

验证CX云代理概述v2.2产品问题请忽略此文章

目录

[简介](#)

[先决条件](#)

[要求](#)

[背景信息](#)

[关键域访问](#)

[特定于CX云代理门户的域](#)

[特定于CX云代理OVA的域](#)

[Cisco DNA Center支持的版本](#)

[支持的浏览器](#)

[支持的产品列表](#)

[连接数据源](#)

[设置CX云代理](#)

[将 CX Cloud Agent 连接到 CX Cloud](#)

[添加Cisco DNA Center作为数据源](#)

[添加其他资产作为数据源](#)

[概述](#)

[发现协议](#)

[连接协议](#)

[使用种子文件添加设备](#)

[设备的遥测处理限制](#)

[使用新的种子文件添加设备](#)

[使用修改的种子文件添加设备](#)

[使用IP范围添加设备](#)

[编辑IP范围](#)

[安排诊断扫描](#)

[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 5.2.30安装](#)

[MicrosoftHyper-V安装](#)

[网络配置](#)

[使用CLI生成配对代码的备选方法](#)

[配置思科DNA中心以向CX云代理转发系统日志](#)

[先决条件](#)

[配置系统日志转发设置](#)

[配置其他资产以将系统日志转发到CX云代理](#)

[具有转发功能的现有系统日志服务器](#)

[现有系统日志服务器无转发功能或不带系统日志服务器](#)

[启用信息级别系统日志设置](#)

[备份和恢复CX云虚拟机](#)

[备份](#)

[恢复](#)

[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](#)

[思科遥测命令](#)

[安全汇总](#)

简介

本文档介绍思科的客户体验(CX)云代理。

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。

要求

部署要求：

- 以下任何虚拟机监控程序：
 - VMware ESXi版本5.5或更高版本
 - Oracle Virtual Box 5.2.30或更高版本
 - Windows虚拟机监控程序版本2012到2022
- 虚拟机监控程序可以托管具有以下要求的虚拟机：
 - 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.cisco.cloud
 - FQDN：ng.acs.agent.us.cisco.cloud
 - FQDN：cloudsso.cisco.com
 - FQDN：api-cx.cisco.com
- 对于使用指定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台服务器：
 - FQDN：agent.us.cisco.cloud
 - FQDN：agent.emea.cisco.cloud

- FQDN : ng.acs.agent.emea.cisco.cloud
- FQDN : cloudsso.cisco.com
- FQDN : api-cx.cisco.com
- 对于使用指定亚太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台服务器：
 - FQDN : agent.us.cisco.cloud
 - FQDN : agent.apjc.cisco.cloud
 - FQDN : ng.acs.agent.apjc.cisco.cloud
 - FQDN : cloudsso.cisco.com
 - FQDN : api-cx.cisco.com
- 对于使用指定的欧洲和亚太地区数据中心作为其主要数据区域的客户，仅在初始设置期间向CX云注册CX云代理时需要连接到FQDN : agent.us.cisco.cloud。在CX云代理成功注册到CX云后，此连接不再需要。
- 对于CX云代理的本地管理，必须可以访问端口22。
- 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：

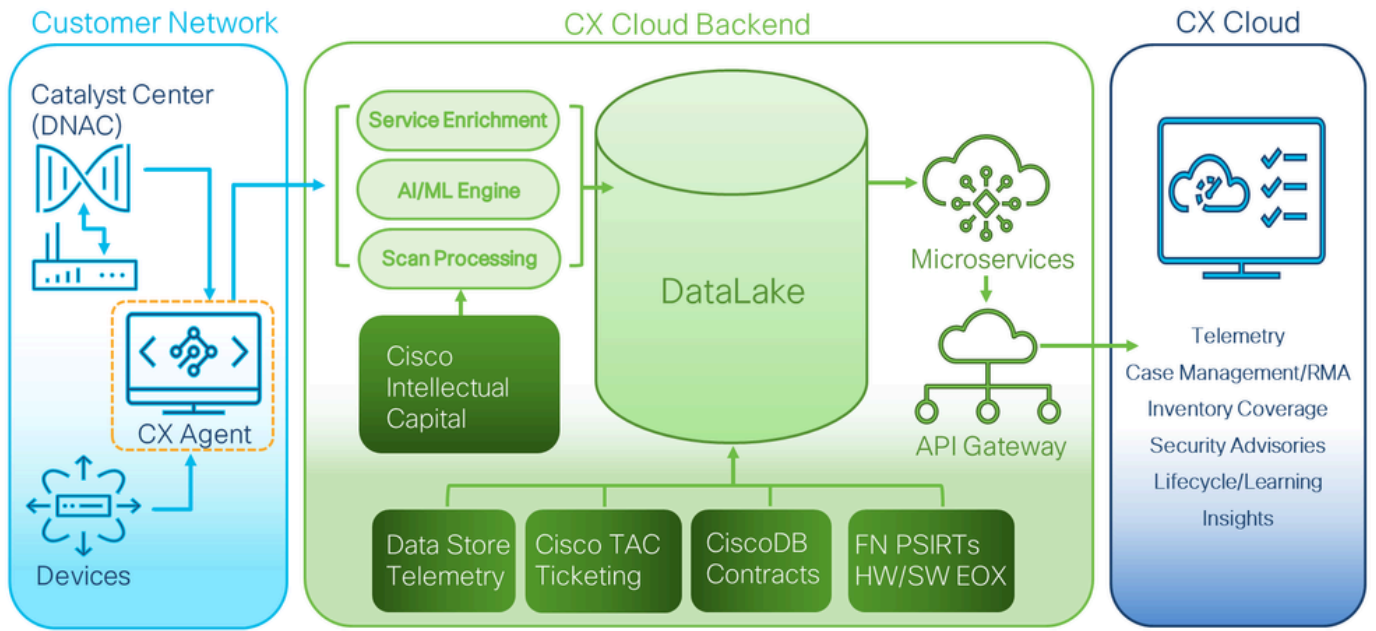
Source		Destination		Protocol	Port	Purpose	Type
IP Address	Hostname						
CX Cloud Agent Traffic							
Data Collection and Transfer							
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.cisco.cloud DNAC Servers Additionally, For Americas region, FQDN: ng.acs.agent.us.cisco.cloud For EMEA region, FQDN: agent.emea.cisco.cloud, and FQDN: ng.acs.agent.emea.cisco.cloud For APJC region, FQDN: agent.apjc.cisco.cloud, and FQDN: ng.acs.agent.apjc.cisco.cloud		HTTPS	TCP/443	Data collection via DNAC servers, Data transfer to CX Cloud, including upgrade functionality	Outbound connection to DNAC servers + Outbound to Cisco AWS regional data centers
Agent IP		Customer Device		SNMP	UDP/161	Collect OIDs and MIBs for other assets collected by CX Cloud Agent	Outbound to LAN
Devices		Agent IP		SYSLOG	UDP/514	Stream Syslog messages from Device to Agent	Inbound from LAN
Agent IP		Customer Device		SSH	TCP/22	Collect CLI commands	Outbound to LAN
Agent IP		Customer Device		Echo	TCP/7	Check the device reachability	Outbound to LAN
Agent IP		Customer Device		Telnet	TCP/23	Collect CLI commands	Outbound to LAN
Agent Administration Access							
Support VM		Agent IP		SSH	TCP/22	Agent Maintenance	Inbound from LAN

背景信息

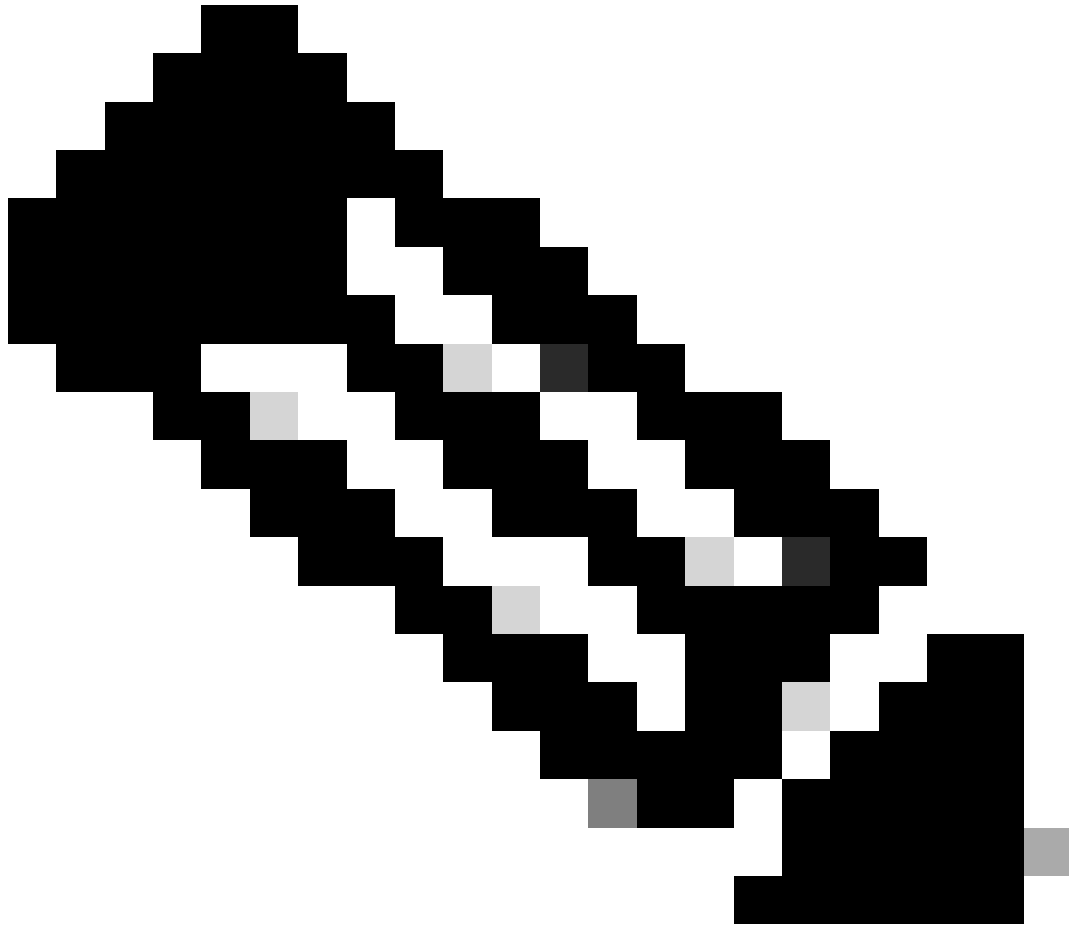
思科(CX)云代理是一个高度可扩展的平台，可从客户网络设备收集遥测数据，为客户提供切实可行的见解。CX Cloud Agent支持将活动运行配置数据转换为在CX Cloud中显示的主动和预测性见解，从而实现人工智能(AI)/机器学习(ML)转换。

本指南特定于CX Cloud Agent v2.2及后续版本。请参阅[Cisco CX云代理](#)页以访问以前的版本。

CX Cloud Architecture



CX云架构



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。

-
- 如果VM环境中启用了动态主机配置协议(DHCP)，则自动检测IP；否则，必须提供空闲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)集群Cisco DNA Center版本为2.1.2.x到2.2.3.x、2.3.3.x、2.3.5.x以及Cisco Catalyst Center Virtual Appliance和Cisco DNA Center Virtual Appliance。
 - 如果网络具有SSL拦截，则允许列表CX云代理的IP地址。
 - 对于所有直接连接的资产，需要15级SSH权限。
 - 请仅使用提供的主机名；不能使用静态IP地址。

关键域访问

要启动CX云之旅，用户需要访问这些域。仅使用提供的主机名；不使用静态IP地址。

特定于CX云代理门户的域

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

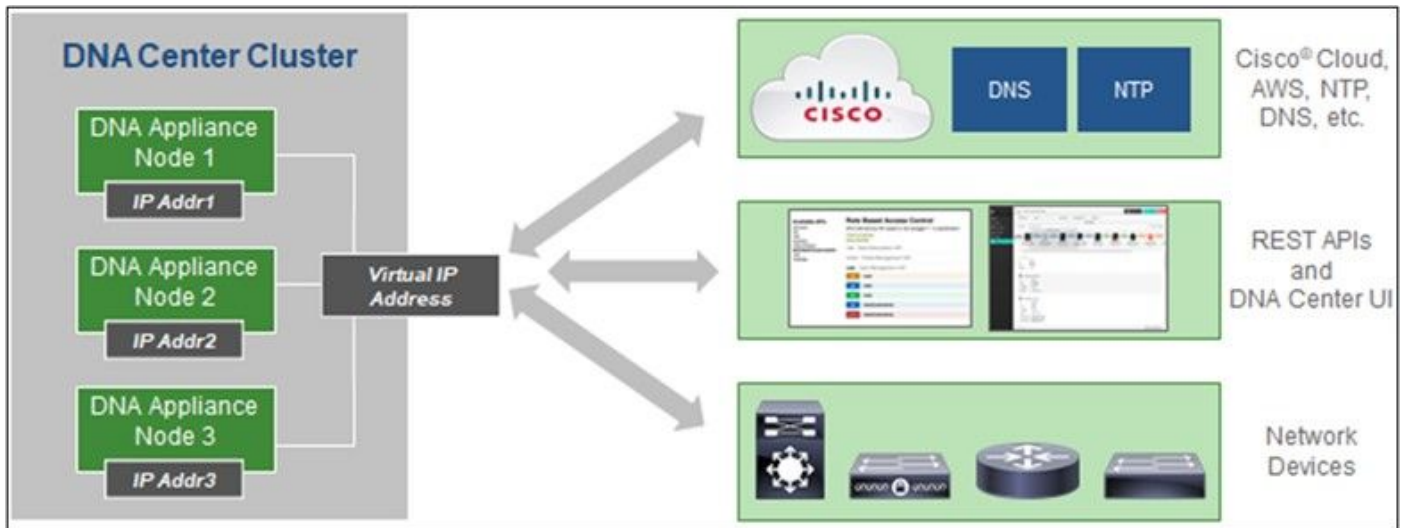
特定于CX云代理OVA的域

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.cisco.cloud	agent.us.cisco.cloud	agent.us.cisco.cloud
ng.acs.agent.us.cisco.cloud	agent.emea.cisco.cloud	agent.apjc.cisco.cloud
	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

 注意：在端口443上为指定FQDN启用重定向时，必须允许出站访问。

Cisco DNA Center支持的版本

支持的单节点和高可用性集群Cisco DNA Center版本为2.1.2.x到2.2.3.x、2.3.3.x、2.3.5.x以及Cisco Catalyst Center Virtual Appliance和Cisco DNA Center Virtual Appliance。



多节点 HA 集群 Cisco DNA Center

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

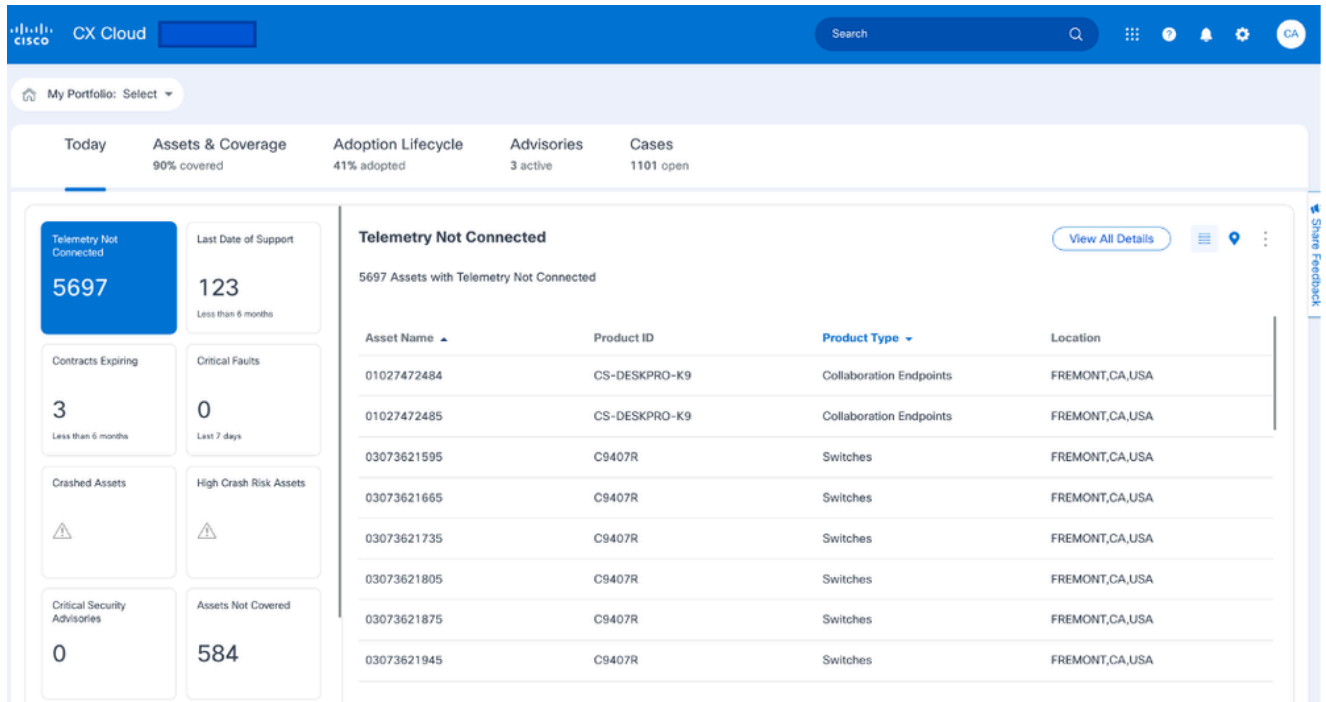
支持的产品列表

要查看CX云代理支持的产品列表，请参阅[支持的产品列表](#)。

连接数据源

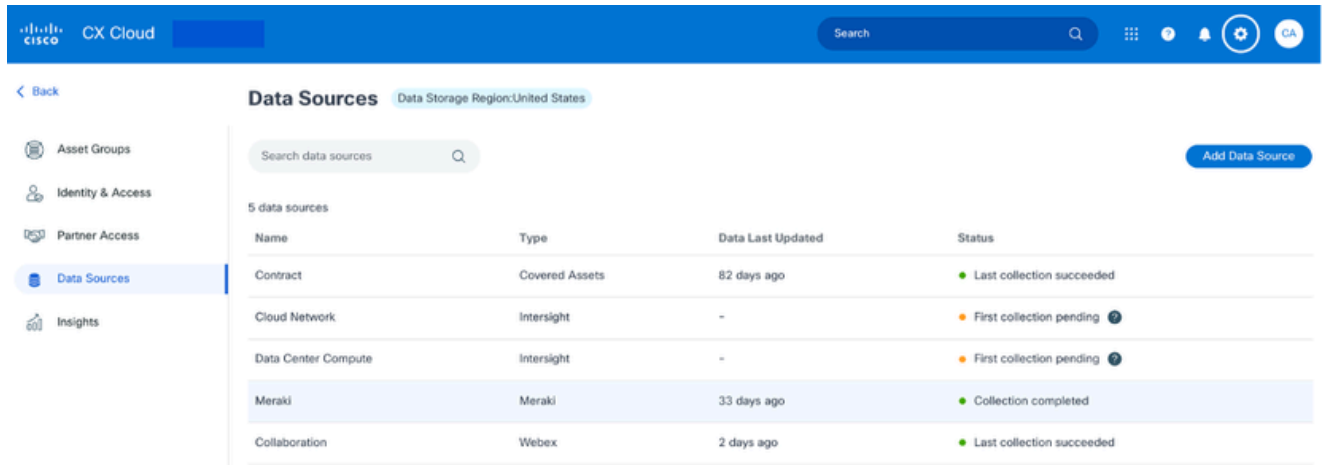
要连接数据源：

1. 单击cx.cisco.com登录到CX云。



CX云主页

2. 选择管理中心图标。数据源窗口打开。










数据源

3. 单击Add Data Source。添加数据源窗口打开。显示的选项因客户订用而异。

Add Data Source

Search data sources Q

-  **Cisco DNA Center**
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types) Add Data Source
-  **Contracts**
Supports all Success Tracks and offers Add Data Source
-  **Intersight**
Supports the Data Center Compute and Cloud Network Success Tracks Add Data Source
-  **Other Assets**
Uses CX Cloud Agent to support Success Tracks Add Data Source
-  **Smart Accounts**
Supports licensing Add Data Source
-  **Webex**
Supports the Success Track for Collaboration Add Data Source
-  **Cisco Catalyst SD-WAN Manager**
Supports the Success Track for WAN Add Data Source


添加数据源

- 单击Add Data Source以选择适用的数据源。如果之前未设置CX云代理，则会打开[设置CX云代理](#)窗口，必须在此完成设置。如果设置完成，则连接继续。请参阅以下章节之一以继续：

[设置CX云代理](#)

[添加思科DNA中心作为数据源](#)

[添加其他资产作为数据源](#)

 **注意：**仅当以前未配置直接设备连接时，其他资产选项才可用。

设置CX云代理

如果以前未完成过CX云代理设置，则在连接数据源时会提示进行设置。

要设置CX云代理，请执行以下操作：

Set Up CX Cloud Agent

Help

SET UP CX CLOUD AGENT

0%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine



Add Cloud Agent to your CX Cloud pit crew

CX Cloud Agent gathers telemetry data from the devices on your network, allowing you to take advantage of all the hyper-relevant insights and trusted expertise that CX Cloud has to offer.



Review deployment requirements

Prepare your network for CX Cloud Agent

CX Cloud Agent runs as a virtual machine (VM), so you'll need a hypervisor to host it.

Before you download and install the image file, make sure CX Cloud Agent is able to connect to the designated server(s) via HTTPS on port 443 using both the FQDN and the IP address:

For **AWS US** data centers:

- FQDN: agent.us.cisco.cloud
- FQDN: ng.acs.agent.us.cisco.cloud
- FQDN: cloudssso.cisco.com
- FQDN: api-cx.cisco.com



Review the [CX Cloud Agent Overview](#) for complete hardware and software prerequisites.



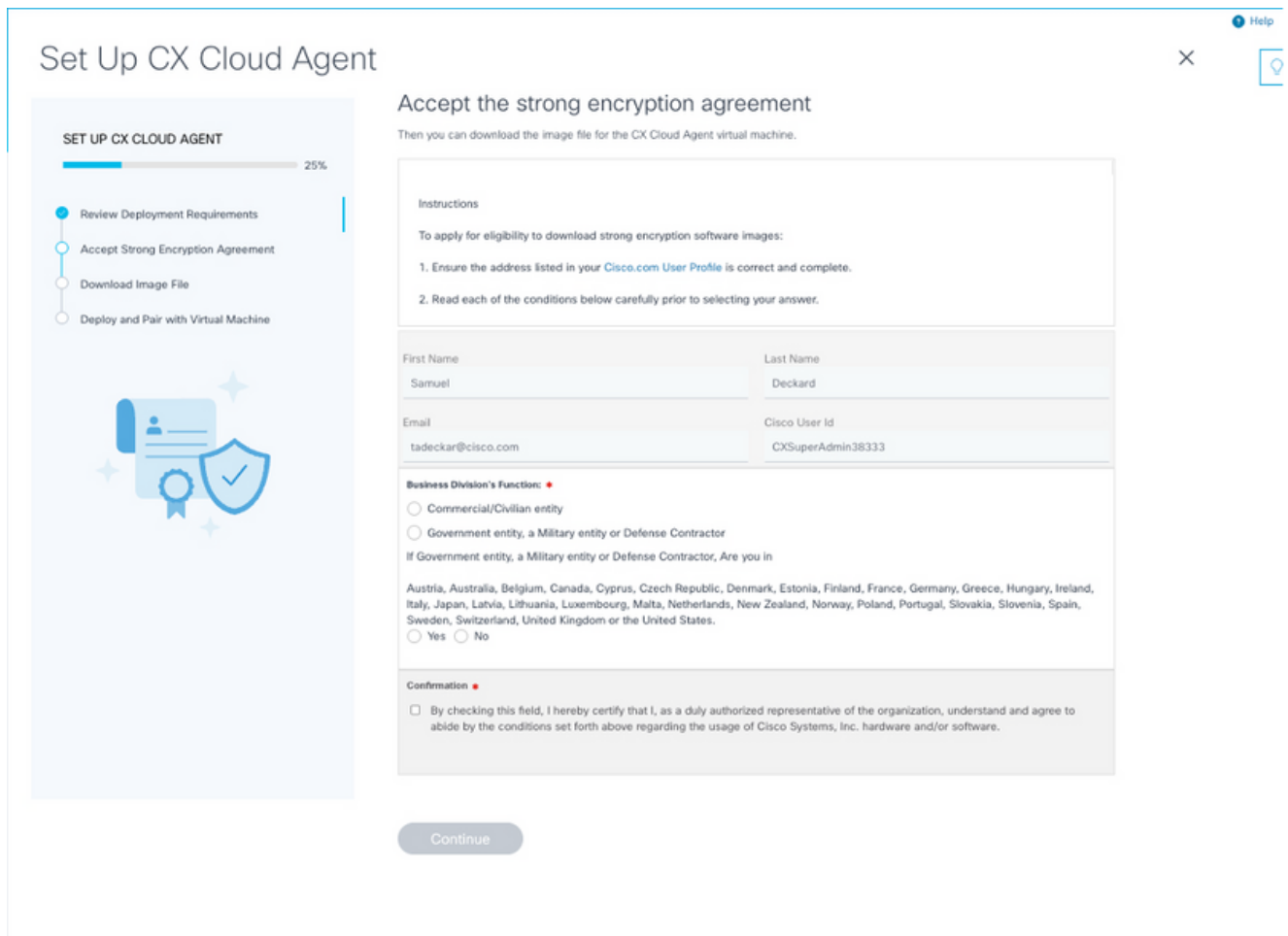
CX Cloud takes security seriously. Review the [Security](#) section of the [CX Cloud Agent Overview](#) to learn how CX Cloud Agent handles and stores your data.

I set up this configuration on port 443

Continue

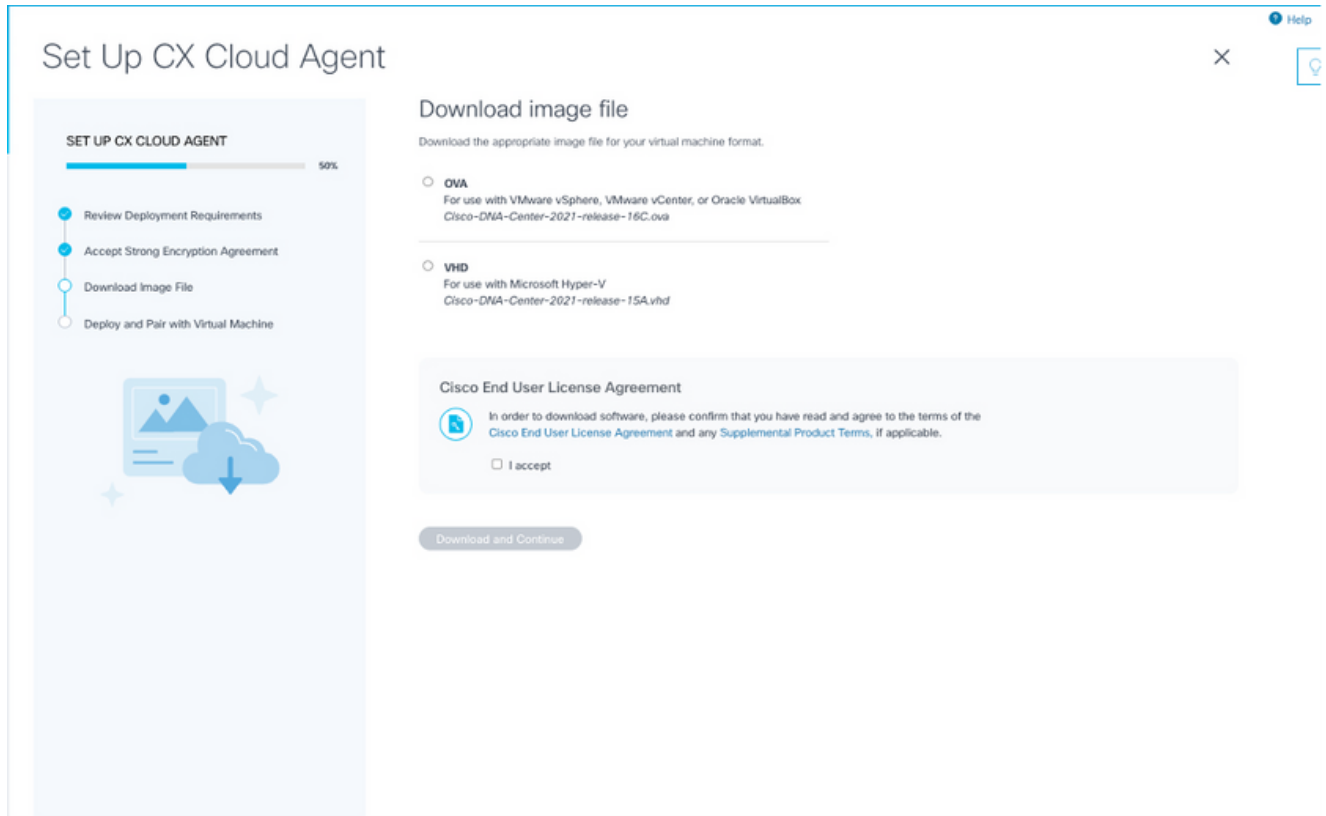
查看部署要求

1. 查看查看部署要求并选择I set up this configuration on port 443 复选框。
2. 单击 Continue。“设置CX云代理-接受强加密协议”窗口打开。



加密协议

3. 验证First Name、Last Name、E-mail和Cisco User Id字段中的预填充信息。
4. 选择适当的业务部门的功能。
5. 选中确认复选框以同意使用条件。
6. 单击 Continue。“设置CX云代理-下载映像文件”窗口打开。



下载映像

7. 选择适当的文件格式下载安装所需的映像文件。
8. 选中I accept复选框同意思科最终用户许可协议。
9. 单击Download and Continue。“设置CX云代理-部署并与虚拟机配对”窗口打开。
10. 要获取下一部分中所需的配对代码，请参阅[网络配置](#)。

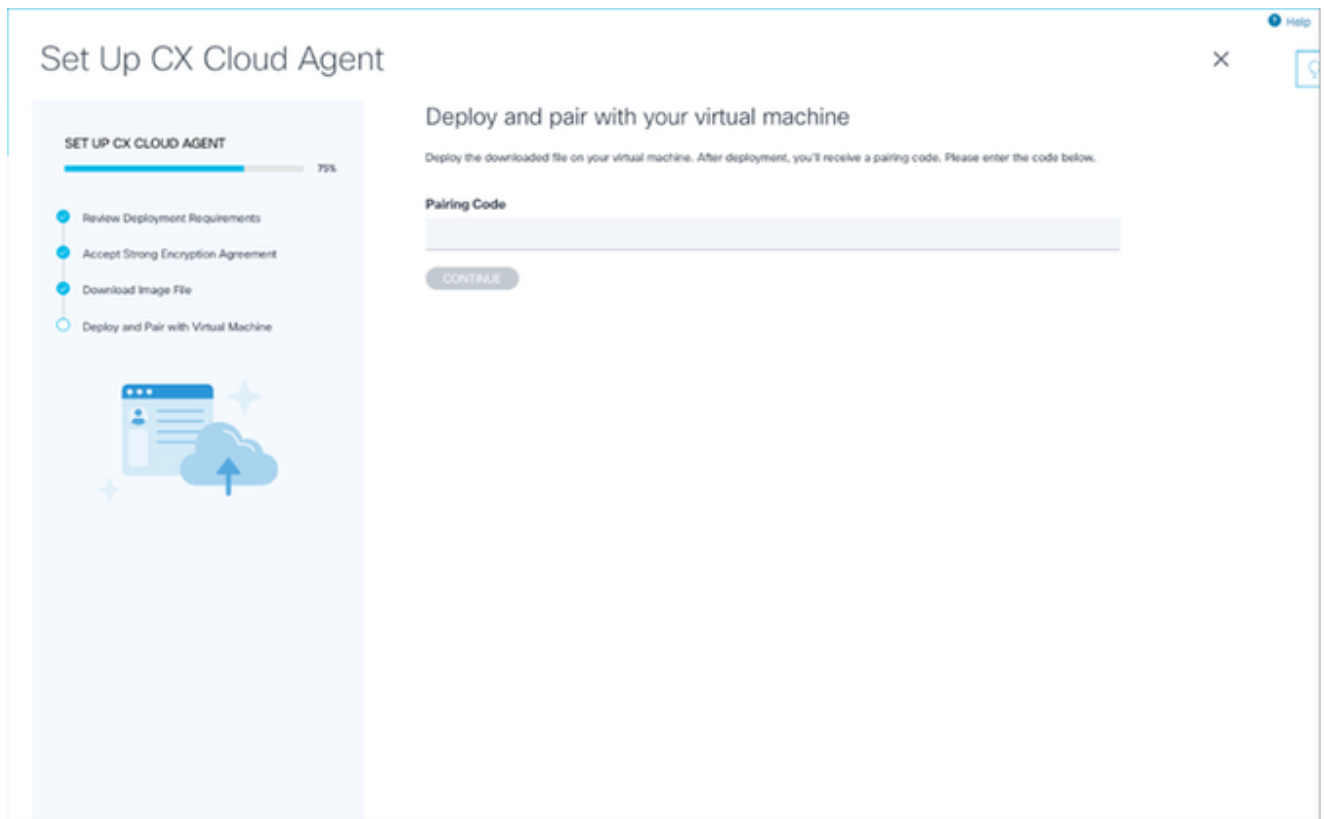
将 CX Cloud Agent 连接到 CX Cloud

要开始遥测收集，需要将CX云代理连接到CX云，以便可以更新UI中的信息以显示当前资产和见解。本节提供完成连接和故障排除指南的详细信息。

要将CX云代理连接到CX云，请执行以下操作：

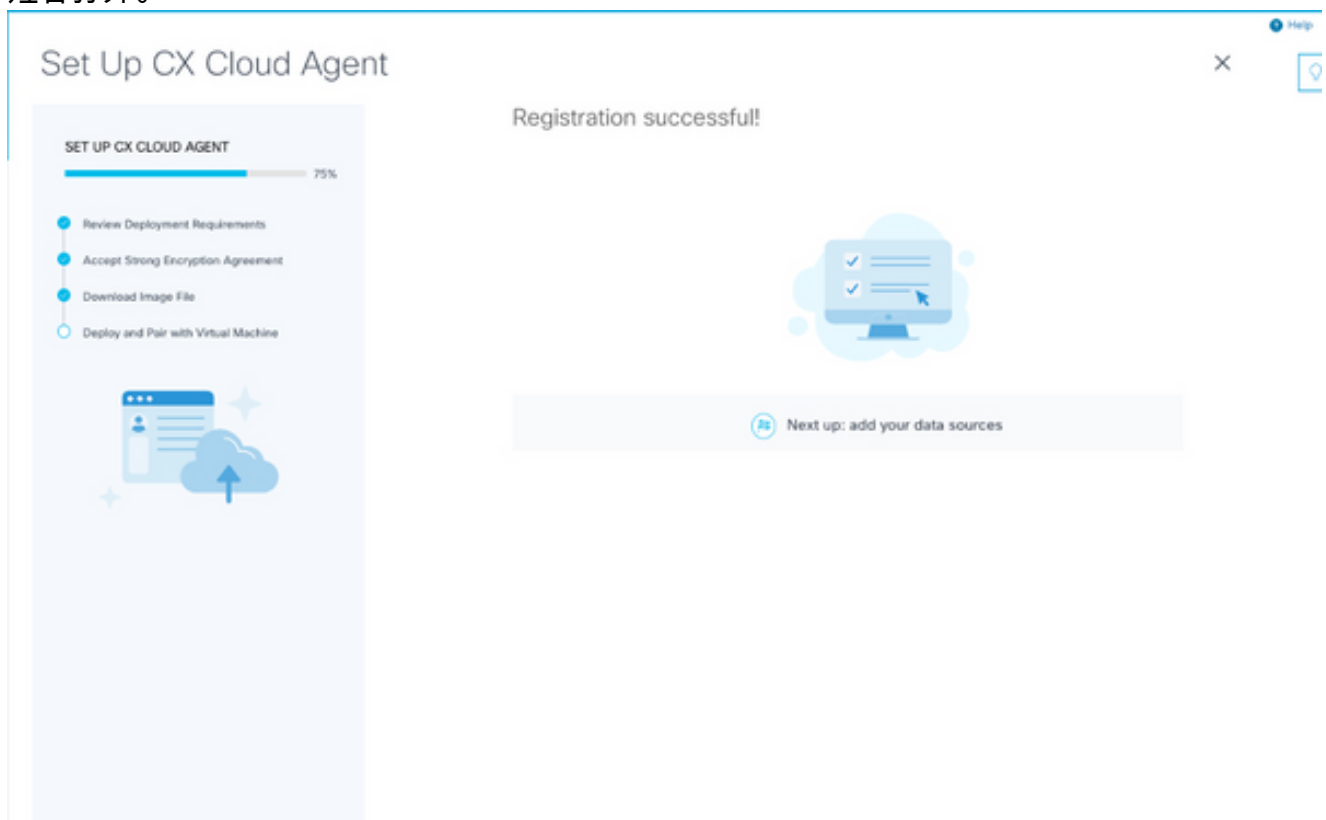
1. 输入通过代理连接的虚拟机的控制台对话框或命令行界面(CLI)中提供的配对代码。

 **注意：**在部署下载的OVA文件后会收到配对代码。



配对代码

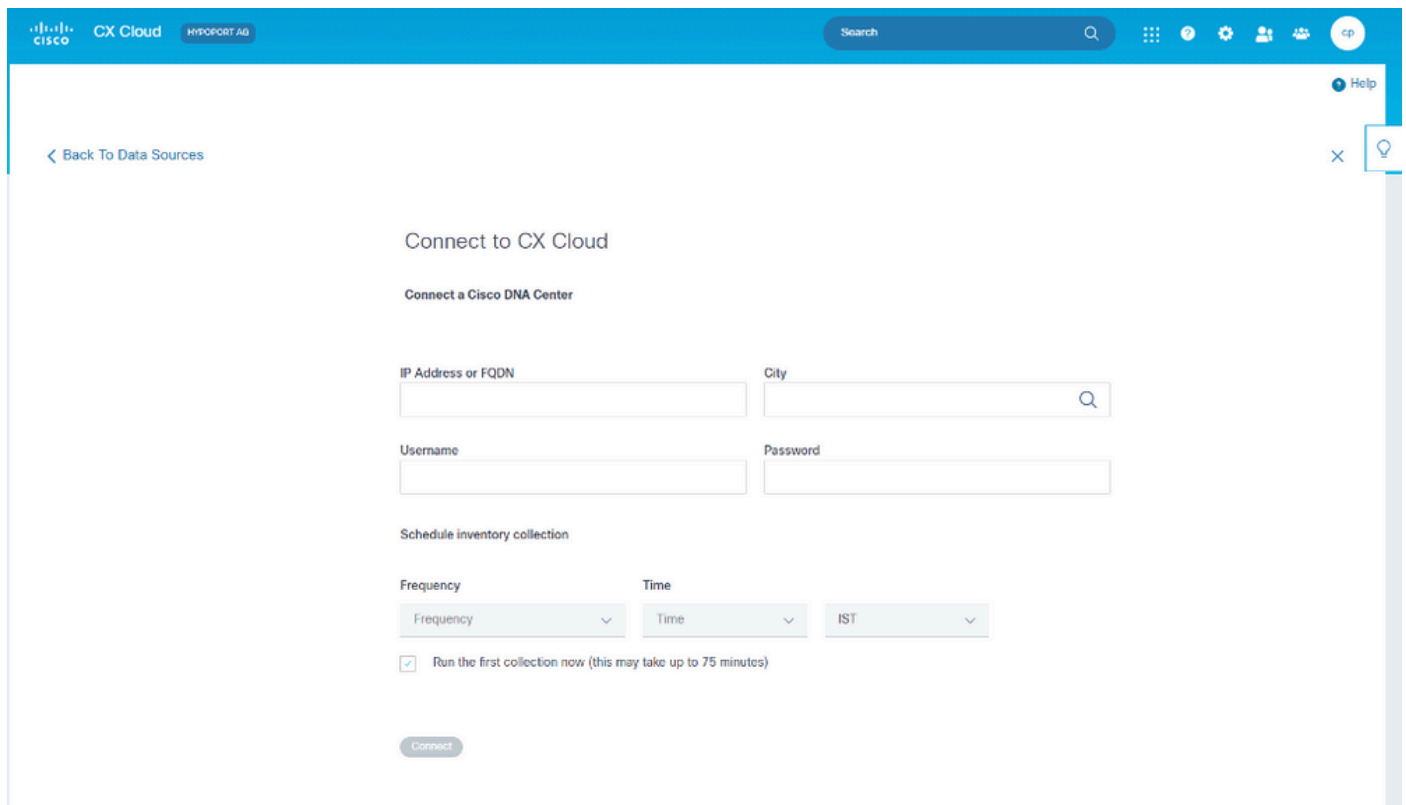
2. 点击继续注册CX云代理。在自动导航到添加数据源页之前，设置CX云代理-注册成功窗口将短暂打开。



注册成功

添加Cisco DNA Center作为数据源

从“Data Sources Connection”窗口（请参阅“Connecting Data Sources”部分中的“Connect Data Sources”图像）中选择Cisco DNA Center，将打开以下窗口：




The screenshot shows a web interface titled "Connect to CX Cloud" with a sub-section "Connect a Cisco DNA Center". It contains the following elements:

- Input fields for "IP Address or FQDN" and "City".
- Input fields for "Username" and "Password".
- A "Schedule inventory collection" section with three dropdown menus: "Frequency", "Time", and "IST".
- A checkbox labeled "Run the first collection now (this may take up to 75 minutes)".
- A "Connect" button at the bottom.


连接到CX云

添加Cisco DNA Center作为数据源的步骤：

1. 输入Cisco DNA Center IP地址或虚拟IP地址或FQDN、City（Cisco DNA Center位置）、Username和Password。

 注意：请勿使用单个集群节点IP。

2. 通过输入频率和时间以指示CX云代理程序多久执行一次网络扫描并更新有关所连接设备的信息，从而安排资产收集。

 注意：第一次资产收集最多可能需要75分钟。

3. 单击 Connect。此时将显示包含思科DNA中心IP地址的确认消息。

Connect to CX Cloud

Connected

**Cisco DNA Center 10.122.58.165**
Inventory collection runs every day At 02:00 AM CST
First collection will run immediately after data sources are added

Connect another data source to CX Cloud Agent?

+ Add Another Cisco DNA Center

Done

已成功连接

- 单击Add Another Cisco DNA Center、Done或Back to Data Sources，导航回Data Sources窗口。

添加其他资产作为数据源

概述

遥测收集已扩展到非思科DNA中心管理的设备，使客户能够查看遥测衍生的见解，并与更广泛的设备分析进行交互。在最初设置CX云代理后，用户可以选择配置CX云代理，以连接到CX云监控的基础设施中的另外20个思科DNA中心。用户还可以将CX云代理直接连接到其环境中的其他硬件资产，最多可连接10,000个直接连接的设备。

用户可以使用种子文件唯一标识此类设备或通过指定IP范围（可由CX云代理进行扫描）来标识要合并到CX云中的设备。这两种方法都依赖简单网络管理协议(SNMP)执行发现(SNMP)，依靠安全外壳(SSH)执行连接。必须正确配置这些字段，才能成功收集遥测数据。



注意：

可以使用种子文件或IP范围。初始设置后无法更改此选择。



注意：

初始种子文件可以替换为另一个种子文件，而初始IP范围可以编辑为新的IP范围。

从数据源连接窗口中选择其他资产时，将打开以下窗口：



Connect to CX Cloud

How would you like to connect these assets?

Upload a seed file (recommended)

Add your devices to a [Seed File Template](#). You can reupload this file later if you need to make changes.

Provide an IP Address range

Select any connection method(s). At least one SNMP and SSH are required.

SNMP v3

SNMP v2c

SSH v2

[More](#)

These options support legacy products

SSH v1

Telnet

[Continue](#)



配置与CX云的连接

要添加其他资产作为数据源，请执行以下操作：

- 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范围的发现都依赖于SNMP作为发现协议。存在不同版本的SNMP，但CX Cloud Agent支持SNMPV2c和SNMP V3，并且可配置任一版本或同时配置两个版本。用户必须提供下面详细介绍的相同信息才能完成配置并启用SNMP管理的设备和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。建议在所有公共网络和面向Internet的网络中使用SNMPv3，以防范安全风险和威胁。在CX云上，最好配置SNMPv3而不是SNMPv2c，但缺少内置的SNMPv3支持的旧版设备除外。如果两个版本的SNMP均由用户配置，默认情况下，CX云代理可以使用SNMPv3尝试与各个设备通信，如果通信无法成功协商，则恢复为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）。可以使用SSHv2，但缺少适当内置支持的个别传统资产除外。请注意，SSHv1协议包含基本漏洞。如果没有额外的安全性，在依赖SSHv1时，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（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。

使用种子文件添加设备


关于种子文件

种子文件是逗号分隔值(csv)文件，其中每行表示一个系统数据记录。在种子文件中，每个种子文件记录都对应于CX云代理可从其中收集遥测数据的唯一设备。系统会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，并将其作为作业日志详细信息的一部分进行捕获。种子文件中的所有设备都被视为受管设备，即使初始配置时这些设备无法访问。如果要上传新的种子文件来替换以前的种子文件，上次上传的日期将显示在CX云中。

CX Cloud Agent可以尝试连接到设备，但在无法确定PID或序列号的情况下，无法处理要在“资源”页中显示的每个设备。种子文件中以分号开头的任何行都将被忽略。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按原样保留或删除此行（建议选项）。

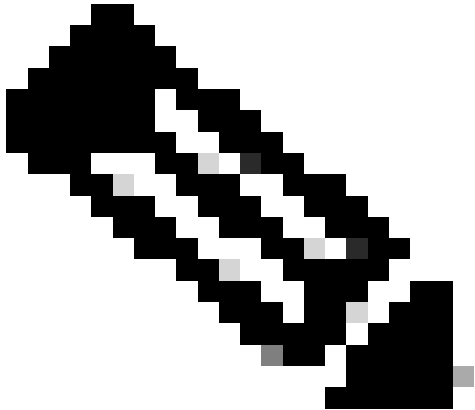
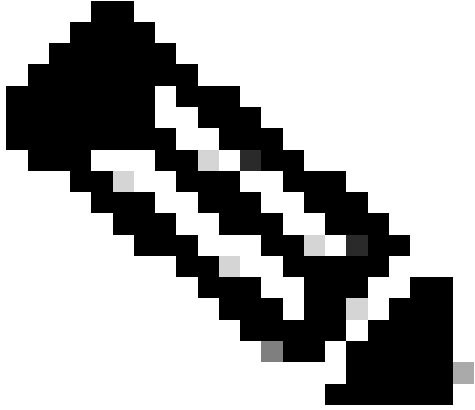
示例种子文件（包括列标题）的格式不得以任何方式更改，这一点非常重要。单击提供的链接以查看PDF格式的种子文件。此PDF仅供参考，可用于创建需要以.csv格式保存的种子文件。

单击此[链接](#)可查看可用于创建.csv格式的种子文件的种子文件。

 注意：此PDF仅供参考，可用于创建需要以.csv格式保存的种子文件。

此表标识所有必要的种子文件列和每个列中必须包括的数据。

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 Cloud Agent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选择为“snmpv2c”，则为必填项	如果为特定设备选择SNMPv2的传统变体，则必须为设备SNMP集合指定snmpRO（只读）凭证。否则，条目可以为空。
D	snmpv3UserName：如果col#=3选择为“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MD5或SHA算法进行身份验证。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。

种子文件列	列标题/标识符	列的用途
		 <p data-bbox="951 779 1453 857">注意：MD5被视为不安全的，并且SHA可在支持它的所有设备上使用。</p>
F	snmpv3AuthPassword：密码	<p data-bbox="855 954 1469 1077">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。</p>
G	snmpv3PrivAlgorithm：值可以是DES，3DES	<p data-bbox="855 1155 1469 1234">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。</p>  <p data-bbox="951 1805 1453 1928">注意：DES所使用的56位密钥太短，无法提供加密安全，并且3DES可用于支持它的所有设备。</p>
H	snmpv3PrivPassword：密码	<p data-bbox="855 2018 1469 2096">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。</p>

种子文件列	列标题/标识符	列的用途
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。此引擎ID在由CX云代理收集SNMP数据集时作为引用发送。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'。如果为空 , 则默认情况下可设置为“sshv2”	CLI用于直接与设备交互。CX云代理使用此协议为特定设备进行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代表SSH , 23代表telnet。
L	CliUser : CLI用户名(可以提供CLI用户名/密码或同时提供两者 , 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选项。
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云代理在CLI收集期间连接到设备时使用此选项。
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
Q	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

种子文件列	列标题/标识符	列的用途
S	未来支持（无需输入）	留作将来使用

设备的遥测处理限制


处理设备的遥测数据时存在以下限制：

- 某些设备在收集摘要中显示为可访问，但在CX云资产页面中不可见。设备检测限制会阻止处理此类设备遥测。
- 对于不属于园区成功跟踪一部分的设备，CX云资产页面中的遥测属性可能不准确或缺失。
- 如果种子文件或IP范围集合中的设备也是Cisco DNA Center资产的一部分，则只会针对Cisco DNA Center条目对设备报告一次。不收集或处理种子文件/ IP范围条目，以避免重复。

使用新的种子文件添加设备

要使用新的种子文件添加设备，请执行以下操作：


1. 使用本文中嵌入的链接（请参阅关于种子文件）或通过配置与CX云的连接窗口中的链接下载种子文件模板(PDF)。

 注意：下载初始种子文件后，“配置与CX云的连接”窗口中的链接不再可用。

Configure connection to CX Cloud

Upload your seed file ✕

Download the [seed file template](#) and add your device info. Then attach the file below.



Drag and Drop files or [browse files](#)
Supports CSV files only. Max file size 5 MB.

Collection Frequency

Frequency ▼

Time

Time ▼

VET ▼

Run the first collection now (this may take up to 75 minutes)


Connect This Data Source


配置连接到CX云窗口

2. 打开Excel电子表格（或任何首选电子表格），然后按模板中所示输入标题。
3. 手动输入数据或将数据导入文件。
4. 完成后，将模板另存为.csv文件以将该文件导入CX云代理。

Configure connection to CX Cloud

Upload your seed file ✕


You've reached your file limit.
To upload a new file, please remove an existing file.

	nextgen_seedfile.csv Completed.	Delete
---	------------------------------------	------------------------

Schedule Inventory Collection

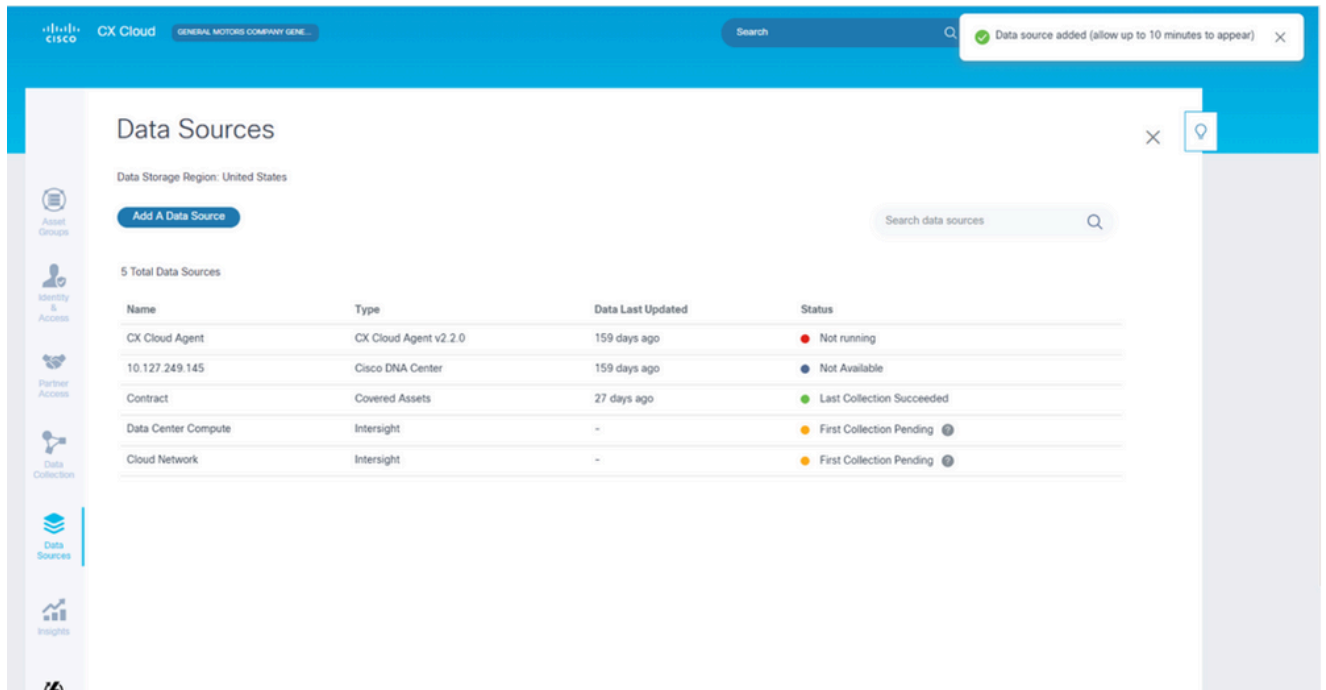
Collection Frequency	Time	Day	
Weekly ▼	12:00am ▼	VET ▼	Sunday ▼

Run the first collection now (this may take up to 75 minutes)

[Connect](#)

上传种子文件窗口

5. 在上传您的种子文件窗口中，拖放新创建的.csv文件，或者点击浏览文件，然后导航到.csv文件。
6. 完成计划资产收集部分并单击连接。“数据源”窗口打开，显示一条确认消息。
7. 在CX云的初始配置完成之前，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和其他因素，此过程可能需要相当长的时间。




确认消息

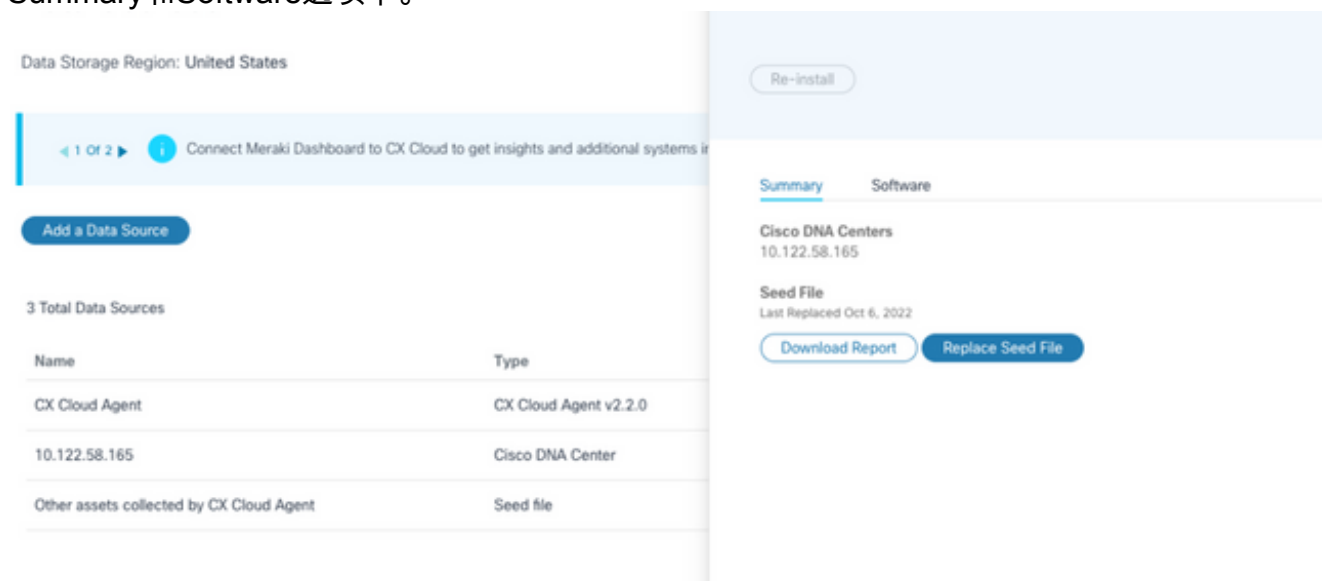
使用修改的种子文件添加设备

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，然后保存该文件。

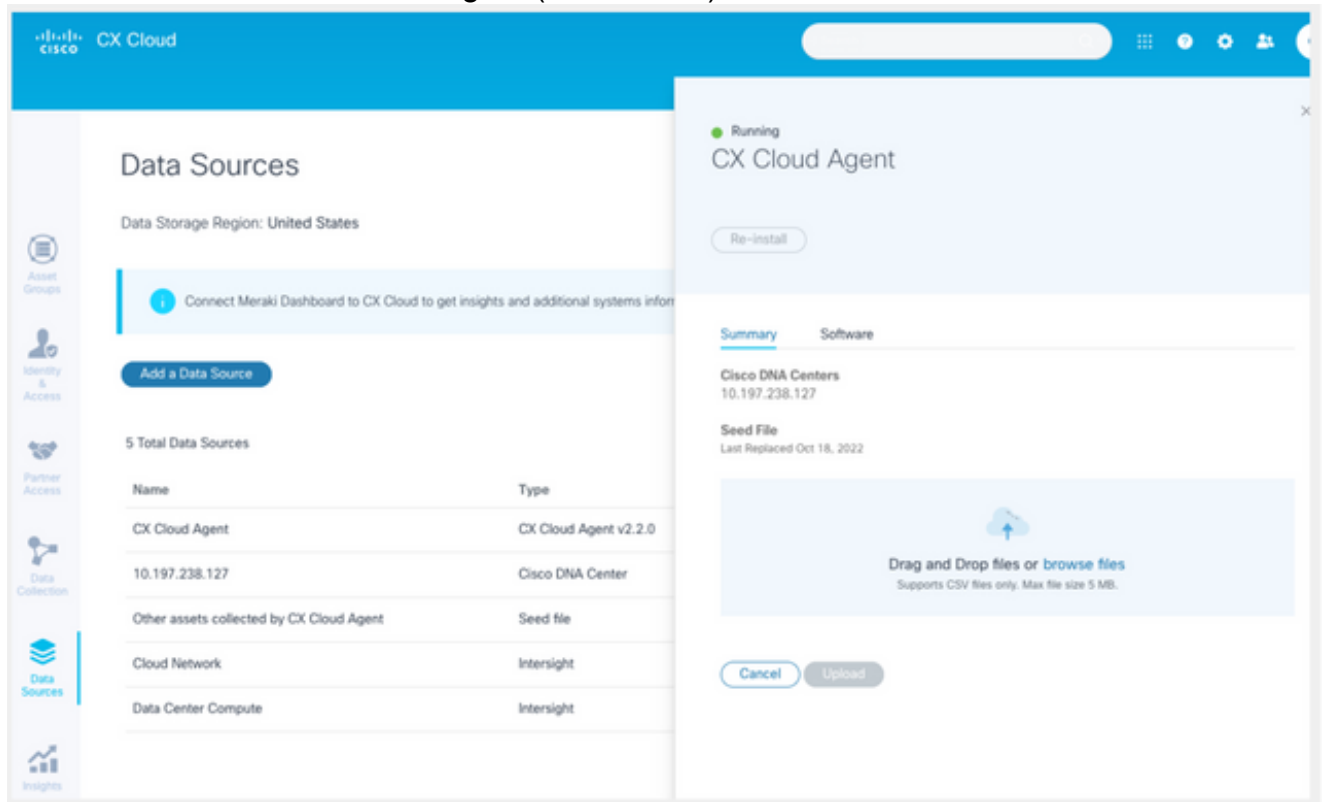
 **注意：**要将资产添加到种子文件，请将这些资产附加到以前创建的种子文件，然后重新加载文件。由于上传新的种子文件会替换当前的种子文件，因此这是必要的。只有最新上传的种子文件用于发现和收集。

2. 在数据源页中，选择类型为CX云代理的数据源。将打开一个详细信息窗口，其中包含 Summary 和 Software 选项卡。



详细信息窗口

- 单击Download Report以生成关于选定数据源的所有资产的报告。报告提供有关设备IP地址、序列号、可接通性、命令类型、命令状态和命令错误的信息（如果适用）。
- 单击替换种子文件。CX Cloud Agent（CX云代理）窗口打开。



CX云代理窗口


- 将修改的种子文件拖放到窗口中，或浏览到该文件并将其添加到窗口中。
- 单击Upload。


使用IP范围添加设备

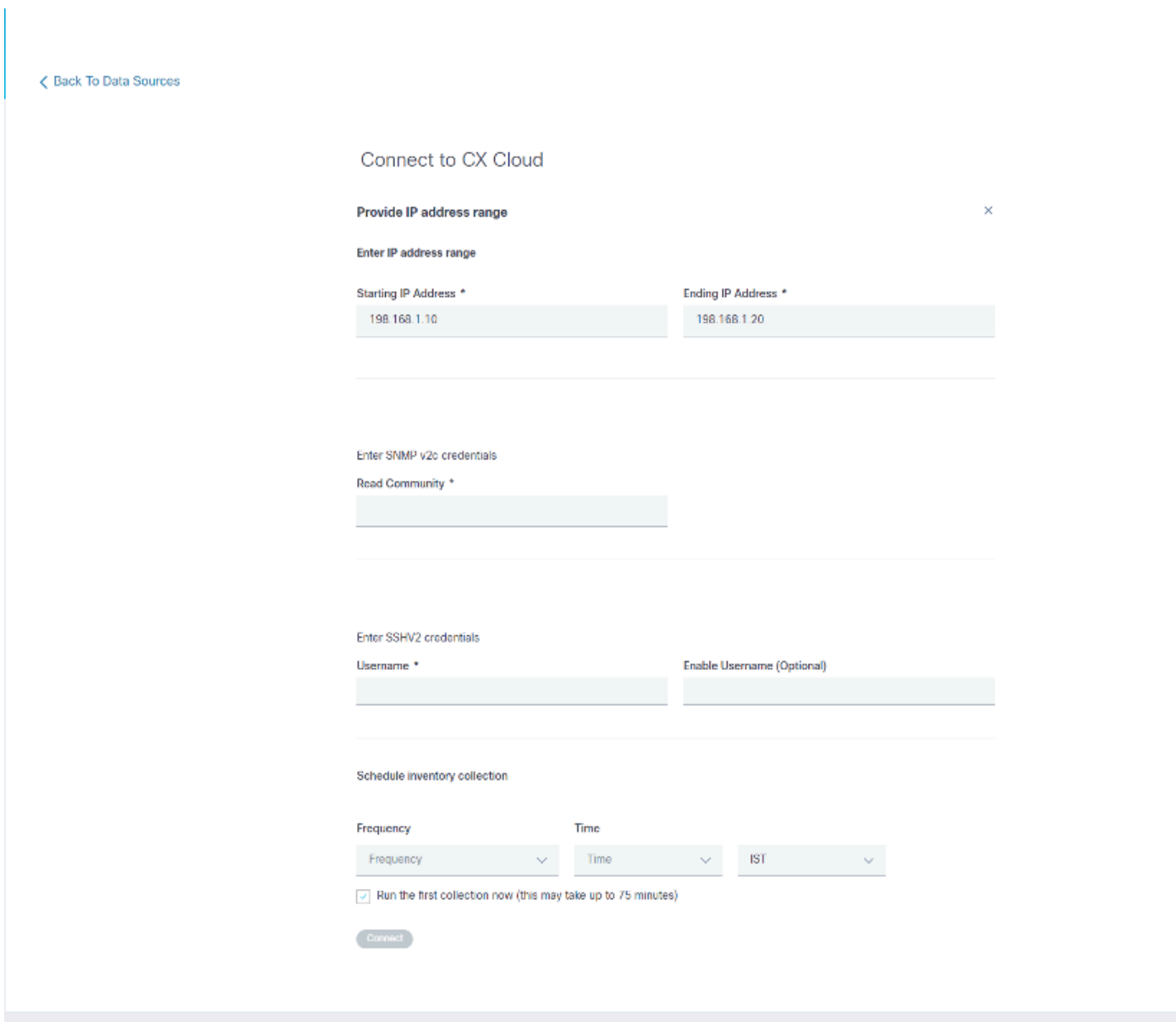
IP范围允许用户识别硬件资产，然后根据IP地址从这些设备收集遥感勘测数据。遥测收集的设备可以通过指定单个网络级IP范围进行唯一标识，CX云代理可以使用SNMP协议对其进行扫描。如果选择IP范围来标识直连设备，则引用的IP地址可以尽可能受到限制，同时允许覆盖所有需要的资产。

- 可以提供特定IP，也可以使用通配符替换IP的八位组来创建范围。
- 如果特定IP地址未包含在设置过程中识别的IP范围内，CX云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云代理将用户提供的凭证用于任何IP。例如：172.16.*.*允许凭证用于172.16.0.0/16子网中的所有设备。
- 如果网络或客户群(IB)发生任何更改，则可以修改IP范围。请参阅[编辑IP范围](#)

CX Cloud Agent可以尝试连接到设备，但在无法确定PID或序列号的情况下，无法处理要在资产视图中显示的每个设备。

 注意：

 点击Edit IP Address Range启动按需设备发现。在向指定的IP范围添加或删除任何新设备（内部或外部）时，客户必须始终单击Edit IP Address Range(请参阅[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 Cloud Agent收集资产中。



初始IP地址范围窗口

使用IP范围添加设备需要用户通过配置UI指定所有适用的凭证。显示的字段因在前几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 Cloud Agent将根据各个设备功能自动协商协议选择。

使用IP地址连接设备时，客户可以确保IP范围内所有相关协议以及SSH版本和Telnet凭证有效，否则连接可能会失败。

要使用IP范围添加设备，请执行以下操作：

1. 在配置与CX云的连接窗口中，选择提供IP地址范围选项。

Configure connection to CX Cloud

Provide IP address range ✕

Enter IP address range

Starting IP Address *

Ending IP Address *

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

使用IP地址表单添加设备

- 请在表格中填写相关信息。
- 可以选择多个连接选项。这些屏幕显示选项的配置凭证。有关每个连接选项的凭证字段的说明，请参阅[关于种子文件](#)。

Configure connection to CX Cloud

Provide IP address range

×

Enter IP address range

Starting IP Address *

Ending IP Address *

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

SNMP v3凭证

Enter SNMP v2c credentials

Read Community *

Enter SSHV2 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

Enter SSHV1 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

SNMP v2、SSHV2和SSHV1凭证

Enter Telnet credentials

Username	Enable Username (Optional)
<input type="text"/>	<input type="text"/>
Password	Enable Password (Optional)
<input type="text"/>	<input type="text"/>

Schedule Inventory Collection

Collection Frequency	Time	IST
Frequency <input type="text"/>	Time <input type="text"/>	IST <input type="text"/>

Run the first collection now (this may take up to 75 minutes)

Connect

Telnet凭证和网络扫描计划

4. 单击 Connect。“数据源”窗口打开，显示一条确认消息。

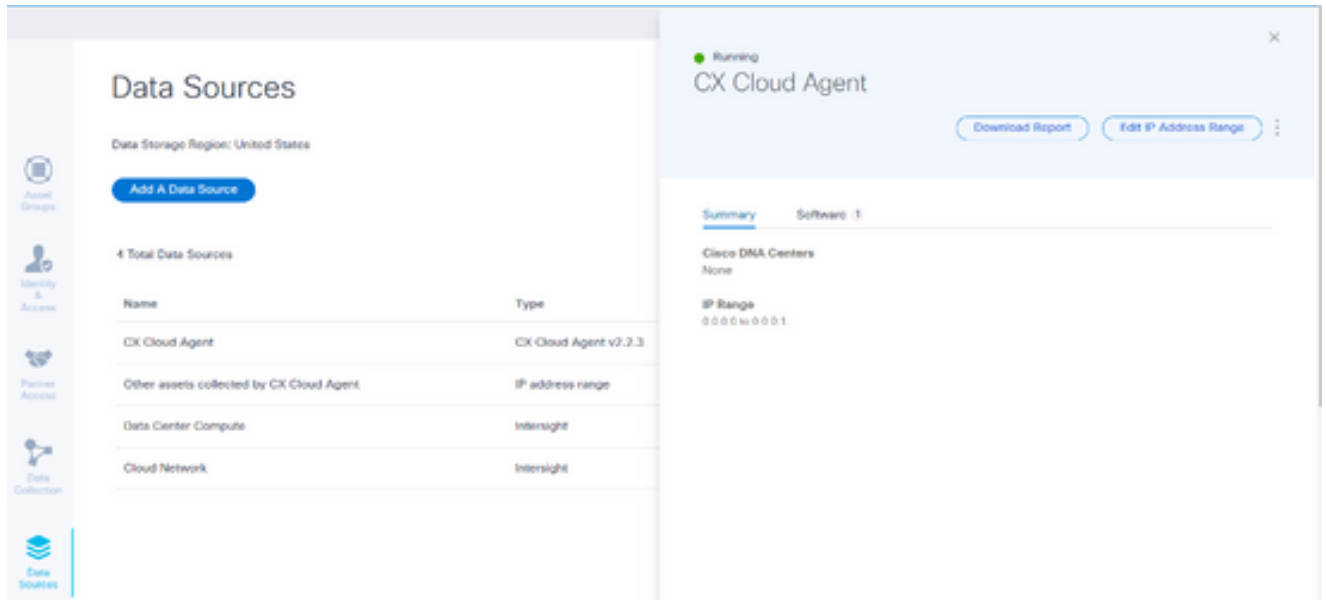
Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.2.0	159 days ago	Not running
10.127.249.145	Cisco DNA Center	159 days ago	Not Available
Contract	Covered Assets	27 days ago	Last Collection Succeeded
Data Center Compute	Intersight	-	First Collection Pending
Cloud Network	Intersight	-	First Collection Pending

确认

编辑IP范围

编辑IP范围；

1. 定位至“数据源”窗口。



数据源

2. 单击需要在“Data Sources”中编辑IP范围的CX Cloud Agent。“详细信息”窗口打开。
3. 单击Edit IP Address Range。“连接到CX云”窗口打开。

[← Back To Data Sources](#)

Connect to CX Cloud

Provide an IP address range

[Edit The Protocols](#)

Enter IP address range

Starting IP address *

0.0.0.0

Ending IP address *

0.0.0.1

Cancel

Continue

提供IP范围

4. 更新起始IP地址和结束IP地址字段中的新IP。
5. 单击Edit the Protocols链接。将会打开“连接到CX云-选择协议”窗口。

[< Back To Data Sources](#)

Connect to CX Cloud

Select a protocol

At least one discovery and collection method are required.

Discovery options

SNMP v3 (recommended)

SNMP v2c

Collection options

SSH v2 (recommended)

SSH v1

Telnet

Cancel

Continue

选择协议

6. 通过点击适当的复选框选择适用的协议。
7. 单击 Continue。“提供IP地址范围”窗口打开。

Provide an IP address range

[Edit The Protocols](#)

Enter IP address range

Starting IP address *

0.0.0.0

Ending IP address *

0.0.0.2

Enter SNMP v2c credentials

Read community *

Enter SSH v1 credentials

Username *

Enable Username (Optional)

Password *

Enable Password (Optional)

Cancel

Connect

输入凭证

8. 输入配置凭证。
9. 单击 Connect。“数据源”窗口打开，显示一条确认消息。

The screenshot shows the Cisco CX Cloud interface. At the top, there's a blue header with the Cisco logo, 'CX Cloud', and 'HQ UNITED STATES'. A search bar is on the right. A notification bubble in the top right corner says 'IP address range updated'. The main content area is titled 'Data Sources' and shows 'Data Storage Region: United States'. There's a search bar for data sources. Below that, it says '4 Total Data Sources'. A table lists the data sources:

Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.2.3	3 minutes ago	Running
Other assets collected by CX Cloud Agent	IP address range	3 minutes ago	1 unreachable
Data Center Compute	Intersight	-	First Collection Pending
Cloud Network	Intersight	-	First Collection Pending

确认

 注意：确认消息无法确保可访问已编辑范围内的设备，并且已接受凭证。

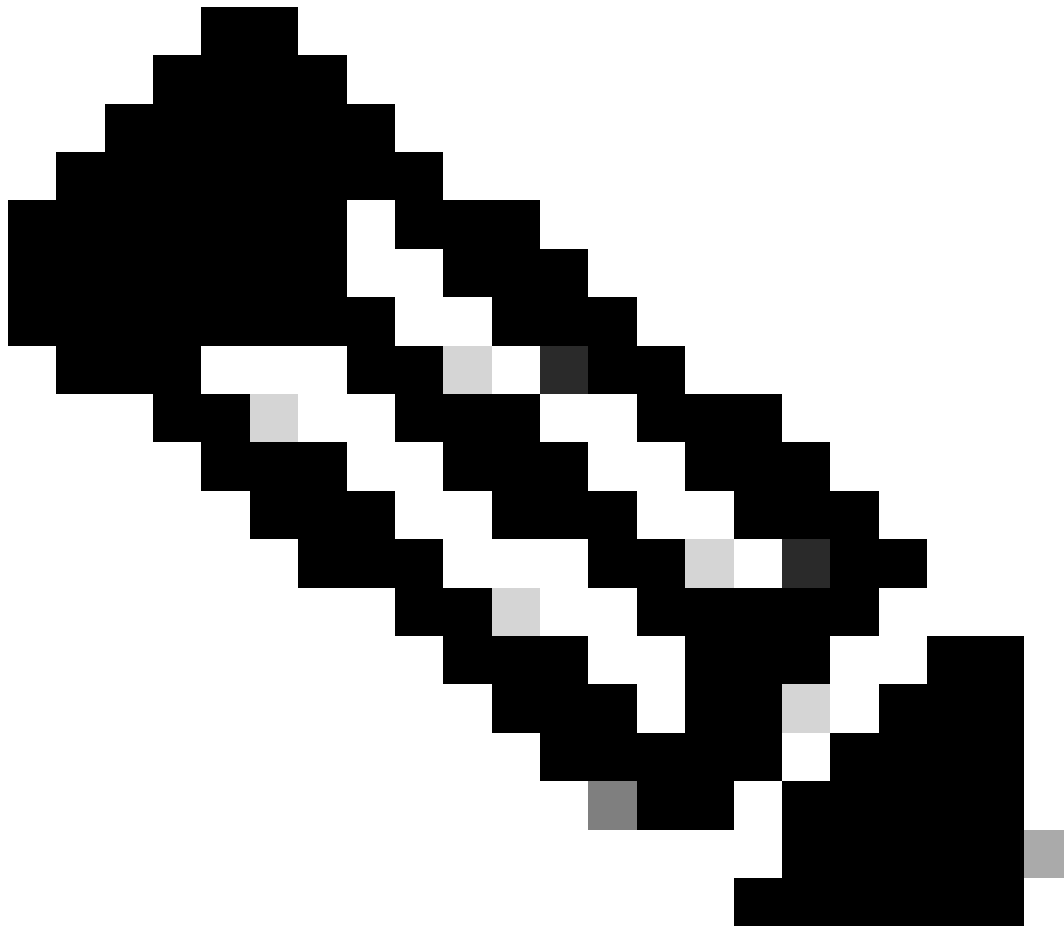
关于从多个控制器中发现的设备

思科DNA中心和与CX云代理的直接设备连接可能会发现某些设备，从而导致从这些设备收集重复数据。为避免收集重复数据，且仅有一个控制器管理设备，需要确定CX Cloud Agent管理设备的优先级。

- 如果设备先由Cisco DNA 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 DNA Center优先控制设备。
- 如果设备首先通过直接连接到CX Cloud Agent被发现，然后由Cisco DNA Center重新发现，则Cisco DNA Center优先控制设备。

安排诊断扫描

客户可以在CX云中安排按需诊断扫描。



注意：思科建议计划诊断扫描或启动按需扫描，时间至少比资产收集计划晚6-7小时，这样扫描就不会重叠。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。

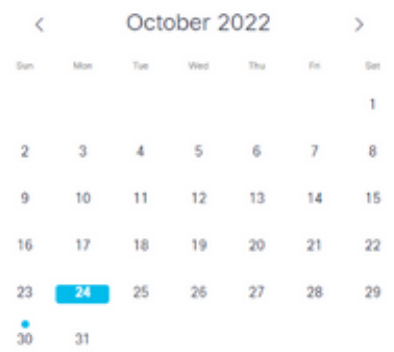
要计划诊断扫描，请执行以下操作：

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。

Data Collection

Diagnostic Scans 3

Schedule Scan



No Diagnostic Scans Found

Inventory Collection 3

3 Collections

Source	Schedule	
Other assets collected by CX Cloud Agent	Monthly on the 30th at 05:30 PM EDT	⋮
10.197.238.127	Monthly on the 30th at 05:00 PM EDT	⋮
22.1.90.1	Monthly on the 30th at 09:00 PM EDT	⋮

Rapid Problem Resolution

Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.

Enable for Campus Network

数据收集

4. 配置此扫描的计划。

Other assets collected by CX Cloud Agent Inventory Collection Details

Schedule History

Weekly on Sunday at 12:00 am EDT
Created: Oct 3, 2022

Save Scheduled Collection

配置扫描计划

5. 在devices列表中，选择要扫描的所有设备，然后单击Add。

New Scheduled Scan

Data Sources
Other assets collected by CX Cloud Agent

Schedule
Frequency: [v] at Time: [v] IST [Save Changes](#)

Description (Optional)

Device	Source IP	IP Address
<input type="checkbox"/> Device_22_0_2_1	10.127.249.156	22.0.2.1
<input type="checkbox"/> Device_22_0_32_1	10.127.249.156	22.0.32.1
<input type="checkbox"/> Device_22_0_36_1	10.127.249.156	22.0.36.1
<input type="checkbox"/> Device_22_0_41_1	10.127.249.156	22.0.41.1
<input type="checkbox"/> Device_22_0_51_1	10.127.249.156	22.0.51.1
<input type="checkbox"/> Device_22_0_55_1	10.127.249.156	22.0.55.1
<input type="checkbox"/> Device_22_0_61_1	10.127.249.156	22.0.61.1
<input type="checkbox"/> Device_22_0_63_1	10.127.249.156	22.0.63.1
<input type="checkbox"/> Device_22_0_64_1	10.127.249.156	22.0.64.1
<input type="checkbox"/> Device_22_0_70_1	10.127.249.156	22.0.70.1

[Add](#) [Remove](#)

Device	Source IP	IP Address
Devices are part of selected list		

1 2 Next

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”(Data Collection)页面编辑和删除。

Data Collection

Diagnostic Scans [Schedule Scan](#)

Asset Count	Source	Schedule
1	10.127.249.152	Not scannable
10	10.127.249.152	Daily at 07:00 PM IST

Inventory Collection

Source	Schedule
Other assets collected by CX Cloud Agent	Daily at 04:00 AM IST
	Daily at 12:30 AM IST
172.20.224.70/live.cisco.com	Monthly on the 9th at 11:30 PM IST
10.127.249.152	Daily at 02:00 AM IST

Rapid Problem Resolution
Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.

Enable for Campus Network

Rapid Problem Resolution for Cloud Network and Data Center Compute is managed in Intersight. Enable or disable tech support bundle collection in Intersight for these Success Tracks.

[View detailed instructions](#)

具有编辑和删除计划选项的数据收集

部署和网络配置

选择以下任一选项以部署CX云代理：

- 要选择VMware vSphere/vCenter Thick Client ESXi 5.5/6.0，请转至[Thick Client](#)
- 要选择VMware vSphere/vCenter Web客户端ESXi 6.0，请转至[Web客户端](#)或[vSphere Center](#)
- 要选择Oracle Virtual Box 5.2.30，请转到[Oracle VM](#)
- 要选择Microsoft Hyper-V，请转至[Hyper-V](#)

OVA 部署

胖客户端 ESXi 5.5/6.0 安装

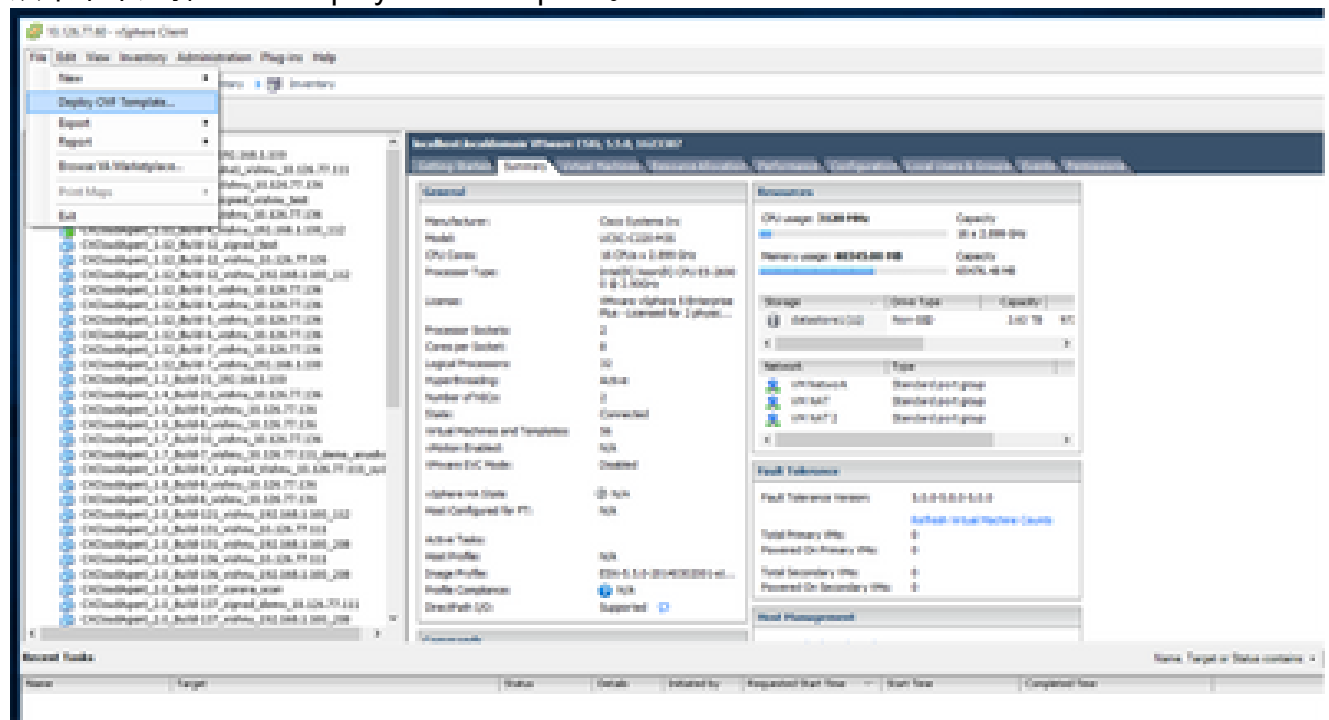
此客户端允许使用vSphere胖客户端部署CX云代理OVA。

1. 下载映像后，启动VMware vSphere客户端并登录。



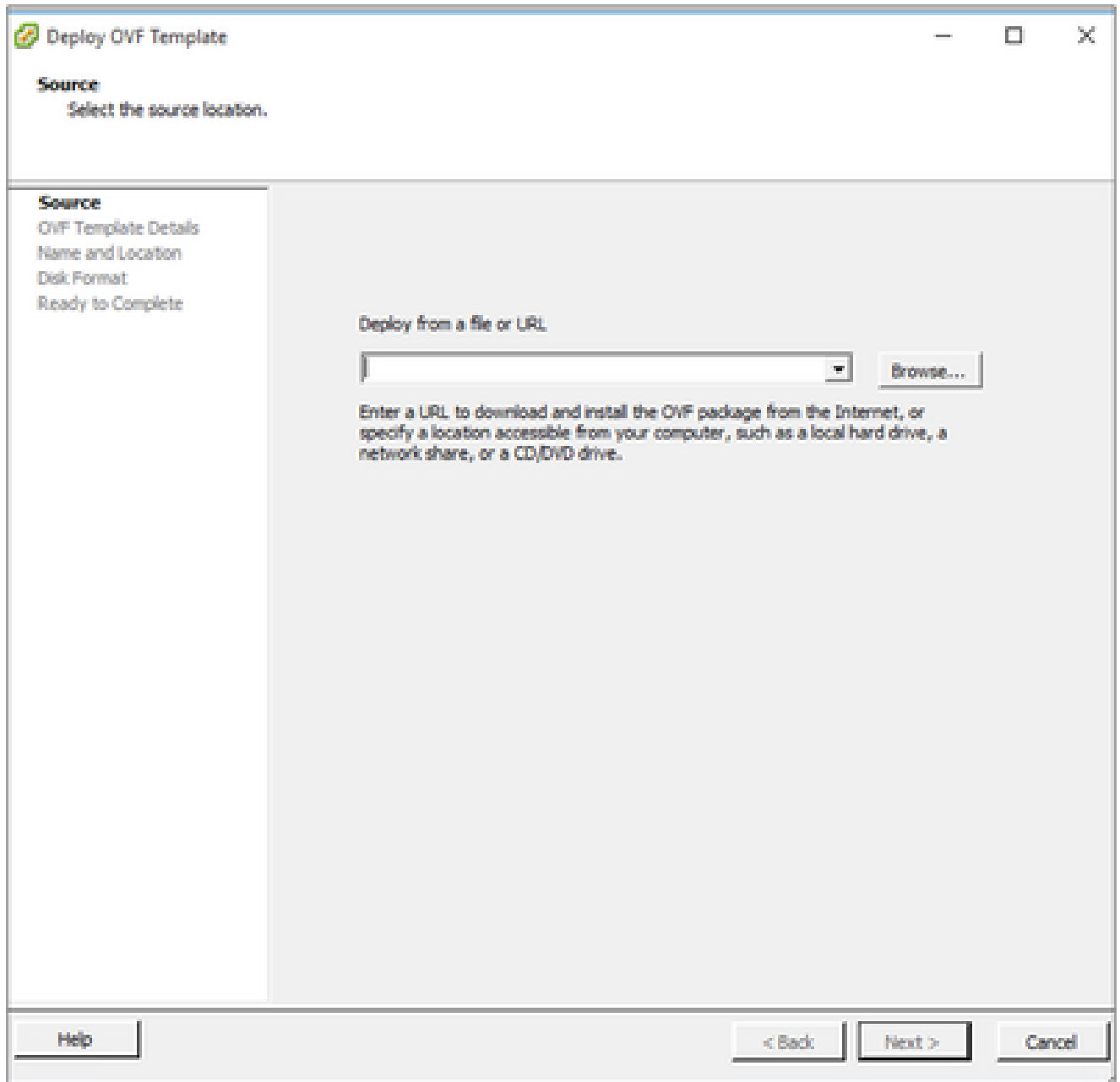
登录

2. 从菜单中选择File > Deploy OVF Template。



vSphere 客户端

3. 浏览并选择OVA文件，然后单击下一步。



OVA 路径

4. 验证OVF详细信息并单击下一步。

OVF Template Details

Verify OVF template details.

SOURCE

OVF Template Details

Name and Location
Disk Format
Network Mapping
Ready to Complete

Product:	CXCloudAgent_2.0_Build-144
Version:	2.0
Vendor:	Cisco Systems, Inc
Publisher:	<input checked="" type="checkbox"/> CISCO SYSTEMS, INC.
Download size:	1.1 GB
Size on disk:	3.1 GB (thin provisioned) 200.0 GB (thick provisioned)
Description:	CXCloudAgent_2.0_Build-144

Help < Back Next > Cancel

模板详细信息

5. 输入唯一名称并单击下一步。

Name and Location

Specify a name and location for the deployed template

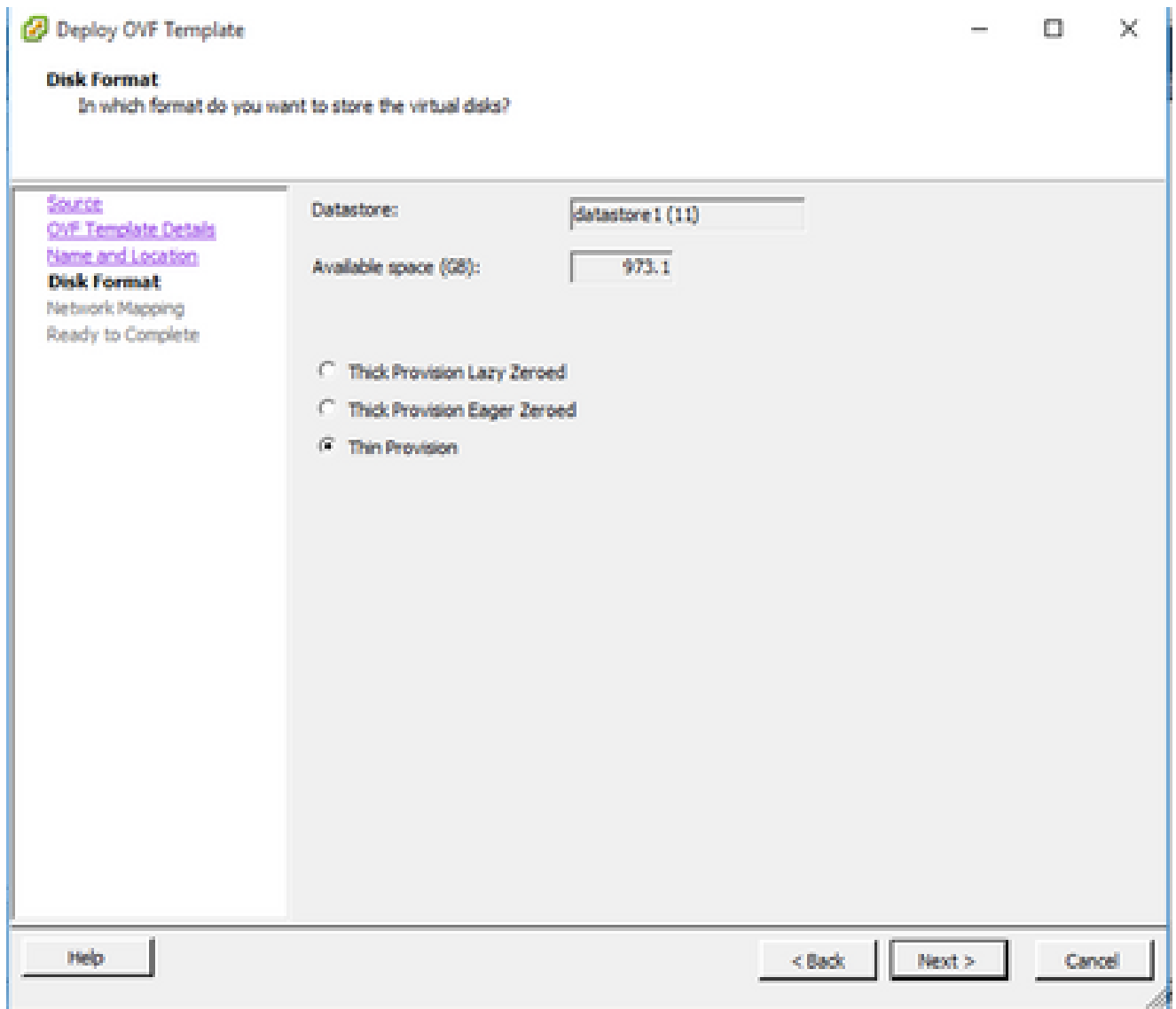
Source
[OVF Template Details](#)
Name and Location
Disk Format
Network Mapping
Ready to Complete

Name:

The name can contain up to 80 characters and it must be unique within the inventory folder.

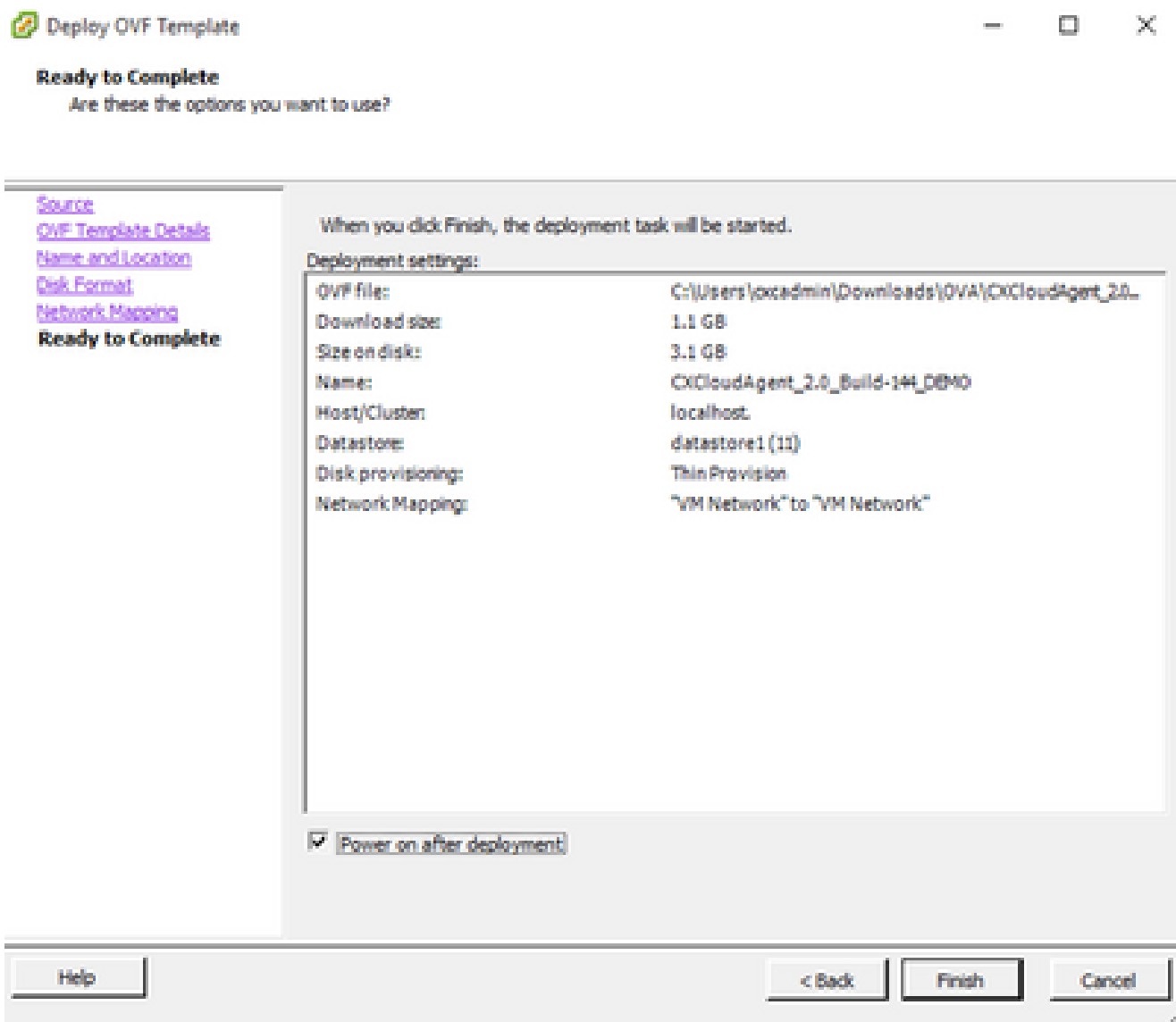
名称和位置

6. 选择Disk Format，然后单击Next（建议使用精简配置）。



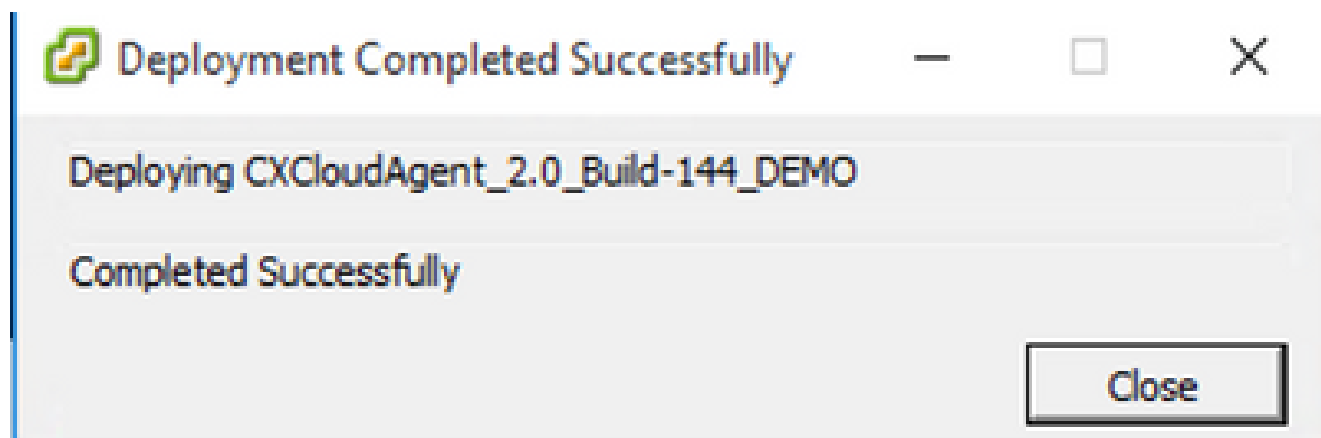
磁盘格式化

7. 选中Power on after deployment复选框并单击Close。



准备完成

部署可能需要几分钟。成功部署后显示确认。



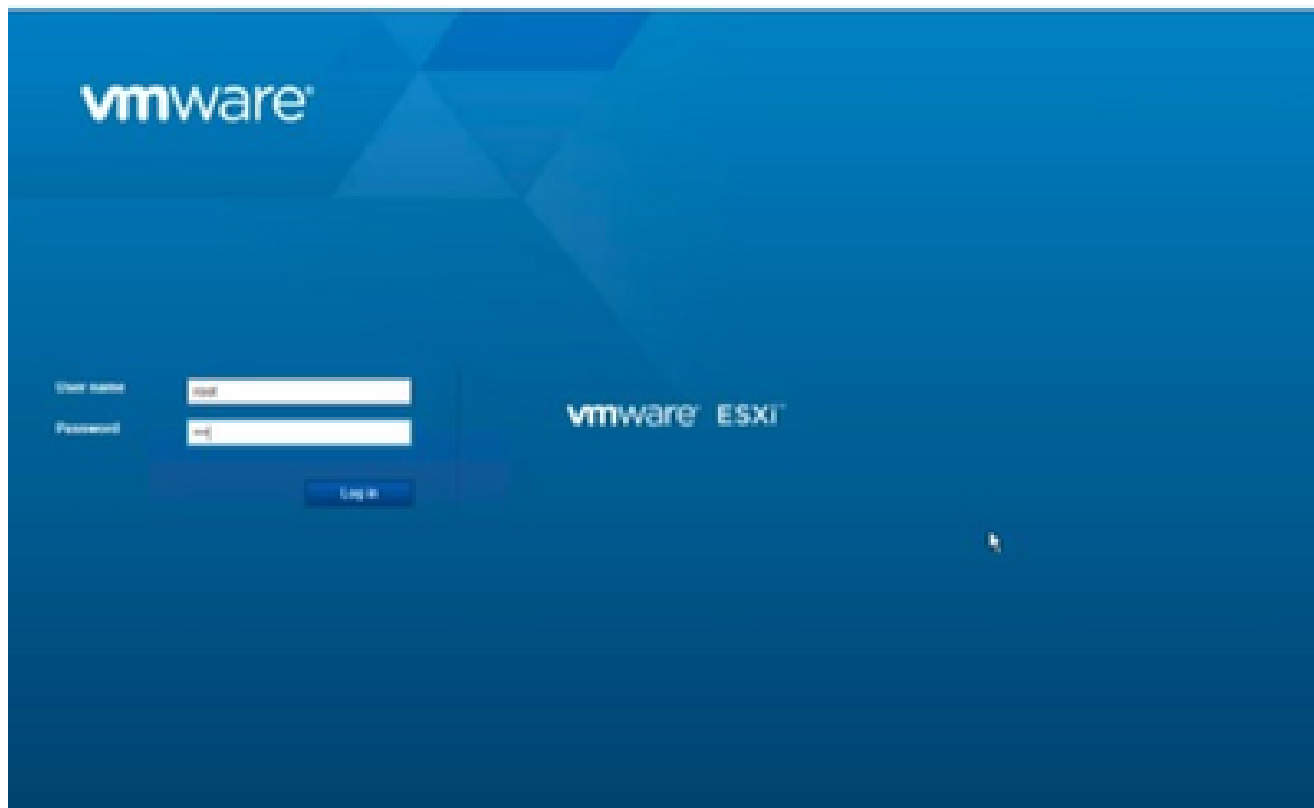
部署完成

8. 选择已部署的VM，打开控制台，然后转到[网络配置](#)以继续执行下一步。

Web 客户端 ESXi 6.0 安装

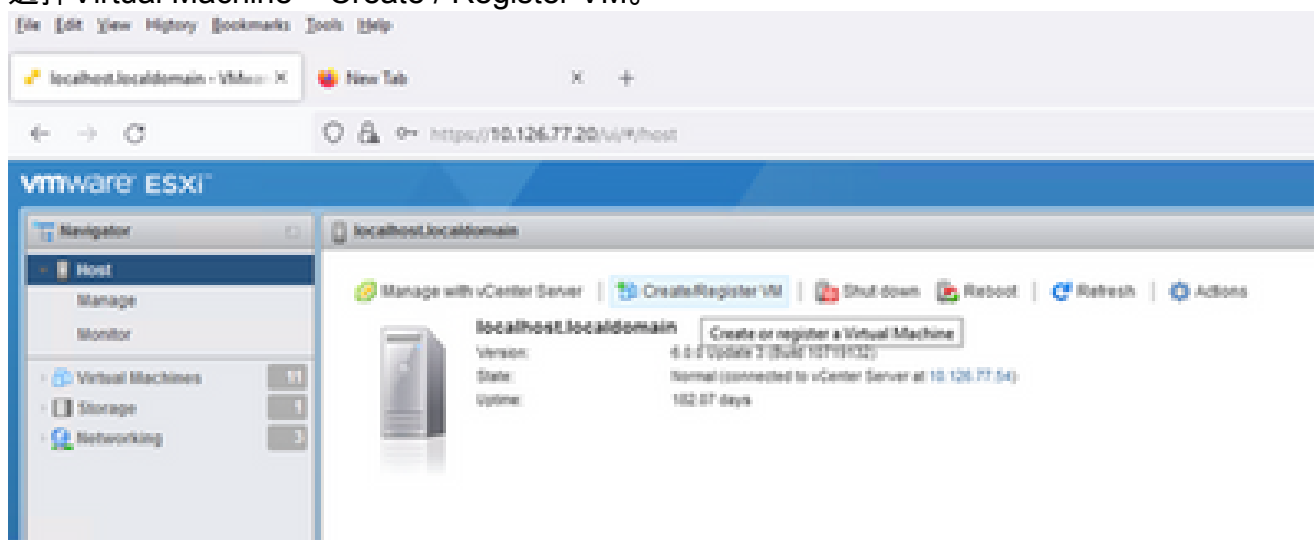
此客户端使用vSphere Web部署CX云代理OVA。

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



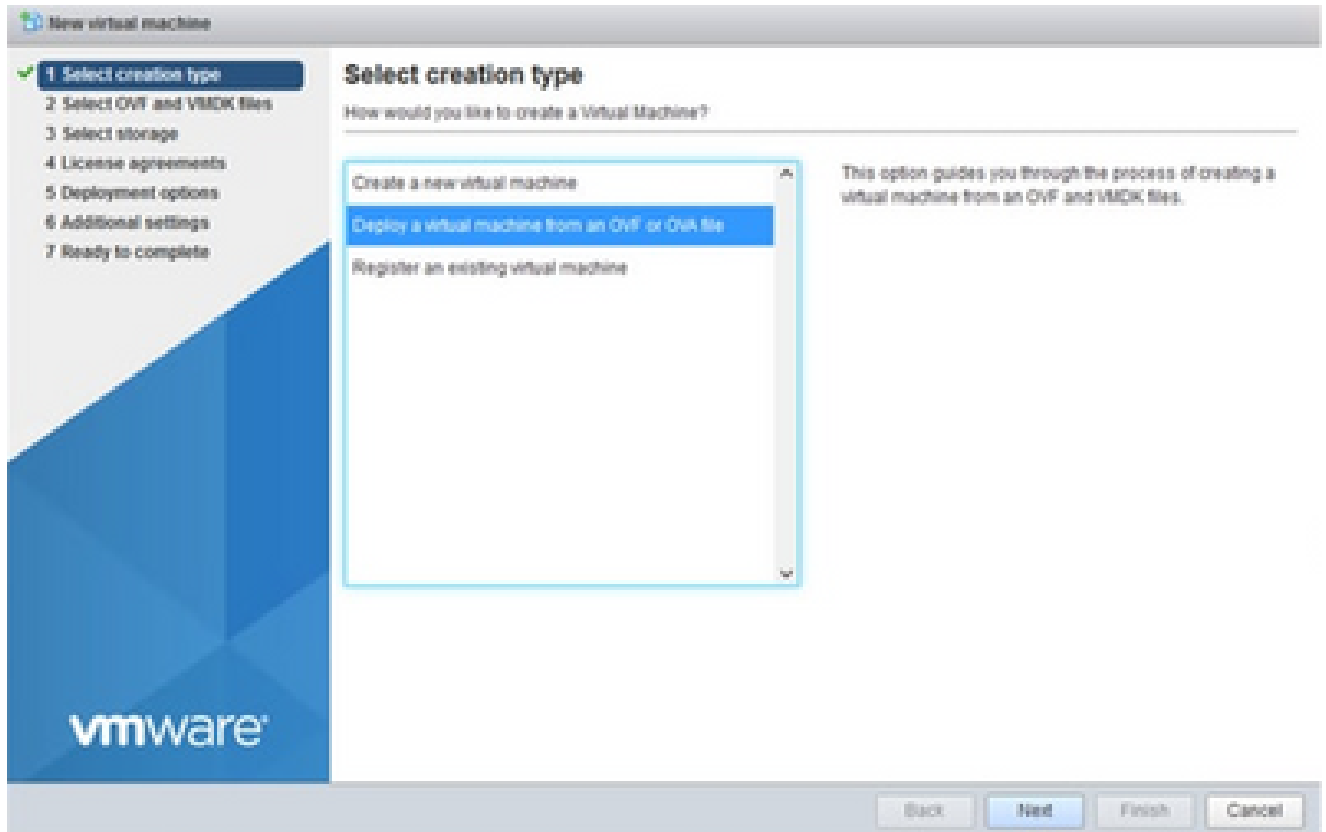
VMware ESXi 登录

2. 选择Virtual Machine > Create / Register VM。



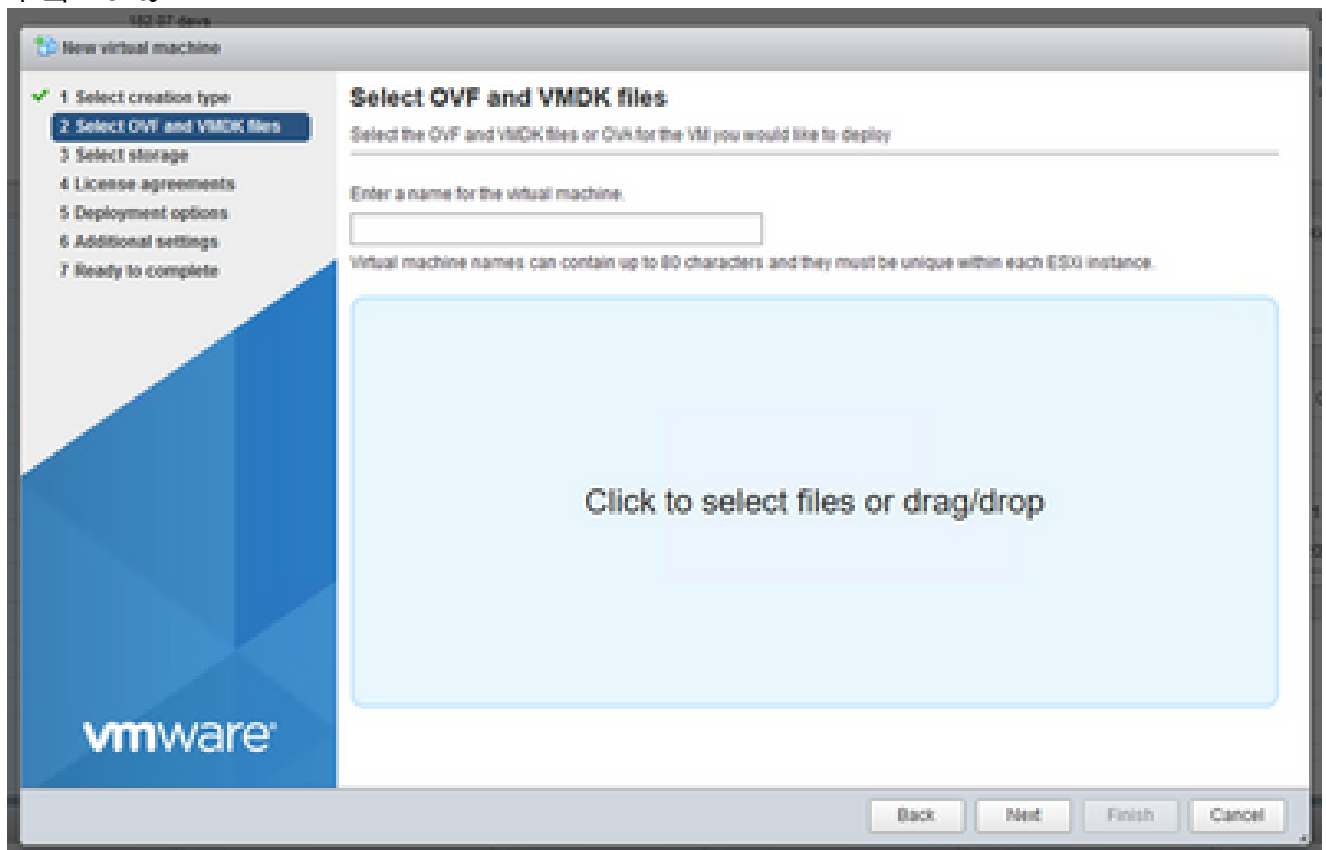
创建 VM

3. 选择通过 OVF 或 OVA 文件部署虚拟机，然后点击下一步。



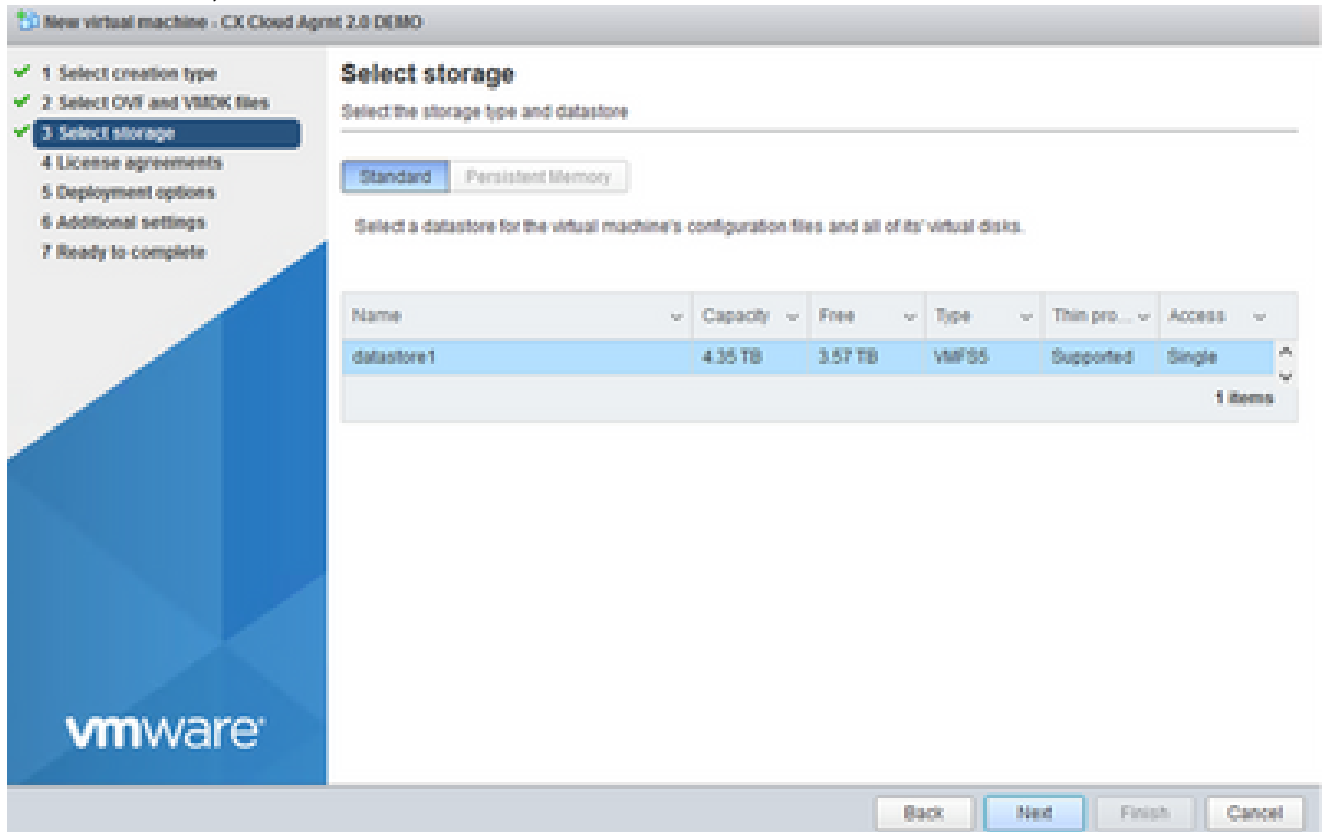
选择创建类型

4. 输入VM的名称，浏览以选择文件，或拖放下载的OVA文件。
5. 单击 Next。



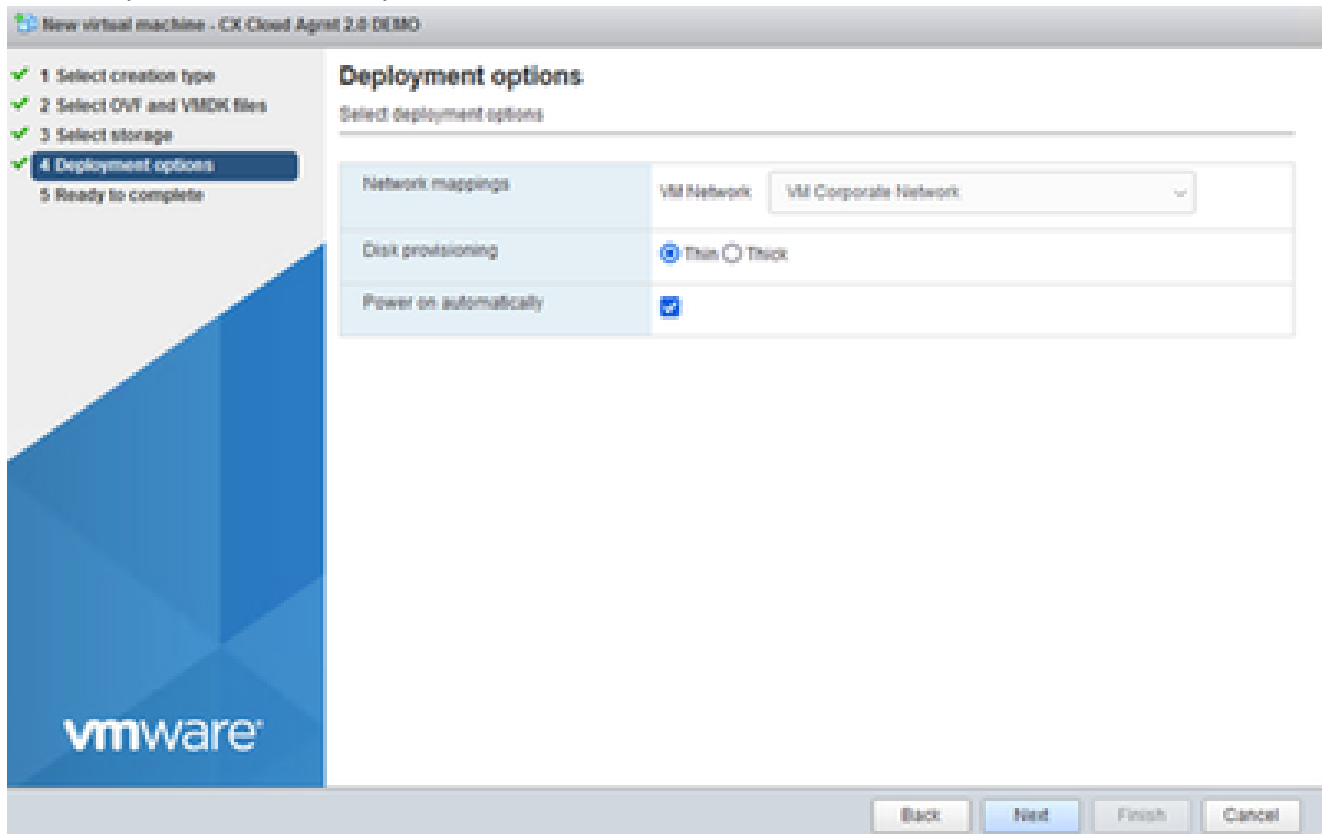
OVA 选择

6. 选择标准存储，然后单击下一步。



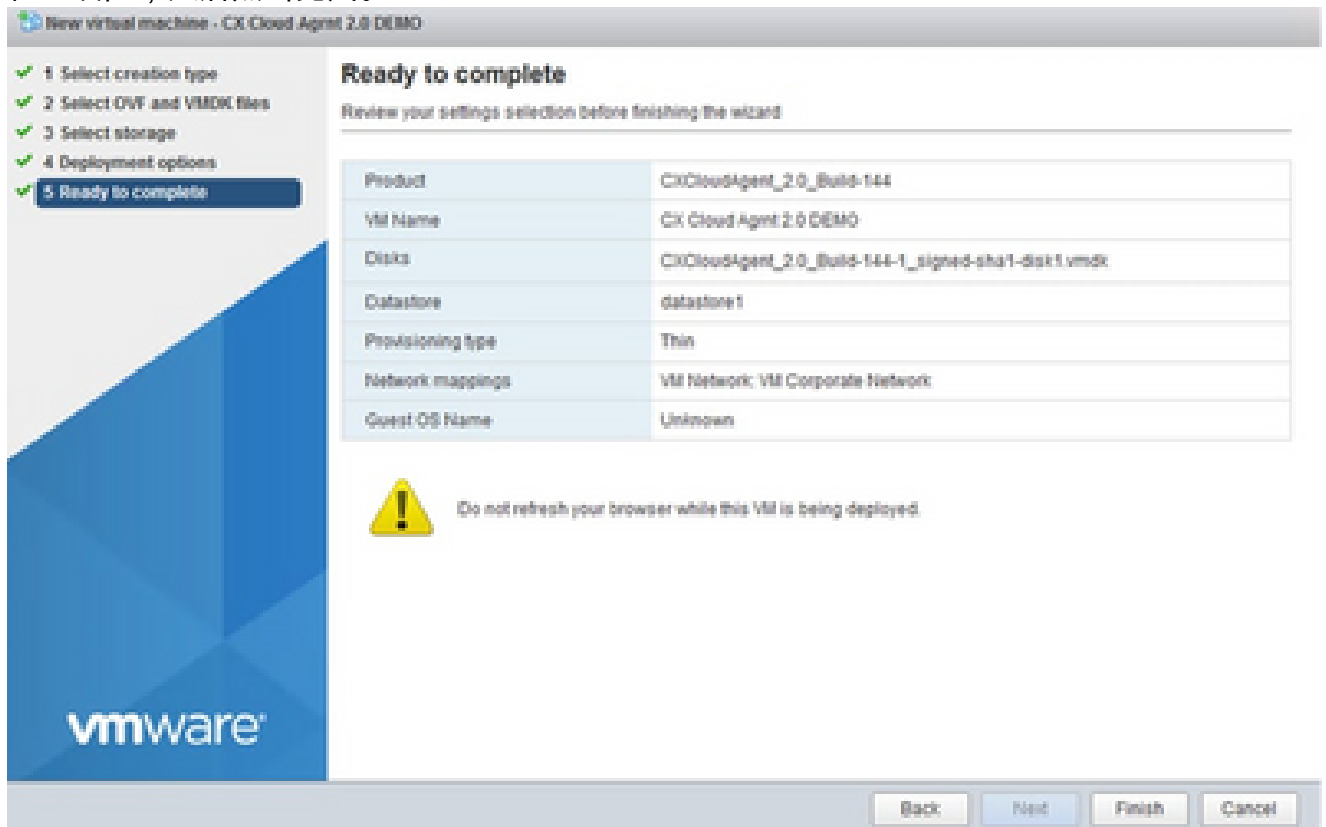
选择存储

7. 选择适当的部署选项并单击下一步。

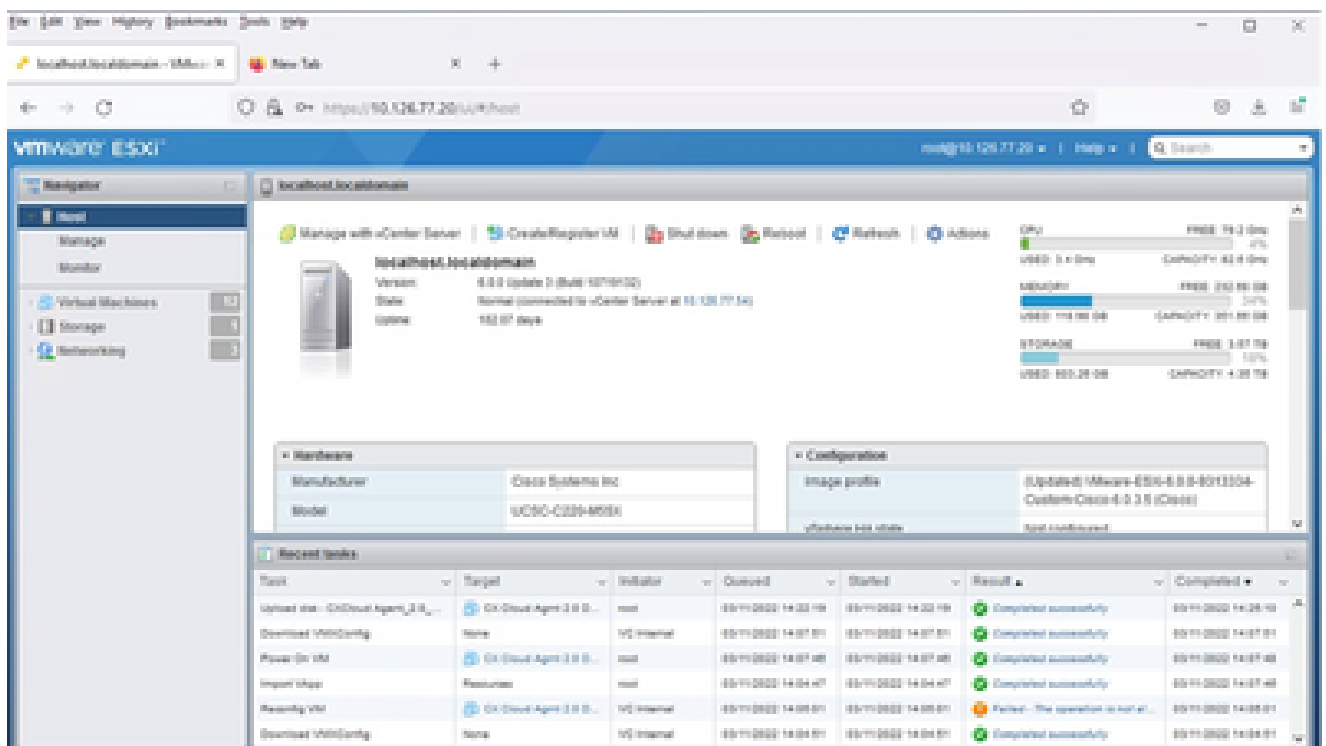


部署选项

8. 检查设置，然后点击完成。

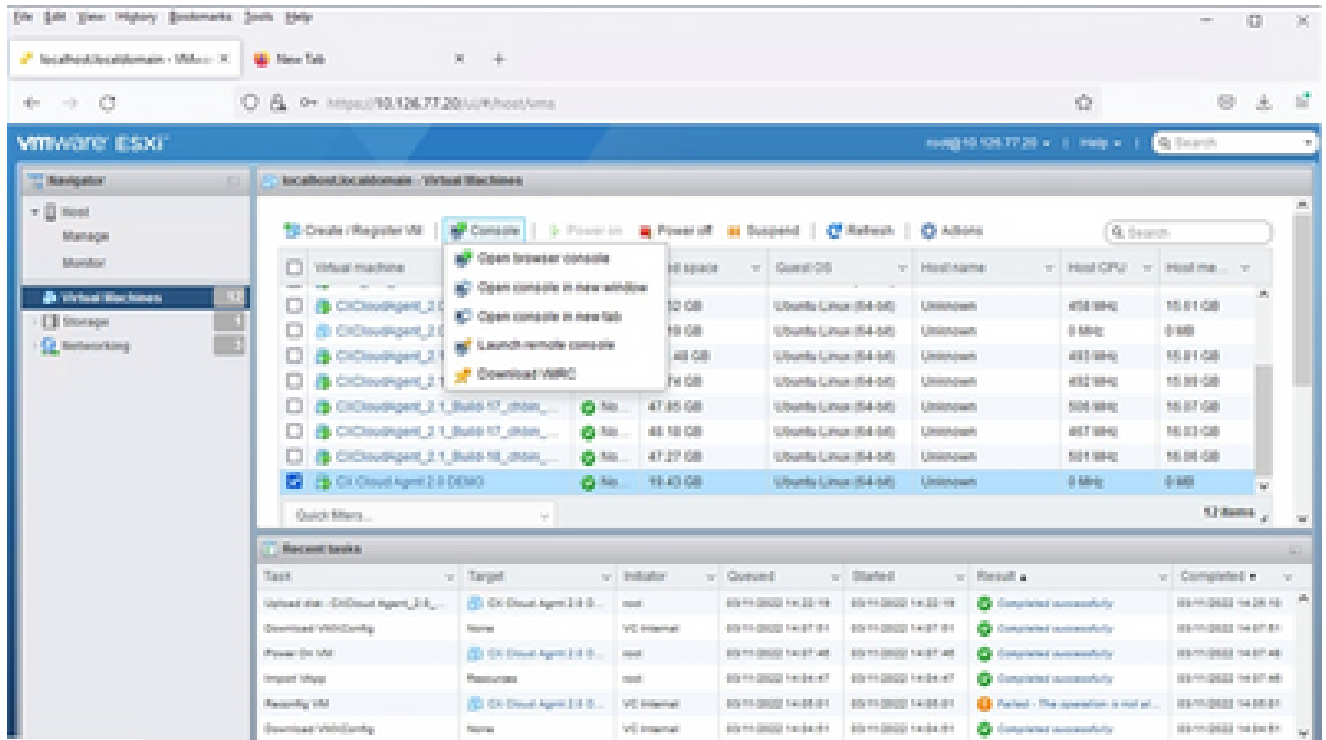


准备完成



成功完成

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



控制台

10. 导航到[网络配置](#)以继续执行下一步。

Web 客户端 vCenter 安装

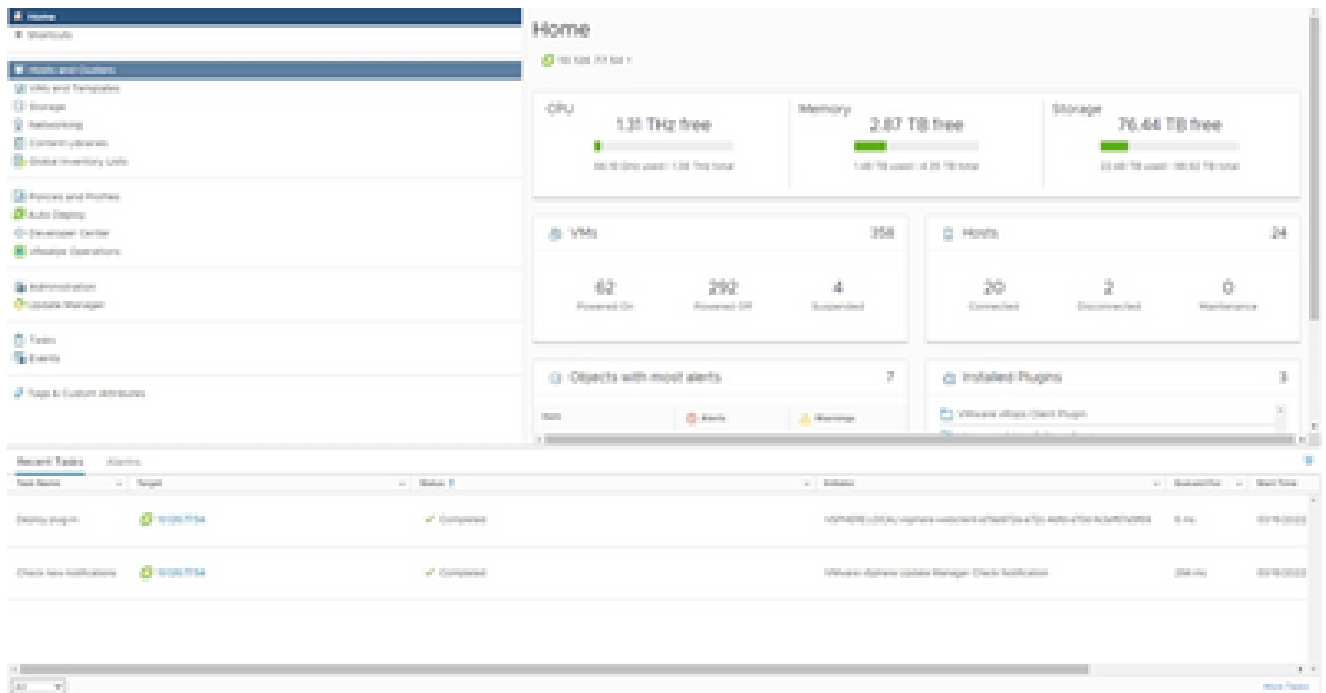
请执行以下步骤：

1. 使用ESXi/虚拟机监控程序凭证登录vCenter客户端。



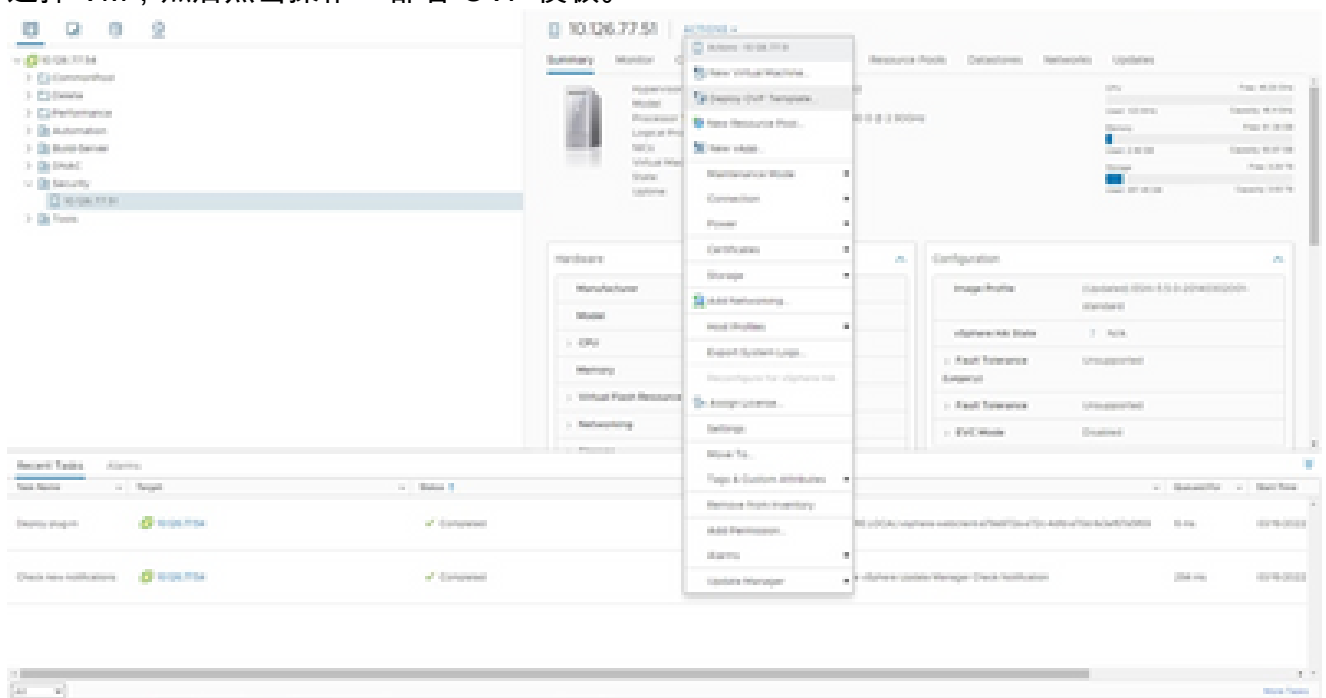
登录

2. 在主页中，单击主机和集群。

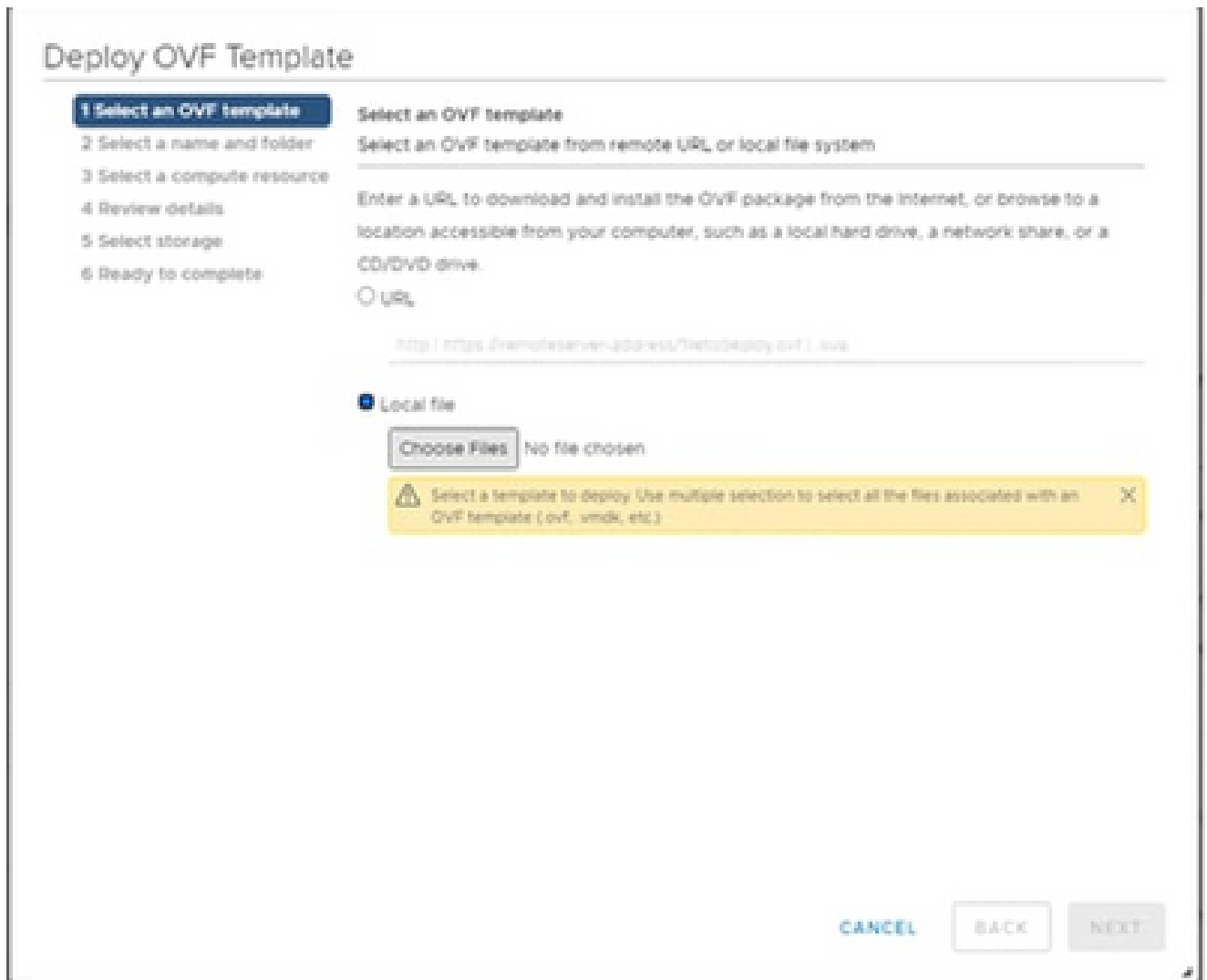


主页

3. 选择 VM，然后点击操作 > 部署 OVF 模板。



操作



选择模板

4. 直接添加URL或浏览以选择OVA文件，然后单击Next。
5. 输入唯一名称，并根据需要浏览至该位置。
6. 单击 Next。

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

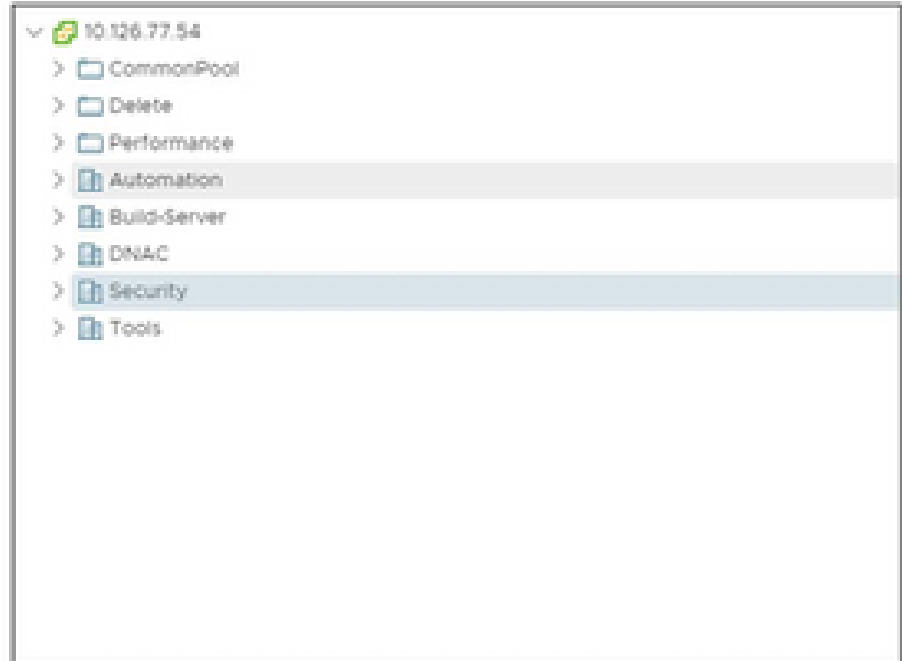
6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: CXCloudAgent_2.0_Build-144-demo

Select a location for the virtual machine.



CANCEL

BACK

NEXT

名称和文件夹


7. 选择计算资源并单击下一步。


Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource**
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

▼  Security

>  10.126.77.51

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

选择计算机资源

8. 检查详细信息，然后点击下一步。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Review details

Verify the template details.

Publisher	DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate)
Product	CxCloudAgent_3.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CxCloudAgent_3.0_Build-144
Download size	1.1 GB
Size on disk	3.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

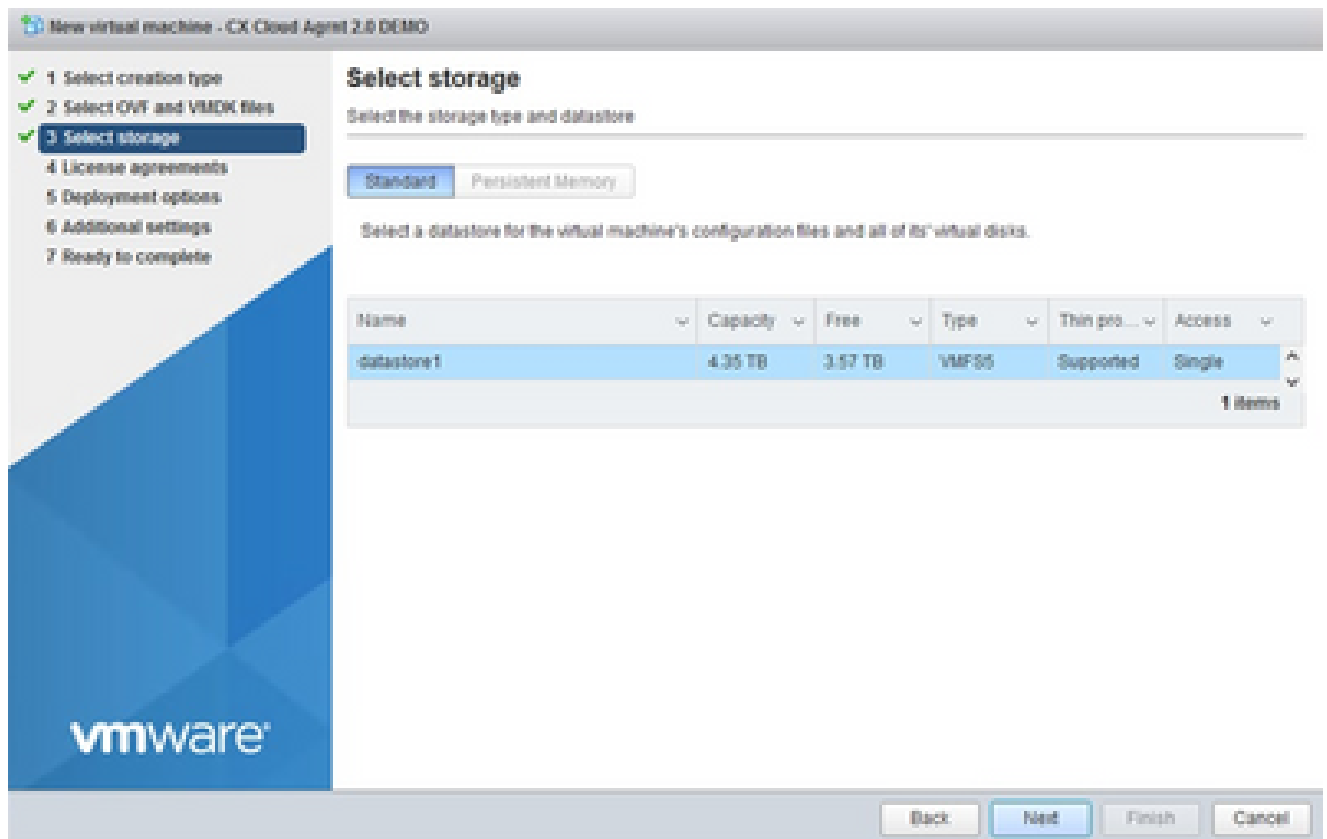
CANCEL

BACK

NEXT

检查详细信息

9. 选择虚拟磁盘格式，然后点击下一步。



选择存储

10. 单击 Next。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Review details

Verify the template details.

Publisher	DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate)
Product	CxCloudAgent_3.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CxCloudAgent_3.0_Build-144
Download size	1.1 GB
Size on disk	3.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

CANCEL

BACK

NEXT

选择网络

11. 单击 完成。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Ready to complete**

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	CxCloudAgent_2.0_Build-144-demo
Template name	CxCloudAgent_2.0_Build-144-1_signed-sha1
Download size	11 GB
Size on disk	3.1 GB
Folder	Security
Resource	10.126.77.51
Storage mapping	1
All disks	Datastore: datastore1 (23); Format: Thin provision
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

CANCEL

BACK

FINISH

准备完成

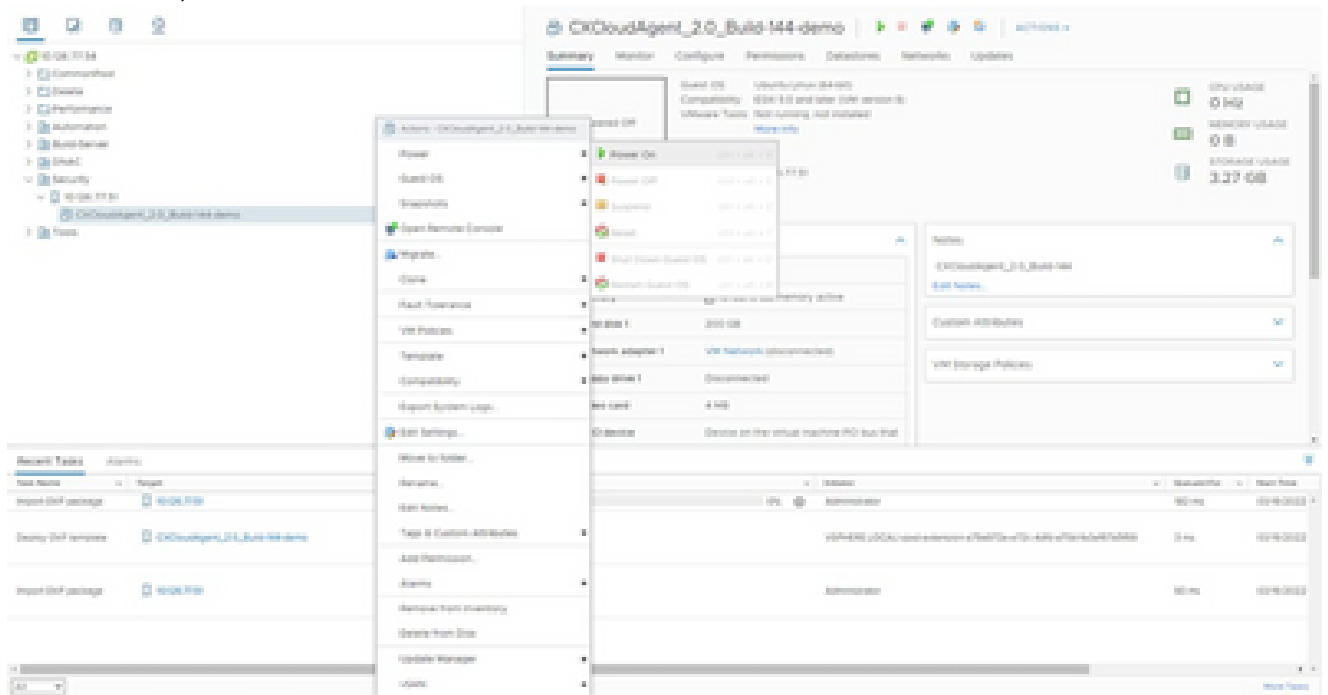
12. 点击新添加的虚拟机的名称以查看状态。

The screenshot shows the vSphere interface for a newly created VM named "CxCloudAgent_2.0_Build-144-demo". The VM is currently powered off. The interface displays various settings including VM Hardware (CPU, Memory, Hard disk, Network adapter, Floppy disk, Video card, VMX gene) and Notes. A table at the bottom shows the status of the VM as "Completed".

VM Name	Power	Status	VMX File	VMX File Location	Size	Created
CxCloudAgent_2.0_Build-144-demo	Off	Completed	CxCloudAgent_2.0_Build-144-demo.vmx	10.126.77.51	3.1 GB	12/18/2022

已添加VM

13. 安装完成后，打开VM的电源并打开控制台。



打开控制台

14. 导航到网络配置以继续执行下一步。

Oracle Virtual Box 5.2.30 安装

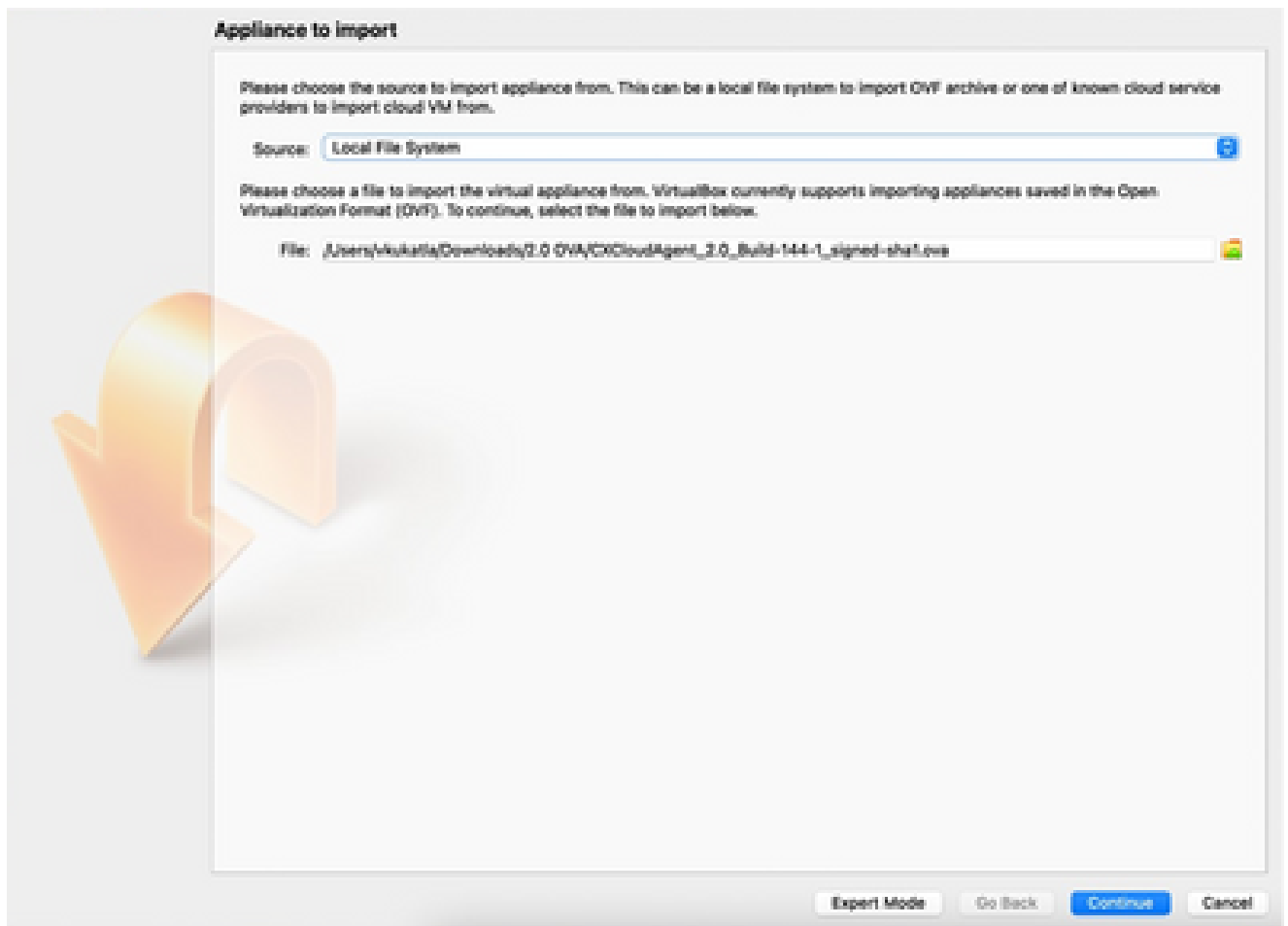
此客户端通过Oracle虚拟盒部署CX云代理OVA。

1. 打开Oracle VM UI，然后选择文件>导入设备。



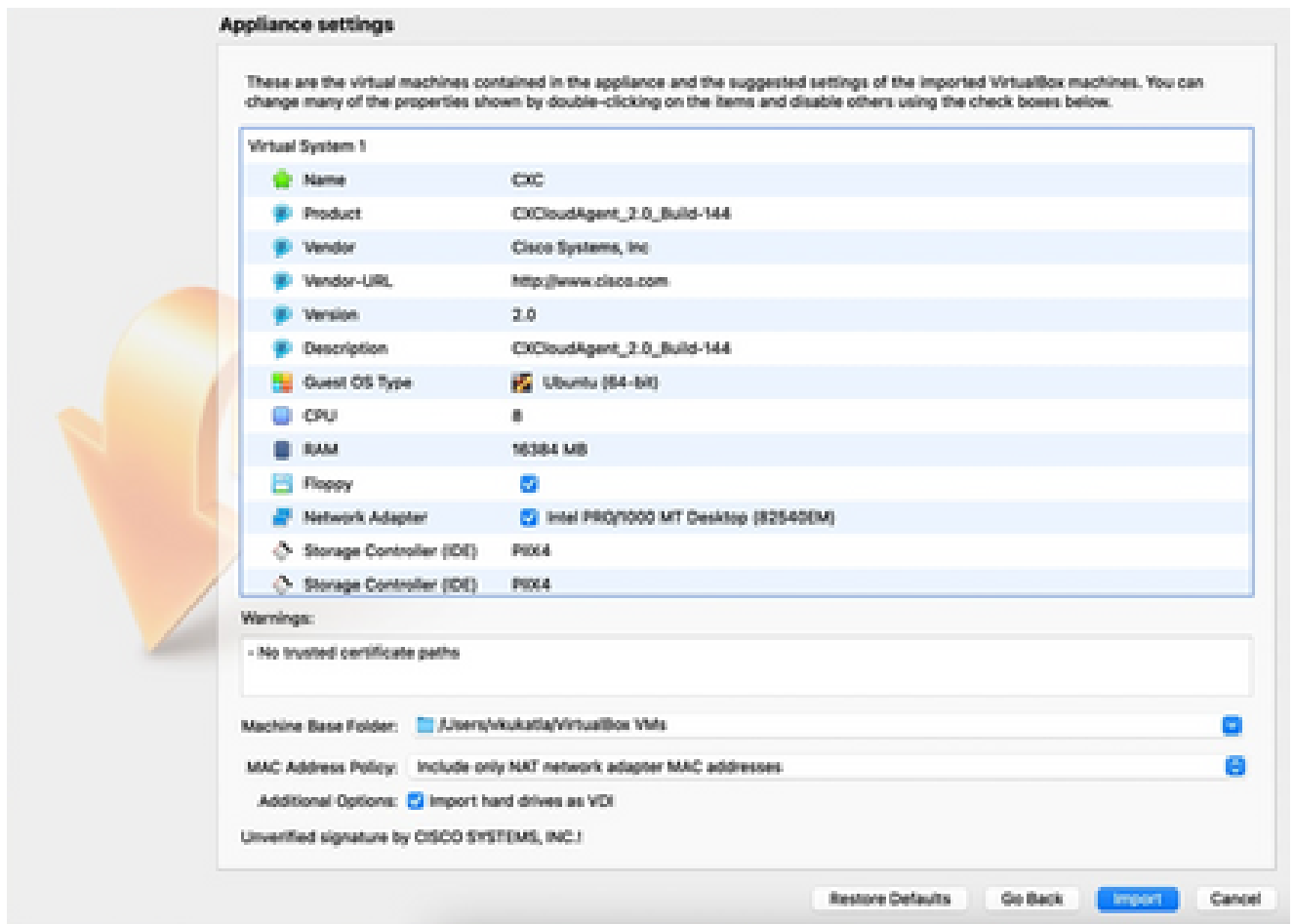
Oracle VM

2. 浏览以导入 OVA 文件。



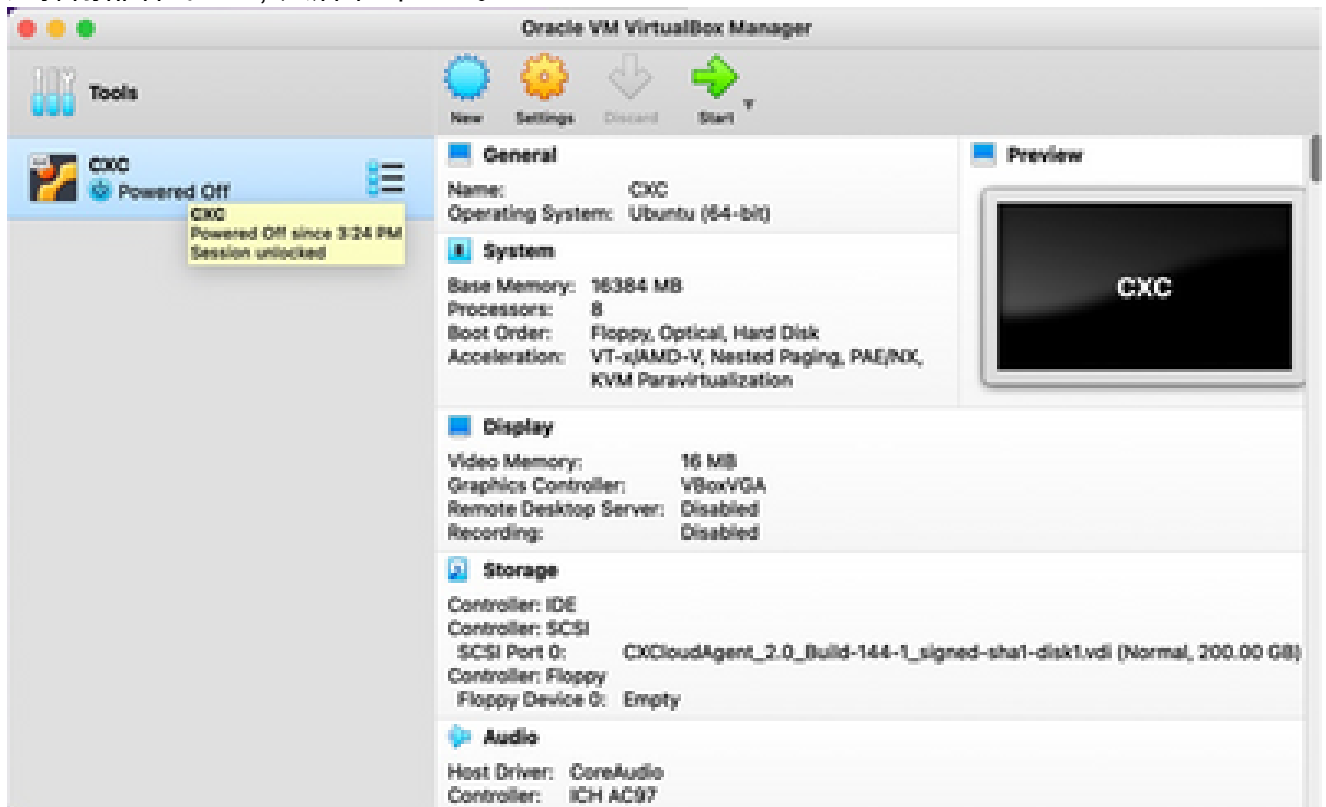
选择文件

3. 单击 Import。

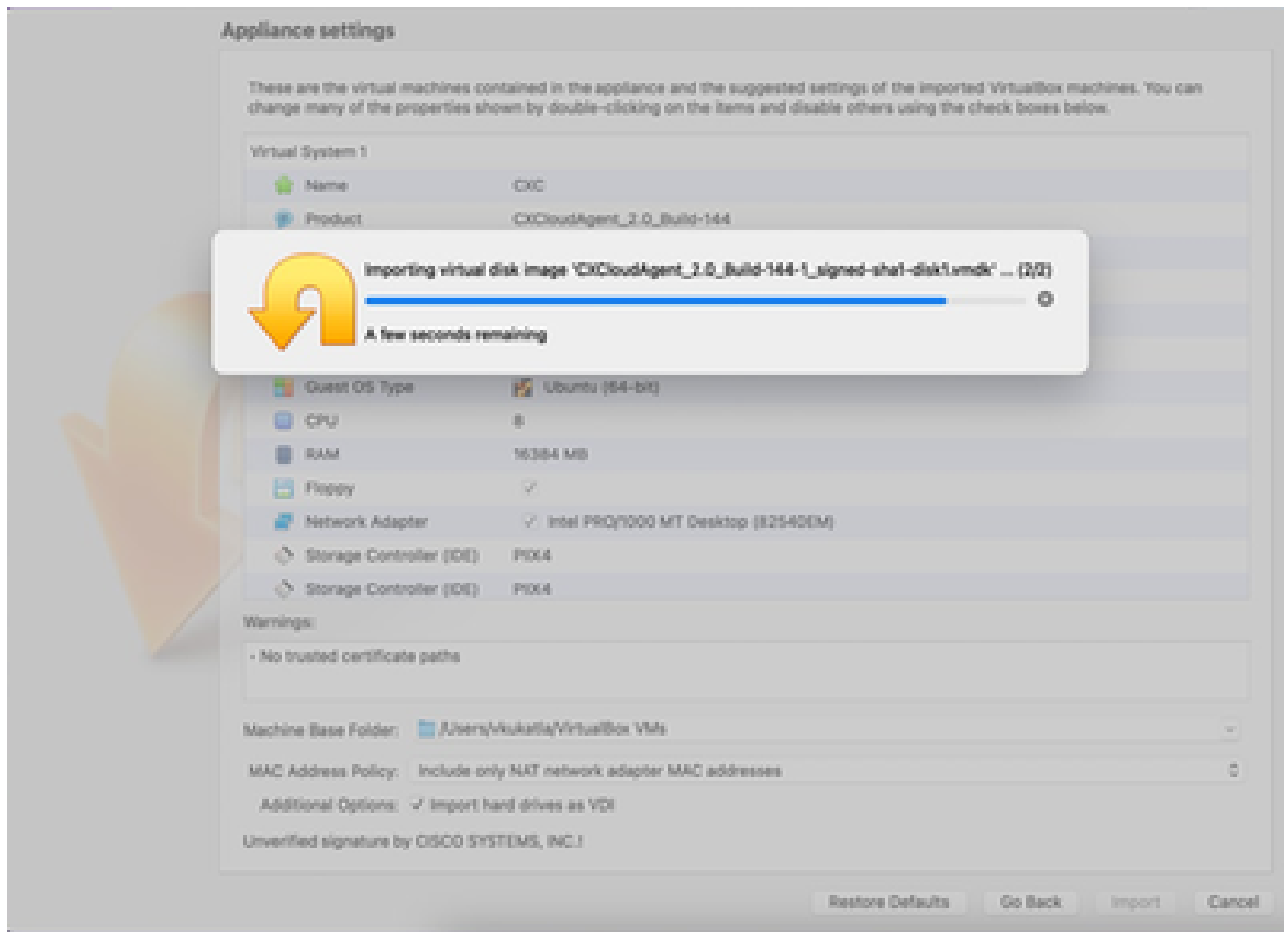


导入文件

4. 选择刚部署的VM，然后单击Start。

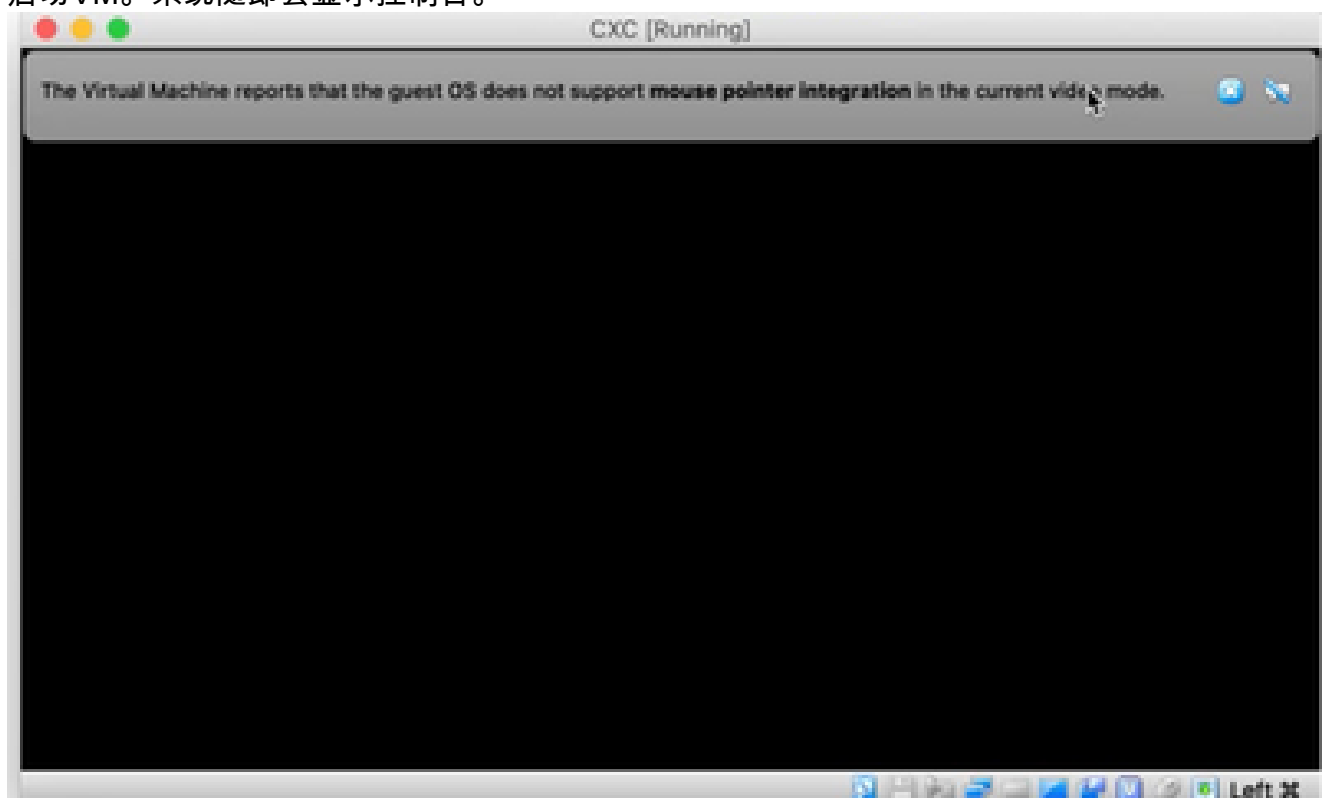


VM 控制台启动



正在导入

5. 启动VM。系统随即会显示控制台。



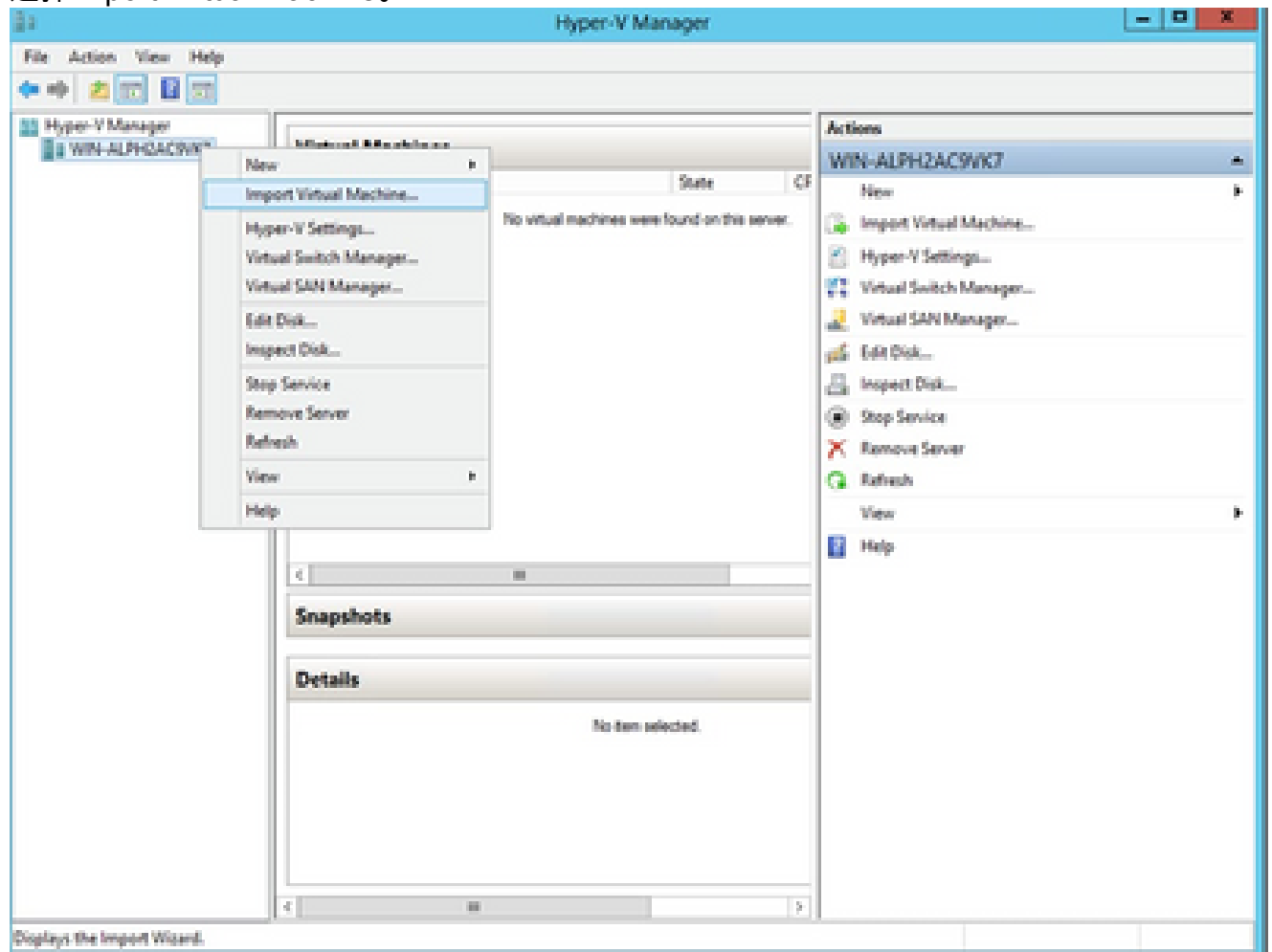
打开控制台

6. 导航到[网络配置](#)以继续执行下一步。

Microsoft Hyper-V 安装

请执行以下步骤：

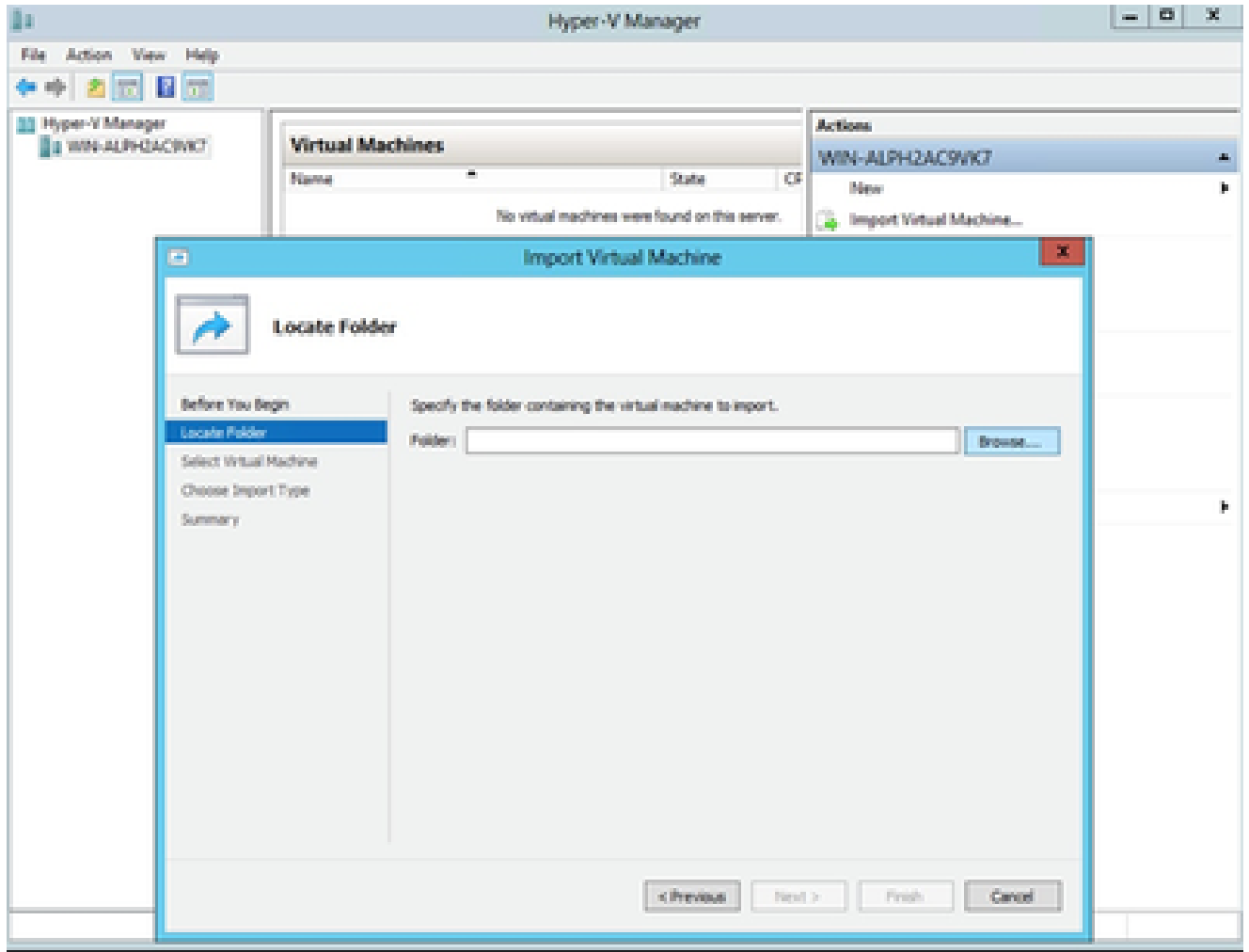
1. 选择Import Virtual Machine。



Hyper V管理器

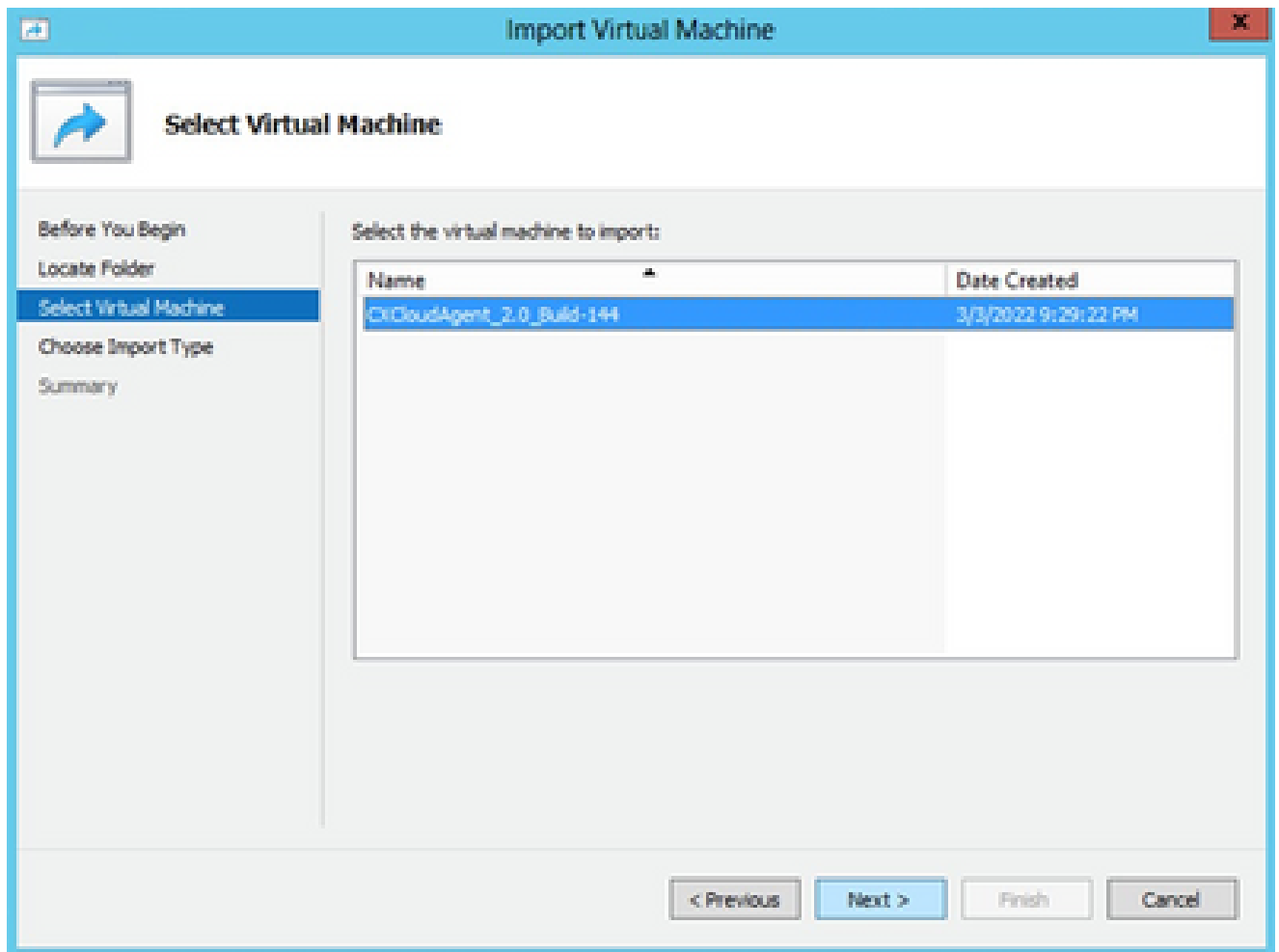
2. 浏览并选择下载文件夹。

3. 单击 Next。



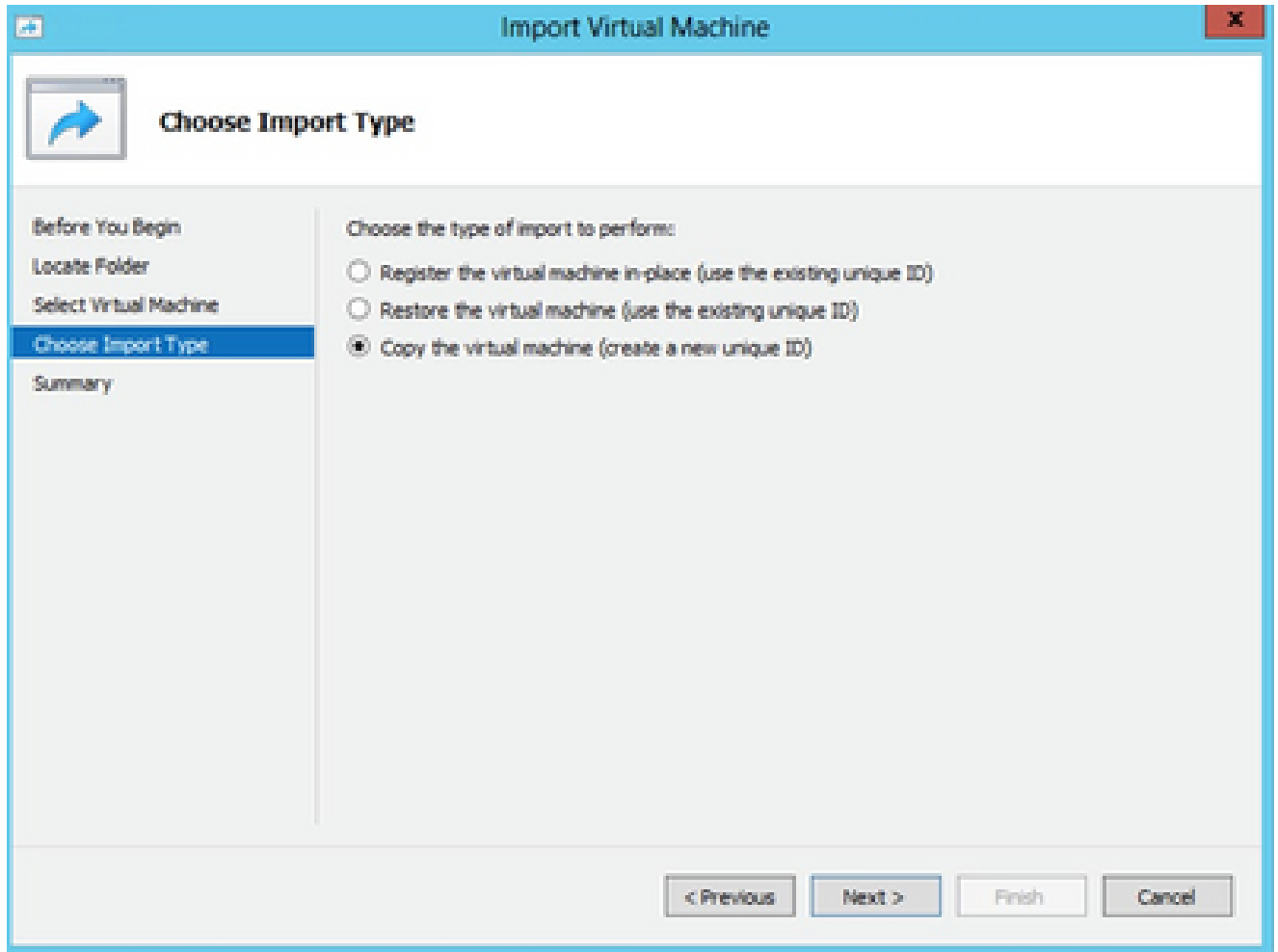
要导入的文件夹

4. 选择VM，然后点击下一步。



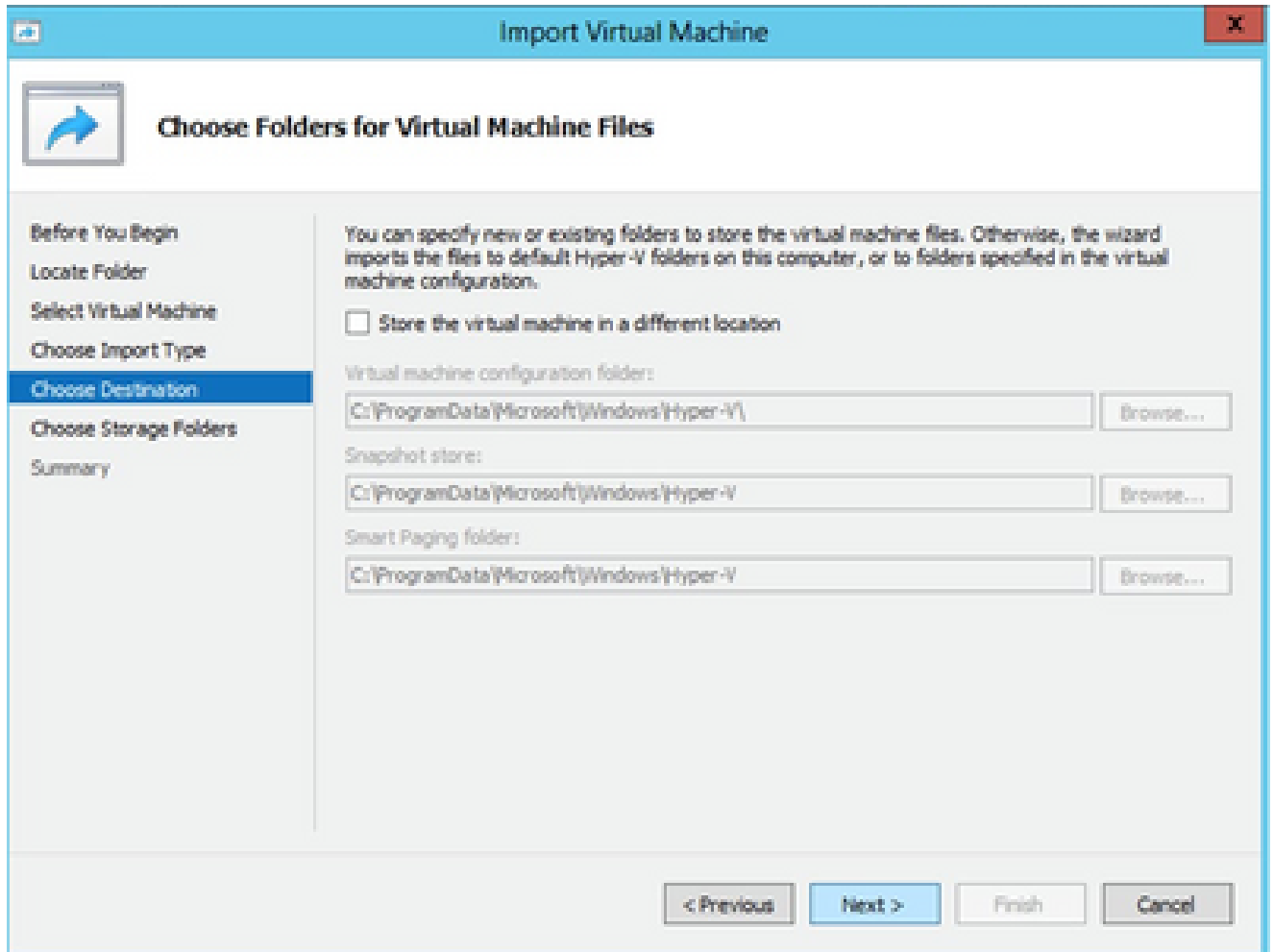
选择 VM

5. 选择Copy the virtual machine (create a new unique ID) 单选按钮，然后单击Next。



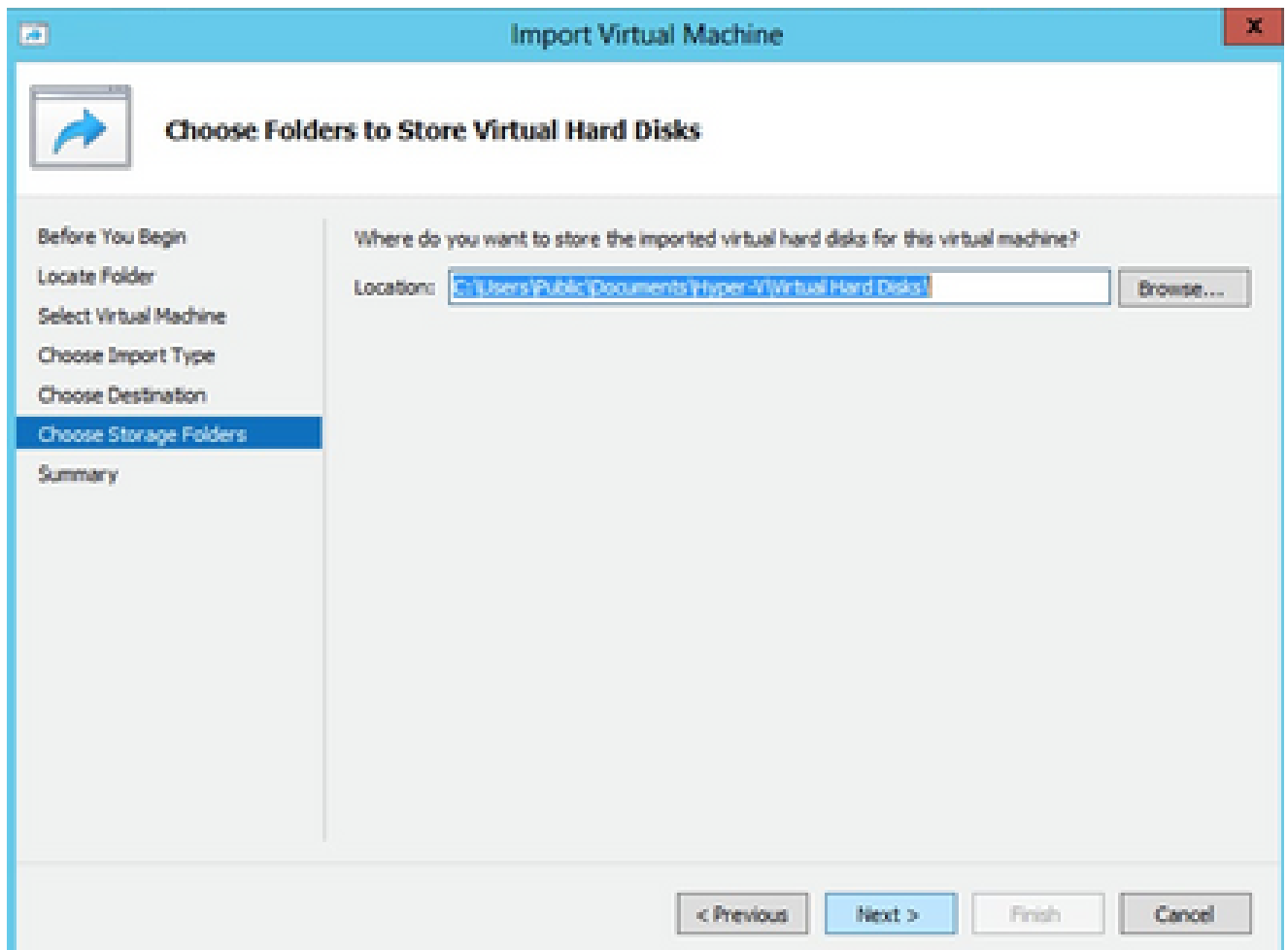
导入类型

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。



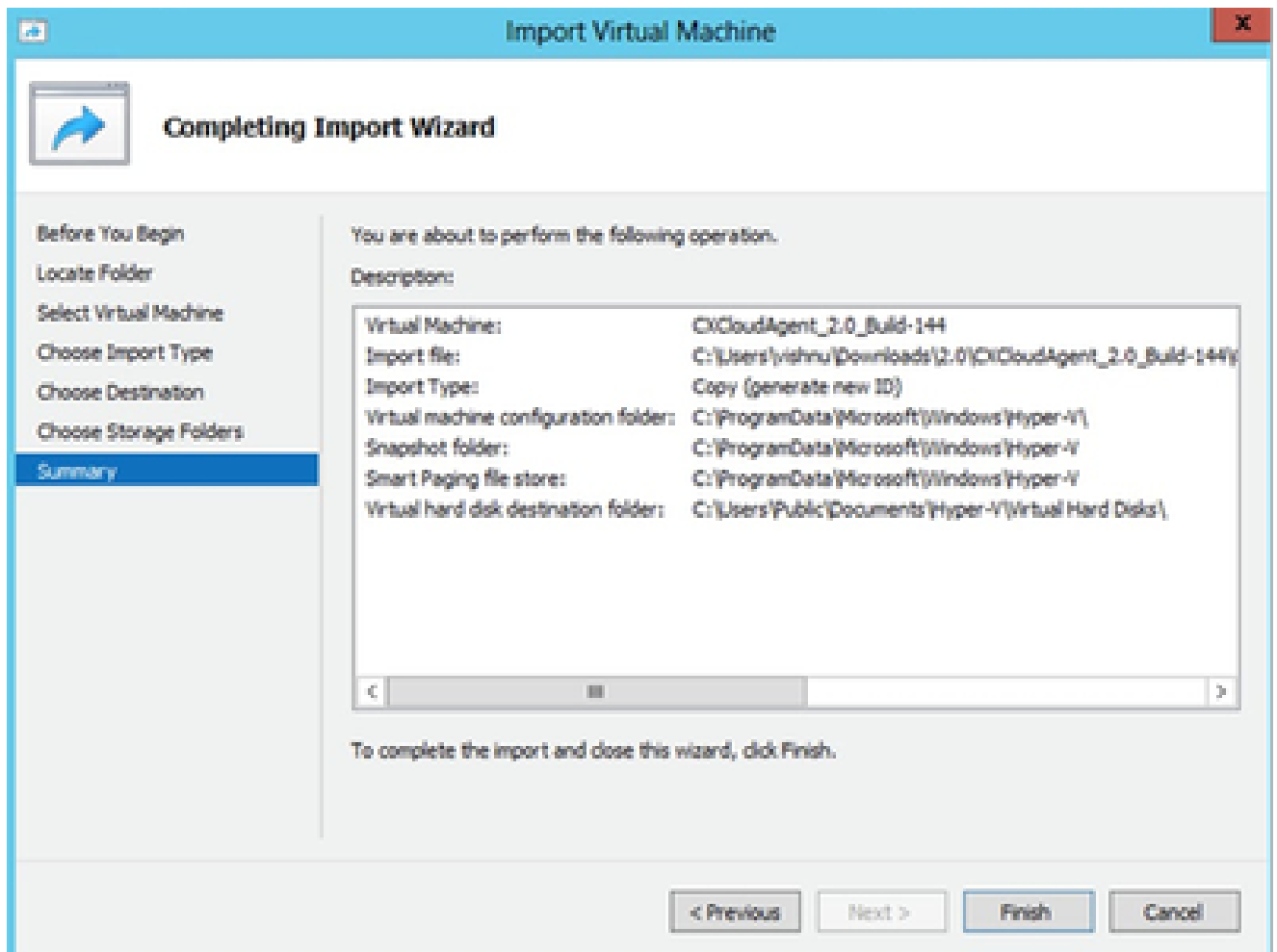
选择虚拟机文件的文件夹

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。



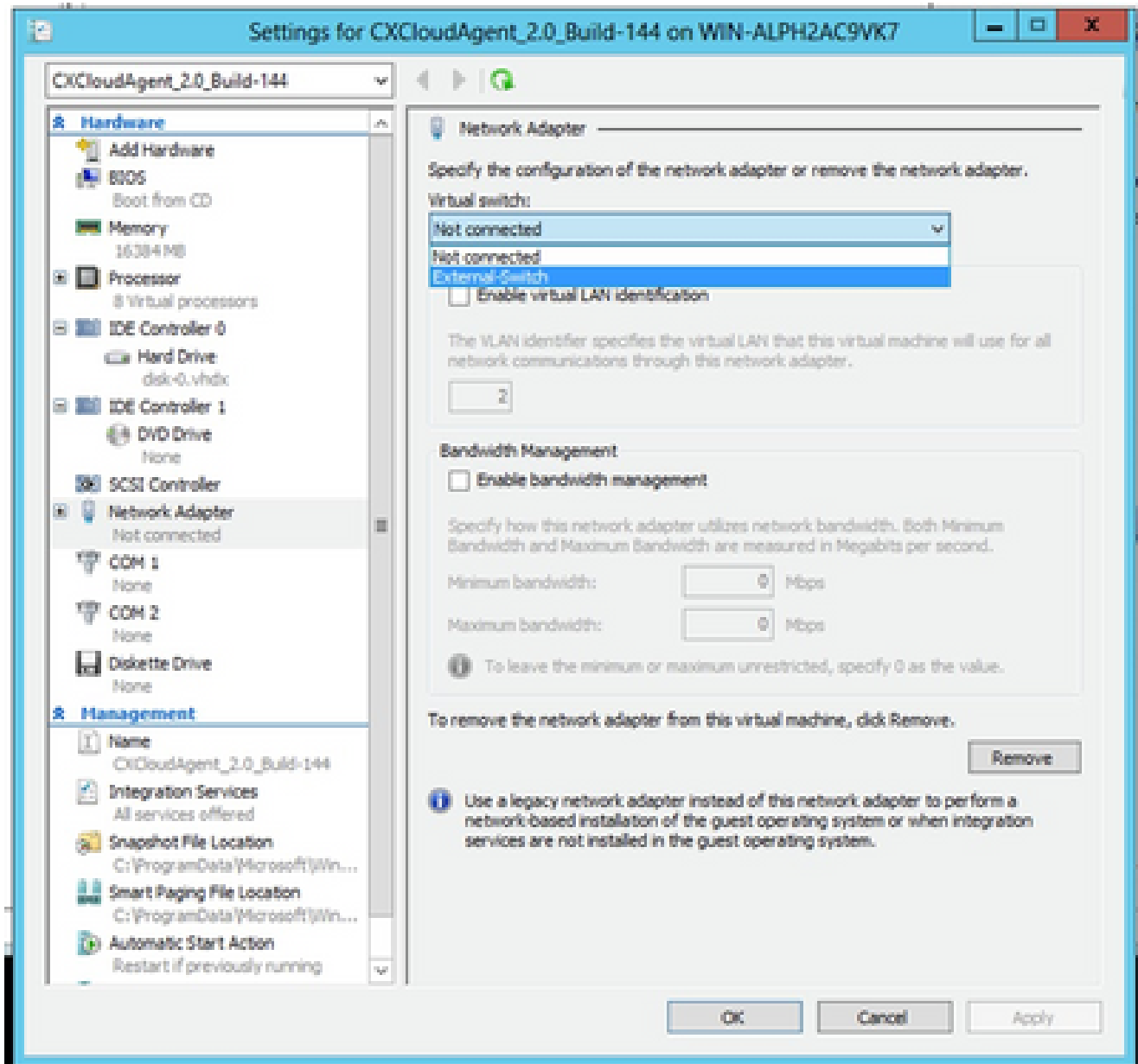
用于存储虚拟硬盘的文件夹

10. 系统随即会显示VM摘要。验证所有输入并单击Finish。



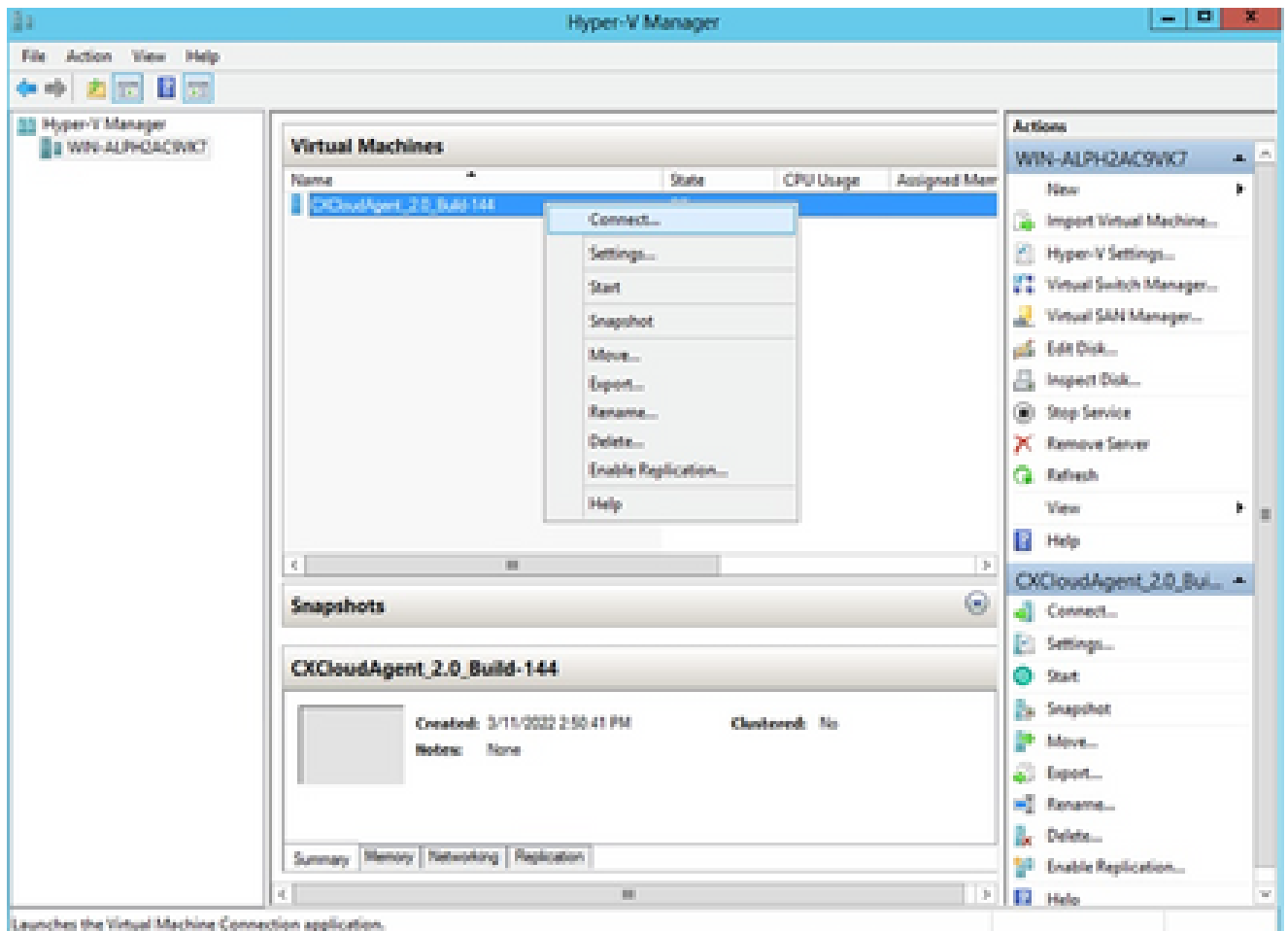
摘要

11. 成功完成导入后，会在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，然后从下拉列表中选择可用的虚拟交换机。



虚拟交换机

13. 选择Connect以启动VM。

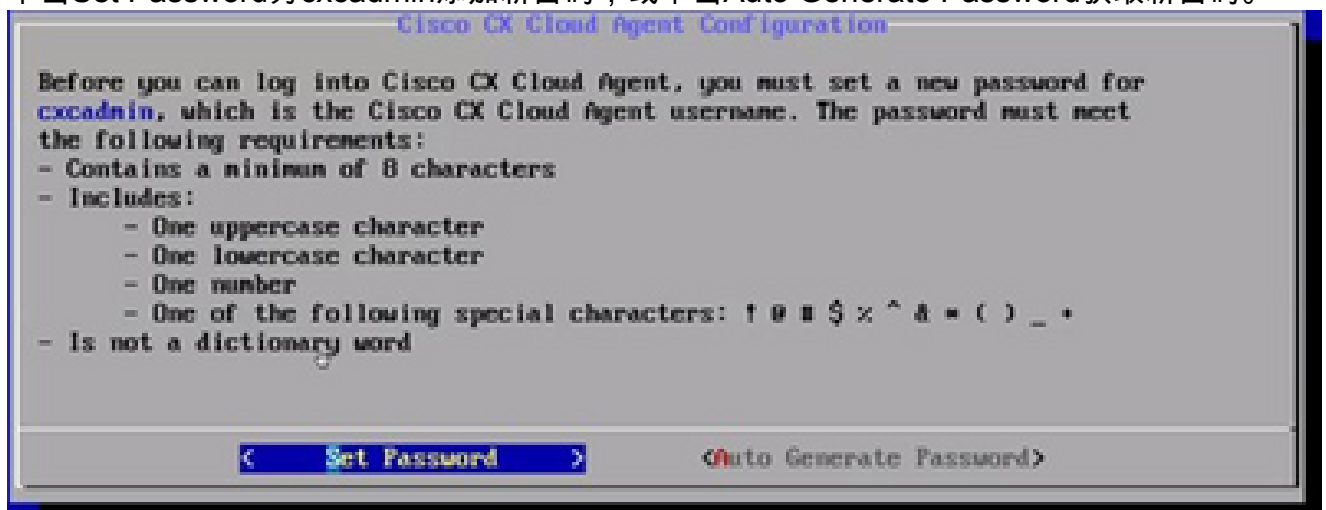


启动 VM

14. 导航到[网络配置](#)以继续执行下一步。

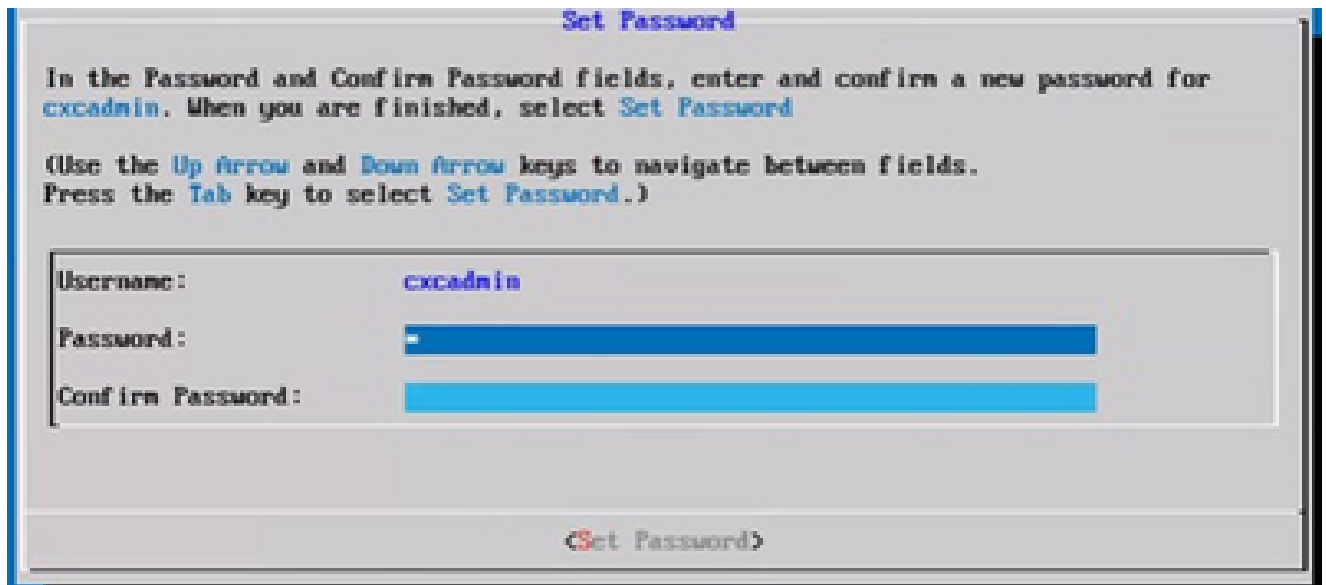
网络配置

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



设置密码

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。



新密码

或者

如果Auto Generate Password处于选中状态，请复制生成的口令并将其存储以备将来使用。点击保存密码并转至步骤 4。



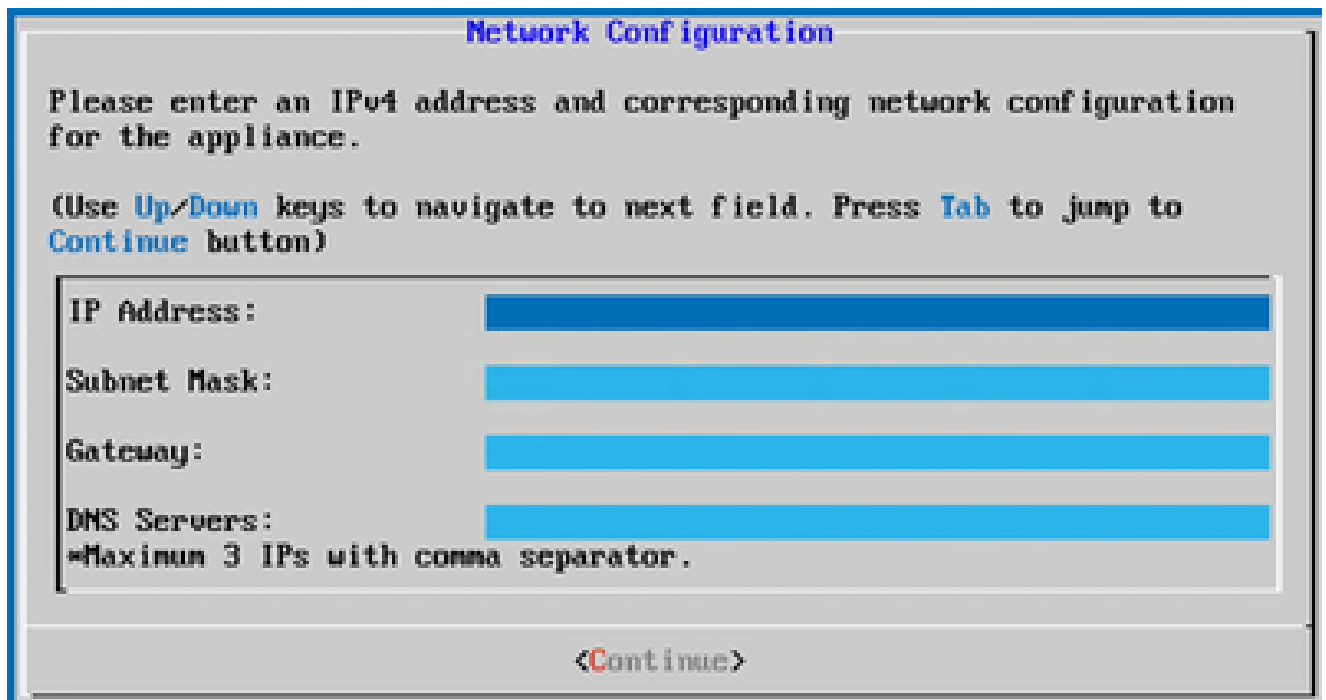
自动生成的密码

3. 点击保存密码以将其用于身份验证。



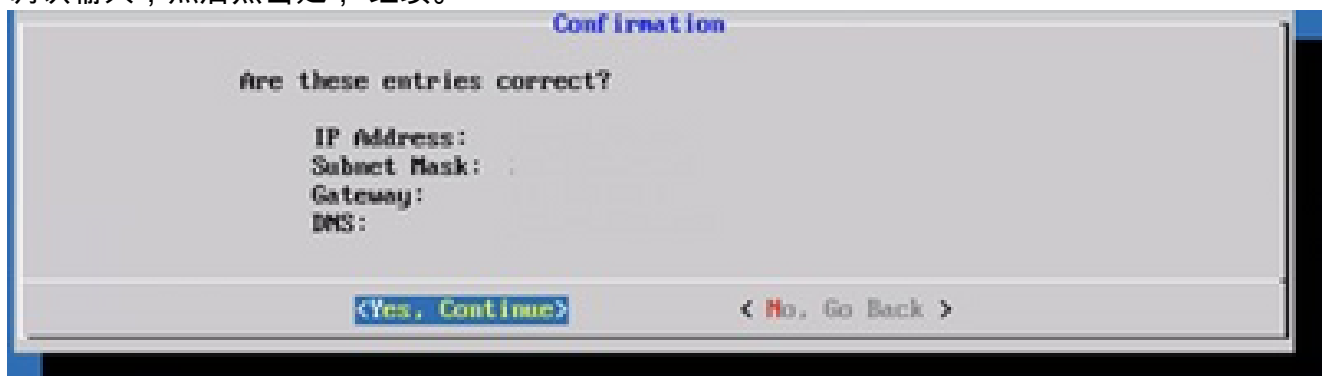
保存密码

4. 输入IP地址、子网掩码、网关和DNS服务器，然后单击继续。



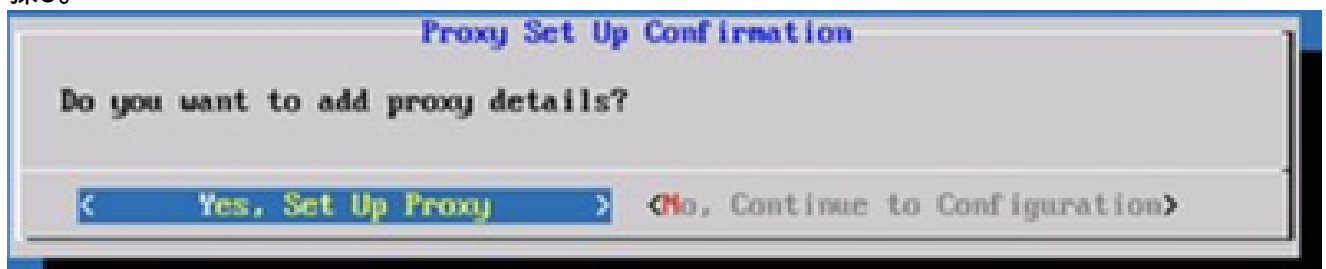
网络配置

5. 确认输入，然后点击是，继续。



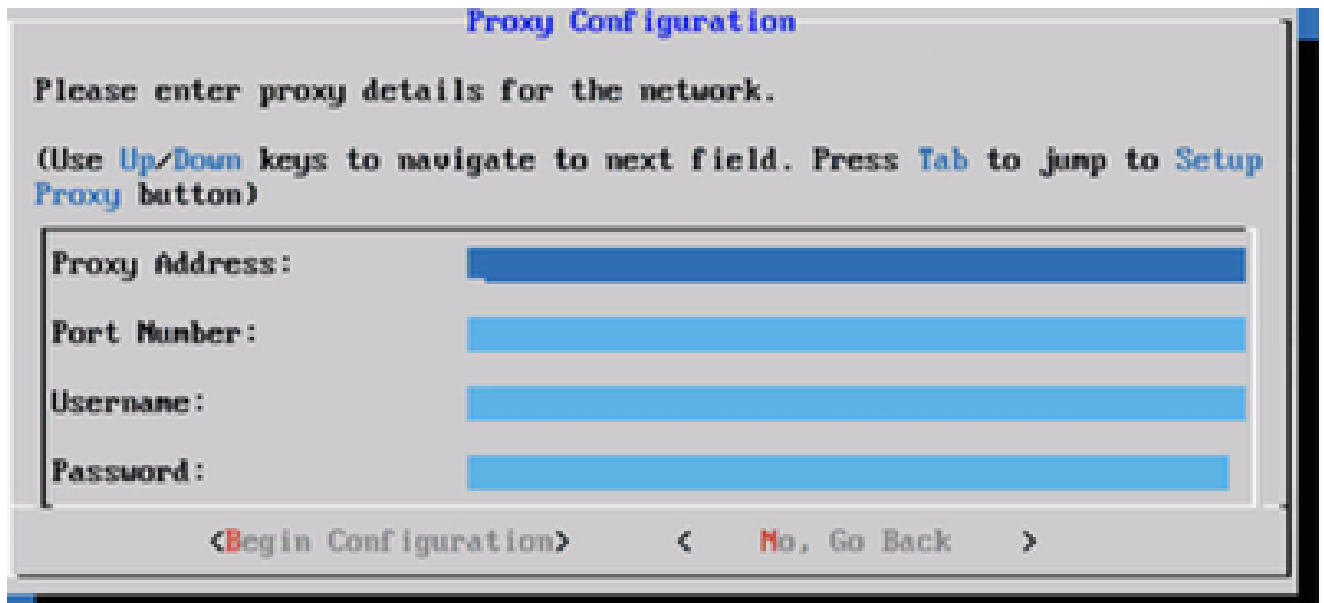
配置

6. 要设置代理详细信息，请点击是，设置代理，或者点击否，继续配置以完成配置，然后转到步骤8。



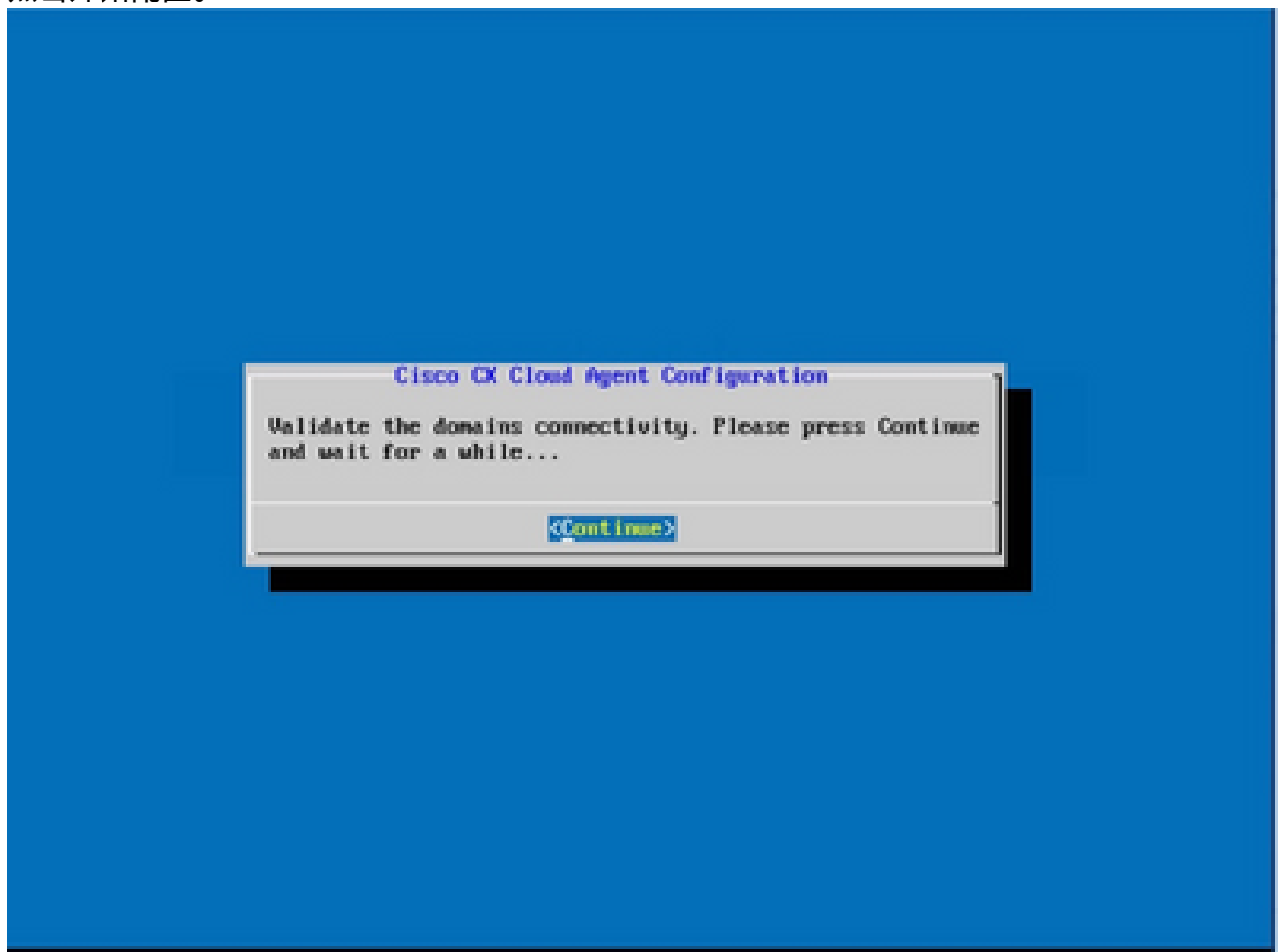
代理设置

7. 输入代理地址、端口号、用户名和密码。



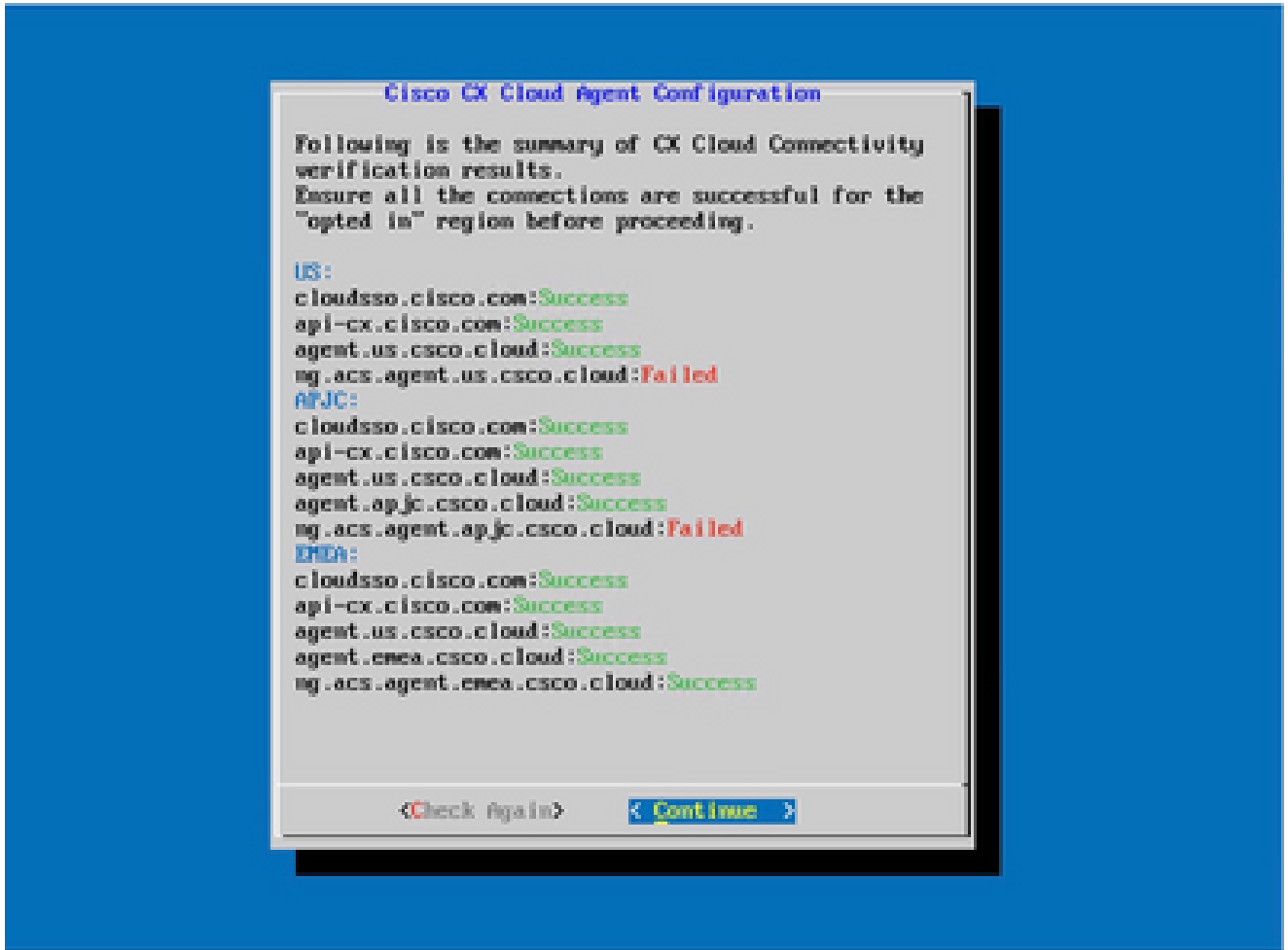
代理配置

8. 点击开始配置。




开始配置

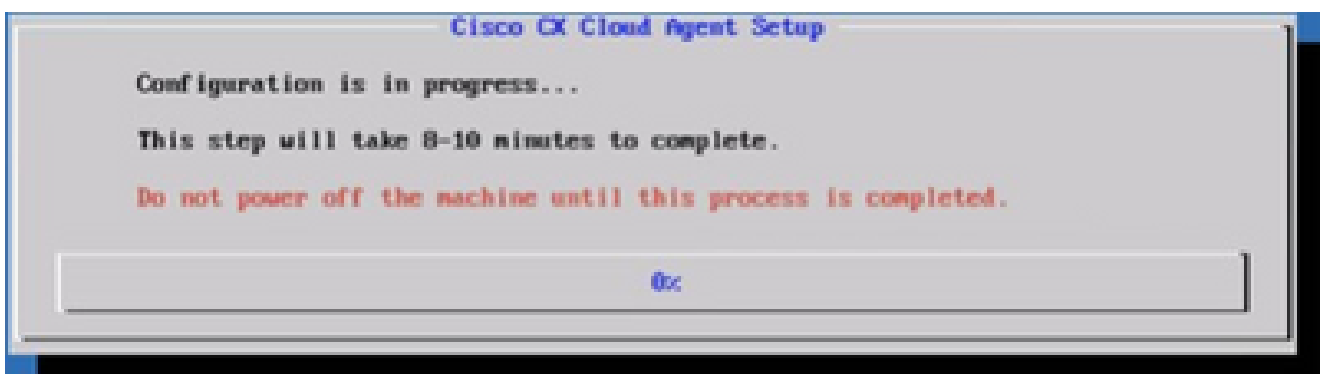
9. 单击 Continue。



继续配置

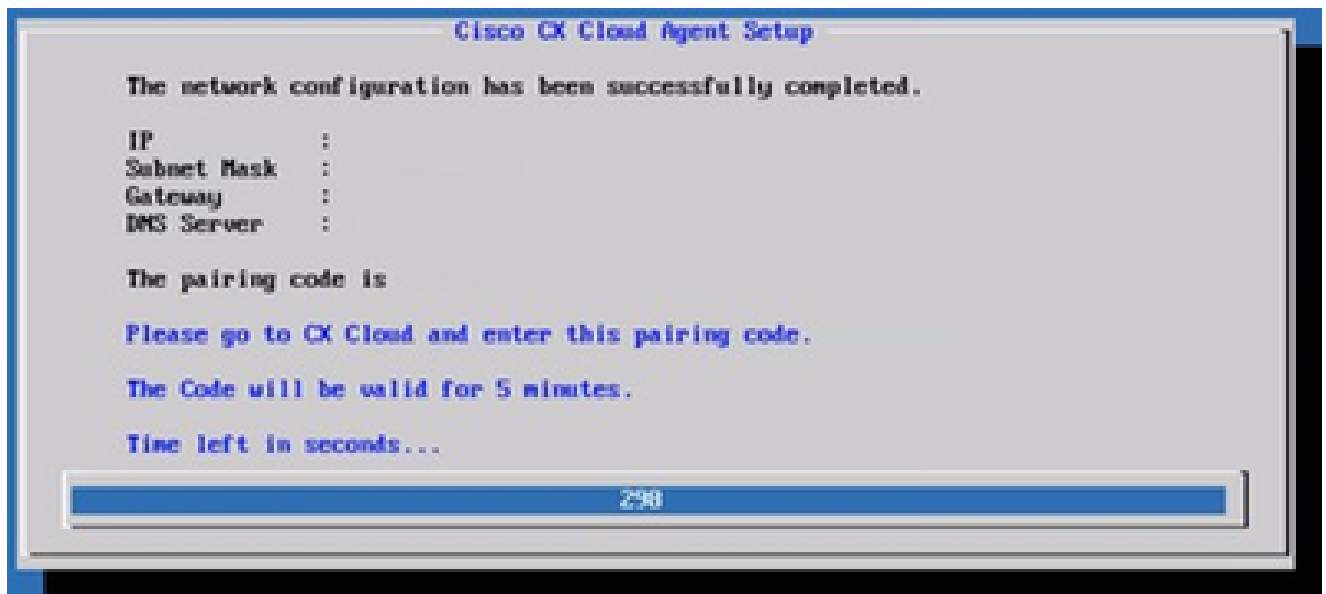
10. 单击Continue以继续进行配置以成功到达域。完成配置可能需要几分钟。

 **注意：**如果域无法成功访问，则客户必须通过在其防火墙中进行更改来修复域可访问性，以确保域可访问。解决域可接通性问题后，单击Check Again。



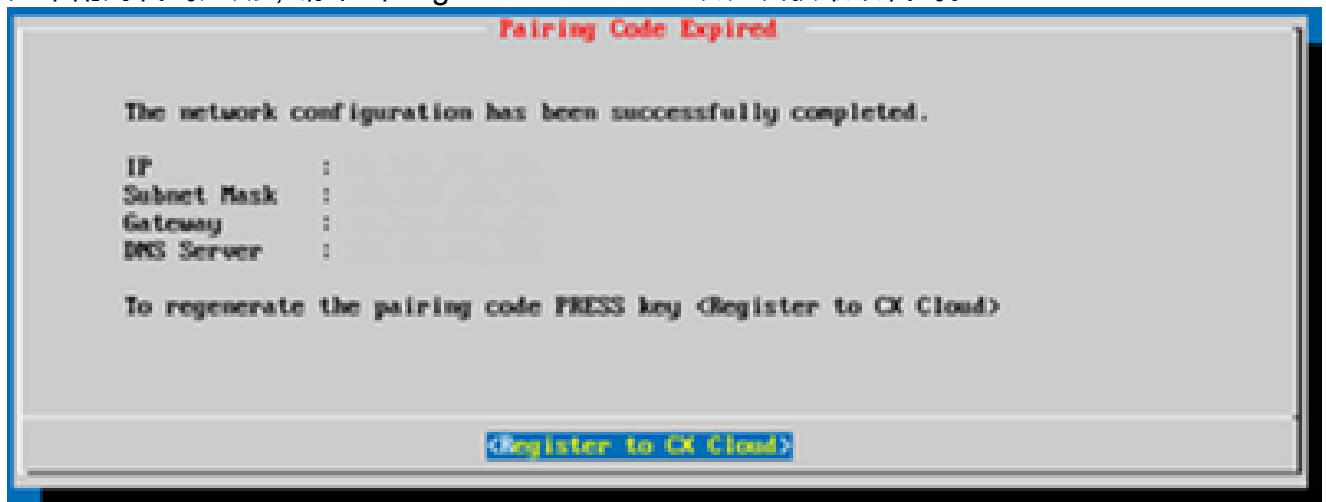
正在配置

11. 复制配对代码并返回到 CX Cloud 以继续设置。



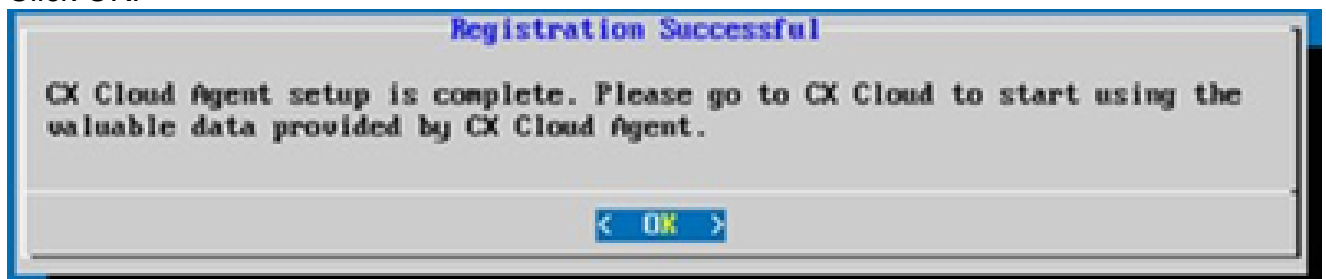
配对代码

12. 如果配对代码过期，请单击Register to CX Cloud以再次获取该代码。



代码已过期

13. Click OK.



注册成功

使用CLI生成配对代码的备选方法

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：

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。

```
cxcadmin@cxcloudagent:~$ cxcli agent generatePairingCode

Pairing Code : xJ7I0P
Expires in: 5 minutes
Please use the Pairing Code in the CX Cloud to proceed with CX Cloud Agent registration.

cxcadmin@cxcloudagent:~$
```

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Cisco DNA Center以将系统日志转发到CX云代理

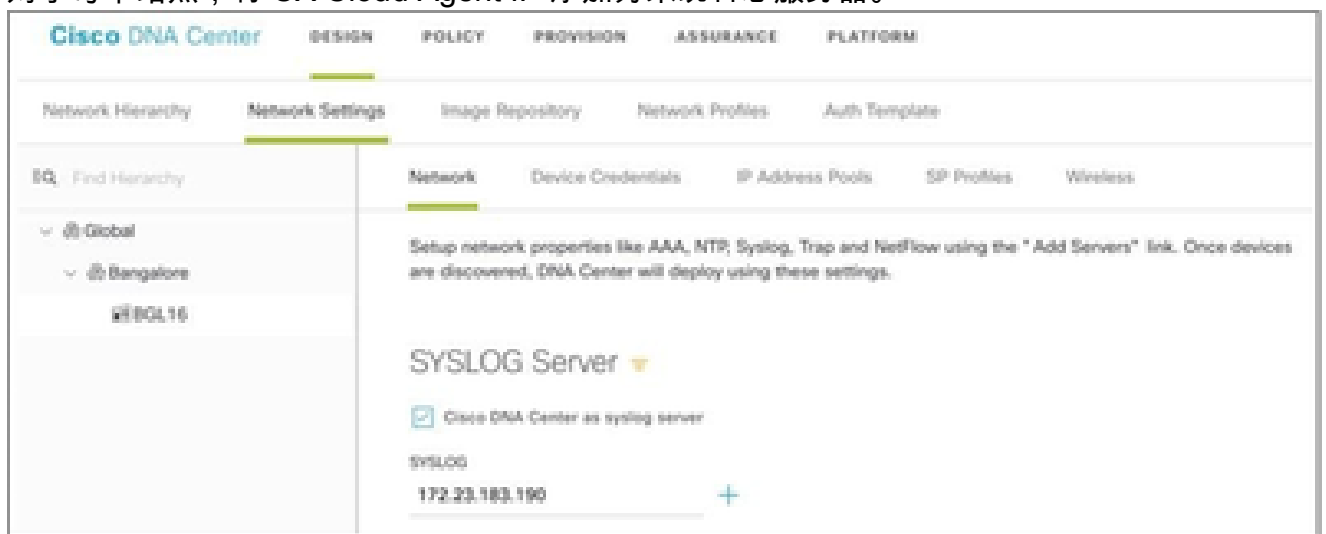
先决条件

支持的Cisco DNA 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 DNA Center Virtual Appliance


配置系统日志转发设置


要在Cisco DNA Center中配置Syslog转发到CX云代理，请执行以下步骤：

1. 启动 Cisco DNA Center。
2. 转至设计 > 网络设置 > 网络。
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，与该站点关联的所有设备都将配置为将级别为“关键”的系统日志发送到CX云代理。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。


配置其他资产以将系统日志转发到CX云代理

必须将设备配置为将系统日志消息发送到CX云代理，才能使用CX云的故障管理功能。

 注意：只有园区成功跟踪第2级设备才有资格配置其他资产以转发系统日志。

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云代理IP地址添加为新目标。

 注意：在转发系统日志时，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云代理IP地址。有关具体的配置步骤，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. 导航到工具>遥测。



TOOLS

Discovery

Inventory

Topology

Image Repository

Command Runner

License Manager

Template Editor

Telemetry

Data and Reports

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. 选择所需站点并使用设备名称复选框选择所有设备。

4. 从操作下拉菜单中选择最佳可视性。



操作

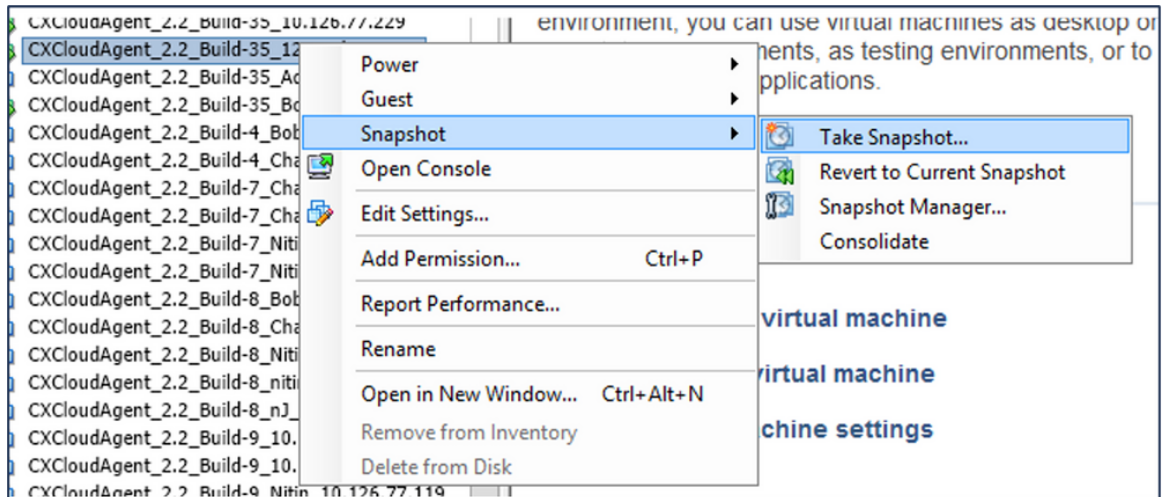
备份和恢复CX云虚拟机

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

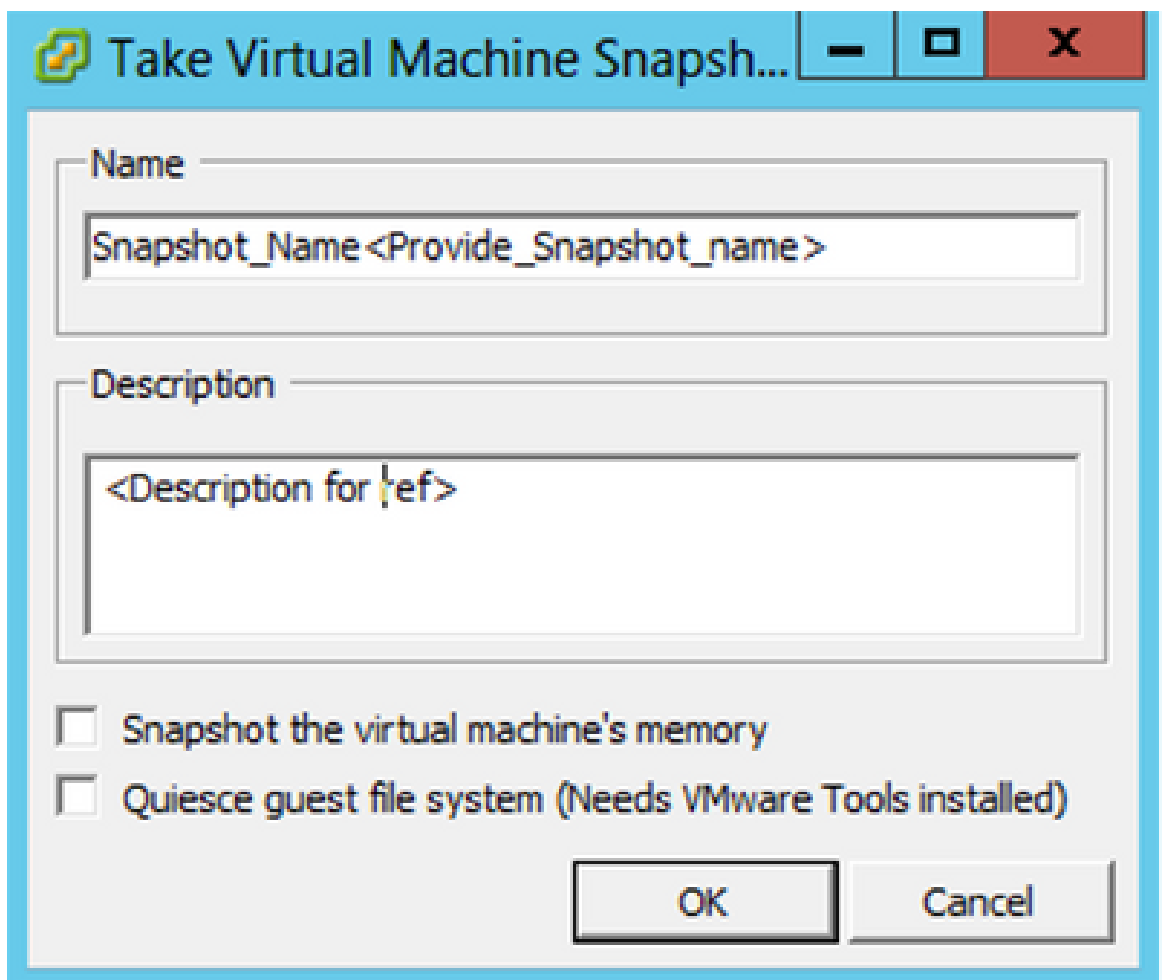
备份

要备份CX云虚拟机，请执行以下操作：

1. 右键单击VM并选择Snapshot > Take Snapshot。拍摄虚拟机快照窗口打开。



选择 VM

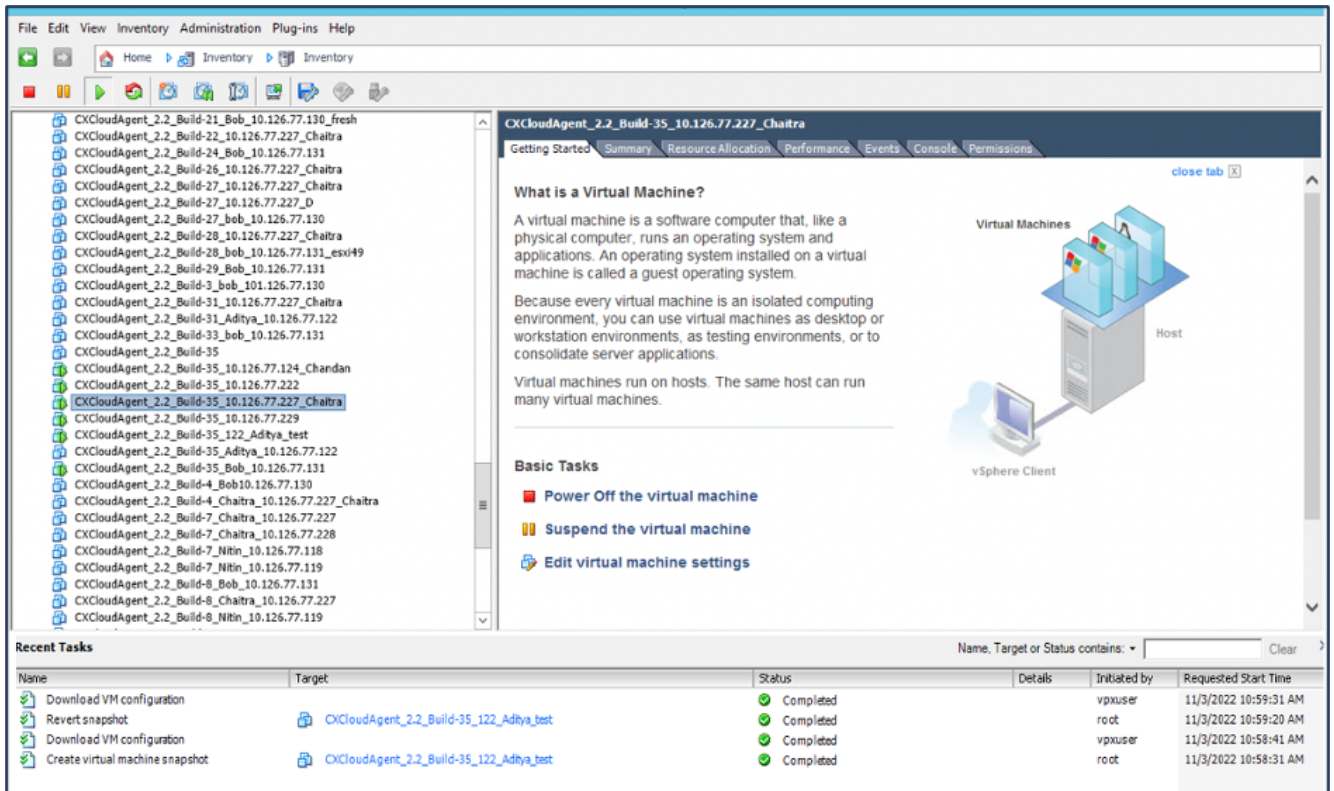


拍摄虚拟机快照

2. 输入Name和Description。

 注：验证是否已清除“Snapshot the virtual machine's memory (虚拟机内存快照)”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。

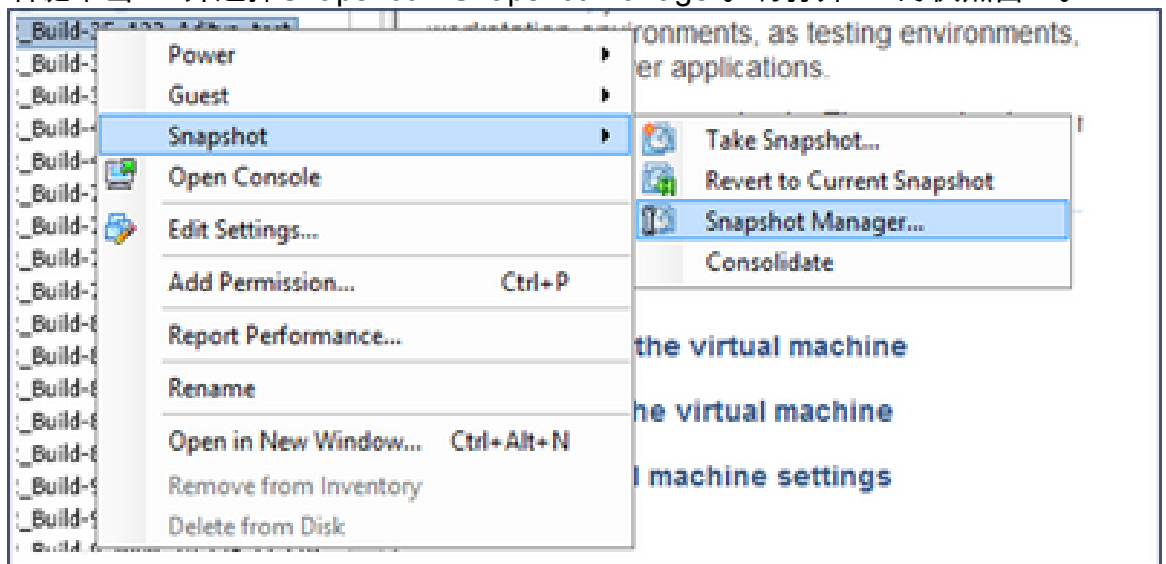


最近任务

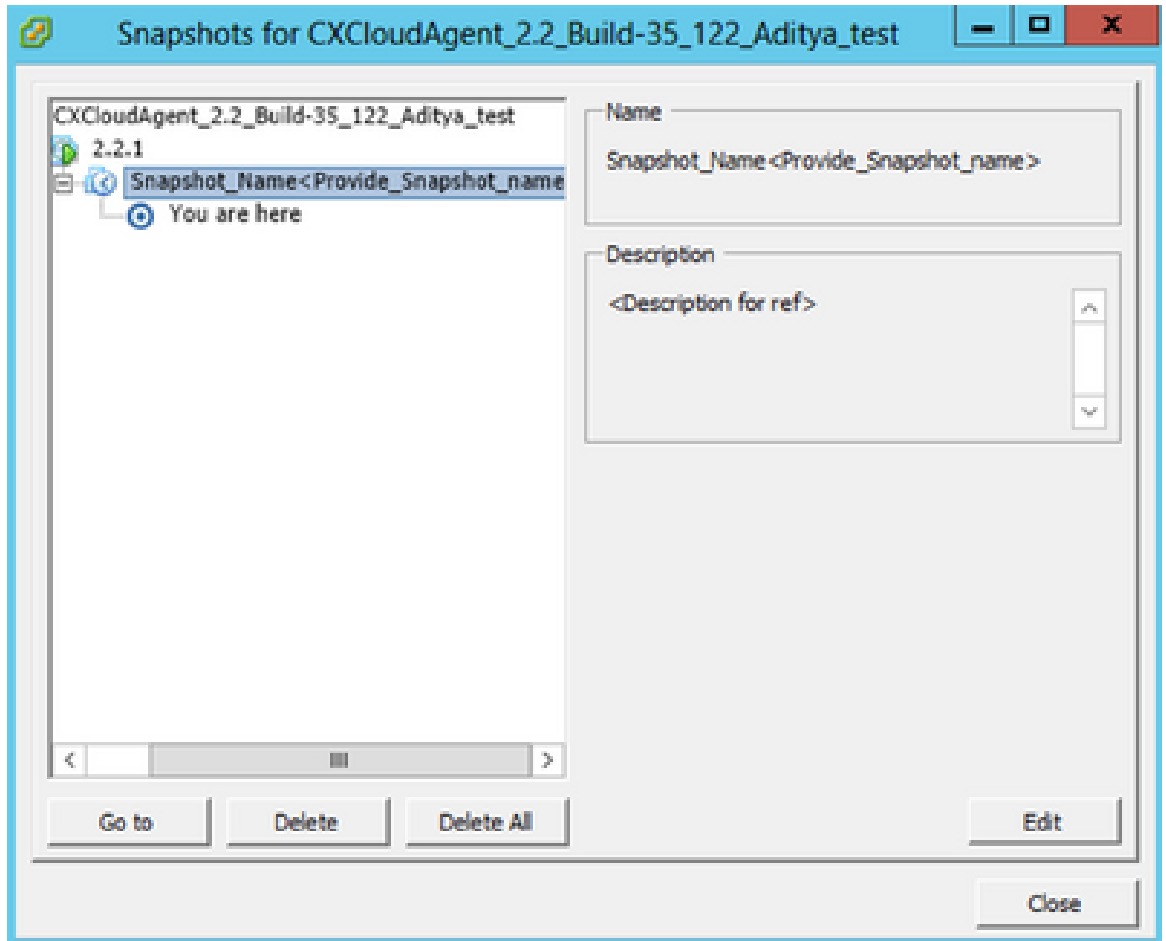
恢复

要恢复CX云虚拟机，请执行以下操作：

1. 右键单击VM并选择Snapshot > Snapshot Manager。将打开VM的快照窗口。

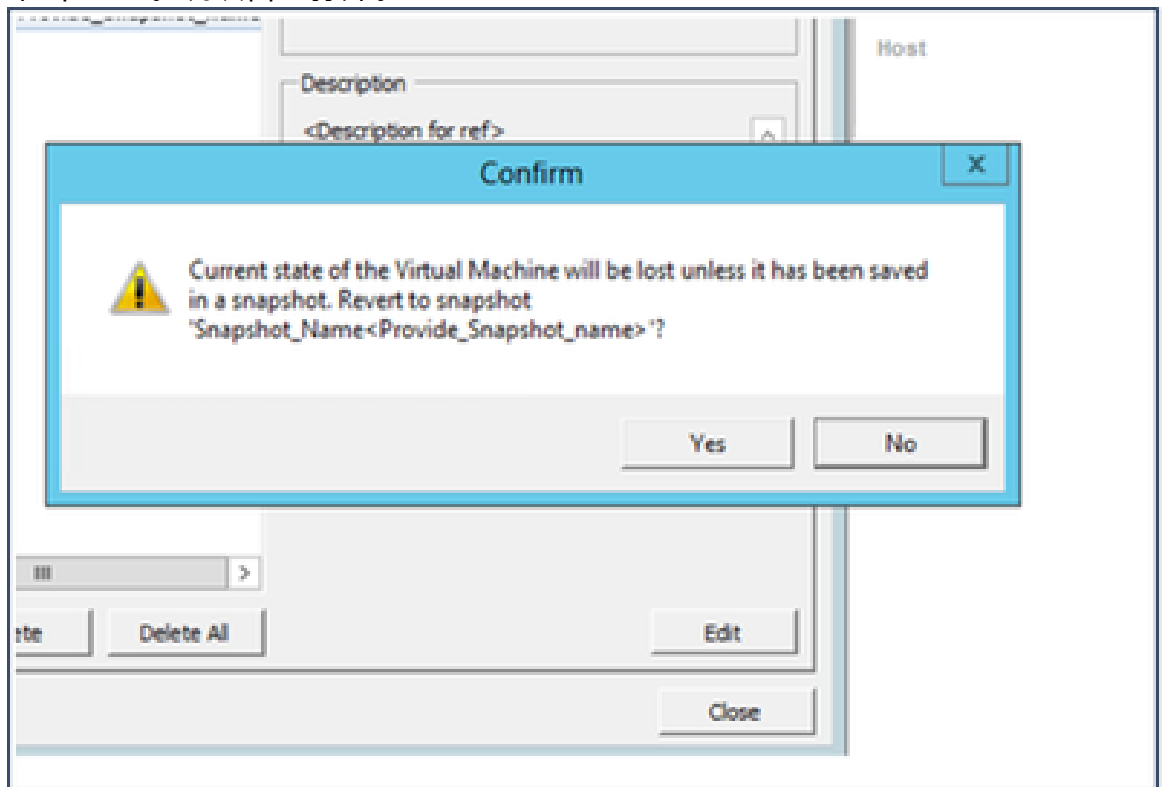


选择VM窗口



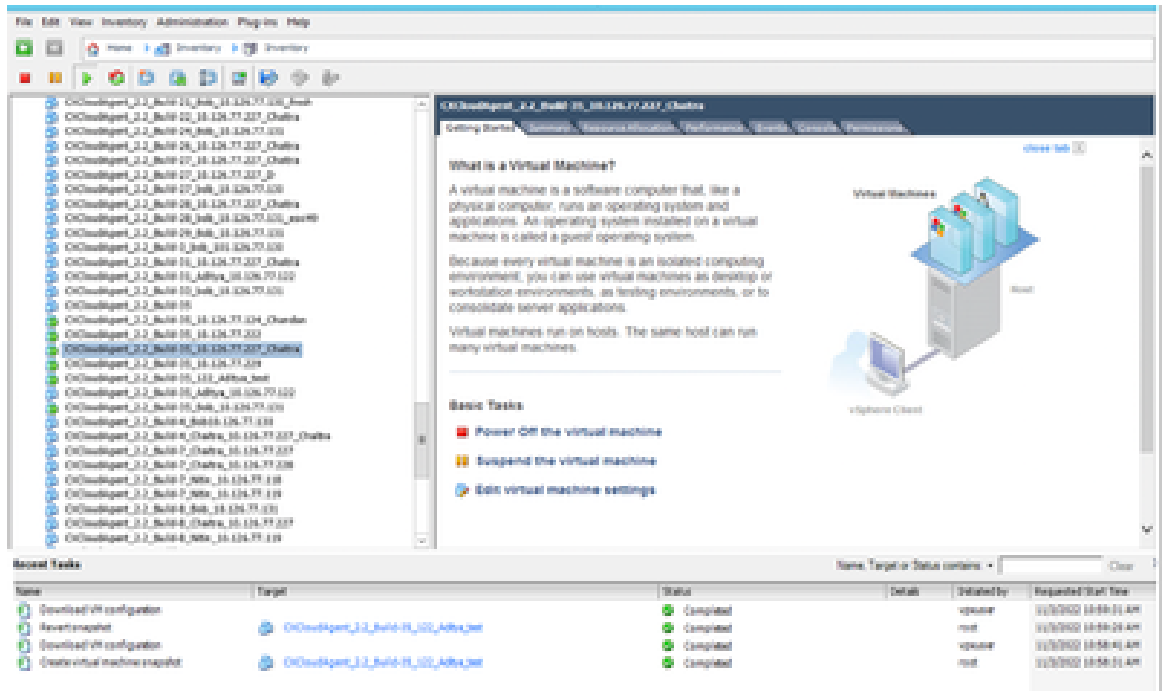
“快照”窗口

2. 单击Go to。确认窗口打开。



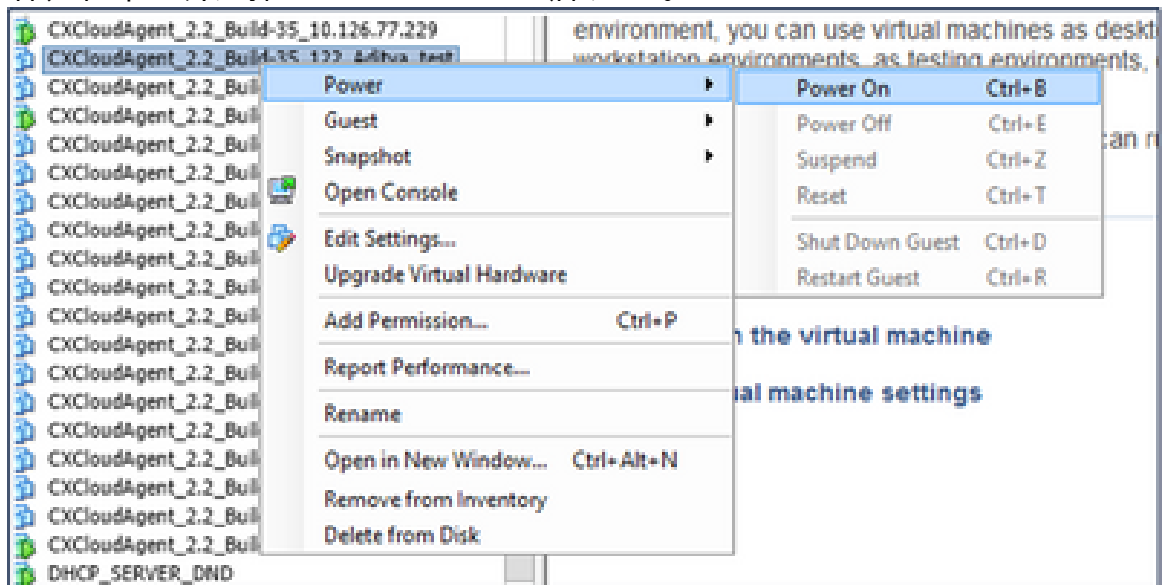
确认窗口

3. 单击 Yes。恢复快照状态在“最近的任务”列表中显示为已完成。



最近任务

4. 右键单击VM并选择Power > Power On启动VM。



安全

CX Cloud Agent可确保客户的端到端安全性。CX云和CX云代理之间的连接是TLS安全的。云代理的默认SSH用户只能执行基本操作。

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。用户必须参考此[常见问题](#)才能设置此引导加载程序（单用户模式）口令。

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被迫设置密码。cxcadmin用户/凭证用于访问CX云代理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，并且是单向散列密码，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云代理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)，使用户能够进行身份验证并与CX云代理通信。

- 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加密口令，该口令只能从SWIM门户([DECRYPT请求表](#))解密。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取root权限。密码短语的有效期限仅为两天。cxcadmin用户必须在密码到期后重新创建帐户并从SWIM门户获取密码。

强化

CX云代理设备遵循互联网安全中心强化标准。

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）将加密的服务器凭证存储在安全数据库中。除了在处理所收集的数据时暂时存储外，所收集的数据不会以任何形式存储在设备内。收集完成后，遥测数据将尽快上传到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

注册软件包包含所需的唯一[X.509](#)设备证书和密钥，用于与IoT核心建立安全连接。使用该代理使用基于传输层安全(TLS) v1.2的消息队列遥测传输(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[思科遥测命令](#)中列出的API和命令检索资产遥测。本文档根据命令对Cisco DNA中心库存、诊断网桥、Intersight、合规性见解、故障和CX云代理收集的所有其他遥测来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云代理会屏蔽所有已收集资产的敏感数据，这些资产会直接将遥测发送到CX云代理。这包括密码、密钥、社区字符串、用户名等。在将控制器管理的资产信息传输到CX云代理之前，控制器会为所有资产提供数据掩码。在某些情况下，控制器管理的资产遥测勘测可以进一步匿名。请参阅相应的[产品支持文档](#)以了解关于遥测匿名化的详细信息(例如，《Cisco DNA Center管理员指南》的[匿名数据](#)部分)。

尽管遥测命令列表无法自定义，并且数据掩码规则无法修改，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（针对CX云代理收集的其他资产）部分所述。

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。用户必须参阅 常见问题 才能设置其引导加载程序（单用户模式）口令。
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：已创建默认用户帐户；用户可以使用cxcli执行CX云代理应用命令，并且在设备上具有最低权限；cxcroot用户及其加密密码使用cxcadmin用户生成。 · cxcroot：cxcadmin可以使用实用程序remoteaccount创建此用户；用户可使用此帐户获得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。 ·至少包含八(8)个字符，包含以下类别中的三种：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。

	<ul style="list-style-type: none"> · 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	<ul style="list-style-type: none"> · 至少包含八个字符，包含以下三个类别：大写、小写、数字和特殊字符。 · 登录尝试失败五次，将密码框锁定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	<ul style="list-style-type: none"> · 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。

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）。