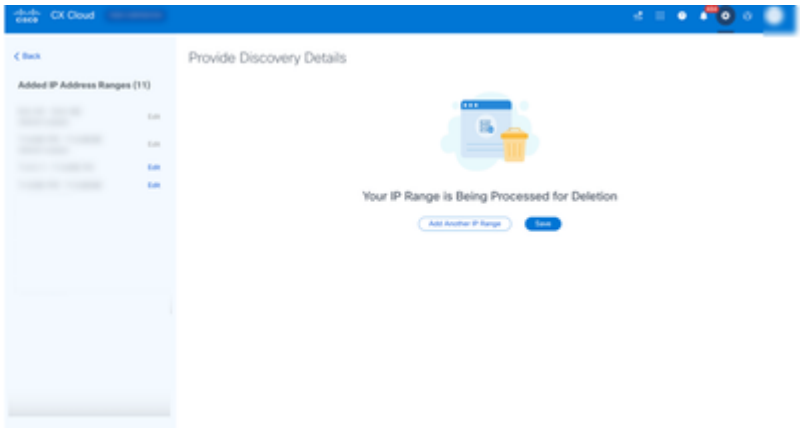
删除IP范围

4. 单击Delete this IP range链接。系统随即会显示确认消息。

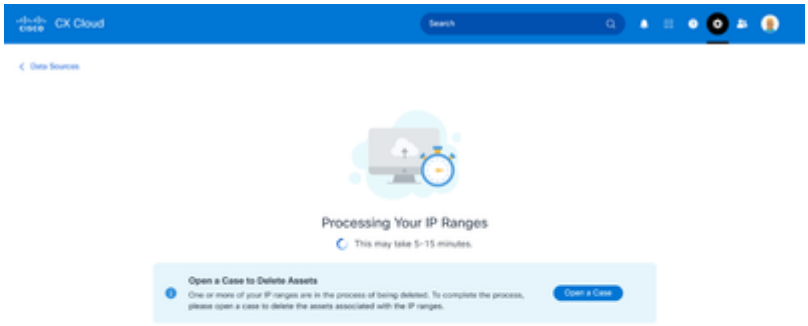


确认删除消息

5. 单击删除。



6. Click Save.系统随即会显示处理消息。



删除IP范围

完成后，数据源窗口将打开并显示确认消息。

关于从多个控制器中发现的设备

如果Catalyst Center和IP范围或种子文件位于同一个CX代理上，则可能由Cisco Catalyst Center发现某些设备，并且直接将设备连接到CX代理，从而导致从这些设备收集重复数据。为避免收集重复数据，且只有一个控制器管理设备，需要确定CX代理管理设备的优先级。

- 如果设备首先由Cisco Catalyst Center发现，然后由直接设备连接（使用种子文件或IP范围）重新发现，则Cisco Catalyst Center将优先控制设备。

注意：CDP（思科发现协议）和LLDP（链路层发现协议）不包括在重复数据消除过程中。

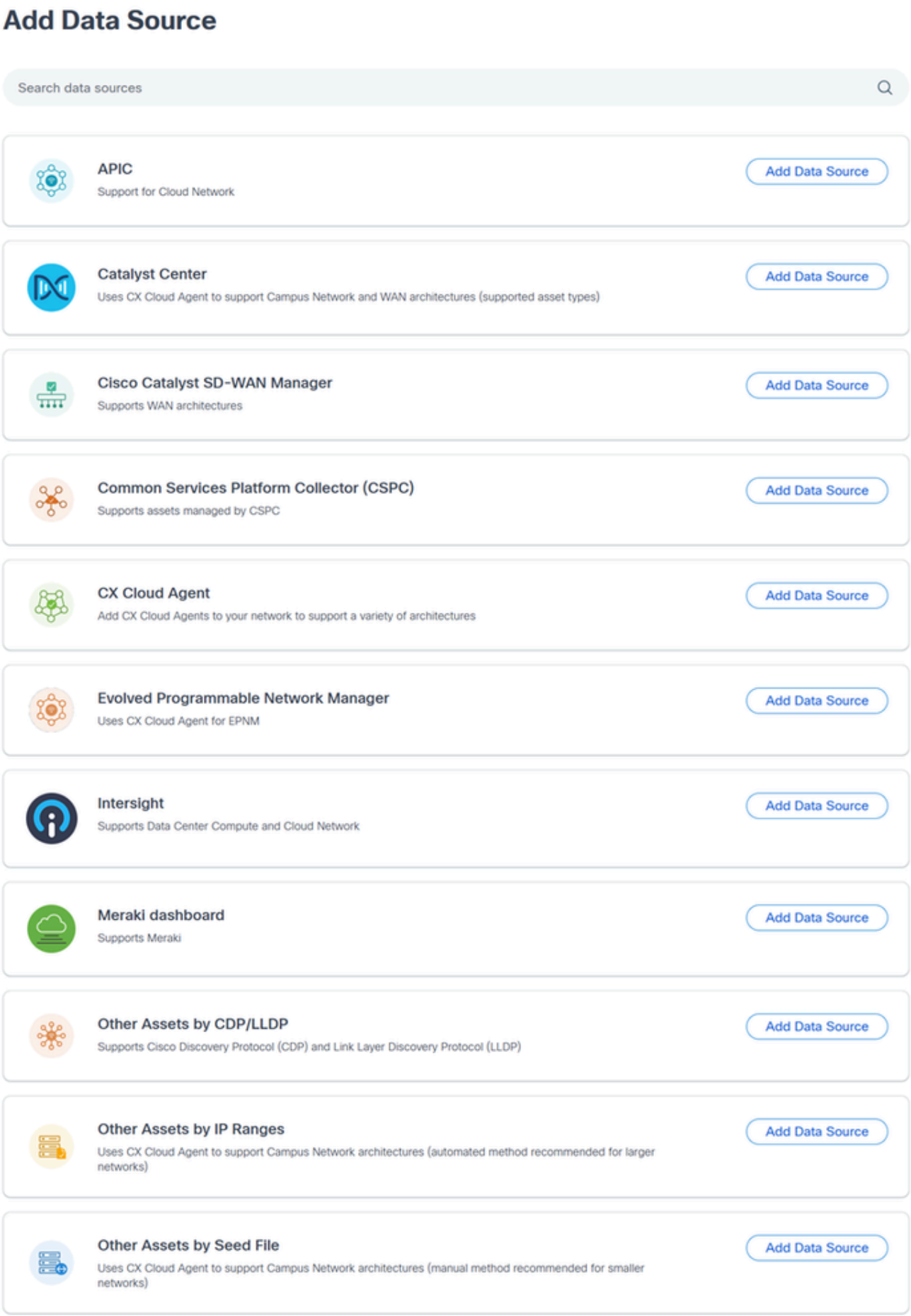
- 如果设备首先通过直接设备连接至CX代理发现，然后由Cisco Catalyst Center重新发现，则Cisco Catalyst Center优先控制设备。

使用CDP或LLDP添加其他资产

CDP和LLDP是使设备能够自动发现网络中直连设备信息的网络协议。当通过CDP或LLDP启用发现时，CX代理与网络设备通信，以收集有关相邻设备的详细信息，例如设备类型、IP地址和连接详细信息，而无需手动输入或预配置。此自动化过程允许CX代理在网络上检测到新设备时，动态地识别这些设备并将其添加到资产中，从而确保设备列表保持最新状态，即使网络不断发展也是如此。与通过CDP或LLDP发现设备相关的任何错误或消息都将捕获为CX云中作业日志详细信息的一部分。使用CDP或LLDP发现设备可简化网络管理，减少手动操作，并有助于维护所有已连接设备的准确最新库存。

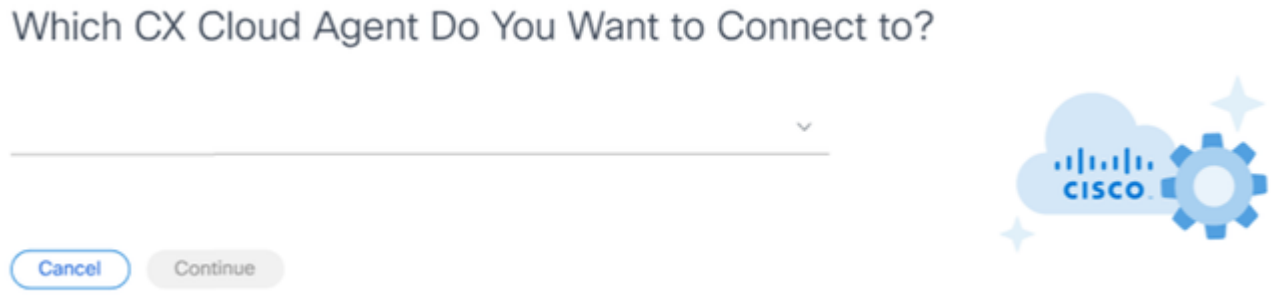
使用CDP或LLDP添加其他资产的步骤：

1. 选择Admin Center图标。Data Sources窗口打开。
2. 单击添加数据源。系统随即会显示添加数据源页。



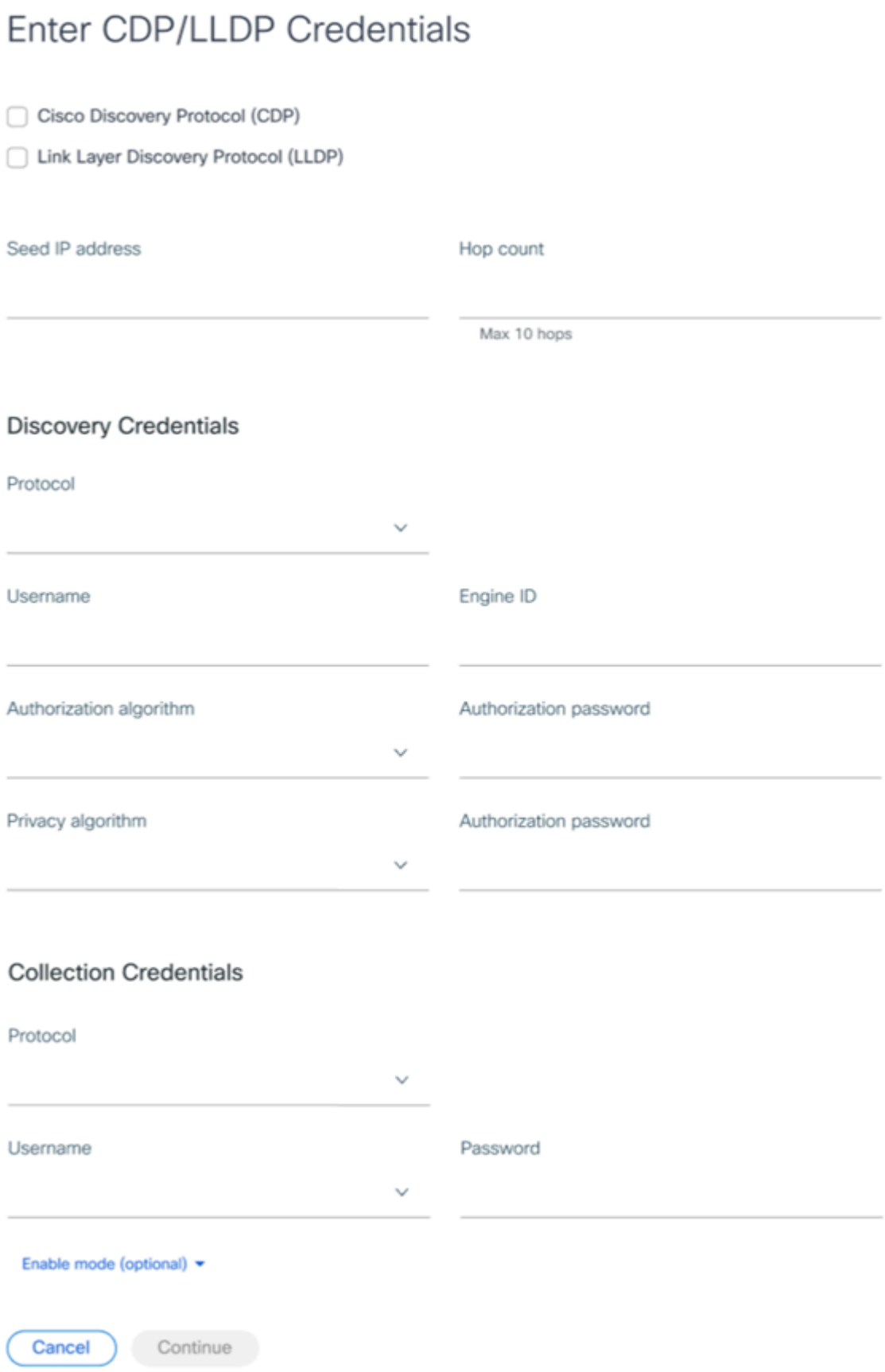
CDP/LLDP的其他资产

3. 单击Other Assets by CDP/LLDP选项中的Add Data Source。您要连接到哪个CX云代理？页面。



您要连接到哪个CX代理？

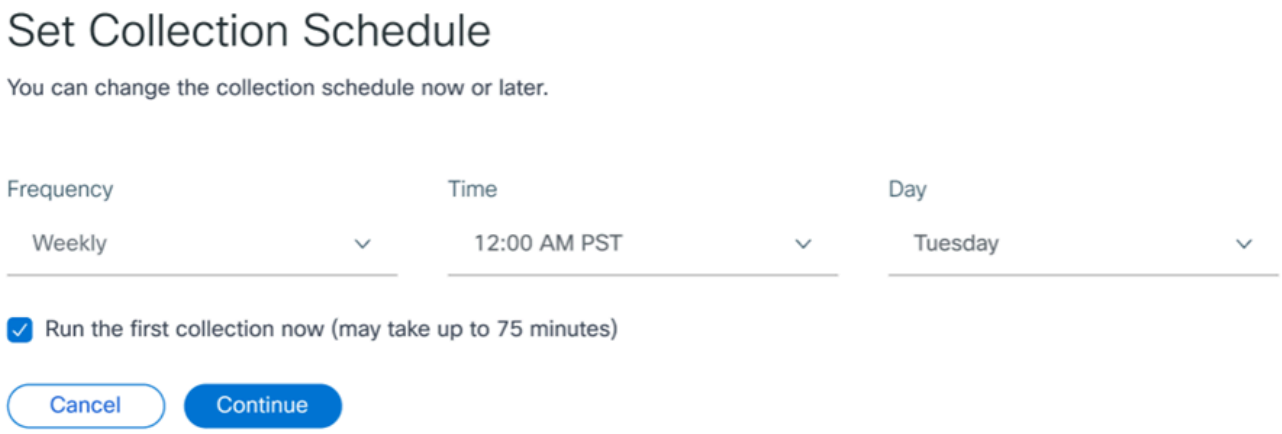
4. 从下拉列表中选择一个选项。
5. 单击 Continue。系统随即会显示输入CDP/LLDP凭证页面。



输入CDP/LLDP凭证

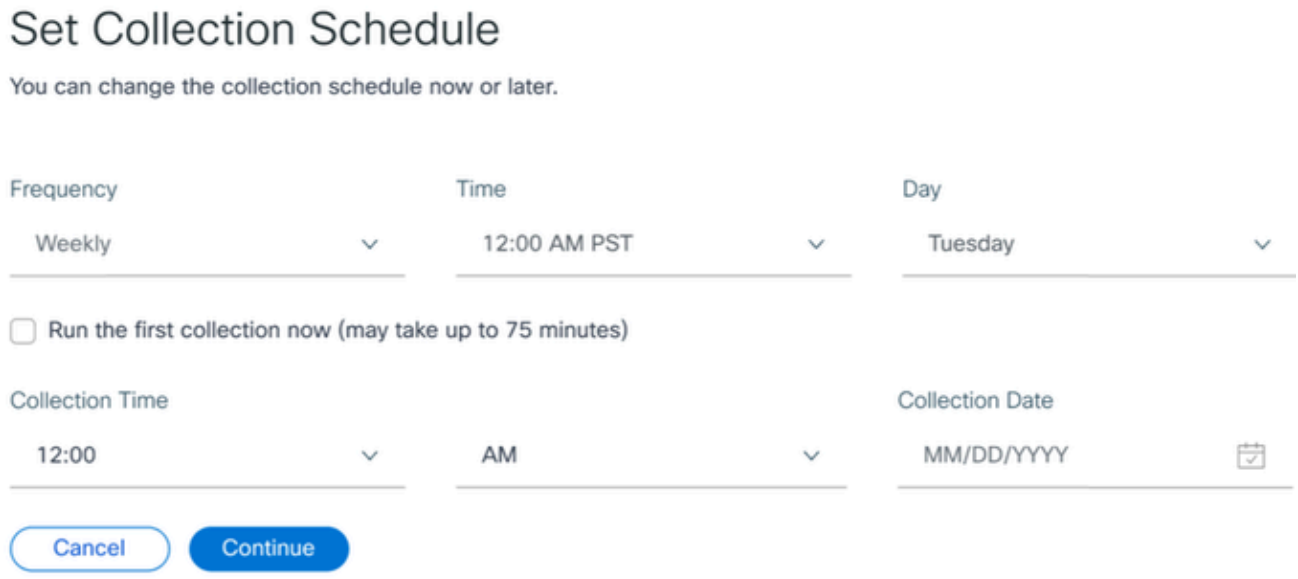
6. 选中Cisco Discovery Protocol(CDP)或Link Layer Discovery Protocol(LLDP)复选框。
7. 输入种子IP地址和跳数（换句话说，发现过程应经过的跳数）。
8. 在Discovery Credentials 部分，从Protocol下拉列表中选择SNMP v3 或SNMP v2 。

9. 输入SNMP凭证。
10. 在Collection Credentials部分，从Protocol下拉列表中选择SSH v2（推荐）。
11. 输入用户名和密码。
12. 单击 Continue。系统随即会显示Set Collection Schedule页面。



设置收集计划

13. 从以下下拉列表中选择选项：
    - 频率
    - 时间
    - 日
14. 选中Run the first collection now复选框。
15. 单击 Continue。



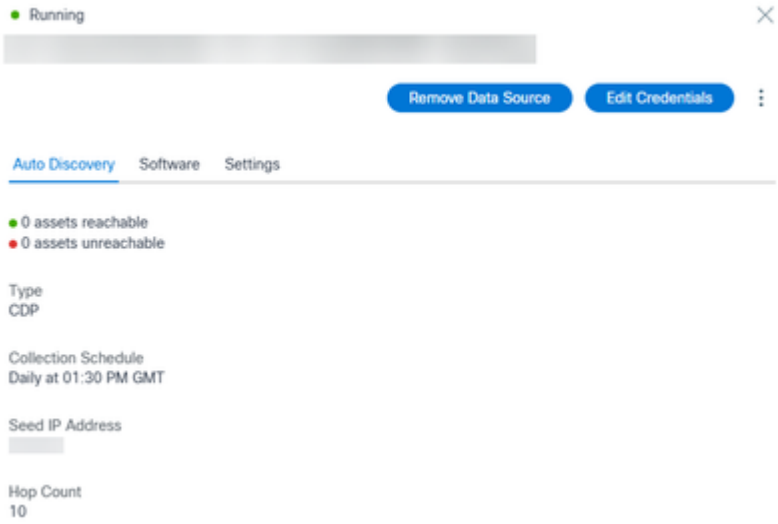
设置收集计划（续）

16. 从以下下拉列表中选择选项：
    - 收集时间
    - 上午/下午
    - 收集日期
17. 单击 Continue。添加数据源后，系统将显示一条确认消息。

编辑CDP或LLDP详细信息

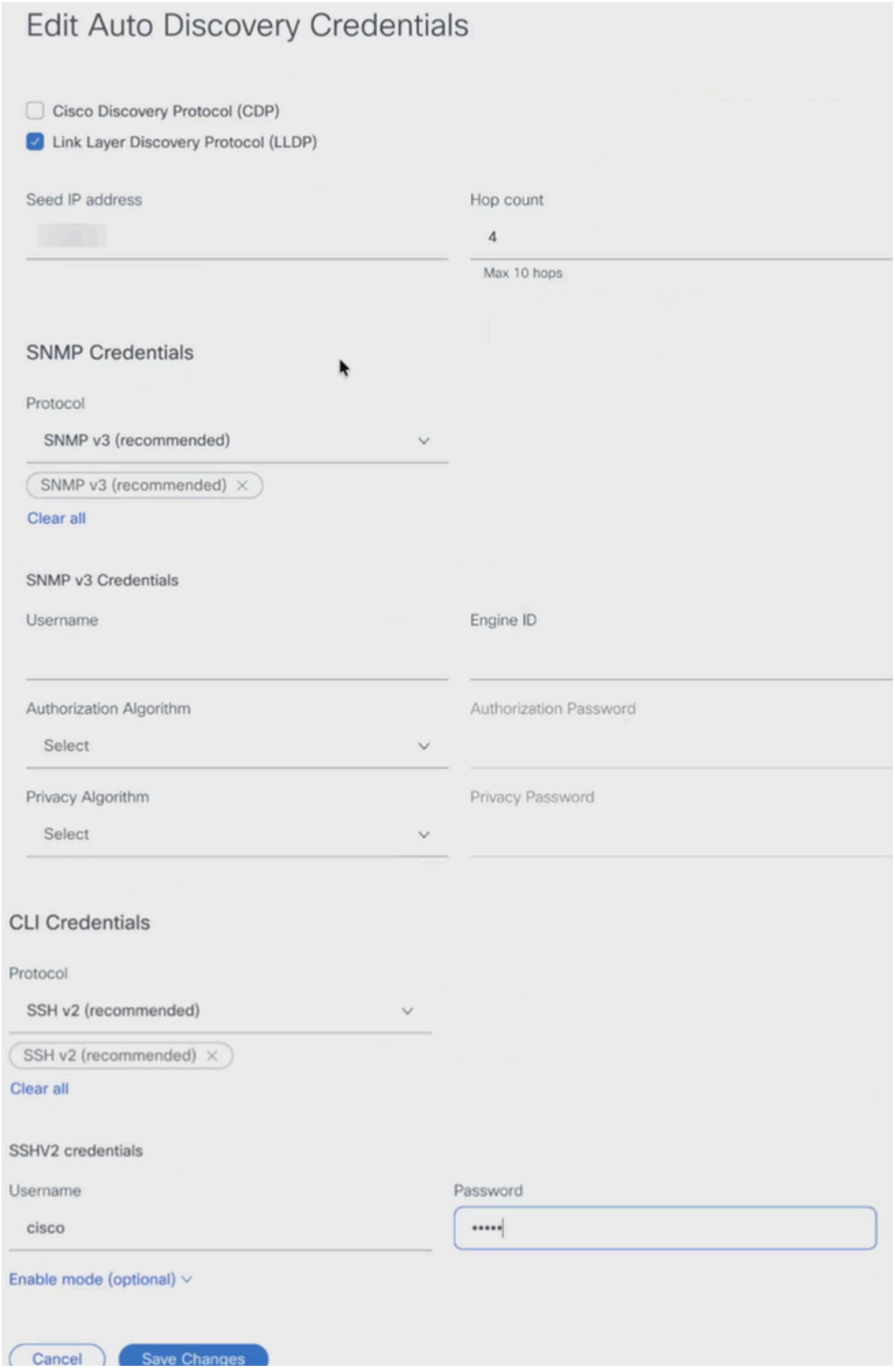
要编辑CDP或LLDP详细信息，请执行以下操作：

1. 定位至“数据源”窗口。
2. 单击需要CX代理详细信息窗口的CX代理。



CX代理详细信息窗口

3. 点击编辑凭证。系统将显示Edit Auto Discovery Credentials页。



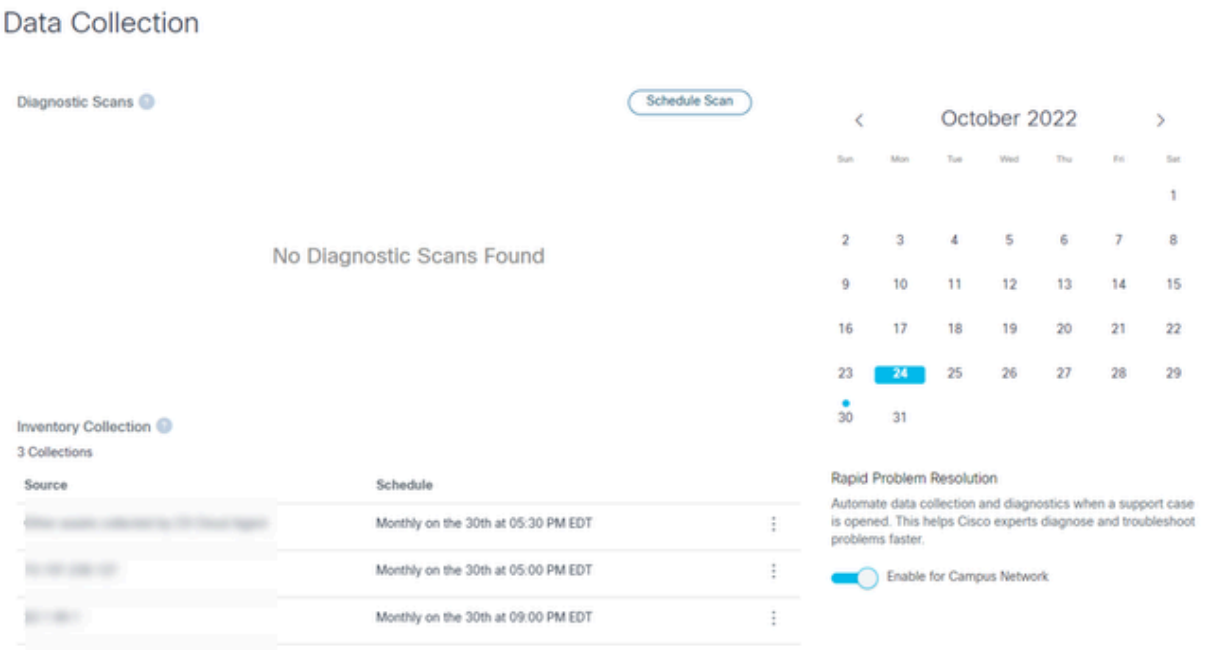
编辑自动发现凭据

4. 进行所需的编辑

思科建议安排诊断扫描或启动按需扫描，这些扫描应至少与资产收集计划相隔6-7小时，这样它们就不会重叠。同时执行多个诊断扫描可能会减慢扫描过程并可能导致扫描失败。

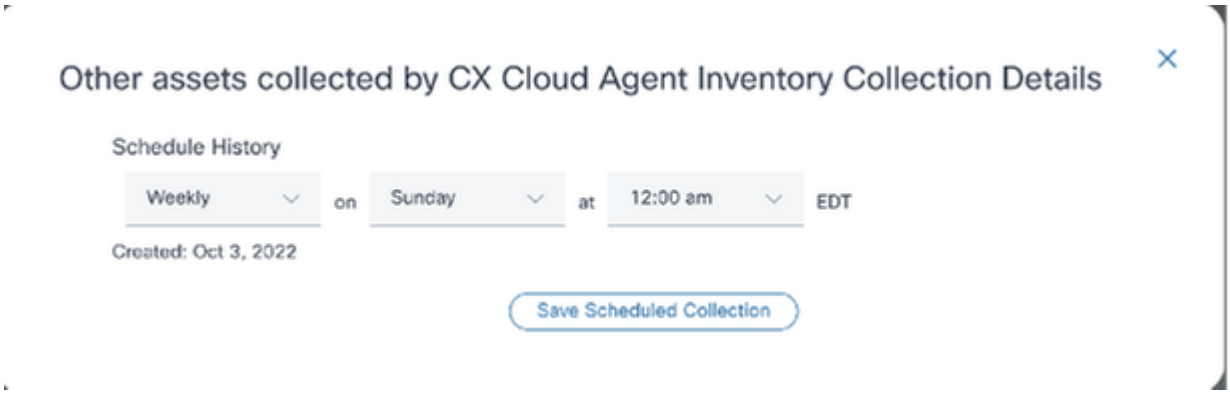
要计划诊断扫描，请执行以下操作：

1. 在主页上，点击设置（齿轮）图标。
2. 在“数据源”页上，在左侧窗格中选择数据收集。
3. 单击Schedule Scan。



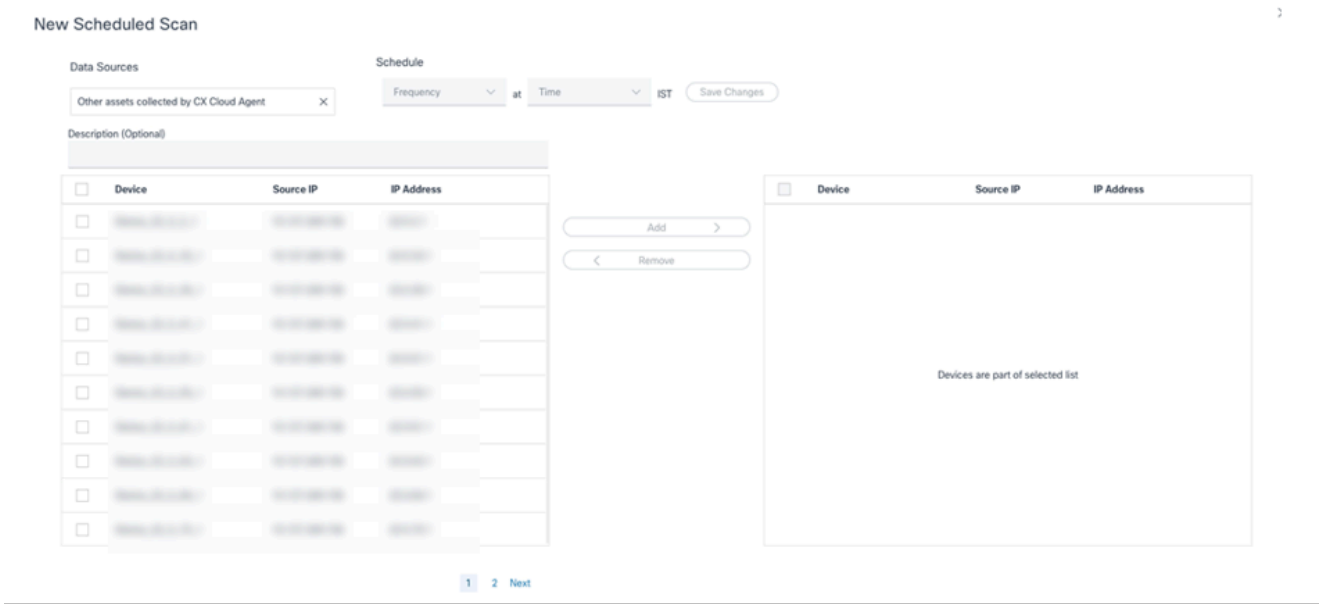
安排扫描

4. 为此扫描配置计划。



配置扫描计划

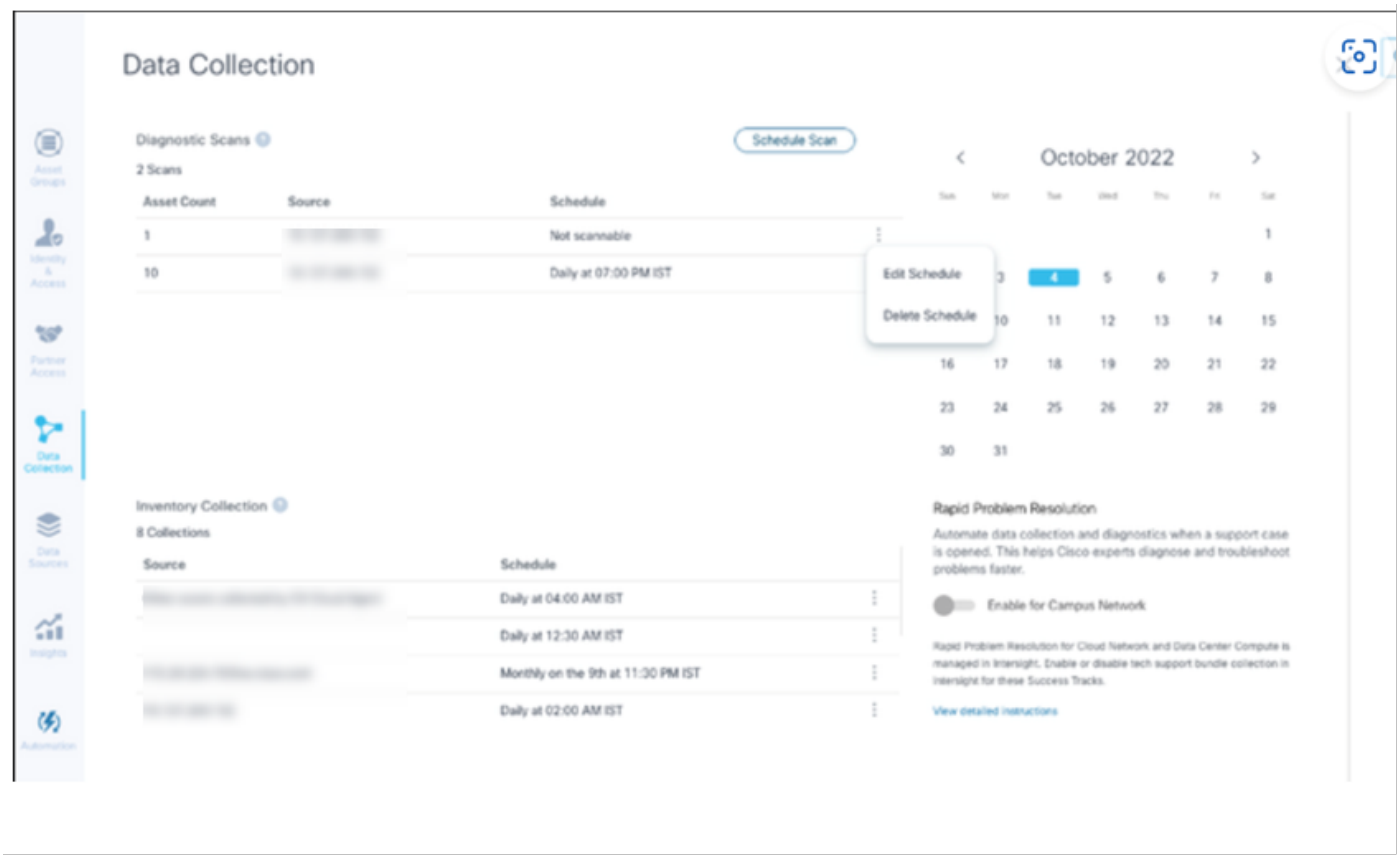
5. 在设备列表中，选择要扫描的所有设备，然后单击Add。



安排扫描

6. 调度完成后，单击Save Changes。

诊断扫描和资产收集计划可从“数据收集”页面编辑和删除。



具有编辑和删除计划选项的数据收集

将CX Agent VM升级到大中型配置

升级VM后，无法执行以下操作：

- 从大配置或中型配置缩减到小型配置
- 从大型配置缩减到中型配置
- 从中型升级到大型配置

在升级VM之前，Cisco建议拍摄快照，以便在发生故障时进行恢复。有关详细信息，请参阅备份和恢复CX云虚拟机。

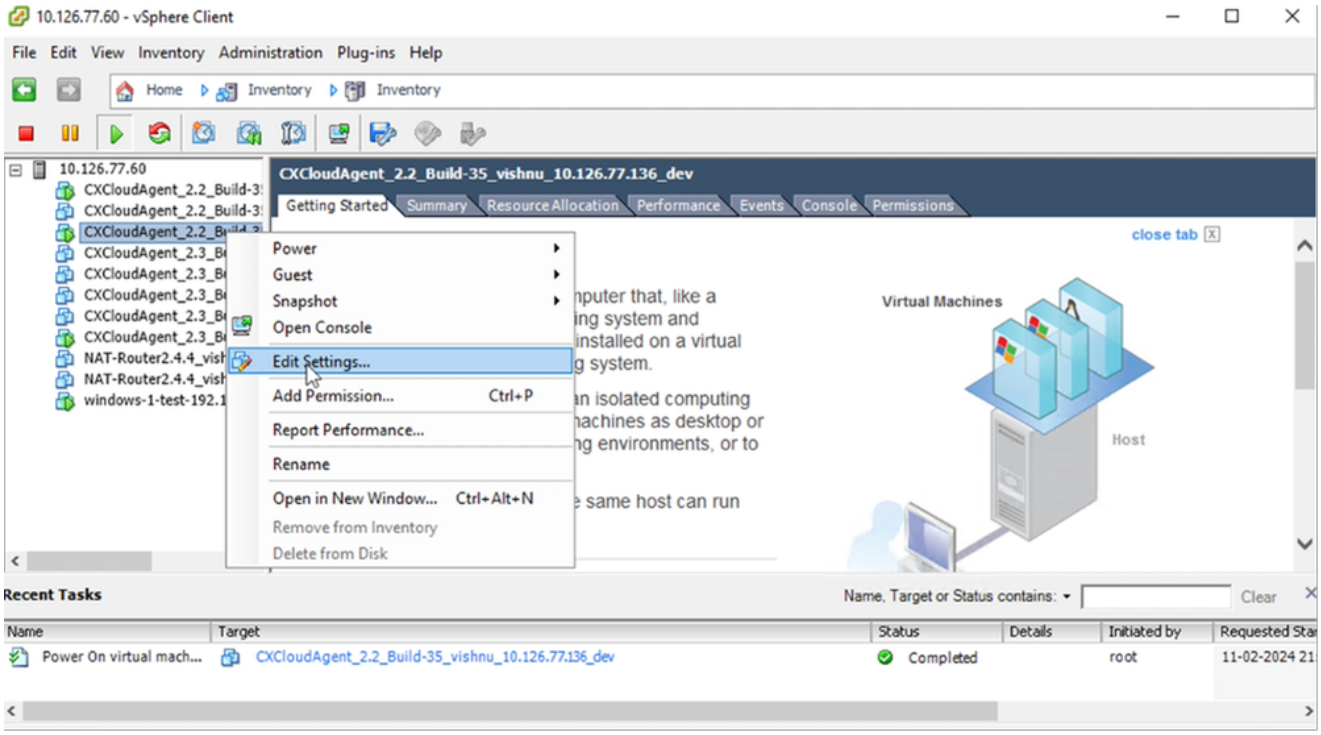
使用VMware vSphere胖客户端重新配置

要使用现有VMware vSphere胖客户端升级VM配置，请执行以下操作：



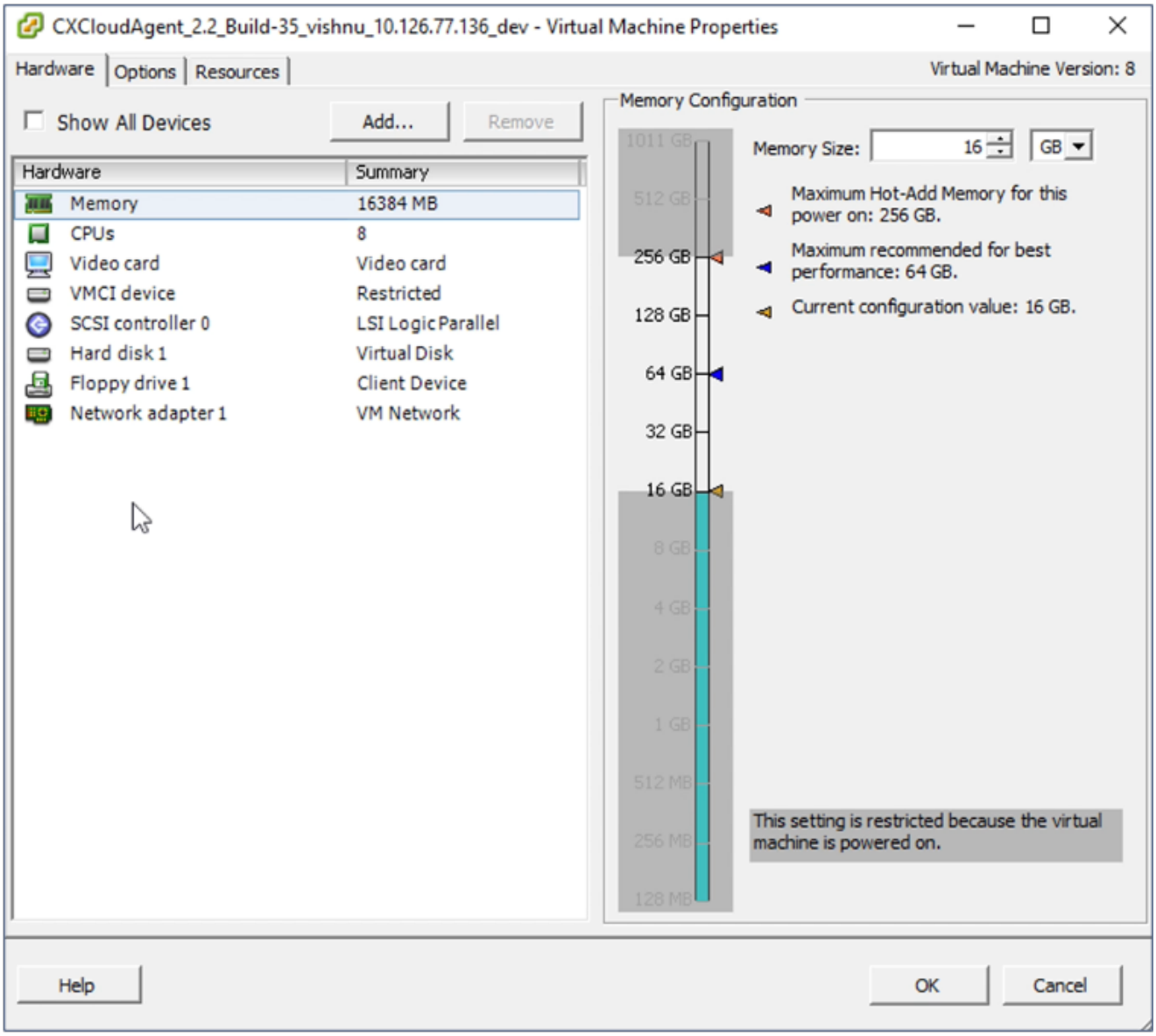
vSphere 客户端

1. 登录到VMware vSphere客户端。Home页面显示VM列表。



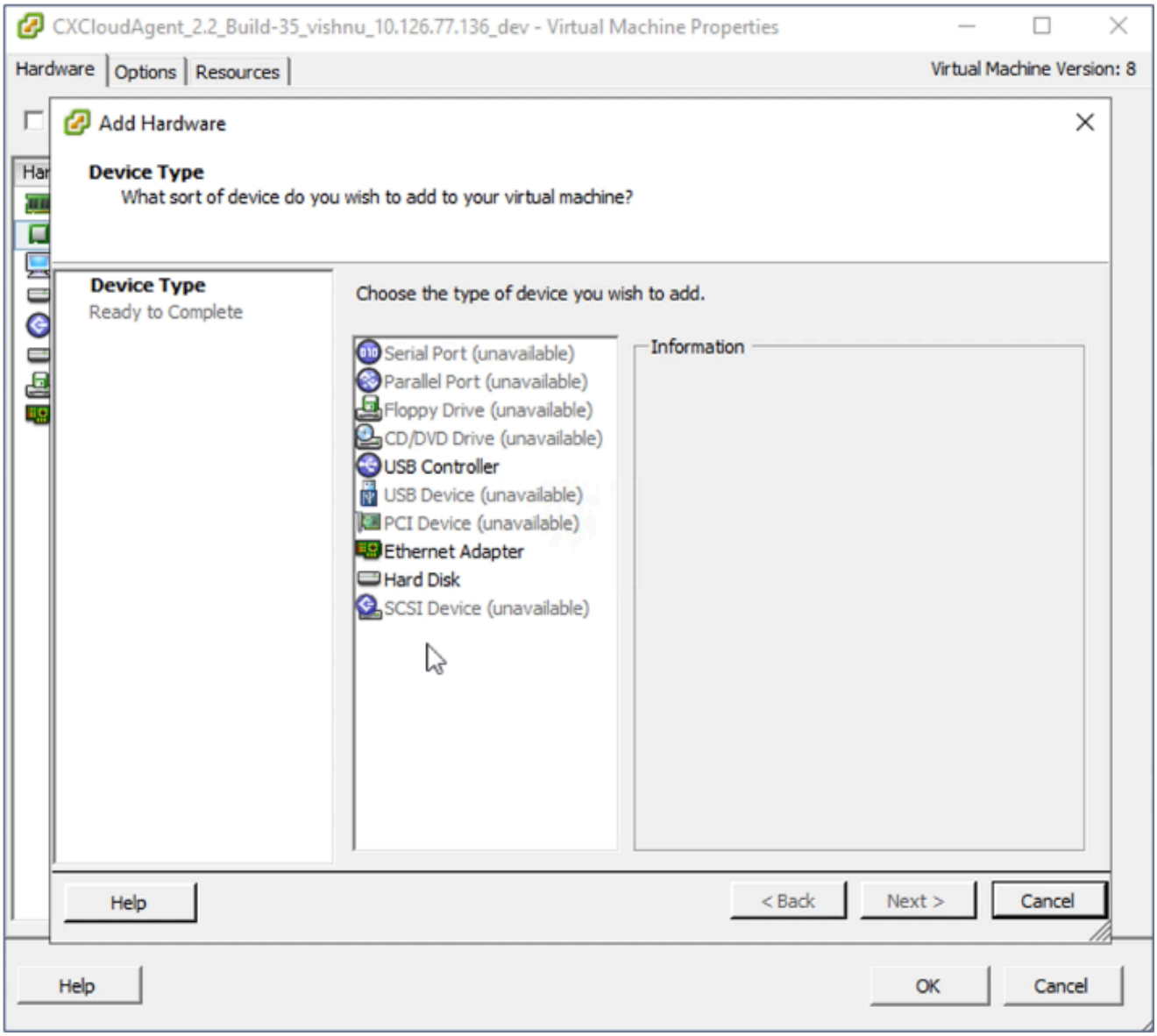
编辑设置

2. 右键单击目标VM，然后从菜单中选择Edit Settings。VM Properties窗口打开。



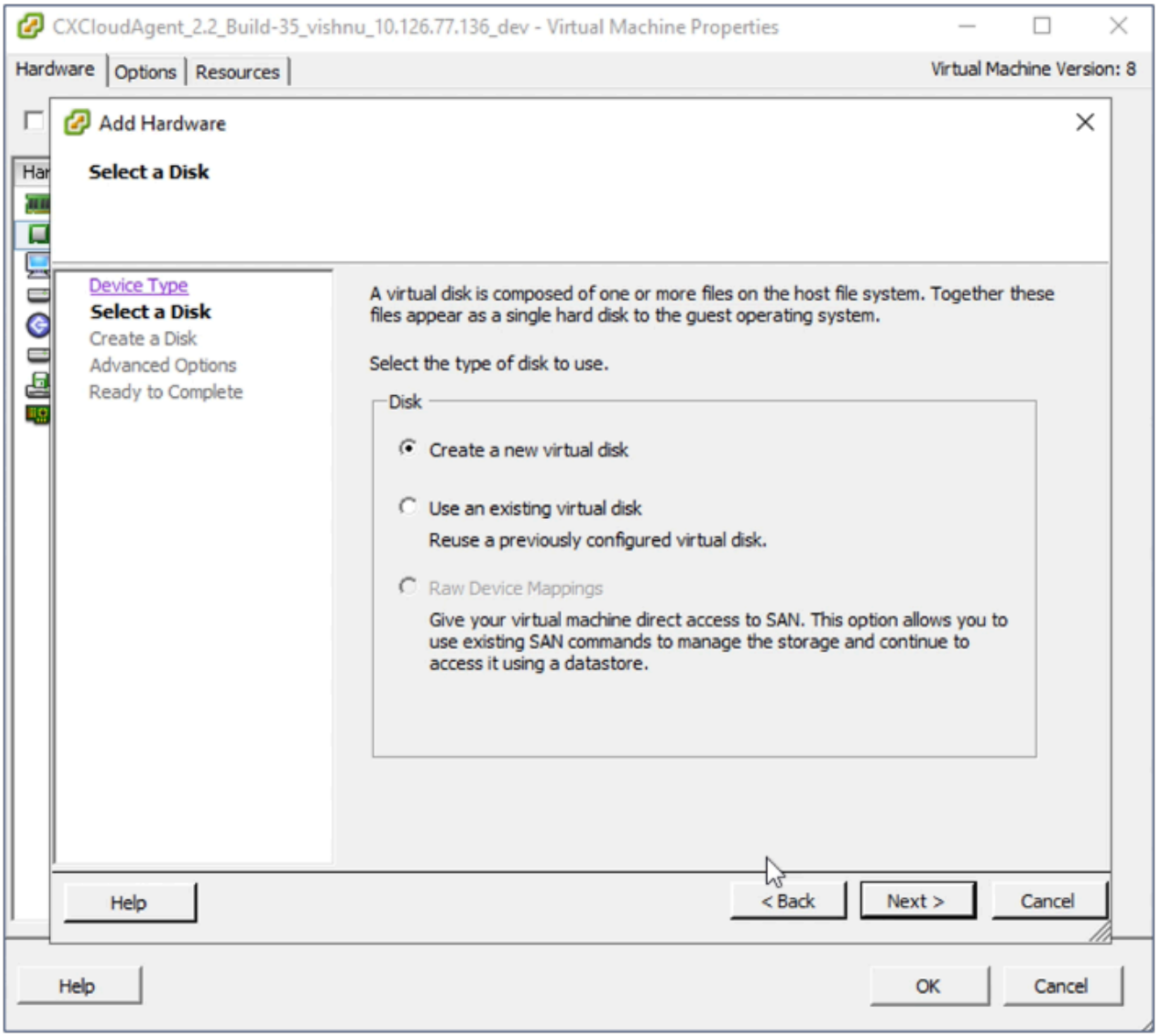
VM属性

3. 按照指定更新Memory Size值：
   中：32 GB(32768 MB)
   大容量：64 GB(65536 MB)
4. 选择CPU并更新指定的值：
   中型：16个内核（8个插槽*2个内核/插槽）
   大型：32个内核（16个插槽*2个内核/插槽）
5. 单击 Add。Add Hardware窗口打开。



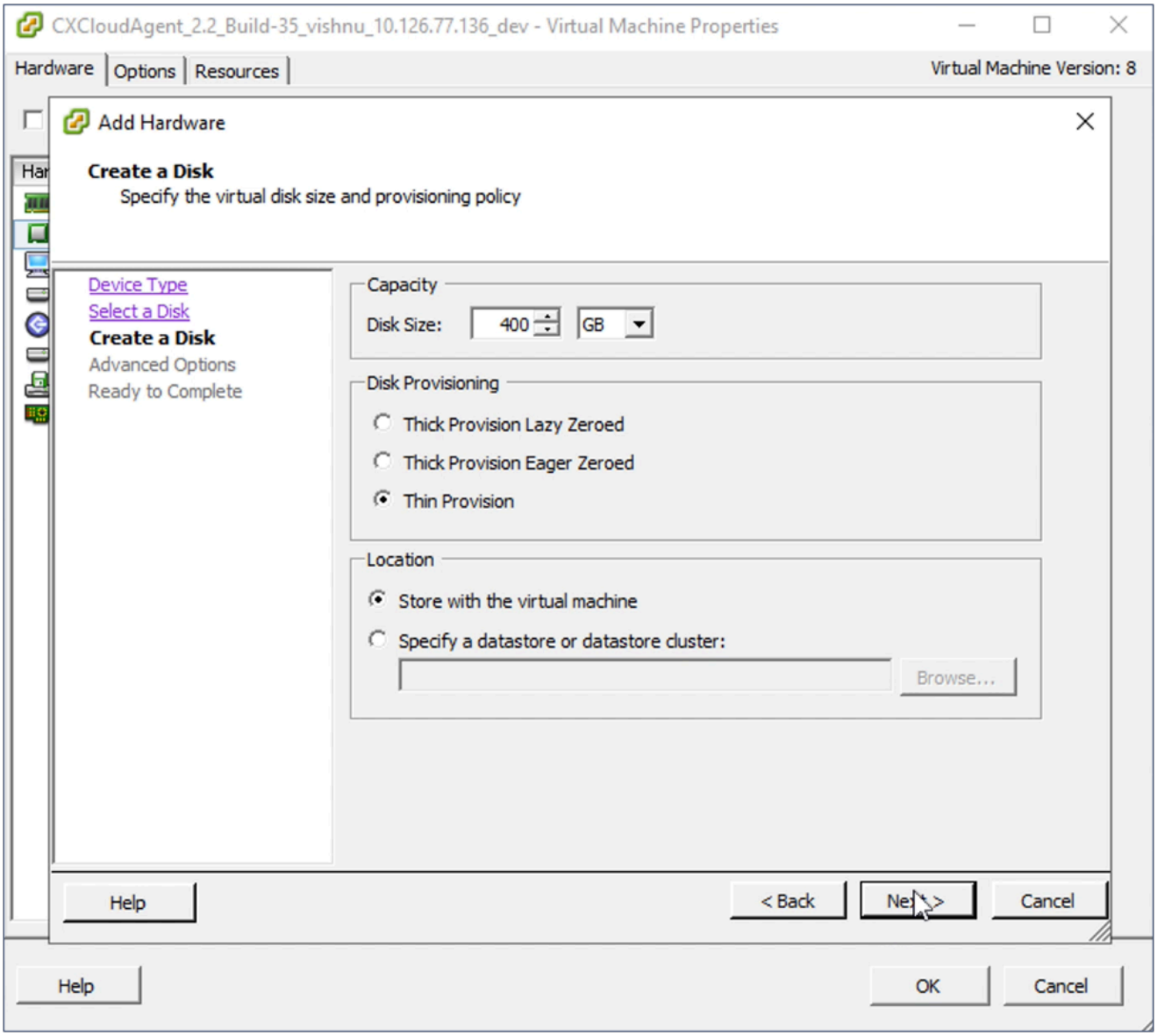
设备类型

6. 选择硬盘作为设备类型。
7. 单击 Next。



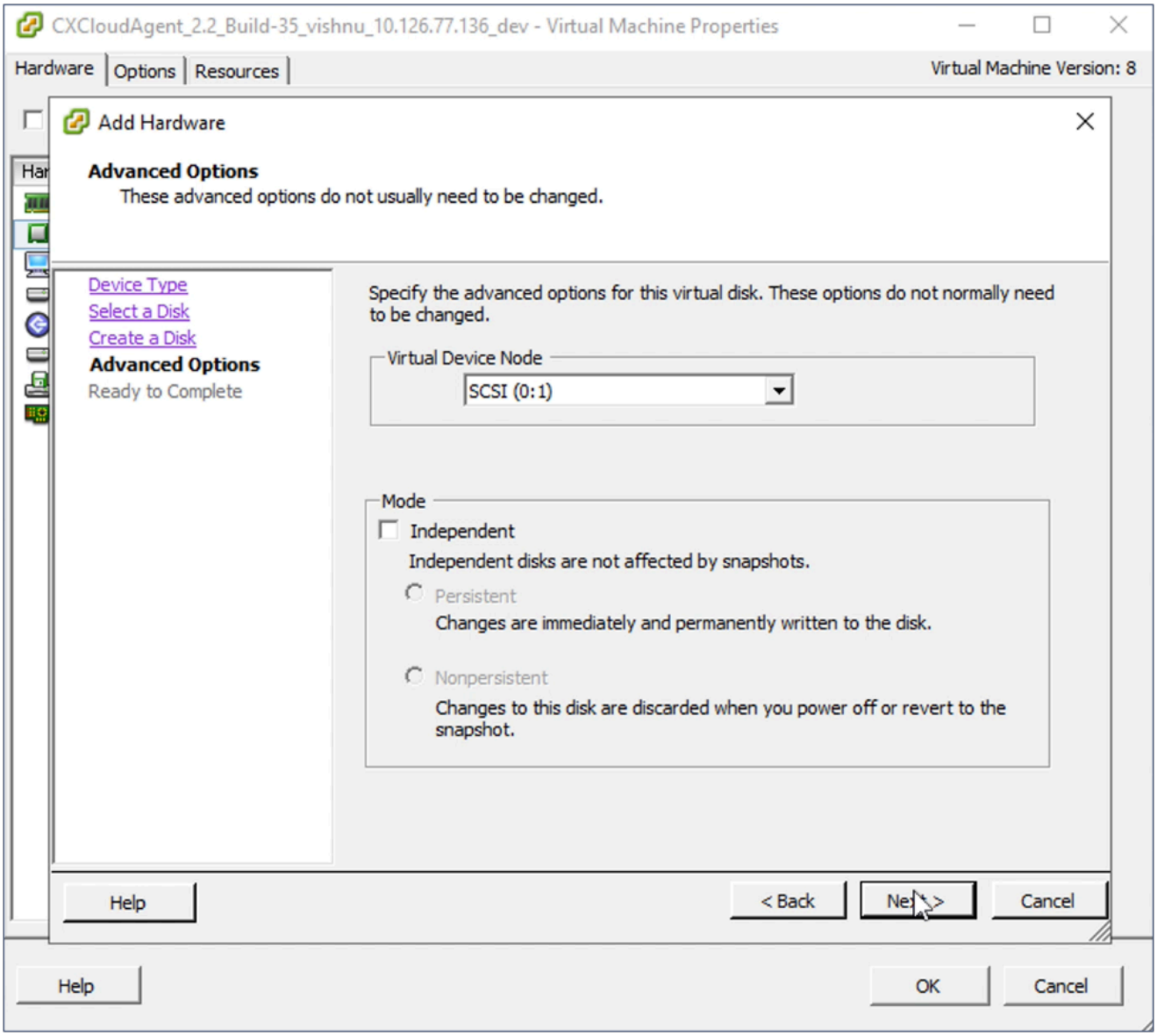
选择磁盘

8. 选择Create a new virtual disk单选按钮，然后单击Next。



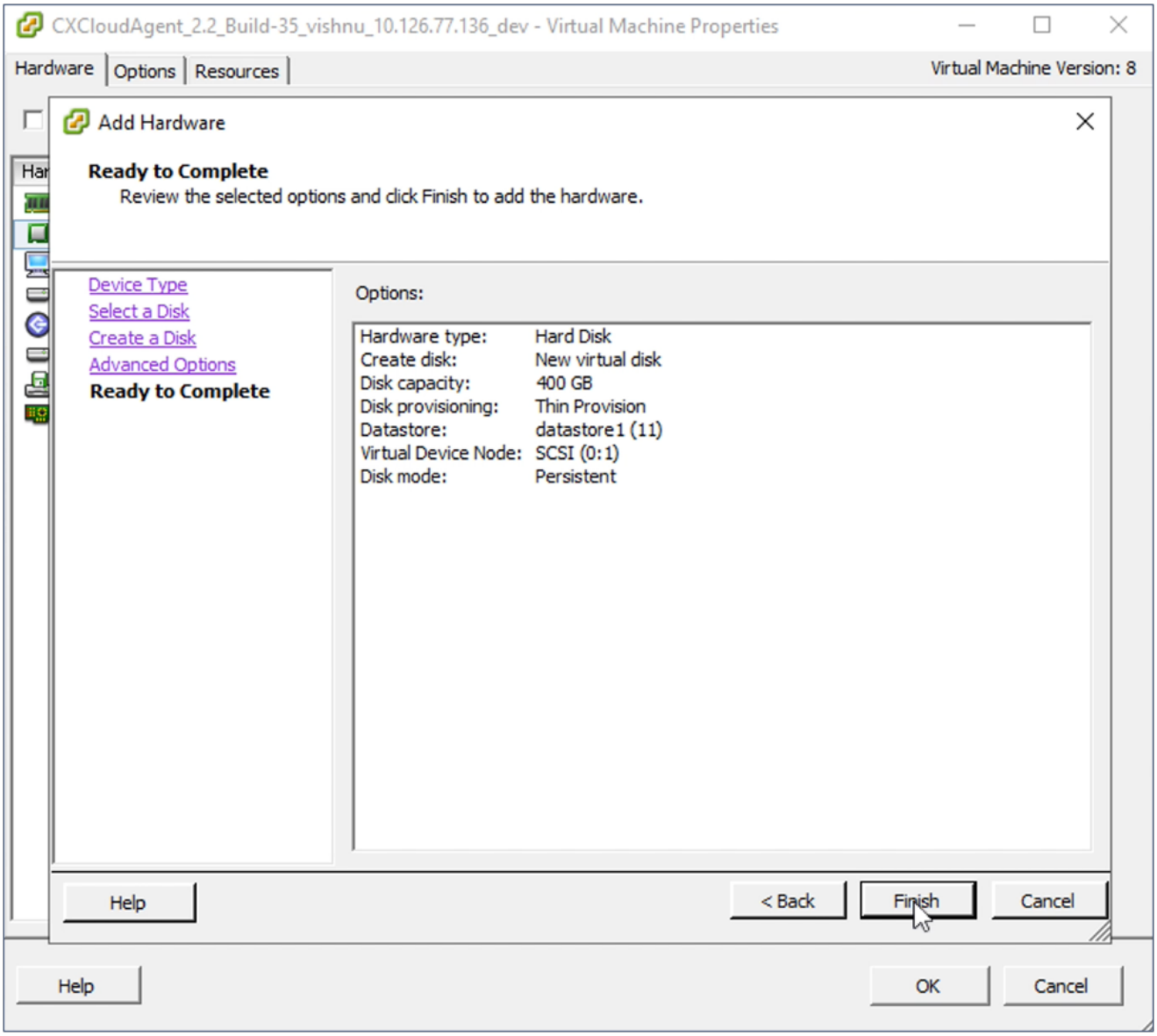
创建磁盘

9. 按指定方式更新Capacity > Disk Size:
   中小型：400 GB（初始大小为200 GB，将总空间增加到600 GB）
   小到大：1000 GB（初始大小为200 GB，将总空间增加到1200 GB）
10. 选择Disk Provisioning的Thin Provision单选按钮。
11. 单击 Next。系统随即会显示高级选项窗口。



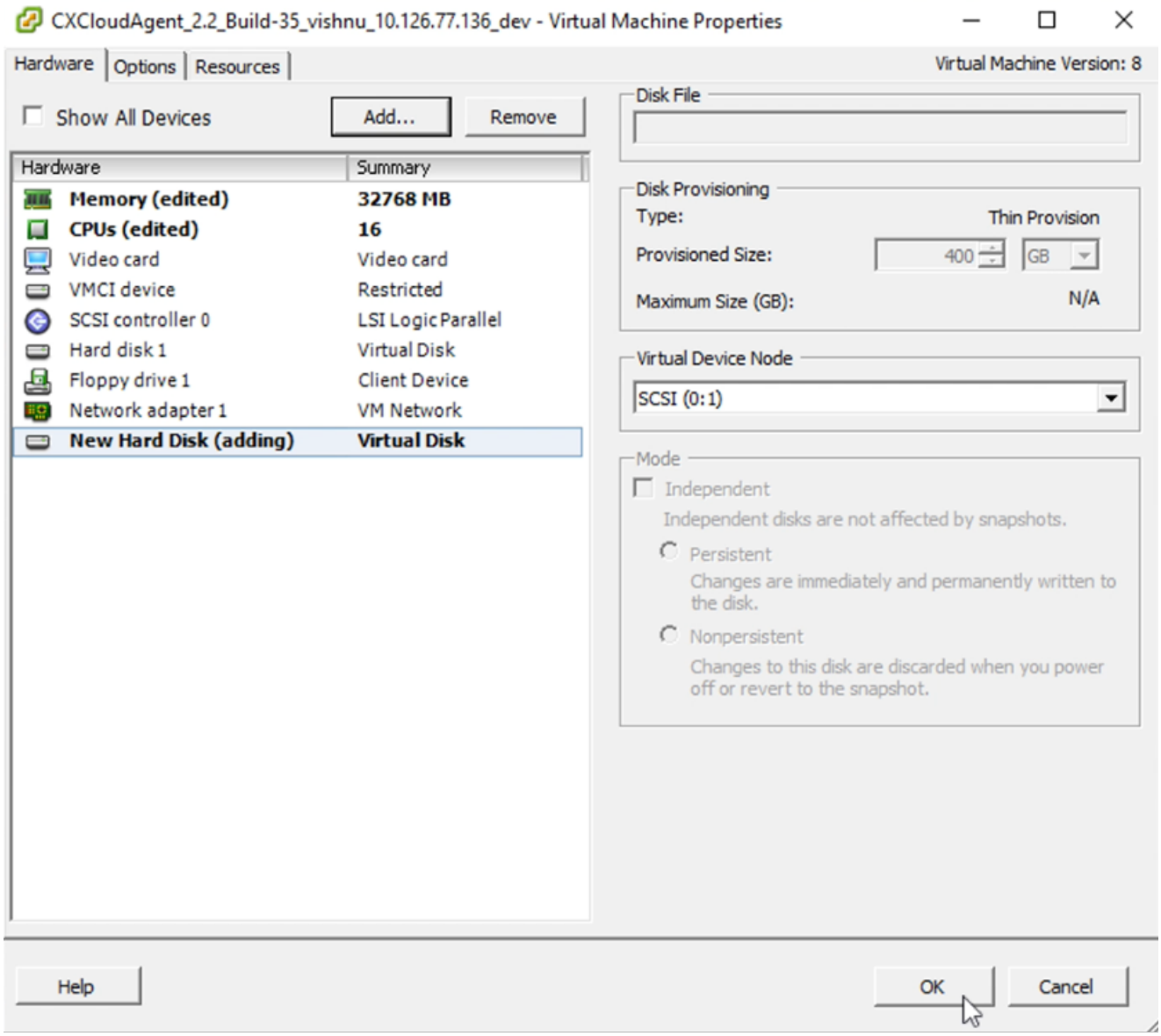
高级选项

12. 请勿进行更改。点击下一步继续。


CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 8
Add Hardware
Ready to Complete
Review the selected options and click Finish to add the hardware.
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Options:
Hardware type: Hard Disk
Create disk: New virtual disk
Disk capacity: 400 GB
Disk provisioning: Thin Provision
Datastore: datastore1 (11)
Virtual Device Node: SCSI (0:1)
Disk mode: Persistent
Help
< Back
Finish
Cancel
Help
OK
Cancel

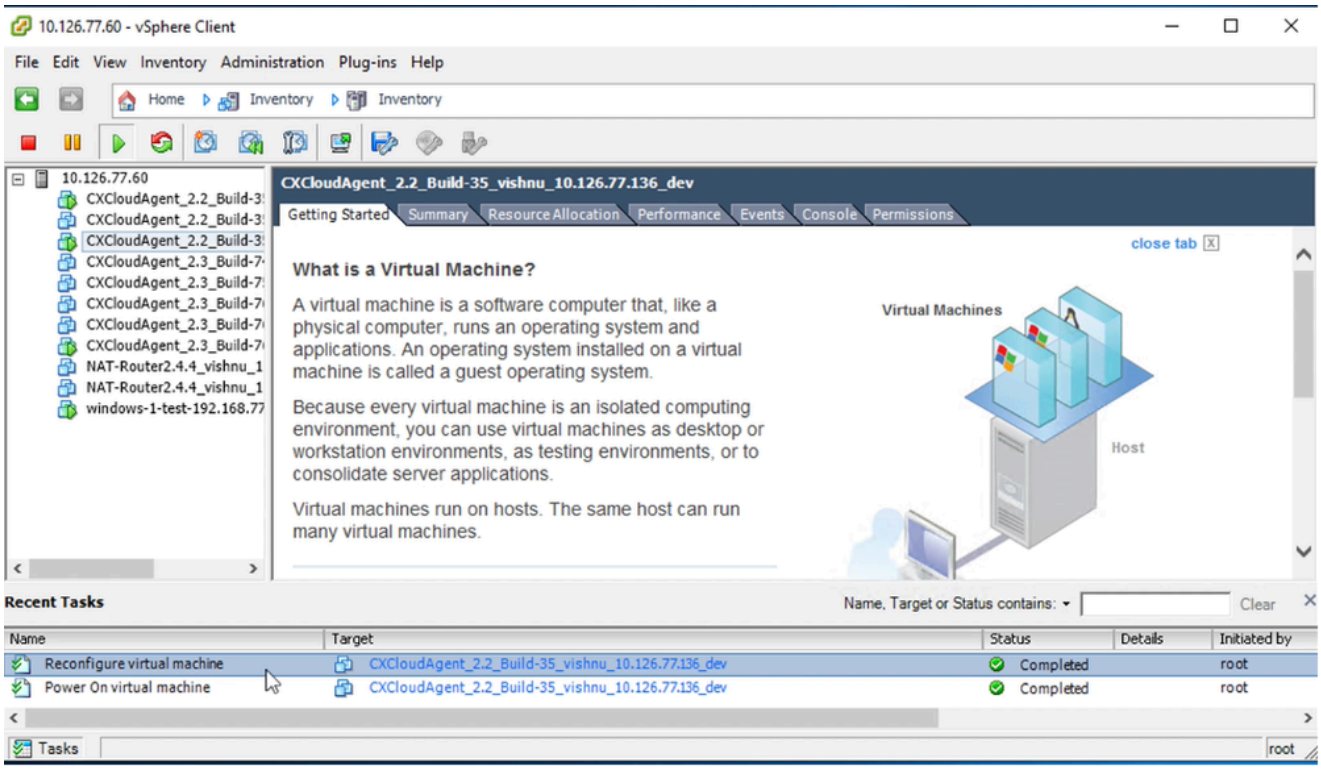
准备完成

13. 单击 完成。



Hardware

14. 单击OK完成重新配置。已完成的重新配置将显示在最近任务面板中。

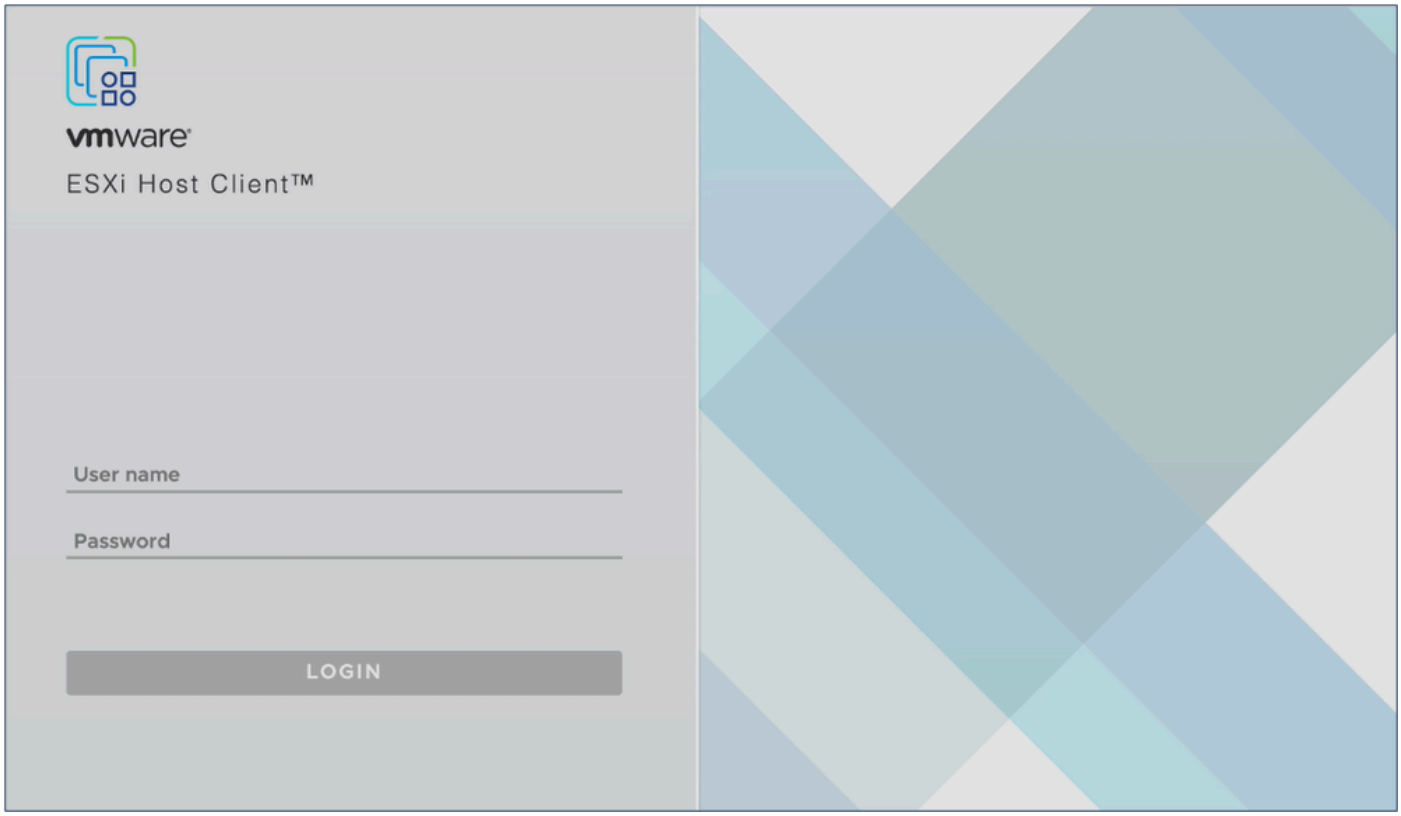


最近的任务

注意：配置更改大约需要五分钟才能完成。

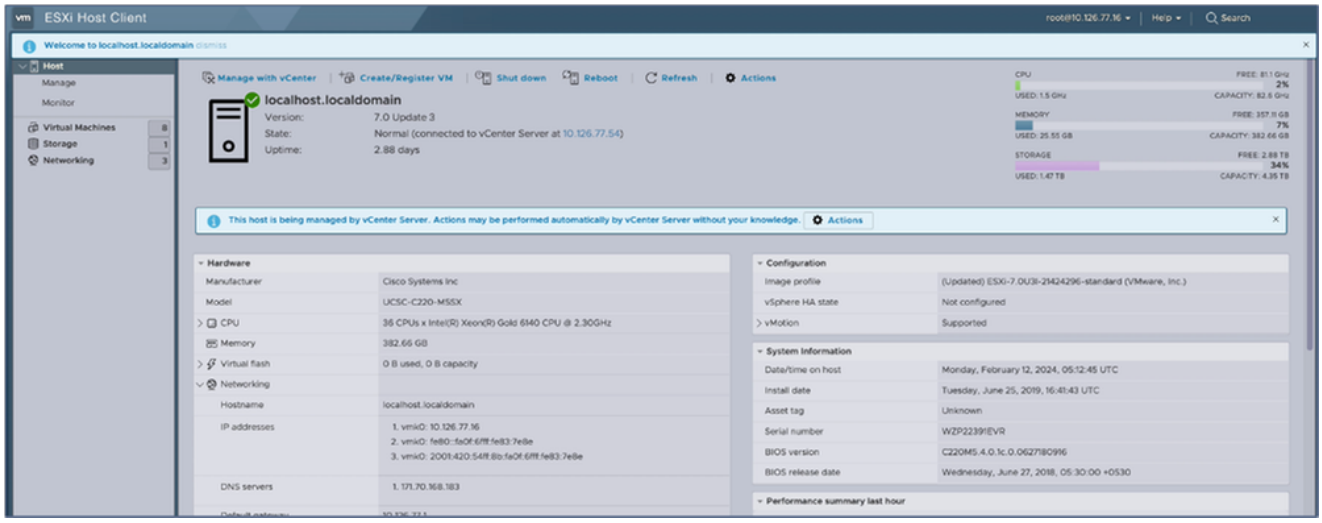
使用Web客户端ESXi v6.0重新配置

要使用Web客户端ESXi v6.0更新虚拟机配置，请执行以下操作：



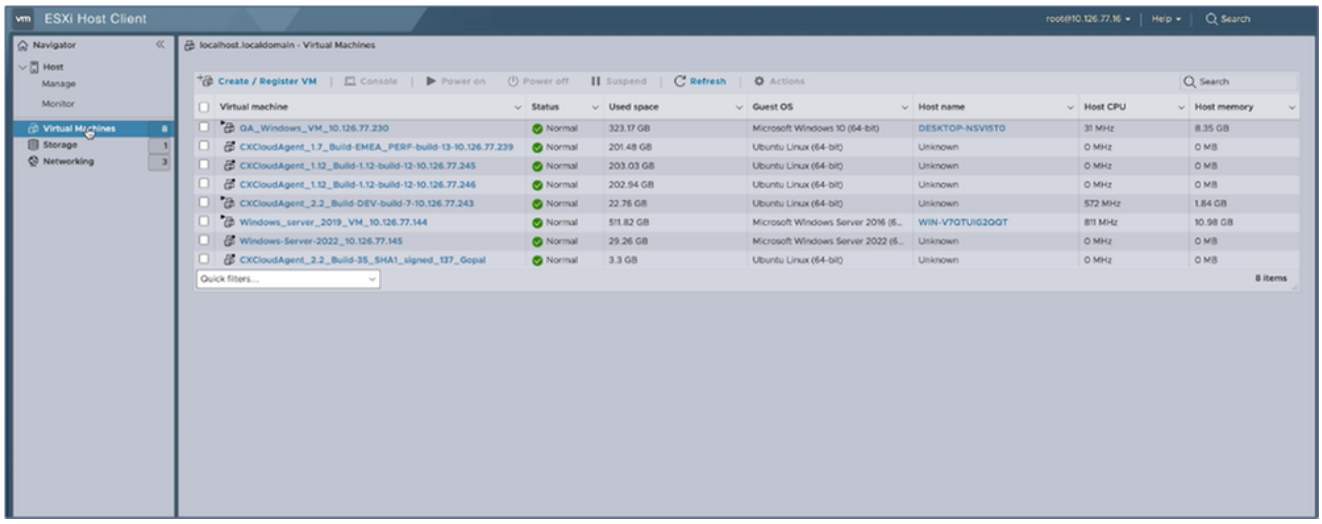
ESXi客户端

1. 登录到VMware ESXi客户端。系统随即会显示Home页面。



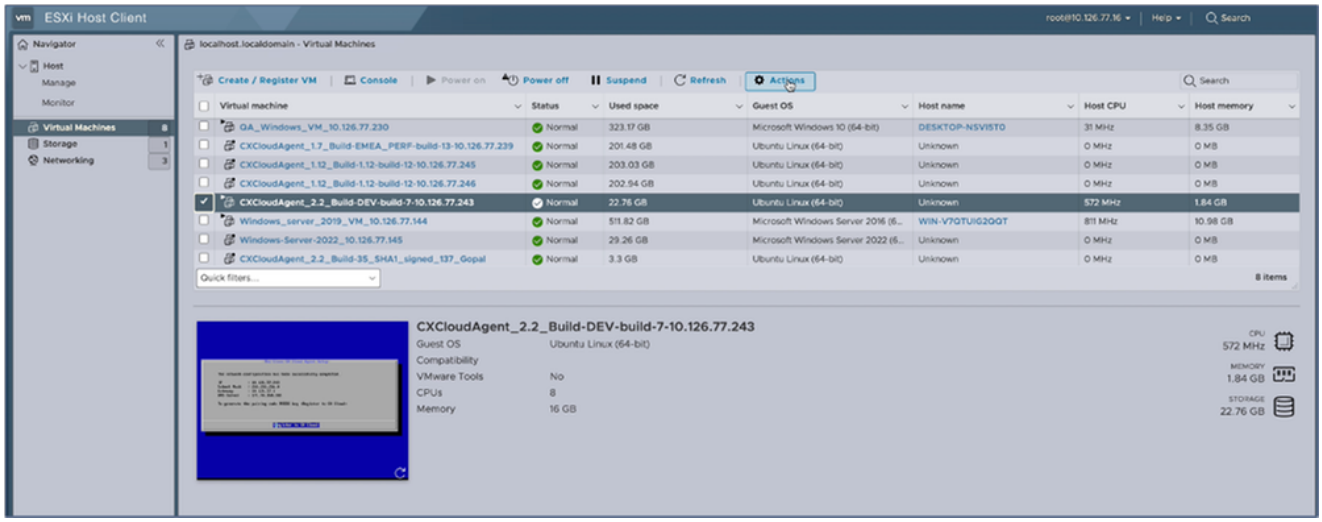
ESXi主页

2. 单击Virtual Machine以显示VM列表。



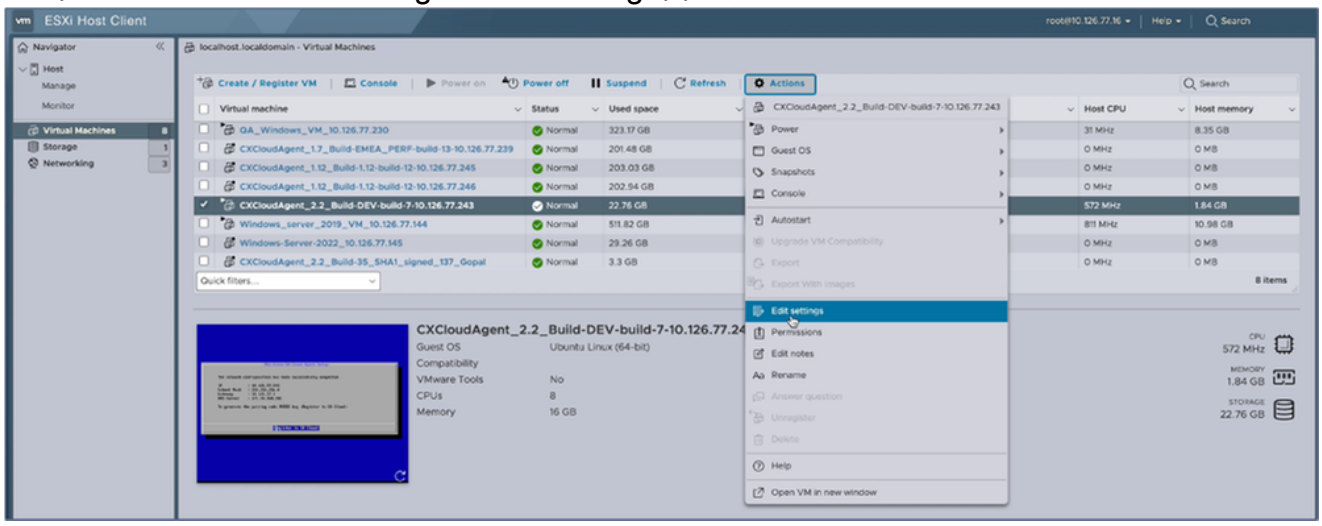
VM列表

3. 选择目标虚拟机。

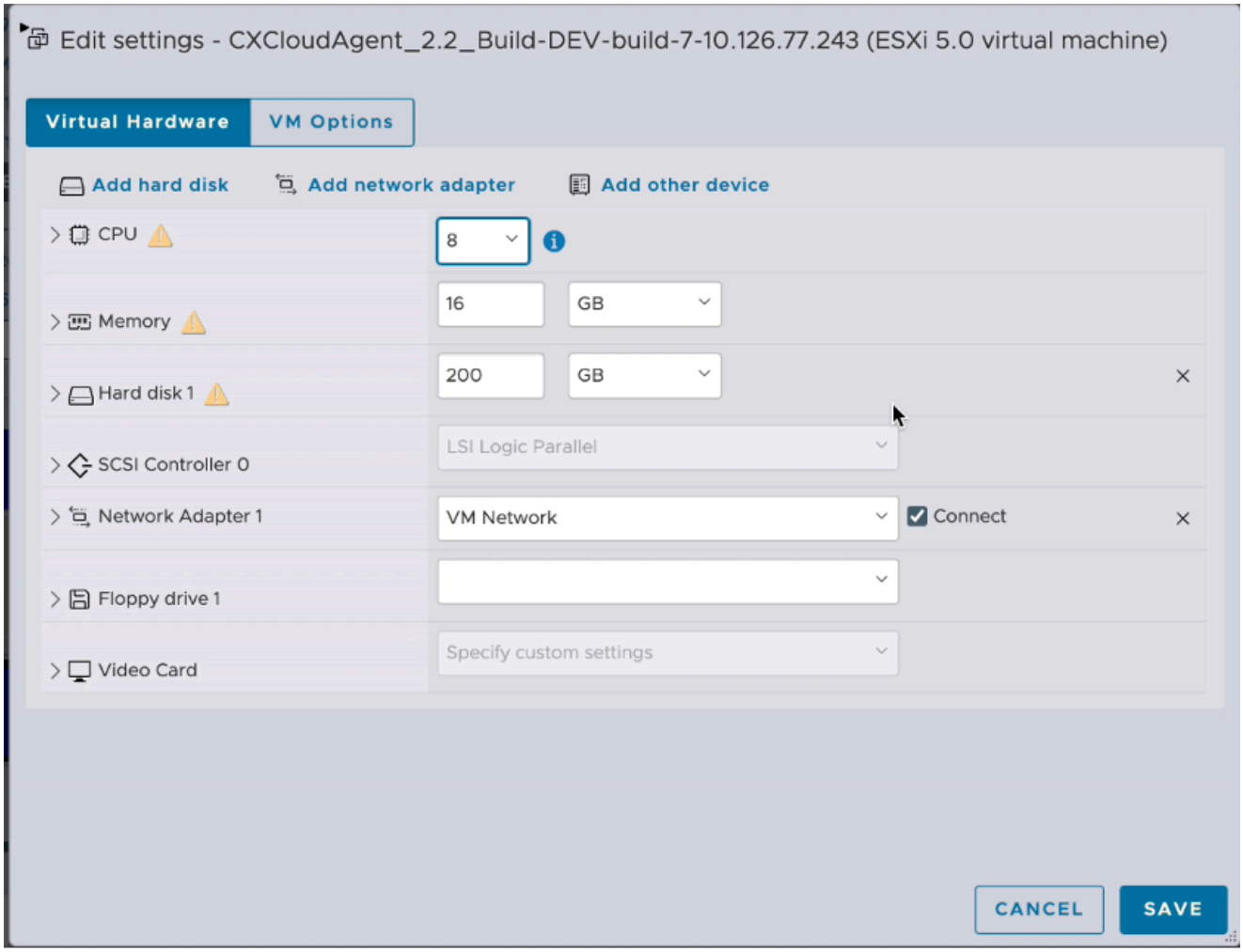


目标VM

4. 单击Actions并选择Edit Settings。Edit Settings窗口打开。

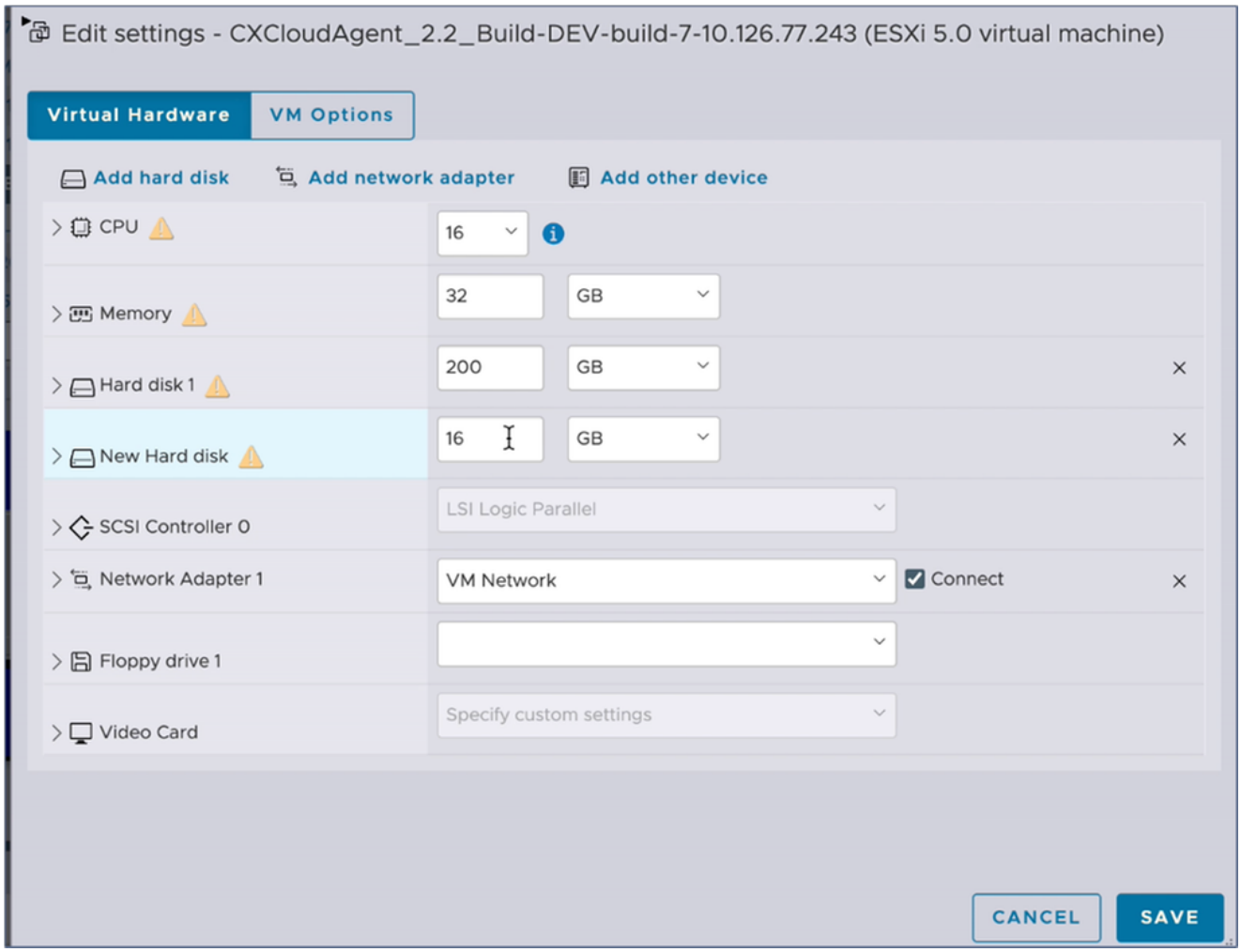


操作



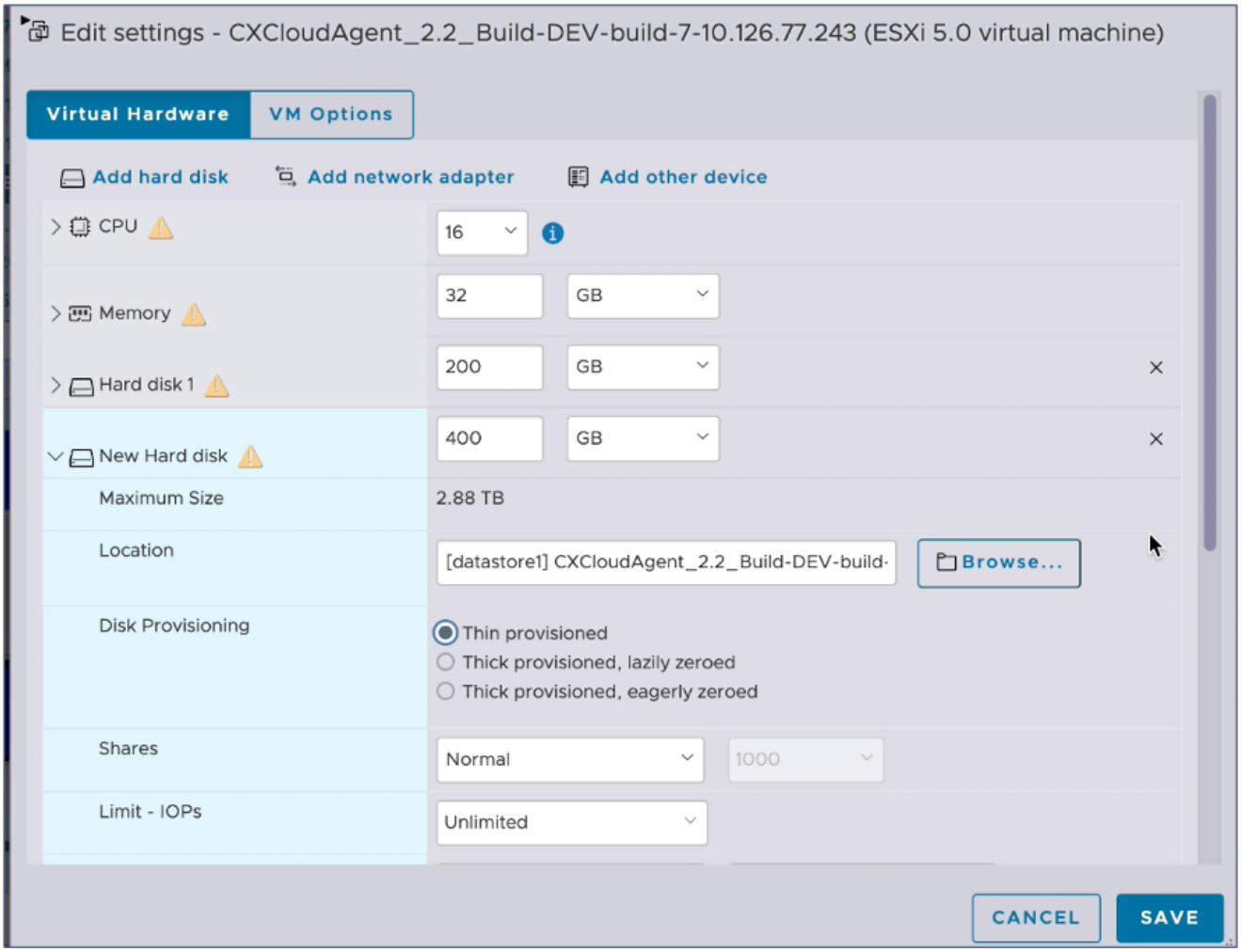
编辑设置

5. 按指定更新CPU值：
   中型：16个内核（8个插槽*2个内核/插槽）
   大型：32个内核（16个插槽*2个内核/插槽）
6. 按指定更新Memory值：
   中：32 GB
   大型：64 GB
7. 单击Add hard disk> New standard hard disk。新的硬盘条目将显示在Edit settings窗口中。



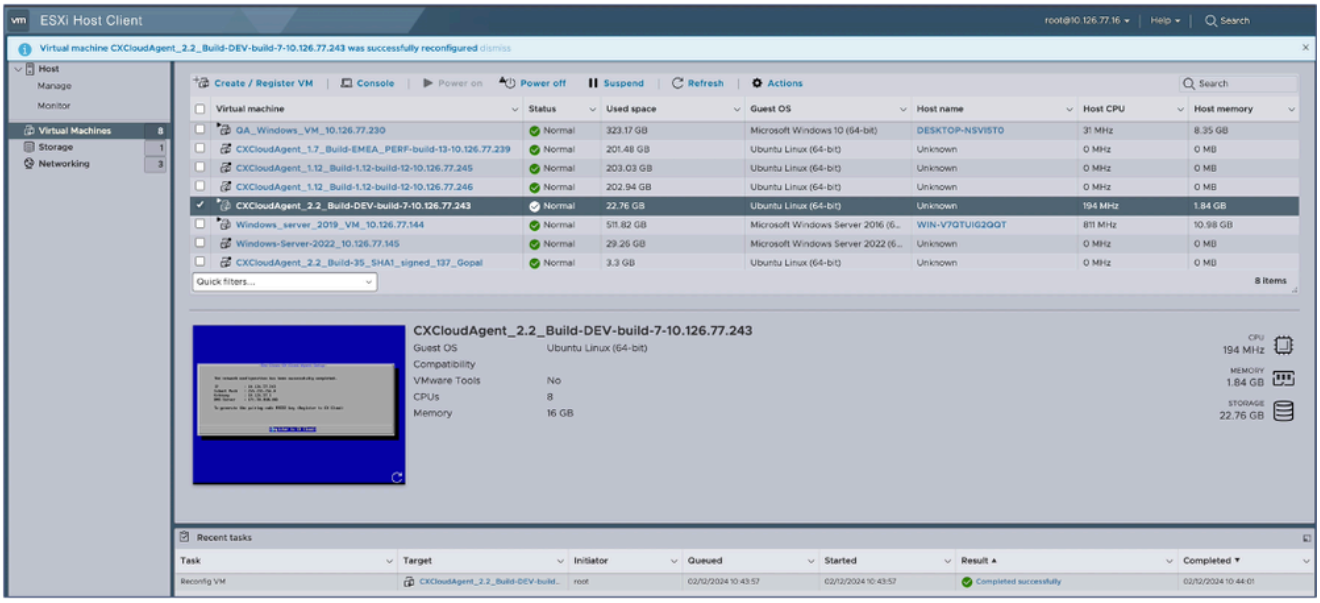
编辑设置

8. 按指定更新新硬盘值：
   中小型：400 GB（初始大小为200 GB，将总空间增加到600 GB）
   小到大：1000 GB（初始大小为200 GB，将总空间增加到1200 GB）
9. 单击箭头展开New Hard disk。系统随即会显示属性。



编辑设置

10. 选择Thin provisioned单选按钮。
11. 单击Save完成配置。配置更新显示在最近任务中。



最近的任务

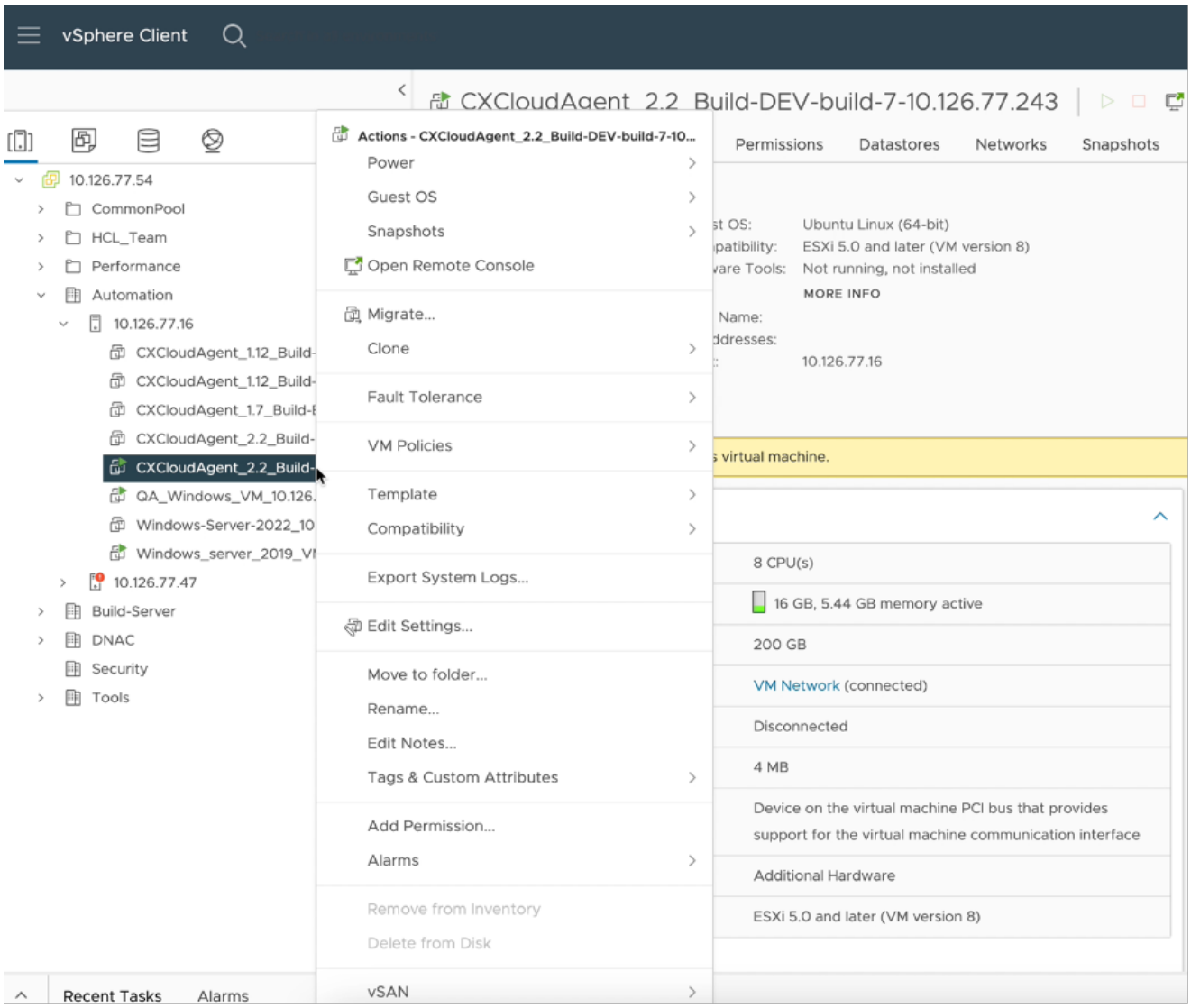
使用Web客户端vCenter重新配置

使用Web客户端vCenter更新VM配置：



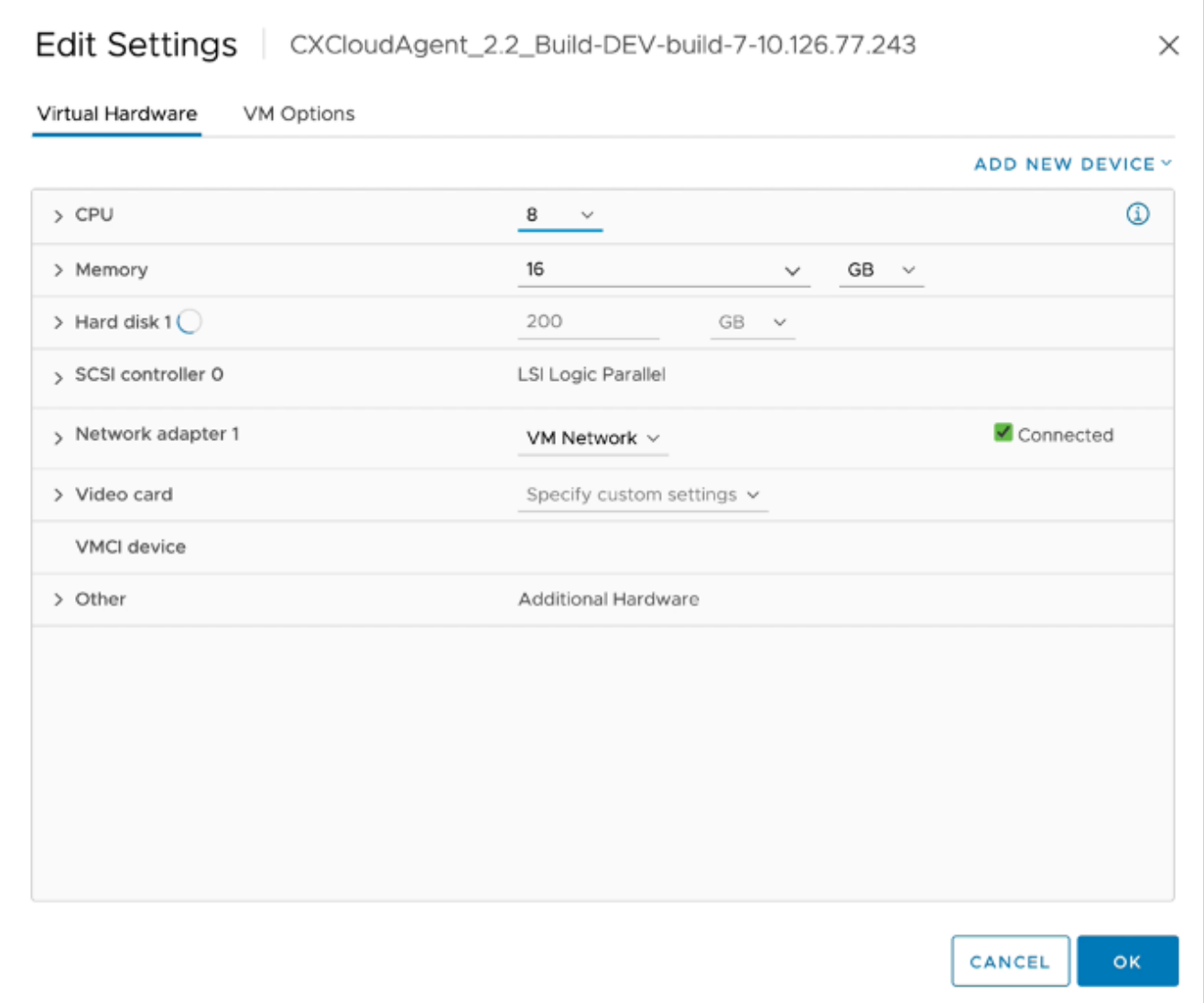
vCenter

1. 登录到vCenter。系统随即会显示Home页面。



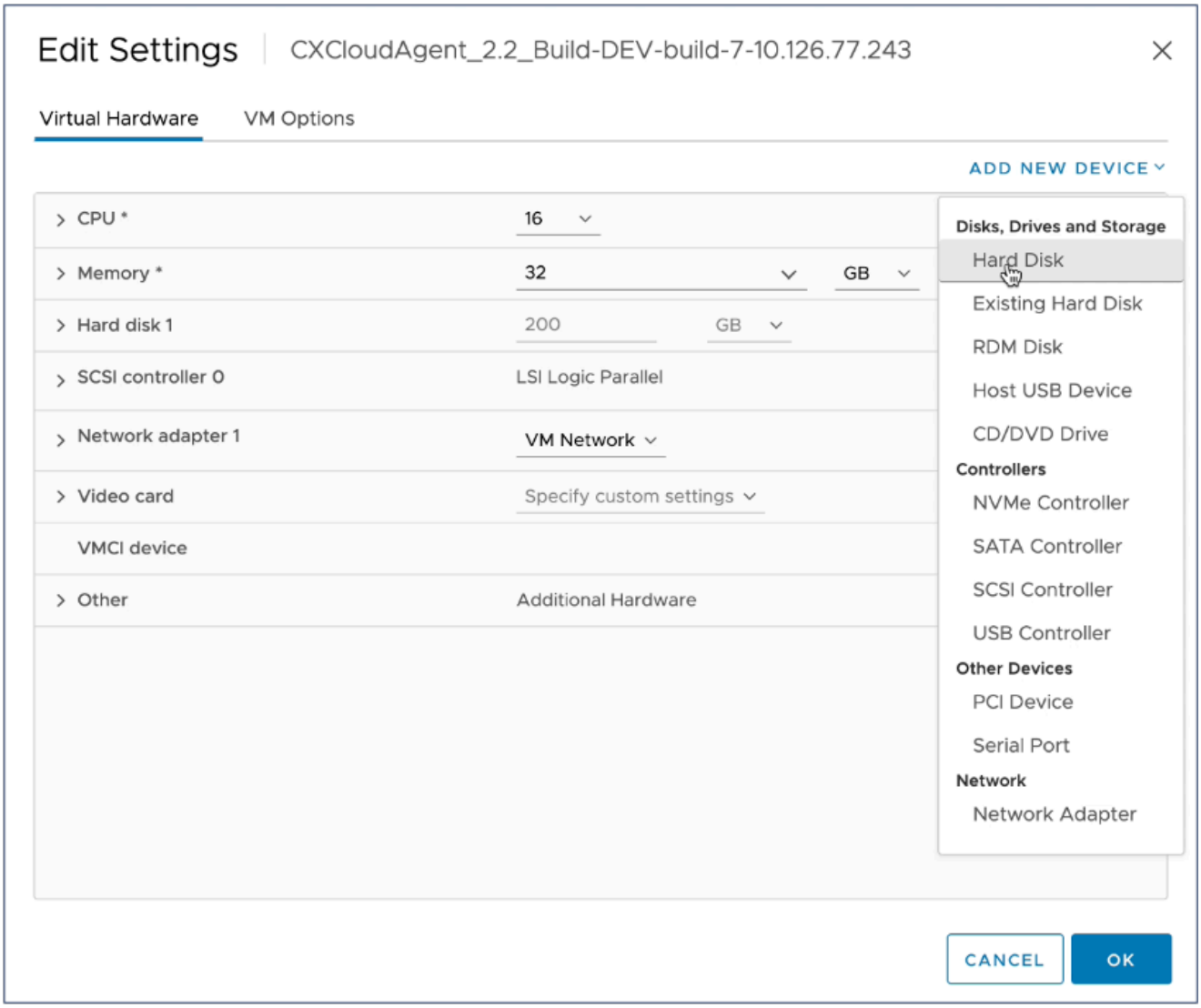
VM列表

2. 右键单击目标VM，然后从菜单中选择Edit Settings。Edit Settings窗口打开。



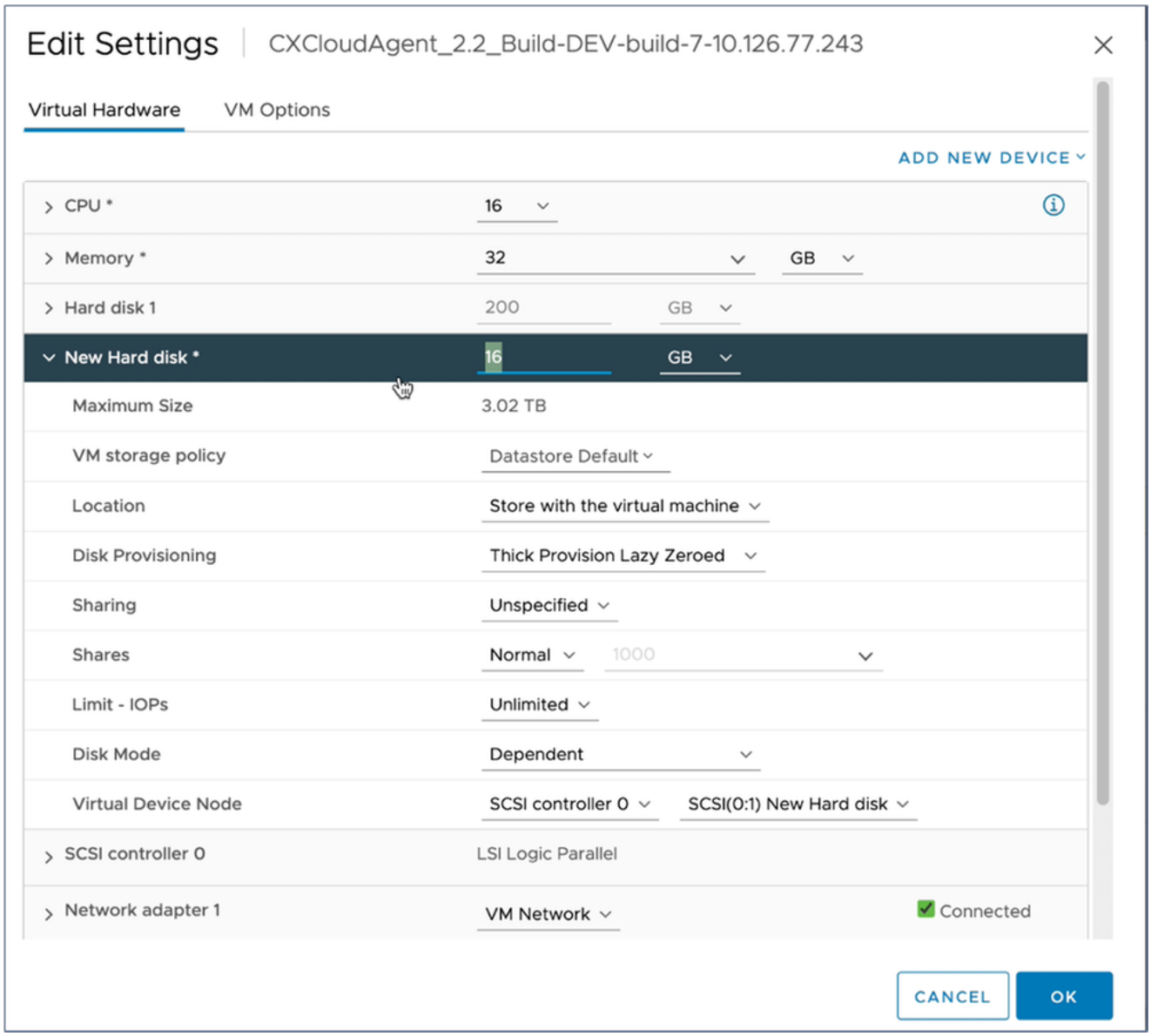
编辑设置

3. 按照指定更新CPU值:
   中型：16个内核（8个插槽*2个内核/插槽）
   大型：32个内核（16个插槽*2个内核/插槽）
4. 按照指定更新Memory值：
   中：32 GB
   大型：64 GB



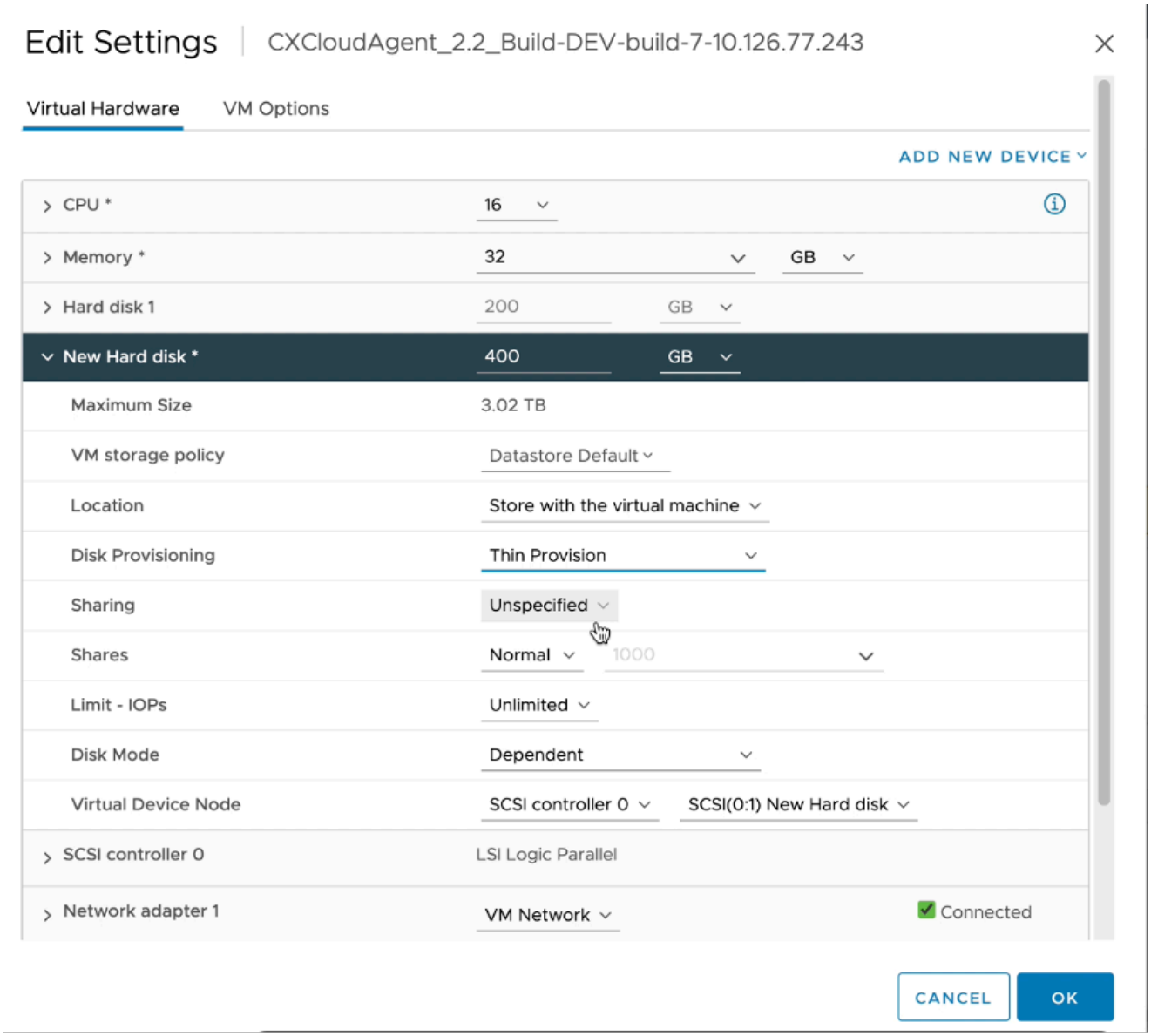
编辑设置

5. 单击Add New Device，然后选择Hard Disk。New Hard disk条目添加成功。



编辑设置

6. 按指定更新新硬盘内存：
   中小型：400 GB（初始大小为200 GB，将总空间增加到600 GB）
   小到大：1000 GB（初始大小为200 GB，将总空间增加到1200 GB）



编辑设置

7. 从Disk Provisioning下拉列表中选择Thin Provision。
8. 单击OK完成升级。

部署和网络配置

选择以下任一选项以部署CX代理：

- VMware vSphere/vCenter胖客户端ESXi 5.5/6.0
- VMware vSphere/vCenter Web客户端ESXi 6.0或Web客户端vCenter安装
- Oracle Virtual Box 7.0.12
- Microsoft Hyper-V 安装

OVA 部署

胖客户端 ESXi 5.5/6.0 安装

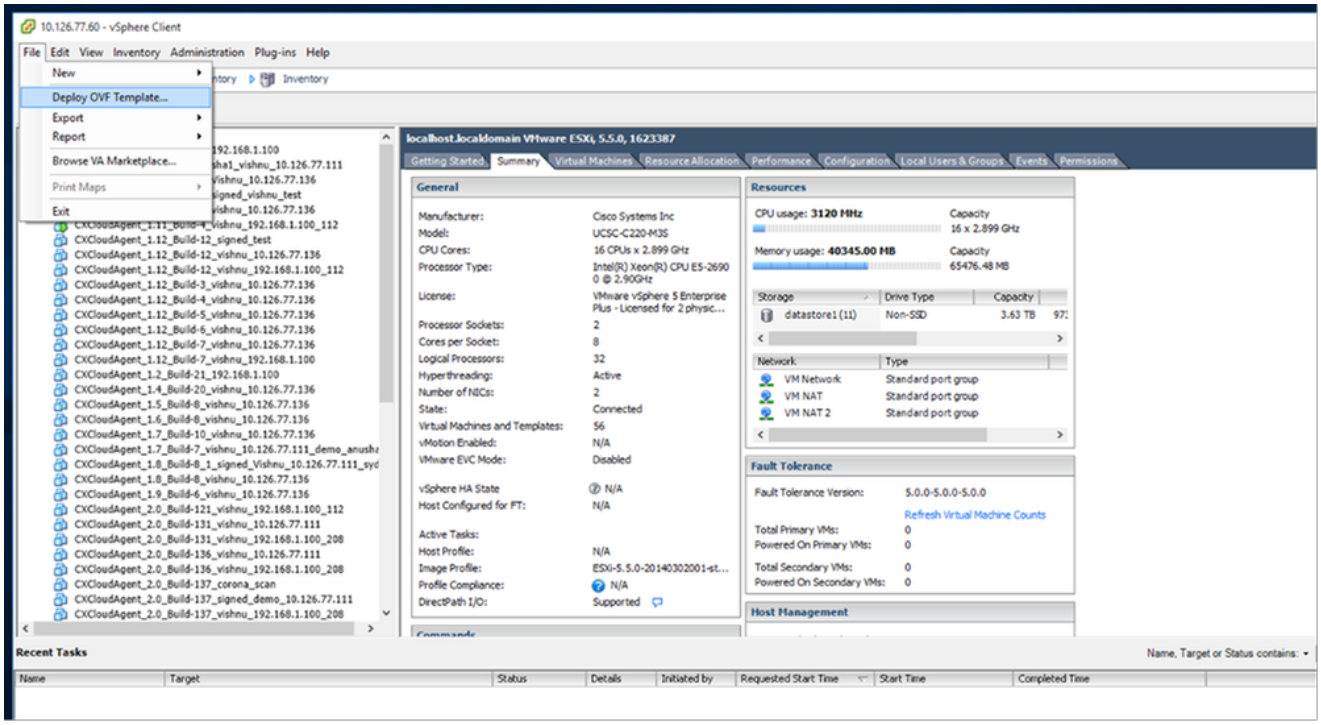
此客户端允许使用vSphere胖客户端部署CX代理OVA。

1. 下载映像后，启动VMware vSphere Client并登录。



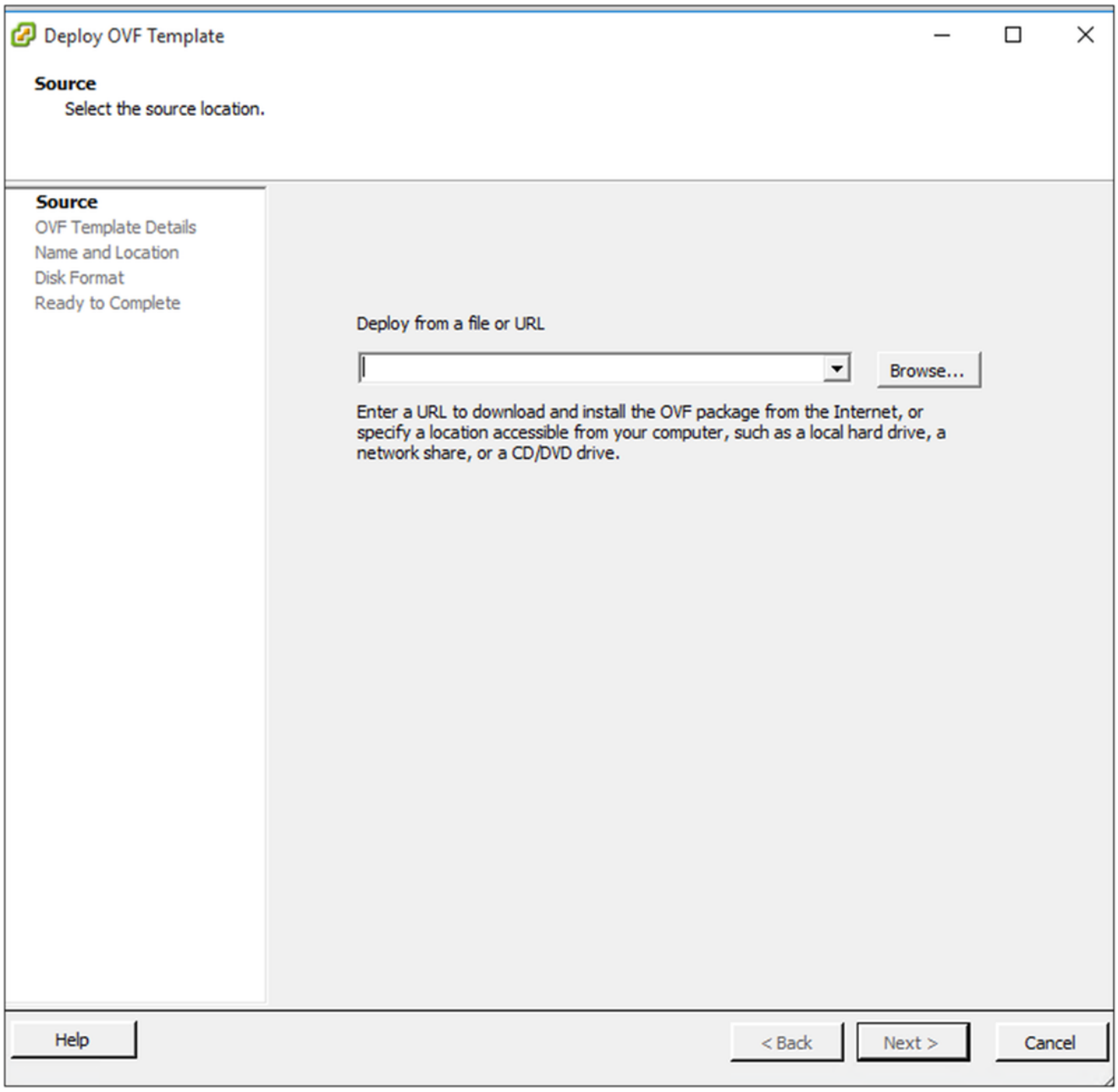
登录

2. 从菜单中选择文件>部署OVF模板。



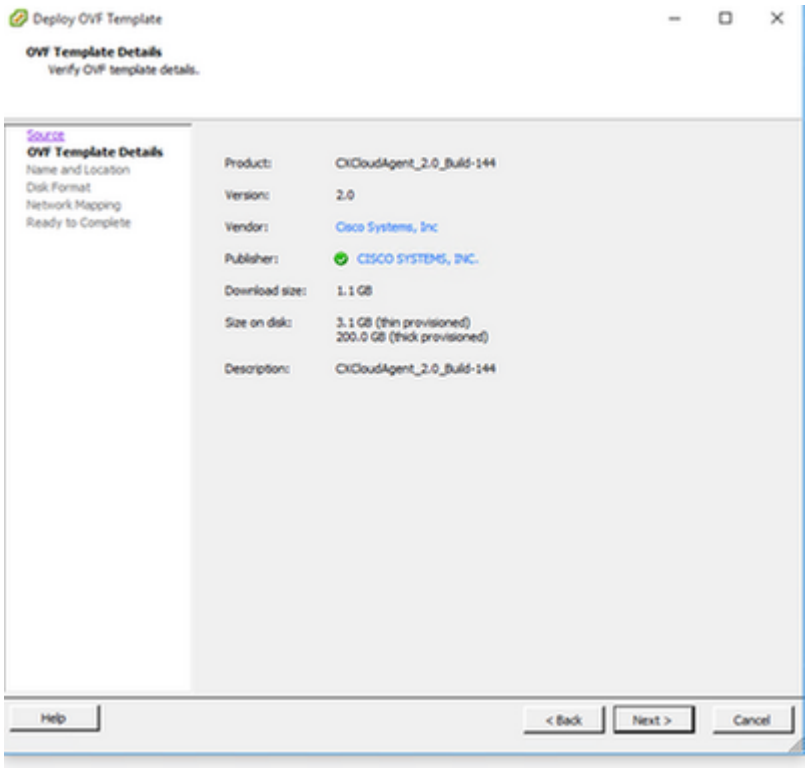
vSphere 客户端

3. 浏览以选择OVA文件，然后单击下一步。



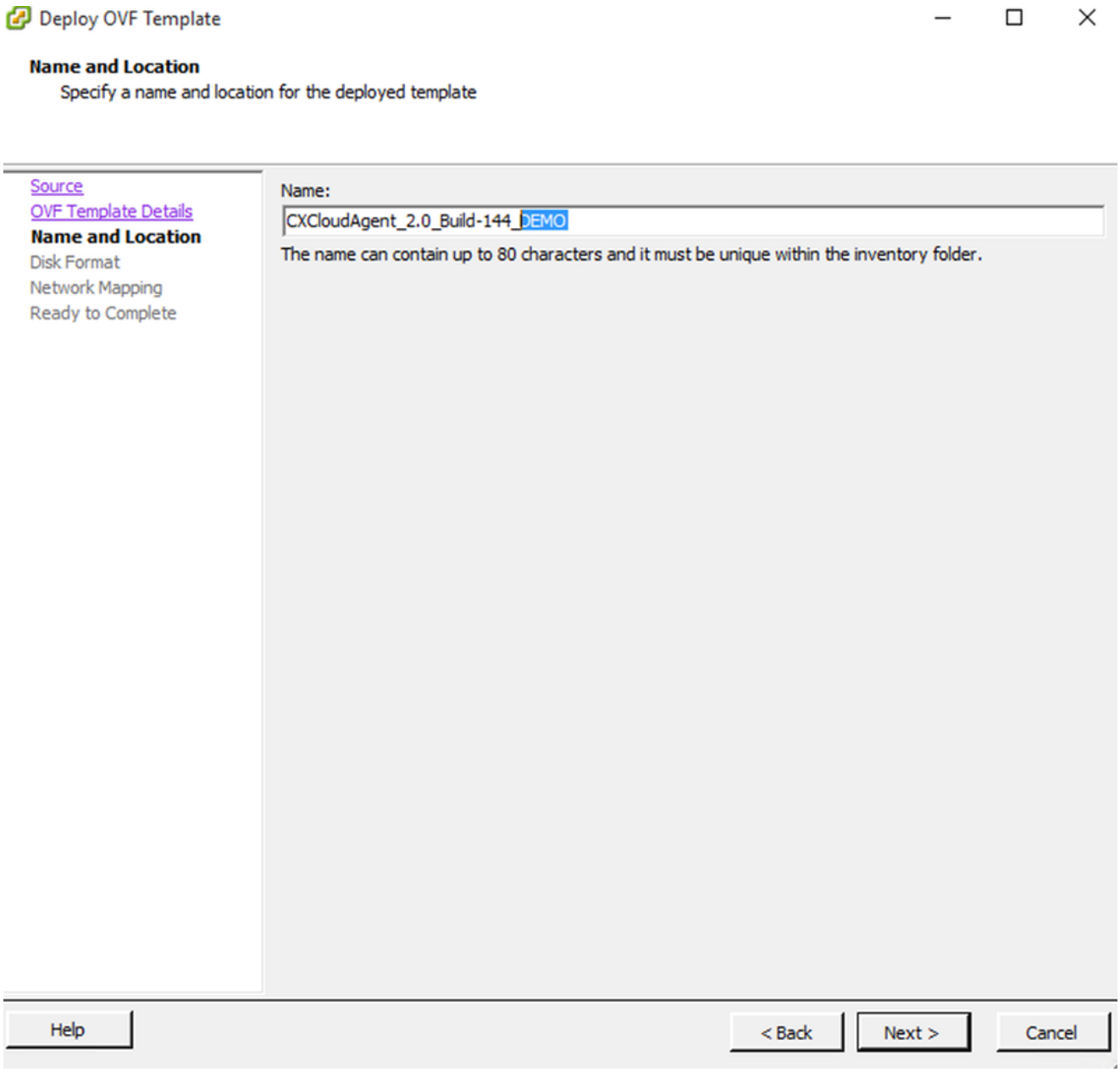
OVA 路径

4. 验证OVF详细信息，然后单击下一步。



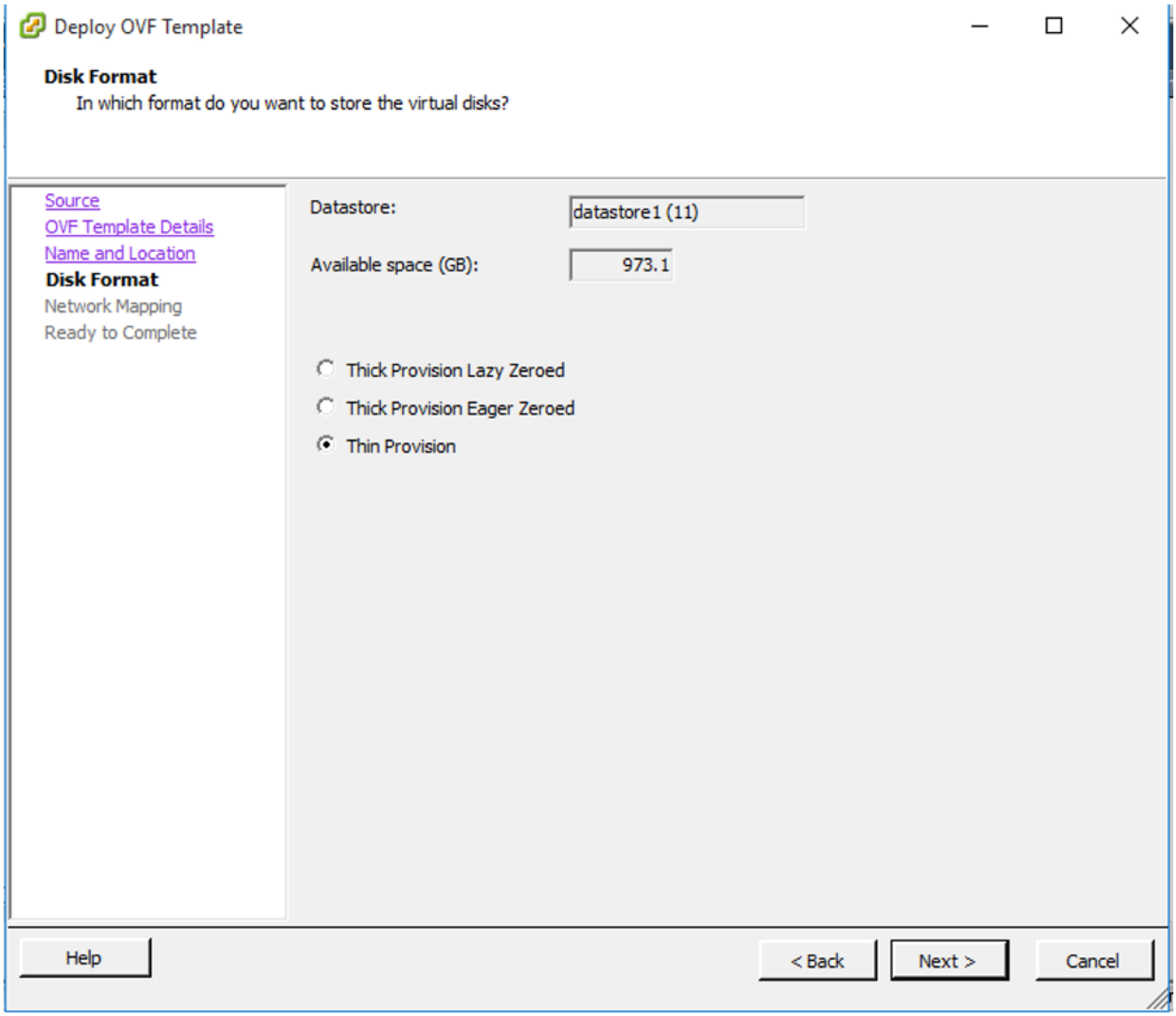
模板详细信息

5. 输入Unique Name，然后单击Next。



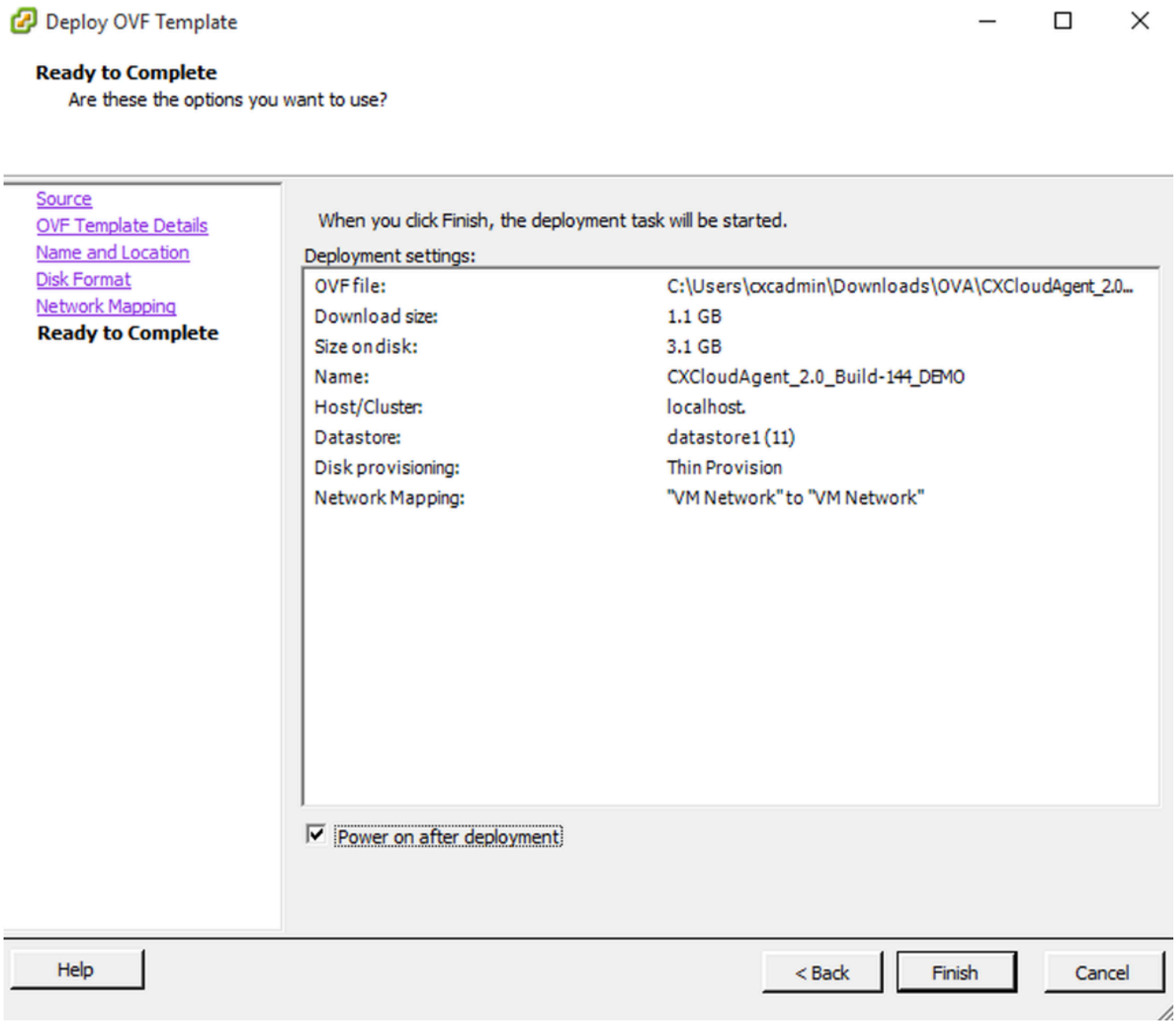
名称和位置

6. 选择Disk Format，然后单击Next（建议使用Thin Provision）。



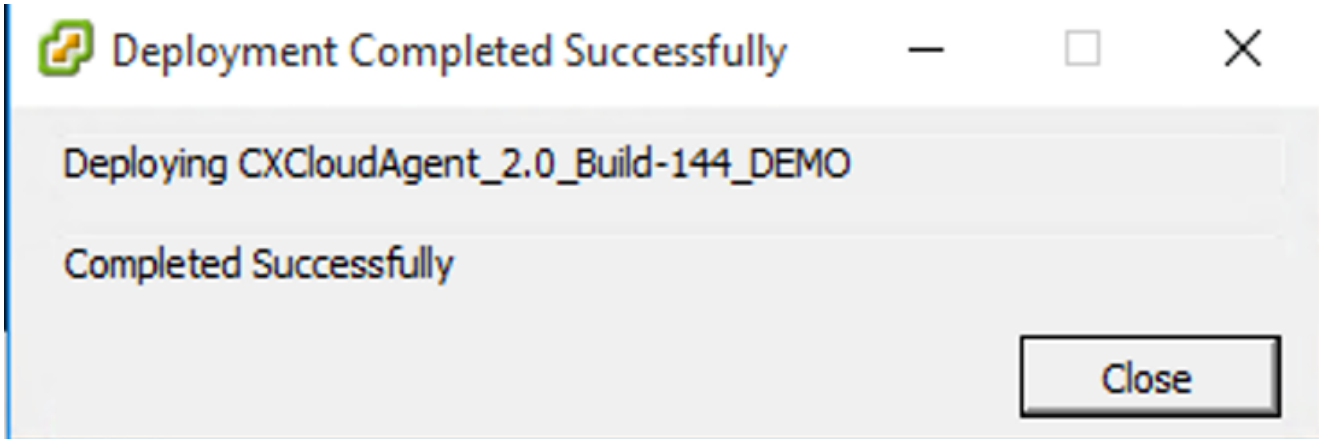
磁盘格式化

7. 选中Power on after deployment复选框，然后单击Close。



准备完成

部署可能需要几分钟。成功部署后会显示确认。



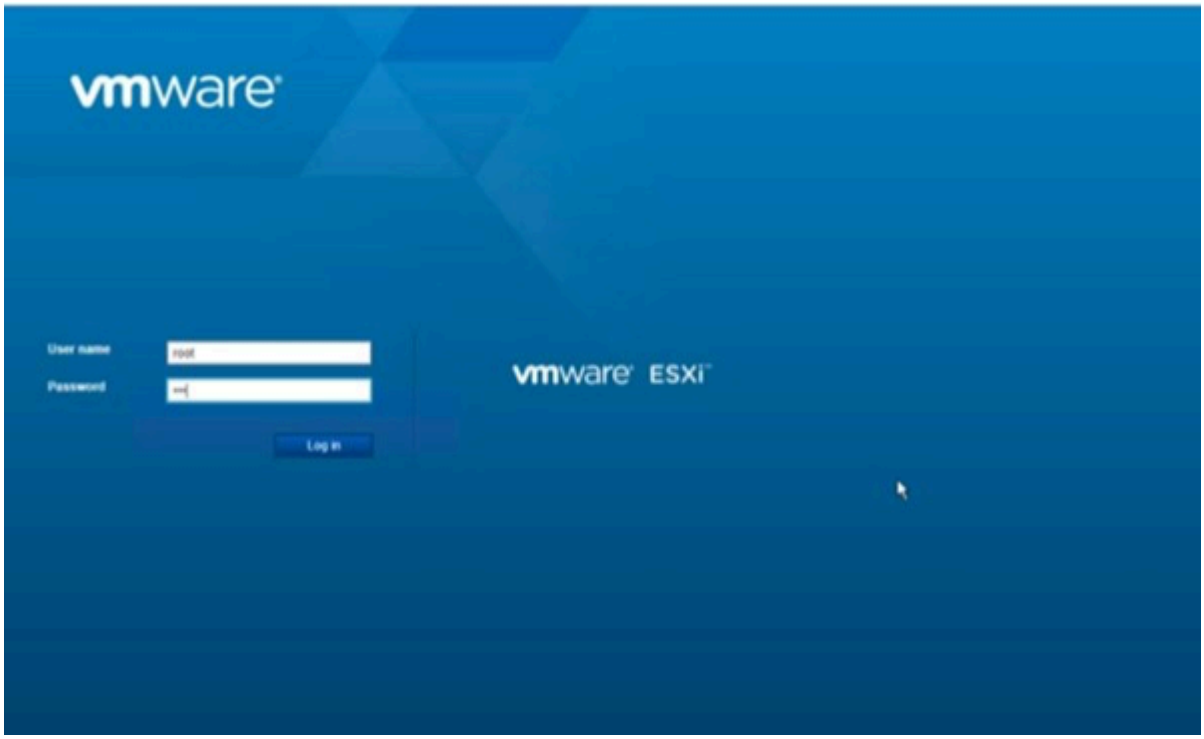
部署完成

8. 选择已部署的VM，打开控制台，然后转到网络配置以继续执行后续步骤。

Web 客户端 ESXi 6.0 安装

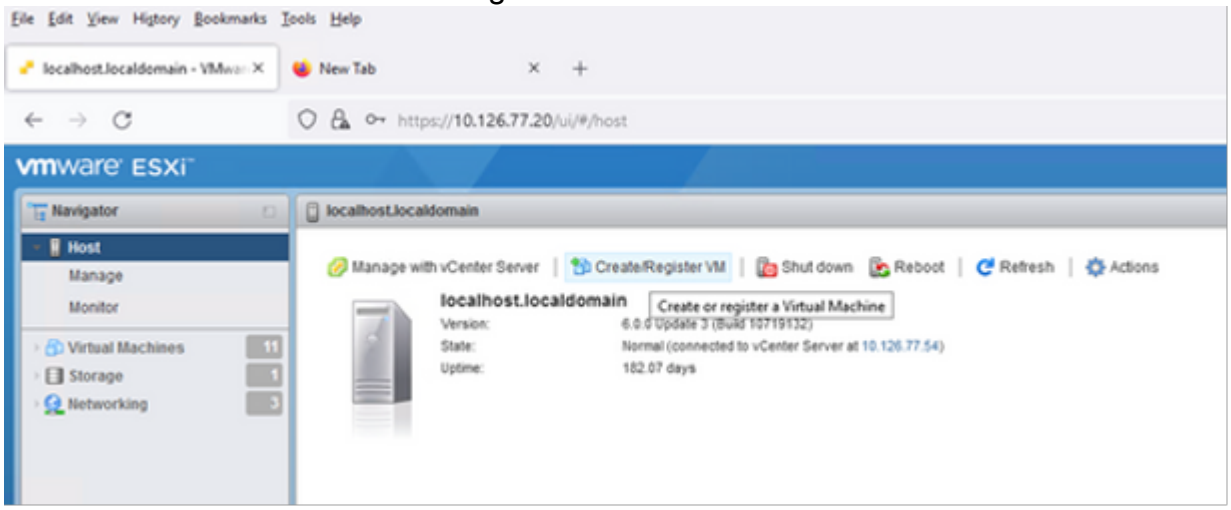
此客户端使用vSphere Web部署CX云OVA。

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



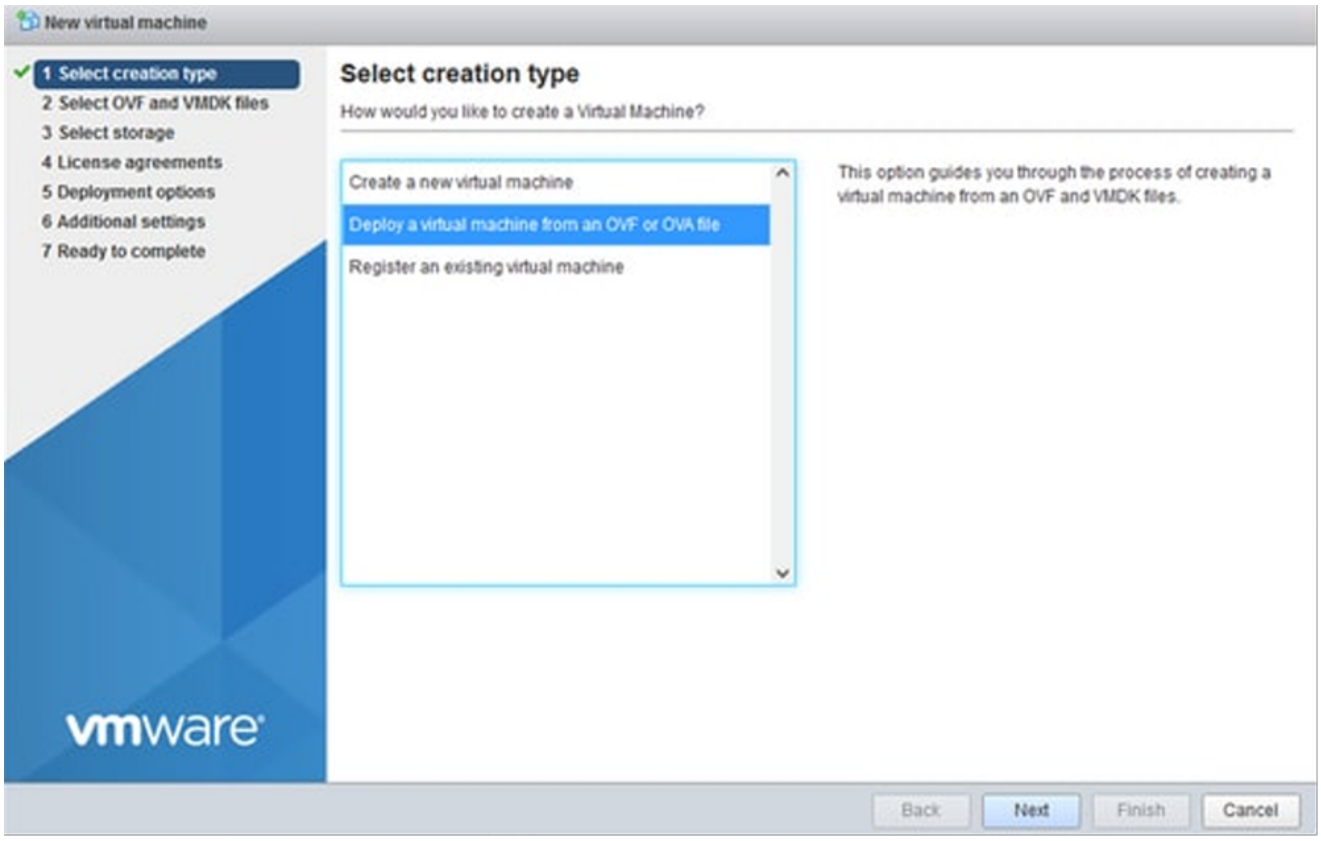
VMware ESXi 登录

2. 选择Virtual Machine > Create / Register VM。



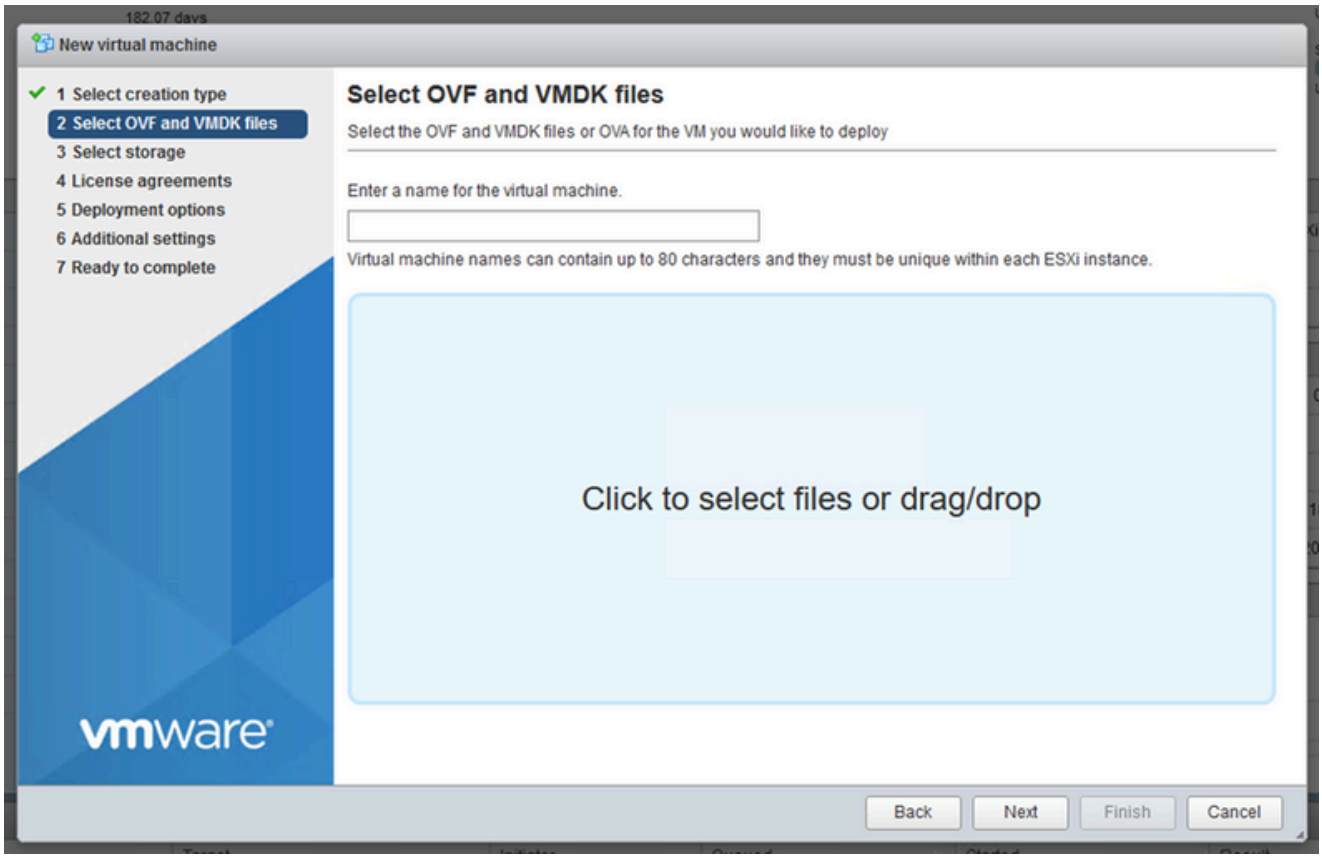
创建 VM

3. 选择通过 OVF 或 OVA 文件部署虚拟机，然后点击下一步。



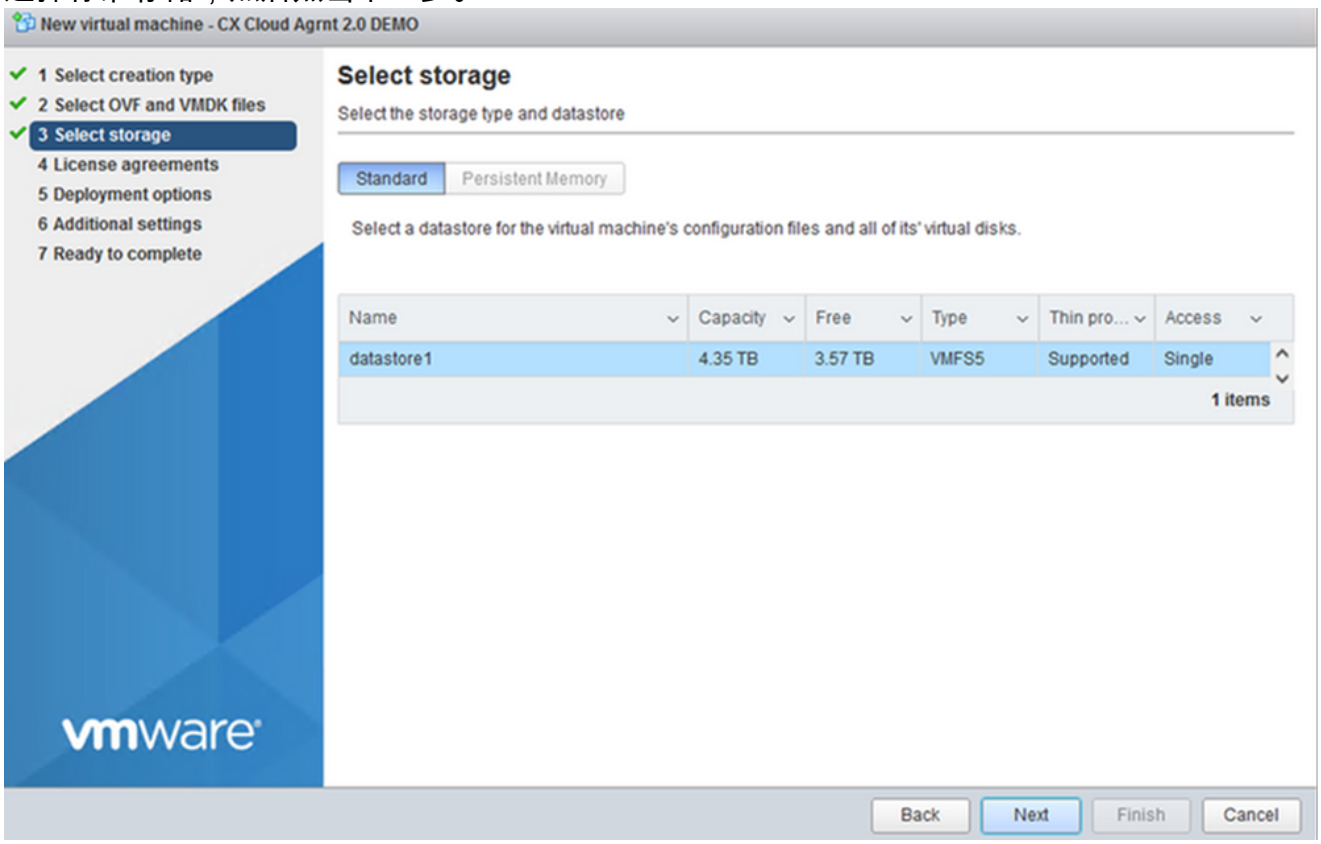
选择创建类型

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。



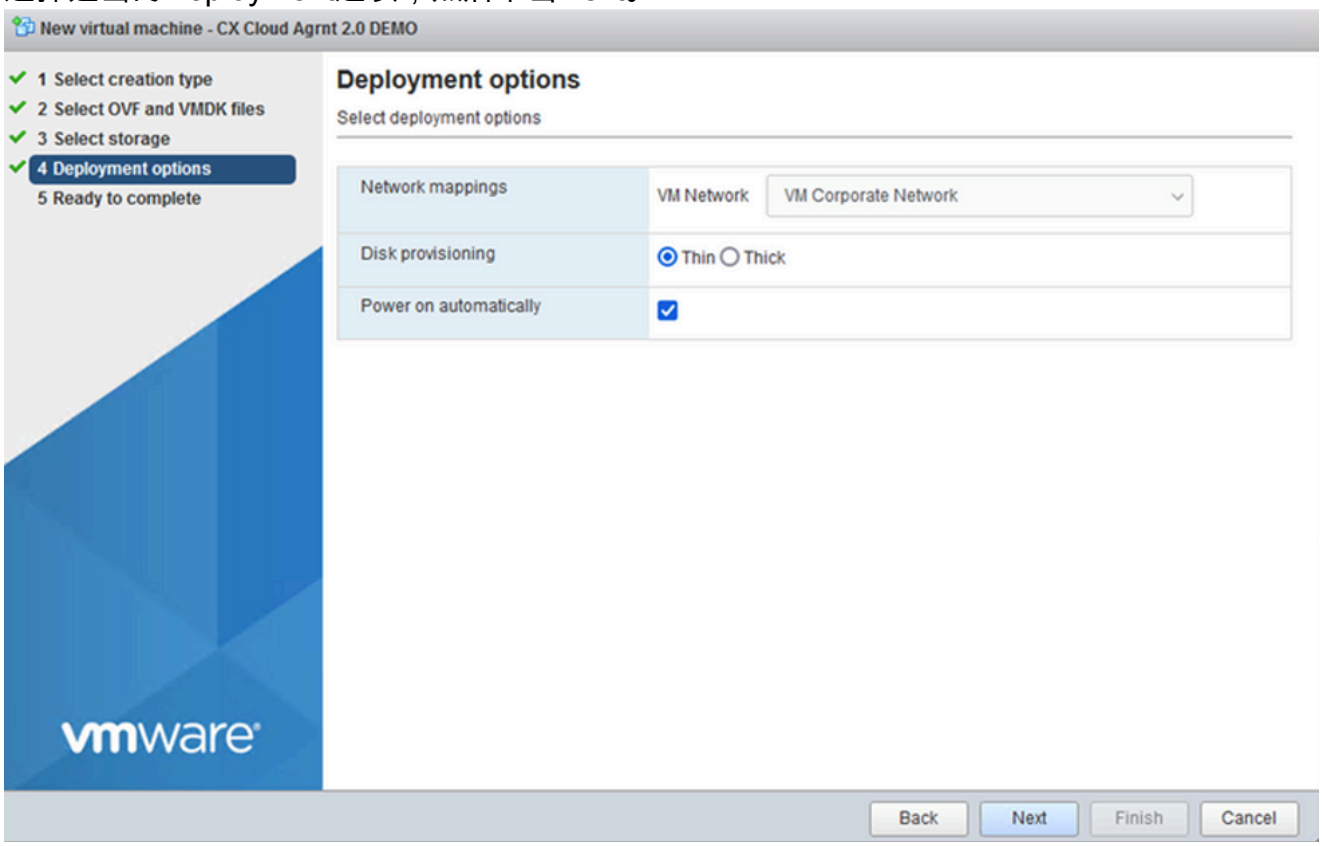
OVA 选择

6. 选择标准存储，然后点击下一步。



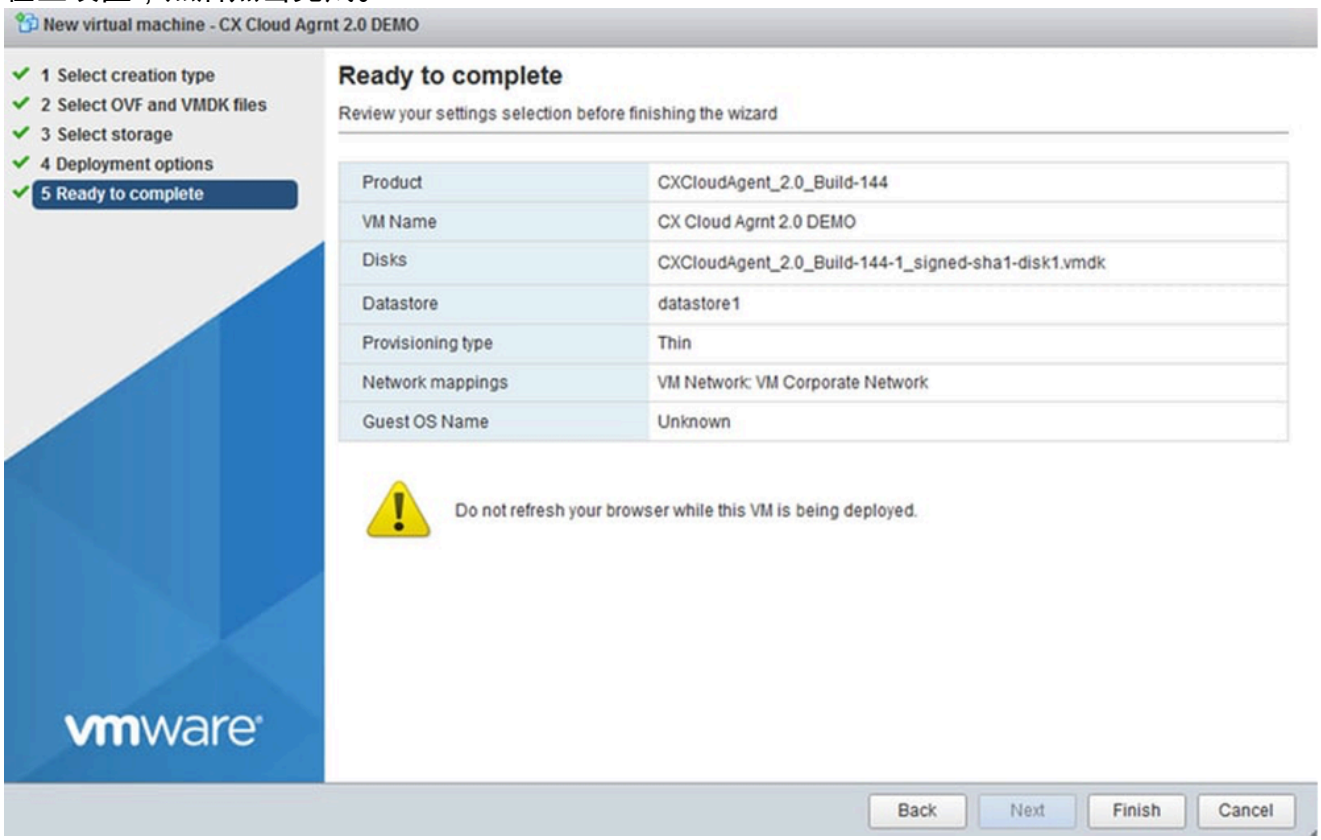
选择存储

7. 选择适当的Deployment选项，然后单击Next。

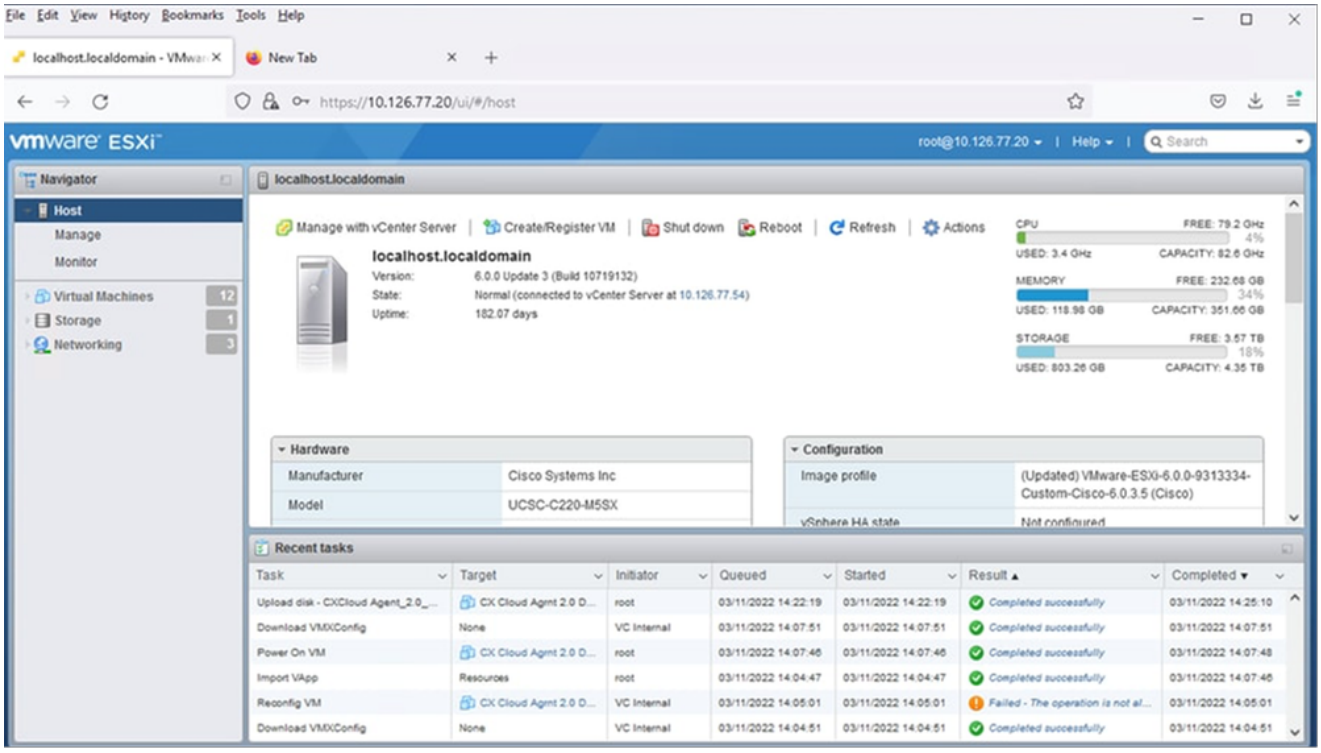


部署选项

8. 检查设置，然后点击完成。

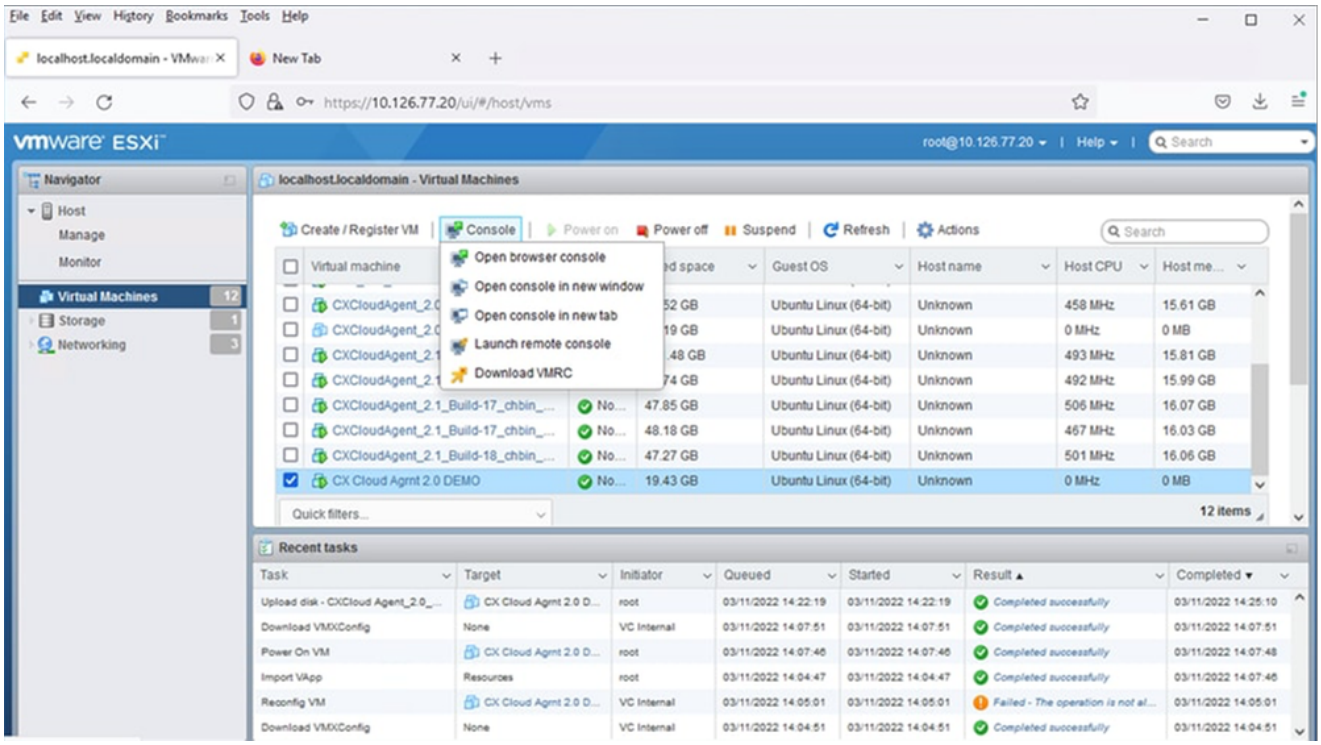


准备完成



成功完成

9. 选择刚部署的虚拟机，然后选择Console > Open browser console。



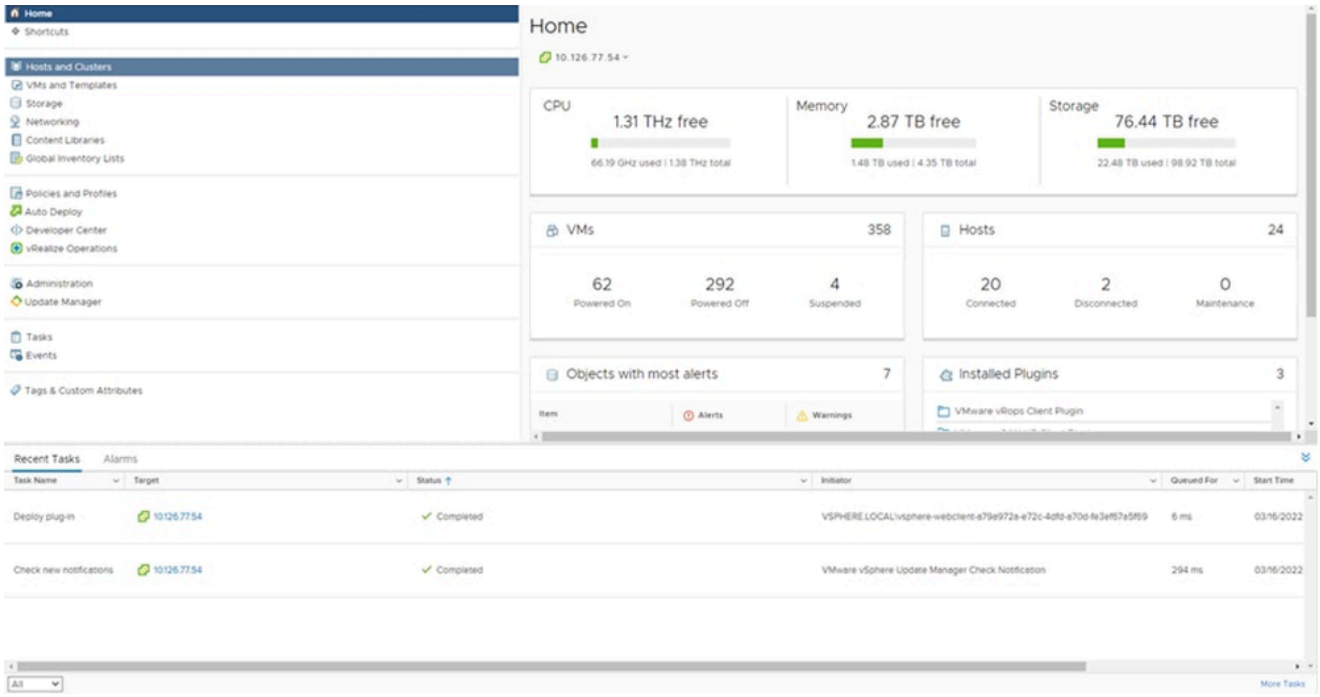
控制台

10. 导航到网络配置以继续执行后续步骤。

Web 客户端 vCenter 安装

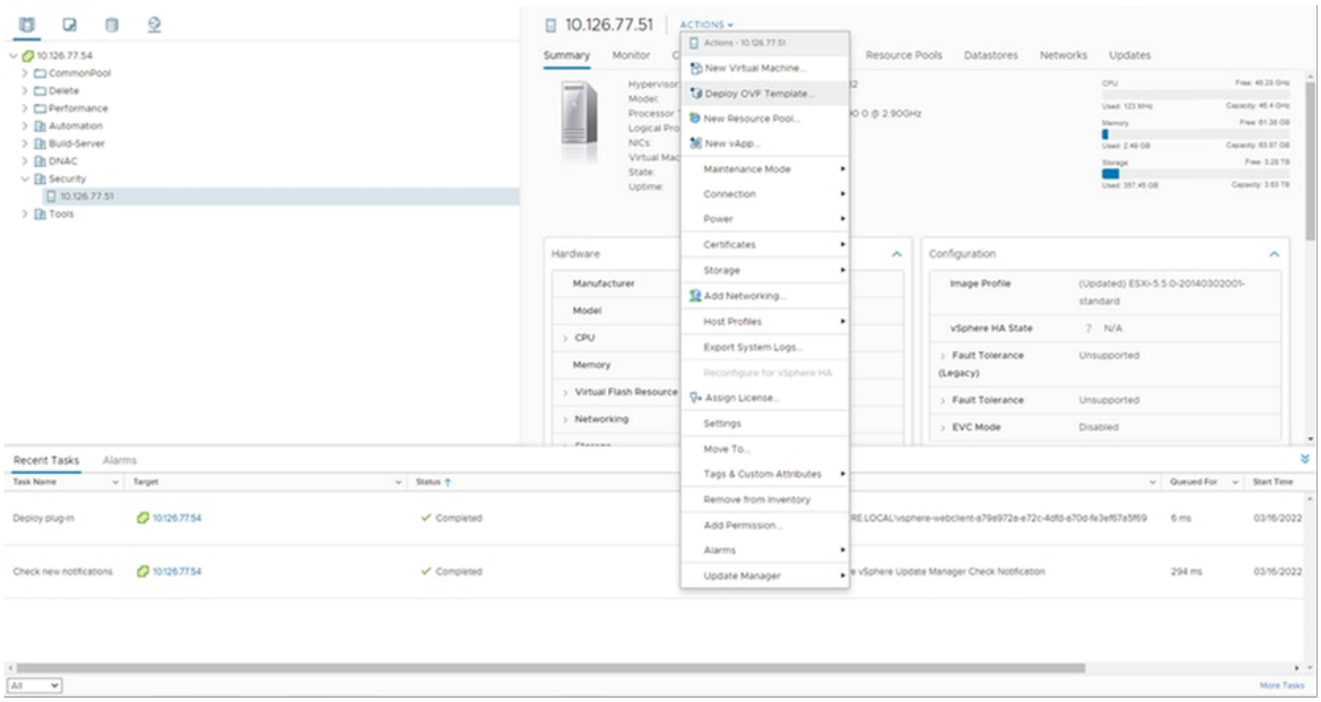
此客户端允许使用Web客户端vCenter部署CX代理OVA。

1. 使用ESXi/虚拟机监控程序凭证登录vCenter客户端。



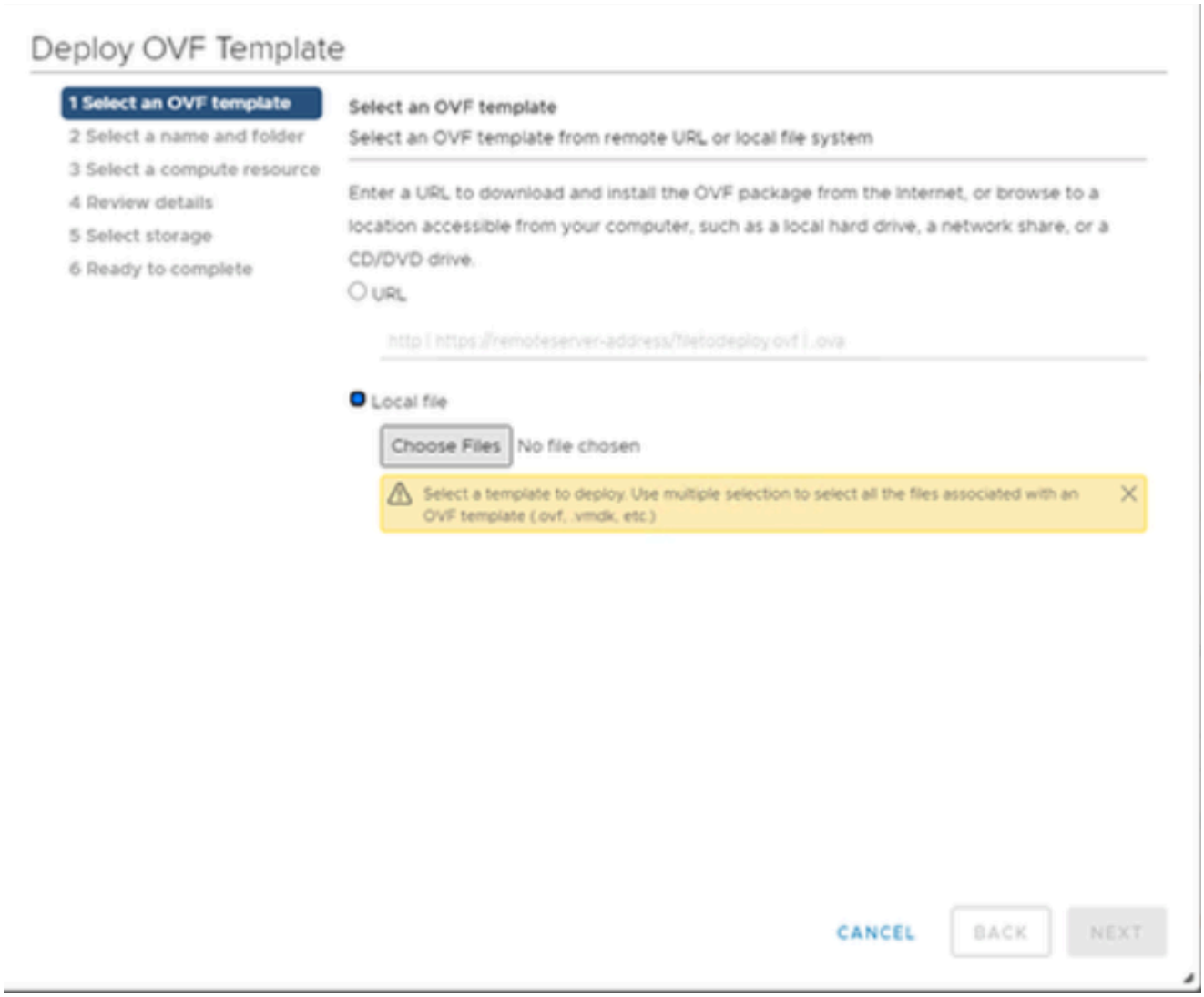
主页

2. 在Home页中，单击Hosts and Clusters。

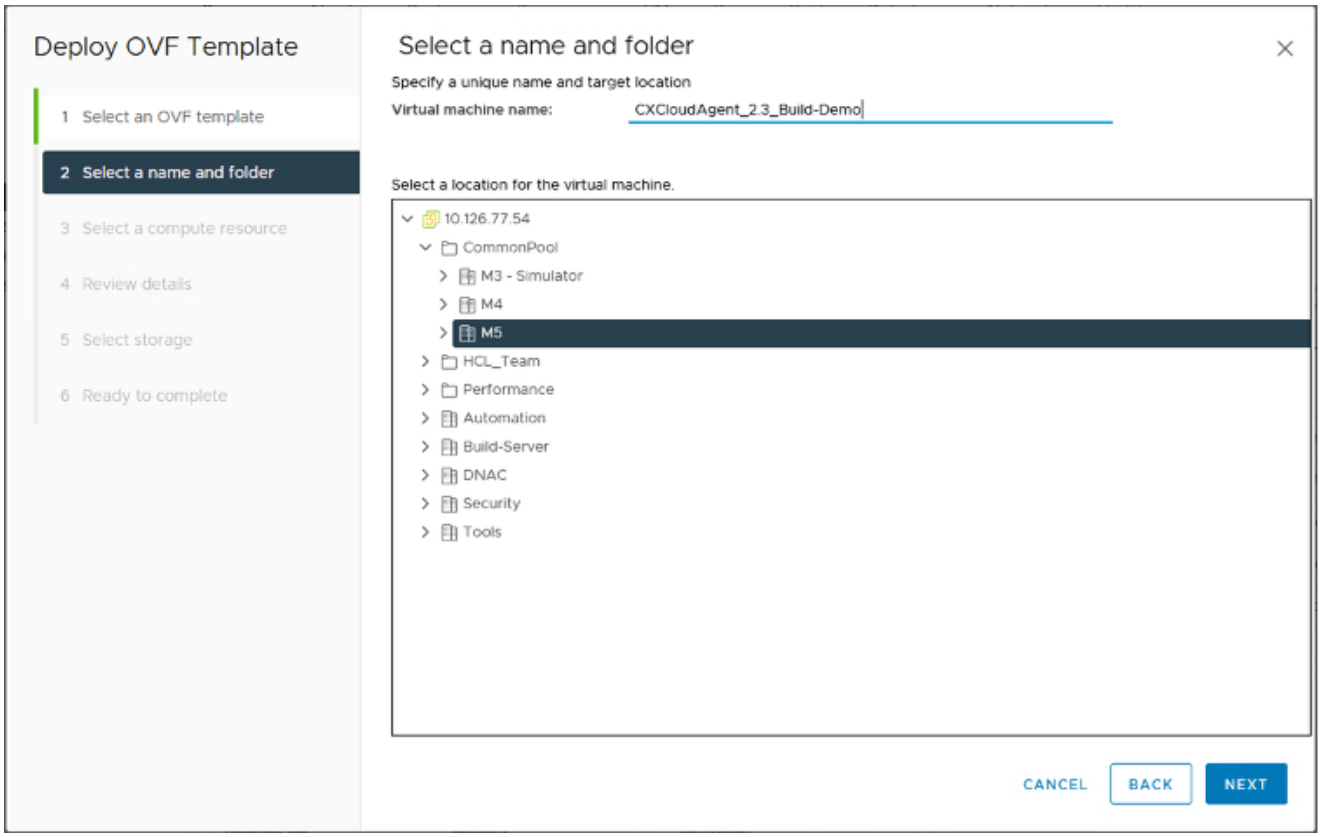


主机和集群

3. 选择VM。然后点击操作>部署OVF模板。

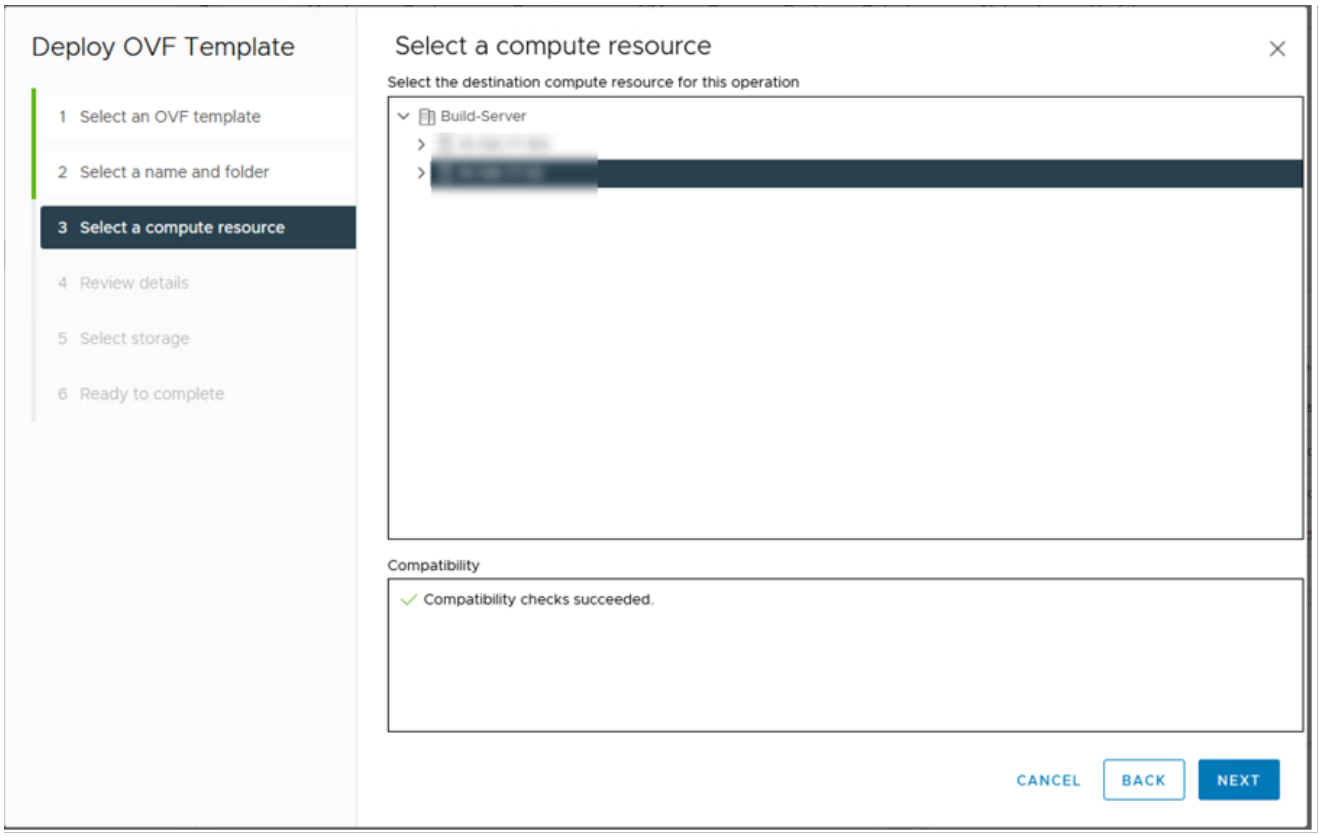


4. 直接添加URL或浏览以选择OVA文件。
5. 单击 Next。



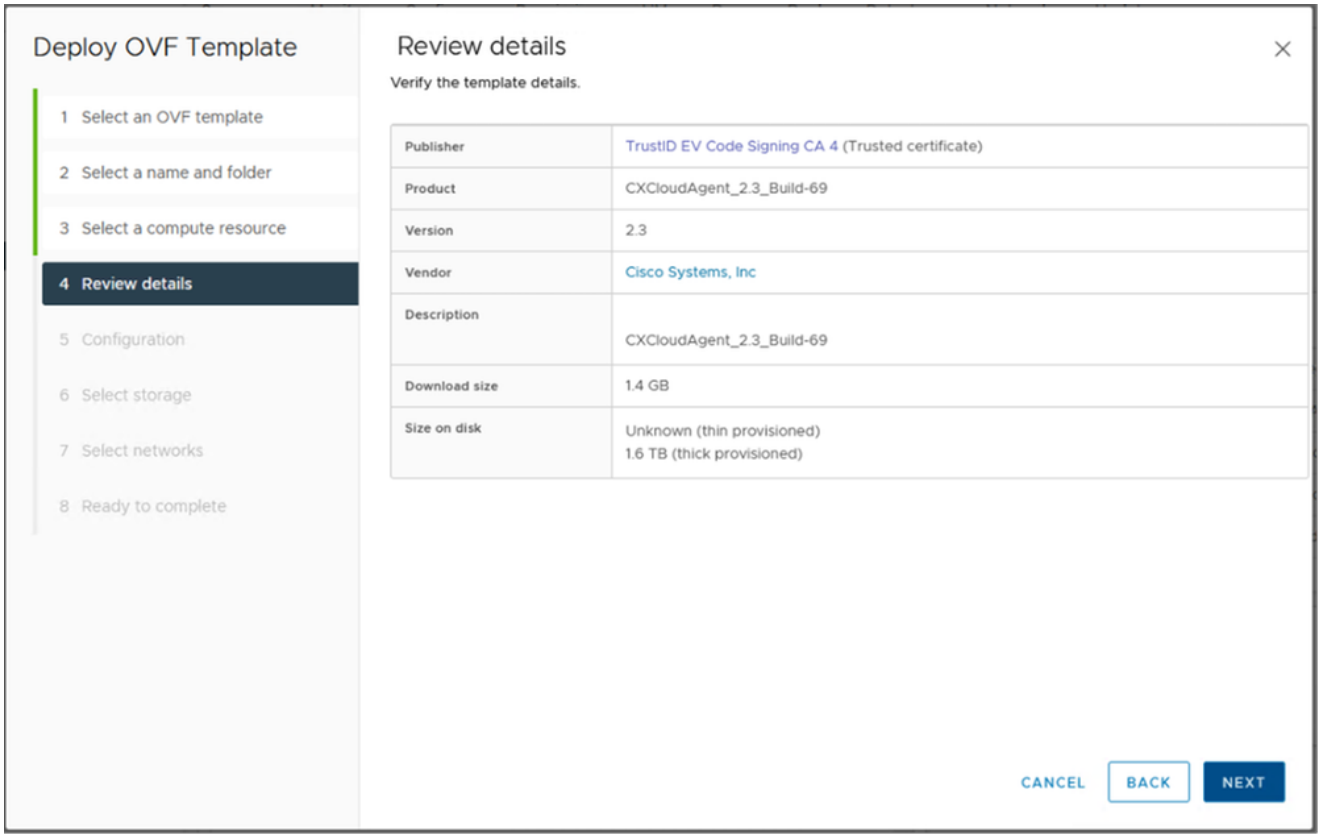
名称和文件夹

6. 输入唯一的名称，并在需要时浏览到该位置。
7. 单击 Next。



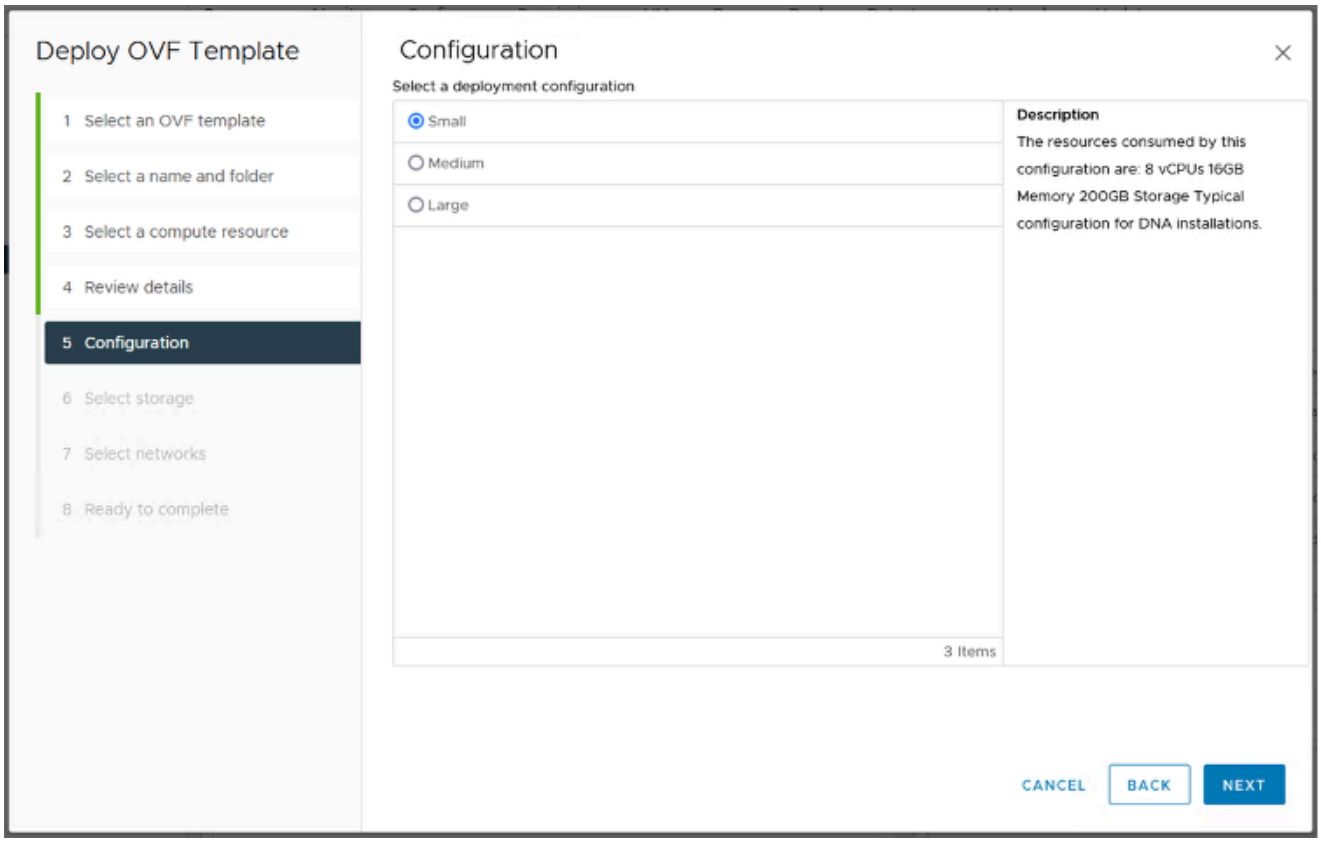
选择计算资源

8. 选择计算资源，然后单击下一步。



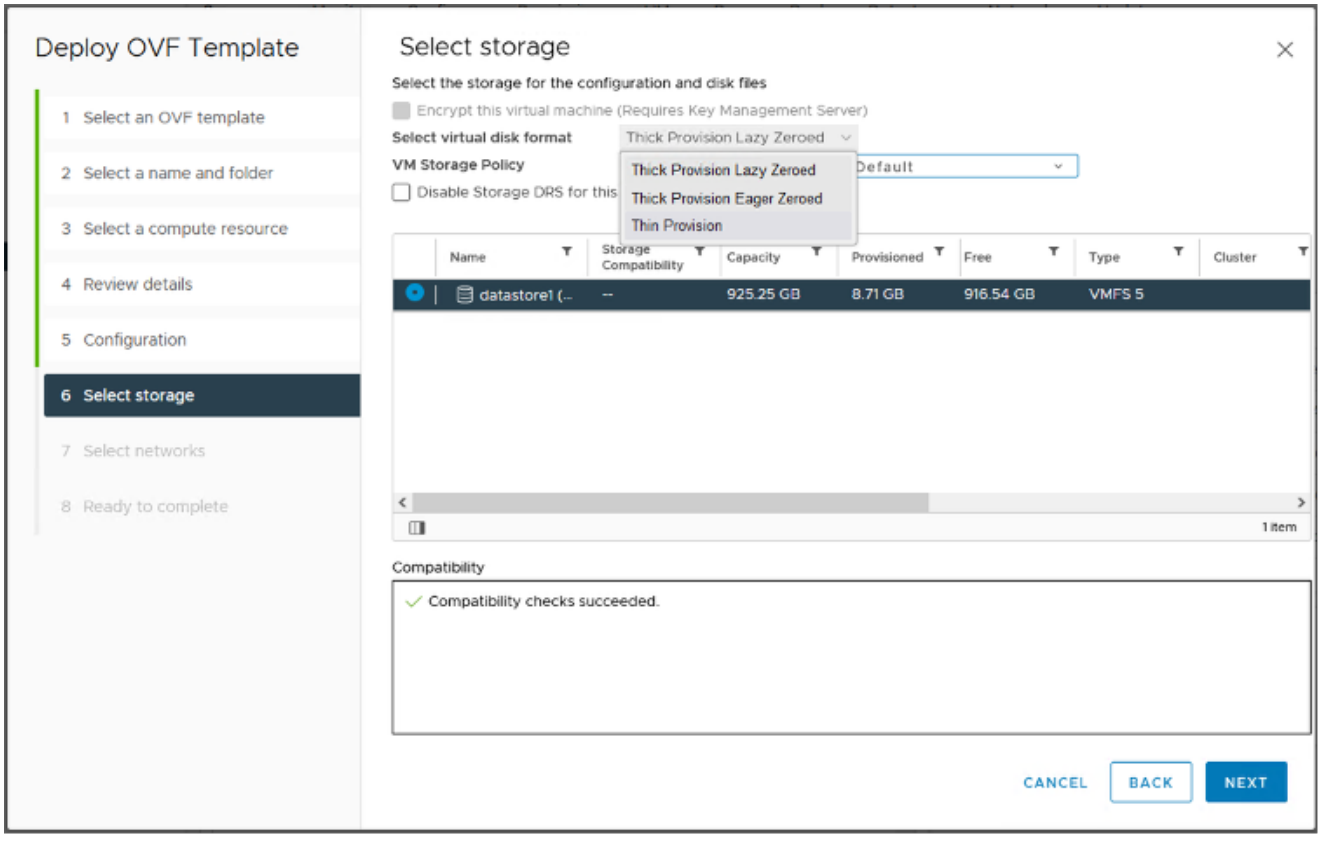
检查详细信息

9. 检查详细信息，然后点击下一步。



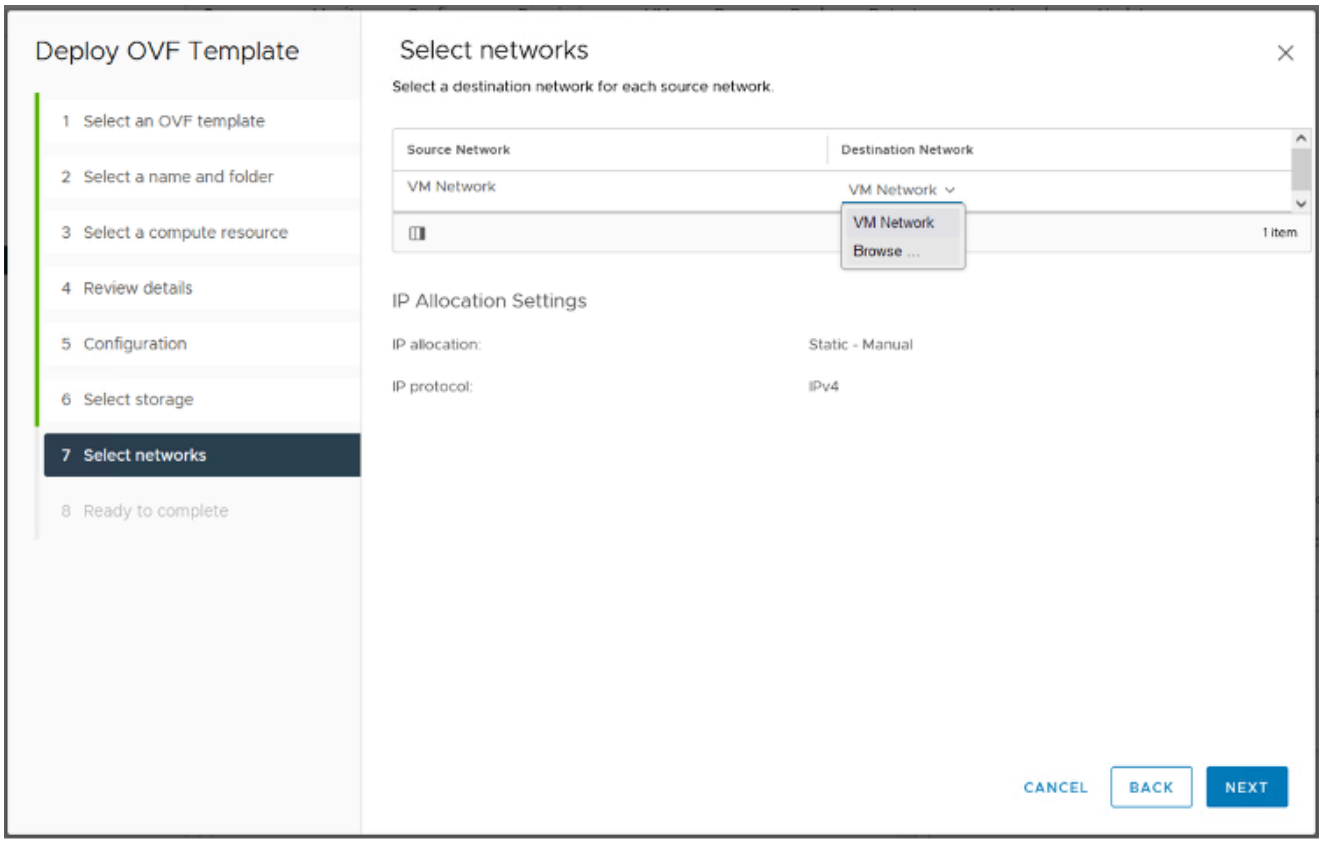
配置

10. 选择部署配置并点击下一步。



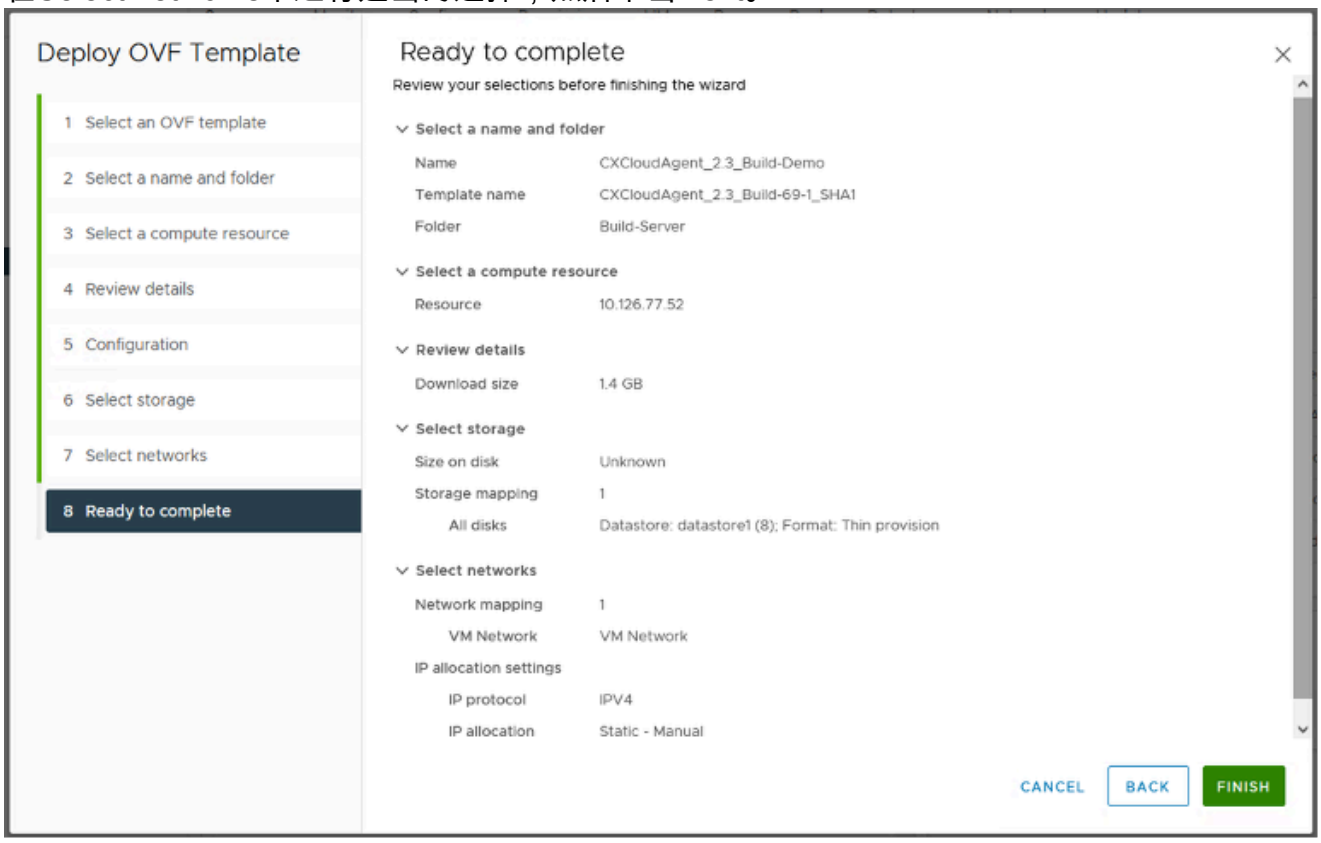
配置

11. 从下拉列表中选择存储> 选择虚拟磁盘格式，然后单击下一步。



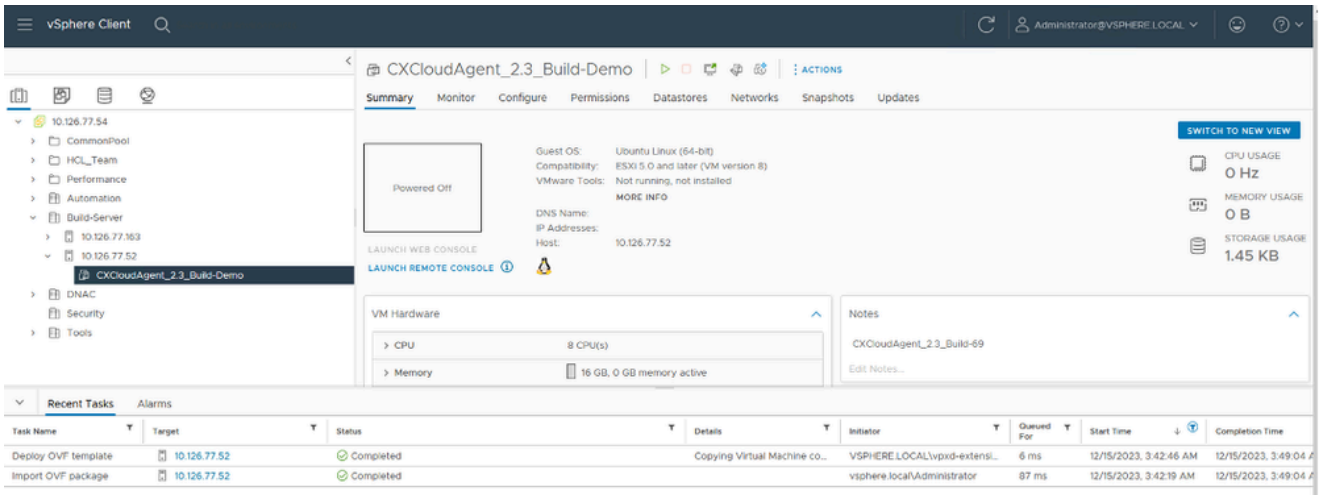
选择网络

12. 在Select networks中进行适当的选择，然后单击Next。



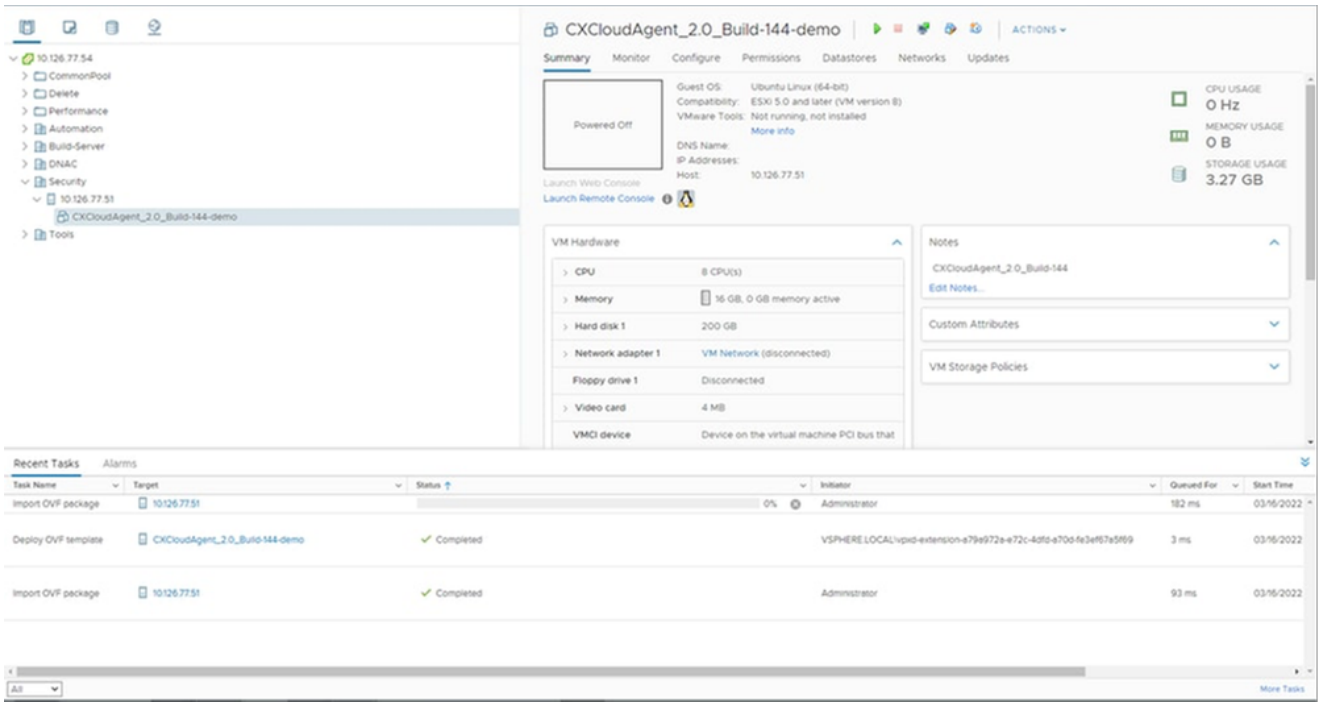
准备完成

13. 查看选择，然后单击Finish。系统随即会显示Home页面。



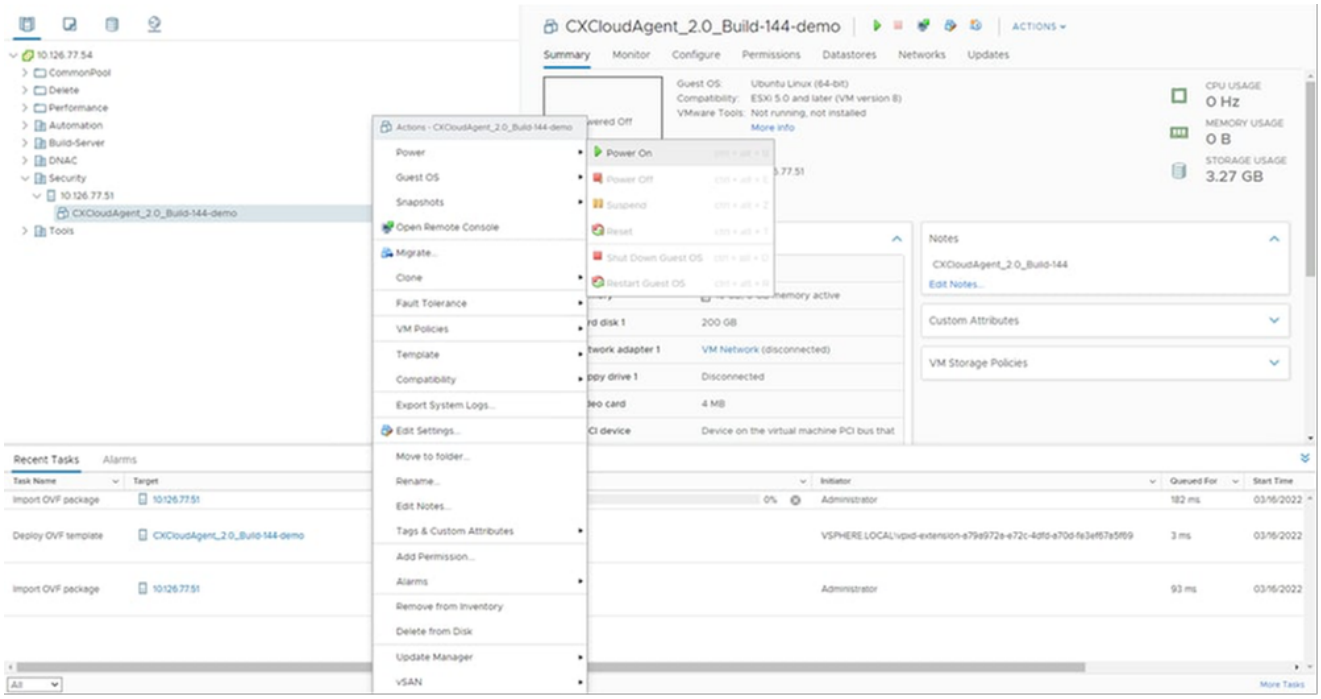
已添加VM

14. 点击随后添加的VM以查看状态。



已添加VM

15. 安装完成后，打开VM并打开控制台。



打开控制台

16. 导航到网络配置以继续执行后续步骤。

Oracle Virtual Box 7.0.12 安装

此客户端通过Oracle虚拟盒部署CX代理OVA。

1. 将CXCloudAgent_3.1 OVA下载到Windows框中任意文件夹。
2. 使用命令行界面浏览到文件夹。
3. 使用命令tar -xvf D:\CXCloudAgent_3.1_Build-xx.ova解压缩OVA文件。

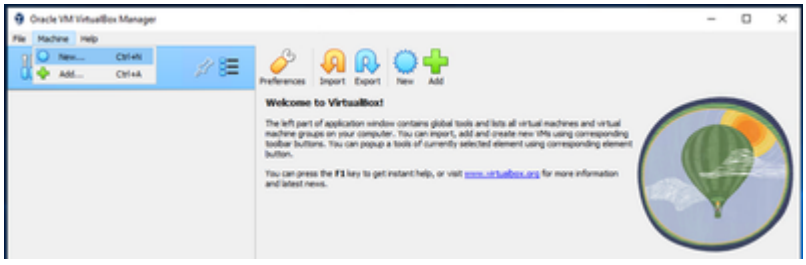
```
D:\>cd CXCAGENT

D:\CXCAGENT>tar -xvf CXCloudAgent_2.3_Build-69-1_SHA1_signed.ova
x CXCloudAgent_2.3_Build-69-1_SHA1.ovf
x CXCloudAgent_2.3_Build-69-1_SHA1.mf
x CXCloudAgent_2.3_Build-69-1_SHA1.cert
x CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk

D:\CXCAGENT>_
```

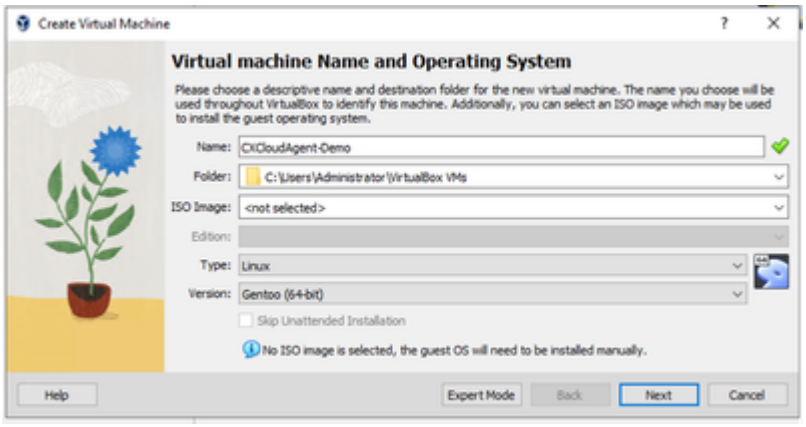
解压缩OVA文件

4. 打开Oracle VM UI。



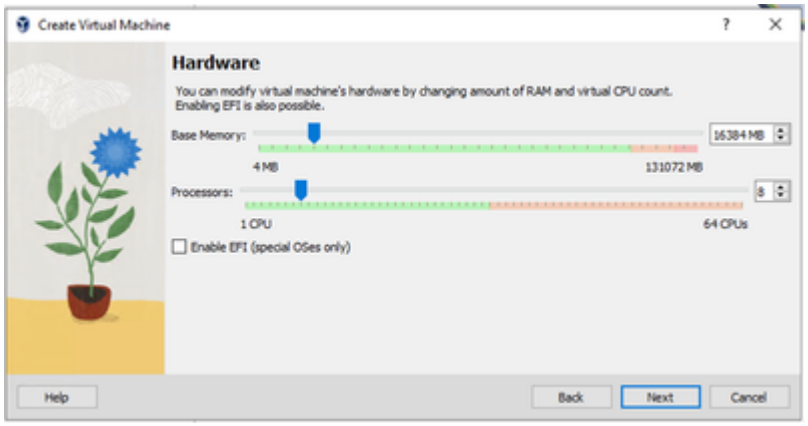
Oracle VM

5. 从菜单中选择Machine>New。Create Virtual Machine窗口打开。



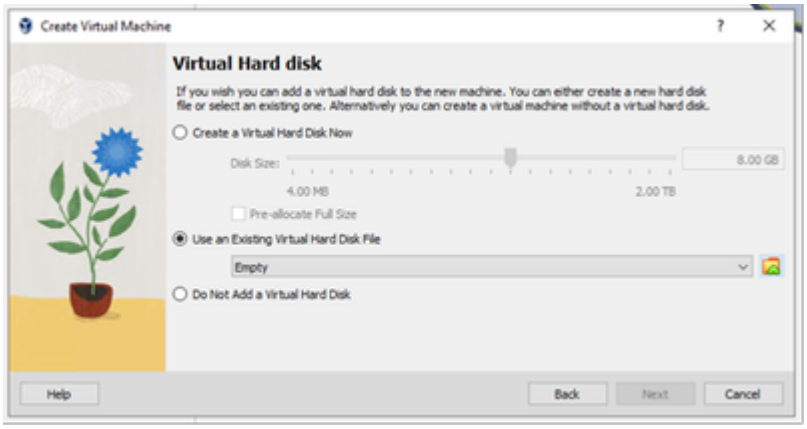
创建虚拟机

6. 在虚拟机名称和操作系统窗口中输入以下详细信息。
   名称：VM名称
   文件夹:要存储VM数据的位置
   ISO映像:none
   type：Linux
   版本:Gentoo（64位）
7. 单击 Next。Hardware窗口打开。



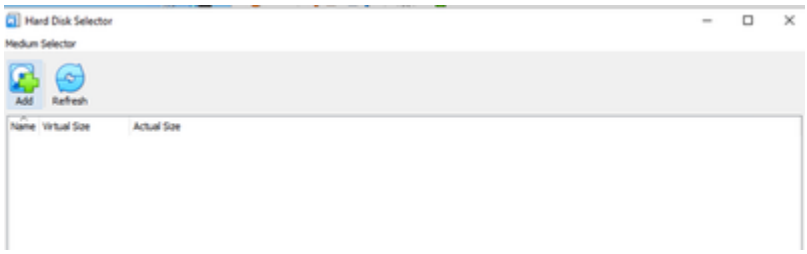
Hardware

8. 输入Base Memory(16384 MB)和Processors(8 CPU)，然后单击Next。Virtual Hard Disk窗口打开。



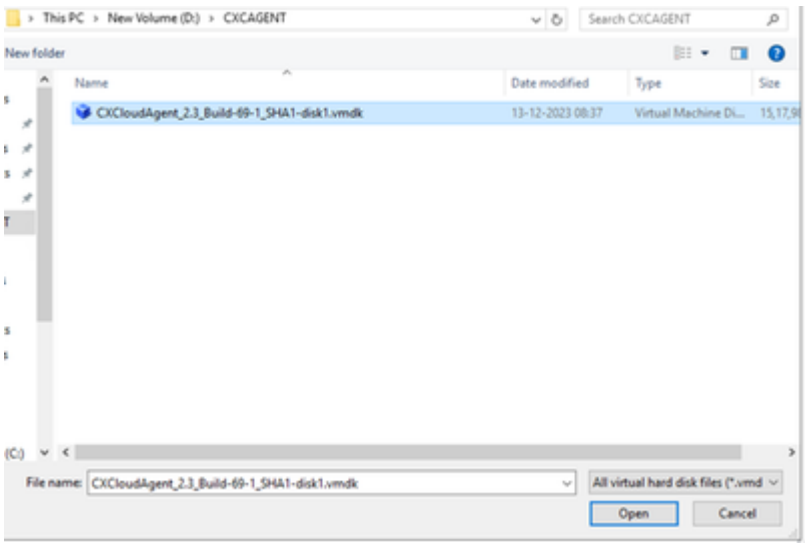
虚拟硬盘

9. 选择使用现有虚拟硬盘文件单选按钮，然后选择浏览图标。Hard Disk Selector窗口打开。



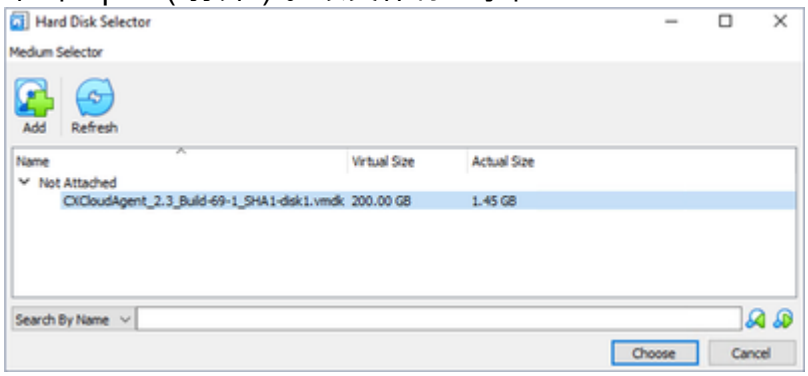
硬盘选择器

10. 浏览到OVA文件夹并选择VMDK文件。



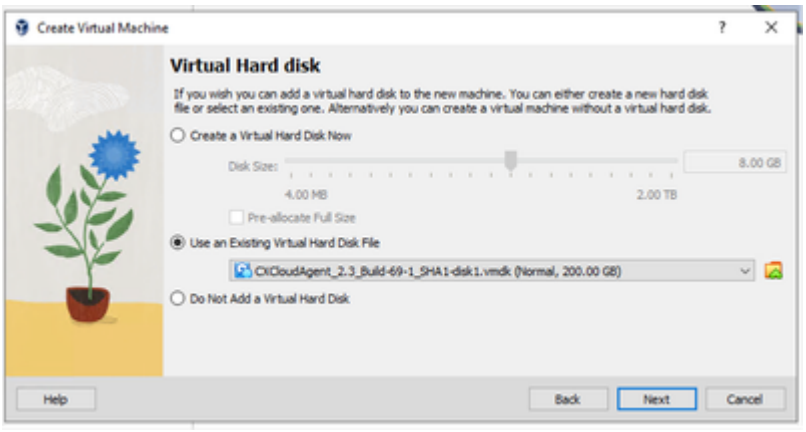
OVA文件夹

11. 单击 Open（打开）。该文件将显示在Hardware Disk Selector窗口中。



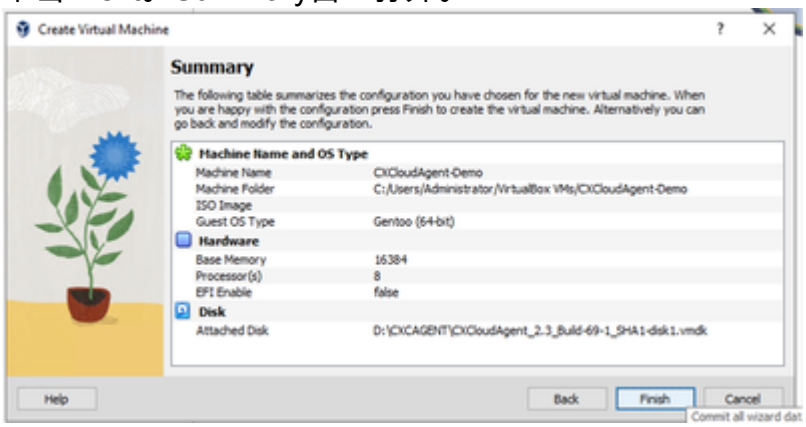
硬盘选择器

12. 单击选择。Virtual Hard Disk窗口打开。确认已选中显示的选项。



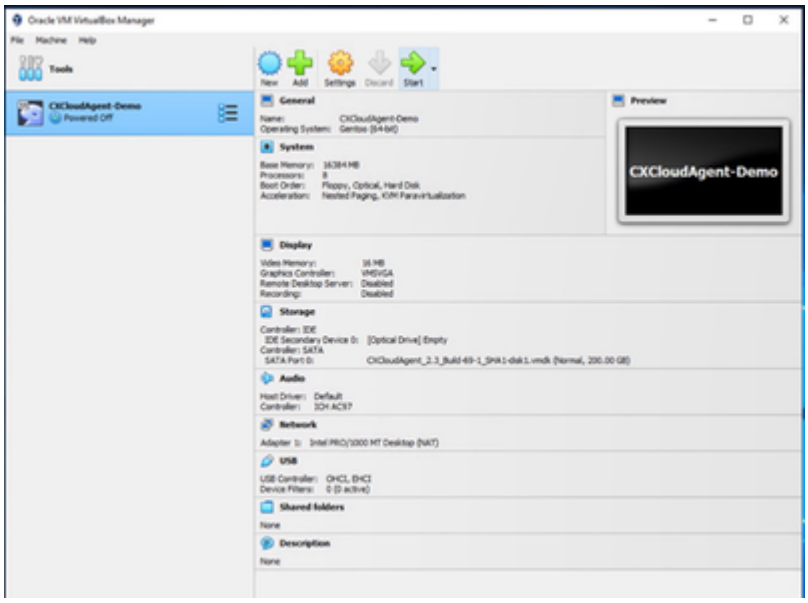
选择文件

13. 单击 Next。Summary窗口打开。



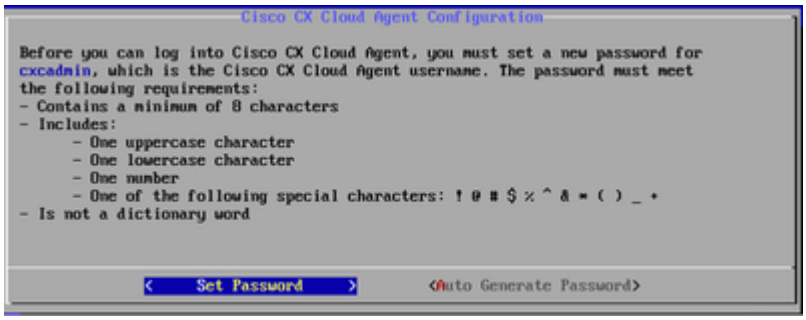
摘要

14. 单击 完成。



VM 控制台启动

15. 选择已部署的VM，然后单击Start。VM通电并显示控制台屏幕进行设置。



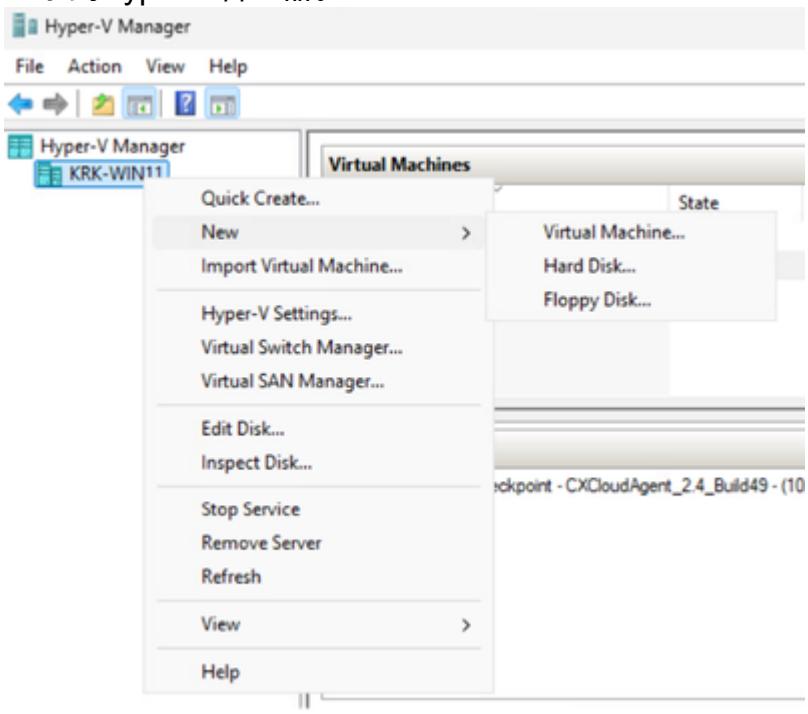
打开控制台

16. 导航到网络配置以继续执行后续步骤。

Microsoft Hyper-V 安装

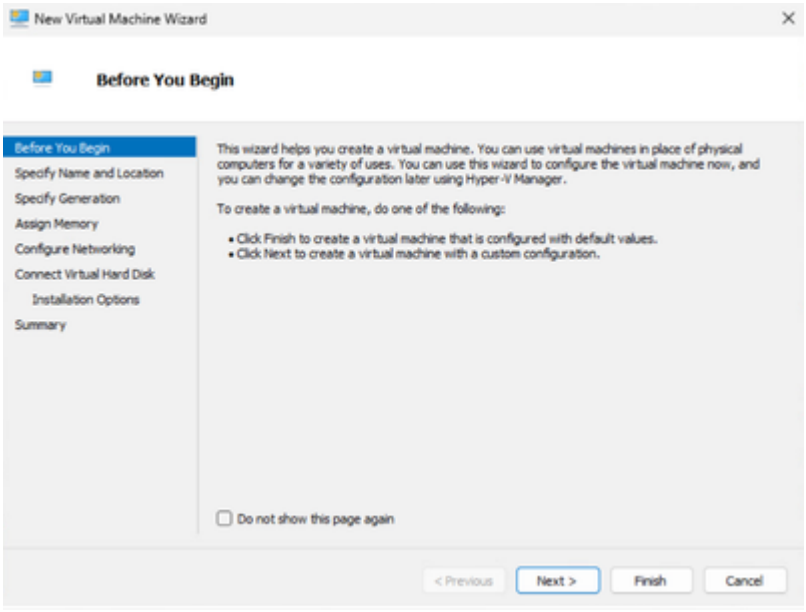
此客户端通过Microsoft Hyper-V安装部署CX代理虚拟磁盘。

1. 登录到Hyper-V管理器。



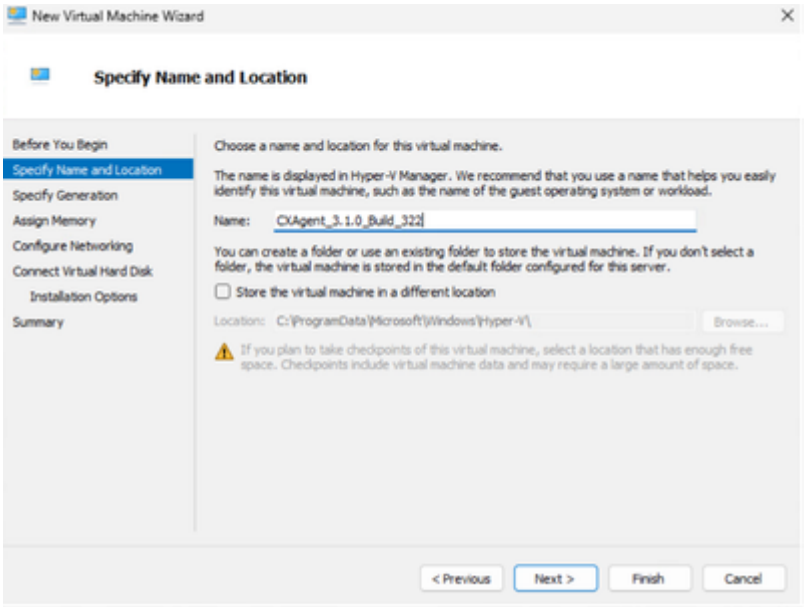
Hyper-V 管理器

2. 右键单击目标VM以打开菜单。
3. 选择New > Virtual Machine。此时将显示New Virtual Machine Wizard - Before You Begin页。



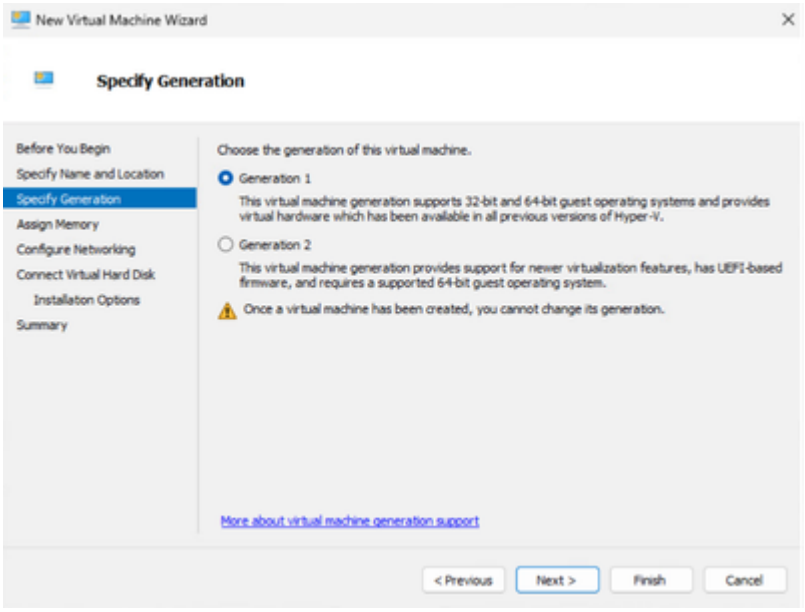
新建虚拟机向导

4. 单击 Next。系统随即会显示“新建虚拟机向导 — 指定名称和位置”页面。



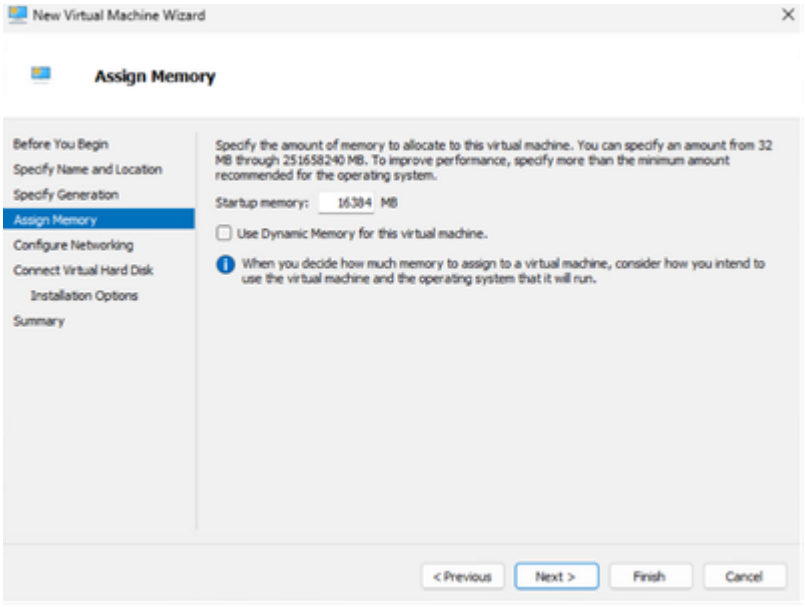
名称和位置

5. 输入Name和location。
6. 单击 Next。系统随即会显示新建虚拟机向导 — 指定生成页面。



指定生成

7. 单击Generation 1单选按钮。
8. 单击 Next。系统将显示“新建虚拟机向导 — 分配内存”页。

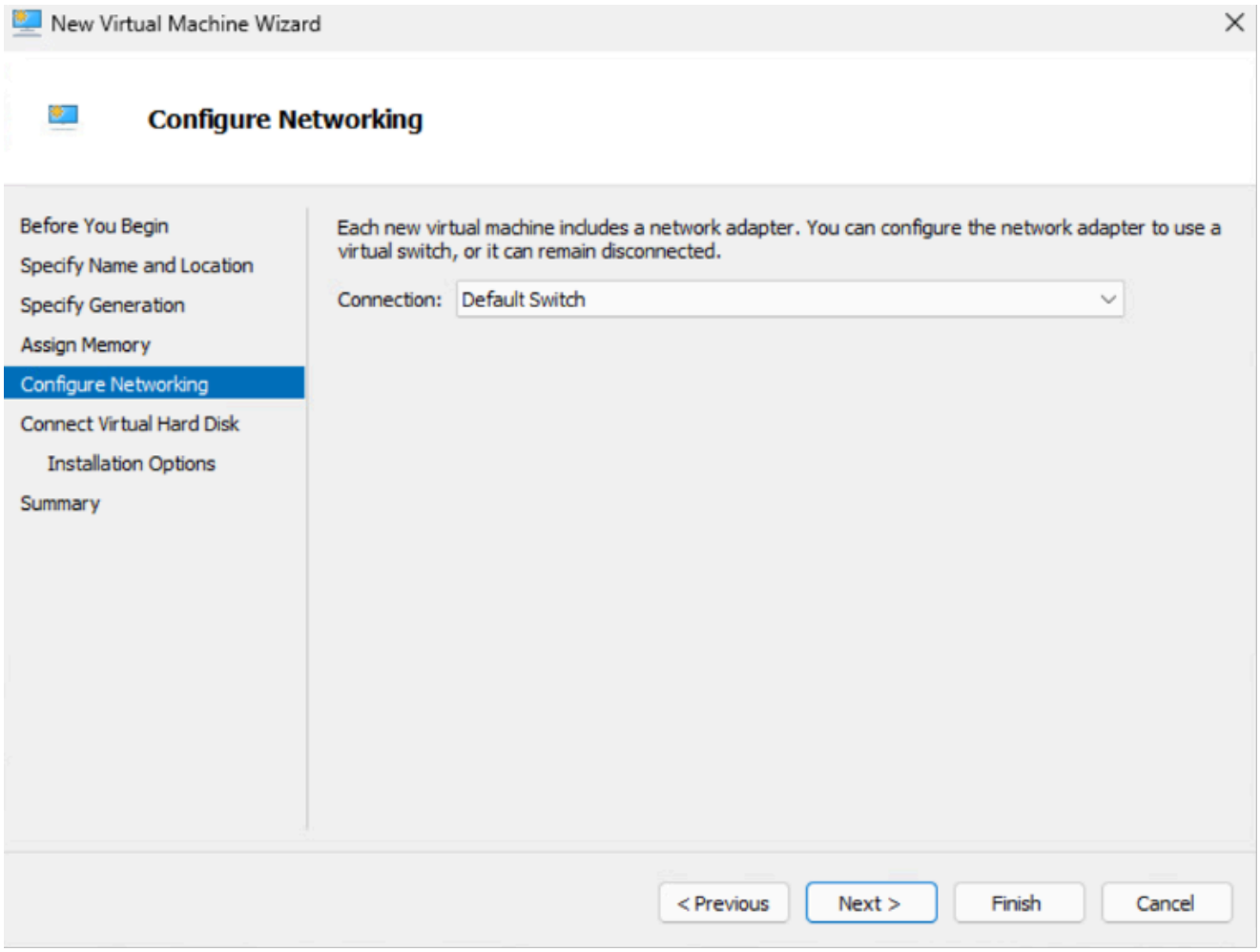


内存

9. 在Startup memory字段中输入所需的RAM大小。
   - 16 GB用于小型部署
   - 32GB用于中型部署
   - 64 GB用于大型部署

   > 注意：
   > — 对于CX代理，分配的最小内存必须至少为16 GB。
   > — 不应选中Use Dynamic Memory for this virtual machine复选框。

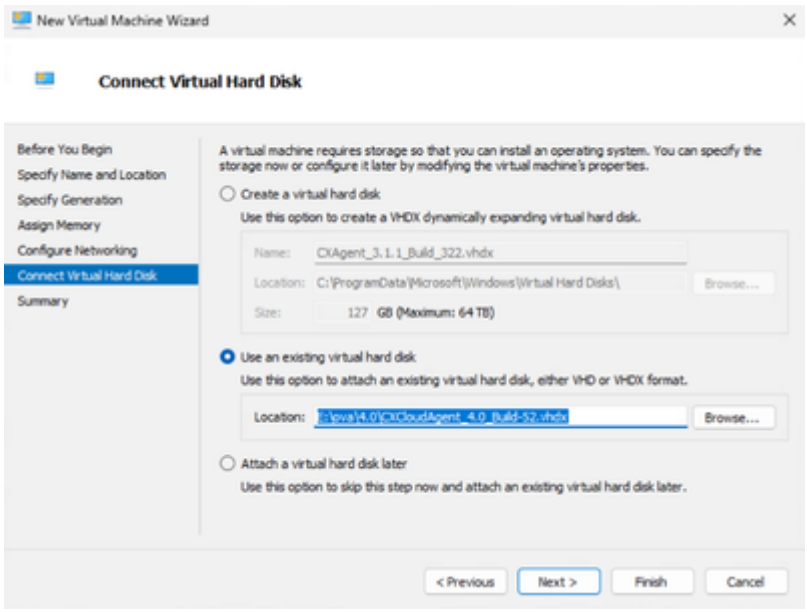
10. 单击 Next。系统随即会显示新建虚拟机向导 — 配置网络页面。



网络

11. 从连接下拉列表中，选择用于网络连接的虚拟交换机。
12. 单击 Next。系统随即会显示New Virtual Machine Wizard - Connect Virtual Hard Disk页面。

注：默认情况下会选择“使用现有虚拟磁盘”。请勿进行任何更改。



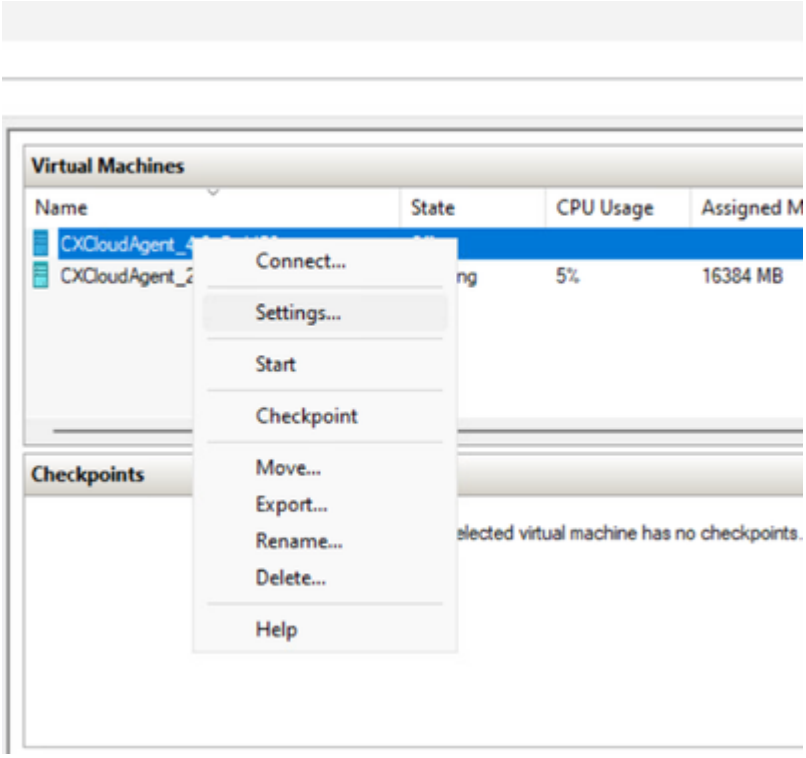
连接虚拟硬盘

13. 查看Summary，然后单击Finish。

处理器设置

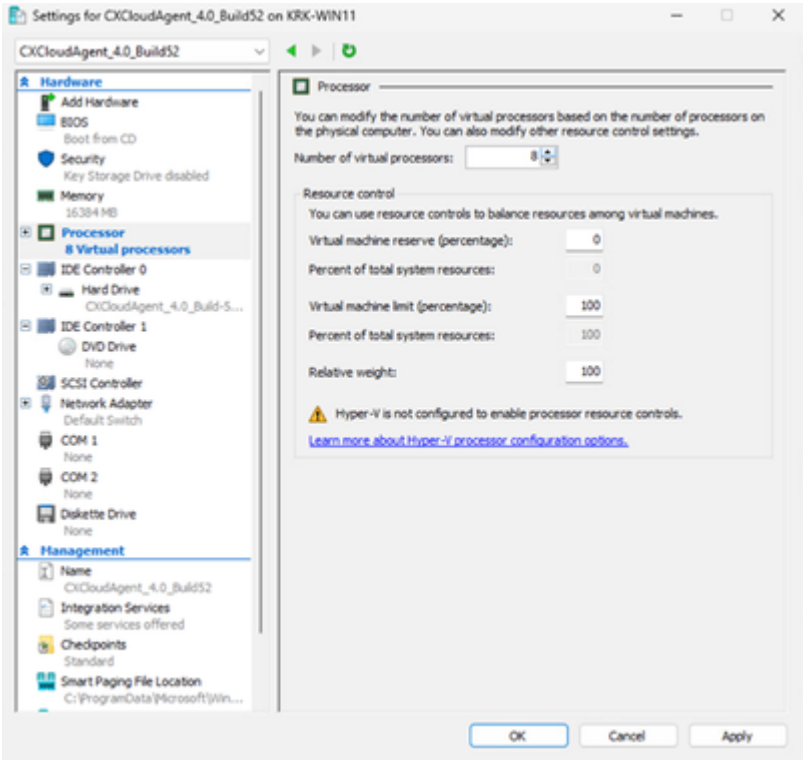
要验证处理器设置，请执行以下操作：

1. 右键单击新创建的虚拟机（如上部分所示）。 系统随即会显示菜单。

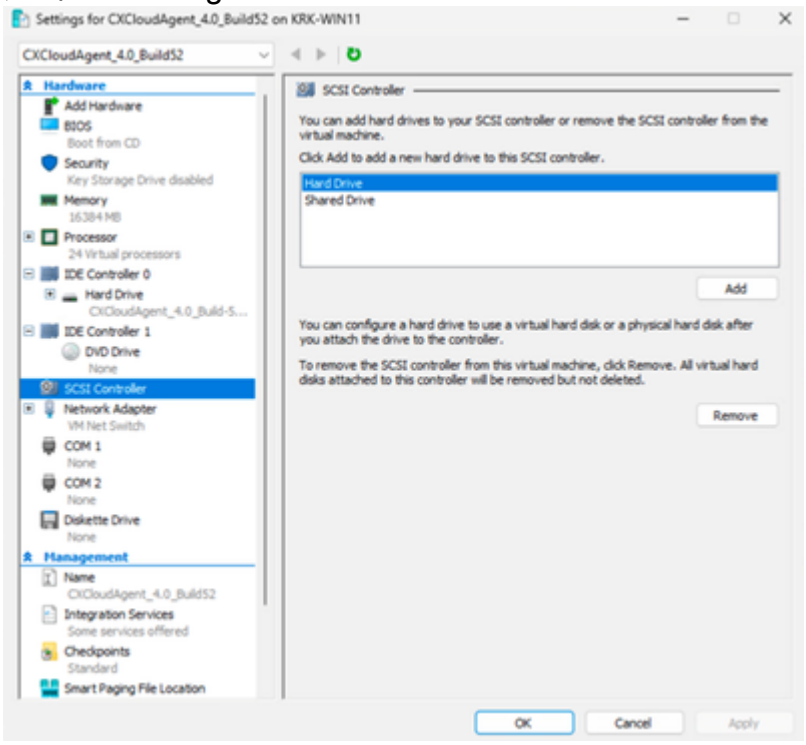


VM设置

2. 选择 Settings。
3. 在Hardware窗格中单击Processor。



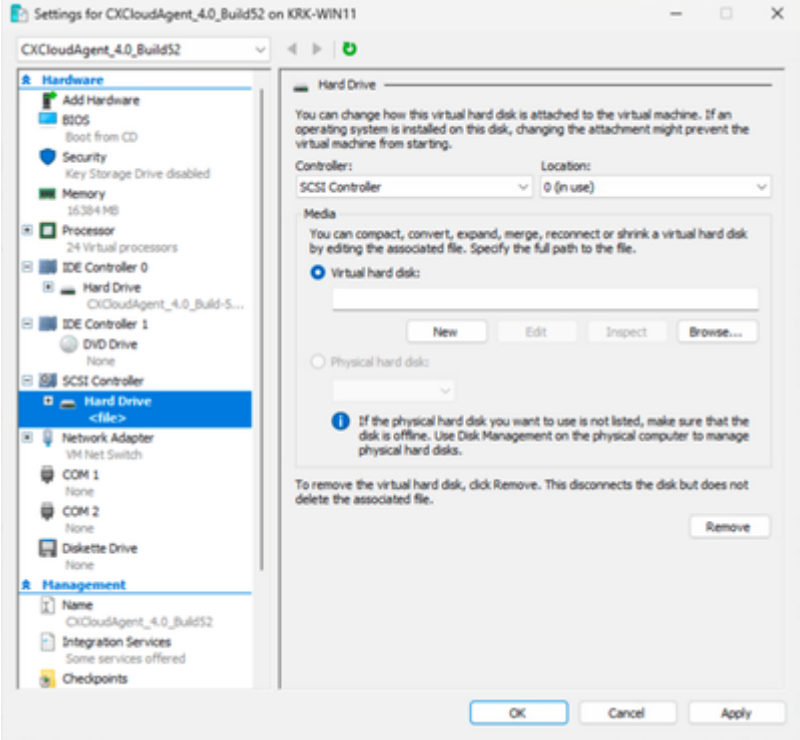
4. 按如下所列，更新Number of virtual processors字段：
    - 小型部署：8
    - 中型部署：16
    - 大型部署：最少 32 根
5. 单击 Apply。
6. Click OK.
7. 如果创建CX Agent的中或大型部署，请更新存储设置。要更新，请执行以下操作：
    1. 点击VM Settings。



SCSI控制器

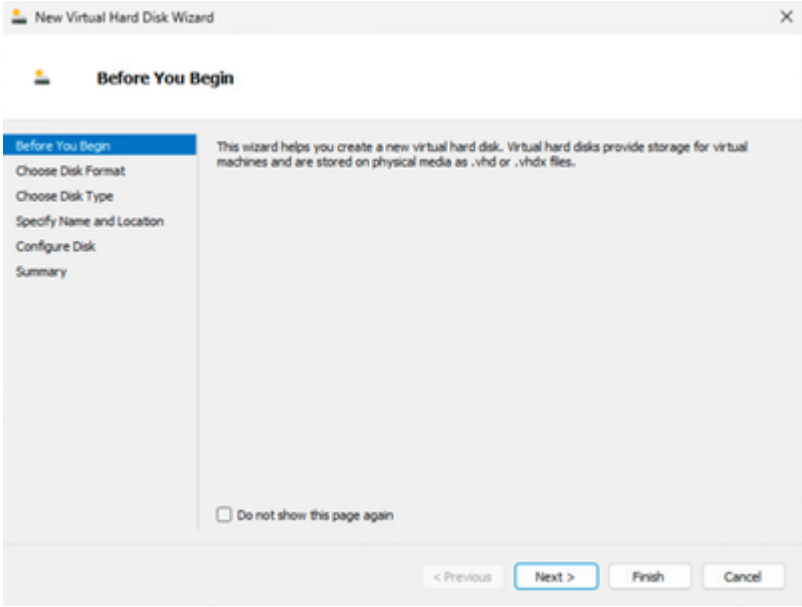
    2. 单击SCSI控制器部分。

3. 选中Hard Drive选项，然后单击Add。



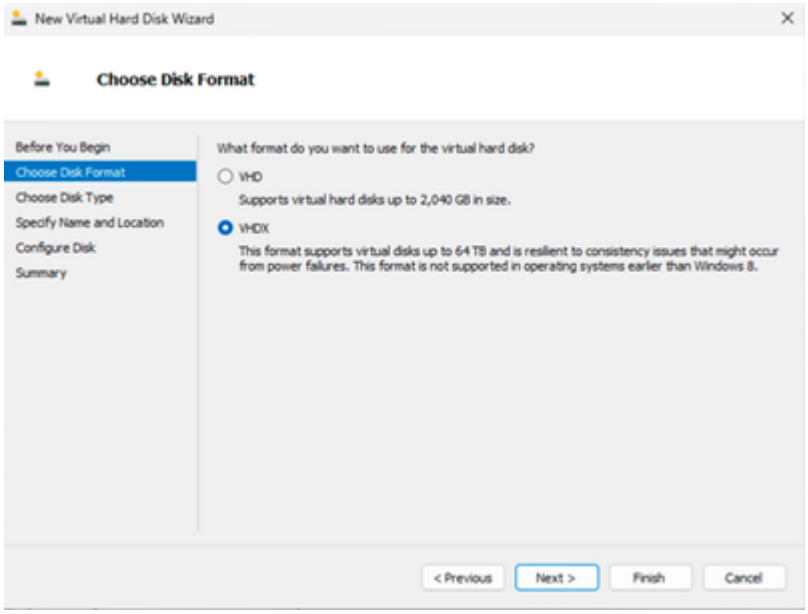
硬盘

4. 单击Media中的New。将打开“新建虚拟硬盘”向导。



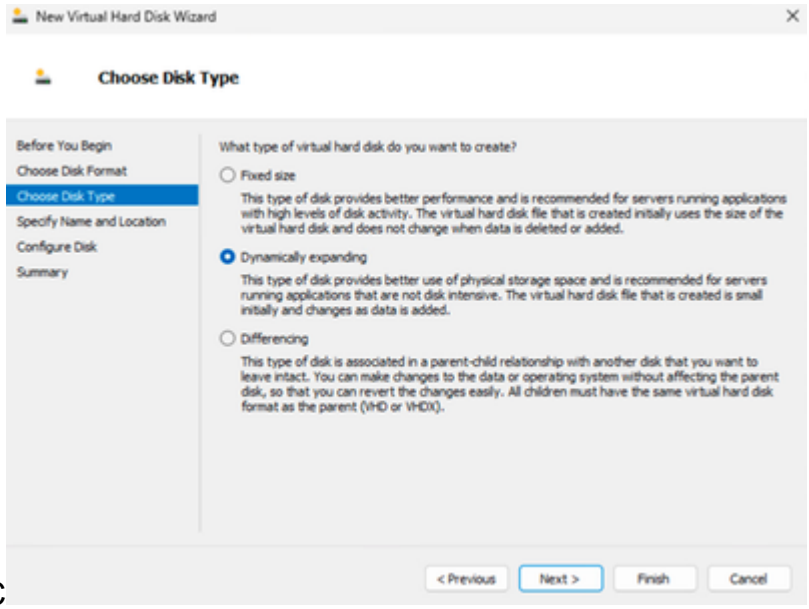
新建硬盘向导

5. 单击 Next。系统随即会显示“选择磁盘格式”页面。



选择磁盘格式

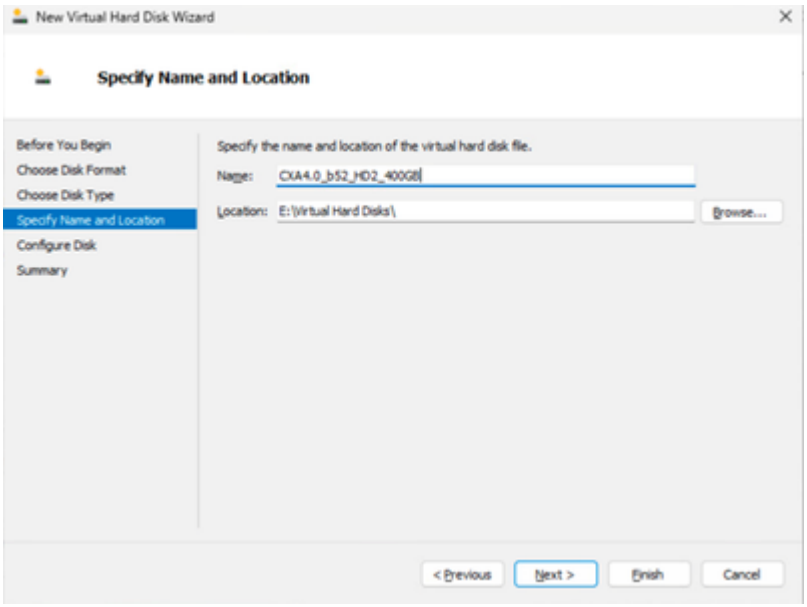
6. 单击VHDX单选按钮以选择磁盘格式。
7. 单击 Next。系统随即会显示选择磁盘类型页面。



C

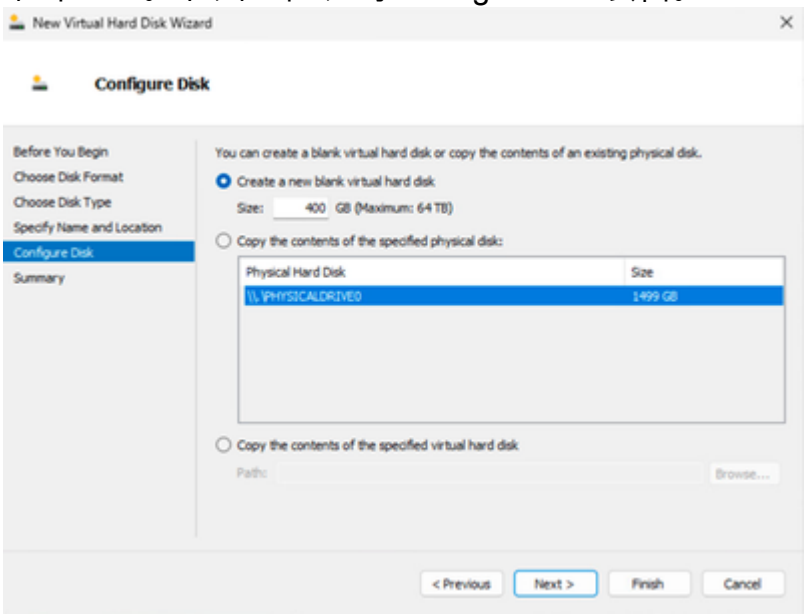
选择磁盘类型

8. 单击动态展开单选按钮。
9. 单击 Next。系统随即会显示指定名称和位置页面。



指定名称和位置

10. 输入磁盘名称和位置。
11. 单击 Next。系统随即会显示Configure Disk页面。



配置磁盘

12. 按照以下建议输入新磁盘的大小：
    - 中型部署：400 GB
    - 大型部署：1000 GB
13. 单击 完成。Hyper-V VM已准备好使用并且可以启动。

8. 请参阅网络配置继续执行后续步骤。

Microsoft Hyper-V映像签名验证

为了确保Microsoft Hyper-V映像的完整性和真实性，将签名验证作为安全流程的一部分来执行。

先决条件

- 能够通过命令行界面运行OpenSSL命令
- 能够通过命令行界面运行grep命令
- Cisco提供的用于签名验证的图像
- 思科签名的x.509终端实体证书，其中包含用于签名验证的公钥；此证书由受思科根CA信任的思科从属CA颁发
- 为映像生成的签名
- 验证3级x.509证书链和签名所需的签名验证程序；首先验证证书链，包括终端实体证书和公认subCA和rootCA证书，然后从指定的本地目录读取或从PKI网站下载subCA和rootCA;经过身份验证的终端实体证书用于验证签名

运行签名验证包

客户可以验证下载的思科ZIP存档是否已使用思科版本证书签名。运行以下示例中的命令以验证签名。

注意：确保在下面的示例命令中引用了正确的属性。

命令1（从PKI网站下载的sha512签名、Cisco rootCA和subCA示例）：

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent__Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -v
dgst –algo sha512 –failExpiredCerts
```

命令输出

<可能出现的错误消息，某些消息包含UNSAFE_LEGACY_RENEGOTIATION_DISABLED代码字>

正在从https://www.cisco.com/security/pki/certs/csirca4096.cer检索rootCA证书.....

已成功检索并验证csirca4096.cer。

正在从https://www.cisco.com/security/pki/certs/cgsisca4096.cer检索subCA证书.....

已成功检索并验证cgsisca4096.cer。

已成功验证根、子证书和终端实体证书链。

已成功从CX_COLLECTOR_HYPER_REL_CERT.pem获取公钥。

使用CX_COLLECTOR_HYPER_REL_CERT.pem成功验证了CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip的签名

命令2(sha512 signature， Cisco Virtual UEFI rootCA & subCA retrieved from Cisco PKI website example):

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -v
dgst —algo sha512 -failExpiredCerts
```

命令输出

<可能出现的错误消息，某些消息包含UNSAFE_LEGACY_RENEGOTIATION_DISABLED代码字>

正在从https://www.cisco.com/security/pki/certs/vuefirca.cer检索CA证书.....

已成功检索并验证vuefirca.cer。

正在从https://www.cisco.com/security/pki/certs/vuefiscav2.cer检索SubCA证书.....

已成功检索并验证vuefiscav2.cer。

已成功验证根、子证书和终端实体证书链。

已成功从CX_COLLECTOR_HYPER_REL_CERT.pem获取公钥。

使用CX_COLLECTOR_HYPER_REL_CERT.pem成功验证了CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip的签名

命令3（本地Cisco rootCA和subCA示例）

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -c
/cert/store -v dgst —algo sha512 -failExpiredCerts
```

命令输出

使用本地提供的rootCA证书/cert/store/vuefirca.cer

使用本地提供的子CA证书/cert/store/vuefiscav2.cer

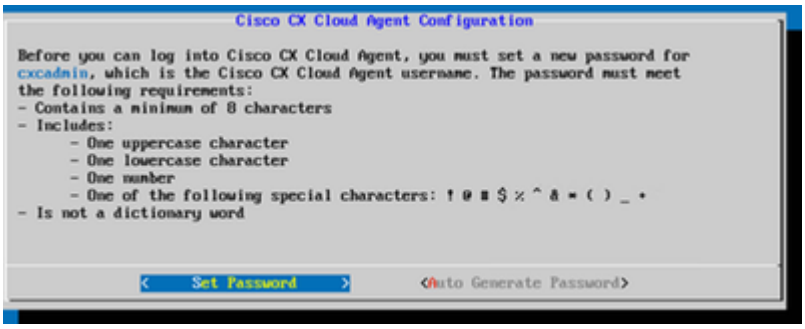
已成功验证根、子证书和终端实体证书链。

已成功从CX_COLLECTOR_HYPER_REL_CERT.pem获取公钥。

使用CX_COLLECTOR_HYPER_REL_CERT.pem成功验证了CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip的签名

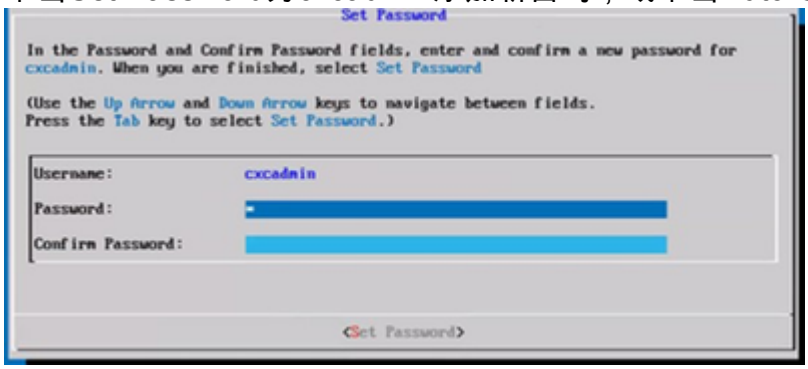
网络配置

要为cxcadmin用户名设置CX云代理密码：



设置密码

1. 单击Set Password为cxcadmin添加新密码，或单击Auto Generate Password以获取新密码。



新密码

2. 如果选择设置密码，请输入 cxcadmin 的密码并确认。点击设置密码并转到步骤 3。
或者

   如果选择Auto Generate Password，请复制生成的密码并将其存储起来供将来使用。点击保存密码并转至步骤 4。

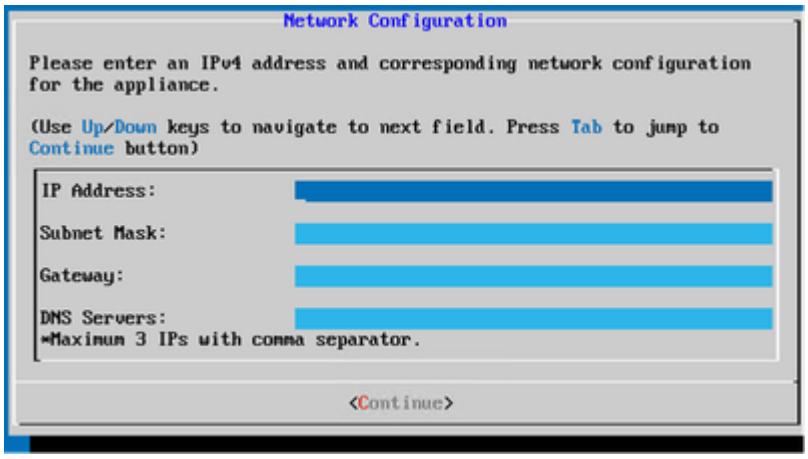


自动生成的密码



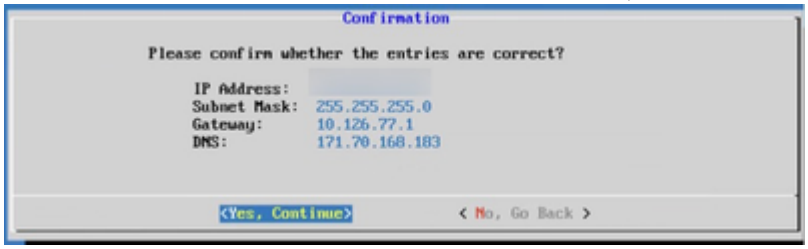
保存密码

3. 点击保存密码以将其用于身份验证。



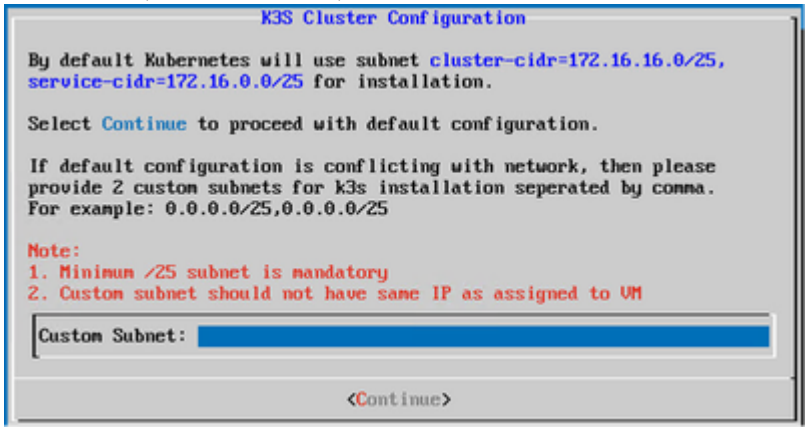
网络配置

4. 输入IP地址、子网掩码、网关和DNS服务器，然后单击继续。



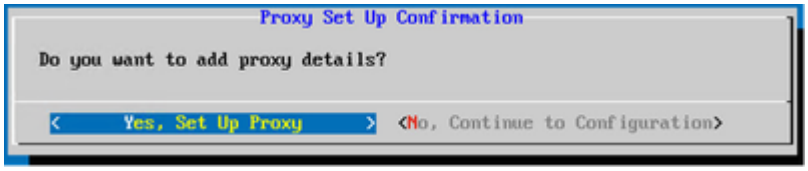
确认

5. 确认输入，然后点击是， 继续。



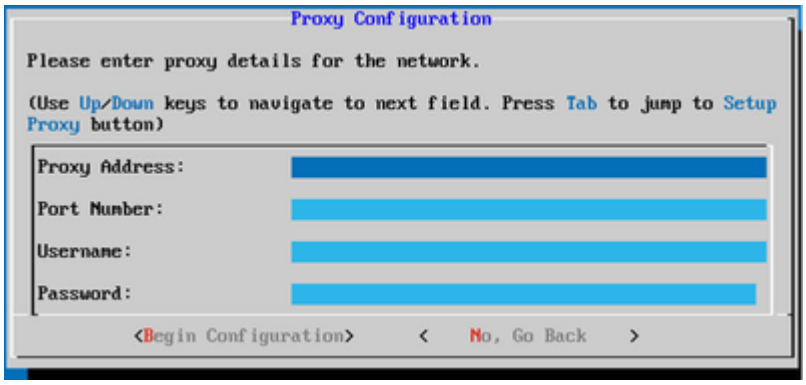
自定义子网

6. 为K3S集群配置输入自定义子网IP（如果客户的默认子网与其设备网络冲突，请选择另一个自定义子网）。
7. 单击 Continue。



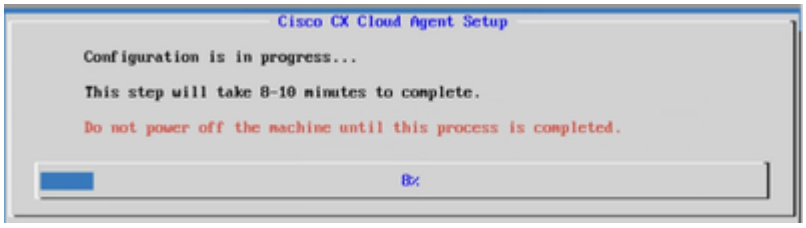
代理设置

8. 单击Yes， Set Up Proxy以设置代理详细信息，或单击No， Continue to Configuration以直接继续执行步骤11。



代理配置

9. 输入代理地址、端口号、用户名和密码。
10. 点击开始配置。

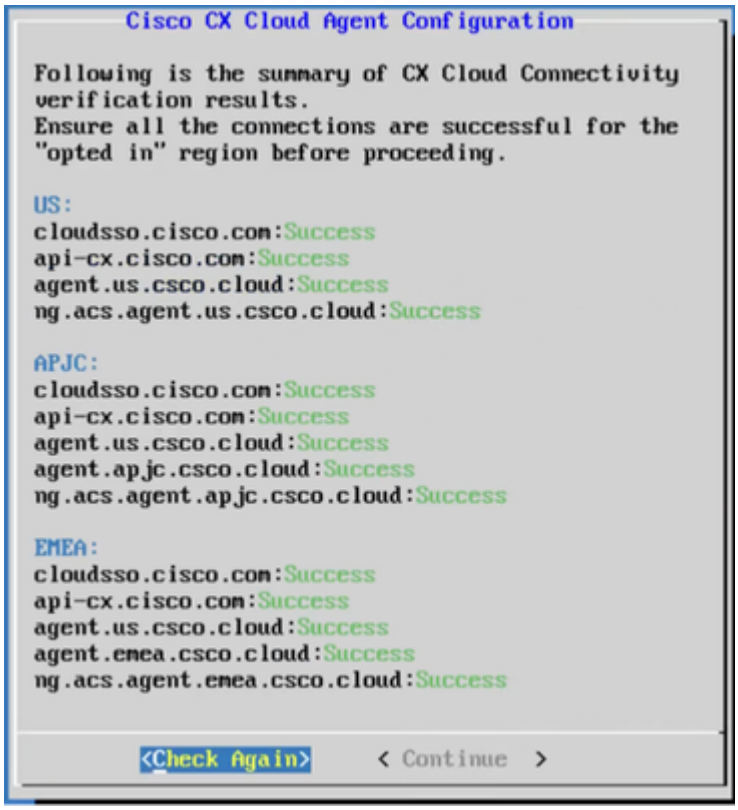


CX云代理设置



CX云代理配置

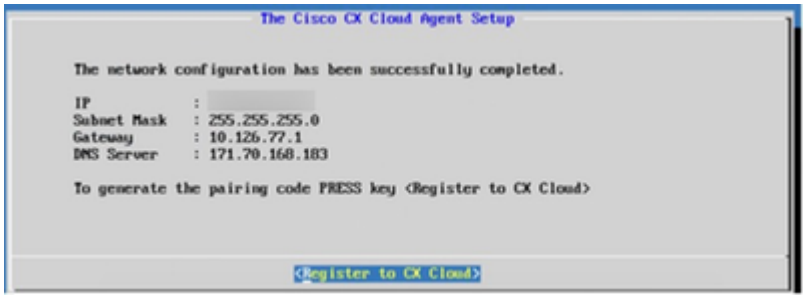
11. 单击 Continue。



继续配置

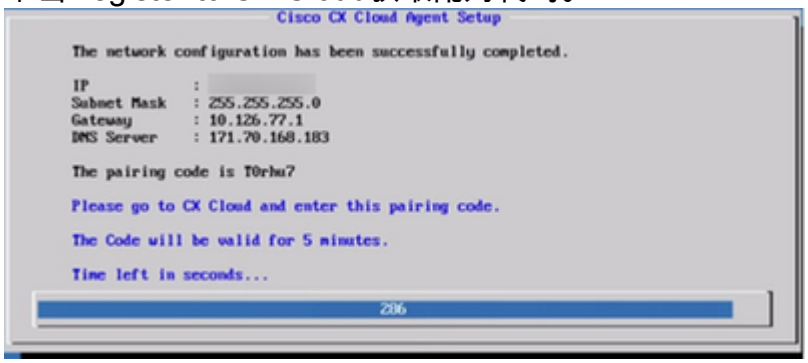
12. 单击Continue继续配置以成功到达域。完成配置可能需要几分钟。

> 注意：如果无法成功访问域，则客户必须通过更改其防火墙来修复域的可达性，以确保域可访问。解决域可达性问题后，单击Check Again。



注册到 CX Cloud

13. 单击Register to CX Cloud获取配对代码。



配对代码

14. 复制配对代码并返回到 CX Cloud 以继续设置。



注册成功

> 注意：如果配对代码过期，请单击Register to CX Cloud以生成新的配对代码（第13步）。

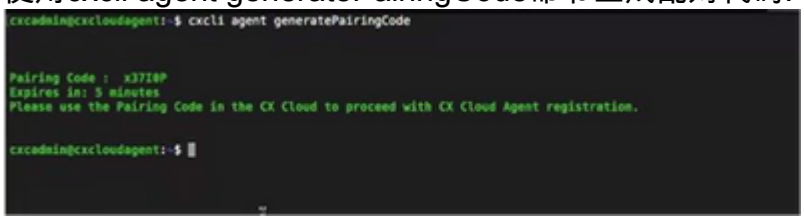
15.单击OK。

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。

使用CLI生成配对代码：

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



生成配对代码 CLI

3. 复制配对代码并返回到 CX Cloud 以继续设置。

配置设备以将系统日志转发到CX云代理

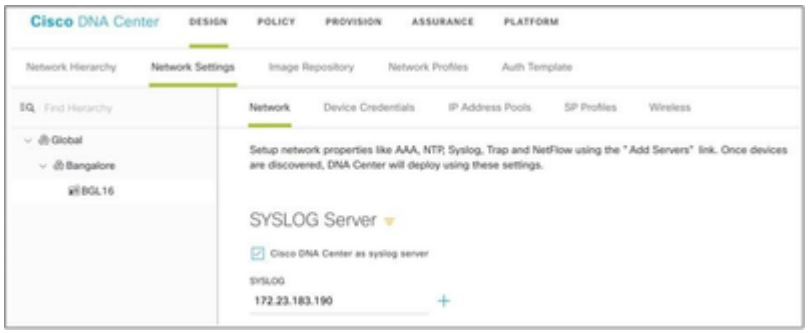
先决条件

支持的Cisco Catalyst Center版本为2.1.2.0到2.2.3.5、2.3.3.4到2.3.3.6、2.3.5.0和Cisco Catalyst Center虚拟设备

配置系统日志转发设置

要在Cisco Catalyst Center中配置到CX代理的系统日志转发，请执行以下步骤：

1. 启动Cisco Catalyst Center。
2. 转至设计 > 网络设置 > 网络。
3. 对于每个站点，添加CX代理IP作为系统日志服务器。



syslog 服务器

注意：配置后，与该站点关联的所有设备都将配置为向CX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后，与该站点关联的所有设备将自动设置为默认关键级别。

配置其他资产（直接设备收集）以将系统日志转发到CX代理

必须配置设备以将系统日志消息发送到CX代理，才能使用CX云的故障管理功能。

注意：CX代理仅将园区成功跟踪第2级资产的系统日志信息报告给CX云。阻止其他资产将其系统日志配置到CX代理，并且不会在CX云中报告其系统日志数据。

具有转发功能的现有系统日志服务器

执行系统日志服务器软件的配置说明，并将CX代理IP地址添加为新目标。

注意：转发系统日志时，请确保保留原始系统日志消息的源IP地址。

没有转发功能的现有系统日志服务器或没有系统日志服务器

将每台设备配置为将系统日志直接发送到CX代理IP地址。有关特定配置步骤，请参阅此文档。

Cisco IOS® XE配置指南

AireOS无线控制器配置指南

启用Cisco Catalyst Center的信息级别系统日志设置

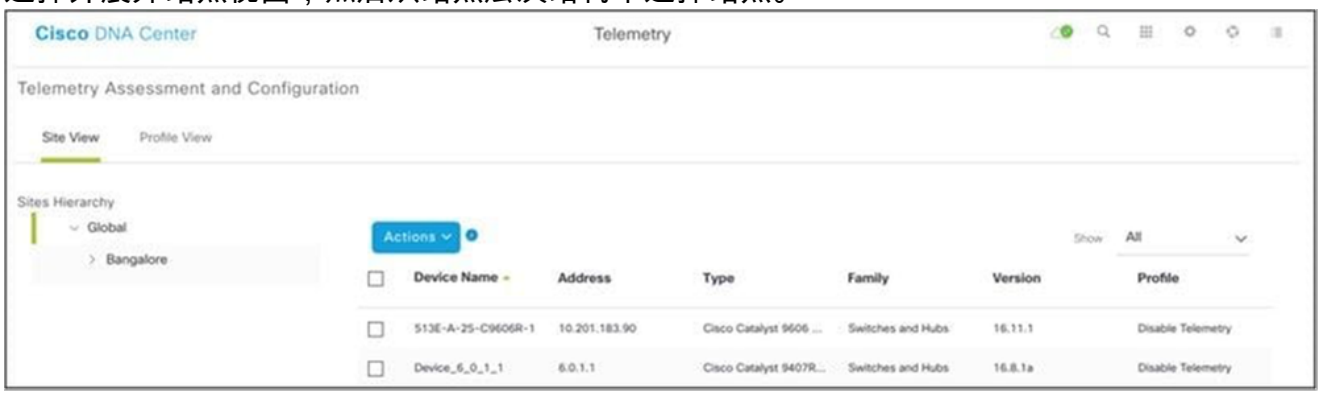
要使系统日志信息级别可见，请执行以下步骤：

1. 导航至工具>遥测。



工具菜单

2. 选择并展开站点视图，然后从站点层次结构中选择站点。



站点视图

3. 选择所需站点并选中使用设备名称复选框的所有设备。

4. 从操作下拉列表中选择最佳可见性。



操作

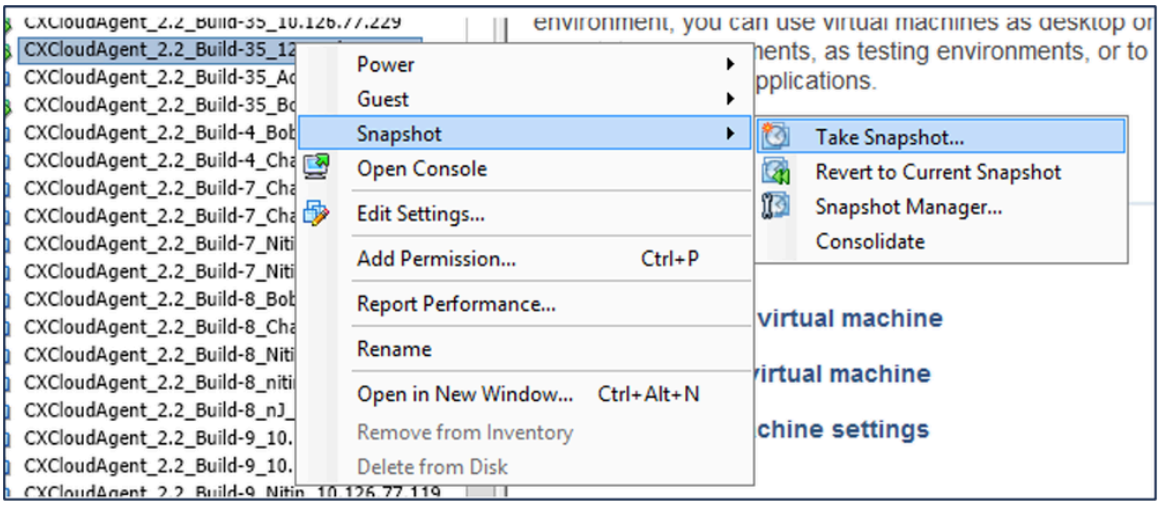
备份和恢复CX云虚拟机

建议使用快照功能在特定时间点保留CX代理VM的状态和数据。此功能有助于将CX云VM恢复到拍摄快照的特定时间。

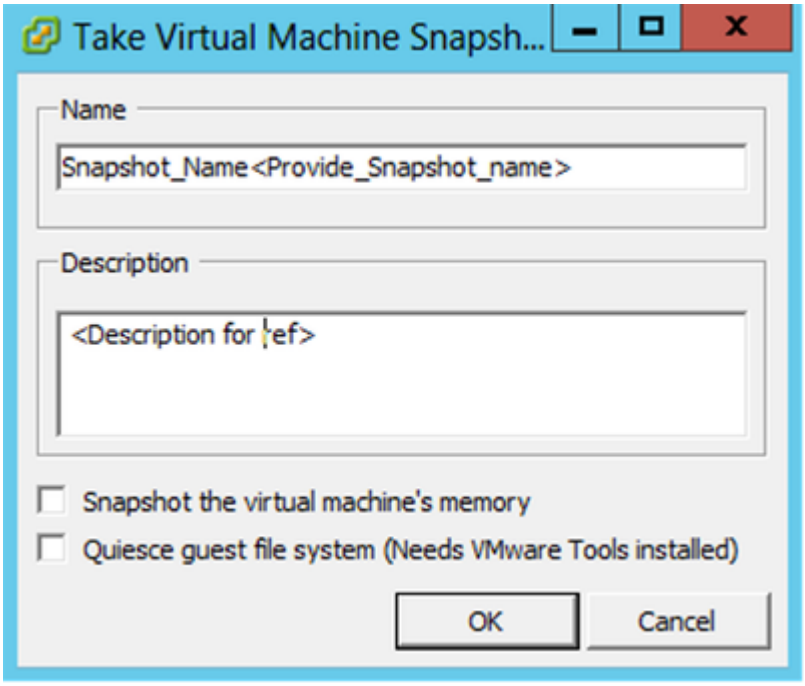
备份CX云虚拟机

要备份CX云虚拟机，请执行以下操作：

1. 右键点击VM，然后选择快照>拍摄快照。Take Virtual Machine Snapshot窗口打开。



选择 VM

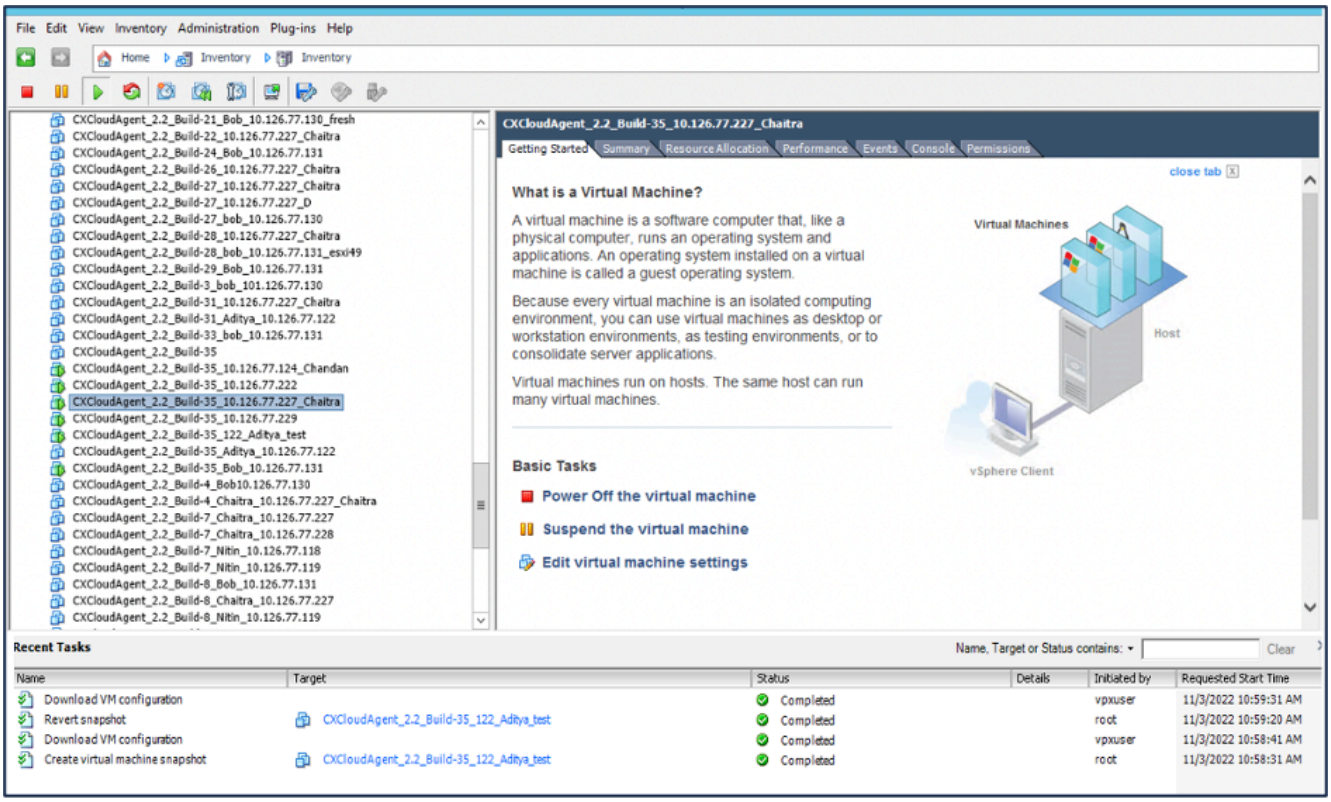


拍摄虚拟机快照

2. 输入名称和说明。

注意：验证是否已清除Snapshot the virtual machine's memory（为虚拟机内存创建快照）复选框。

3.单击确定。创建虚拟机快照状态在"最近的任务"列表中显示为已完成。

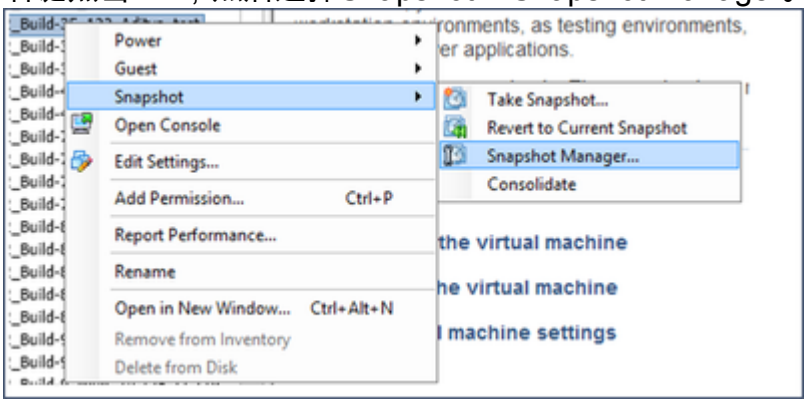


最近的任务

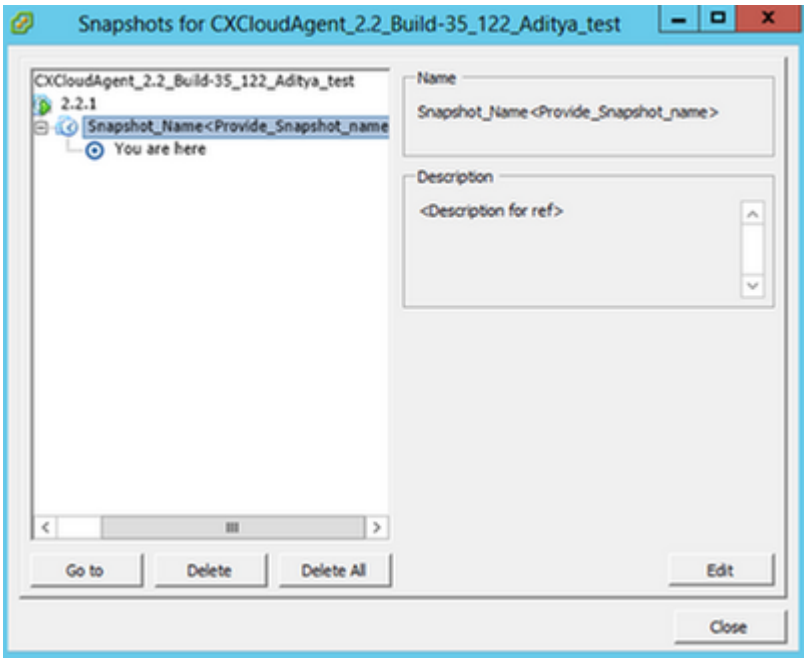
恢复CX云虚拟机

要恢复CX云虚拟机，请执行以下操作：

1. 右键点击VM，然后选择Snapshot > Snapshot Manager。将打开VM的快照窗口。

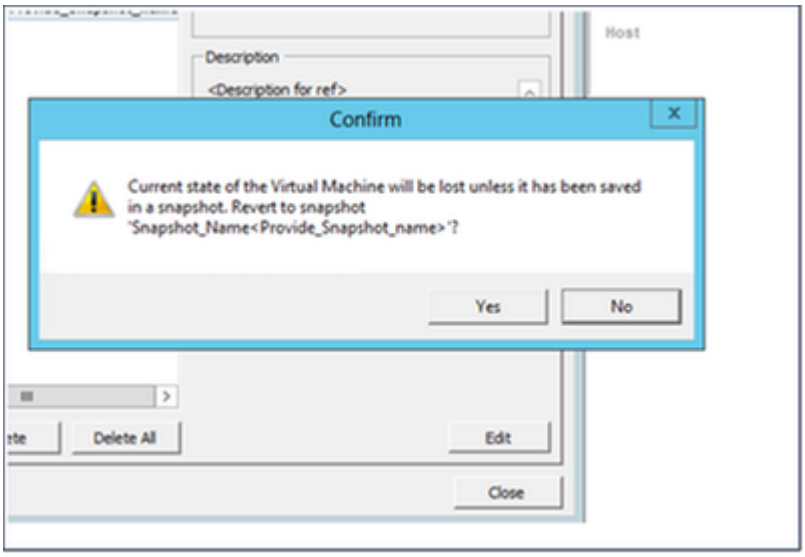


选择VM窗口



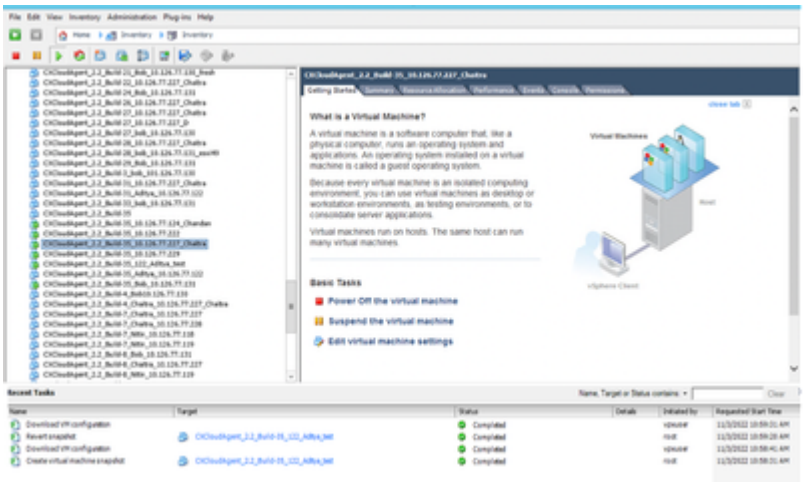
Snapshots窗口

2. 单击Go to。Confirm窗口打开。



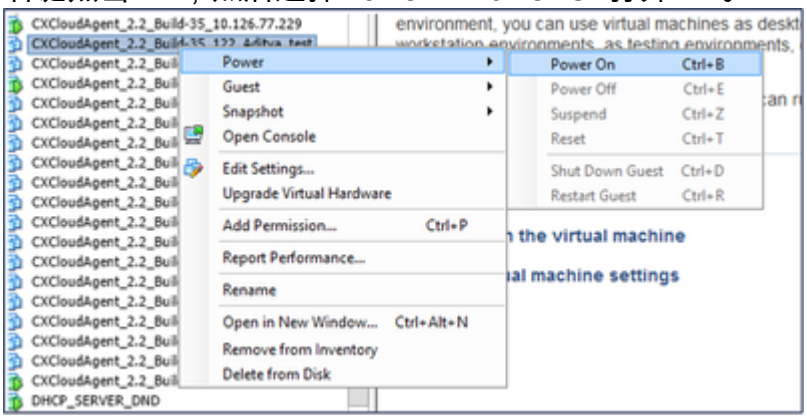
确认窗口

3. 单击 Yes。Revert snapshot状态在“Recent Tasks”列表中显示为Completed。



最近的任务

4. 右键点击VM，然后选择Power > Power On打开VM。



安全

CX代理可确保客户获得端到端安全性。CX云和CX代理之间的连接是TLS安全的。云代理的默认SSH用户仅限于执行基本操作。

物理安全

在安全的VMware服务器公司中部署CX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。用户必须参考此FAQ才能设置此引导加载程序（单用户模式）密码。

账户安全

在部署过程中，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代理API和通过SSH连接到设备。

cxcadmin用户具有权限最低的受限访问权限。cxcadmin密码遵循安全策略，是单向散列密码，有效期限为90天。cxcadmin用户可以使用名为remoteaccount的实用程序创建cxcroot用户。cxcroot用户可以获得root权限。

网络安全

可以使用SSH和cxcadmin用户凭证访问CX代理VM。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：设备维护单个用户(cxcadmin)，使用户能够对CX代理进行身份验证和通信。

- 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门户解密(DECRYPT请求表)。 只有授权人员才能访问此门户。cxcroot用户可使用此解密的密码获得root权限。密码有效期仅为两天。cxcadmin用户必须重新创建帐户，并在密码到期后从SWIM门户获取密码。

强化

CX代理设备遵循Center of Internet Security强化标准。

数据安全

CX代理设备不存储任何客户个人信息。设备凭据应用程序（作为其中一个Pod运行）将加密的服务器凭据存储在安全数据库中。收集的数据不会以任何形式存储在设备内，除非在处理时临时存储。收集完成后，遥测数据会尽快上传到CX云，并在确认上传成功后立即从本地存储中删除。

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。使用该代理通过传输层安全(TLS)v1.2使用消息队列遥测传输(MQTT)建立安全连接

日志和监控

日志不包含任何形式的个人身份信息(PII)数据。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。

思科遥测命令

CX云使用Cisco遥测命令中列出的API和命令检索资产遥测。本文档根据命令对Cisco Catalyst Center库存、诊断网桥、Intersight、合规性见解、故障以及CX代理收集的所有其他遥测源的适用性对命令进行分类。

资产遥测中的敏感信息在传输到云之前会被屏蔽。CX代理屏蔽所有收集到的将遥测直接发送到CX代理的资产的敏感数据。这包括密码、密钥、社区字符串、用户名等。控制器在将此信息传输到CX代理之前，为所有由控制器管理的资产提供数据掩码。在某些情况下，控制器管理的资产遥感勘测可以进一步匿名化。请参阅相应的产品支持文档了解有关遥测匿名化的详细信息(例如，Cisco Catalyst Center管理员指南的匿名数据部分)。

虽然无法自定义遥测命令列表且无法修改数据掩码规则，但客户可以通过指定数据源来控制哪些资

产的可遥测CX云访问，如控制器受管设备的产品支持文档或本文档的连接数据源部分所述（针对CX代理收集的其他资产）。

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FAQ来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：创建的默认用户帐户；用户可以使用cxcli执行CX代理应用程序命令，并且对该设备的权限最低；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，包含以下三类字符：大写、小写、数字和特殊字符。
cxcroot 密码政策	· cxcroot密码是RSA/ECB/PKCS1v1_5加密的 ·生成的密码需要在 SWIM 门户中解密。 · cxcroot用户和密码有效期为两天，可以使用cxcadmin用户重新生成。
SSH 登录密码政策	·至少包含下列三个类别的八个字符：大写、小写、数字和特殊字符。 ·五次失败的登录尝试将设备锁定30分钟；密码将在90天后过期。
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 Catalyst Center服务器凭证已加密并存储在数据库中。

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）。