

Visão geral do CX Cloud Agent v2.0

Contents

[Introduction](#)

[Prerequisites](#)

[Acesso a domínios essenciais](#)

[Pré-requisitos para atualizar para o CX Cloud Agent v2.0](#)

[Versões certificadas do Cisco DNA Center](#)

[Navegadores compatíveis](#)

[Implante o CX Cloud Agent](#)

[Conectar o CX Cloud Agent à CX Cloud](#)

[Implantação e configuração de rede](#)

[Implantação do OVA](#)

[Instalação do Thick Client ESXi 5.5/6.0](#)

[Instalação do Web Client ESXi 6.0](#)

[Instalação do Web Client vCenter](#)

[Instalação do Oracle Virtual Box 5.2.30](#)

[Instalação do Microsoft Hyper-V](#)

[Configuração de rede](#)

[Abordagem alternativa para gerar código de emparelhamento usando CLI](#)

[Configurar o Cisco DNA Center para encaminhar o Syslog para o CX Cloud Agent](#)

[Pré-requisito](#)

[Configurar definição do encaminhamento de syslog](#)

[Habilitar Configurações de Syslog de Nível de Informação](#)

[Security](#)

[Segurança física](#)

[Acesso do usuário](#)

[Segurança da conta](#)

[Segurança de rede](#)

[Autenticação](#)

[Blindagem](#)

[Segurança de dados](#)

[Transmissão de Dados](#)

[Registros e monitoramento](#)

[Resumo de segurança](#)

[Perguntas mais frequentes](#)

[CX Cloud Agent](#)

[Implantação](#)

[Versões e correções](#)

[Autenticação e configuração de proxy](#)

[Secure Shell SSH](#)

[Portas e serviços](#)

[Conexão do CX Cloud Agent com o Cisco DNA Center](#)

[Verificação de diagnóstico usada pelo CX Cloud Agent](#)

[Registros de sistema do CX Cloud Agent](#)

[Troubleshooting](#)

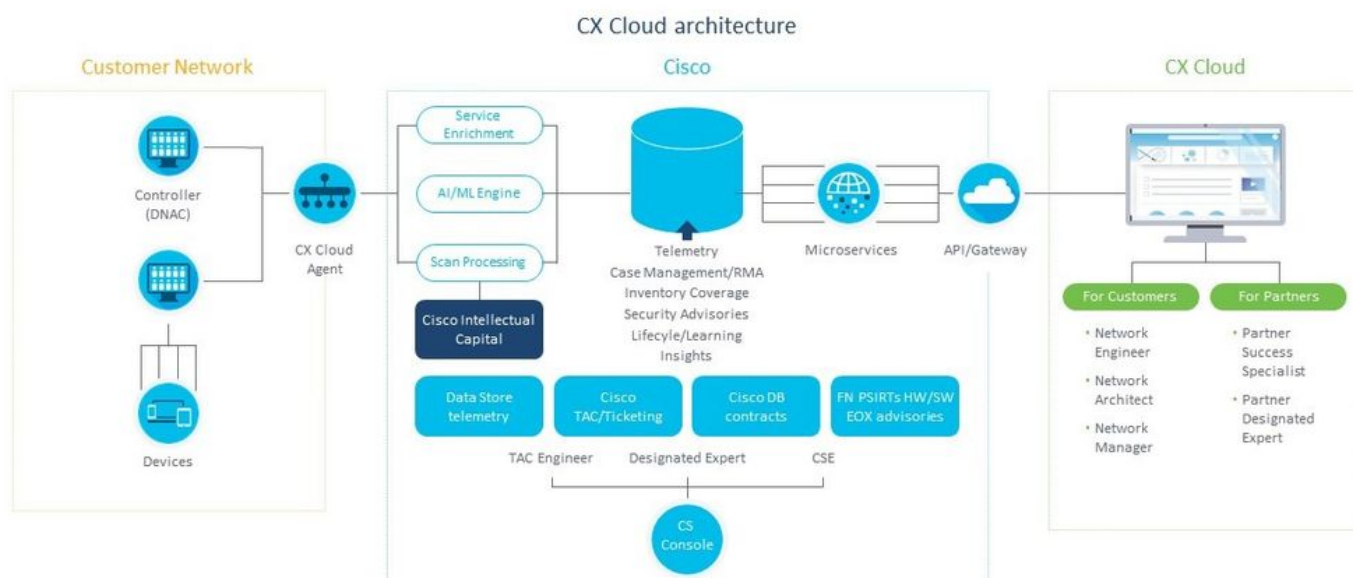
[Respostas à falha de coleta](#)

[Respostas à falha de verificação de diagnóstico](#)

Introduction

Este documento descreve o Cisco Customer Experience (CX) Cloud Agent. O Cisco Cloud Agent (CX) é uma plataforma de software modular modernizada no local que hospeda recursos leves de microsserviços em contêineres. Esses recursos podem ser instalados, configurados e gerenciados no local do cliente na nuvem. O CX Cloud Agent acelera a monetização de novas ofertas, dimensiona recursos e ajuda a desenvolver serviços de próxima geração orientados por big data, análises, automação, aprendizagem automática/inteligência artificial (ML/AI) e transmissão.

Note: Este guia destina-se a usuários do CX Cloud Agent v2.0. Consulte o [Cisco CX Cloud Agent](#) para obter outras informações relacionadas.



CX Cloud Agent Architecture

Note: As imagens (e o conteúdo contido neste guia) são apenas para fins de referência. O conteúdo real pode variar.

Prerequisites

O CX Cloud Agent é executado como máquina virtual (VM) e está disponível para download como Open Virtual Appliance (OVA) ou um Virtual Hard Disk (VHD).

Requisitos para implantação:

- Qualquer um destes hipervisores: VMWare ESXi versão 5.5 ou posterior Oracle Virtual Box 5.2.30 Hypervisor Windows versão 2012 a 2016

- O hipervisor pode hospedar uma VM que requer: CPU de 8 núcleos 16 GB de memória/RAM 200 GB de espaço em disco
- Para clientes que usam data centers designados da Cisco US como a região de dados principal para armazenar dados da nuvem CX:
O CX Cloud Agent deve ser capaz de se conectar aos servidores mostrados aqui, usando o FQDN e usando HTTPS na porta TCP 443:
FQDN agent.us.cisco.cloud
FQDN ng.acs.agent.us.cisco.cloud
FQDN cloudsso.cisco.com
FQDN api-cx.cisco.com
- Para clientes que usam data centers designados da Cisco Europe como a principal região de dados para armazenar dados da nuvem CX:
O CX Cloud Agent deve ser capaz de se conectar aos dois servidores mostrados aqui, usando o FQDN e usando HTTPS na porta TCP 443:
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
- Para clientes que usam data centers designados da Cisco Ásia-Pacífico como a região de dados principal para armazenar dados da nuvem CX:
O CX Cloud Agent deve ser capaz de se conectar aos dois servidores mostrados aqui, usando o FQDN e usando HTTPS na porta TCP 443:
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
- Para clientes que usam os data centers designados da Cisco Europa e da Cisco Ásia Pacífico como sua região de dados principal, a conectividade com o FQDN: agent.us.cisco.cloud é necessário apenas para registrar o CX Cloud Agent no CX Cloud durante a configuração inicial. Depois que o CX Cloud Agent é registrado com êxito no CX Cloud, essa conexão não é mais necessária.
- Para o gerenciamento local do CX Cloud Agent, a porta 22 deve estar acessível.

Outras observações sobre o CX Cloud Agent:

- Um IP será detectado automaticamente se o protocolo DHCP estiver habilitado no ambiente da VM. Caso contrário, um endereço IPv4 livre, uma máscara de sub-rede, um endereço IP de gateway padrão e um endereço IP de servidor DNS devem estar disponíveis.
- Somente o IPv4 é compatível, o IPv6 não.
- As versões do Cisco Digital Network Architecture (DNA) Center de nó único certificado e Cluster de alta disponibilidade (HA) de 1.2.8 a 1.3.3.9 e 2.1.2.0 a 2.2.3.5 são necessárias.
- Se a rede tiver interceptação SSL, permita listar o endereço IP do CX Cloud Agent.

Acesso a domínios essenciais

Para iniciar a jornada do CX Cloud, os usuários precisam de acesso a esses domínios.

Principais domínios	Outros domínios
cisco.com	mixpanel.com
cisco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

Domínios específicos da região:

AMÉRICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	m
agent.us.cisco.cloud	agent.us.cisco.cloud	api-cx.cisco.com
ng.acs.agent.us.cisco.cloud	agent.us.cisco.cloud	agent.us.cisco.cloud
	agent.emea. cisco.cloud	d
	ud	agent.apjc. cisco.cloud
	ng.acs.agent.emea. cisco.cloud	oud
		ng.acs.agent.apjc.cisco.cloud

Pré-requisitos para atualizar para o CX Cloud Agent v2.0

Os pré-requisitos descritos nesta seção devem ser atendidos antes da atualização para o CX Cloud Agent v2.0.

1. Verifique se o CX Cloud Agent v1.12.x e posterior deve ser instalado antes do início da atualização.
2. Execute estas etapas para configurar o Servidor de Nomes de Domínio, caso ele ainda não esteja configurado:
Faça login no console Command Line Interface (CLI) da máquina virtual do CX Cloud Agent. Execute o comando *cxcli agent configureDNS*. Insira o endereço IP do DNS. Clique em Exit.
3. Certifique-se de que a rede do cliente permita que os nomes de domínio no [Acesso de Domínio Crítico](#) concluam o novo registro do Agente de Nuvem durante a migração. O CX Cloud Agent deve ser capaz de acessar esses domínios, e os domínios também devem ser resolvíveis a partir do servidor DNS. Entre em contato com a equipe de rede se algum domínio estiver inacessível.
4. Tire um instantâneo da VM do Agente de Nuvem antes de iniciar a atualização da v2.0 (acesso apropriado necessário).

Note: As versões anteriores à 1.10 devem primeiro ser atualizadas para a v1.10, seguidas de atualizações incrementais para a v1.12.x e, em seguida, para a v2.0. Os usuários podem atualizar a partir de Configurações do administrador > Fontes de dados no portal da nuvem do CX. Clique em View Update para concluir a atualização.

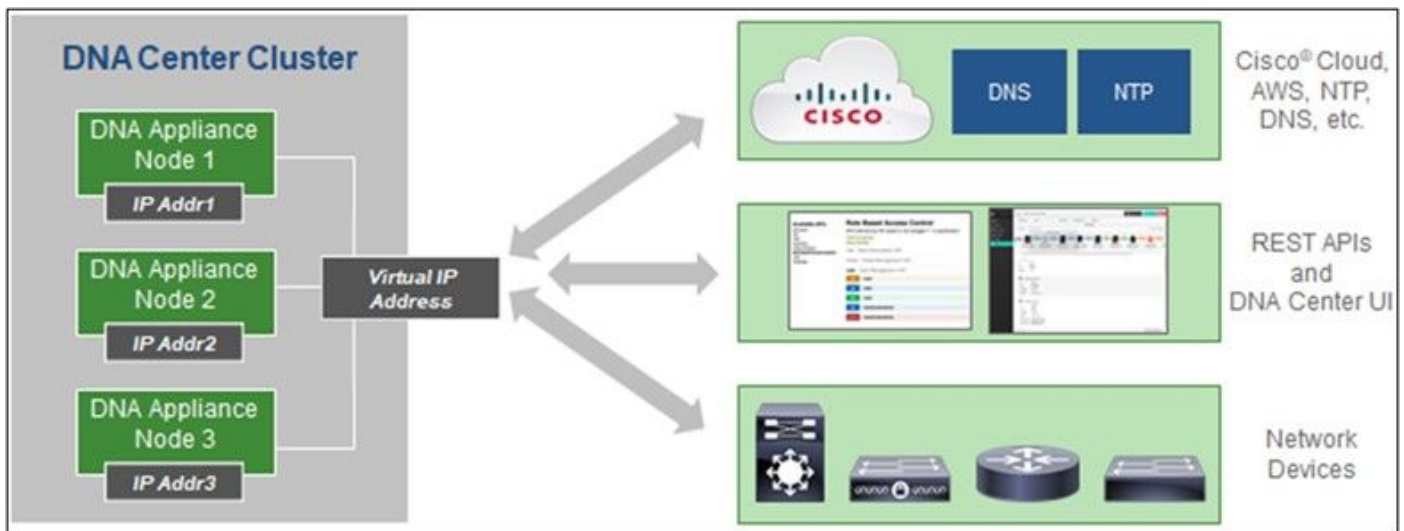
As seguintes condições devem ser atendidas para uma configuração bem-sucedida:

1. Lista de DNACs e suas credenciais

2. Usuário DNAC com **acesso de função Admin** ou **Observer**
3. Endereço IP virtual ou endereço IP físico/autônomo para cluster DNAC
4. Acessibilidade bem-sucedida entre o Agente de Nuvem e o DNAC
5. O DNAC deve ter no mínimo 1 (um) dispositivo gerenciado

Versões certificadas do Cisco DNA Center

As versões certificadas de nó individual e HA Cluster Cisco DNA Center são de 1.2.8 a 1.3.3.9 e 2.1.2.0 a 2.2.3.5.



Multi-Node HA Cluster Cisco DNA Center

Navegadores compatíveis

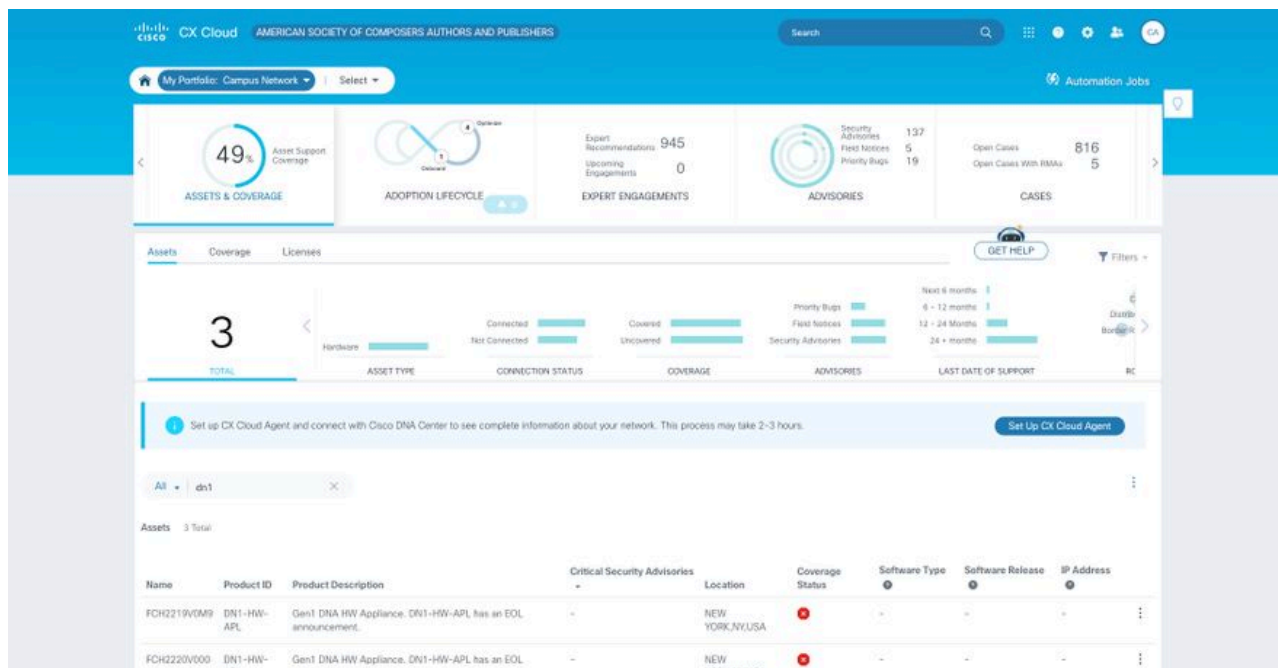
Para obter a melhor experiência em Cisco.com, recomendamos a versão oficial mais recente dos seguintes navegadores:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Implante o CX Cloud Agent

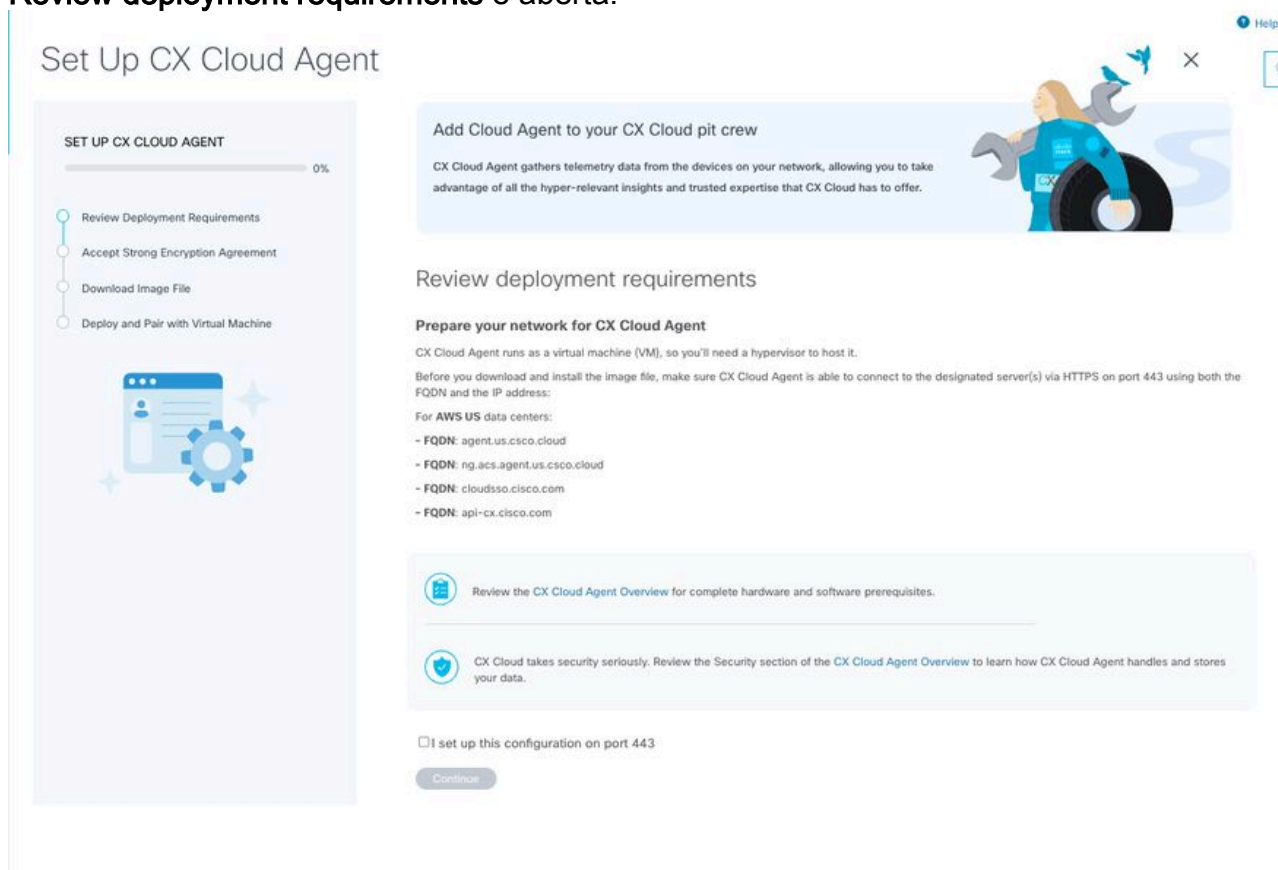
Para implantar o CX Cloud Agent:

1. Clique em cx.cisco.com para fazer login na CX Cloud.
2. Selecionar **Campus Network** e navegue até **ASSETS & COVERAGE** lado a lado.



Página inicial

3. Clique em **Configurar CX Cloud Agent** no banner. A janela **Set Up CX Cloud Agent - Review deployment requirements** é aberta.



Analisar os requisitos de implantação

4. Leia os pré-requisitos em **Analisar requisitos de implantação** e marque a caixa de seleção para **Eu defini essa configuração na porta 443**.

Note: As imagens (e o conteúdo contido neste guia) são apenas para fins de referência. O conteúdo real pode variar.

5. Clique em **Continuar**. A janela **Set Up CX Cloud Agent - Accept the strong encryption agreement** é exibida.

Set Up CX Cloud Agent

Help

SET UP CX CLOUD AGENT 25%

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

Accept the strong encryption agreement

Then you can download the image file for the CX Cloud Agent virtual machine.

Instructions

To apply for eligibility to download strong encryption software images:

1. Ensure the address listed in your Cisco.com User Profile is correct and complete.
2. Read each of the conditions below carefully prior to selecting your answer.

First Name: Samuel

Last Name: Deckard

Email: tadeckar@cisco.com

Cisco User Id: CXSUPERADMIN38333

Business Division's Function:

- Commercial/Civilian entity
- Government entity, a Military entity or Defense Contractor

If Government entity, a Military entity or Defense Contractor, Are you in

Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom or the United States.

Yes No

Confirmation

By checking this field, I hereby certify that I, as a duly authorized representative of the organization, understand and agree to abide by the conditions set forth above regarding the usage of Cisco Systems, Inc. hardware and/or software.

Continue

Contrato de criptografia

6. Verifique as informações pré-preenchidas nos campos **Nome, Sobrenome, E-mail e ID de Usuário do CCO**.
7. Selecione o Business division's function.
8. Selecione a opção Confirmation para concordar com as condições de uso.
9. Clique em **Continuar**. A janela **Set Up CX Cloud Agent - Download image file** se abre.

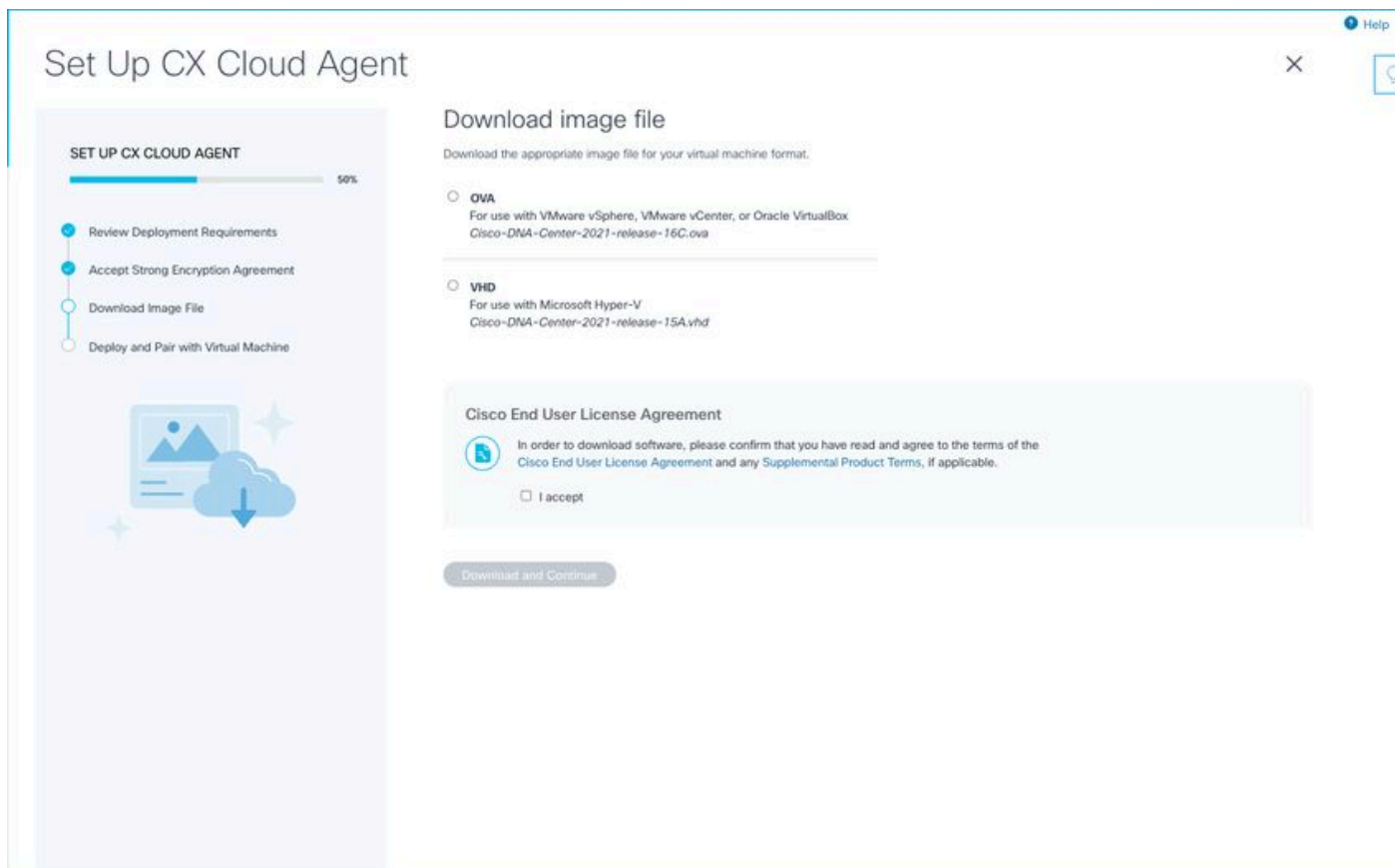


Imagem do download

10. Selecione o formato de arquivo apropriado para fazer o download do arquivo de imagem necessário para a instalação.

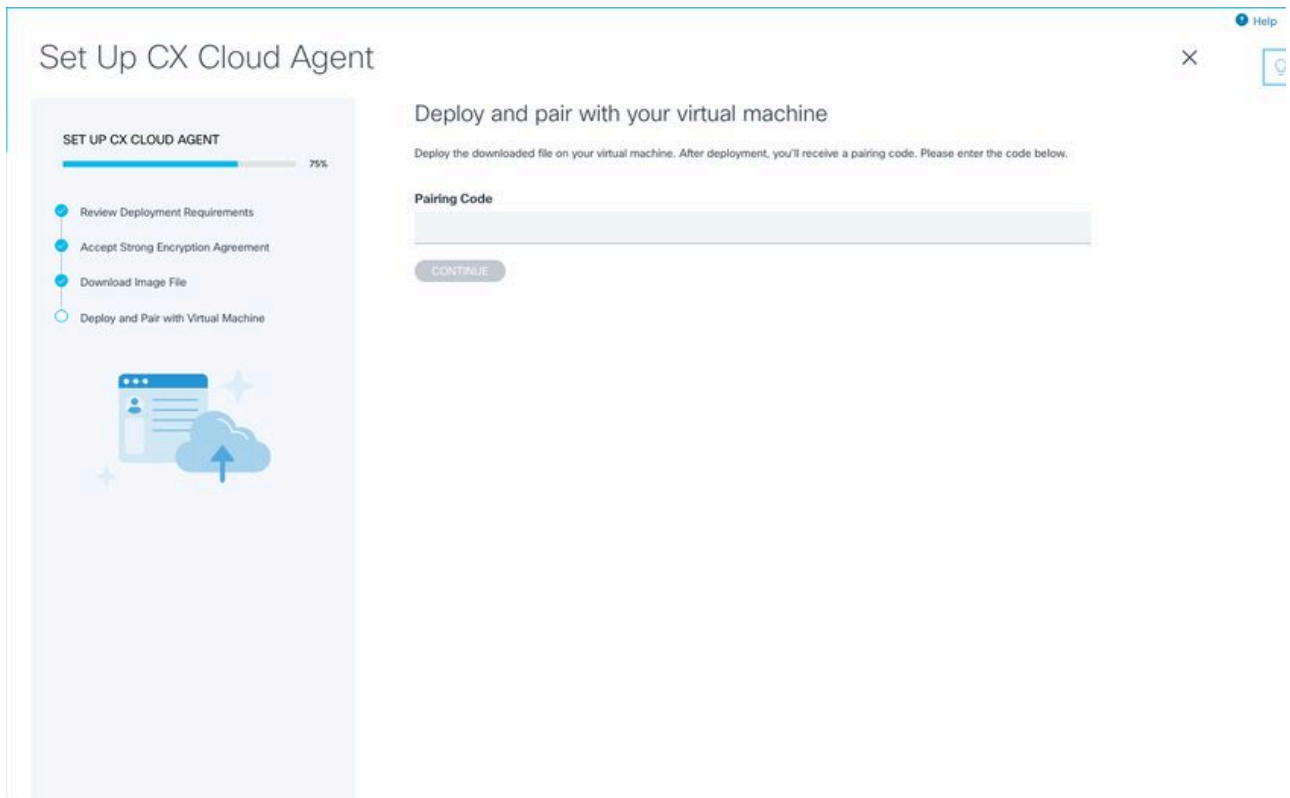
11. Marque a caixa de seleção **Aceito** para concordar com o Contrato de Licença de Usuário Final da Cisco.

12. Clique em **Download e Continuar**. A janela **Set Up CX Cloud Agent - Deploy and pair with your virtual machine** se abre.

13. Consulte [Configuração de Rede](#) para instalação do OVA e continue na próxima seção para instalar o CX Cloud Agent.

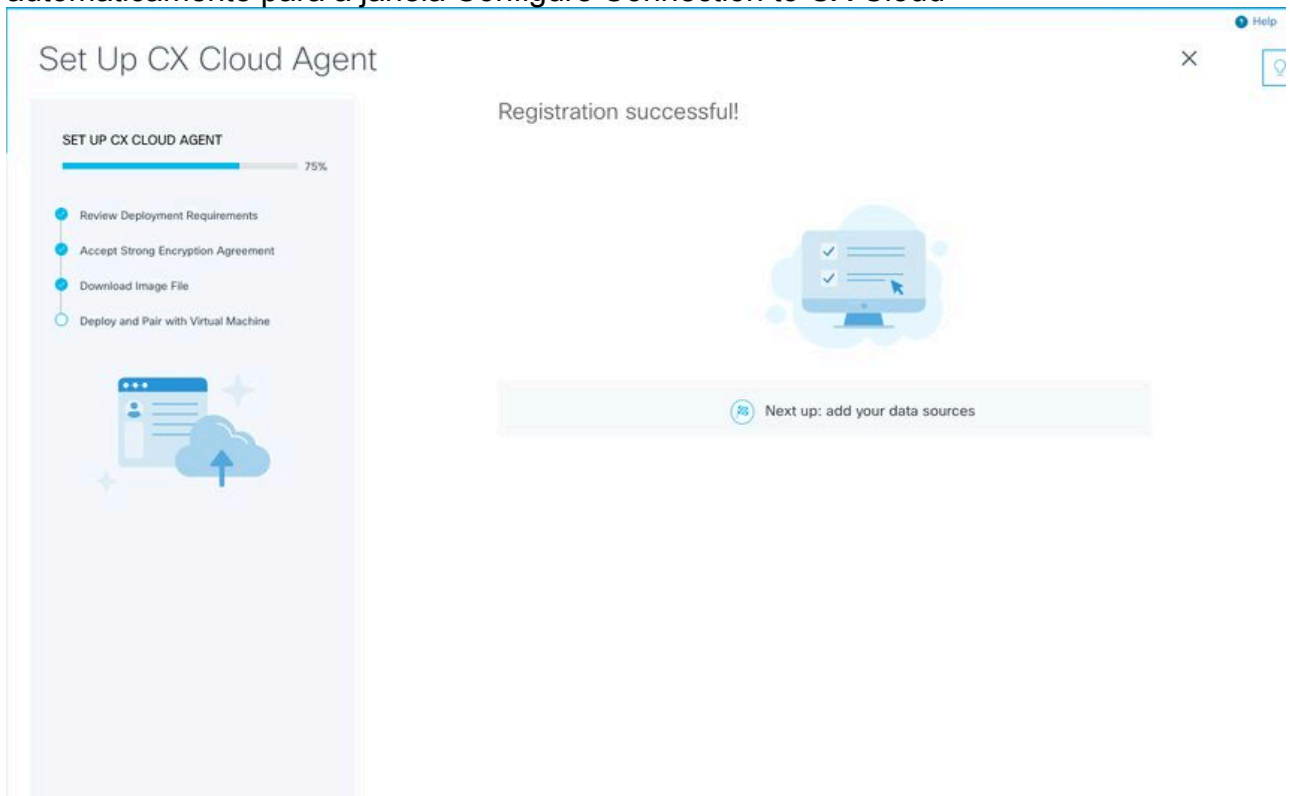
Conectar o CX Cloud Agent à CX Cloud

1. Digite o **código de emparelhamento** fornecido na caixa de diálogo do console ou na interface de linha de comando (CLI).



Código de emparelhamento

2. Clique em **Continuar** para registrar o CX Cloud Agent. A janela **Set Up CX Cloud Agent - Registration successful** é exibida por alguns segundos antes de navegar automaticamente para a janela **Configure Connection to CX Cloud**



Registro bem-sucedido

Help

[Back to Data Sources](#)

Configure connection to CX Cloud

Connect a Cisco DNA Center

IP Address or FQDN Location (City, State, Country)

Username Password

Collection Frequency: Time: IST:

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

The first data source you add must be a Cisco DNA Center. After that you can add additional Cisco DNA Centers and devices not connected to a controller.


[Connect This Data Source](#)

Configurar conexão

3. Insira os dados e clique em **Conectar Esta Fonte de Dados**. A mensagem de confirmação "Conectado com êxito" é exibida.

Configure connection to CX Cloud

Successfully Connected



Cisco DNA Center live.com
Inventory collection runs every day At 02:00 AM IST
First inventory collection will run immediately when you finish adding your data sources

Connect another data source to CX Cloud Agent?

[+](#) Add Another Cisco DNA Center


[Done Connecting Data Sources](#)

DNAC adicionado com êxito


Note: Clique em **Add Another Cisco DNA Center** para adicionar vários DNACs.

Configure connection to CX Cloud


Successfully Connected



Cisco DNA Center live.com
Inventory collection runs every day At 02:00 AM IST
First inventory collection will run immediately when you finish adding your data sources



Cisco DNA Center live.com
Inventory collection runs every day At 01:00 AM IST
First inventory collection will run immediately when you finish adding your data sources



Cisco DNA Center demo.com
Inventory collection runs every day At 01:00 AM IST
First inventory collection will run immediately when you finish adding your data sources

Connect another data source to CX Cloud Agent?



Add Another Cisco DNA Center

Done Connecting Data Sources

Vários DNACs adicionados

4. Clique em **Conexão Concluída de Origens de Dados**. A janela **Fontes de dados** se abre.

Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.0.3	1 minutes ago	Running
10.197.238.126	Cisco DNA Center	1 minutes ago	Reachable
22.1.90.1	Cisco DNA Center	1 minutes ago	Reachable

Origem dos dados

Implantação e configuração de rede

Qualquer uma destas opções pode ser selecionada para implantar o CX Cloud Agent:

- Se você selecionar VMware vSphere/vCenter Thick Client ESXi 5.5/6.0, acesse [Thick Client](#)
- Se você selecionar VMware vSphere/vCenter Web Client ESXi 6.0, acesse [Web Client](#) vSphere ou [Center](#)
- Se você selecionar Oracle Virtual Box 5.2.30, acesse [Oracle VM](#)
- Se você selecionar Microsoft Hyper-V, acesse [Hyper-V](#)

Implantação do OVA

Instalação do Thick Client ESXi 5.5/6.0

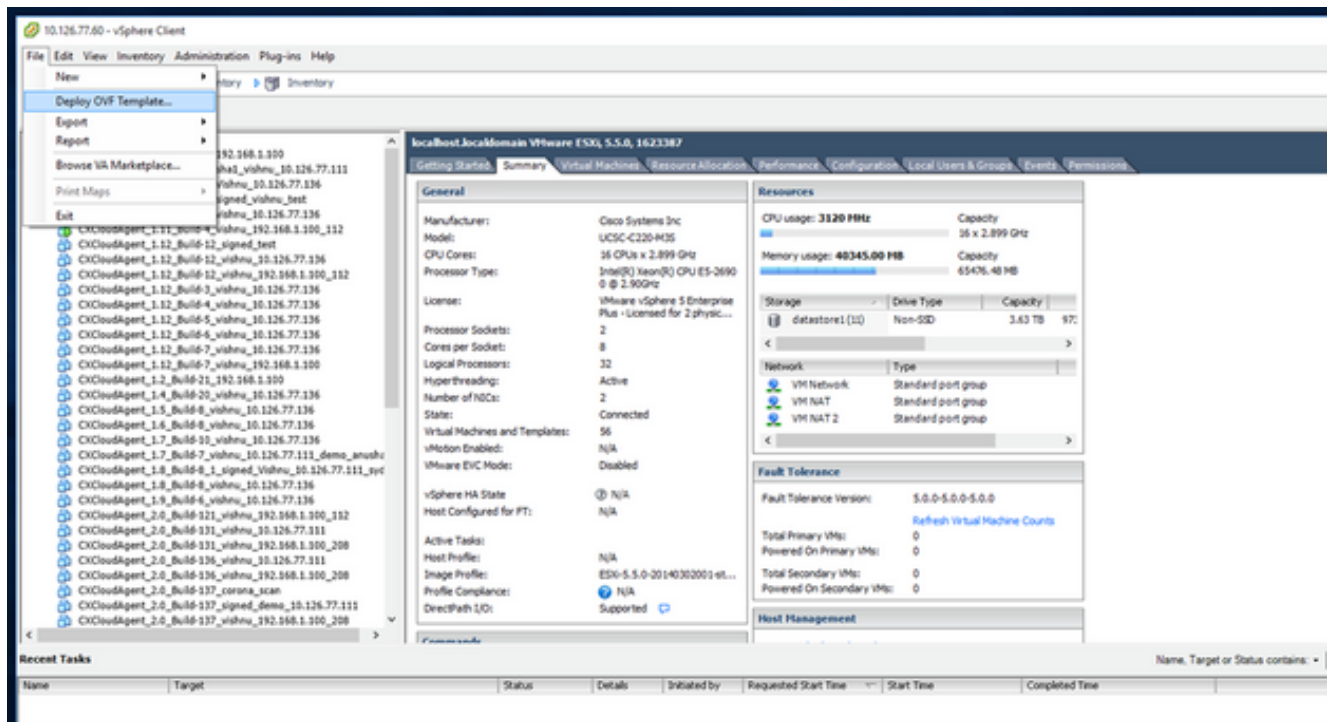
Esse cliente permite a implantação do CX Cloud Agent OVA usando o cliente thick vSphere.

1. Após fazer o download da imagem, inicie o VMware vSphere Client e faça login.



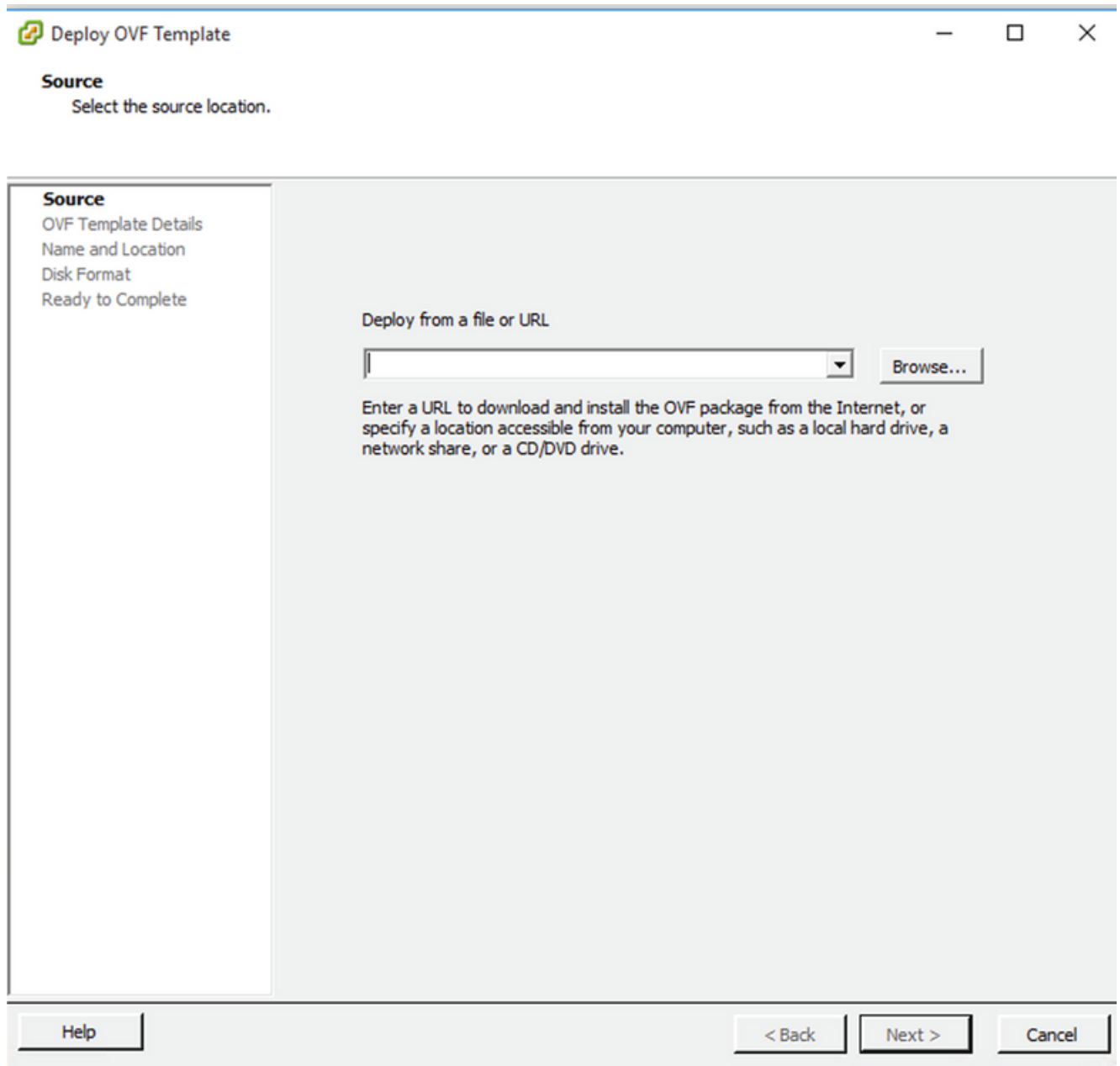
Login

2. Navegue até File > Deploy OVF Template.



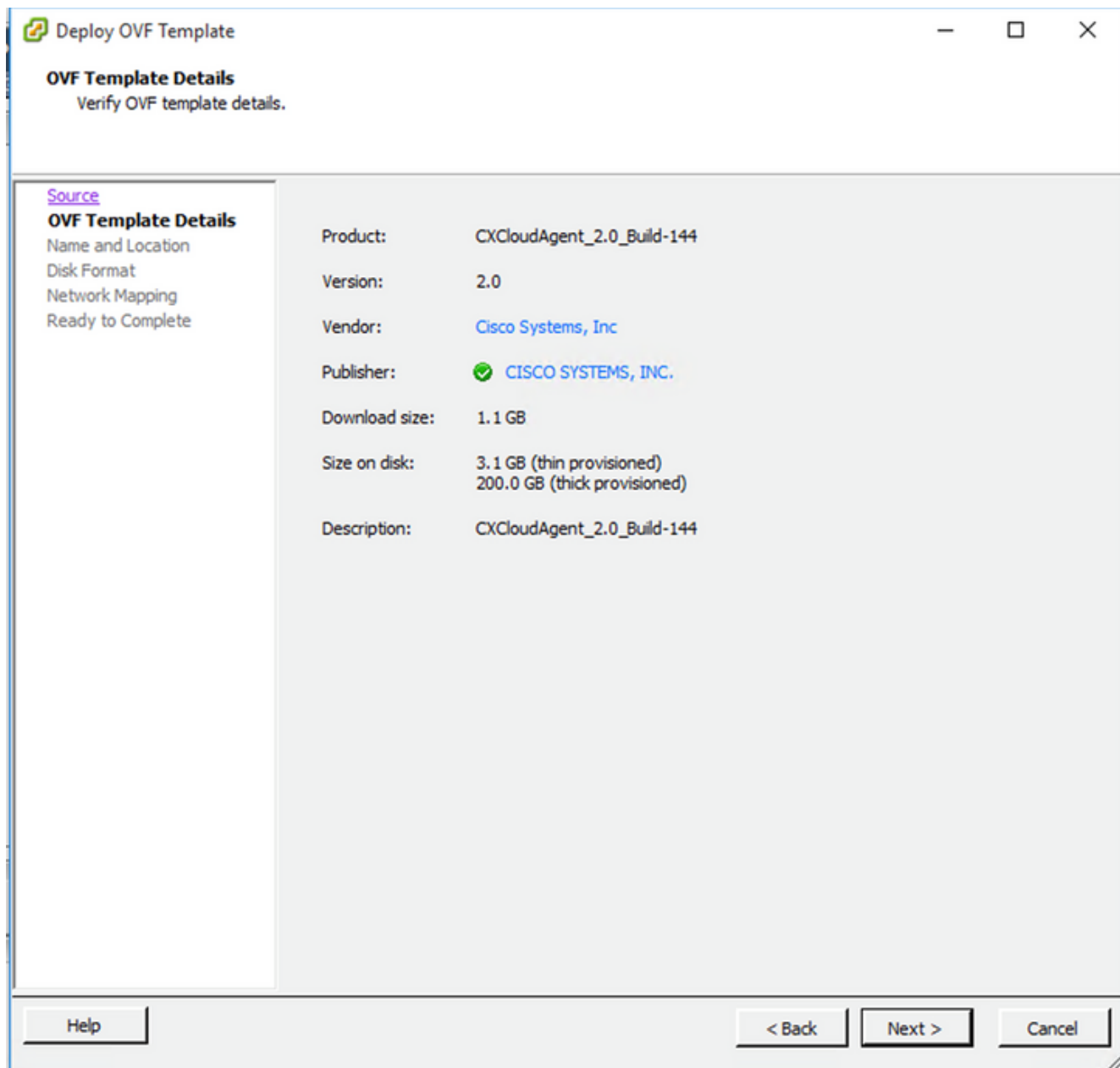
vSphere Client

3. Procure para selecionar o arquivo OVA e clique em Next.



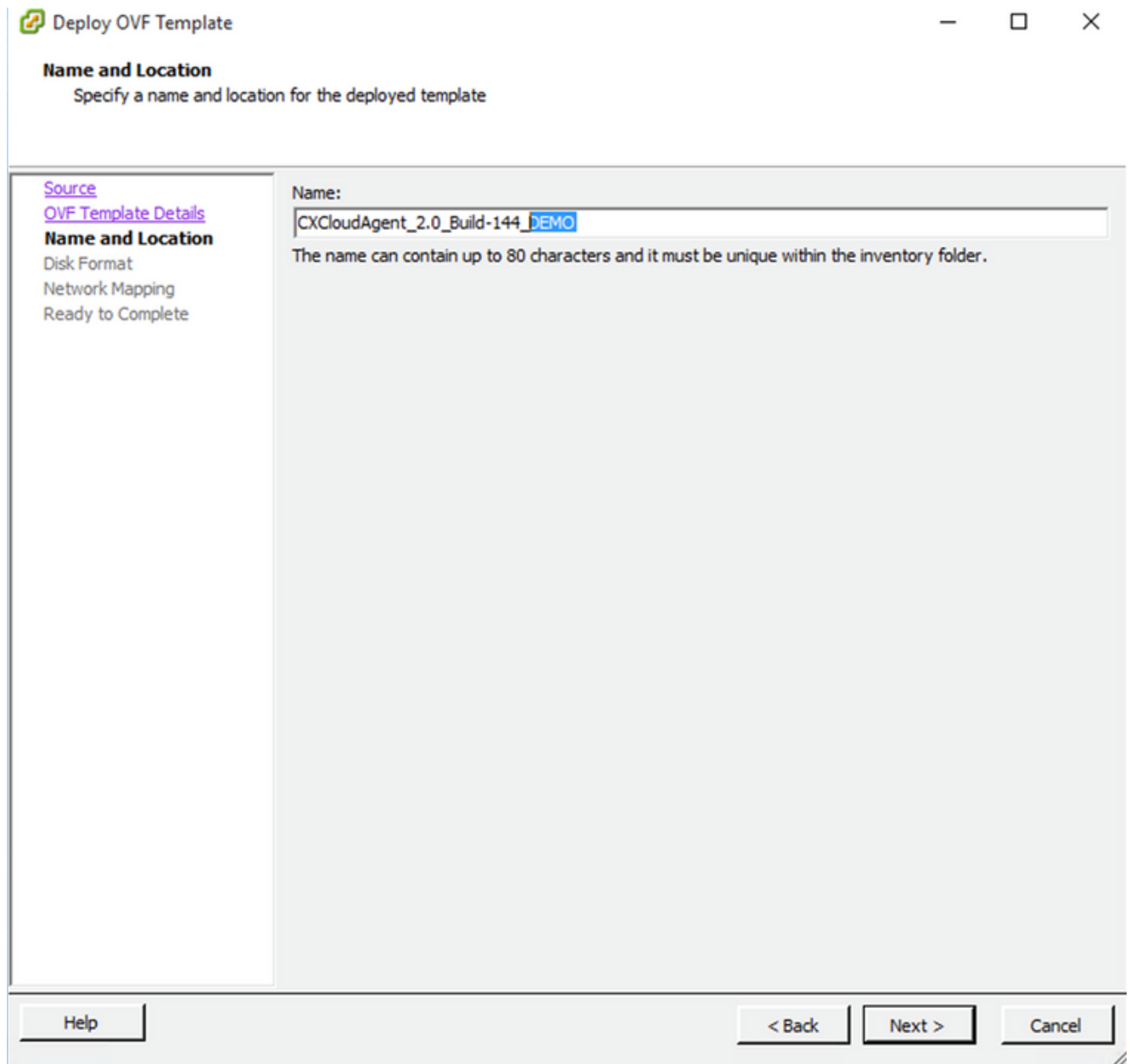
Caminho do OVA

4. Verifique a OVF Details e clique em Next.



Detalhes do modelo

5. Insira um Unique Name e clique em Next.



Nome e local

6. Selecione um **Disk Format** e clique em **Next** (Recomenda-se provisionamento reduzido).

Disk Format

In which format do you want to store the virtual disks?

Source OVF Template Details Name and Location Disk Format Network Mapping Ready to Complete	<p>Datastore: <input type="text" value="datastore1 (11)"/></p> <p>Available space (GB): <input type="text" value="973.1"/></p> <p><input type="radio"/> Thick Provision Lazy Zeroed <input type="radio"/> Thick Provision Eager Zeroed <input checked="" type="radio"/> Thin Provision</p>
---	--

Formato de disco

7. Seleccione o Power on after deployment e clique em Finish.

Ready to Complete

Are these the options you want to use?

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

When you click Finish, the deployment task will be started.

Deployment settings:

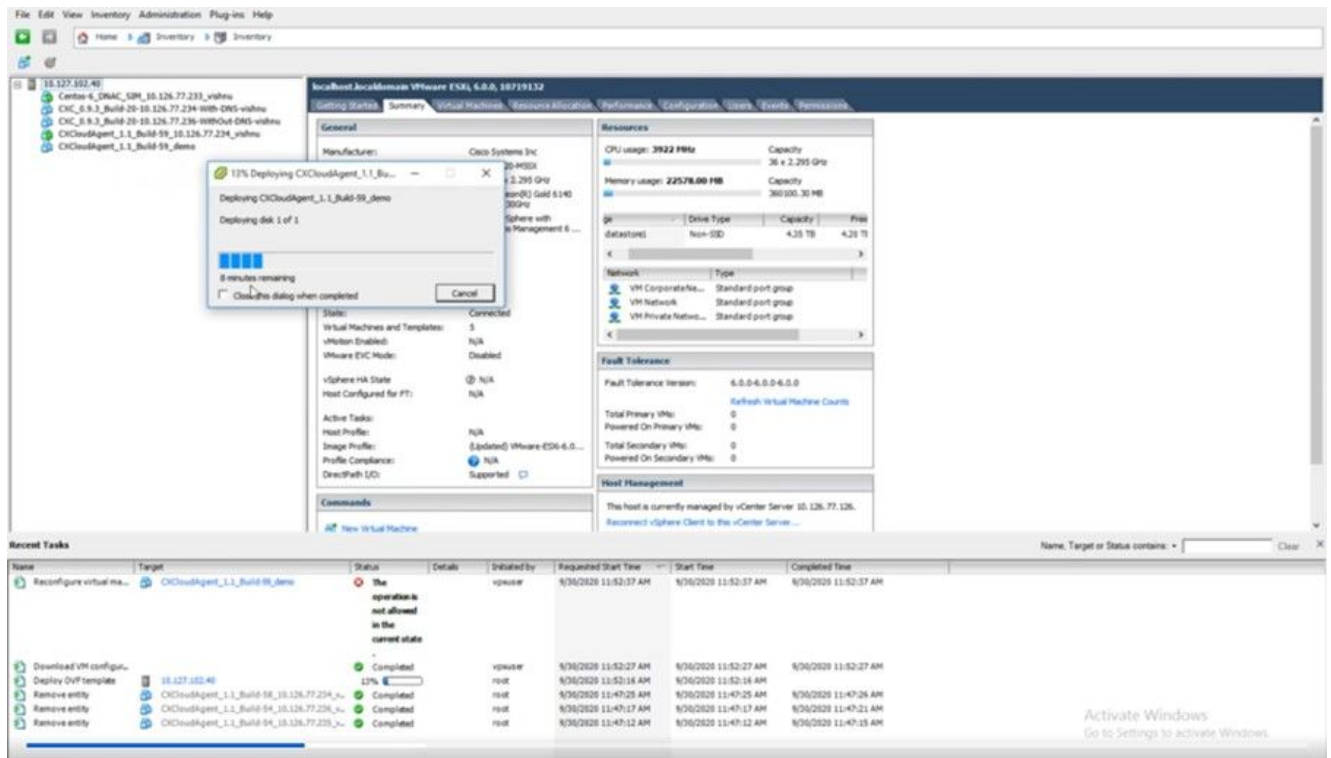
OVF file:	C:\Users\oxcadmin\Downloads\OVA\CXCloudAgent_2.0...
Download size:	1.1 GB
Size on disk:	3.1 GB
Name:	CXCloudAgent_2.0_Build-144_DEMO
Host/Cluster:	localhost
Datastore:	datastore1 (11)
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"

Power on after deployment

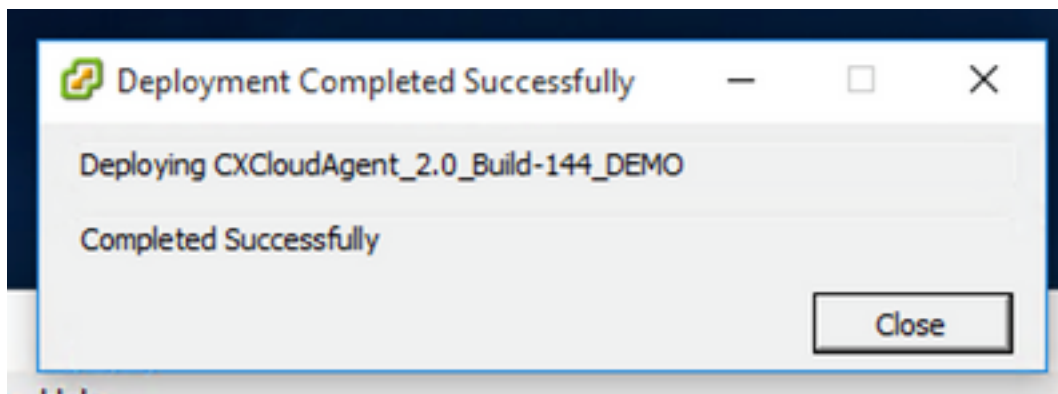
Help < Back Finish Cancel

Pronto para concluir

A implantação pode levar vários minutos. Aguarde até receber uma mensagem de que foi realizado com sucesso.



Implantação em andamento



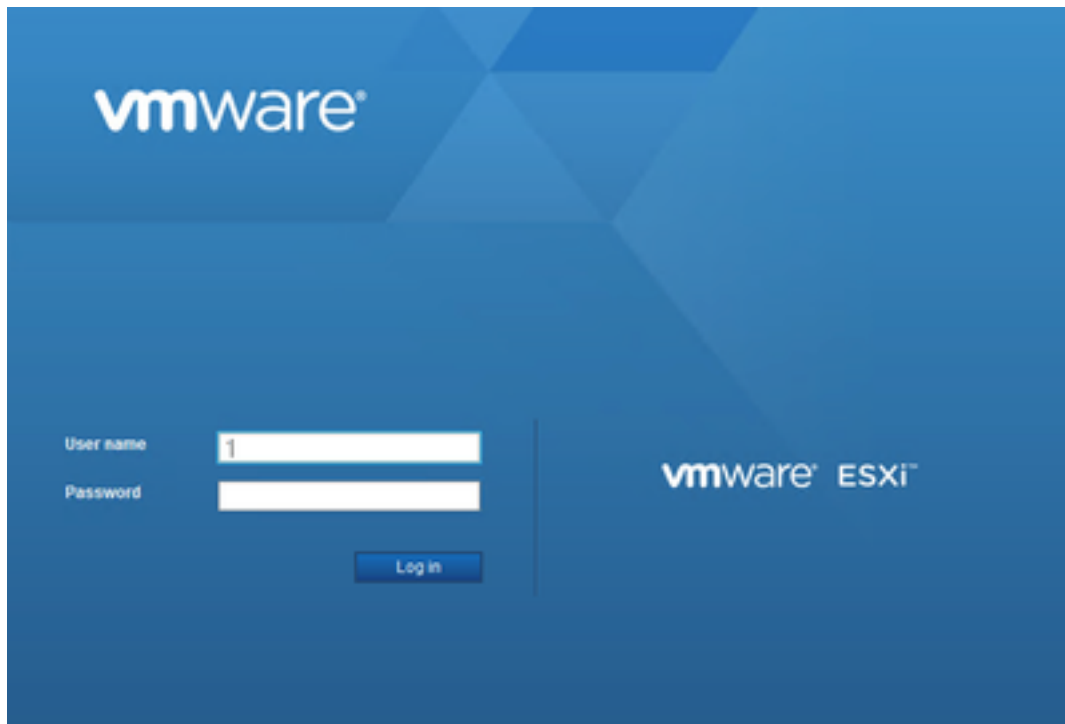
Implantação concluída

8. Selecione a VM recém-implantada, abra o console e vá para [Network Configuration](#).

Instalação do Web Client ESXi 6.0

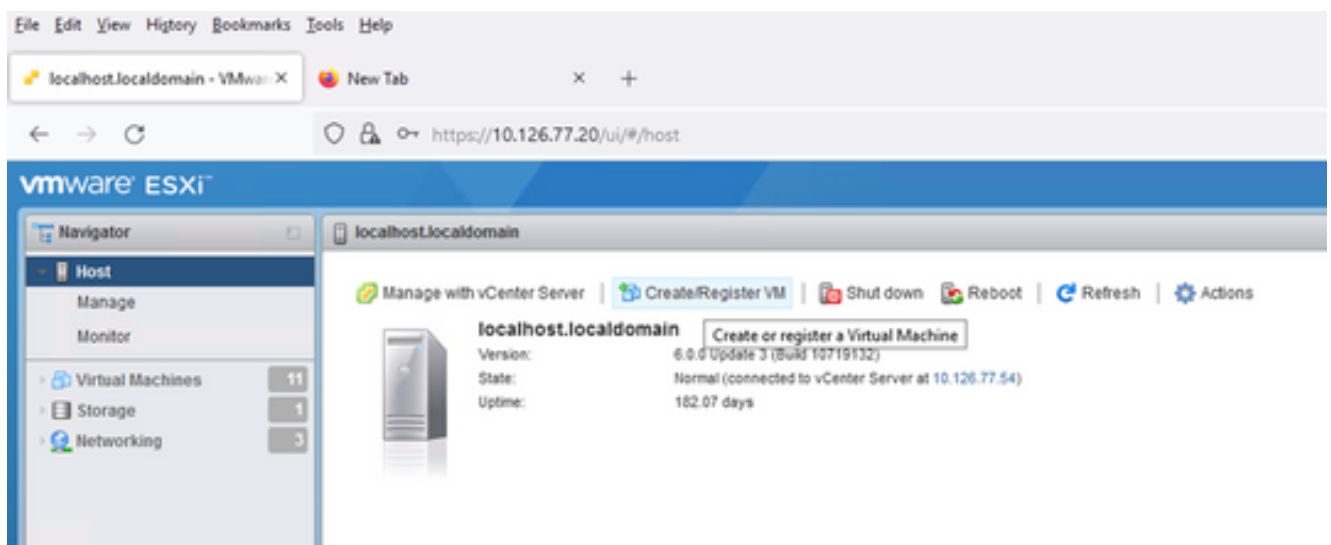
Esse cliente implanta o CX Cloud Agent OVA usando a Web do vSphere.

1. Faça login na interface do usuário do VMWare com as credenciais do ESXi/hipervisor usadas para implantar a VM.

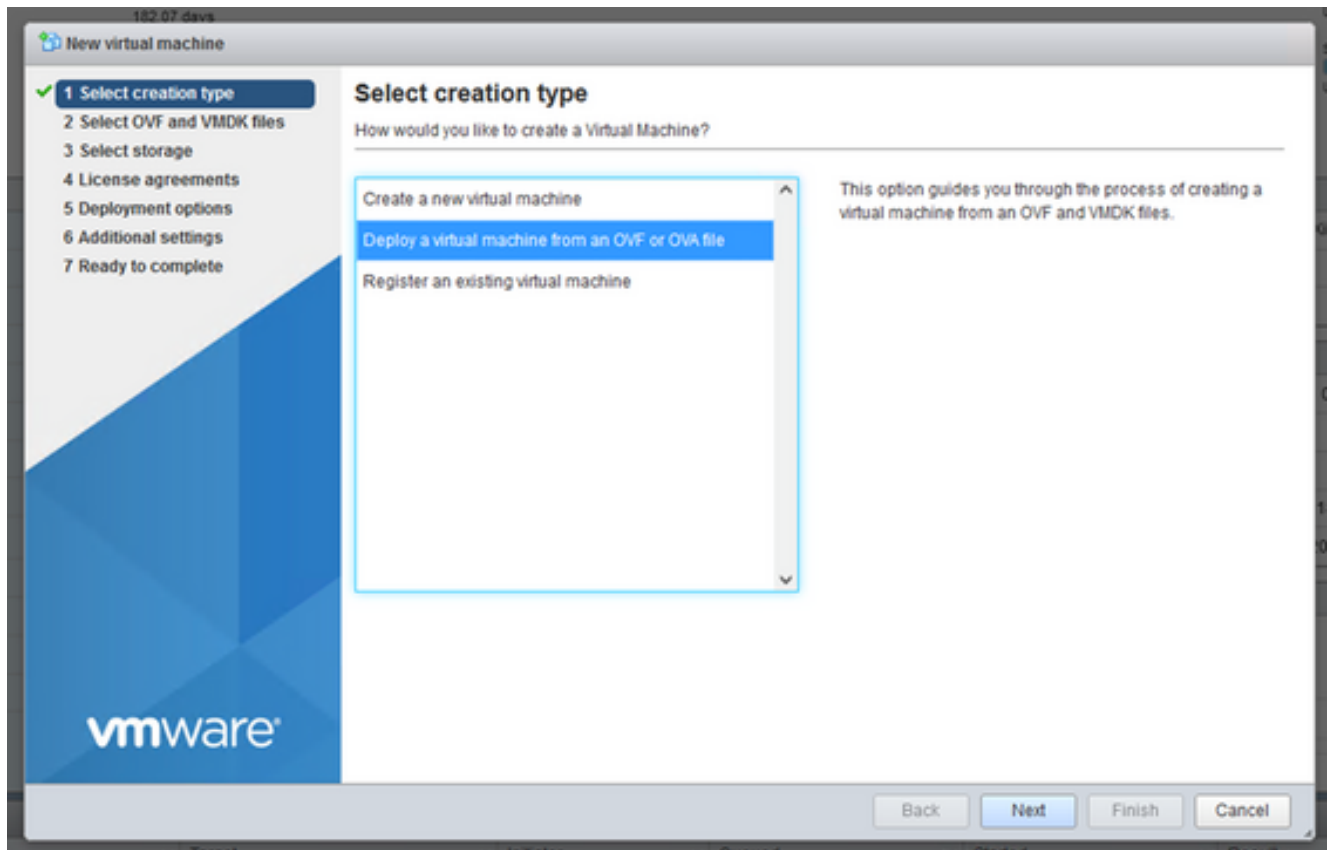


Login no VMware ESXi

2. Selecionar Virtual Machine > Create / Register VM.

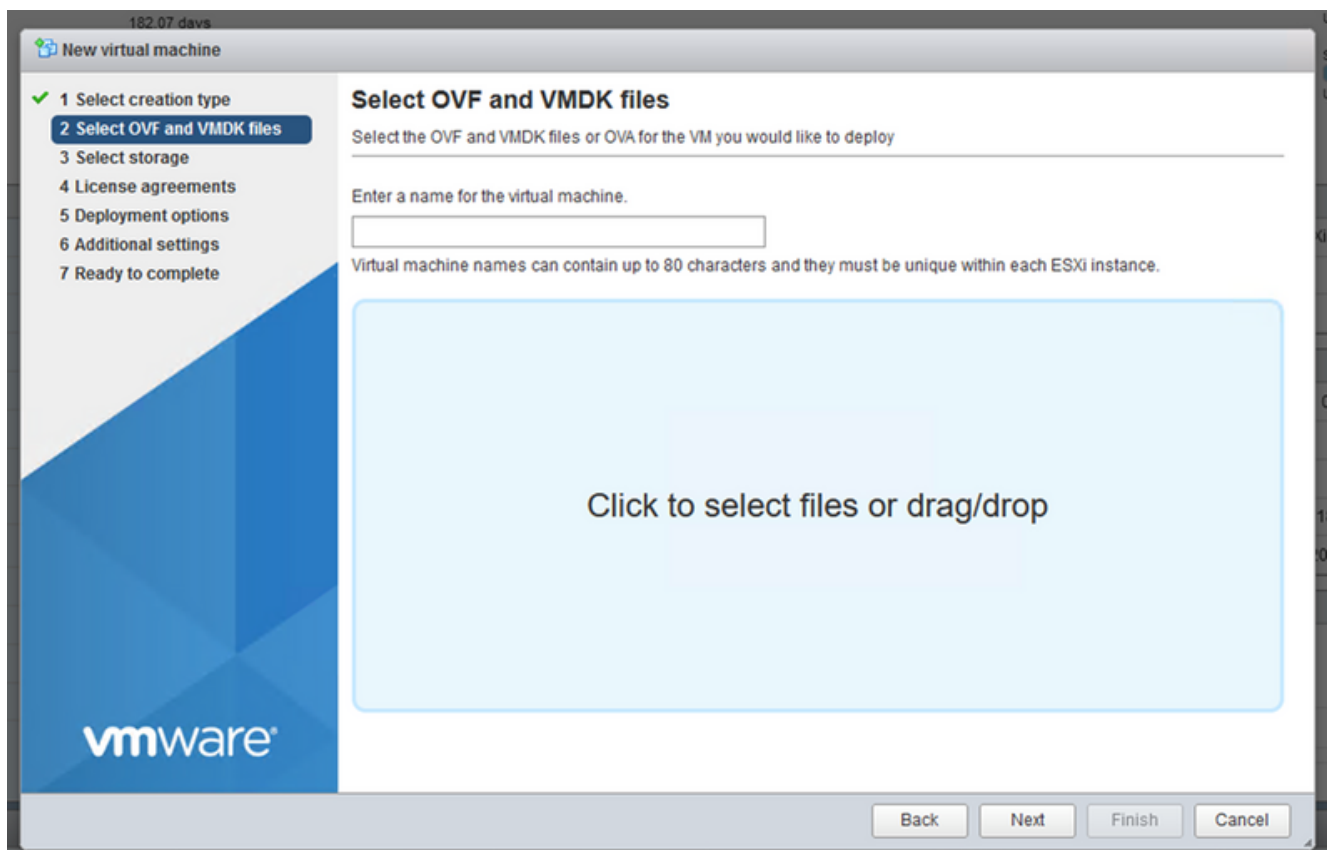


Criar VM



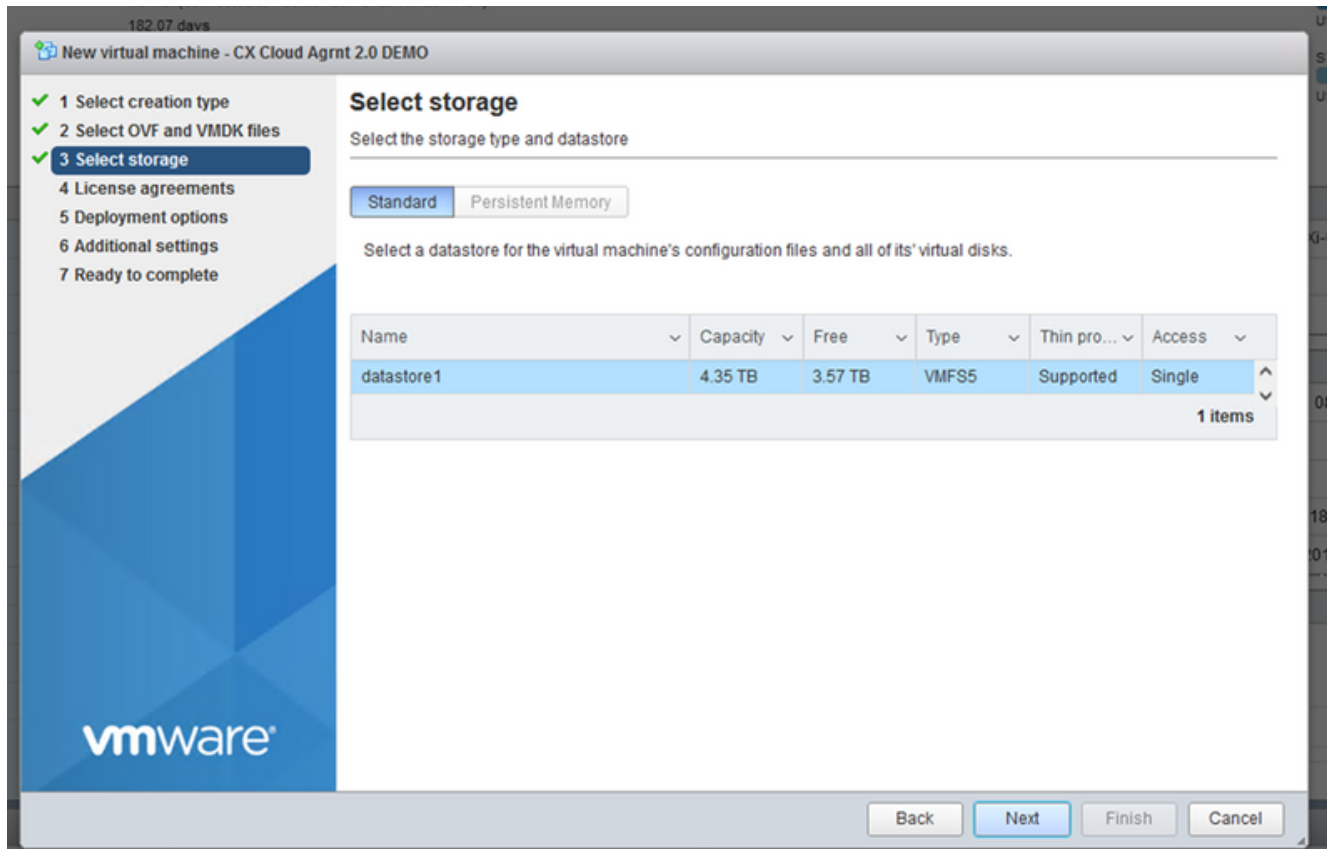
Implantação do OVA

3. Selecionar Deploy a virtual machine from an OVF or OVA file e clique em Next.
4. Insira o nome da VM, procure para selecionar o arquivo ou arraste e solte o arquivo OVA baixado.
5. Clique em Next.

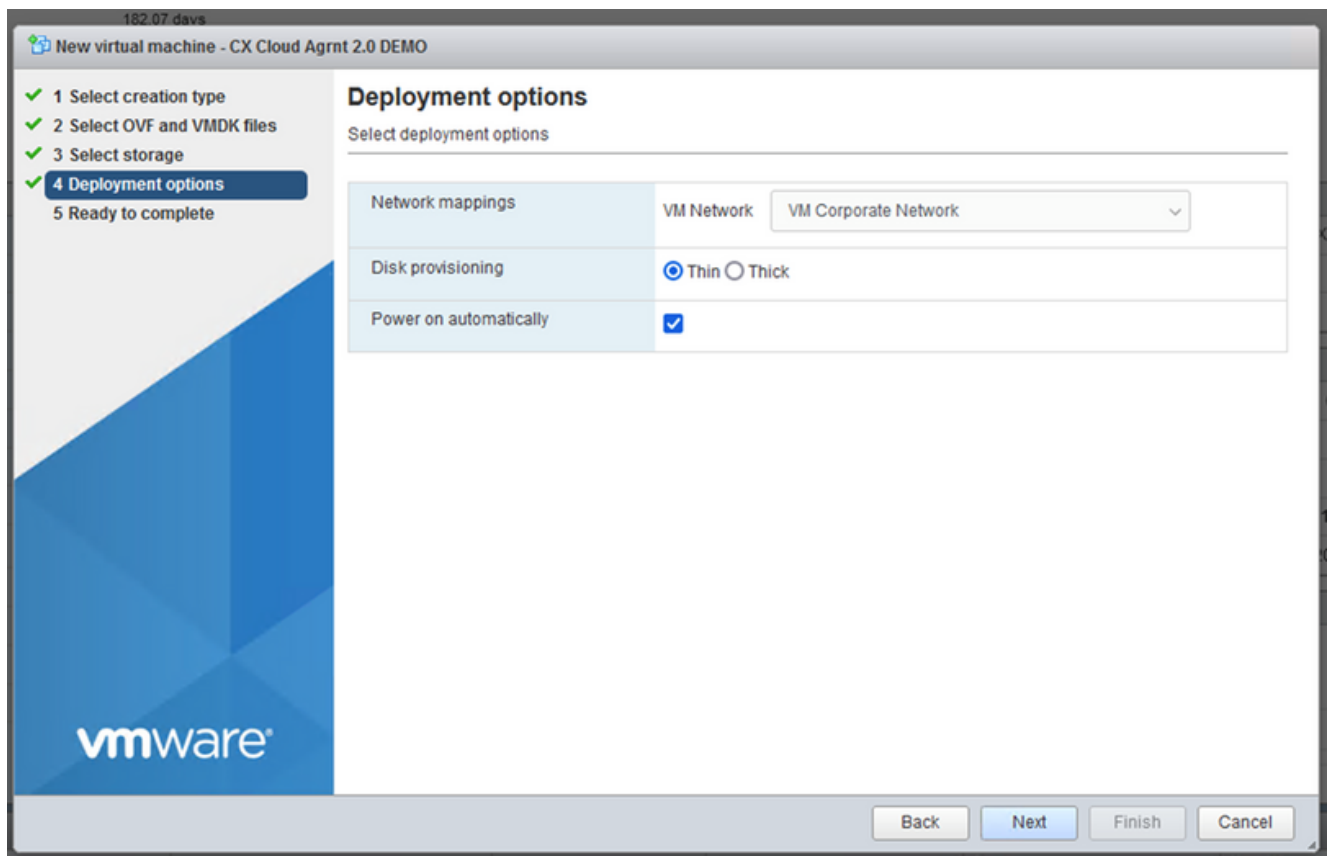


Seleção do OVA

6. Selecionar Standard Storage e clique em Next.



Selecionar armazenamento



Opções de implantação

7. Selecione as opções de Implantação apropriadas e clique em Next.

New virtual machine - CX Cloud Agrnt 2.0 DEMO

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	CXCloudAgent_2.0_Build-144
VM Name	CX Cloud Agrnt 2.0 DEMO
Disks	CXCloudAgent_2.0_Build-144-1_signed-sha1-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: VM Corporate Network
Guest OS Name	Unknown

⚠ Do not refresh your browser while this VM is being deployed.

Back Next Finish Cancel

Pronto para concluir

File Edit View History Bookmarks Tools Help

localhost.localdomain - VMware vSphere

https://10.126.77.20/ui/#/host

root@10.126.77.20 | Help | Search

localhost.localdomain

Version: 6.0.0 Update 3 (Build 10719132)
State: Normal (connected to vCenter Server at 10.126.77.54)
Uptime: 182.07 days

CPU: FREE: 79.2 GHz, USED: 3.4 GHz, CAPACITY: 82.6 GHz
MEMORY: FREE: 232.68 GB, USED: 118.98 GB, CAPACITY: 351.66 GB
STORAGE: FREE: 3.57 TB, USED: 803.28 GB, CAPACITY: 4.35 TB

Hardware	
Manufacturer	Cisco Systems Inc
Model	UCSC-C220-M5SX

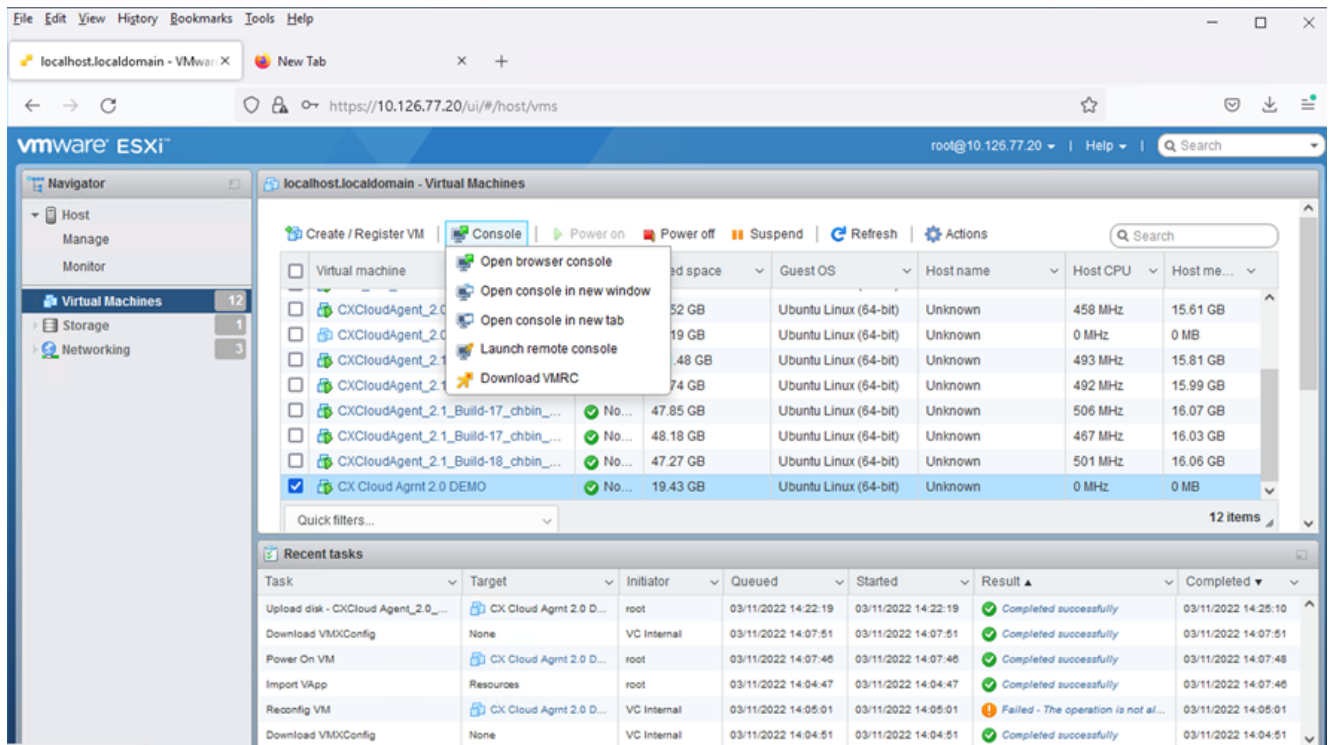
Configuration	
Image profile	(Updated) VMware-ESXi-6.0.0-9313334-Custom-Cisco-6.0.3.5 (Cisco)
vSphere HA state	Not configured

Task	Target	Initiator	Queued	Started	Result	Completed
Upload disk - CXCloud Agent_2.0...	CX Cloud Agrnt 2.0 D...	root	03/11/2022 14:22:19	03/11/2022 14:22:19	Completed successfully	03/11/2022 14:25:10
Download VMXConfig	None	VC Internal	03/11/2022 14:07:51	03/11/2022 14:07:51	Completed successfully	03/11/2022 14:07:51
Power On VM	CX Cloud Agrnt 2.0 D...	root	03/11/2022 14:07:46	03/11/2022 14:07:46	Completed successfully	03/11/2022 14:07:48
Import VApp	Resources	root	03/11/2022 14:04:47	03/11/2022 14:04:47	Completed successfully	03/11/2022 14:07:46
Reconfig VM	CX Cloud Agrnt 2.0 D...	VC Internal	03/11/2022 14:05:01	03/11/2022 14:05:01	Failed - The operation is not al...	03/11/2022 14:05:01
Download VMXConfig	None	VC Internal	03/11/2022 14:04:51	03/11/2022 14:04:51	Completed successfully	03/11/2022 14:04:51

Conclusão realizada com sucesso

8. Revise as configurações e clique em Finish.

9. Selecione a VM recém-implantada e selecione Console > Open browser console.



Abrir console

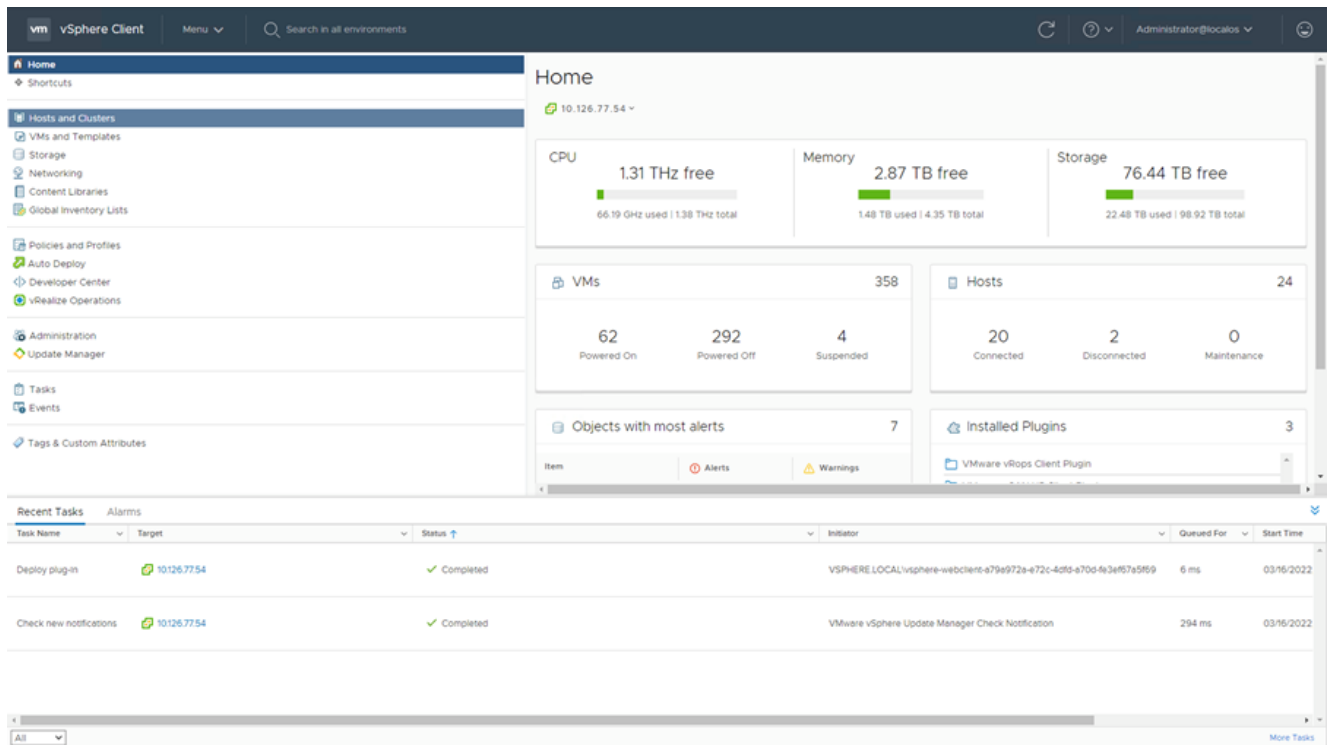
10. Navegue até [Configuração de rede](#).

Instalação do Web Client vCenter

1. Faça login no vCenter Client usando as credenciais do ESXi/hypervisor.

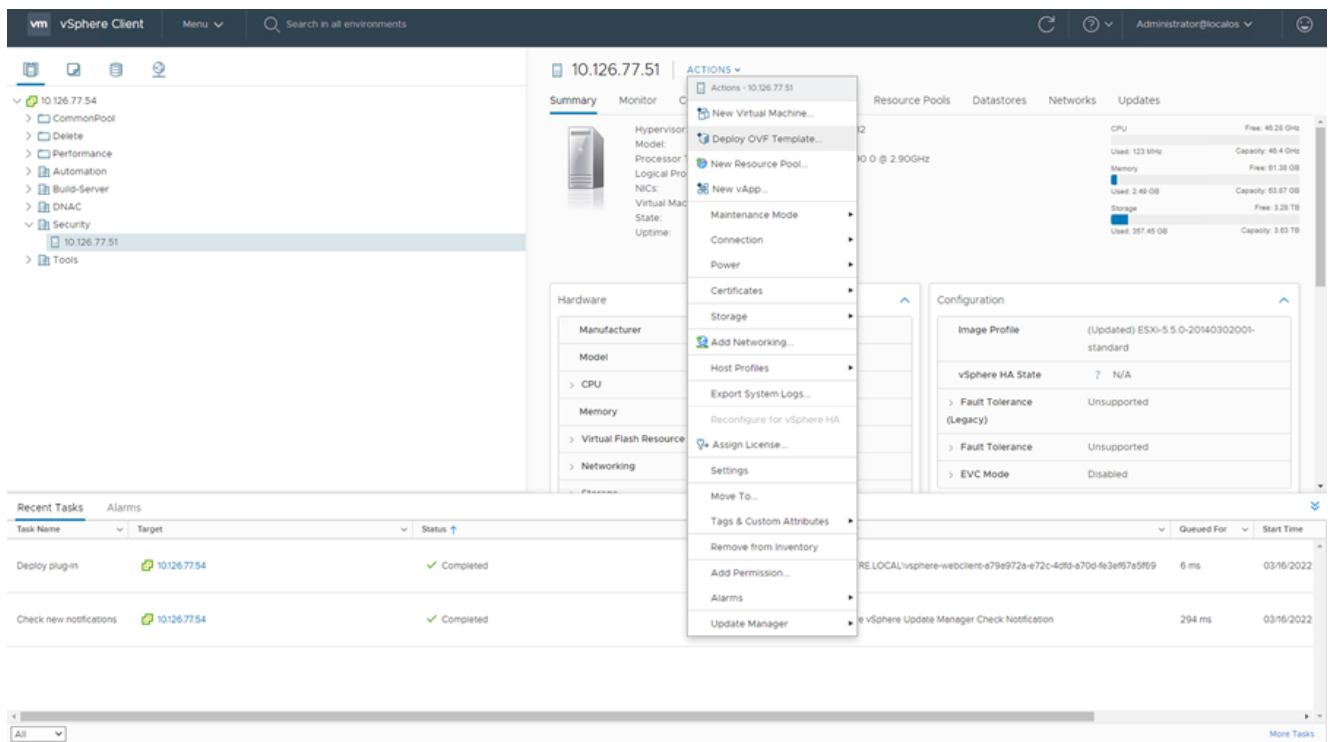


Login

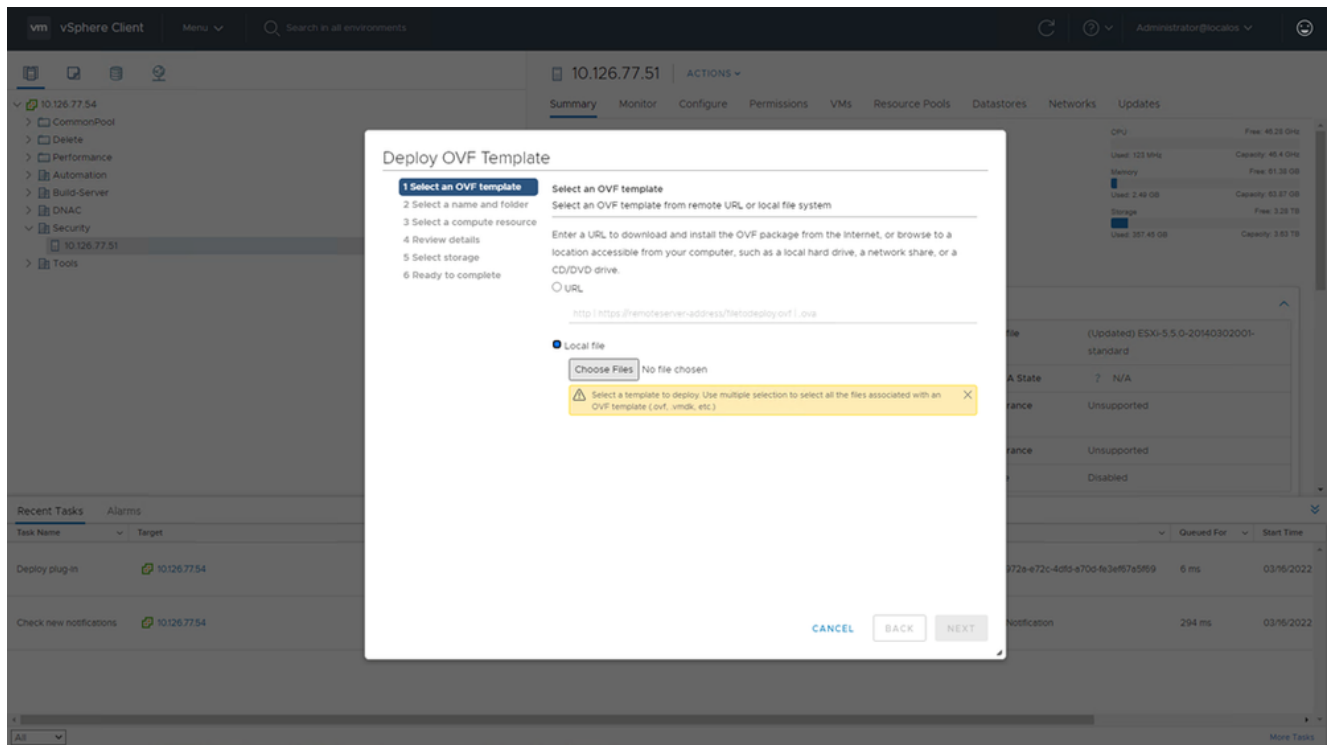


Tela inicial

2. Na página inicial, clique em Hosts and Clusters.
3. Selecione a VM e clique em Action > Deploy OVF Template.



Ações



Selecionar modelo

4. Adicione o URL diretamente ou navegue para selecionar o arquivo OVA e clique em Next.
5. Insira um nome exclusivo e procure o local, se necessário .
6. Clique em 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.

10.126.77.54

> CommonPool

> Delete

> Performance

> Automation

> Build-Server

> DNAC

> Security

> Tools

CANCEL

BACK

NEXT

Nome e Pasta

7. Selecione o recurso de computação e clique em 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 compute resource

Select the destination compute resource for this operation

▼ Security

> 10.126.77.51

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

Selecionar recurso de computação

8. Revise os detalhes e clique em 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_2.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CXCloudAgent_2.0_Build-144
Download size	1.1 GB
Size on disk	3.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

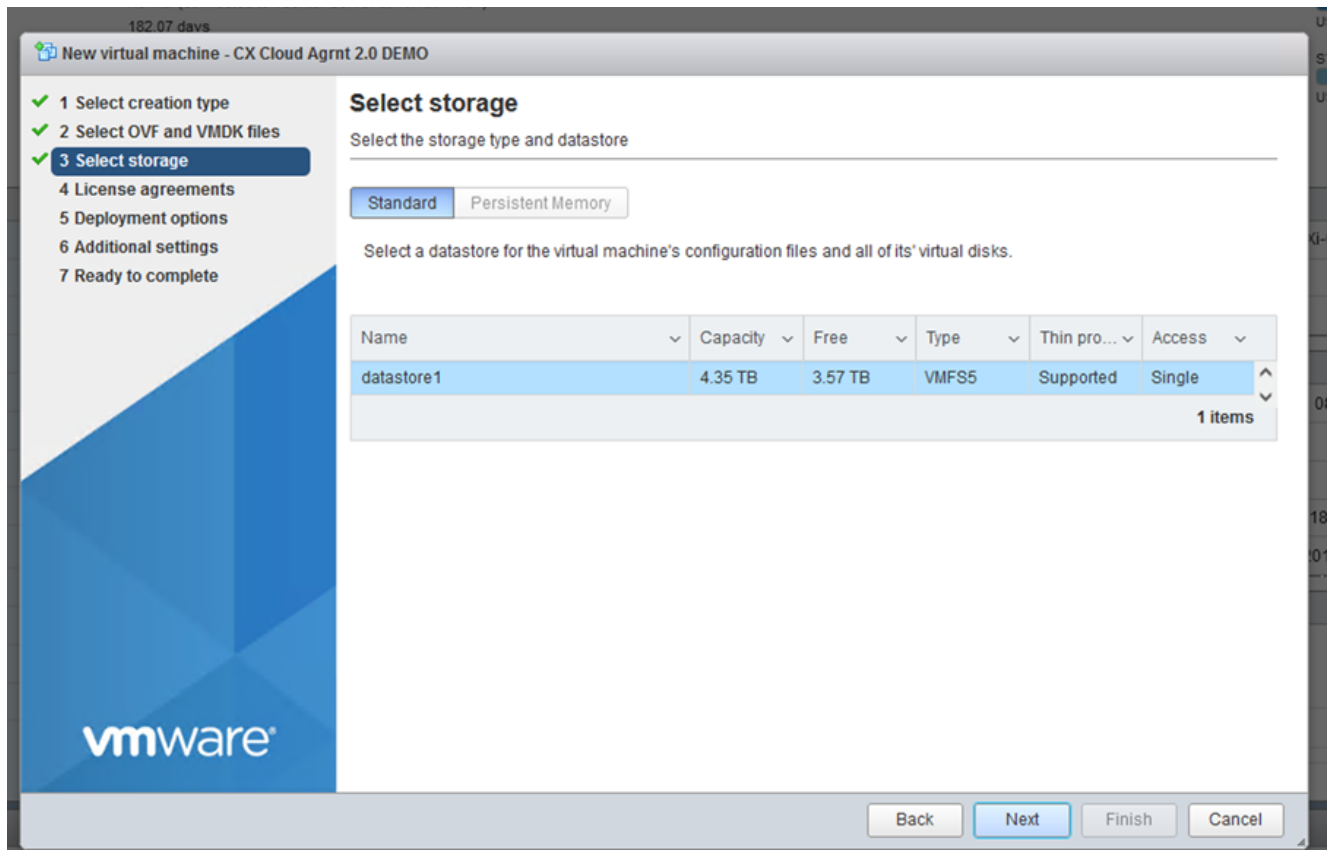
CANCEL

BACK

NEXT

Analisar detalhes

9. Selecione o formato do disco virtual e clique em Next.



Selecionar armazenamento

10. Clique em 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

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

Selecionar redes

11. Clique em Finish.

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	1.1 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

Pronto para concluir

12. Uma nova VM é adicionada. Clique no nome para ver o status.

The screenshot shows the vSphere Client interface for a VM named 'CXCloudAgent_2.0_Build-144-demo'. The VM is currently 'Powered Off'. Key configuration details include:

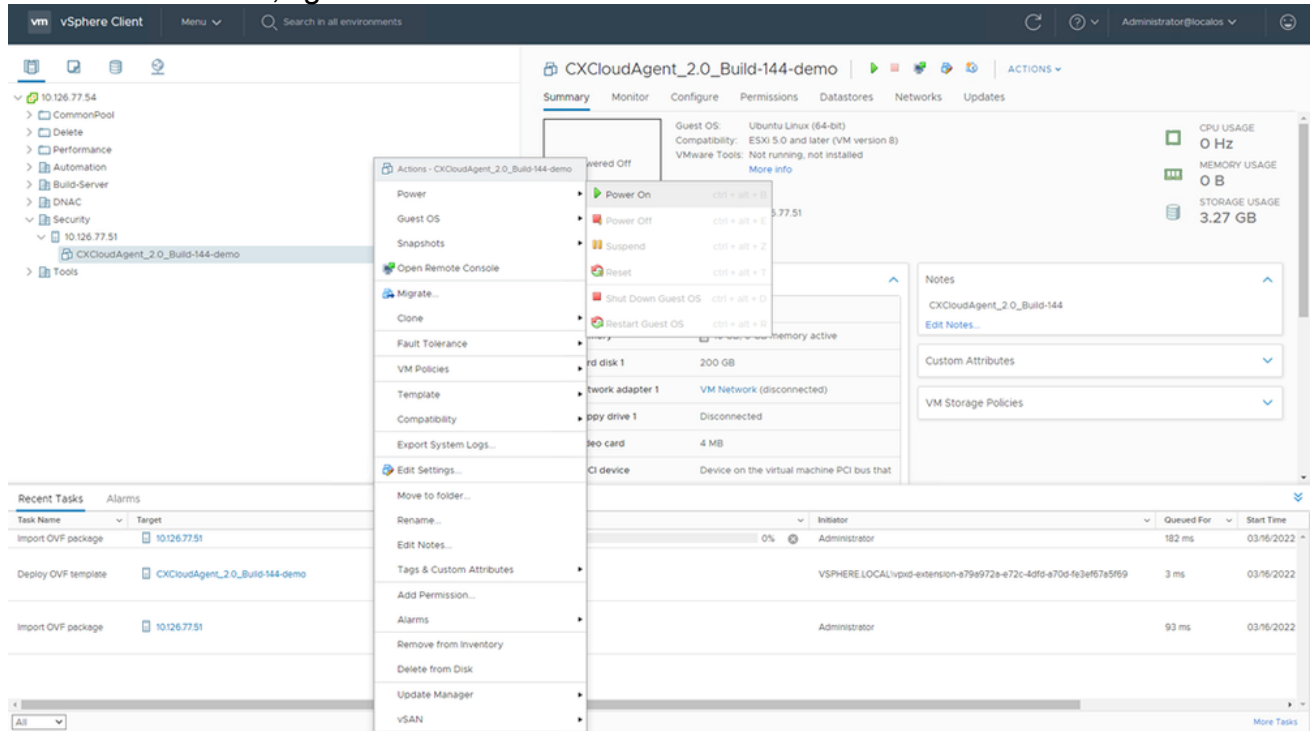
- Guest OS: Ubuntu Linux (64-bit)
- Compatibility: ESXi 5.0 and later (VM version 8)
- VMware Tools: Not running, not installed
- DNS Name: IP Addresses: Host: 10.126.77.51
- VM Hardware: 8 CPU(s), 16 GB memory active, 200 GB Hard disk 1, VM Network (disconnected) Network adapter 1, Disconnected Floppy drive 1, 4 MB Video card, Device on the virtual machine PCI bus that VMCI device.
- Notes: CXCloudAgent_2.0_Build-144
- Custom Attributes: (empty)
- VM Storage Policies: (empty)

The 'Recent Tasks' table at the bottom shows the following tasks:

Task Name	Target	Status	Initiator	Queued For	Start Time
Import OVF package	10.126.77.51	0%	Administrator	182 ms	03/16/2022
Deploy OVF template	CXCloudAgent_2.0_Build-144-demo	✓ Completed	VSPHERE LOCAL/vpxd-extension-e79e972e-e72c-4dfd-e70d-f63ef67a5f69	3 ms	03/16/2022
Import OVF package	10.126.77.51	✓ Completed	Administrator	93 ms	03/16/2022

VM adicionada

13. Uma vez instalada, ligue a VM e abra o console.



Abrir console

14. Navegue até [Configuração de rede](#).

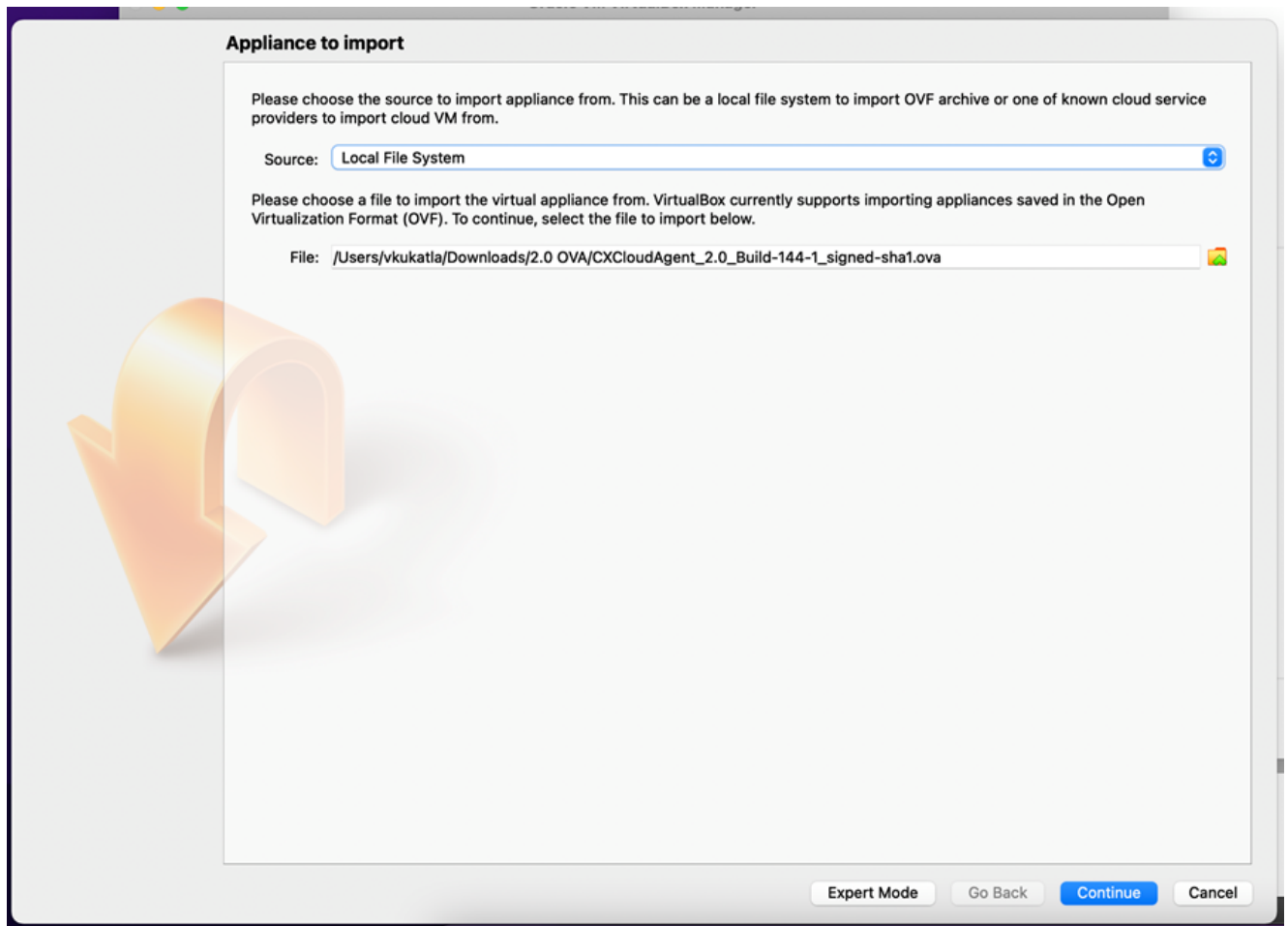
Instalação do Oracle Virtual Box 5.2.30

Esse cliente implanta o CX Cloud Agent OVA por meio do Oracle Virtual Box.



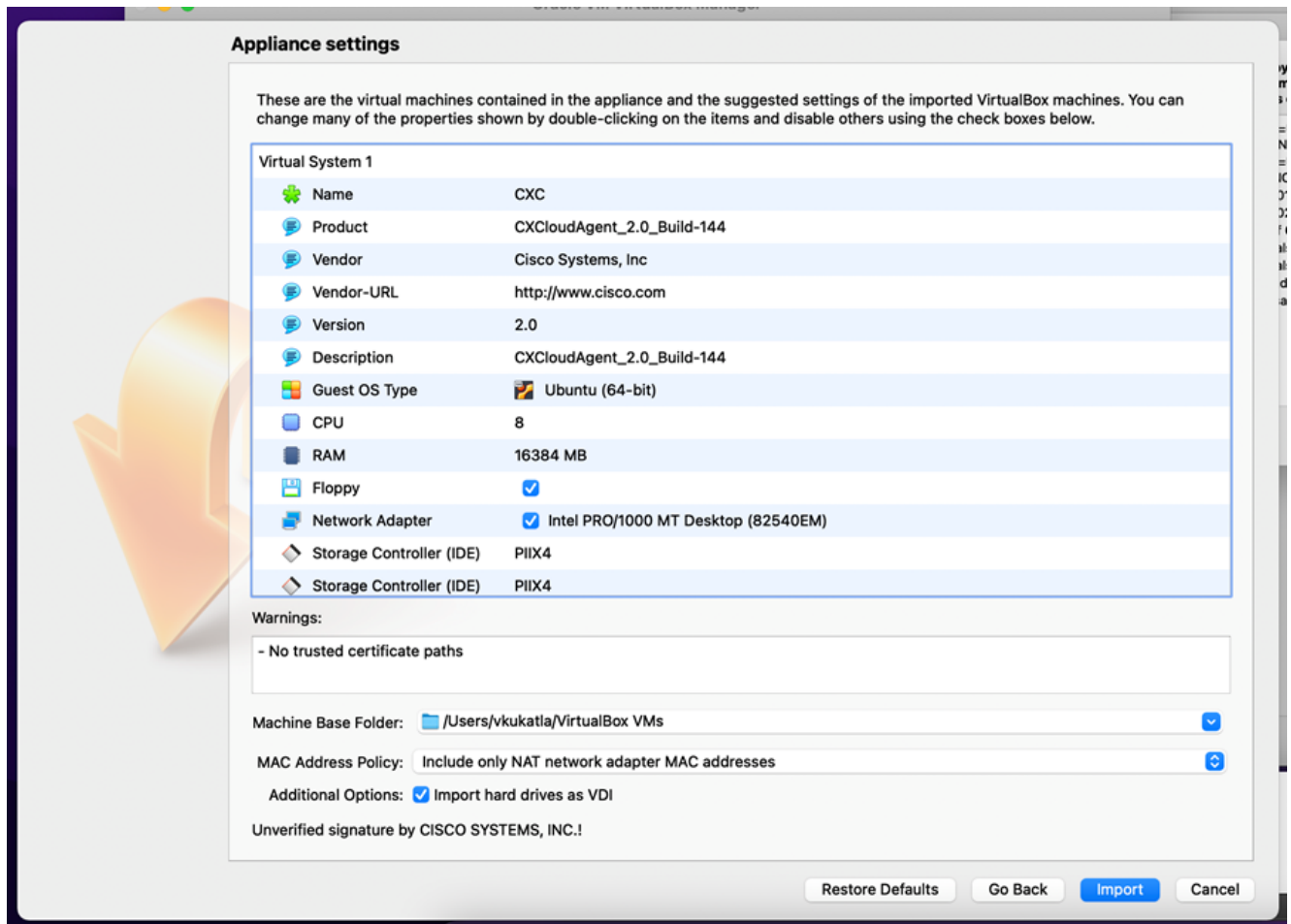
Oracle VM

1. Abra a interface do usuário do Oracle VM e selecione File > Import Appliance.
2. Navegue para importar o arquivo de OVA.



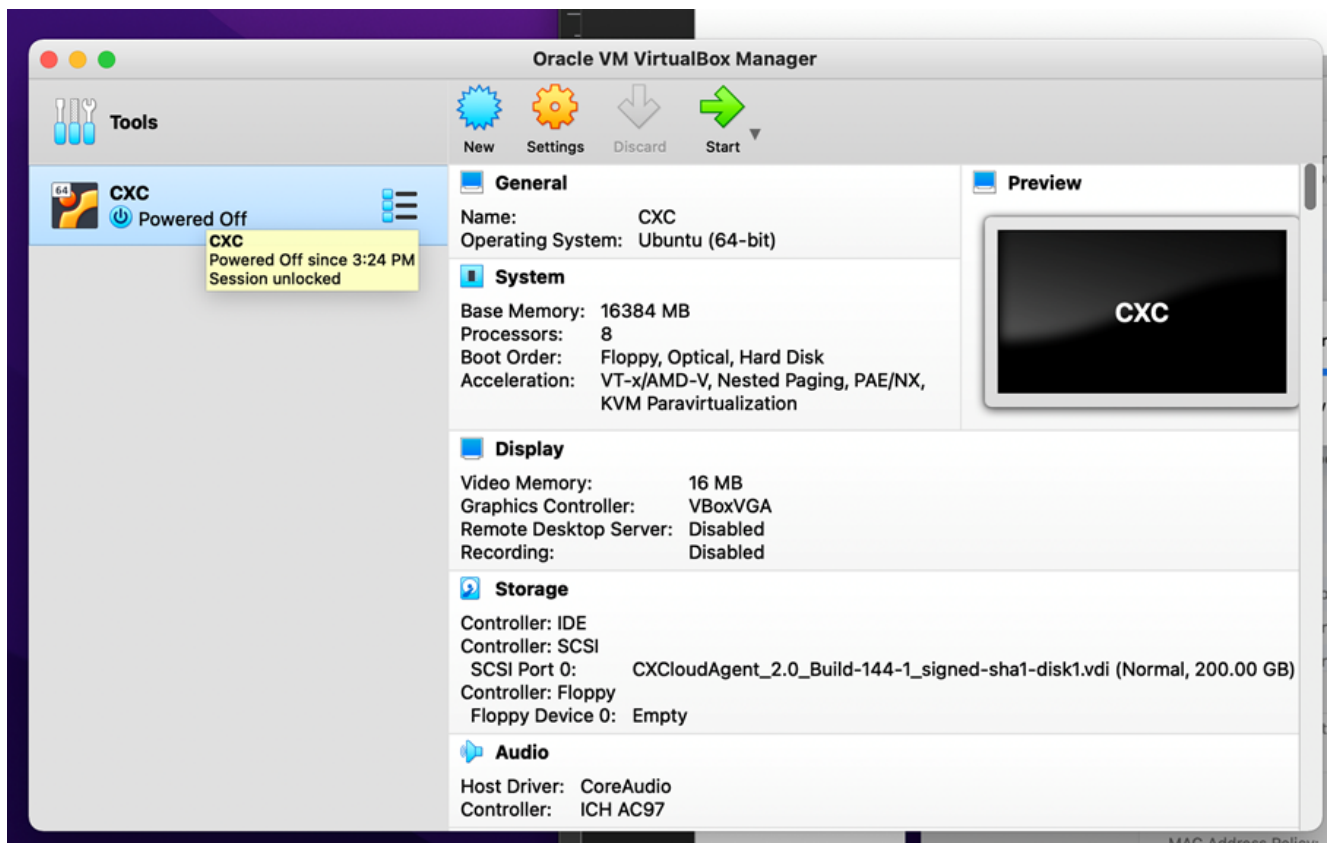
Selecionar arquivo

3. Clique em Import.

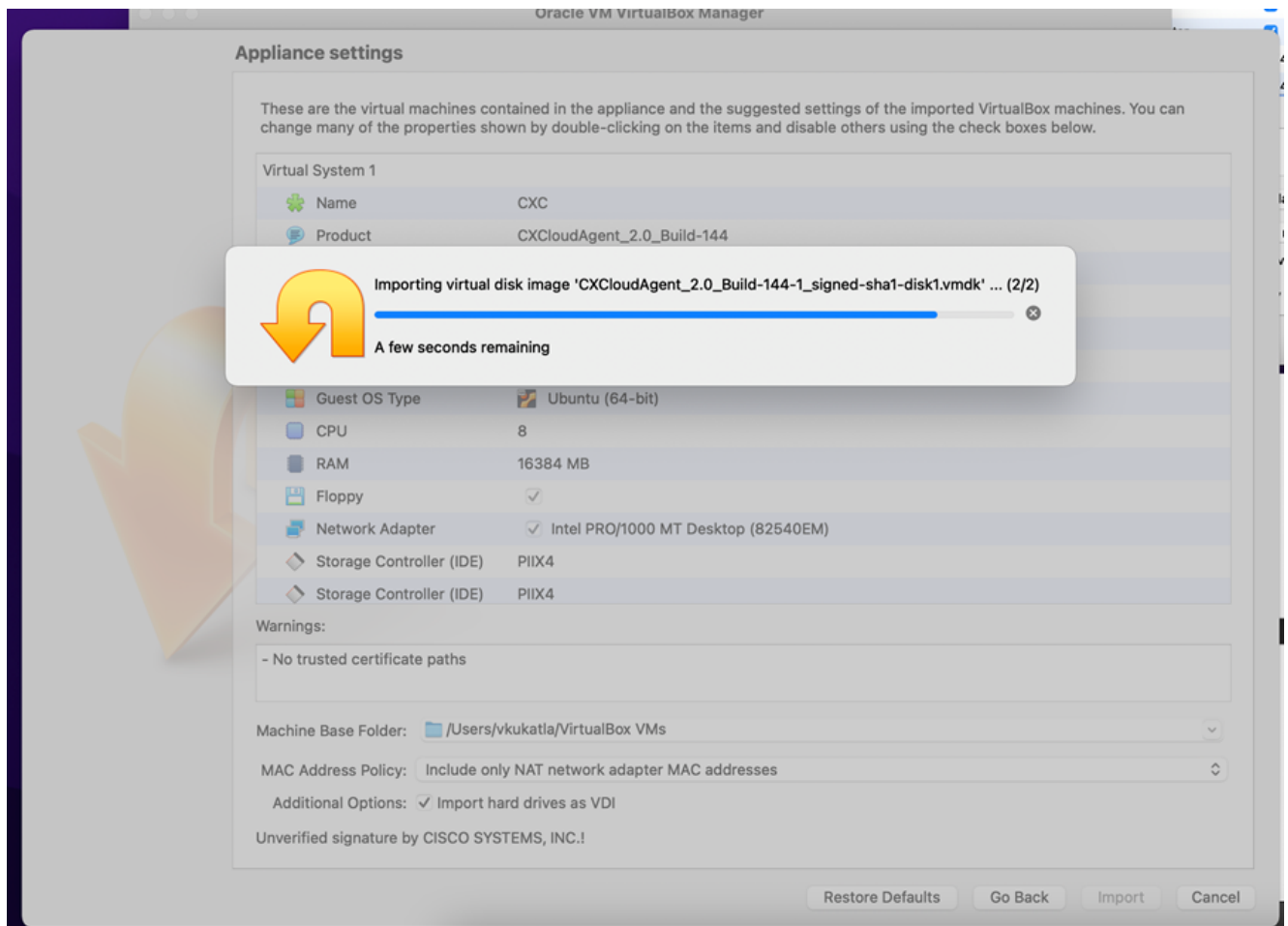


Importar arquivo

4. Selecione a VM recém-implantada e clique em Start.

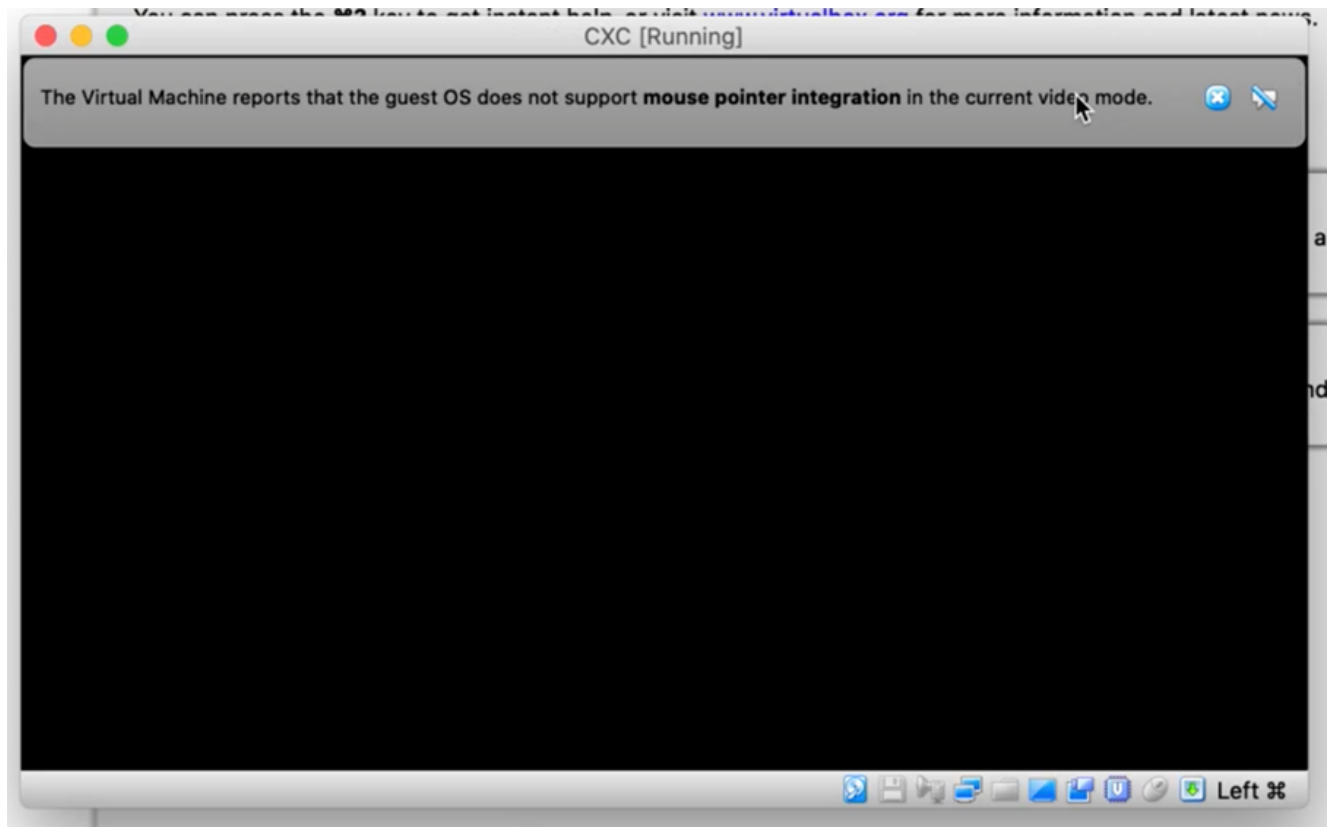


Inicialização do console da VM



Importação em andamento

5. Ligue a VM. O console exibirá.

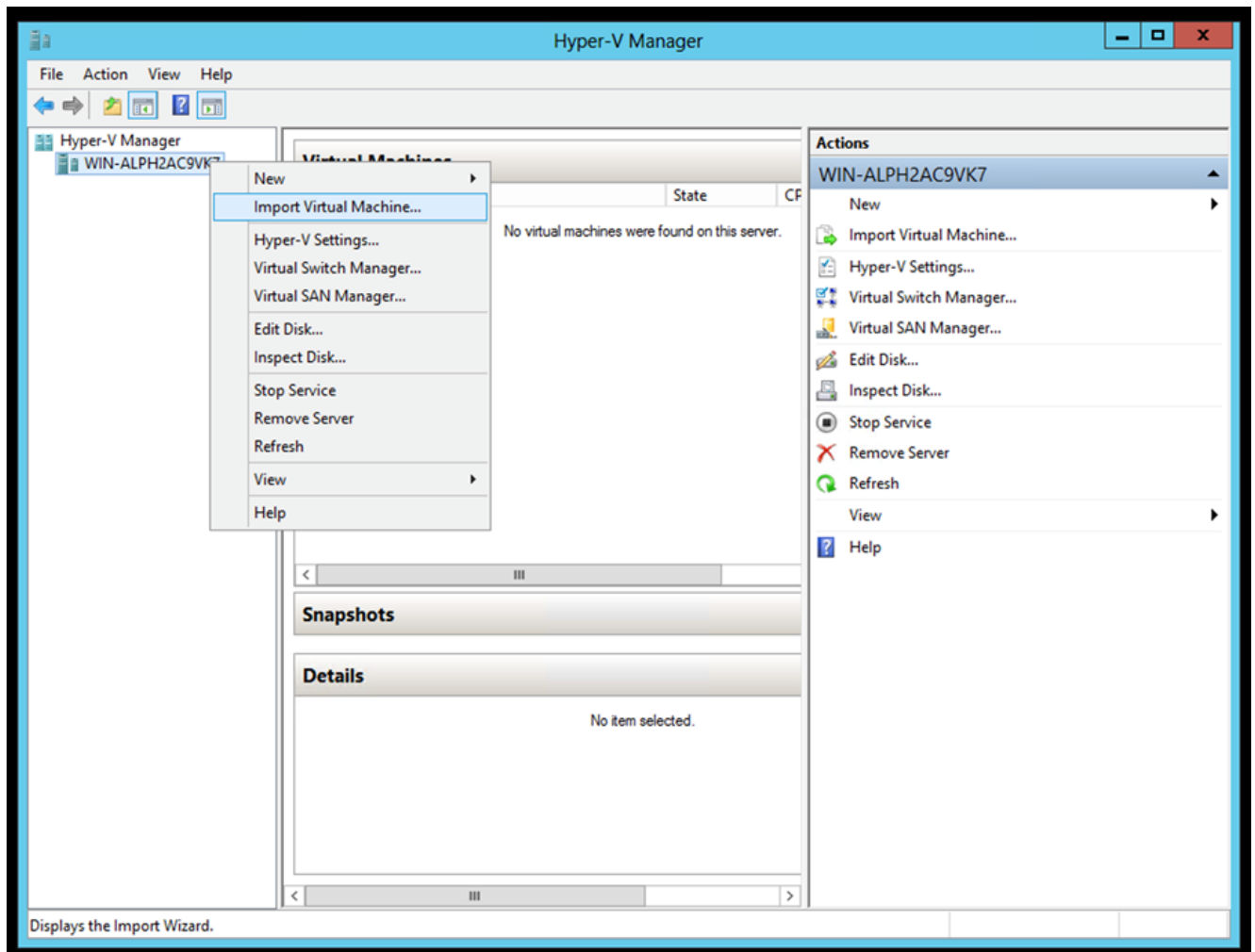


Abrir o console

6. Navegue até [Configuração de rede](#).

Instalação do Microsoft Hyper-V

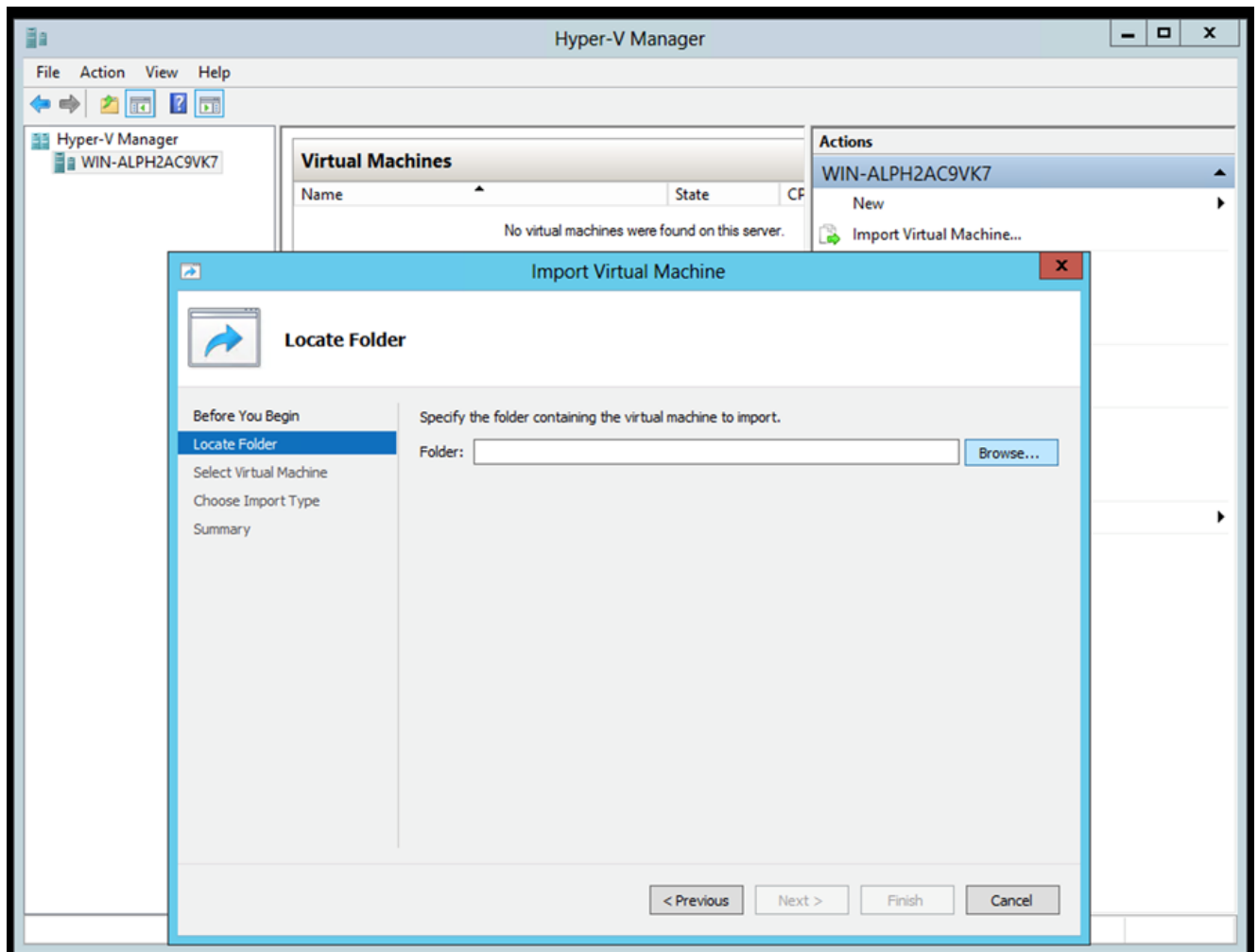
1. Selecionar Import Virtual Machine.



Hyper-V Manager

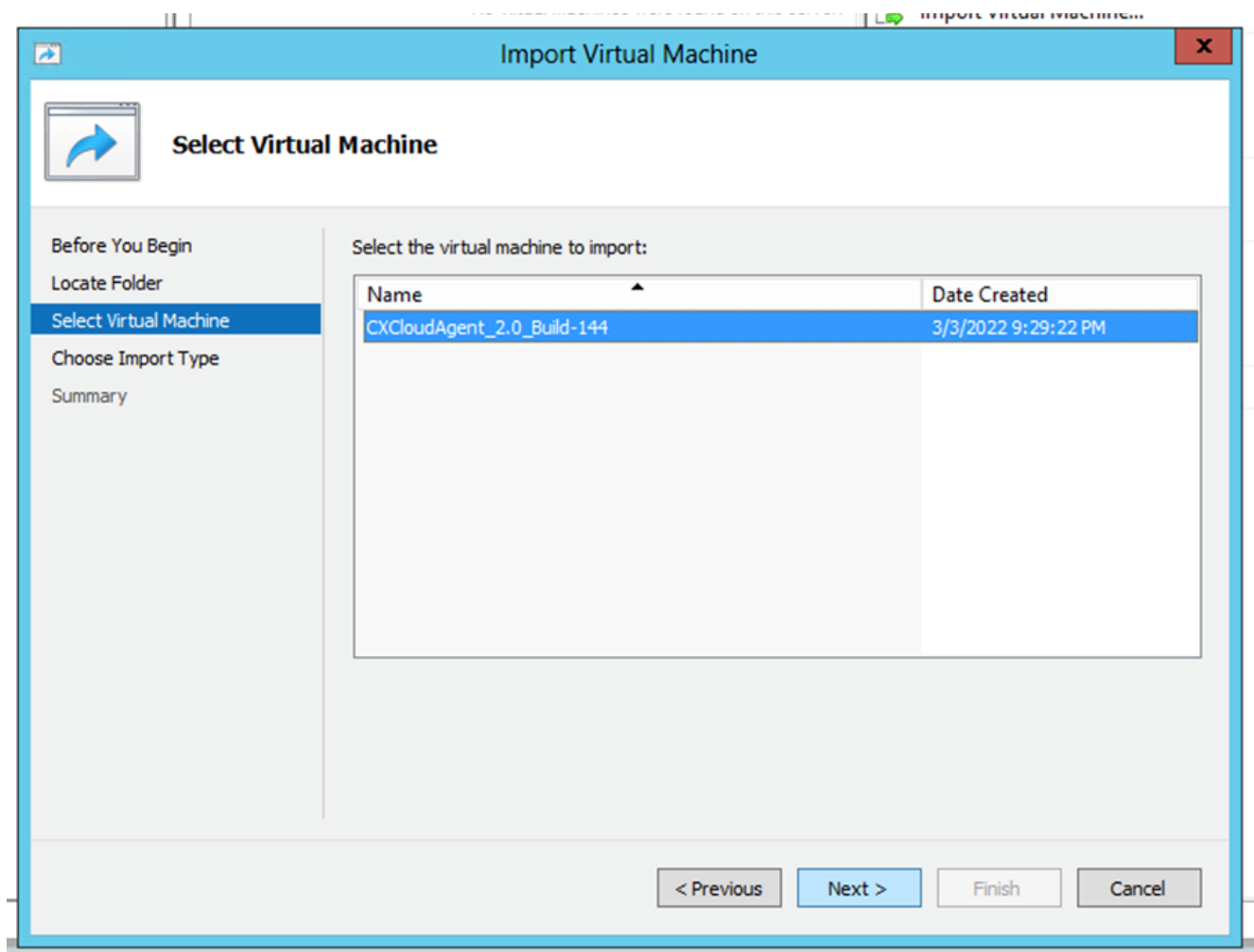
2. Procure e selecione a pasta de download.

3. Clique em Next.



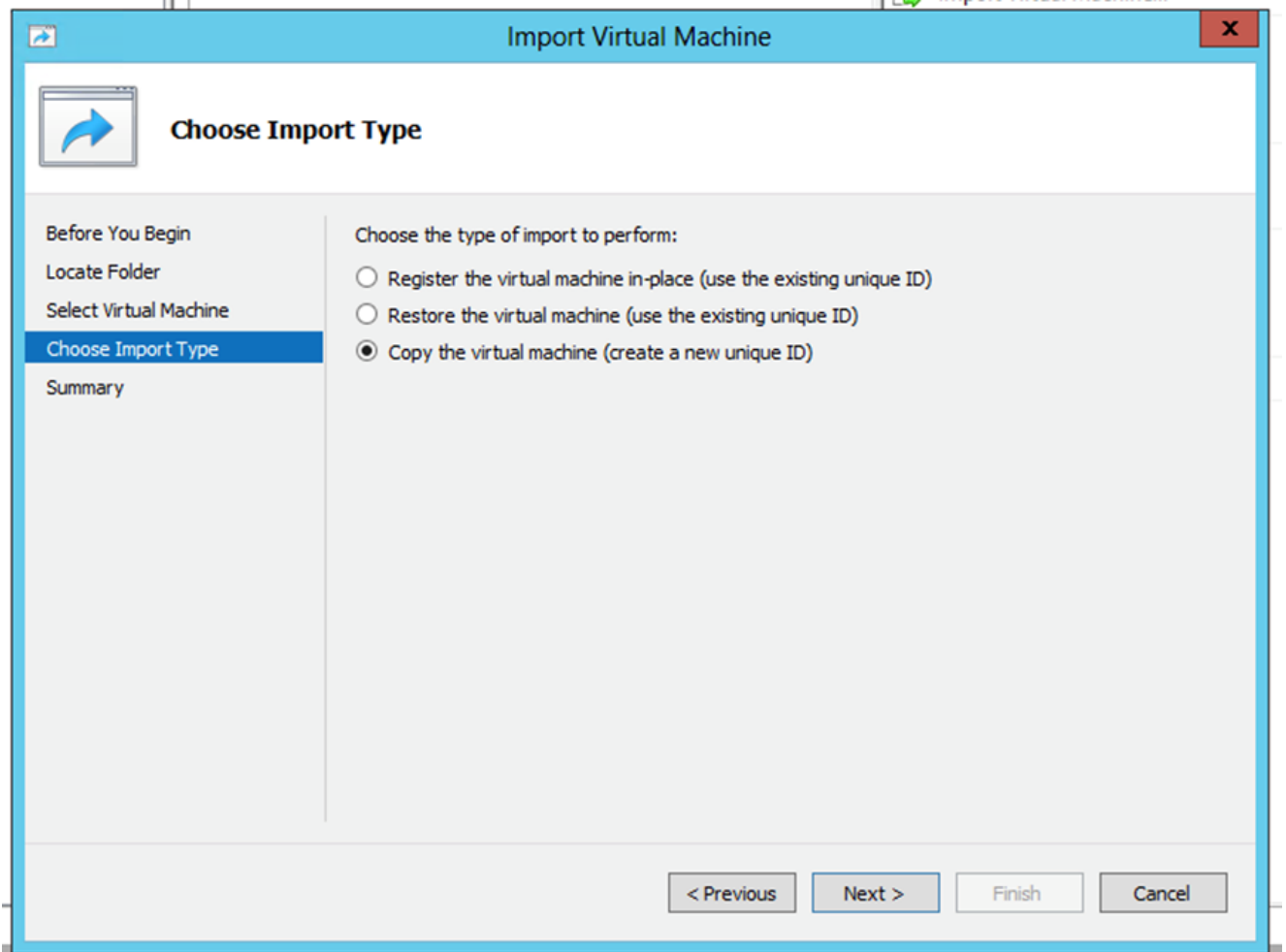
Pasta para importar

4. Selecione a VM e clique em Next.



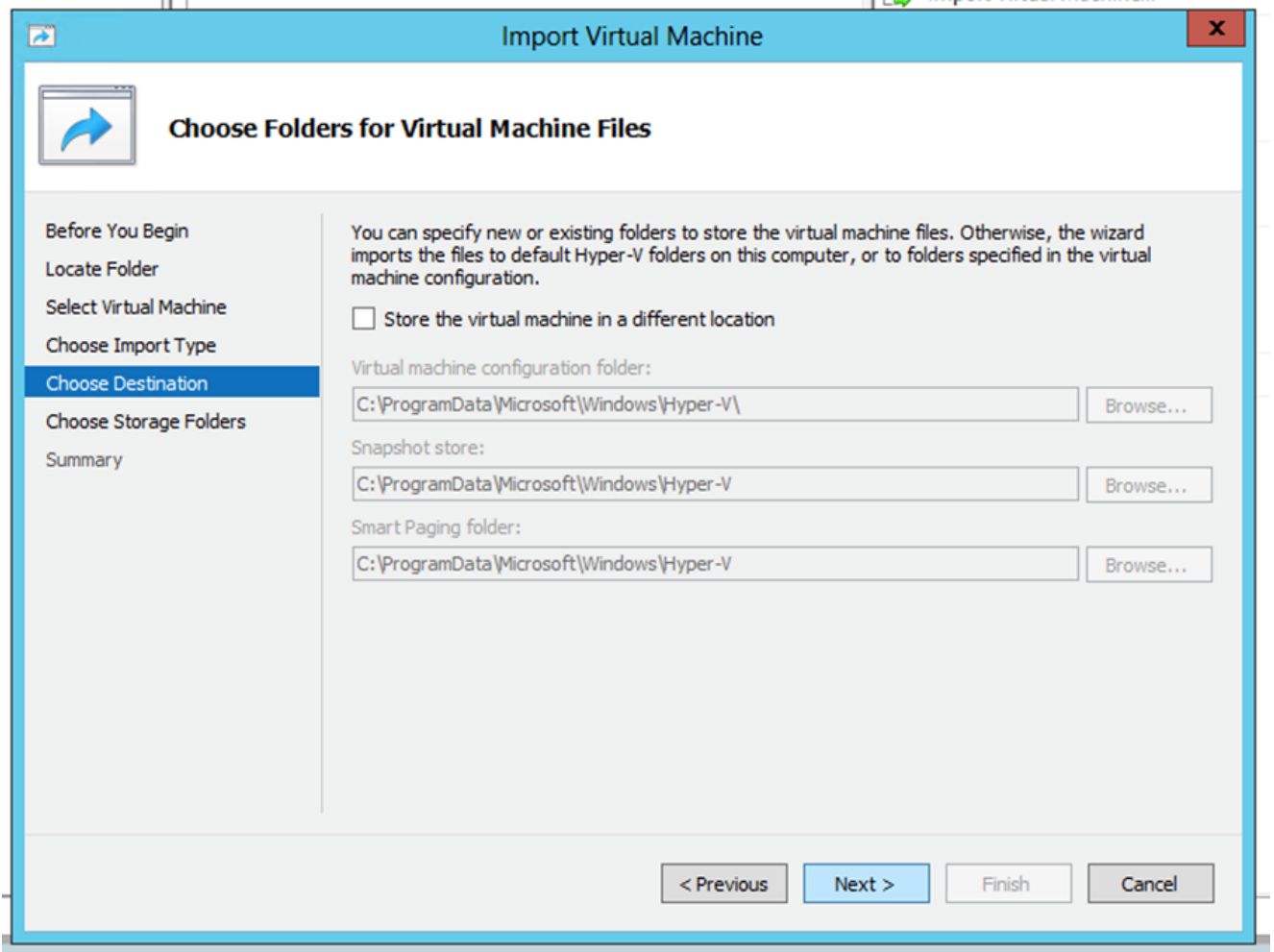
Selecionar VM

5. Selecione o Copy the virtual machine (create a new unique ID) e clique em Next.



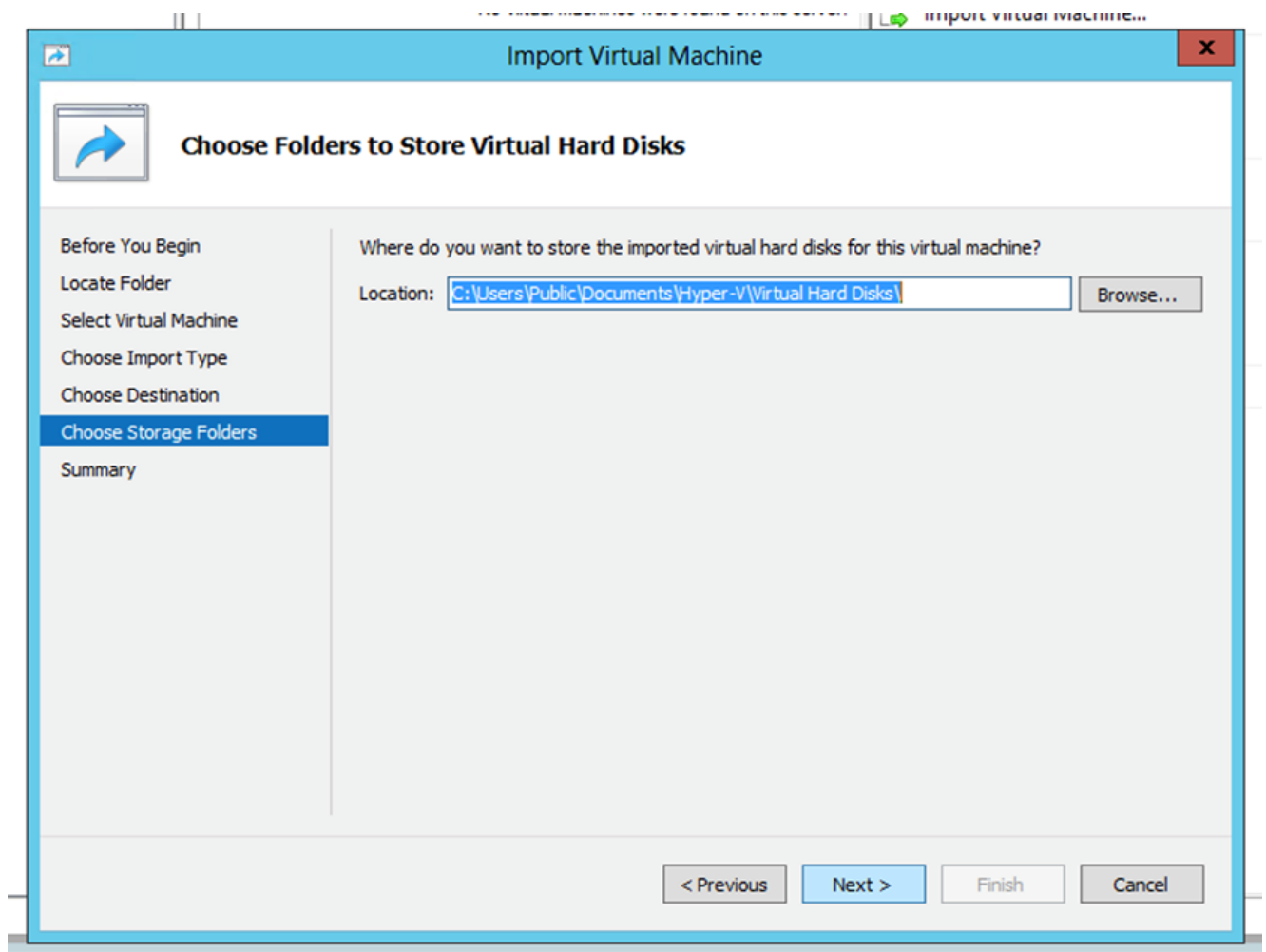
Tipo de importação

6. Navegue para selecionar a pasta para arquivos de VM. É recomendável usar caminhos padrão.
7. Clique em Next.



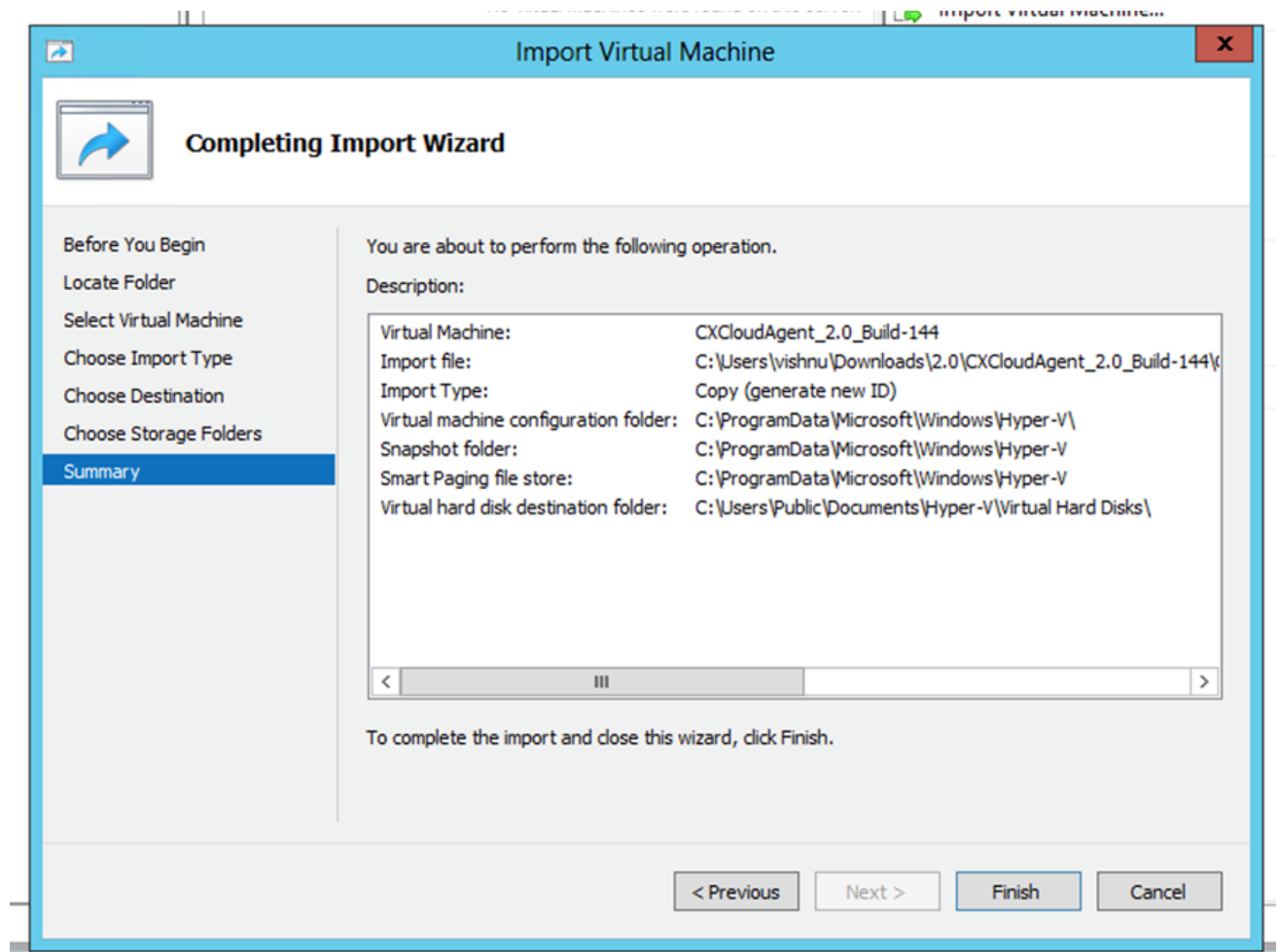
Escolher pasta

8. Procure e selecione a pasta para armazenar o disco rígido da VM. É recomendável usar caminhos padrão.
9. Clique em Next.



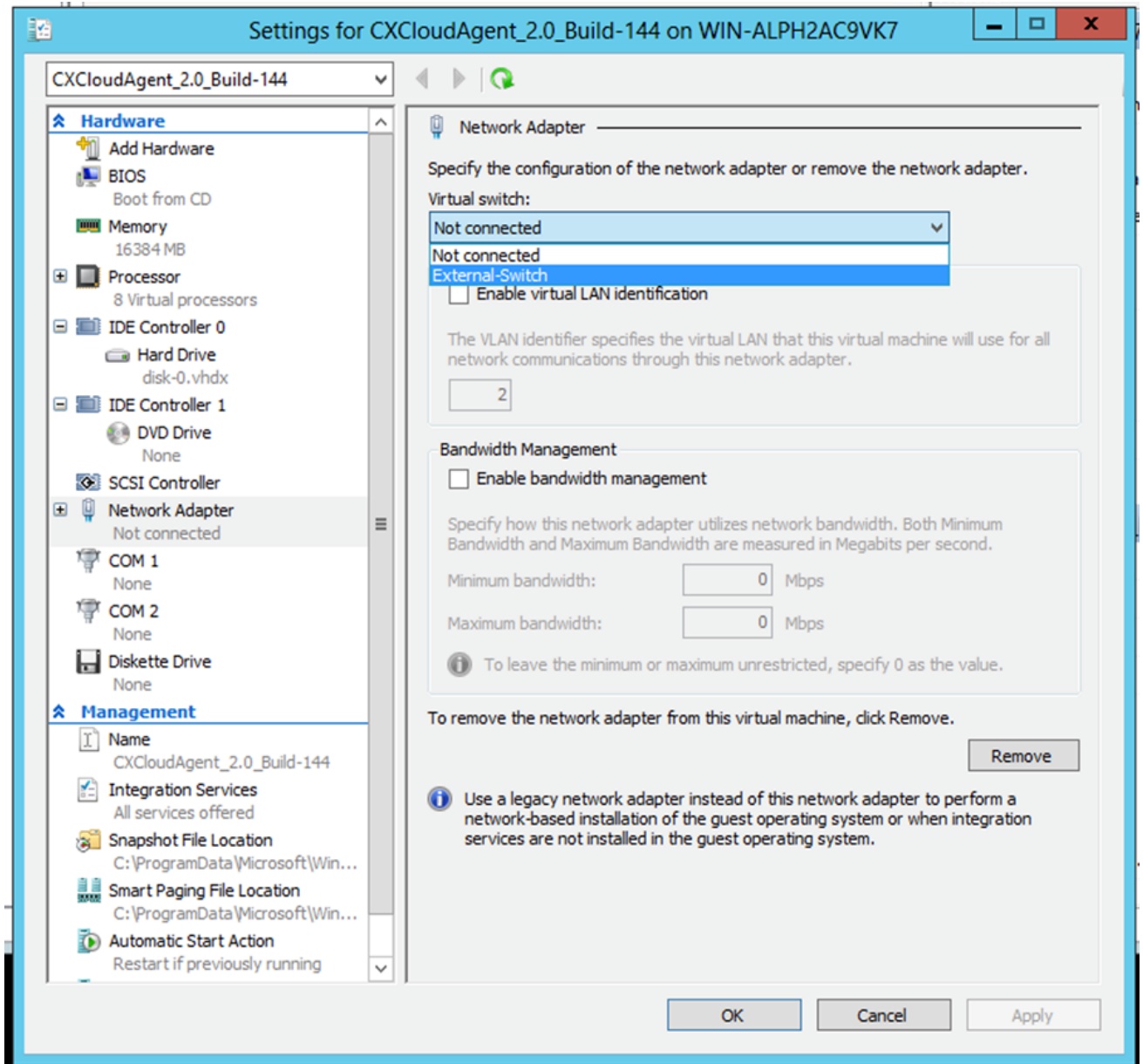
Pasta para armazenar Virtual Hard Disks

10. O resumo da VM é exibido. Verifique todas as entradas e clique em Finish.



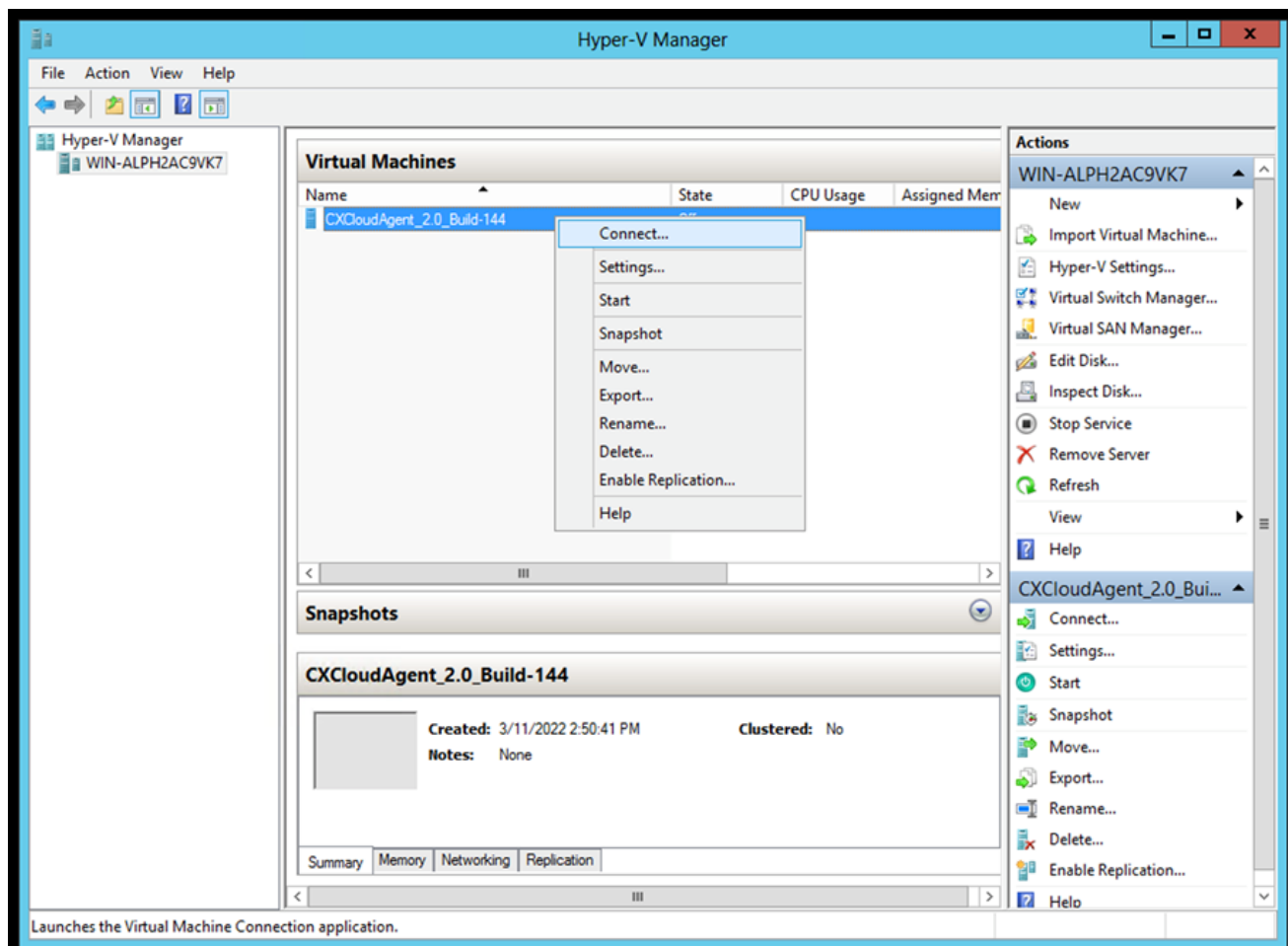
Summary

11. Quando a importação for concluída com êxito, uma nova VM será criada no Hyper-V. Abra a configuração da VM.
12. Selecione o adaptador de rede no painel esquerdo e escolha a opção disponível Virtual Switch no menu suspenso.



Switch Virtual

13. Seleccionar Connect para iniciar a VM.



Inicialização da VM

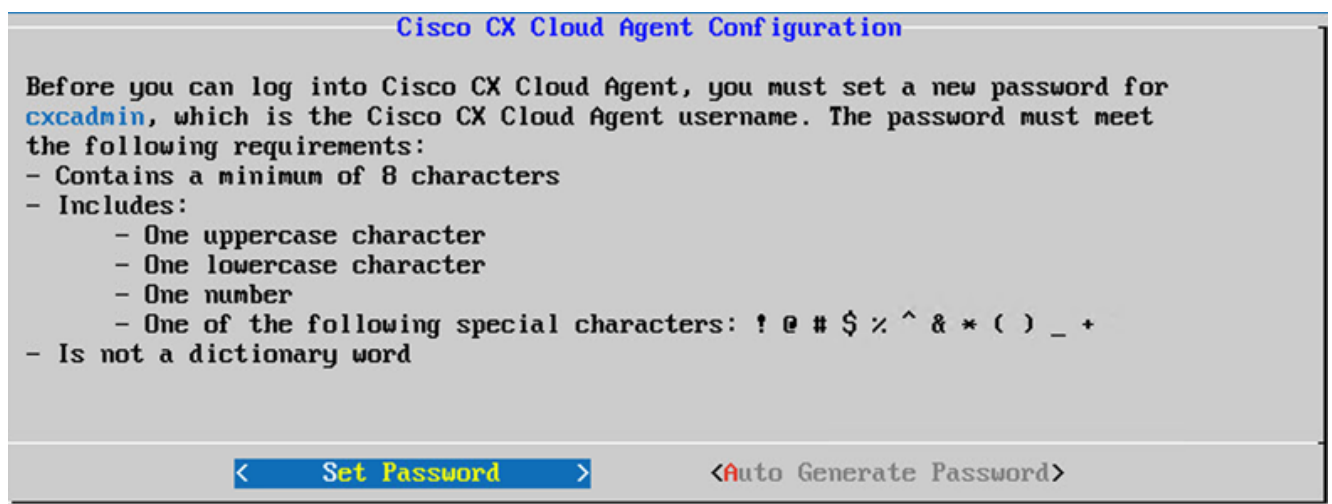
14. Navegue até [Configuração de rede](#).

Configuração de rede



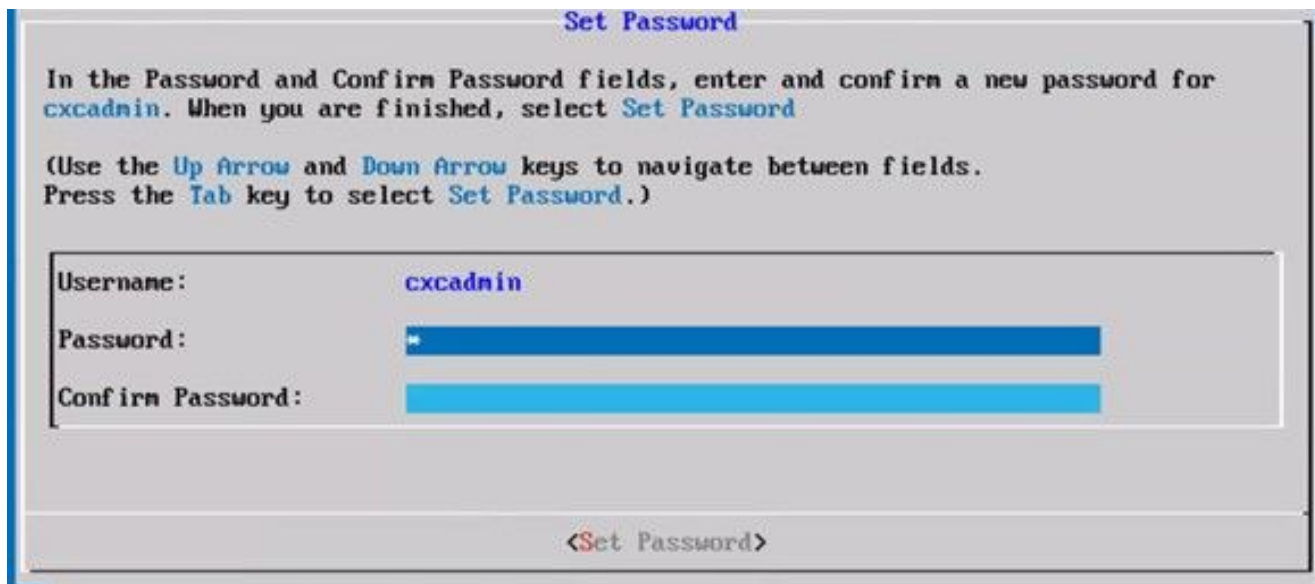
Console da VM

1. Clique em **Set Password** para adicionar uma nova senha para `cxcadmin` OU clique em **Auto Generate Password** para obter uma nova senha.



Definir senha

2. Se **Set Password** estiver selecionado, insira a senha para `cxcadmin` e confirme-a. Clique em **Set Password** e vá para a Etapa 3.



Nova senha

OU Se Auto Generate Password estiver selecionado, copie a senha gerada e armazene-a para uso futuro. Clique em Save Password e vá para a Etapa

4.



Senha gerada automaticamente

3. Clique em Save Password para usá-la para autenticação.



Salvar senha

4. Digite o IP Address, Subnet Mask, Gateway, e DNS Server e clique em Continue.

Network Configuration

Please enter an IPv4 address and corresponding network configuration for the appliance.

(Use **Up/Down** keys to navigate to next field. Press **Tab** to jump to **Continue** button)

IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Gateway:	<input type="text"/>
DNS Servers:	<input type="text"/>

*Maximum 3 IPs with comma separator.

<Continue>

Configuração de rede

5. Confirme as entradas e clique em Yes, Continue.

Confirmation

Are these entries correct?

IP Address:	192.168.0.100
Subnet Mask:	255.255.255.0
Gateway:	192.168.0.1
DNS:	192.168.0.64

<Yes, Continue> < No, Go Back >

Confirmação

6. Para definir os detalhes do proxy, clique em Yes, Set Up Proxy ou clique em No, Continue to Configuration para concluir a configuração e vá para a Etapa 8.

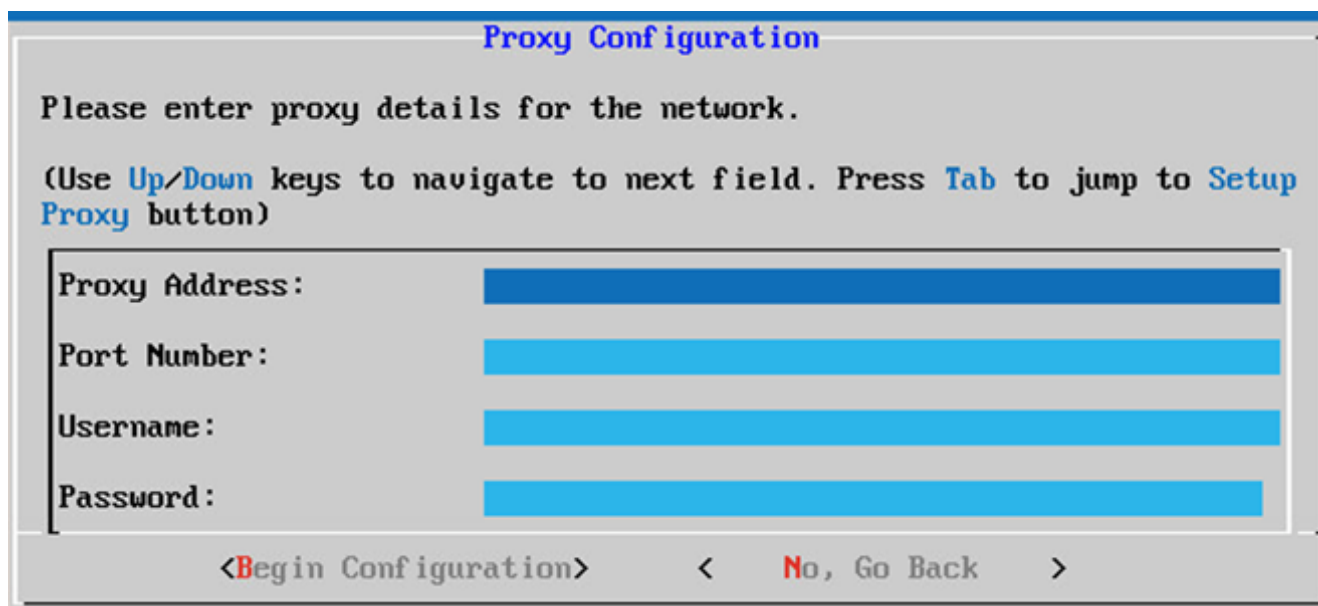
Proxy Set Up Confirmation

Do you want to add proxy details?

< **Yes, Set Up Proxy** > **<No, Continue to Configuration>**

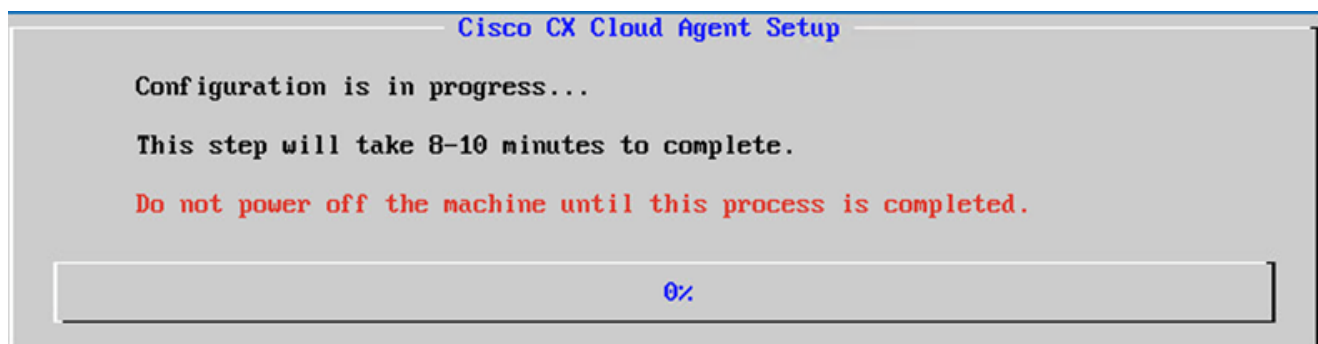
Instalação de proxy

7. Digite o Proxy Address, Port Number, Username, e Password.



Configuração de proxy

8. Clique em `Begin Configuration`. A configuração pode levar vários minutos para ser concluída.



Configuração em andamento

9. Copie o `Pairing Code` e retorne ao CX Cloud para continuar a configuração.



Código de emparelhamento

10. Se o Código de Emparelhamento expirar, clique em `Register to CX Cloud` para obter o código novamente.



Código expirado

11. Clique em OK.



Registro realizado com sucesso

12. Retorne à seção [Conectando o CX Cloud Agent ao CX Cloud](#) e execute as etapas listadas.

Abordagem alternativa para gerar código de emparelhamento usando CLI

Os usuários também podem gerar um código de emparelhamento usando opções CLI.

Para gerar um código de emparelhamento usando CLI:

1. Faça login no Agente de nuvem via SSH usando a credencial de usuário cxcadmin.
2. Gere o código de emparelhamento usando o comando `cxcli agent generatePairingCode`.

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

Pairing Code : x37I0P
Expires in: 5 minutes
Please use the Pairing Code in the CX Cloud to proceed with CX Cloud Agent registration.

cxcadmin@cxcloudagent:~$
```

Gerar CLI do código de emparelhamento

3. Copie o Pairing Code e retorne ao CX Cloud para continuar a configuração. Para obter mais

informações, consulte Conexão com o Portal do Cliente.

Configurar o Cisco DNA Center para encaminhar o Syslog para o CX Cloud Agent

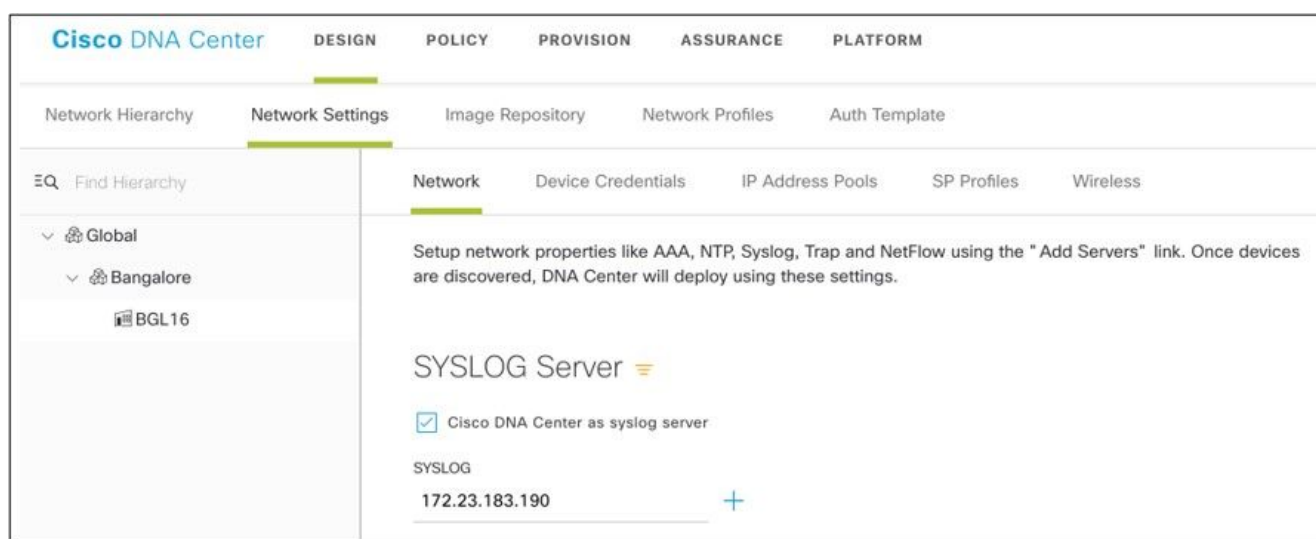
Pré-requisito

As versões do Cisco DNA Center suportadas são de 1.2.8 a 1.3.3.9 e de 2.1.2.0 a 2.2.3.5.

Configurar definição do encaminhamento de syslog

Para configurar o encaminhamento de syslog para o CX Cloud Agent no Cisco DNA Center usando a interface do usuário, execute estas etapas:

1. Inicie o Cisco DNA Center.
2. Ir para Design > Network Settings > Network.
3. Para cada local, adicione o IP do CX Cloud Agent como o Servidor Syslog.



Servidor Syslog

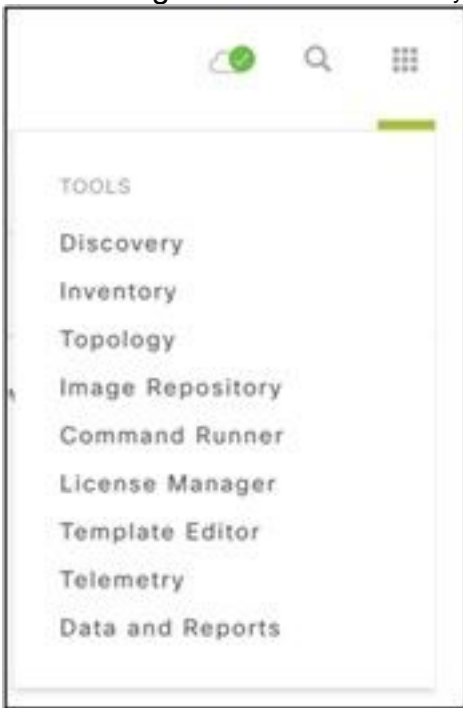
Notas:

- Depois de configurados, todos os dispositivos associados a esse site são configurados para enviar syslog com nível crítico para o CX Cloud Agent.
- Os dispositivos devem ser associados a um site para permitir o encaminhamento de syslog do dispositivo para o CX Cloud Agent.
- Quando uma configuração do Servidor syslog é atualizada, todos os dispositivos associados a esse site são automaticamente definidos para o nível crítico padrão.

Habilitar Configurações de Syslog de Nível de Informação

Para tornar visível o nível de informações do Syslog, execute estas etapas:

1. Navegue até Tools > Telemetry.



Menu Ferramentas

2. Selecione e expanda a Site View e selecione um site na hierarquia de sites.



Visualização do local

3. Selecione o local necessário e selecione todos os dispositivos usando o Device name caixa de seleção.

4. A partir da Actions , selecione Optimal Visibility.



Security

O CX Cloud Agent garante ao cliente segurança de ponta a ponta. A conexão entre o CX Cloud e o CX Cloud Agent é criptografada. O Secure Socket Shell (SSH) do CX Cloud Agent comporta 11 cifras diferentes.

Segurança física

Implante a imagem OVA do CX Cloud Agent em uma empresa de servidores VMware segura. O OVA é compartilhado de forma segura pelo Cisco Software Download Center. A senha do bootloader (modo de usuário individual) é definida com uma senha aleatoriamente exclusiva. Os usuários devem consultar as [Perguntas frequentes](#) para definir a senha deste bootloader (modo de usuário individual).

Acesso do usuário

Os usuários da nuvem CX só podem obter autenticação e acessar as APIs do Cloud Agent.

Segurança da conta

Na implantação, a conta de usuário cxcadmin é criada. Os usuários são forçados a definir uma senha durante a configuração inicial. As credenciais de usuário de cxcadmin são usadas para acessar as APIs do CX Cloud Agent e conectar o dispositivo sobre ssh.

O usuário cxcadmin restringiu o acesso com os privilégios mínimos. A senha cxcadmin segue a política de segurança e tem um hash unidirecional com um período de expiração de 90 dias. O usuário cxcadmin pode criar um usuário cxcroot usando o utilitário chamado remoteaccount. O usuário de cxcroot pode obter privilégios de root. A senha expira em dois dias.

Segurança de rede

A VM do CX Cloud Agent pode ser acessada usando ssh com credenciais de usuário cxcadmin. As portas de entrada estão restritas a 22 (ssh), 514 (Syslog).

Autenticação

Autenticação baseada em senha: O dispositivo mantém um único usuário - 'cxcadmin', que permite que o usuário seja autenticado e se comunique com o CX Cloud Agent.

- Ações com privilégios do root no dispositivo usando o ssh o usuário cxcadmin pode criar o usuário cxcroot, usando um utilitário chamado conta remota. Este utilitário exibe uma senha criptografada RSA/ECB/PKCS1v1_5 que pode ser descriptografada somente no portal SWIM (<https://swims.cisco.com/abraxas/decrypt>). Somente o pessoal autorizado tem acesso a esse portal. O usuário de cxcroot pode obter privilégios do root usando essa senha descriptografada. A frase secreta é válida apenas por dois dias. O usuário de cxcadmin precisa recriar a conta e obter a senha no portal do SWIM depois que a senha expirar.

Blindagem

O dispositivo CX Cloud Agent segue os padrões de proteção de CIS.

Segurança de dados

O dispositivo do CX Cloud Agent não armazena as informações pessoais do cliente.

A aplicação de credenciais do dispositivo (em execução como um dos pods) armazena as credenciais criptografadas do servidor Cisco DNA Center dentro do banco de dados seguro. Os dados coletados do Cisco DNA Center não são armazenados de forma alguma dentro do dispositivo. Os dados coletados são carregados no backup logo após a conclusão da coleta e os dados são eliminados do agente.

Transmissão de Dados

O pacote de registro contém o número exclusivo [X.509](#) certificado de dispositivo e chaves para estabelecer conexão segura com o lot Core. Usar esse agente estabelece uma conexão segura usando MQTT sobre TLS v1.2

Registros e monitoramento

Os registros não contêm forma alguma de informações confidenciais. Os logs de auditoria capturam todas as ações confidenciais de segurança executadas no dispositivo CX Cloud Agent.

Resumo de segurança

Recursos de segurança

Descrição

Senha do bootloader

A senha do bootloader (modo de usuário individual) é definida com uma senha aleatoriamente exclusiva. O usuário deve consultar as [Perguntas frequentes](#) para definir a senha do bootloader (modo de usuário individual).

SSH:

Acesso do usuário

- O acesso ao dispositivo usando o usuário de cxcadmin exige as credenciais criadas durante a instalação.
- O acesso ao equipamento usando o usuário cxcroot requer que as credenciais sejam descriptografadas usando o portal SWIM por pessoal autorizado.

Contas do usuário

- cxcadmin: Esta é uma conta de usuário padrão criada. O usuário pode executar comandos de aplicação do CX Cloud Agent usando cxcli e tem menos privilégios no dispositivo. O usuário de cxcroot e a senha criptografada são gerados com o usuário de cxcadmin
- cxcroot: O cxcadmin pode criar esse usuário com o utilitário 'remoteaccount'. O usuário obtém privilégios do root com essa conta.

Política de senha de cxcadmin

- A senha é um hash unidirecional que usa o SHA-256 e é armazenada com segurança.
- Mínimo de oito (8) caracteres, que contém três destas categorias: maiúsculas, minúsculas, números e caracteres especiais

Política de senha de cxcroot

- A senha de cxcroot é criptografada por RSA/ECB/PKCS1v1_5.
- A frase secreta gerada precisa ser descriptografada no portal do SWIM.
- A senha e o usuário do cxcroot são válidos por, no máximo, dois dias e podem ser gerados

	novamente usando o usuário de cxcadmin.
Política de senha de login de ssh	<ul style="list-style-type: none"> • Mínimo de oito (8) caracteres, que contém três destas categorias: maiúsculas, minúsculas, números e caracteres especiais. • 5 tentativas de login com falha bloquearão a caixa por 30min. A senha expira em 90 dias.
Portas	Portas de entrada abertas – 514 (Syslog) e 22 (ssh)
Segurança de dados	<p>Não há informações de cliente armazenadas.</p> <p>Não há dados de dispositivo armazenados.</p> <p>Credenciais do servidor Cisco DNA Center criptografadas e armazenadas no banco de dados.</p>

Perguntas mais freqüentes

CX Cloud Agent

Implantação

P – Com a opção "Reinstalar", o usuário pode implantar o novo Cloud Agent com o novo endereço IP?

R – Sim

P - Quais são os formatos de arquivo disponíveis para instalação?

R – OVA e VHD

P – Qual é o ambiente em que o instalável pode ser implantado?

R – OVA

VMWare ESXi versão 5.5 ou posterior

Oracle Virtual Box 5.2.30 ou posterior

VHD

Hipervisor Windows 2012 a 2016

P – O CX Cloud Agent pode detectar o endereço IP em um ambiente DHCP?

R – Sim, no caso de ambiente DHCP, a atribuição de endereço IP durante a configuração de IP é realizada. No entanto, não há suporte para a alteração de endereço IP esperada para o CX Cloud Agent eventualmente. Além disso, recomenda-se que o cliente reserve o IP para o Cloud Agent no ambiente DHCP.

P – O CX Cloud Agent é compatível com as configurações de IPv4 e IPv6?

R – Não, apenas o IPv4 é compatível.

P – Durante a configuração de IP, o endereço IP é validado?

R – Sim, a sintaxe do endereço IP e a atribuição de endereço IP duplicado serão validadas.

P – Qual é o tempo aproximado necessário para a implantação do OVA e a configuração de IP?

R – A implantação do OVA depende da velocidade da rede para copiar os dados. A configuração de IP leva aproximadamente de 8 a 10 minutos, o que inclui o Kubernetes e as criações de contêiner.

P – Há limitações em relação a algum tipo de hardware?

A - A máquina host na qual o OVA é implantado deve atender aos requisitos fornecidos como parte da configuração do portal CX. O CX Cloud Agent é testado com a caixa VMware/Virtual executada em um hardware com processadores Intel Xeon E5 com taxa de vCPU para CPU definida em 2:1. Se for usada uma CPU de processador menos potente ou uma taxa maior, o desempenho poderá diminuir.

P – Podemos gerar o código de emparelhamento a qualquer momento?

R – Não, o código de emparelhamento só poderá ser gerado se o Cloud Agent não estiver registrado.

P - Quais são os requisitos de largura de banda entre DNACs (para até 10 clusters ou 20 não clusters) e o Agente?

A - A largura de banda não é uma restrição quando o Agente e o DNAC estão na mesma rede LAN/WAN no ambiente do cliente. A largura de banda de rede mínima necessária é de 2,7 Mbits/s para coletas de inventário de 5.000 dispositivos + Pontos de Acesso 13000 para uma conexão de Agente para DNAC. Se syslogs forem coletados para insights de L2, a largura de banda mínima necessária será de 3,5 Mbits/s para coberturas de 5.000 dispositivos +13000 Pontos de acesso para inventário, 5.000 dispositivos syslogs e 2.000 dispositivos para varreduras - todos executados em paralelo do Agente.

Versões e correções

P – Quais são os diferentes tipos de versões listadas para a atualização do CX Cloud Agent?

R - Aqui está o conjunto das versões lançadas do CX Cloud Agent listadas:

- A.x0 (onde x é a principal versão do recurso de produção mais recente, exemplo: 1.3.0).
- A.x.y (onde A.x.0 é obrigatório e o upgrade incremental deve ser iniciado, x é a versão mais recente do recurso principal de produção e y é o patch de upgrade mais recente que está ativo, por exemplo: 1.3.1).
- A.x.y-z (onde A.x.0 é obrigatório e o upgrade incremental a ser iniciado, x é a versão mais recente do recurso principal de produção e y é o patch de upgrade mais recente que está ativo e z é o patch spot que é uma correção instantânea por um período de tempo muito curto, por exemplo: 1.3.1-1)

em que A é uma versão de longo prazo distribuída por um período de 3 a 5 anos.

P - Onde encontrar a versão mais recente do CX Cloud Agent e como atualizar o CX Cloud Agent existente?

A - Ir para Admin Settings > Data Sources. Clique no botão View Update e executar as instruções compartilhadas na tela.

Autenticação e configuração de proxy

P – Qual é o usuário padrão da aplicação do CX Cloud Agent?

R – cxcadmin

P - Como a senha é definida para o usuário padrão?

R – A senha é definida durante a configuração de rede.

P – Há opções disponíveis para redefinir a senha após o dia 0?

R – O agente não fornece opções específicas para redefinir a senha, mas você pode usar os comandos linux para redefinir a senha para cxcadmin.

P – Quais são as políticas de senha para configurar o CX Cloud Agent?

R – As políticas de senha são:

- Tempo máximo da senha (duração) definido como 90 dias
- Tempo mínimo da senha (duração) definido como 8
- Tamanho máximo da senha de 127 caracteres.
- Pelo menos uma letra maiúscula e uma minúscula devem ser fornecidas.
- Deve conter pelo menos um caractere especial (por exemplo, !\$%^&*()_+|~-=\`{}[]:~<>?,/).
- Esses caracteres não são permitidos Caracteres especiais de 8 bits (por exemplo, ¬£, √Å √', √¥, √ë, ¬ø, √ü)Espaços
- A senha não deve ser a última das 10 senhas usadas recentemente.
- Não deve conter expressão regular, isto é
- Não podem conter estas palavras ou seus derivados: cisco, sanjose e sanfran

P – Como definir a senha do Grub?

A - Para definir a senha do Grub, execute estas etapas:

1. Execute o ssh como cxcroot e forneça o token [entre em contato com a equipe de suporte para obter o token de cxcroot]
2. Execute sudo su, forneça o mesmo token
3. Execute o comando grub-mkpasswd-pbkdf2 e defina a senha do GRUB. O hash da senha fornecida será impresso, copie o conteúdo.
4. vi para o arquivo /etc/grub.d/00_header. Navegue até o final do arquivo e substitua a saída de hash seguida do conteúdo password_pbkdf2 root ***** pelo hash obtido para a senha recebida na etapa 3
5. Salve o arquivo com o comando :wq!
6. Execute o comando update-grub

P - Qual é o período de expiração da senha de cxcadmin?

R – A senha expira em 90 dias.

P – O sistema desativa a conta após tentativas de login com falha consecutivas?

R – Sim, a conta é desativada após 5 tentativas com falha consecutivas. O período de bloqueio é

de 30 minutos.

P – Como gerar a frase secreta?

A - Execute estas etapas,

1. Execute o ssh e faça login como usuário de cxcadmin
2. Execute o comando *remoteaccount cleanup -f*
3. Execute o comando *remoteaccount create*

P – O host de proxy é compatível com nome de host e IP?

A - Sim, mas para usar o nome do host, o usuário deve fornecer o IP do DNS durante a configuração da rede.

Secure Shell SSH

P – Quais são as cifras compatíveis com o ssh shell?

R – chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com , aes256-ctr, aes192-ctr, aes128-ctr

P – Como fazer login no console?

R – Siga as etapas para fazer login:

1. Faça login como usuário de cxcadmin.
2. Forneça a senha cxcadmin.

P – Os logins de ssh estão registrados?

A - Sim, eles são registrados como parte do `var/logs/audit/audit.log`.

P – Qual é o tempo limite da sessão ociosa?

A - O tempo limite da sessão SSH ocorre se o agente de nuvem estiver ocioso por cinco (5) minutos.

Portas e serviços

P – Quais são as portas mantidas abertas por padrão no CX Cloud Agent?

A - Estas portas estão disponíveis:

- Outbound port: O CX Cloud Agent implantado pode se conectar ao back-end da Cisco conforme indicado na tabela na porta 443 HTTPS ou por meio de um proxy para enviar dados à Cisco. O CX Cloud Agent implantado pode ser conectado ao Cisco DNA Center na porta HTTPS 443.

api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.cisco.cloud	agent.emea. cisco.cloud	agent.apjc. cisco.cloud
ng.acs.agent.us.cisco.cloud	ng.acs.agent.emea. cisco.cloud	ng.acs.agent.apjc.cisco.cloud

Note: Além dos domínios listados, quando os clientes da EMEA ou APJC reinstalarem o Agente de nuvem, o domínio agent.us.cisco.cloud deverá ser permitido no firewall do cliente.

O domínio agent.us.cisco.cloud não é mais necessário após uma reinstalação bem-sucedida.

Note: Certifique-se de que o tráfego de retorno deve ser permitido na porta 443.

- Inbound port: Para o gerenciamento local do CX Cloud Agent, 514(Syslog) e 22 (ssh) devem estar acessíveis. O cliente deve permitir que a porta 443 em seu firewall receba dados do CX Cloud.

Conexão do CX Cloud Agent com o Cisco DNA Center

P – Qual é a finalidade e a relação do Cisco DNA Center com o CX Cloud Agent?

R - O Cisco DNA Center é o agente de nuvem que gerencia os dispositivos de rede nas instalações do cliente. O CX Cloud Agent coleta as informações de inventário dos dispositivos do Cisco DNA Center configurado e carrega as informações de inventário disponíveis como "Visualização de recursos" na CX Cloud.

P – Quando o usuário pode fornecer detalhes do Cisco DNA Center no CX Cloud Agent?

R - Durante o dia 0 - configuração do CX Cloud Agent, o usuário pode adicionar os detalhes do Cisco DNA Center no portal CX Cloud. Além disso, durante as operações do Dia N, os usuários podem adicionar outros Centros do DNA em Admin Settings > Data source.

P – Quantos Cisco DNA Centers podem ser adicionados?

A - 10 clusters DNAC da Cisco ou 20 não clusters DNAC.

P - Que função o usuário do Cisco DNA Center pode ter?

A - A função de usuário pode ser admin OR observer.

P - Como refletir as modificações no CX Agent devido a alterações nas credenciais do DNA Center conectado?

A - Execute estes comandos no console do CX Cloud Agent:

```
cxcli agent modifyController
```

Entre em contato com o suporte em caso de problemas durante a atualização de credenciais DNAC.

P – Como os detalhes do Cisco DNA Center são armazenados no CX Cloud Agent?

R – As credenciais do Cisco DNA Center são criptografadas usando o AES-256 e armazenadas no banco de dados do CX Cloud Agent. O banco de dados do CX Cloud Agent é protegido por ID de usuário e senha seguras.

P – Qual tipo de criptografia será usada ao acessar a API do Cisco DNA Center no CX Cloud Agent?

R – HTTPS sobre TLS 1.2 é usado para a comunicação entre o Cisco DNA Center e o CX Cloud Agent.

P – Quais são as operações realizadas pelo CX Cloud Agent no Cloud Agent do Cisco DNA Center integrado?

R - O CX Cloud Agent coleta dados que o Cisco DNA Center tem sobre os dispositivos de rede e usa a interface de execução de comandos do Cisco DNA Center para falar com os dispositivos finais e executar comandos CLI (comando show). Os comandos de alteração de configuração não são executados

P – Quais são os dados padrão coletados no Cisco DNA Center e carregados no backend?

R-

- Entidade de rede
- Módulos
- show version
- Config
- Informações da imagem do dispositivo
- Tags

P – Quais são os dados adicionais coletados no Cisco DNA Center e carregados no backend da Cisco?

R – Você obtém todas as informações [aqui](#).

P – Como os dados de inventário são carregados no back-end?

R – O CX Cloud Agent carrega os dados usando o protocolo TLS 1.2 para o servidor back-end da Cisco.

P – Qual é a frequência de upload de inventário?

A - A coleta é acionada de acordo com a programação definida pelo usuário e é carregada no back-end da Cisco.

P – O usuário pode reagendar o inventário?

A - Sim, há uma opção disponível para modificar as informações de programação de Admin Settings> Data Sources.

P – Quando ocorre o tempo limite da conexão entre o Cisco DNA Center e o Cloud Agent?

R – Os tempos limite são categorizados da seguinte forma:

- Para conexão inicial, o tempo limite é de no máximo 300 segundos. Se a conexão não for estabelecida entre o Cisco DNA Center e o Cloud Agent em no máximo 5 minutos, a conexão será encerrada.
- Para conexões recorrentes, típicas ou atualizações: o tempo limite de resposta é de 1800 segundos. Se a resposta não for recebida ou não puder ser lida em 30 minutos, a conexão será encerrada.

Verificação de diagnóstico usada pelo CX Cloud Agent

P – Quais são os comandos executados no dispositivo para verificação?

A - Os comandos que precisam ser executados no dispositivo para a verificação são determinados dinamicamente durante o processo de verificação. O conjunto de comandos pode mudar ao longo do tempo, mesmo para o mesmo dispositivo (e não no controle de Diagnostic Scan).

P – Onde os resultados da verificação são armazenados e gerados?

R – Os resultados verificados são armazenados e perfilados no back-end da Cisco.

P – As duplicatas (por nome de host ou IP) no Cisco DNA Center são adicionadas à verificação de diagnóstico quando a origem do Cisco DNA Center está conectada?

R - Não, as duplicatas serão filtradas e apenas os dispositivos exclusivos serão extraídos.

P – O que acontece quando ocorre uma falha em uma das verificações de comando?

R – A verificação do dispositivo será totalmente interrompida e marcada como falha.

Registros de sistema do CX Cloud Agent

P - Que informações de integridade são enviadas para a nuvem CX?

R – Registros de aplicação, status de pod, detalhes do Cisco DNA Center, registros de auditoria, detalhes do sistema e detalhes de hardware.

P – Quais detalhes do sistema e do hardware são coletados?

R – Exemplo de saída:

```
system_details":{
  "os_details":{
    "VersãoTempoExecuçãoContêiner":"docker://19.3.12",
    "kernelVersion":"5.4.0-47-generic",
    "kubeProxyVersion":"v1.15.12",
    "kubletVersion":"v1.15.12",
    "machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
    "sistema operacional":"linux",
    "osImage":"Ubuntu 20.04.1 LTS",
    "UUID do sistema":"42002151-4131-2ad8-4443-8682911bdadb"
  },
```

```
"detalhes_do_hardware":{
"total_cpu":"8",
"utilização_da_cpu":"12,5%",
"memória_total":"16007 MB",
"memória_livre":"994 MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}
```

P – Como os dados de integridade são enviados para o back-end?

R - Com o CX Cloud Agent, o serviço de saúde (manutenção) transmite os dados para o back-end da Cisco.

P – Qual é a política de retenção de registro de dados de integridade do CX Cloud Agent no backend?

R – A política de retenção de registro de dados de integridade do CX Cloud Agent no backend é de 120 dias.

P – Quais são os tipos de upload disponíveis?

A - Três tipos de uploads disponíveis,

1. Carregamento de inventário
2. Carregamento de Syslog
3. Carregamento de integridade do agente: 3 itens como parte do upload de integridade
Integridade dos serviços - a cada 5 minutos
Podlog - a cada 1 hora
Log de auditoria - a cada 1 hora

Troubleshooting

Problema: Não é possível acessar o IP configurado.

Solução: Execute o ssh usando o IP configurado. Se o tempo limite da conexão for excedido, o possível motivo será a configuração incorreta do IP. Nesse caso, reinstale configurando um IP válido. Isso pode ser feito através do portal com a opção de reinstalação fornecida no Admin Setting

Problema: Como verificar se os serviços estão funcionando depois do registro?

Solução: Execute o comando mostrado aqui e verifique se os pods estão em execução.

1. ssh para o IP configurado como cxcadmin.
2. Forneça a senha.
3. Execute o comando *kubectl get pods*.

Os pods podem estar em qualquer estado, como em execução, Inicializando ou Criando

contêiner, mas após 20 minutos, os pods devem estar em estado de execução.

Se o estado *não estiver em execução* ou *Inicialização do Pod*, verifique a descrição do pod com o comando mostrado aqui

```
kubectl describe pod <podname>
```

A saída terá as informações sobre o status do pod.

Problema: Como verificar se o Interceptor SSL está desabilitado no Proxy do cliente?

Solução: Execute o comando curl mostrado aqui para verificar a seção do certificado do servidor. A resposta tem os detalhes do certificado do servidor consoweb.

```
curl -v --header 'Autorização: Básico xxxxxx' https://concsoweb-prd.cisco.com/
```

* Certificado do servidor:

* assunto: C=US; ST=Califórnia; L=San Jose; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

* data de início: Fev 16 11:55:11 2021 GMT

* data de expiração: Fev 16 12:05:00 2022 GMT

* nomeAltassunto: o host "concsoweb-prd.cisco.com" correspondeu ao "concsoweb-prd.cisco.com" do cert

* emitente: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL CA G3

* Verificação de certificado SSL ok.

```
>GET / HTTP/1.1
```

Problema: Os comandos kubectl falharam e mostram o erro como "A conexão com o servidor X.X.X.X:6443 foi recusada - você especificou o host ou a porta correta"

Solução:

- Verifique quanto à disponibilidade de recursos. [exemplo: CPU e memória]
- Aguarde o início do serviço do Kubernetes

Problema: Como obter os detalhes da falha de coleta para um comando/dispositivo

Solução:

- Execute `kubectl get pods` e obtenha o nome do pod de coleta.

- Execute `kubectl logs` para obter os detalhes específicos do comando/dispositivo.

Problema: O comando `kubectl` não funciona com o erro "[authentication.go:64] Não é possível autenticar a solicitação devido a um erro: [x509: o certificado expirou ou ainda não é válido, x509: o certificado expirou ou ainda não é válido]"

Solução: execute os comandos mostrados aqui como `cxcroot user`

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

Respostas à falha de coleta

A causa da falha de coleta pode ser qualquer restrição ou problema observado no controlador adicionado ou nos dispositivos presentes no controlador.

A tabela mostrada aqui tem o trecho de erro para casos de uso vistos no microsserviço de Coleta durante o processo de coleta.

Caso de uso

Snippet de registro no microsserviço de coleta

Se o dispositivo solicitado não for encontrado no Cisco DNA Center

```
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e8827"
}
```

Se o dispositivo solicitado não estiver acessível no Cisco DNA Center

```
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "Error occurred while executing command: show version\nError connecting to device [Host: 172.21.137.221:22]No route to host : No route to host"
}
```

Se o dispositivo solicitado não estiver acessível no Cisco DNA Center

```
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "Error occurred while executing command : show version\nError connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connection timed out: /X.X.X.X:22"
}
```

Se o comando solicitado não estiver disponível no dispositivo

```
{
  "command": "show run-config",
  "status": "Success",
  "commandResponse": " Error occurred while executing command : show run-config\n\nshow run-config\n      ^\n% Invalid input detected at \u0027^\u0027 marker.\n\nXXCT5760#",
  "errorMessage": ""
}
```

Se o dispositivo solicitado não tiver SSHv2 e o Cisco DNA Center tentar conectar o dispositivo com SSHv2

```
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "Error occurred while executing command : show version\nSSH2"
}
```

Se o comando estiver desativado no microsserviço de coleta	<pre> channel closed : Remote party uses incompatible protocol, it is not SSH-2 compat } { "command": "config paging disable", "status": "Command_Disabled", "commandResponse": "Command collection is disabled", "errorMessage": "" } </pre>
Se a tarefa do executor de comandos falhou e o URL da tarefa não foi retornado pelo Cisco DNA Center	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s. Task URL is em } </pre>
Se a tarefa do executor de comandos não foi criada no Cisco DNA Center	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: % task details." } </pre>
Se o microsserviço de coleta não recebe a resposta de uma solicitação do executor de comandos do Cisco DNA Center	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: % } </pre>
Se o Cisco DNA Center não conclui a tarefa no tempo limite configurado (5 minutos por comando no microsserviço de coleta)	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Operation Timedout. The command runner task failed for device RequestURL: %s. No progress details." } </pre>
Se a tarefa do executor de comandos falhou e a ID do arquivo está vazia para a tarefa enviada pelo Cisco DNA Center	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: % id is empty." } </pre>
Se a tarefa do executor de comandos falhou e a tag de ID do arquivo não foi retornada pelo Cisco DNA Center	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: % file id details." } </pre>
Se o dispositivo não estiver qualificado para a ação do executor de comandos	<pre> { "command": "config paging disable", "status": "Failed", "commandResponse": "", "errorMessage": "Requested devices are not in inventory,try with other devices available in inventory" } </pre>
Se o executor de comandos está desativado para o usuário	<pre> { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "{\nmessage\": \"Role does not have valid permissions to access th API\\\"}\n" } </pre>

Respostas à falha de verificação de diagnóstico

A falha na verificação e a causa podem ser de qualquer um dos componentes listados

Quando o usuário inicia uma verificação no portal, ocasionalmente, isso resulta em "falha: erro interno do servidor"

A causa do problema pode ser qualquer um dos componentes listados

- Ponto de controle
- Gateway de dados de rede
- Conector
- Verificação de diagnóstico
- Microserviço do CX Cloud Agent [gerenciador de dispositivos, coleta]
- Cisco DNA Center
- APIX
- Mashery
- Ping Access
- IRONBANK
- IRONBANK
- Broker de Big Data (BDB)

Para ver os logs:

1. Faça login no console do CX Cloud Agent
2. ssh para cxcadmin e forneça a senha
3. Execute `kubectl get pods`
4. Obtenha o nome do pod da coleção, do conector e da facilidade de manutenção.
5. Para verificar a coleta, o conector e os registros de microserviço de manutenção

- Execute `kubectl logs`
- Execute `kubectl logs`
- Execute `kubectl logs`

A tabela mostrada aqui exibe o snippet de erro visto nos logs de microserviço de coleção e microserviço de manutenção que ocorrem devido aos problemas/restrições com os componentes.

Caso de uso

O dispositivo pode ser acessado e suportado, mas os comandos a serem executados nesse dispositivo estão listados em bloco no microserviço de coleta

Se o dispositivo em que você tentou fazer a verificação não estiver disponível.

Ocorre em um cenário, quando há um problema de sincronização entre os componentes, como portal, verificação de diagnóstico, componente da CX e Cisco DNA Center

Se o dispositivo em que você tentou fazer a verificação estiver ocupado, (em um cenário) em que o mesmo dispositivo fez parte de outro trabalho

Snippet de registro no microserviço de coleta

```
{
  "command": "config paging disable",
  "status": "Command_Disabled",
  "commandResponse": "Command collection disabled",
}
```

No device found with id 02eb08be-b13f-49d63-eaf4e882f71a

All requested devices are already being queried by command runner in another session. Please try other devices".

e nenhuma solicitação paralela será resolvida no Cisco DNA Center para o dispositivo.

Se o dispositivo não for compatível para verificação

Se o dispositivo que tentou fazer a varredura estiver inacessível

Se o Cisco DNA Center não estiver acessível no Cloud Agent ou se o microsserviço de coleta do Cloud Agent não recebe a resposta de uma solicitação do executor de comandos do Cisco DNA Center

```
Requested devices are not in inventory, try
other devices available in inventory
"Error occurred while executing command
ud\nError connecting to device [Host: x.x.x
No route to host : No route to host
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "The command runner ta
failed for device %s, RequestURL: %s."
}
```

Caso de uso

Se os detalhes do agendamento da solicitação de verificação estiverem ausentes

Se os detalhes do dispositivo da solicitação de verificação estiverem ausentes

Se a conexão entre o CPA e a conectividade estiver inativa

Se o dispositivo solicitado para verificação não estiver disponível em Verificações de diagnóstico

Snippet de registro no microsserviço do agente de ponto de controle

Failed to execute request

```
{"message":"23502: null value in column \"schedule\" violates
null constraint"}
```

Failed to create scan policy. No valid devices in the request

Failed to execute request.

Failed to submit the request to scan. Reason =

```
{"message\": \"Device with Hostname=x.x.x.x' was not found
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.