

Guia de visão geral do CX Agent v3.1

Contents

[Introdução](#)

[Pré-requisitos](#)

[Acesso a domínios críticos](#)

[Domínios específicos do CX Agent Portal](#)

[Domínios específicos do CX Agent OVA](#)

[Versões suportadas do Catalyst Center](#)

[Navegadores compatíveis](#)

[Lista de produtos suportados](#)

[Atualizando/instalando o CX Agent v3.1](#)

[Atualização de VMs existentes para configurações grandes e médias](#)

[Fazendo upgrade para o CX Agent v3.1](#)

[Atualizações automáticas](#)

[Atualizações manuais](#)

[Adicionando agente CX](#)

[Configurando o CX Agent para BCS/LCS](#)

[Pré-requisitos](#)

[Configurando o agente CX](#)

[Configurando capacidades RADKit](#)

[Integrando o cliente RADKit através da CLI](#)

[Configurando o Vault para agentes CX existentes](#)

[Configurando o HashiCorp Vault na interface de usuário da nuvem do CX](#)

[Integração do CX Agent com o HashiCorp Vault através da CLI](#)

[Pré-requisitos](#)

[Integração com o HashiCorp Vault](#)

[Habilitando a integração do compartimento HashiCorp](#)

[Desativando a integração do compartimento HashiCorp](#)

[Esquema de Credenciais de Dispositivo do HashiCorp Vault](#)

[Configurando credenciais de dispositivo no HashiCorp Vault \(primeira vez\)](#)

[Adicionando mais credenciais ao HashiCorp Vault](#)

[Arquivo semente de nuvem CX com credenciais padrão](#)

[Adicionando o Catalyst Center como Origem de Dados](#)

[Adição do SolarWinds® como uma fonte de dados](#)

[Adição de Outros Ativos como Origens de Dados](#)

[Protocolos de descoberta](#)

[Protocolos de conectividade](#)

[Limitações de Processamento de Telemetria para Dispositivos](#)

[Adicionando outros ativos usando um arquivo de propagação](#)

[Adicionando outros recursos usando um novo arquivo de seed](#)

[Adicionando outros recursos usando um arquivo de propagação modificado](#)



[Credenciais padrão para o arquivo de propagação](#)

[Adicionando outros ativos usando intervalos de IP](#)

[Adicionando outros ativos por intervalos de IP](#)

[Editando Intervalos IP](#)

[Excluindo intervalo de IPs](#)

[Sobre os dispositivos descobertos de vários controladores](#)

[Programando verificações de diagnóstico](#)

[Atualizando VMs do CX Agent para configurações médias e grandes](#)

[Reconfiguração usando o VMware vSphere Thick Client](#)

[Reconfiguração usando o cliente da Web ESXi v6.0](#)

[Reconfiguração usando o Web Client vCenter](#)

[Implantação e configuração de rede](#)

[Implantação do OVA](#)

[Instalação do ThickClient ESXi 5.5/6.0](#)

[Instalação do WebClient ESXi 6.0](#)

[Instalação do WebClient vCenter](#)

[Instalação do OracleVirtual Box 7.0.12](#)

[Instalação do Microsoft Hyper-V](#)

[Configuração de rede](#)

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

[Configurando dispositivos para encaminhar syslog para o CX Cloud Agent](#)

[Pré-requisitos](#)

[Definir Configuração De Encaminhamento De Syslog](#)

[Configurando outros ativos \(coleta direta de dispositivos\) para encaminhar o Syslog ao agente CX](#)

[Servidores Syslog existentes com capacidade de encaminhamento](#)

[Servidores Syslog existentes sem capacidade de encaminhamento OU sem servidor Syslog](#)

[Habilitando configurações de syslog de nível de informação para o Cisco Catalyst Center](#)

[Backup e restauração da VM em nuvem do CX](#)

[Fazendo backup da máquina virtual em nuvem do CX](#)

[Restaurando a VM em nuvem do CX](#)

[Security](#)

[Segurança física](#)

[Segurança da conta](#)

[Segurança de rede](#)

[Autenticação](#)

[Blindagem](#)

[Segurança de dados](#)

[Transmissão de Dados](#)

[Registros e monitoramento](#)

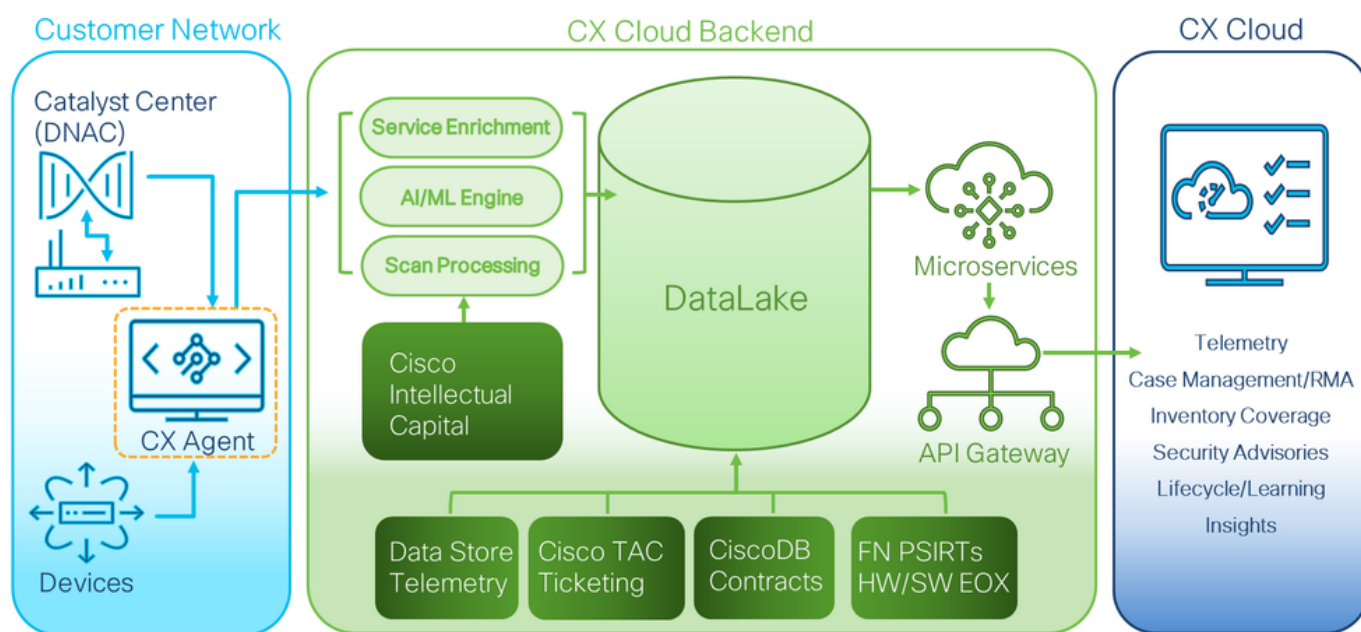
[Comandos de telemetria da Cisco](#)

[Resumo de segurança](#)

Introdução

Este documento descreve o agente de experiência do cliente (CX) da Cisco. O CX Agent da Cisco é uma plataforma altamente escalável que coleta dados de telemetria dos dispositivos de rede do cliente para fornecer insights práticos para os clientes. O CX Agent permite a transformação da Inteligência Artificial (AI)/Aprendizagem Automática (ML) dos dados de configuração ativa em execução em insights proativos e preditivos exibidos na nuvem CX (incluindo ofertas de Controles de sucesso, Smart Net Total Care (SNTC) e Business Critical Services (BCS) ou Lifecycle Services (LCS)).

CX Cloud Architecture



Arquitetura de nuvem CX

Este guia destina-se apenas aos administradores de nuvem e parceiros da CX. Os usuários com as funções SUA (Super User Admin) e Admin têm as permissões necessárias para executar as ações descritas neste guia.

Este guia é específico do CX Agent v3.1. Consulte a página [Cisco CX Agent](#) para acessar versões anteriores.

Observação: as imagens deste guia são apenas para referência. O conteúdo real pode variar.

Pré-requisitos

O CX Agent é executado como uma máquina virtual (VM) e está disponível para download como um dispositivo virtual aberto (OVA) ou um disco rígido virtual (VHD).

Requisitos de implantação

- Um dos seguintes hipervisores é necessário para uma nova instalação:
 - VMware ESXi v5.5 ou posterior

- Oracle Virtual Box v5.2.30 ou posterior
- Hypervisor Windows versão 2012 a 2022 e versão 2025
- As configurações na tabela a seguir são necessárias para a implantação da VM:

Tipo de Implantação do Agente CX	Número de núcleos da CPU	RAM	Disco rígido	*Número máximo de ativos diretamente conectado ao CX Agent	Hipervisores compatíveis
OVA pequeno	8C	16 GB	200 GB	10,000	VMware ESXi, Oracle VirtualBox e Windows Hyper-V
ÓVULOS médios	16 C	32 GB	600 GB	20,000	VMware ESXi
ÓVULOS GRANDES	32 C	64 GB	1.200 GB	50,000 :	VMware ESXi

*Além de conectar 20 clusters do Cisco Catalyst Center (Catalyst Center) ou 10 clusters do Catalyst Center para cada instância do CX Cloud Agent.

 Nota: O serviço RADKit está disponível exclusivamente para implantações de agentes CX de tipos OVA médios e grandes.

- Para clientes que usam data centers designados dos EUA como a região de dados principal para armazenar dados da nuvem CX, o agente CX deve ser capaz de se conectar aos servidores mostrados aqui, usando o nome de domínio totalmente qualificado (FQDN) e usando HTTPS na porta TCP 443:
 - FQDN agent.us.cisco.cloud
 - FQDN ng.acs.agent.us.cisco.cloud
 - FQDN cloudssso.cisco.com
 - FQDN api-cx.cisco.com
- Para clientes que usam data centers designados na Europa como a principal região de dados para armazenar dados da nuvem CX: o CX 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 cloudssso.cisco.com
 - FQDN api-cx.cisco.com
- Para clientes que usam data centers designados do Pacífico Asiático como a região de dados principal para armazenar dados da nuvem CX: o CX 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 data centers designados da Europa e do Pacífico Asiático 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.
- Para clientes que usam RADKit usando FQDN e HTTPS na porta TCP 443:
 - FQDN US: radkit.us.cisco.cloud
 - FQDN EMEA: radkit.emea.cisco.cloud
 - FQDN APJC: radkit.apjc.cisco.cloud
- Para permitir que o RADKit anexe saída a uma solicitação de serviço, o FQDN cxd.cisco.com deve estar acessível para o agente CX.
- A tabela a seguir fornece um resumo das portas e dos protocolos que devem ser abertos e ativados para que o CX Cloud Agent funcione corretamente:

CX Cloud Agent Traffic

Source	Destination	Protocol	Port	Purpose	Type
CX Cloud Agent	All regions: cloudsso.cisco.com api-cx.cisco.com agent.us.cisco.cloud radkit.emea.cisco.cloud Catalyst Center AMER region: ng.acs.agent.us.cisco.cloud EMEA region: agent.emea.cisco.cloud ng.acs.agent.emea.cisco.cloud APJC region: agent.apjc.cisco.cloud ng.acs.agent.apjc.cisco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- Um IP é detectado automaticamente se o Dynamic Host Configuration Protocol (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 de Serviço de Nome de Domínio (DNS) devem estar disponíveis.
- Somente IPv4 é suportado.
- As versões certificadas do Cluster de HA (High Availability, nó único) do Catalyst Center são 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x e Catalyst Center Virtual Appliance e Catalyst Center Virtual Appliance.

- Se a rede tiver interceptação SSL, permita a listagem do endereço IP do agente CX.
- Para todos os ativos diretamente conectados, é necessário o nível de privilégio SSH 15.
- Usar somente os nomes de host fornecidos; endereços IP estáticos não podem ser usados.

Acesso a domínios críticos

Para iniciar a jornada da CX Cloud, os usuários precisam acessar os seguintes domínios. Use apenas os nomes de host fornecidos; não use endereços IP estáticos.

Domínios específicos do CX Agent Portal

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

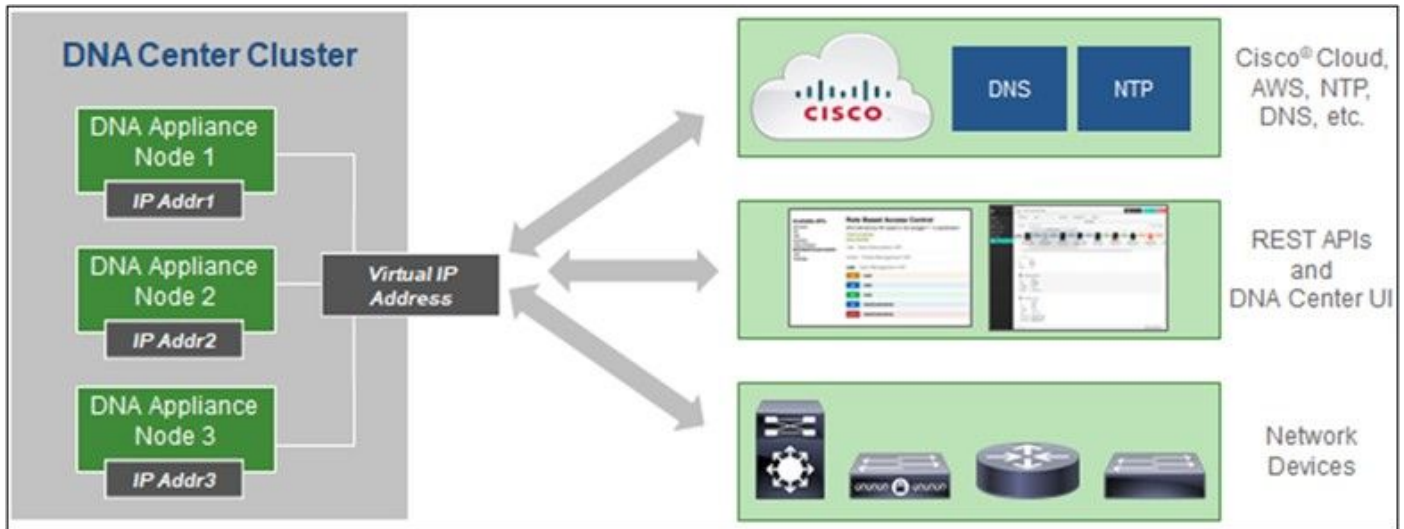
Domínios específicos do CX Agent OVA

AMÉRICAS	EMEA (Europa, Oriente Médio e África)	APJC
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

 Note: O acesso de saída deve ser permitido com o redirecionamento habilitado na porta 443 para os FQDNs especificados.

Versões suportadas do Catalyst Center

As versões compatíveis de nó único e cluster HA do Catalyst Center são 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x e Catalyst Center Virtual Appliance e Catalyst Center Virtual Appliance.



Multi-Node HA Cluster Cisco DNA Center

Navegadores compatíveis

Para obter a melhor experiência em Cisco.com, a versão oficial mais recente desses navegadores é recomendada:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Lista de produtos suportados

Para exibir a lista de produtos suportados pelo CX Agent, consulte a [Lista de produtos suportados](#).

Atualizando/instalando o CX Agent v3.1

- Os clientes atuais que estão fazendo upgrade para a nova versão devem consultar [Upgrading CX Agent v3.1](#).
- Os novos clientes que implementarem uma nova instalação flexível do OVA v3.1 devem consultar [Adicionando o CX Agent](#).

Atualização de VMs existentes para configurações grandes e médias

Os clientes podem atualizar sua configuração de VM existente para médio ou grande usando as opções de OVA flexível com base no tamanho e na complexidade da rede.

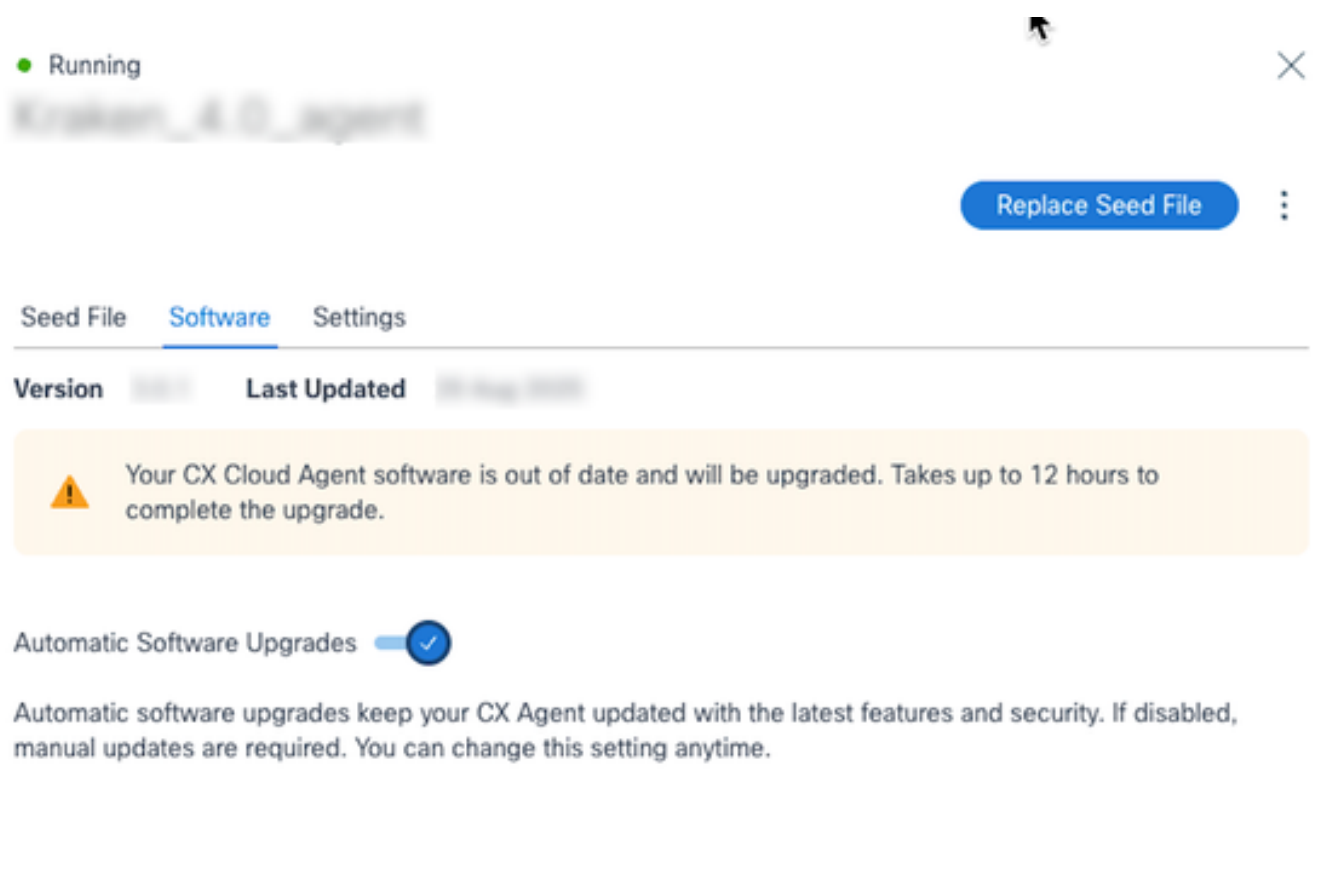
Para atualizar a configuração de VM existente de pequena para média ou grande, consulte a seção [Atualizando VMs do Agente CX para média e grande configuração](#).

Fazendo upgrade para o CX Agent v3.1

Os clientes existentes podem atualizar para a versão mais recente ativando atualizações automáticas ou optando por atualizar manualmente a partir da versão existente.

Atualizações automáticas

Os clientes podem ativar a alternância Atualização automática de software para garantir que seu sistema seja atualizado quando as novas versões forem lançadas. Essa opção é ativada por padrão para novas instalações, mas pode ser modificada a qualquer momento para alinhar-se com as políticas da empresa ou para programar atualizações durante as janelas de manutenção planejadas.



Atualizações automáticas

 Observação: os upgrades automáticos são desativados por padrão para instâncias do CX Agent existentes, mas os usuários podem ativá-los a qualquer momento.

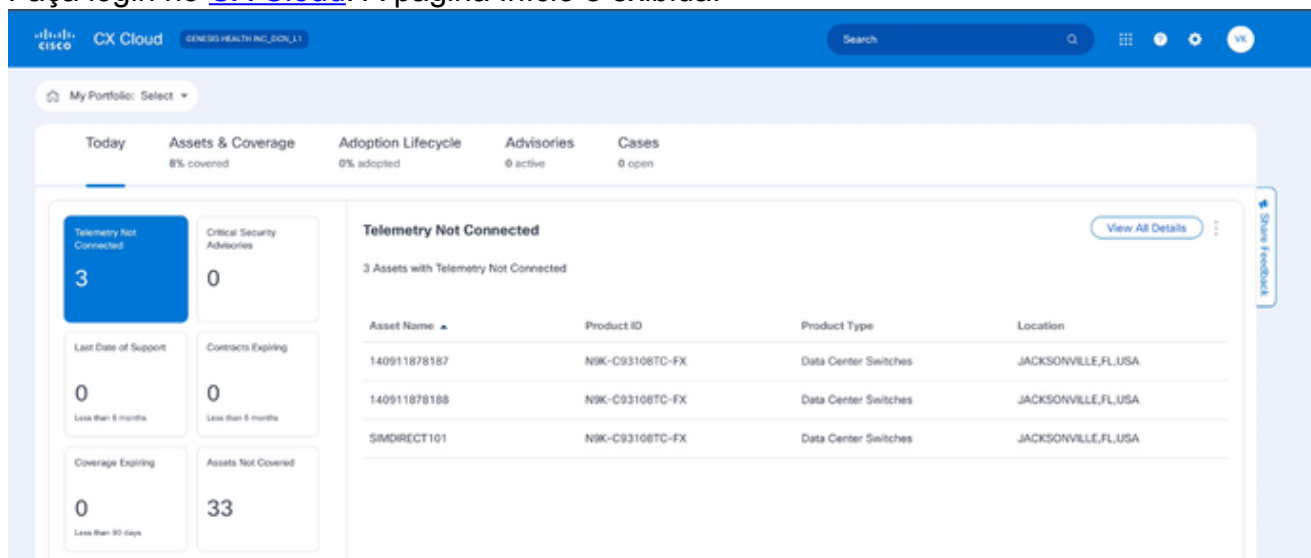
Atualizações manuais

Os clientes que preferirem não usar atualizações automáticas e não tiverem habilitado Atualizações automáticas de software podem optar por atualizar manualmente. O CX Agent v2.4.x ou superior oferece suporte a um upgrade direto para v3.1 seguindo as etapas descritas nesta seção.

 Observação: os clientes com CX Agent v2.3.x ou anterior devem fazer upgrade incremental para v2.4.x antes de fazer upgrade para v3.1 ou executar uma nova instalação do OVA.

Para instalar o upgrade do CX Agent v3.1 a partir do CX Cloud:

1. Faça login no [CX Cloud](#). A página Início é exibida.

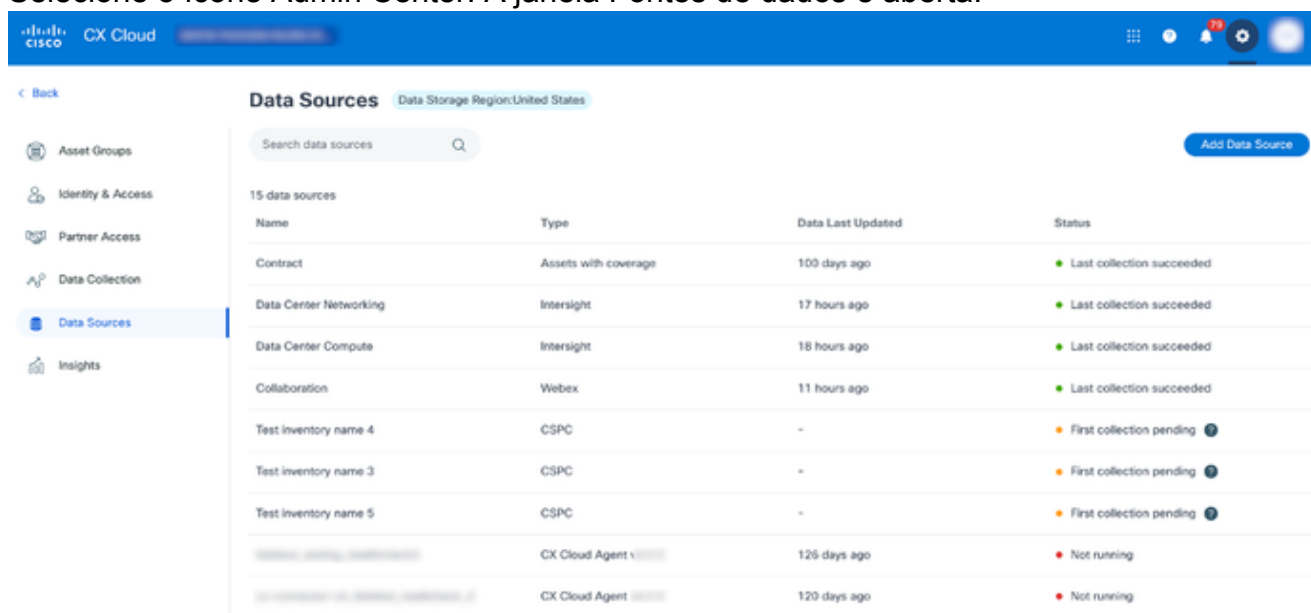


The screenshot shows the CX Cloud dashboard. At the top, there's a navigation bar with the Cisco logo, 'CX Cloud', and a search bar. Below the navigation bar, there's a 'My Portfolio' section with tabs for 'Today', 'Assets & Coverage' (8% covered), 'Adoption Lifecycle' (0% adopted), 'Advisories' (0 active), and 'Cases' (0 open). The main content area features several cards: 'Telemetry Not Connected' (3), 'Critical Security Advisories' (0), 'Last Date of Support' (0), 'Contracts Expiring' (0), 'Coverage Expiring' (0), and 'Assets Not Covered' (33). To the right, there's a section titled 'Telemetry Not Connected' with a table of 3 assets.

Asset Name	Product ID	Product Type	Location
140911878187	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA
140911878188	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA
SIMDIRECT101	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA

Página inicial do CX Cloud

2. Selecione o ícone Admin Center. A janela Fontes de dados é aberta.

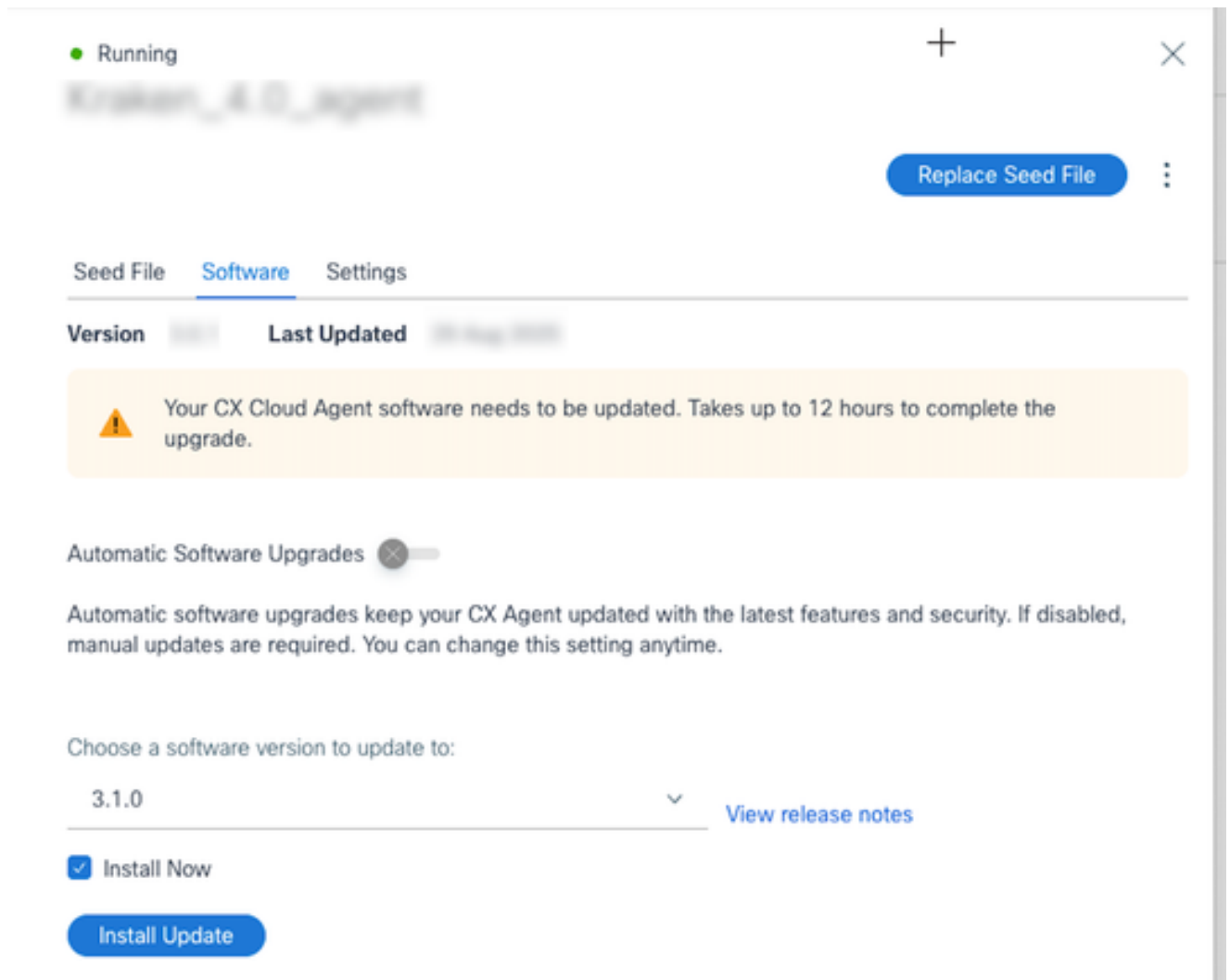


The screenshot shows the 'Data Sources' page in the CX Cloud Admin Center. The page has a left sidebar with navigation links: 'Back', 'Asset Groups', 'Identity & Access', 'Partner Access', 'Data Collection', 'Data Sources' (selected), and 'Insights'. The main content area is titled 'Data Sources' and shows a table of 15 data sources. The table has columns for 'Name', 'Type', 'Data Last Updated', and 'Status'.

Name	Type	Data Last Updated	Status
Contract	Assets with coverage	100 days ago	Last collection succeeded
Data Center Networking	Intersight	17 hours ago	Last collection succeeded
Data Center Compute	Intersight	18 hours ago	Last collection succeeded
Collaboration	Webex	11 hours ago	Last collection succeeded
Test inventory name 4	CSPC	-	First collection pending
Test inventory name 3	CSPC	-	First collection pending
Test inventory name 5	CSPC	-	First collection pending
CX Cloud Agent v2.4.x	CX Cloud Agent	126 days ago	Not running
CX Cloud Agent v2.3.x	CX Cloud Agent	120 days ago	Not running

Origem dos dados

3. Clique na fonte de dados CX Agent. A janela de detalhes do CX Agent será aberta.



Running

Replace Seed File

Seed File Software Settings

Version Last Updated

⚠ Your CX Cloud Agent software needs to be updated. Takes up to 12 hours to complete the upgrade.

Automatic Software Upgrades

Automatic software upgrades keep your CX Agent updated with the latest features and security. If disabled, manual updates are required. You can change this setting anytime.

Choose a software version to update to:

3.1.0 View release notes

☒ Install Now

Install Update

Atualizações manuais

4. Selecione a versão de software 3.1.0 na lista suspensa Escolha uma versão de software para atualizar para.
5. Clique em Install Update para instalar o CX Agent v3.1.

 Observação: os clientes podem agendar a atualização para mais tarde desmarcando a caixa de seleção Instalar agora, que exibe opções de agendamento.

Adicionando agente CX

Os clientes podem adicionar até 20 instâncias de agentes CX na nuvem CX.

Para adicionar um agente CX:

1. Faça login no [CX Cloud](#). A página Início é exibida.

The screenshot displays the Cisco CX Cloud dashboard. At the top, the navigation bar includes the Cisco logo, 'CX Cloud', and a search bar. Below this, a 'My Portfolio' dropdown is visible. The main dashboard is divided into several sections:

- Summary Cards:** A grid of cards showing key metrics:
 - Telemetry Not Connected:** 10882 (Last 7 days)
 - Crashed Assets:** 0 (Last 7 days)
 - High Crash Risk Assets:** 0 (Last 7 days)
 - Software Last Date of Support:** 8 (Less than 6 months)
 - Critical Faults:** 0 (Last 7 days)
 - Critical Security Advisories:** 1 (Last 7 days)
 - Hardware Last Date of Support:** 407 (Less than 6 months)
 - Contracts Expiring:** 1 (Less than 6 months)
- Telemetry Not Connected Table:** A table listing 10882 assets with telemetry not connected. The table has columns for Asset Name, Product ID, Product Type, and Location. A mouse cursor is pointing at the 'SAN FRANCISCO, CA, USA' location in the last row.

Asset Name	Product ID	Product Type	Location
[Redacted]	[Redacted]	Collaboration Endpoints	LITHIA SPRINGS, GA, USA
[Redacted]	[Redacted]	Collaboration Endpoints	LITHIA SPRINGS, GA, USA
[Redacted]	[Redacted]	Collaboration Endpoints	LITHIA SPRINGS, GA, USA
[Redacted]	[Redacted]	Collaboration Endpoints	LITHIA SPRINGS, GA, USA
[Redacted]	[Redacted]	Collaboration Endpoints	LITHIA SPRINGS, GA, USA
[Redacted]	[Redacted]	Collaboration Endpoints	LITHIA SPRINGS, GA, USA
[Redacted]	[Redacted]	Switches	SAN FRANCISCO, CA, USA
[Redacted]	[Redacted]	Switches	SAN FRANCISCO, CA, USA
[Redacted]	[Redacted]	Switches	SAN FRANCISCO, CA, USA
- Cases Section:** Shows 'My open cases' as 1935 and 'Action required' as 12. A link 'View all open cases (2310)' is present.
- Adoption Lifecycle Section:** Displays progress for 'Service Provider Networking SR-MPLS Enabled Network' and 'Service Provider Networking SRv6 Enabled Network', both at 0% complete. It includes 'Next task' links for each.

Página inicial do CX Cloud

2. Selecione o ícone Admin Center. A janela Fontes de dados é aberta.

Cisco

CX Cloud

9999

Back

Asset Groups

Identity & Access

Partner Access

Data Collection

Data Sources

Insights

16 data sources

Collaboration

Webex

16 hours ago

Last collection succeeded

Firewall Management Center

-

First collection pending

CXAgent-2

CX Cloud Agent v2.4.0

2 minutes ago

Running

CX Cloud Agent v2.4.0

27 days ago

Not running

CX Cloud Agent v2.4.0

1 minutes ago

Running

CX Cloud Agent v2.4.0

1 minutes ago

Running

CX Cloud Agent v2.4.0

1 minutes ago

Running

CX Cloud Agent v2.4.0

1 minutes ago

Running

Catalyst Center

3 minutes ago

Reachable

Catalyst Center

3 minutes ago

Reachable

CX Cloud Agent v2.4.0

1 minutes ago

Running

Add Data Source

16 data sources	Collaboration	Webex	16 hours ago	Last collection succeeded
		Firewall Management Center	-	First collection pending
	CXAgent-2	CX Cloud Agent v2.4.0	2 minutes ago	Running
		CX Cloud Agent v2.4.0	27 days ago	Not running
		CX Cloud Agent v2.4.0	1 minutes ago	Running
		CX Cloud Agent v2.4.0	1 minutes ago	Running
		CX Cloud Agent v2.4.0	1 minutes ago	Running
		CX Cloud Agent v2.4.0	1 minutes ago	Running
		Catalyst Center	3 minutes ago	Reachable
		Catalyst Center	3 minutes ago	Reachable
		CX Cloud Agent v2.4.0	1 minutes ago	Running

Origem dos dados

- Clique em Adicionar fonte de dados. A página Adicionar fonte de dados é aberta. As opções exibidas variam de acordo com as assinaturas do cliente.

Add Data Source

Search data sources



Catalyst Center
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)

Add Data Source



Cisco Catalyst SD-WAN Manager
Supports the Success Track for WAN

Add Data Source



Common Services Platform Collector (CSPC)
Supports assets managed by CSPC

Add Data Source



Contracts
Supports assets associated with a contract

Add Data Source



CX Cloud Agent
Add CX Cloud Agents to your network to support a variety of Success Tracks.

Add Data Source



Intersight
Supports the Data Center Compute and Data Center Networking Success Tracks

Add Data Source



Meraki dashboard
Supports Meraki

Add Data Source



Other Assets by IP Ranges
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

Add Data Source



Other Assets by Seed File
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

Add Data Source

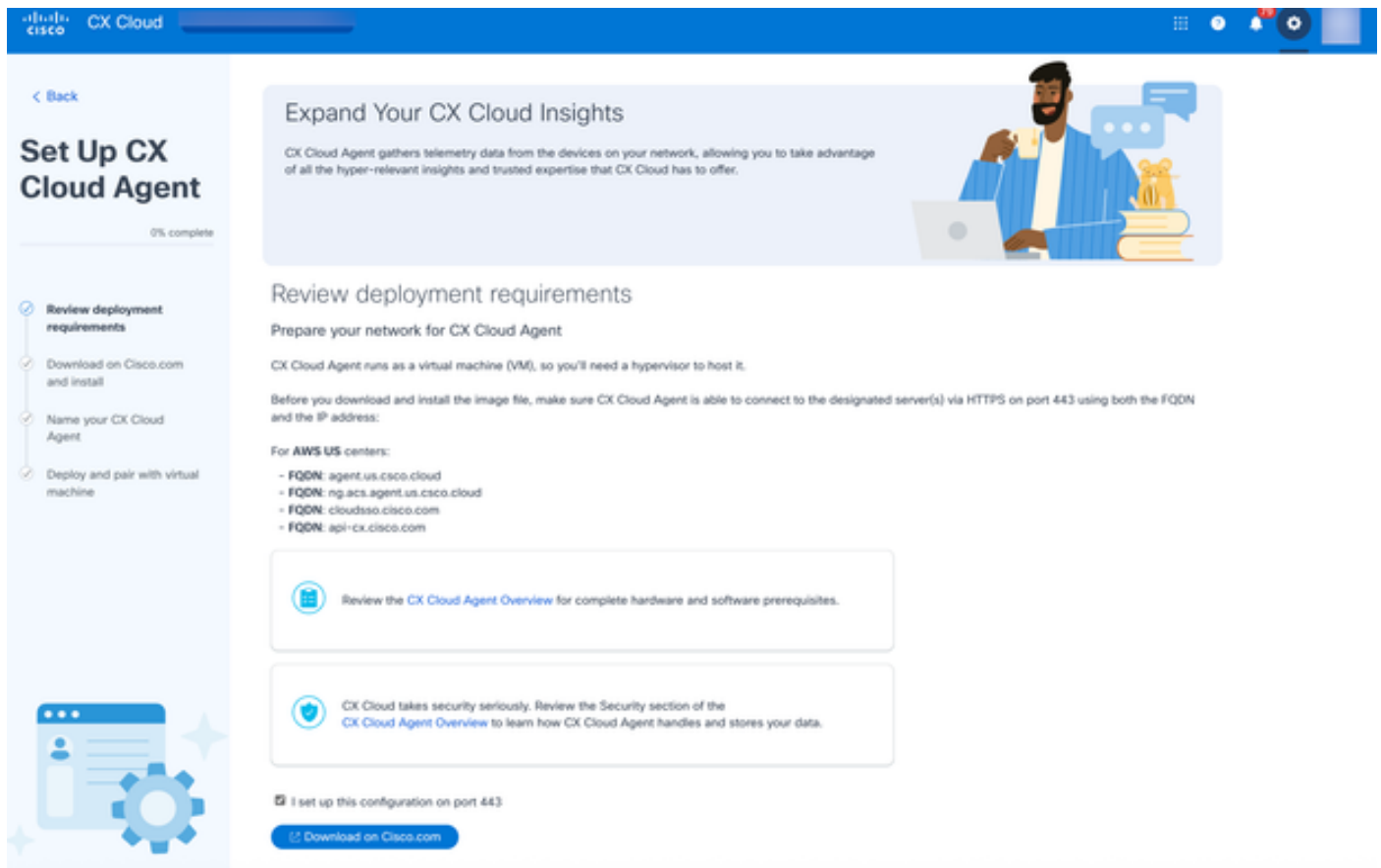


Webex
Supports the Success Track for Collaboration

Add Data Source

Adicionar Fonte de Dados

4. Clique em Add Data Source na opção CX Agent. A janela Configurar agente CX se abre.

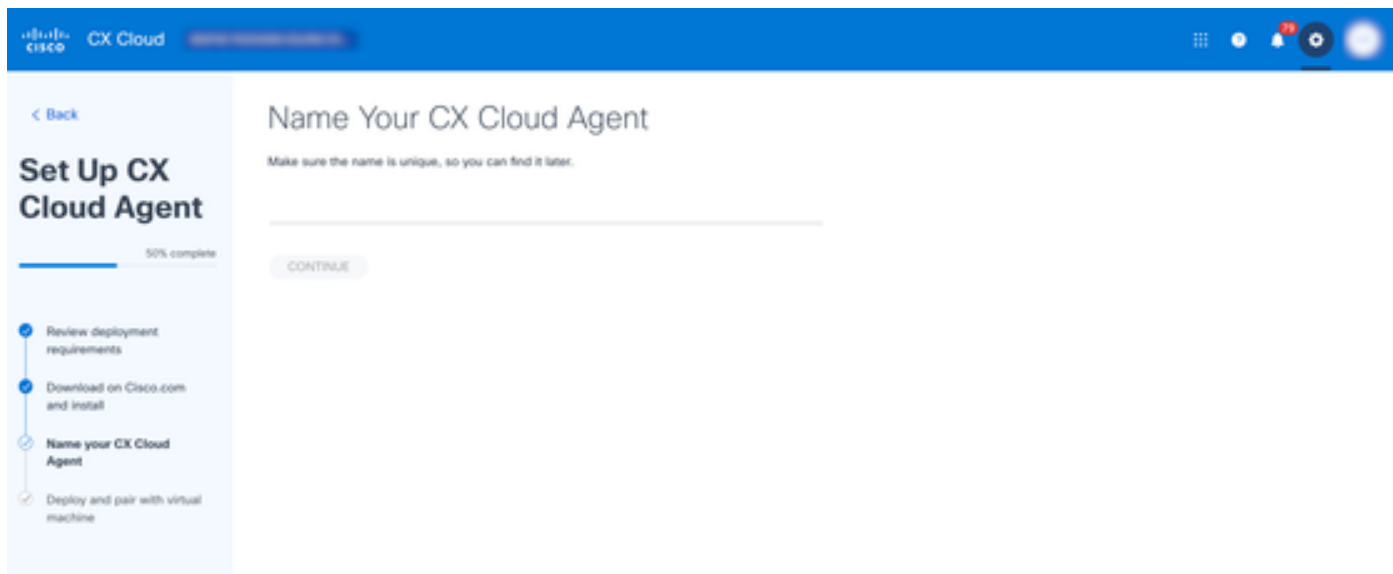


Adicionando agente CX

5. Revise a seção Review deployment requirements e marque a caixa de seleção I set up this configuration on port 443.
6. Clique em Download em Cisco.com. A janela Download de software é aberta em outra guia.
7. Faça download do arquivo "CX Agent v3.1.0 OVA".

 Observação: um código de emparelhamento necessário para concluir a configuração do CX Agent é gerado após a implantação do arquivo "OVA".

8. Insira o nome do agente CX no campo Name Your CX Cloud Agent.



Set Up CX Cloud Agent

50% complete

- Review deployment requirements
- Download on Cisco.com and install
- Name your CX Cloud Agent**
- Deploy and pair with virtual machine

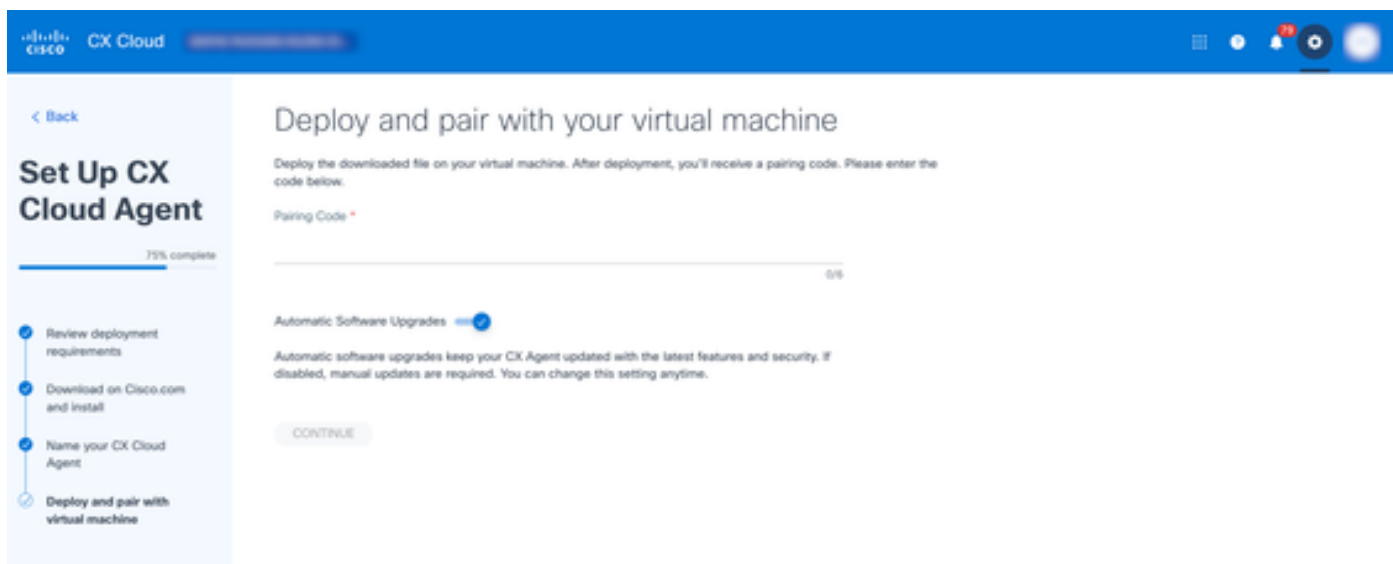
Name Your CX Cloud Agent

Make sure the name is unique, so you can find it later.

CONTINUE

Nome Agente CX

9. Clique em Continuar. A janela Implantar e emparelhar com sua máquina virtual se abre.



Set Up CX Cloud Agent

75% complete

- Review deployment requirements
- Download on Cisco.com and install
- Name your CX Cloud Agent
- Deploy and pair with virtual machine**

Deploy and pair with your virtual machine

Deploy the downloaded file on your virtual machine. After deployment, you'll receive a pairing code. Please enter the code below.

Pairing Code *

0/6

Automatic Software Upgrades 

Automatic software upgrades keep your CX Agent updated with the latest features and security. If disabled, manual updates are required. You can change this setting anytime.

CONTINUE

Código de emparelhamento

10. Insira o código de emparelhamento recebido após a implantação do arquivo "OVA" baixado.

11. Clique em Continuar. O andamento do registro é exibido, seguido por uma mensagem de confirmação.

 Note: Repita as etapas acima para adicionar instâncias adicionais do CX Agent como uma fonte de dados.

Configurando o CX Agent para BCS/LCS

O novo recurso de coleta convergente da Cisco otimiza a configuração do CX Agent v3.1 para BCS/LCS, simplificando a experiência do cliente.

 Nota: Esta configuração é específica para os engenheiros de suporte da Cisco responsáveis pela configuração do coletor para clientes BCS/LCS.

Os clientes do BCS/LCS podem visitar a [CX Cloud Community](#) para saber mais sobre a integração de usuários e outras informações relacionadas.

Pré-requisitos

Engenheiros de suporte com SUA (Super User Administrator, administrador superusuário) e acesso de administrador só podem executar a configuração do CX Agent para BCS/LCS.

Configurando o agente CX

Para configurar o CX Agent para BCS/LCS, entre em contato com o Suporte da Cisco.

Configurando capacidades RADKit

O CX Agent v3.1 fornece uma configuração RADKit opcional projetada para aprimorar o gerenciamento remoto e a solução de problemas de dispositivos Cisco no CX Cloud. Quando habilitados, os usuários autorizados podem executar com segurança operações como captura de dados, configuração e atualizações de software remotamente. Essas configurações podem ser ativadas ou desativadas a qualquer momento com base nos requisitos operacionais do cliente.

Para obter detalhes abrangentes sobre RADKit, consulte [Cisco RADKit](#).

Integrando o cliente RADKit através da CLI

Para integrar o serviço de cliente RADKit, crie uma conta de administrador e inscreva o serviço executando as seguintes etapas:

 Observação: as etapas a seguir exigem acesso raiz à VM do agente CX.

1. Abra o terminal e o Secure Shell (SSH) em uma VM usando as credenciais apropriadas, por exemplo:

```
ssh your_username@your_vm_ip
```

2. Execute o seguinte comando para ativar a conectividade de rede:

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

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

3. Na máquina local, envie uma solicitação POST ao endpoint do gerente para criar uma conta de administrador. O corpo do pedido deve incluir:

- `admin_name` (obrigatório): O nome de usuário da conta de administrador
- `email` (opcional): O endereço de email da conta de administrador
- `nome_completo` (opcional): O nome completo do Administrador
- `descrição` (opcional): Uma descrição da conta de administrador

O exemplo a seguir mostra como enviar essa solicitação usando cURL:

```
curl -X POST \
  http://<seu_vm_ip>:30100/radkitmanager/v1/createAdmin \
  -H "Tipo de conteúdo: aplicativo/json" \
  -d '{
    "admin_name": "admin_user123",
    "e-mail": "admin@example.com",
    "nome_completo": "Usuário administrador",
    "Descrição": "Conta de administrador para gerenciar o sistema"
  }'
```

Após a criação bem-sucedida de uma conta de administrador, o servidor responde com uma mensagem de confirmação indicando que a conta de administrador foi criada com êxito. Essa resposta também inclui uma senha temporária que deve ser alterada no primeiro login. No entanto, se a conta de administrador já existir, o servidor retornará um código de status 400 com a mensagem "Admin já criado".

4. Abra o navegador da Web e navegue até a IU da Web do RADKit:
`https://<your_vm_ip>:30101/`.
5. Faça login usando o nome de usuário administrador (`admin_name`) e a senha temporária fornecida na resposta.

 **Note:** No primeiro login, os usuários são solicitados a alterar a senha. Siga as instruções para definir uma nova senha.

6. Execute o cliente RADKit no computador local para registrar o serviço.
7. Após a autenticação, gere uma senha descartável executando o seguinte comando:

```
grant_service_otp()
```

8. Na máquina local, envie uma solicitação POST ao endpoint do gerente para inscrever o serviço. O corpo do pedido deve incluir:
 - `OTP` (obrigatório): A cadeia de caracteres de senha ocasional

O exemplo a seguir mostra como enviar essa solicitação usando cURL:

```
curl -X POST \
  http://<seu_vm_ip>:30100/radkitmanager/v1/enrollService \
  -H "Tipo de conteúdo: aplicativo/json" \
  -d '{
    "senha_única": "PROD.: 1234-1234-1234"
  }'
```

Após a inscrição bem-sucedida, uma mensagem de confirmação é exibida e os usuários podem gerenciar o serviço RADKit usando uma conta de administrador.

Para desabilitar a conectividade de rede, execute o seguinte comando:

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

Configurando o Vault para agentes CX existentes

O recurso opcional de configuração do Vault permite que o CX Cloud se conecte com segurança a um serviço do Vault para acessar dados confidenciais, como tokens e listas de inventário, usando as credenciais mais recentes. Quando habilitado, o CX Cloud usa automaticamente o endereço e o token configurados. Essa configuração pode ser ativada ou desativada a qualquer momento. Atualmente, somente a configuração de cofre da HashiCorp é suportada.

O cofre pode ser configurado de duas maneiras:

- Por meio da interface de usuário da nuvem do CX
- Através do CLI

Configurando o HashiCorp Vault na interface de usuário da nuvem do CX

Para configurar o cofre HashiCorp para um agente CX existente:

1. Selecione o ícone Admin Center. A janela Fontes de dados é aberta.
2. Clique na fonte de dados do agente CX. A janela de detalhes do CX Agent será aberta.

Configurações

3. Clique na guia Configurações.
4. Ative a alternância Configuração do cofre.

Configuração do Cofre

5. Informe detalhes nos campos Endereço e Token.

6. Clique em Submeter. Uma confirmação e o endereço IP adicionado são exibidos.

Os clientes podem remover o cofre configurado clicando em Remover.

Integração do CX Agent com o HashiCorp Vault através da CLI

Esta seção descreve o procedimento para configurar a conexão entre o Cisco CX Agent e uma instância do HashiCorp Vault. Essa integração permite o armazenamento seguro e a recuperação de credenciais de dispositivo, melhorando a postura geral de segurança.

Pré-requisitos

- acesso cxcroot à VM do agente CX
- Uma instância do Vault em execução e acessível

Integração com o HashiCorp Vault

- Para habilitar a integração do Vault, execute o seguinte comando:

```
cxcli agent vault on
```

- Para desabilitar a integração do Vault, execute o seguinte comando:

```
cxcli agent vault off
```

- Para verificar o status atual da integração do Vault, execute o seguinte comando:

```
status do cxcli agent vault
```

Habilitando a integração do compartimento HashiCorp

Para ativar a integração do Vault:

1. Faça login no CX Agent via SSH usando a conta de usuário cxcroot para acessar o CX Agent.
2. Alterne para o usuário raiz para elevar privilégios executando o seguinte comando:

```
sudo su
```

3. Execute o seguinte comando para verificar o Status de Integração atual do Vault:

```
root@cxcloudagent: /home/cxcroot# cxcli status do cofre do agente  
integração de cofre desabilitada
```

4. Execute o seguinte comando para ativar a Integração do Vault:

```
cxcli agent vault on
```

5. Atualize os seguintes campos:

- Endereço do Cofre
- Token raiz de cofre

6. Para verificar, verifique o status da integração com o Vault. A mensagem de resposta deve confirmar se a integração está ativada:

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

Insira o endereço do cofre da HashiCorp:

Insira o token de cofre da HashiCorp:

```
integração do vault habilitada root@cxcloudagent: /home/cxcroot#
```

Desativando a integração do compartimento HashiCorp

Para acessar o CX Agent:

1. Faça login no CX Agent via SSH usando a conta de usuário cxcroot.
2. Alterne para o usuário raiz para elevar privilégios executando o seguinte comando:

```
sudo su
```

3. Execute o seguinte comando para desativar a Integração de Cofre da HashiCorp:

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

```
integração de cofre desabilitada
```

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

HashiCorp Esquema de Credenciais do Dispositivo do Cofre

Esquema de Credenciais do Cofre: Para obter informações detalhadas sobre as opções disponíveis e os campos suportados para credenciais de dispositivo, faça download do arquivo "Esquema de credenciais do cofre" ([vault-credentials-schema.json](#)).

Exemplo: A seguir está um exemplo de uma credencial JSON baseada no esquema:

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

```
"password": "*****",
"enableUser": "cisco",
"enablePassword": "*****"
}
}
}
```

 Nota: Os usuários podem especificar vários protocolos em um único arquivo JSON de credencial. No entanto, evite incluir protocolos duplicados da mesma família (por exemplo, não inclua SNMPv2c e SNMPv3 no mesmo arquivo de credencial).

## Configurando credenciais de dispositivo no HashiCorp Vault (primeira vez)

1. Efetue login em uma instância do Vault.

### Secrets Engines

[Enable new engine +](#)

|                                                                                                                                                        |                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|  <b>cubbyhole/</b><br><small>per-token private secret storage</small> |   |
|  <b>secret/</b><br><small>key/value secret storage</small>          |  |

Segredo

2. Crie um novo segredo de chave-valor usando o seguinte caminho: secret/seed/credentials.
3. Escolha o mecanismo de armazenamento secreto do valor da chave (secret/).

Secrets / **secret**

 **secret** version 2

[Secrets](#) [Configuration](#)

[Create secret +](#)

### No secrets yet

When created, secrets will be listed here.  
Create a secret to get started.

Segredo do valor da chave

4. Clique em Criar segredo. A janela Create Secret é aberta.

## Create Secret

☐ JSON

### Path for this secret

Names with forward slashes define hierarchical path structures.

seed/credentials

### Secret data

credentialName1

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

⚠ This value will be saved as a string. If you need to save a non-string value, please use the JSON editor.

key

Add

▼ Show secret metadata

Save

Cancel

Segredo do cliente

### 5. Atualize os seguintes campos:

- Caminho do segredo: seed/credenciais
- Dados secretos: coleção de chaves - segredos de valor
- chave: nome de credencial exclusivo personalizado
- valor: Credenciais JSON

6. Clique em Salvar. O segredo deve agora ser armazenado no HashiCorp Vault.

# seed/credentials

Overview Secret Metadata Paths Version History

☐ JSON

DeleteDestroyCopyVersion 1Create new version +

KeyValueVersion 1 created Jun 04, 2025 03:39 PM

credentialName1



```
{
 "targetIp": "5.0.1.*",
 "credentials": {
 "snmpv3": {
 "user": "cisco",
 "authPassword": "cisco123",
 "authAlgorithm": "MD5",
 "privacyPassword": "cisco123",
 "privacyAlgorithm": "AES-256"
 }
 }
}
```

Credenciais

## Adicionando mais credenciais ao HashiCorp Vault

1. Faça login em uma instância do cofre HashiCorp.

# seed/credentials

Overview Secret Metadata Paths Version History

☐ JSON

DeleteDestroyCopyVersion 1Create new version +

KeyValueVersion 1 created Jun 04, 2025 03:39 PM

credentialName1



\*\*\*\*\*

Adicionar Credenciais

2. Navegue até o segredo "segredo/semente/credenciais" já criado.

## Create New Version

☐ JSON

### Path for this secret

Names with forward slashes define hierarchical path structures.

seed/credentials

### Version data

credentialName1

\*

⚠ This value will be saved as a string. If you need to save a non-string value, please use the JSON editor.

key

Add

☐ Show diff

No changes to show. Update secret to view diff

Save

Cancel

Criar Versão

3. Clique em Criar nova versão.

4. Adicione novos segredos fornecendo qualquer número de pares de chave-valor conforme necessário.

5. Clique em Salvar.

## Arquivo semente de nuvem CX com credenciais padrão

- Simplifique o arquivo de propagação: Ao usar as credenciais configuradas através do cofre Hashicorp, simplifique o arquivo de propagação omitindo informações confidenciais
- Especifique somente o endereço IP ou o nome de host: Os usuários podem passar apenas o endereço IP ou o nome de host no arquivo de propagação, deixando outros campos em branco

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

IP ou nome de host

- Use as credenciais de HashiCorp vault e Seed File: Forneça credenciais para alguns dispositivos no Arquivo de Propagação enquanto confia no cofre para gerenciar credenciais para outros dispositivos

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

IP ou nome de host

## Adicionando o Catalyst Center como Origem de Dados

Os usuários com a função Usuário Superadministrador podem adicionar a Origem de Dados do Catalyst Center.

Para adicionar o Catalyst Center como uma Origem de Dados:

1. Selecione o ícone Admin Center. A janela Fontes de dados é aberta.
2. Clique em Adicionar fonte de dados. A página Adicionar Origem de Dados é exibida.

## Add Data Source

Search data sources



**Catalyst Center**  
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)

Add Data Source



**Cisco Catalyst SD-WAN Manager**  
Supports the Success Track for WAN

Add Data Source



**Common Services Platform Collector (CSPC)**  
Supports assets managed by CSPC

Add Data Source



**Contracts**  
Supports assets associated with a contract

Add Data Source



**CX Cloud Agent**  
Add CX Cloud Agents to your network to support a variety of Success Tracks.

Add Data Source



**Intersight**  
Supports the Data Center Compute and Data Center Networking Success Tracks

Add Data Source



**Meraki dashboard**  
Supports Meraki

Add Data Source



**Other Assets by IP Ranges**  
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

Add Data Source



**Other Assets by Seed File**  
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

Add Data Source



**Webex**  
Supports the Success Track for Collaboration

Add Data Source

Adicionar Fonte de Dados

3. Clique em Add Data Source na opção Catalyst Center.

## Which CX Cloud Agent Do You Want to Connect to?

Select option



Cancel

Continue



Selecionar Agente CX

4. Selecione o CX Agent na lista suspensa Qual CX Agent Você Deseja Conectar.
5. Clique em Continuar. A janela Connect to CX Cloud é aberta.

## Connect to CX Cloud

### Connect a Catalyst Center

IP Address or FQDN \*

City \*

Select option



Username \*

Password \*

### Schedule inventory collection

Frequency

Select Time

Frequ... ▾

12:00 ▾

AM ▾

WEDT

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

Connect

Frequência

6. Insira os seguintes detalhes:

- Endereço IP virtual ou FQDN (isto é, endereço IP do Catalyst Center)
- Cidade (ou seja, a localização do Catalyst Center)
- Nome de usuário
- Senha
- Frequência e Selecionar hora para indicar a frequência com que o agente CX deve executar verificações de rede nas seções Agendar coleta de inventário

Note: Marque a caixa de seleção Run the first collection now para executar a coleta agora.

7. Clique em Conectar. Uma confirmação é exibida com o endereço IP do Catalyst Center.

## Adição do SolarWinds® como uma fonte de dados

Note: Se for necessário adicionar a fonte de dados SolarWinds®, entre em contato com o Suporte da Cisco para obter assistência.

Agora, os clientes do BCS/LCS podem usar o recurso CX Agent para integrar externamente o SolarWinds®, fornecendo maior transparência, melhor capacidade de gerenciamento e uma experiência de usuário aprimorada por meio de maior automação. O agente CX coleta dados de inventário e outros dados necessários para gerar vários relatórios que são consistentes em termos de formato, integridade de dados e precisão de dados para os relatórios atuais gerados pelo agente CX do coletor de insights operacionais suporta integração com o SolarWinds® permitindo que um cliente do BCS/LCS substitua o OIC pelo agente CX para coletar dados do Solarwinds®. Esse recurso, incluindo a fonte de dados Solarwinds®, está disponível exclusivamente para clientes BCS/LCS.

O agente CX deve ser configurado no encaminhamento BCS antes da primeira coleta; caso contrário, os arquivos permanecerão não processados. Consulte a seção [Configuração do CX Agent para BCS ou LCS](#) para obter mais informações sobre a configuração do Encaminhamento BCS.

Notas:

- Várias coleções da mesma instância do SolarWinds® substituem arquivos anteriores (carregamentos posteriores têm precedência)
- Há suporte para várias fontes, mas cada instância da SolarWinds® deve ter um IP e uma ID de aplicativo exclusivos

## Adição de Outros Ativos como Origens de Dados

A coleta de telemetria foi estendida para dispositivos não gerenciados pelo Catalyst Center, permitindo que os usuários visualizem e interajam com insights e análises derivados de telemetria para uma gama mais ampla de dispositivos. Após a configuração inicial do CX Agent, os usuários têm a opção de configurar o CX Agent para se conectar a mais 20 Centros Catalyst na infraestrutura monitorada pelo CX Cloud.

Os usuários podem identificar os dispositivos a serem incorporados na nuvem CX identificando exclusivamente esses dispositivos usando um arquivo de seed ou especificando um intervalo de IP, que deve ser examinado pelo agente CX. Ambas as abordagens dependem do Simple Network Management Protocol (SNMP) para fins de descoberta e do Secure Shell (SSH) para conectividade. Eles devem ser configurados corretamente para permitir a coleta de telemetria bem-sucedida.

Para adicionar outros ativos como origens de dados, use qualquer uma das seguintes opções:

- Carregar um arquivo de seed usando um modelo de arquivo de seed
- Fornecer um intervalo de endereços IP

## Protocolos de descoberta

A detecção direta de dispositivos baseada em arquivos de seed e a detecção baseada em intervalo de IPs dependem do SNMP como o protocolo de detecção. Existem versões diferentes de SNMP, mas o agente CX oferece suporte a SNMPv2c e SNMPv3 e uma ou ambas as versões podem ser configuradas. As mesmas informações, descritas abaixo em detalhes completos, devem ser fornecidas pelo usuário para concluir a configuração e permitir a conectividade entre o dispositivo gerenciado por SNMP e o gerenciador de serviços SNMP.

O SNMPv2c e o SNMPv3 diferem em termos de segurança e modelo de configuração remota. O SNMPv3 usa um sistema avançado de segurança criptográfica que suporta criptografia SHA para autenticar mensagens e garantir sua privacidade. Recomenda-se que o SNMPv3 seja usado em todas as redes públicas e na Internet para proteger contra riscos e ameaças à segurança. Na Nuvem CX, é preferível que o SNMPv3 seja configurado e não o SNMPv2c, exceto para dispositivos herdados mais antigos que não têm suporte interno para o SNMPv3. Se ambas as versões do SNMP forem configuradas pelo usuário, o Agente CX tentará, por padrão, se comunicar com cada dispositivo respectivo usando o SNMPv3 e reverte para o SNMPv2c se a comunicação não puder ser negociada com êxito.

## Protocolos de conectividade

Como parte da configuração da conectividade direta do dispositivo, os usuários devem especificar detalhes do protocolo de conectividade do dispositivo: SSH (ou, alternativamente, Telnet). O SSHv2 deve ser usado, exceto nos casos de ativos legados individuais que não têm o suporte interno apropriado. Esteja ciente de que o protocolo SSHv1 contém vulnerabilidades fundamentais. Sem segurança adicional, os dados de telemetria e os ativos subjacentes podem ser comprometidos devido a essas vulnerabilidades ao depender do SSHv1. O Telnet também é inseguro. As informações de credencial (por exemplo, nomes de usuário e senhas) enviadas através do telnet não são criptografadas e, portanto, vulneráveis a comprometimento, sem segurança adicional.

## Limitações de Processamento de Telemetria para Dispositivos

A seguir, há limitações ao processar dados de telemetria para dispositivos:

- Alguns dispositivos podem ser exibidos como alcançáveis no Resumo da coleta, mas não são visíveis na página Ativos de nuvem do CX.
- Se um dispositivo do arquivo de seed ou das coletas de intervalo de IPs também fizer parte do inventário do Catalyst Center, o dispositivo será relatado apenas uma vez para a entrada do Catalyst Center. Os respectivos dispositivos dentro do arquivo de seed ou da entrada de intervalo de IPs são ignorados para evitar duplicação.
- Os telefones IP da Cisco não são suportados no CX Cloud para coleta de dados pelo CX Agent. Como resultado, os telefones IP da Cisco não são exibidos na lista de ativos.

## Adicionando outros ativos usando um arquivo de propagação

Um arquivo de propagação é um arquivo .csv em que cada linha representa um registro de dados do sistema. Em um arquivo de seed, cada registro de arquivo de seed corresponde a um dispositivo exclusivo do qual a telemetria deve ser coletada pelo CX Agent. Todas as mensagens de erro ou de informações para cada entrada de dispositivo do arquivo de seed que está sendo importado são capturadas como parte dos detalhes do log de jobs. Todos os dispositivos em um arquivo de seed são considerados dispositivos gerenciados, mesmo que os dispositivos estejam inalcançáveis no momento da configuração inicial. Caso um novo arquivo de seed esteja sendo carregado para substituir um anterior, a data do último upload é exibida no CX Cloud.

O agente CX tentará se conectar aos dispositivos, mas talvez não consiga processar cada um para ser exibido nas páginas Ativos nos casos em que não seja capaz de determinar os PIDs ou os Números de série.

Qualquer linha no arquivo de seed que comece com um ponto-e-vírgula será ignorada. A linha de cabeçalho no arquivo de seed começa com um ponto-e-vírgula e pode ser mantida como está (opção recomendada) ou excluída durante a criação do arquivo de seed do cliente.

Os usuários podem carregar um arquivo semente do Common Services Platform Collector (CSPC) da mesma forma que um arquivo semente de nuvem CX padrão, e qualquer reformatação necessária é gerenciada na nuvem CX.

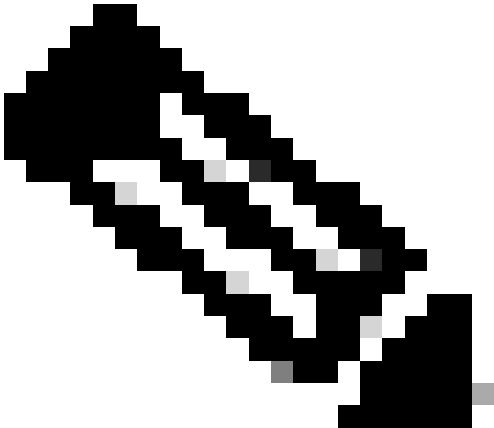
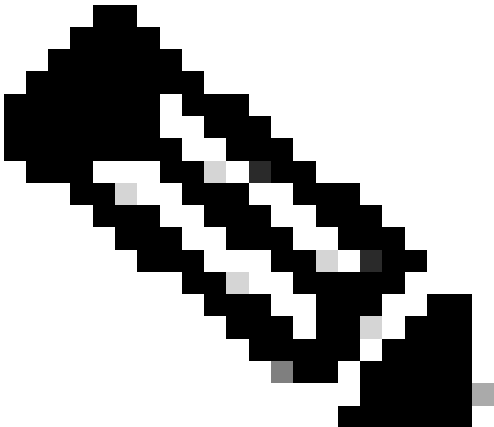
Para o CX Agent v3.1 e posterior, os clientes podem fazer upload dos arquivos semente no formato CSPC ou CX; somente o arquivo semente do formato CX é suportado nas versões anteriores do CX Agent.

É importante que o formato do arquivo semente de exemplo, incluindo os cabeçalhos das colunas, não seja alterado de forma alguma.

A tabela a seguir identifica todas as colunas de arquivo de seed necessárias e os dados que devem ser incluídos em cada coluna.

| Coluna do arquivo de propagação | Cabeçalho/Identificador de Coluna | Finalidade da Coluna                   |
|---------------------------------|-----------------------------------|----------------------------------------|
| R                               | Endereço IP ou nome de            | Forneça um endereço IP ou nome de host |

| Coluna do arquivo de propagação | Cabeçalho/Identificador de Coluna                                   | Finalidade da Coluna                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | host                                                                | válido e exclusivo do dispositivo.                                                                                                                                                                                                   |
| B                               | versão do protocolo SNMP                                            | O protocolo SNMP é exigido pelo CX Agent e é usado para a descoberta de dispositivos na rede do cliente. Os valores podem ser snmpv2c ou snmpv3, mas o snmpv3 é recomendado devido a considerações de segurança.                     |
| C                               | snmpRo: Obrigatório se col#=3 for selecionado como 'snmpv2c'        | Se a variante herdada de SNMPv2 for selecionada para um dispositivo específico, as credenciais snmpRO (somente leitura) para a coleção SNMP do dispositivo devem ser especificadas. Caso contrário, a entrada pode ficar em branco.  |
| D                               | snmpv3UserName: Obrigatório se col#=3 for selecionado como 'snmpv3' | Se o SNMPv3 for selecionado para se comunicar com um dispositivo específico, o respectivo nome de usuário de login deverá ser fornecido.                                                                                             |
| E                               | snmpv3AuthAlgorithm: podem ser MD5 ou SHA                           | O protocolo SNMPv3 permite a autenticação através do Message Digest (MD5) ou Secure Hash Algorithm (SHA). Se o dispositivo estiver configurado com autenticação segura, o respectivo Algoritmo de autenticação deverá ser fornecido. |

| Coluna do arquivo de propagação | Cabeçalho/Identificador de Coluna                    | Finalidade da Coluna                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                                      |  <p>Note: MD5 é considerado inseguro, e SHA pode ser usado em todos os dispositivos que o suportam.</p>                                                                                     |
| F                               | snmpv3AuthPassword :<br>senha                        | Se um algoritmo de criptografia MD5 ou SHA estiver configurado no dispositivo, a senha de autenticação relevante deverá ser fornecida para acesso ao dispositivo.                                                                                                             |
| G                               | snmpv3PrivAlgorithm: os valores podem ser DES , 3DES | <p>Se o dispositivo estiver configurado com o algoritmo de privacidade SNMPv3 (esse algoritmo é usado para criptografar a resposta), o respectivo algoritmo precisará ser fornecido.</p>  |

| Coluna do arquivo de propagação | Cabeçalho/Identificador de Coluna                                                                                                      | Finalidade da Coluna                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                                                                                                                        | <p>Note: As chaves de 56 bits usadas pelo Data Encryption Standard (DES) são consideradas muito curtas para fornecer segurança criptográfica, e esse Triple Data Encryption Standard (3DES) pode ser usado em todos os dispositivos que o suportam.</p>                                                                                                                                                                                  |
| H                               | snmpv3PrivPassword : senha                                                                                                             | Se o algoritmo de privacidade SNMPv3 estiver configurado no dispositivo, sua respectiva senha de privacidade deverá ser fornecida para a conexão do dispositivo.                                                                                                                                                                                                                                                                         |
| I                               | snmpv3EngineID: EngineID, ID exclusivo que representa o dispositivo, especifique o Engine ID se configurado manualmente no dispositivo | O EngineID SNMPv3 é um ID exclusivo que representa cada dispositivo. Esse ID do mecanismo é enviado como referência durante a coleta dos conjuntos de dados SNMP pelo agente CX. Se o cliente configurar o EngineID manualmente, o respectivo EngineID precisará ser fornecido.                                                                                                                                                          |
| J                               | cliProtocol: podem ser 'telnet', 'sshv1', 'sshv2'. Se vazio, pode ser definido como 'sshv2' por padrão                                 | A Interface de linha de comando (CLI) tem a intenção de interagir diretamente com o dispositivo. O agente CX usa esse protocolo para a coleta de CLI de um dispositivo específico. Esses dados de coleta de CLI são usados para ativos e outros relatórios de insights na nuvem CX. SSHv2 é recomendado; na ausência de outras medidas de segurança de rede, os protocolos SSHv1 e Telnet não fornecem segurança de transporte adequada. |
| K                               | cliPort: Número de porta do protocolo CLI                                                                                              | Se algum protocolo CLI for selecionado, seu respectivo número de porta precisará ser fornecido. Por exemplo, 22 para SSH e 23 para telnet.                                                                                                                                                                                                                                                                                               |

| Coluna do arquivo de propagação | Cabeçalho/Identificador de Coluna                                                                                                                            | Finalidade da Coluna                                                                                                                                                     |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I                               | cliUser: Nome de usuário CLI (pode ser fornecido nome de usuário/senha CLI ou AMBOS, MAS as duas colunas (col#=12 e col#=13) não podem estar vazias.)        | O nome de usuário CLI respectivo do dispositivo precisa ser fornecido. Isso é usado pelo CX Cloud Agent no momento da conexão com o dispositivo durante a coleta da CLI. |
| M                               | cliPassword : Senha de usuário CLI (é possível fornecer nome de usuário/senha CLI ou AMBOS, MAS as duas colunas (col#=12 e col#=13) não podem estar vazias.) | A respectiva senha CLI do dispositivo precisa ser fornecida. Isso é usado pelo CX Agent no momento da conexão com o dispositivo durante a coleta da CLI.                 |
| N                               | cliEnableUser                                                                                                                                                | Se enable estiver configurado no dispositivo, o valor enableUsername do dispositivo precisará ser fornecido.                                                             |
| O                               | cliEnablePassword                                                                                                                                            | Se enable estiver configurado no dispositivo, o valor enablePassword do dispositivo precisará ser fornecido.                                                             |
| P                               | Suporte futuro (sem necessidade de entradas)                                                                                                                 | Reservado para uso futuro                                                                                                                                                |
| P                               | Suporte futuro (sem necessidade de entradas)                                                                                                                 | Reservado para uso futuro                                                                                                                                                |
| R                               | Suporte futuro (sem necessidade de entradas)                                                                                                                 | Reservado para uso futuro                                                                                                                                                |
| S                               | Suporte futuro (sem necessidade de entradas)                                                                                                                 | Reservado para uso futuro                                                                                                                                                |

Adicionando outros recursos usando um novo arquivo de seed

Para adicionar outros ativos usando um novo arquivo de seed:

1. Clique em Adicionar fonte de dados na janela Centro de administração > Fontes de dados.

## Add Data Source

**Catalyst Center**  
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)

Add Data Source

**Cisco Catalyst SD-WAN Manager**  
Supports the Success Track for WAN

Add Data Source

**Common Services Platform Collector (CSPC)**  
Supports assets managed by CSPC

Add Data Source

**Contracts**  
Supports assets associated with a contract

Add Data Source

**CX Cloud Agent**  
Add CX Cloud Agents to your network to support a variety of Success Tracks.

Add Data Source

**Intersight**  
Supports the Data Center Compute and Data Center Networking Success Tracks

Add Data Source

**Meraki dashboard**  
Supports Meraki

Add Data Source

**Other Assets by IP Ranges**  
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

Add Data Source

**Other Assets by Seed File**  
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

Add Data Source

**Webex**  
Supports the Success Track for Collaboration

Add Data Source

Adicionar Fonte de Dados

2. Clique em Add Data Source na opção Other Assets by Seed File.

Which CX Cloud Agent Do You Want to Connect to?

Select option



Cancel

Continue



Selecionar Agente CX

3. Selecione o CX Agent na lista suspensa Qual CX Cloud Agent Você Deseja Conectar.

Which CX Cloud Agent Do You Want to Connect to?

OIC\_Team\_test\_CXCAGENT\_IP\_104



Cancel

Continue

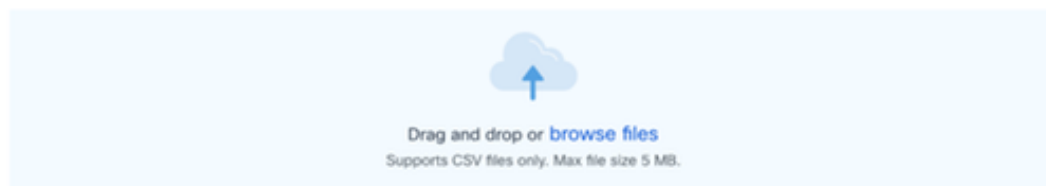


Continuar

4. Clique em Continuar. A página Upload Your Seed File é exibida.

### Upload your seed file

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



### Schedule inventory collection

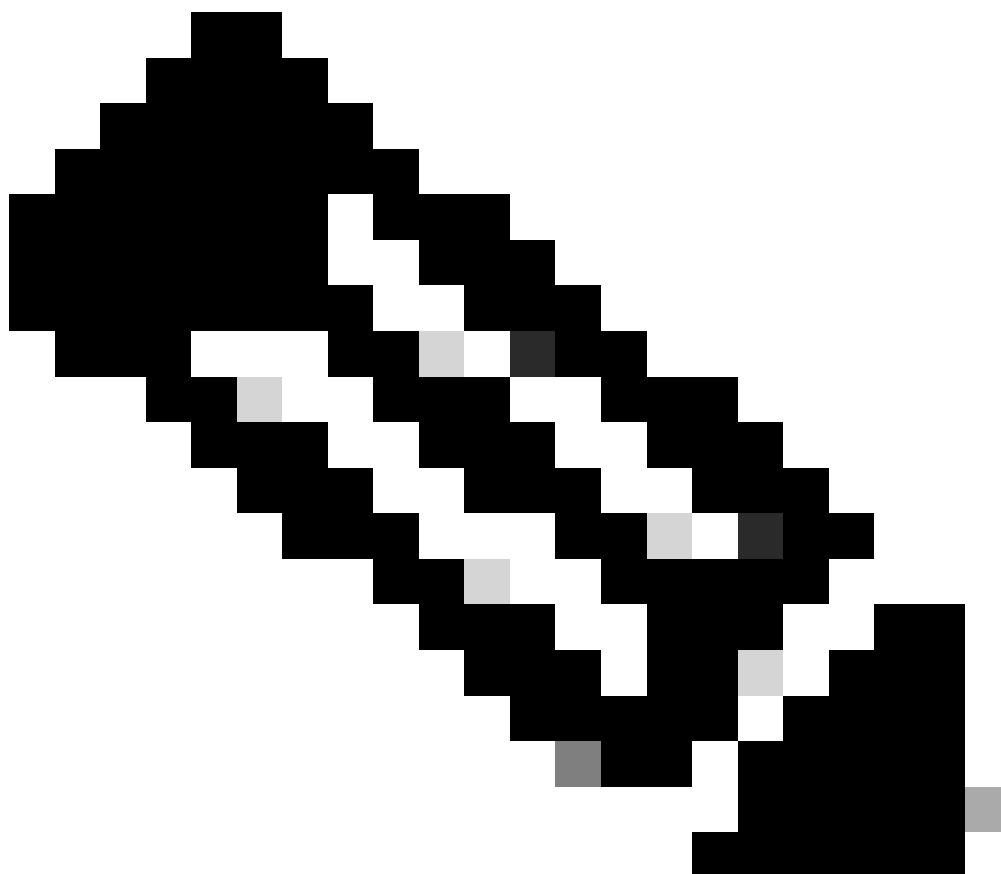
| Frequency   | Select time | Time Zone |                         |
|-------------|-------------|-----------|-------------------------|
| Frequency ▾ | 12:00 ▾     | AM ▾      | Europe/Amsterdam (... ▾ |

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

Connect

Carregar seu arquivo de seed

5. Clique no modelo de arquivo semente com hiperlink para fazer download do modelo.
6. Insira ou importe dados manualmente no arquivo. Depois de concluir, salve o modelo como um arquivo .csv para importar o arquivo para o CX Agent.
7. Arraste e solte ou clique em procurar arquivos para carregar o arquivo .csv.
8. Conclua a seção Agendar coleta de inventário.



Note: Antes de concluir a configuração inicial do CX Cloud, o CX Cloud Agent deve realizar a primeira coleta de telemetria processando o arquivo de seed e estabelecendo conexão com todos os dispositivos identificados. A coleta pode ser iniciada sob demanda ou executada de acordo com uma programação definida aqui. Os usuários podem executar a primeira conexão de telemetria marcando a caixa de seleção Executar a primeira coleta agora. Dependendo do número de entradas especificadas no arquivo de seed e de outros fatores, este processo pode levar um tempo considerável.

- 
9. Clique em Conectar. A janela Fontes de dados é aberta, exibindo uma mensagem de confirmação.

## Adicionando outros recursos usando um arquivo de propagação modificado

Para adicionar, modificar ou excluir dispositivos usando o arquivo de propagação atual:

1. Abra o arquivo de seed criado anteriormente, faça as alterações necessárias e salve o arquivo.



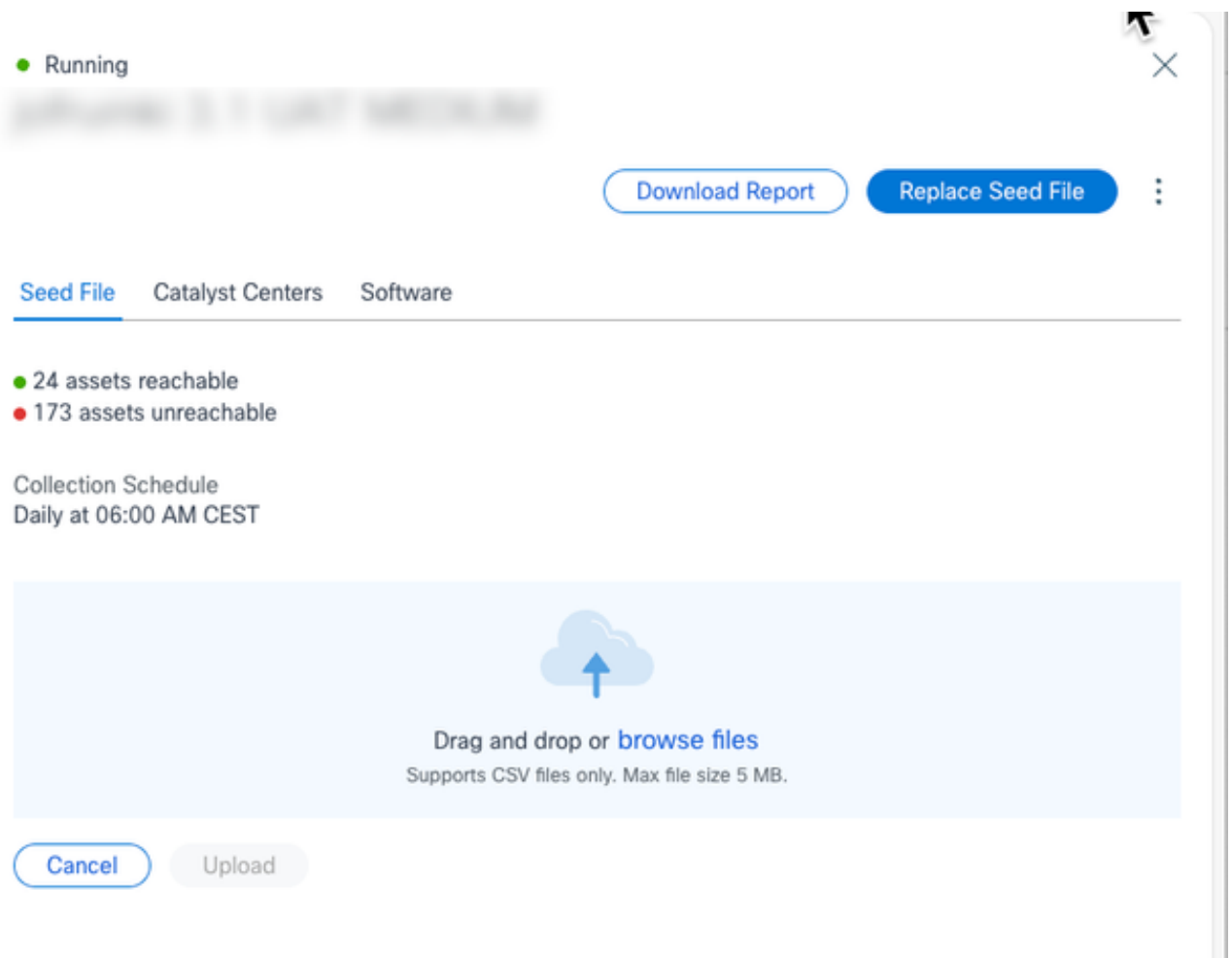
Note: Para adicionar ativos ao arquivo de seed, anexe esses ativos ao arquivo de seed criado anteriormente e recarregue o arquivo. Isso é necessário já que o upload de um novo arquivo de seed substitui o arquivo de seed atual. Somente o último arquivo de propagação carregado é usado para descoberta e coleta.

2. Na página Fontes de dados, clique na fonte de dados do agente CX que requer um arquivo semente atualizado. A janela de detalhes do CX Cloud Agent é aberta.

The screenshot shows the Cisco CX Cloud interface. The main section is titled 'Data Sources' and shows a list of 16 data sources. The table has columns for 'Name', 'Type', and 'Data Last Updated'. The right sidebar shows the status of the CX Cloud Agent, including a 'Running' status, a 'Download Report' button, and a 'Replace Seed File' button. Below this, it indicates '24 assets reachable' and '173 assets unreachable'.

Arquivo semente

3. Clique em Substituir arquivo semente.



Substituir arquivo de propagação

4. Arraste e solte ou clique em procurar arquivos para carregar o arquivo semente modificado.
5. Clique em Fazer upload.

## Credenciais padrão para o arquivo de propagação

O agente CX fornece credenciais padrão que os clientes podem configurar localmente no agente, eliminando a necessidade de incluir senhas confidenciais diretamente no arquivo de propagação. Isso aumenta a segurança, reduzindo a exposição de informações confidenciais e resolvendo uma das principais preocupações do cliente.

## Adicionando outros ativos usando intervalos de IP

Os intervalos de IP permitem que os usuários identifiquem ativos de hardware e, subsequentemente, coletem telemetria desses dispositivos com base em endereços IP. Os dispositivos para coleta de telemetria podem ser identificados exclusivamente especificando-se um único intervalo de IP de nível de rede, que pode ser verificado pelo agente CX usando o protocolo SNMP. Se o intervalo de IPs for escolhido para identificar um dispositivo conectado diretamente, os endereços IP referenciados poderão ser o mais restritivos possível, permitindo cobertura para todos os ativos necessários.

- IPs específicos podem ser fornecidos ou curingas podem ser usados para substituir octetos

de um IP para criar um intervalo.

- Se um endereço IP específico não estiver incluído no intervalo de IPs identificado durante a configuração, o CX Agent não tentará se comunicar com um dispositivo que tenha esse endereço IP, nem coletará telemetria desse dispositivo.
- Inserir \*.\*.\* permite que o Agente CX use a credencial fornecida pelo usuário com qualquer IP. Por exemplo: 172.16.\*.\* permite que as credenciais sejam usadas para todos os dispositivos na sub-rede 172.16.0.0/16.
- Se houver qualquer alteração na rede ou na base instalada (IB), o intervalo de IPs poderá ser modificado. Consulte a seção [Edição de Intervalos IP](#)

O agente CX tentará se conectar aos dispositivos, mas talvez não consiga processar cada um para ser mostrado na exibição Assets nos casos em que não seja capaz de determinar os PIDs ou os números de série.



#### Notas:

Clicar em Editar intervalo de endereços IP inicia a descoberta de dispositivos sob demanda. Quando qualquer dispositivo novo é adicionado ou excluído (dentro ou fora) a um intervalo de IPs especificado, o cliente deve sempre clicar em Editar intervalo de endereços IP (consulte a seção [Edição de intervalos de IP](#)) e concluir as etapas necessárias para iniciar a descoberta de dispositivos sob demanda para incluir qualquer dispositivo recém-adicionado ao inventário de coleta do CX Agent.

---

Adicionar dispositivos usando um intervalo de IPs exige que os usuários especifiquem todas as credenciais aplicáveis por meio da interface de usuário da configuração. Os campos visíveis variam de acordo com os protocolos selecionados nas janelas anteriores. Se várias seleções forem feitas para o mesmo protocolo, por exemplo, selecionar SNMPv2c e SNMPv3 ou selecionar SSHv2 e SSHv1, o agente CX negocia automaticamente a seleção do protocolo com base nos recursos do dispositivo individual.

Ao conectar dispositivos usando endereços IP, o cliente deve garantir que todos os protocolos relevantes no intervalo IP, juntamente com as versões SSH e as credenciais Telnet, sejam válidos ou que as conexões falhem.

## Adicionando outros ativos por intervalos de IP

Para adicionar dispositivos usando o intervalo IP:

1. Selecione o ícone Centro de Administração. A janela Fontes de Dados será aberta.
2. Clique em Adicionar fonte de dados na janela Centro de administração > Fontes de dados.

## Add Data Source

Search data sources



### Catalyst Center

Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)

Add Data Source



### Cisco Catalyst SD-WAN Manager

Supports the Success Track for WAN

Add Data Source



### Common Services Platform Collector (CSPC)

Supports assets managed by CSPC

Add Data Source



### Contracts

Supports assets associated with a contract

Add Data Source



### CX Cloud Agent

Add CX Cloud Agents to your network to support a variety of Success Tracks.

Add Data Source



### Intersight

Supports the Data Center Compute and Data Center Networking Success Tracks

Add Data Source



### Meraki dashboard

Supports Meraki

Add Data Source



### Other Assets by IP Ranges

Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

Add Data Source



### Other Assets by Seed File

Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

Add Data Source



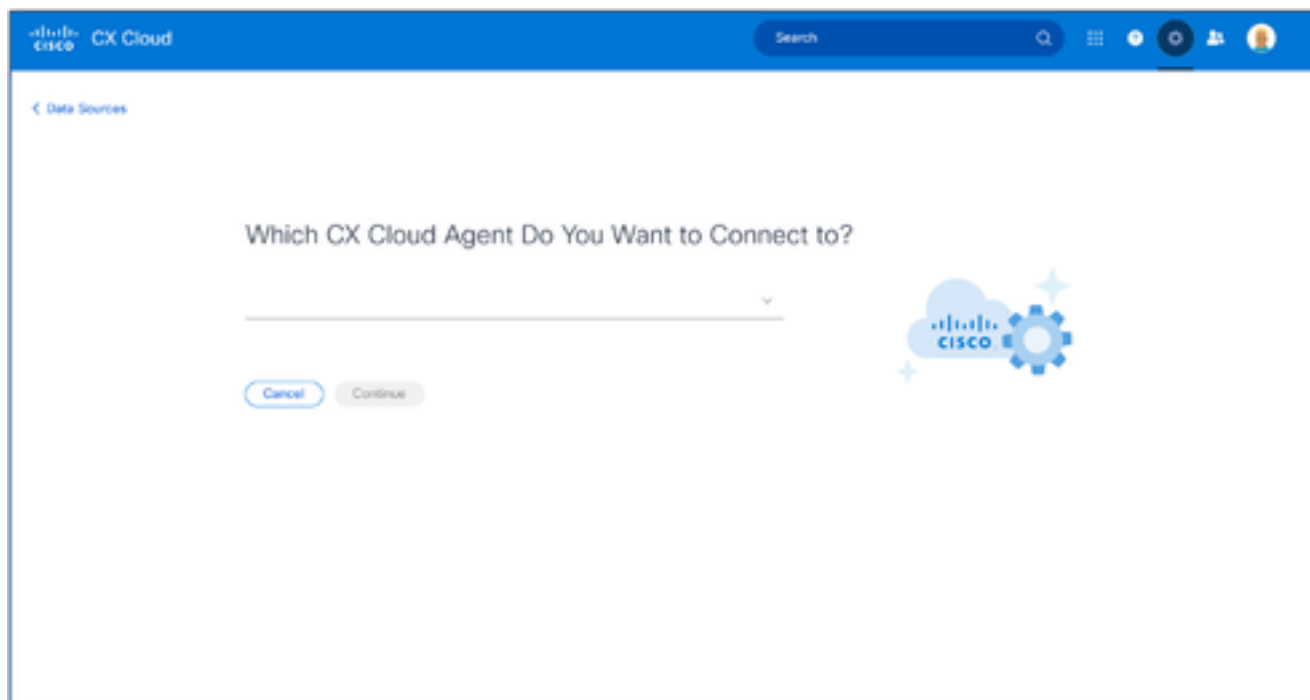
### Webex

Supports the Success Track for Collaboration

Add Data Source

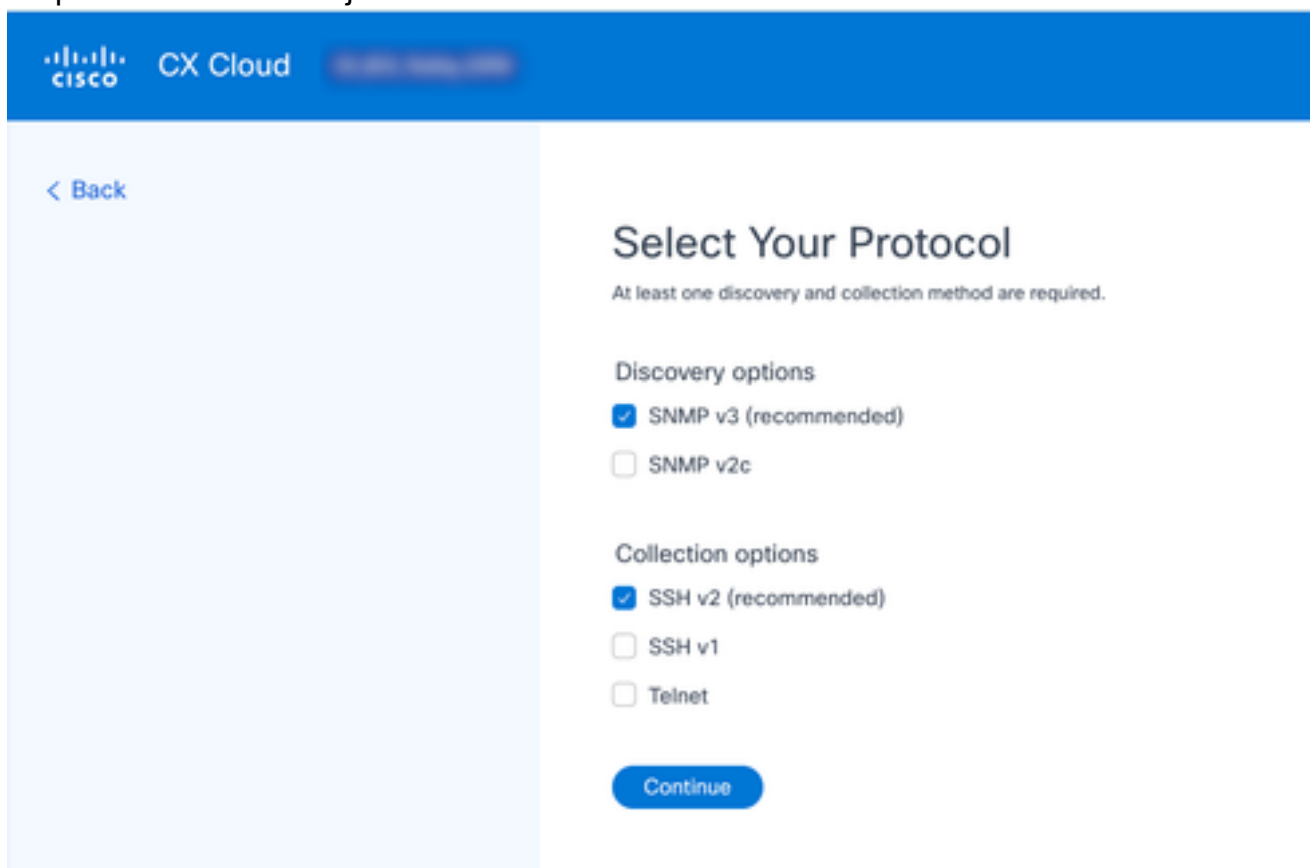
Adicionar Fonte de Dados

3. Clique em Add Data Source na opção Other Assets by IP Ranges.



Selecionar CX Cloud Agent

4. Selecione o CX Agent na lista suspensa Qual CX Cloud Agent Você Deseja Conectar.
5. Clique em Continuar. A janela Select Your Protocol é aberta.



Selecione seu protocolo

6. Marque as caixas de seleção aplicáveis para as opções Discovery e Collection.
7. Clique em Continuar.

## Provide Discovery Details

[Edit the protocols](#)

Starting IP Address

Ending IP Address

### SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Select



Authorization Password

Privacy Algorithm

Select



Privacy Password

### SSHv2 credentials

Username

Password

[Enable mode \(optional\)](#)

## Schedule Inventory Collection

Frequency

Select Time

Freq...

12:00

AM

WEDT

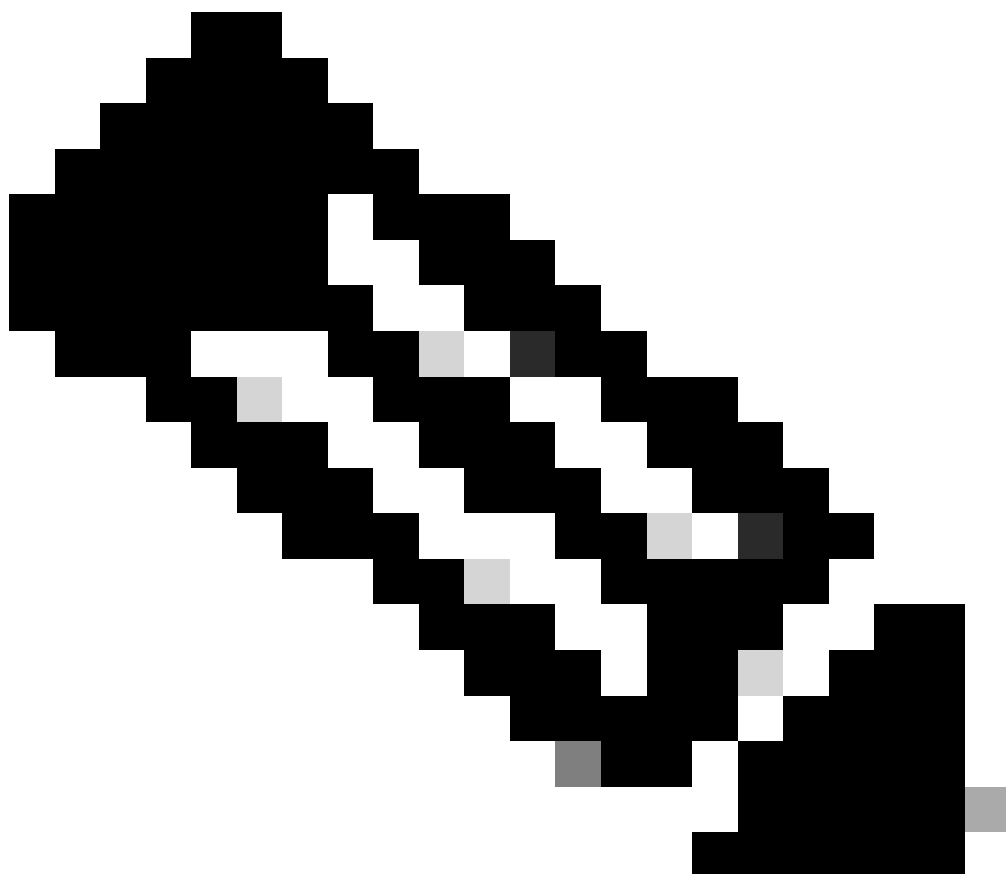
☒ Run the first collection now (this may take up to 75 minutes)

Add Another IP Range

Complete Setup

Detalhes da descoberta

8. Insira os detalhes necessários nas seções Fornecer detalhes da descoberta e Agendar coleta de inventário.



Note: Para adicionar outro intervalo de IPs para o CX Agent selecionado, clique em Add Another IP Range para voltar à janela Set Your Protocol e repita as etapas desta seção.

- 
9. Clique em Complete Setup. Uma confirmação é exibida após a implantação bem-sucedida.

**Data Sources** Region: United States

Search data sources

4 data sources

| Name             | Type                | Data Last Updated | Status                |
|------------------|---------------------|-------------------|-----------------------|
| CX Cloud Agent 1 | CX Cloud Agent v1.2 | 15 minutes ago    | Running               |
| 99.387.29.01     | Catalyst Center     | 6 hours ago       | Reachable             |
| 475.92.968.3     | Catalyst Center     | 1 month ago       | Reachable             |
| Merski           | Merski - L1         | 23 hours ago      | Last update succeeded |

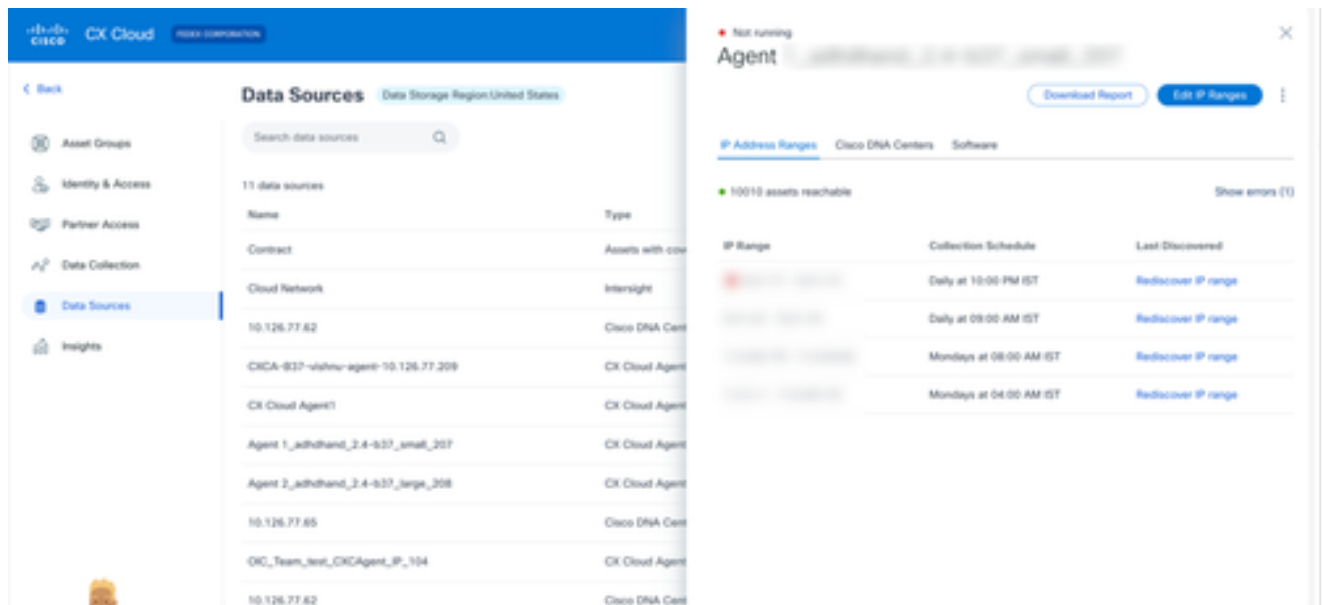
Message: Your IP ranges are being processed. It may take up to an hour to complete.

Mensagem de confirmação

## Editando Intervalos IP

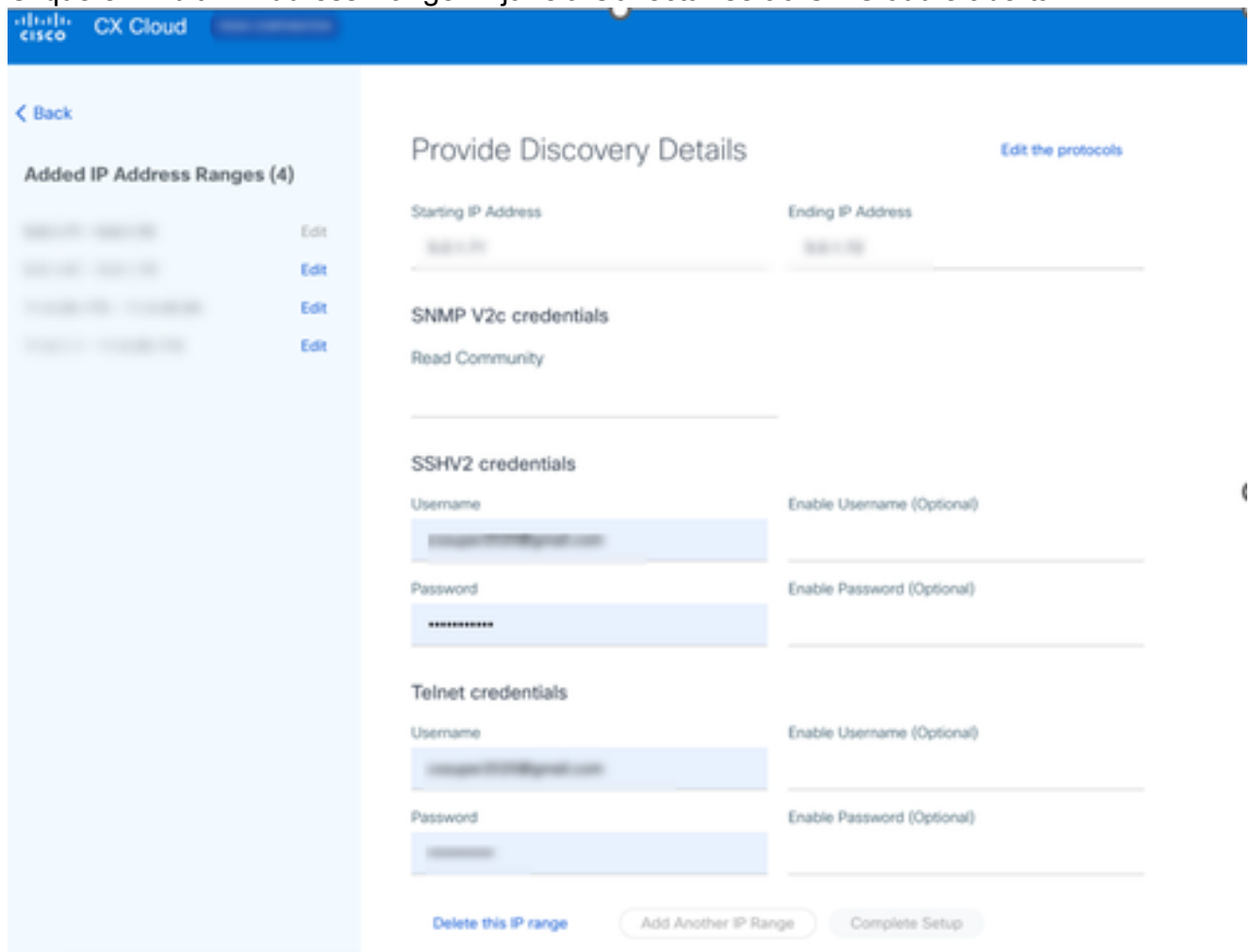
Para editar um intervalo IP:

1. Navegue até a janela Origens de Dados.
2. Clique no agente CX que requer a edição do intervalo IP em Fontes de dados. A janela de detalhes é aberta.



Origem dos dados

3. Clique em Edit IP Address Range. A janela Conectar-se ao CX Cloud é aberta.



4. Clique em Edit the protocols. A janela Select Your Protocol é aberta.

[< Back](#)

**Added IP Address Ranges (4)**

Edit

Edit

Edit

Edit

## Select Your Protocol

At least one discovery and collection method are required.

**Discovery options**

☐ SNMP v3 (recommended)

☒ SNMP v2c

**Collection options**

☒ SSH v2 (recommended)

☐ SSH v1

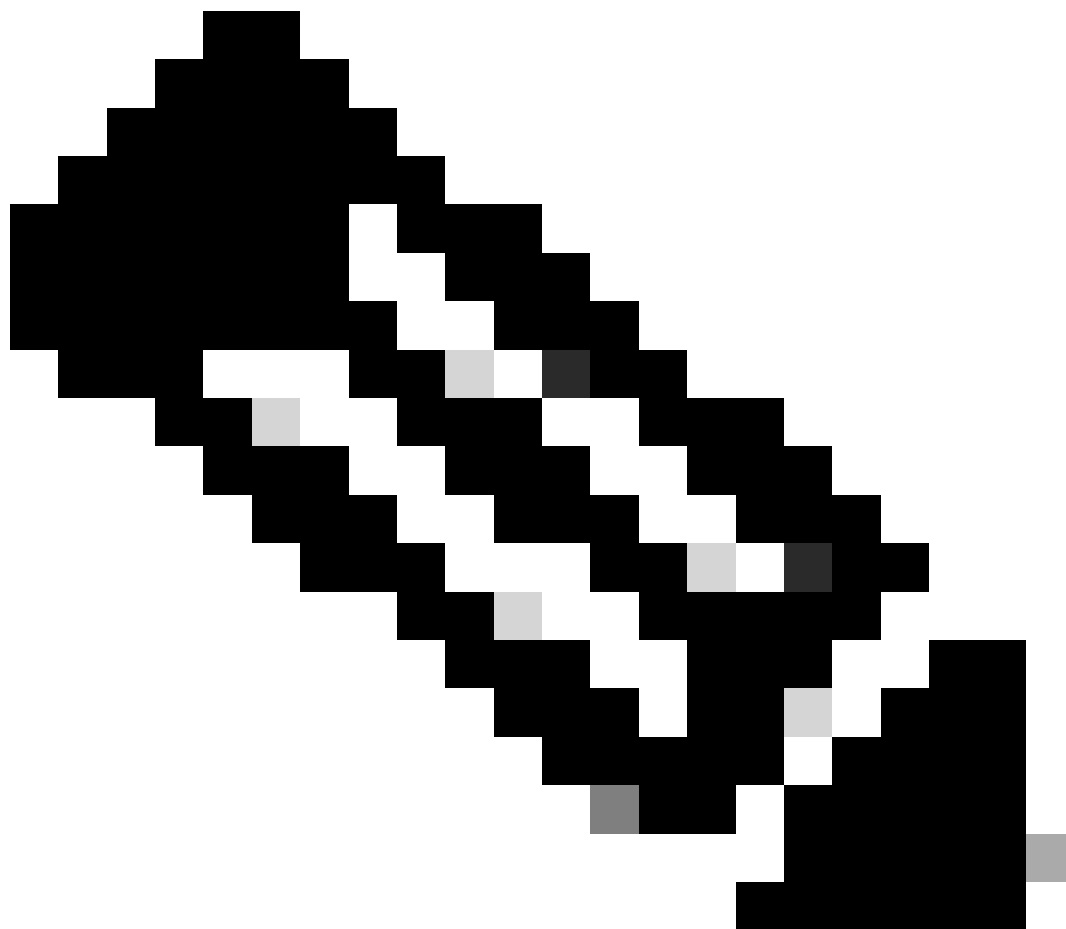
☒ Telnet

Continue

Selecione seu protocolo

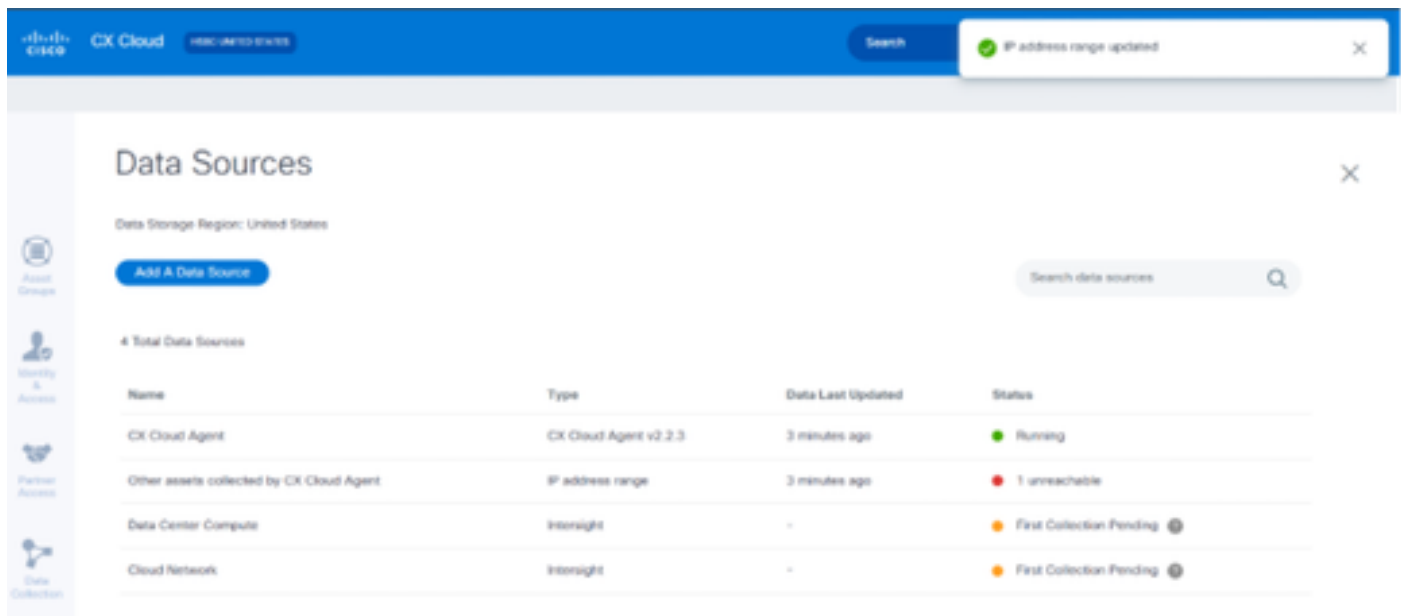
5. Marque as caixas de seleção apropriadas para escolher os protocolos aplicáveis e clique em Continuar para voltar à janela Fornecer detalhes da descoberta.





Note: Esta mensagem de confirmação não verifica se os dispositivos dentro do intervalo modificado estão acessíveis ou se suas credenciais são aceitas. Essa confirmação ocorre quando o cliente inicia o processo de descoberta.

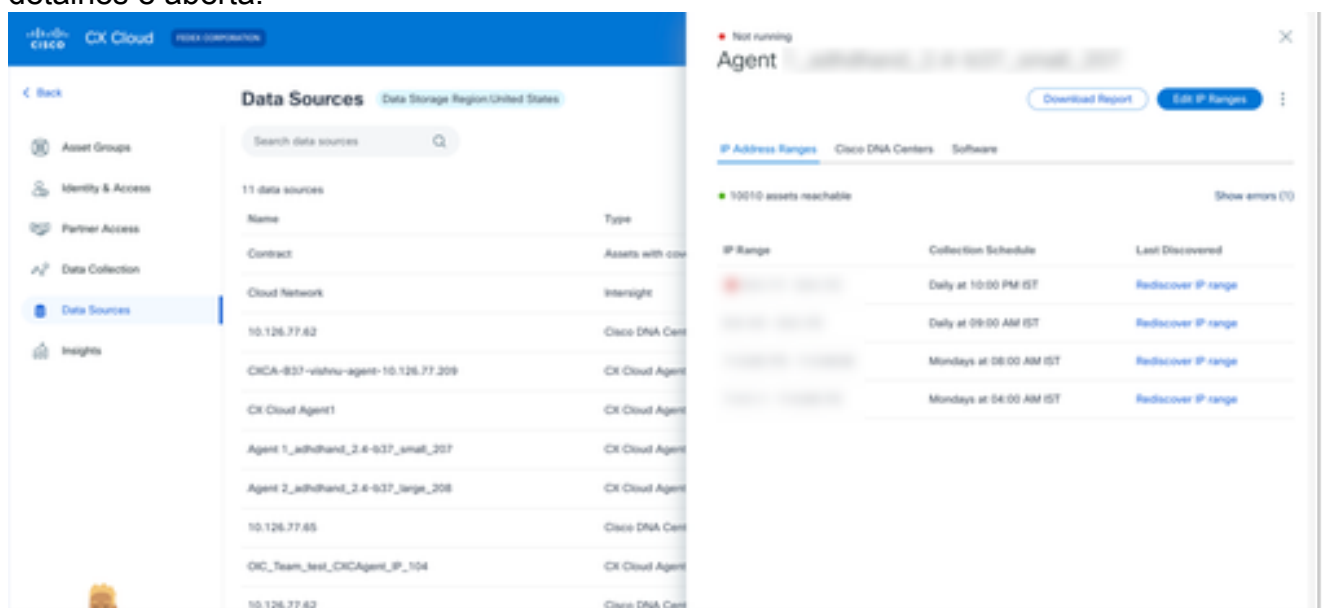
---



## Excluindo intervalo de IPs

Para excluir um intervalo IP:

1. Navegue até a janela Origens de Dados.
2. Selecione o respectivo CX Agent com o intervalo de IP que precisa ser excluído. A janela de detalhes é aberta.



Origem dos dados

3. Clique em Edit IP Ranges. A janela Fornecer Detalhes da Descoberta é aberta.

 CX Cloud FEDEx CORPORATION

[Back](#)

**Added IP Address Ranges (4)**

|             |                      |
|-------------|----------------------|
| 10.0.0.0/24 | <a href="#">Edit</a> |
| 10.0.0.0/24 | <a href="#">Edit</a> |
| 10.0.0.0/24 | <a href="#">Edit</a> |
| 10.0.0.0/24 | <a href="#">Edit</a> |

### Provide Discovery Details

[Edit the protocols](#)

Starting IP Address:  Ending IP Address:

**SNMP V2c credentials**

Read Community:

**SSHv2 credentials**

Username:  Enable Username (Optional):

Password:  Enable Password (Optional):

**Telnet credentials**

Username:  Enable Username (Optional):

Password:  Enable Password (Optional):

[Delete this IP range](#) [Add Another IP Range](#) [Complete Setup](#)

Fornecer Detalhes da Descoberta

4. Clique no link Delete this IP range. A mensagem de confirmação é exibida.



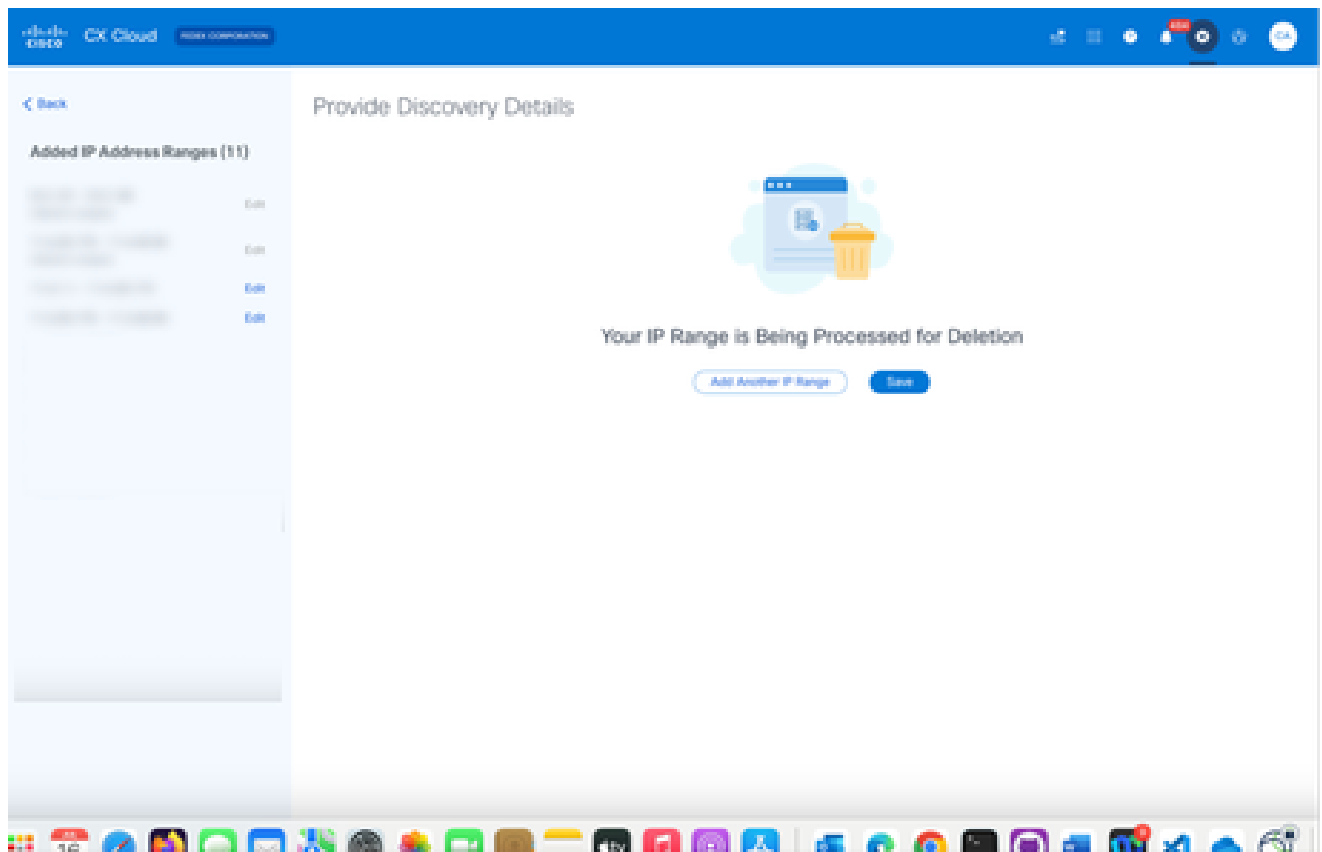
## Delete This IP Range

Any edits you've made won't be saved.

[Continue Editing](#) [Delete](#)

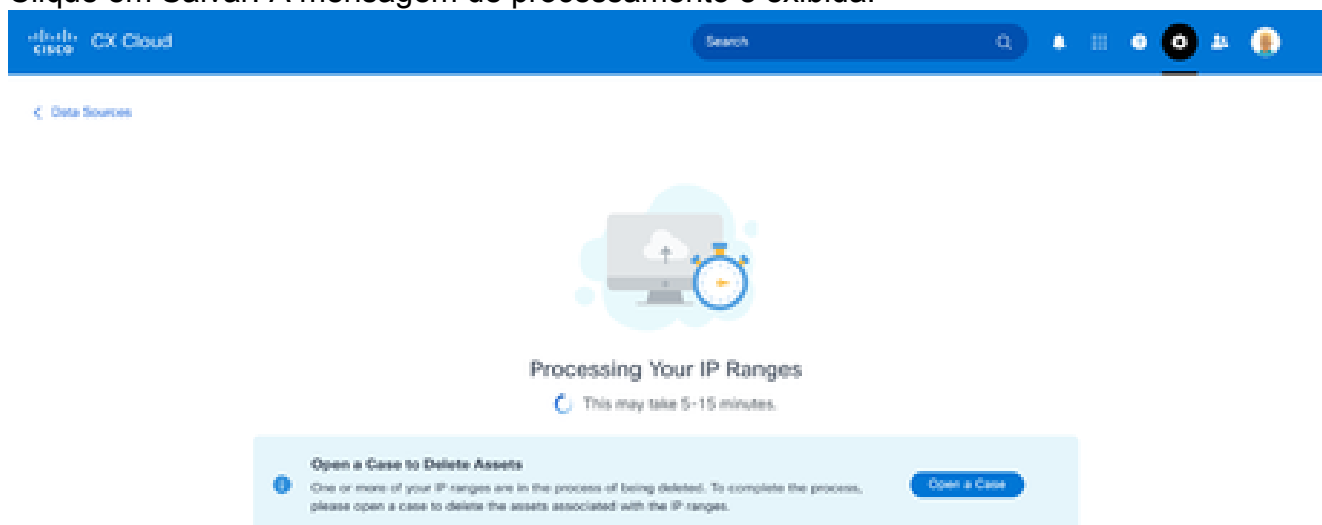
Confirmação - Excluir mensagem

5. Clique em Excluir.



Exclusão de intervalo de IPs

6. Clique em Salvar. A mensagem de processamento é exibida.



7. Clique em Abrir um caso para criar um caso e excluir os ativos associados ao intervalo de IPs. A janela Fontes de dados é aberta, exibindo uma mensagem de confirmação.

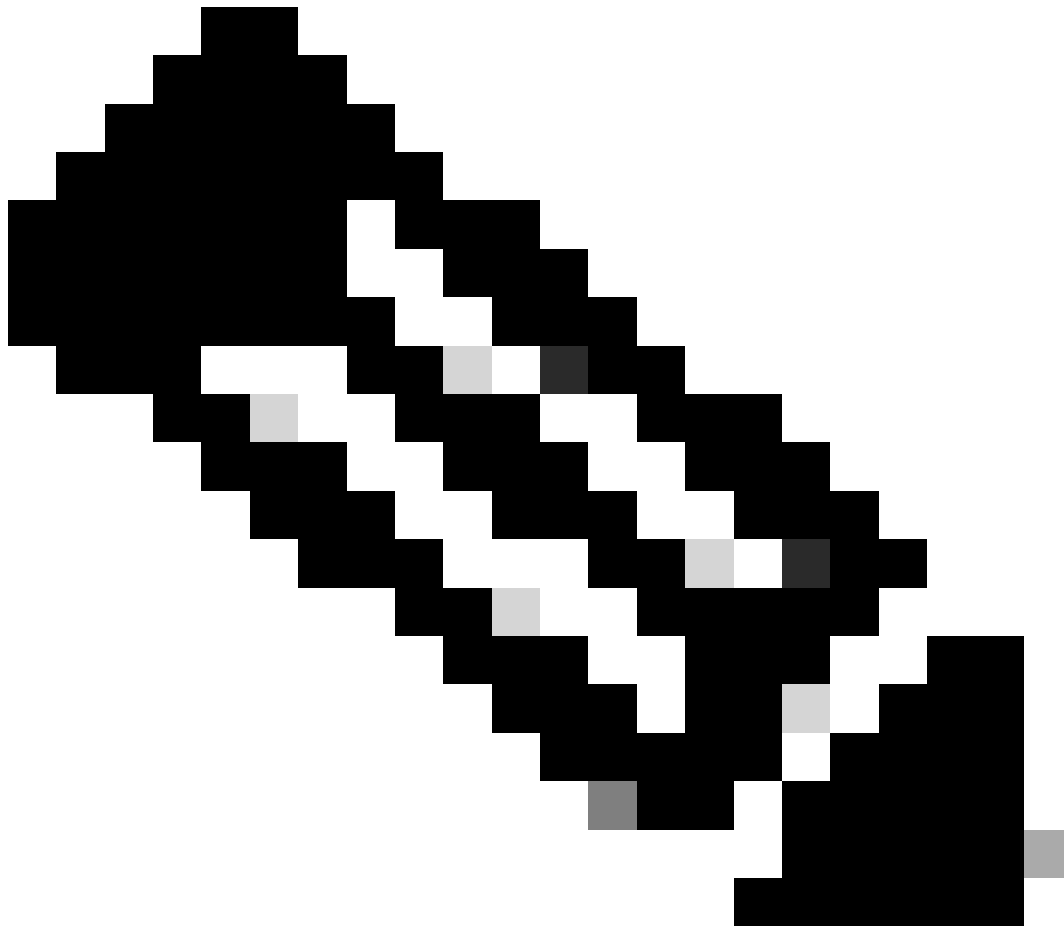
## Sobre os dispositivos descobertos de vários controladores

Se o Catalyst Center e Outros Ativos Coletados pelo Agente CX (Conexão Direta de Dispositivo) estiverem no mesmo Agente CX, é possível que alguns dispositivos possam ser descobertos pelo Cisco Catalyst Center e pela conexão direta de dispositivo ao Agente CX, fazendo com que dados duplicados sejam coletados desses dispositivos. Para evitar a coleta de dados duplicados e ter apenas um controlador para gerenciar os dispositivos, é necessário determinar uma precedência para a qual o agente CX gerencia os dispositivos.

- Se um dispositivo for primeiramente descoberto pelo Cisco Catalyst Center e, em seguida, redescoberto pela conexão direta do dispositivo (usando um arquivo de seed ou um intervalo de IP), o Cisco Catalyst Center terá precedência no controle do dispositivo.
- Se um dispositivo for detectado primeiro pela conexão direta do dispositivo com o CX Agent e depois redetectado pelo Cisco Catalyst Center, o Cisco Catalyst Center terá precedência no controle do dispositivo.

## Programando verificações de diagnóstico

Os clientes podem programar varreduras de diagnóstico sob demanda na nuvem CX para rastreamentos de sucesso qualificados e seus dispositivos cobertos para preencher os bugs de prioridade em conselhos.



Note: A Cisco recomenda programar varreduras de diagnóstico ou iniciar varreduras por solicitação com, pelo menos, 6 a 7 horas de diferença em relação às programações de coleta de inventário, para que elas não se sobreponham. A execução simultânea de várias varreduras de diagnóstico pode retardar o processo de varredura e resultar potencialmente em falhas.

---

Para programar varreduras de diagnóstico:

1. Na página Início, clique no ícone Configurações (equipamento).
2. Na página Fontes de dados, selecione Coleta de dados no painel esquerdo.
3. Clique em Agendar verificação.

## Data Collection

Diagnostic Scans ⓘ

Schedule Scan

< October 2022 >

Sun Mon Tue Wed Thu Fri Sat

1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

23 24 25 26 27 28 29

30 31

No Diagnostic Scans Found

Inventory Collection ⓘ

3 Collections

| Source                                   | Schedule                            |   |
|------------------------------------------|-------------------------------------|---|
| Other assets collected by CX Cloud Agent | Monthly on the 30th at 05:30 PM EDT | ⋮ |
| Switches                                 | Monthly on the 30th at 05:00 PM EDT | ⋮ |
| Wired LAN                                | 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

Programando varreduras

4. Configure um agendamento para esta verificação.

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

Configurar programação de verificação

5. Na lista de dispositivos, selecione todos os dispositivos para a verificação e clique em Adicionar.

## New Scheduled Scan

**Data Sources**  
Other assets collected by CX Cloud Agent X

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

Description (Optional)

| <input type="checkbox"/> | Device | Source IP | IP Address |
|--------------------------|--------|-----------|------------|
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |
| <input type="checkbox"/> |        |           |            |

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

| <input type="checkbox"/>          | Device | Source IP | IP Address |
|-----------------------------------|--------|-----------|------------|
| Devices are part of selected list |        |           |            |

1 2 Next

Agendar verificação

6. Clique em Save Changes quando o agendamento estiver concluído.

As verificações de diagnóstico e os agendamentos de coleta de inventário podem ser editados e excluídos da página Coleta de dados.

Asset Groups

Identity & Access

Partner Access

**Data Collection**

Data Sources

Insights

Automation

## Data Collection

Diagnostic Scans

2 Scans

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

[Schedule Scan](#)

Inventory Collection

8 Collections

| Source | Schedule                           |
|--------|------------------------------------|
|        | Daily at 04:00 AM IST              |
|        | Daily at 12:30 AM IST              |
|        | Monthly on the 9th at 11:30 PM IST |
|        | Daily at 02:00 AM IST              |

October 2022

|     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|
| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|     |     |     |     |     |     | 1   |
| 3   | 4   | 5   | 6   | 7   | 8   |     |
| 9   | 10  | 11  | 12  | 13  | 14  | 15  |
| 16  | 17  | 18  | 19  | 20  | 21  | 22  |
| 23  | 24  | 25  | 26  | 27  | 28  | 29  |
| 30  | 31  |     |     |     |     |     |

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 InSight. Enable or disable tech support bundle collection in InSight for these Success Tracks.

[View detailed instructions](#)

Coleta de dados com opções Editar e Excluir agenda

## Atualizando VMs do CX Agent para configurações médias e

## grandes

Depois que as VMs são atualizadas, não é possível:

- Fazer downscale de uma configuração grande ou média para uma configuração pequena
- Fazer downscale de uma configuração grande para média
- Atualizar de uma configuração média para uma grande

Antes de atualizar a VM, a Cisco recomenda tirar um instantâneo para fins de recuperação em caso de falha. Consulte [Backup e restauração da CX Cloud VM](#) para obter mais detalhes.

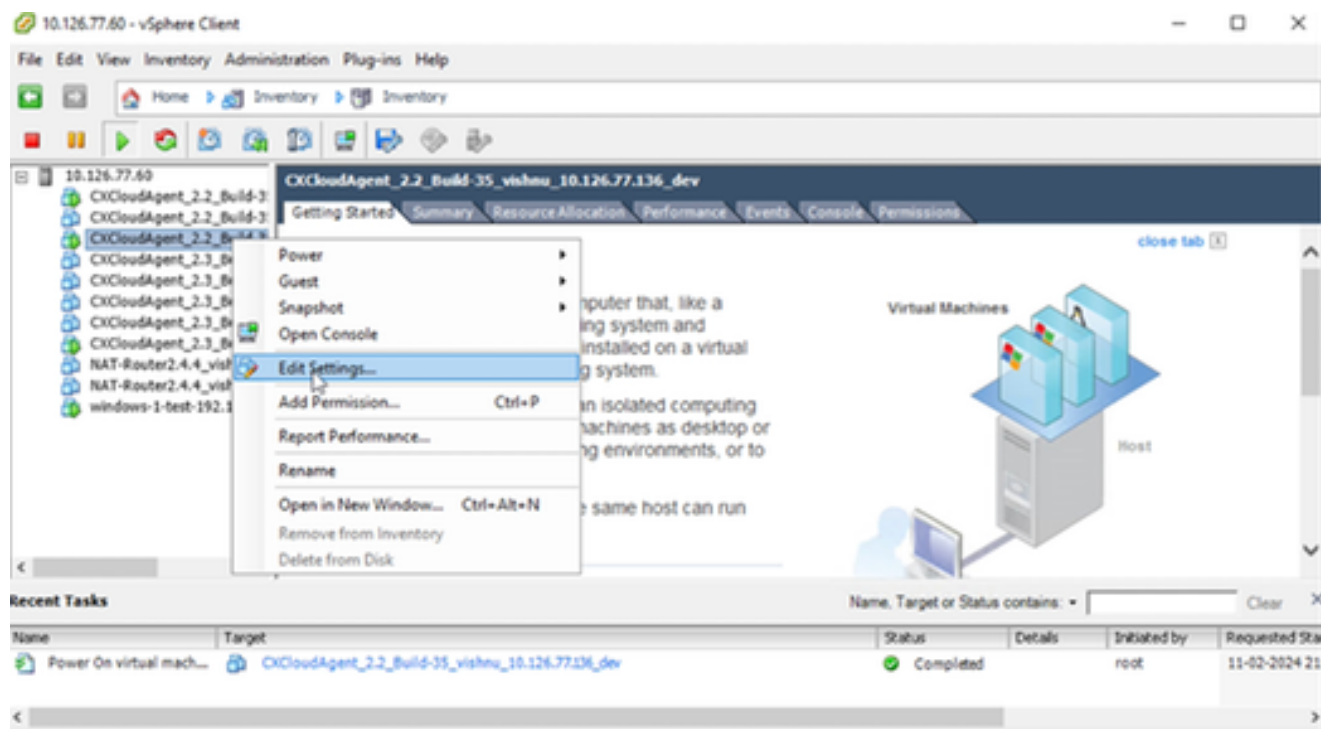
## Reconfiguração usando o VMware vSphere Thick Client

Para atualizar a configuração da VM usando o VMware vSphere Thick Client existente:



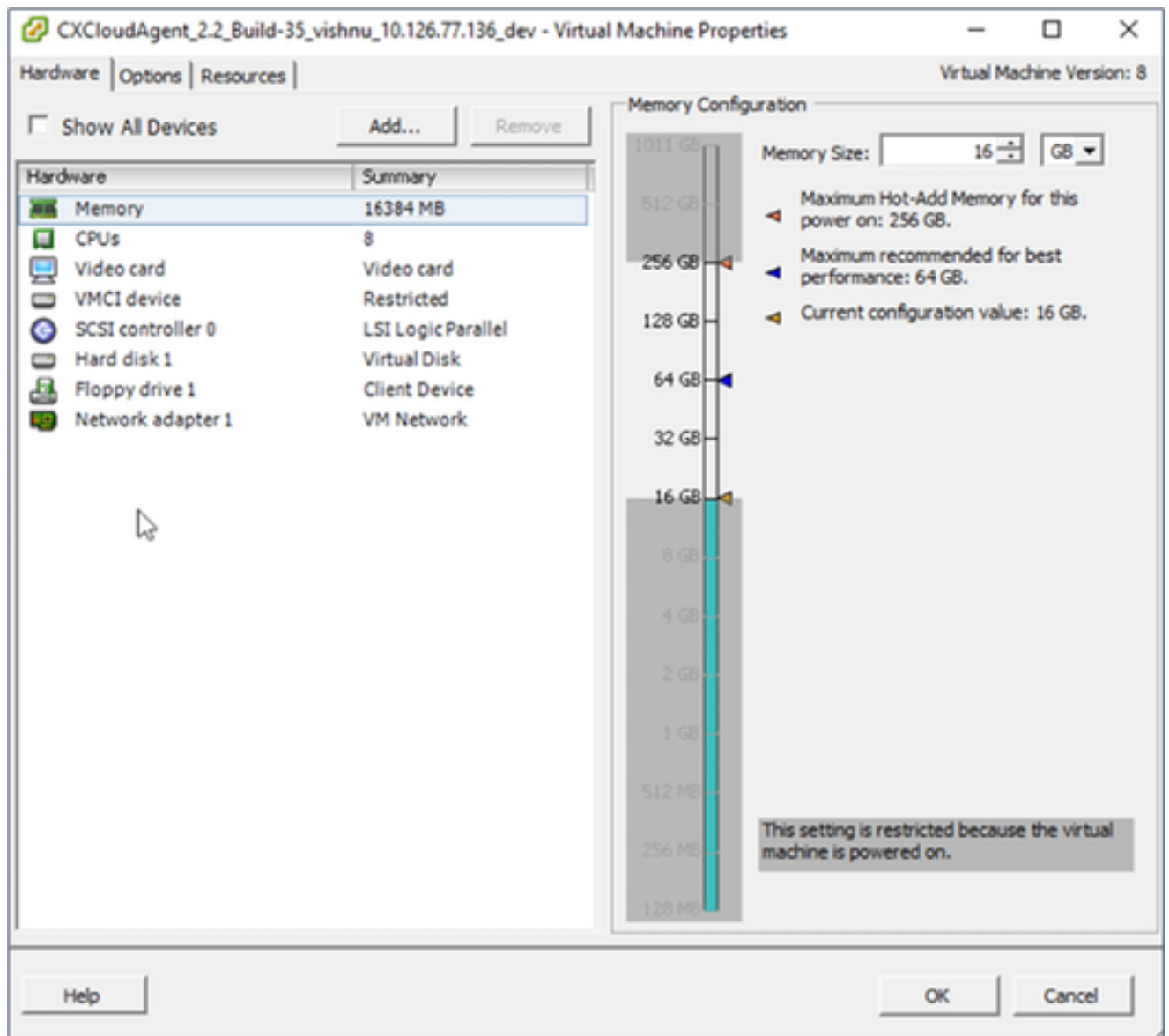
vSphere Client

1. Faça login no VMware vSphere Client. A página Início exibe uma lista de VMs.



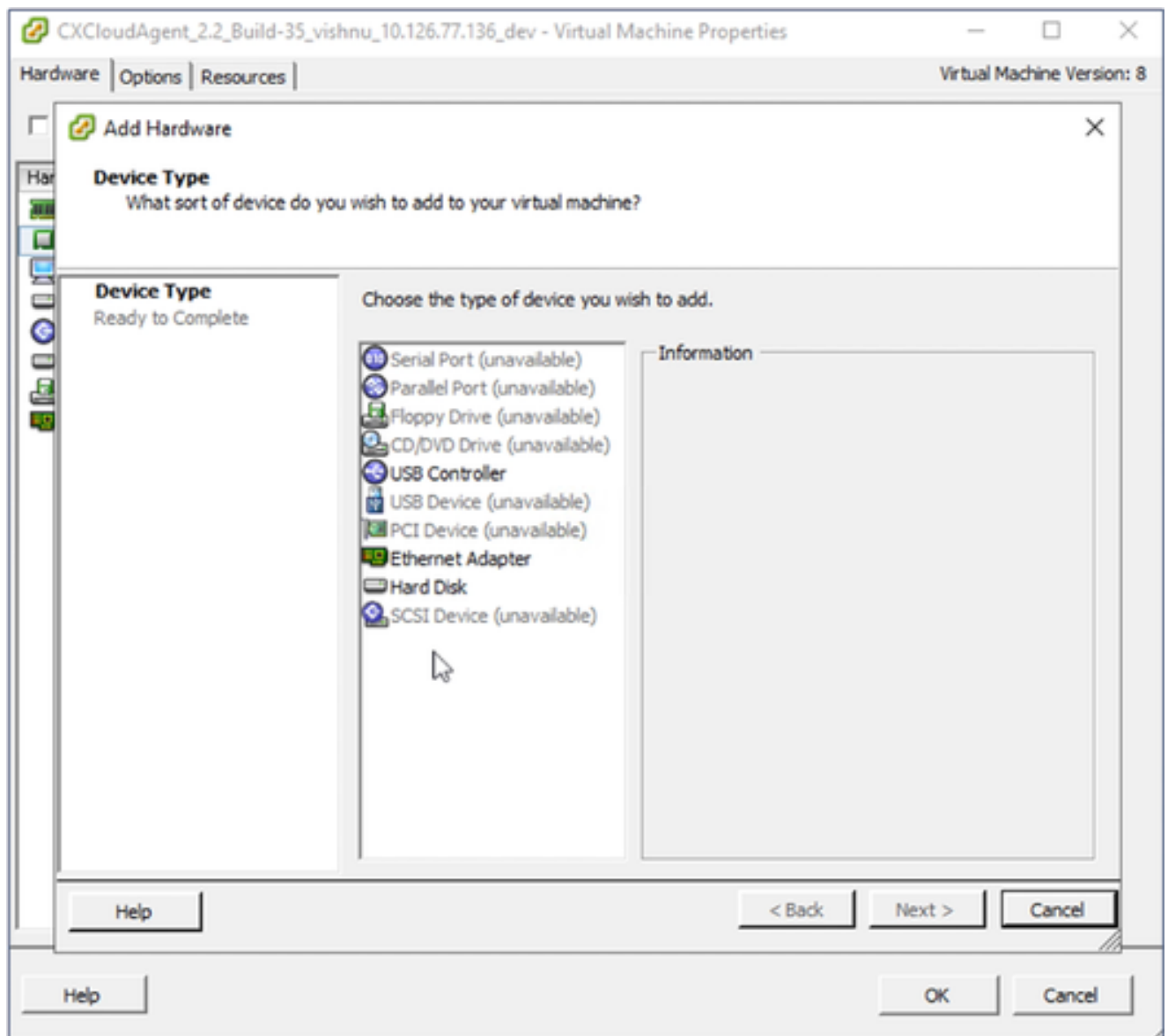
Editar configurações

2. Clique com o botão direito do mouse na VM de destino e selecione Editar configurações no menu. A janela Propriedades da VM é aberta.



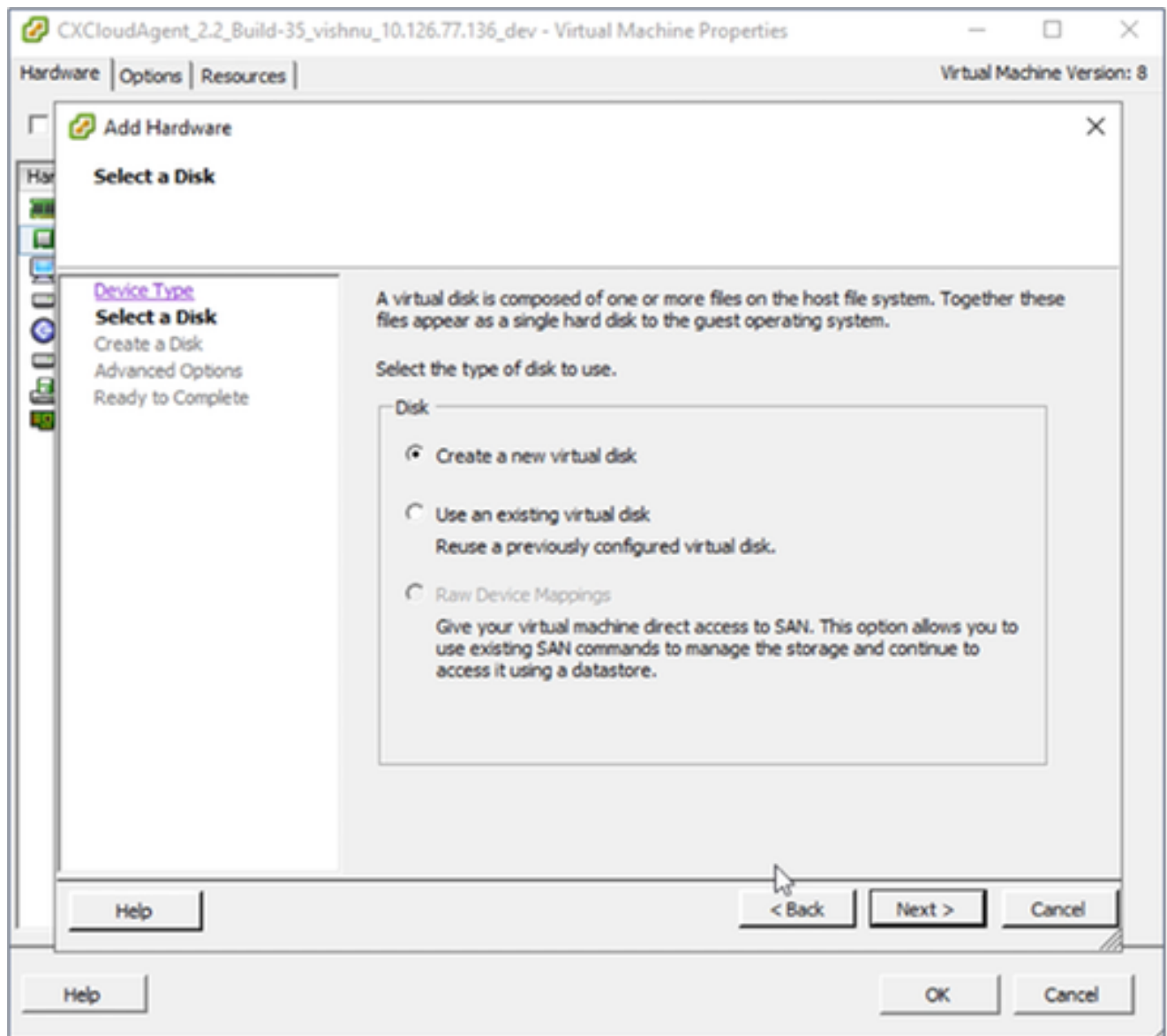
Propriedades da VM

3. Atualize os valores de Memory Size conforme especificado:  
Médio: 32 GB (32768 MB)  
Grande: 64 GB (65536 MB)
4. Selecione CPUs e atualize os valores conforme especificado:  
Médio: 16 núcleos (8 soquetes \* 2 núcleos/soquete)  
Grande: 32 núcleos (16 soquetes \* 2 núcleos/soquete)
5. Clique em Add. A janela Add Hardware é aberta.



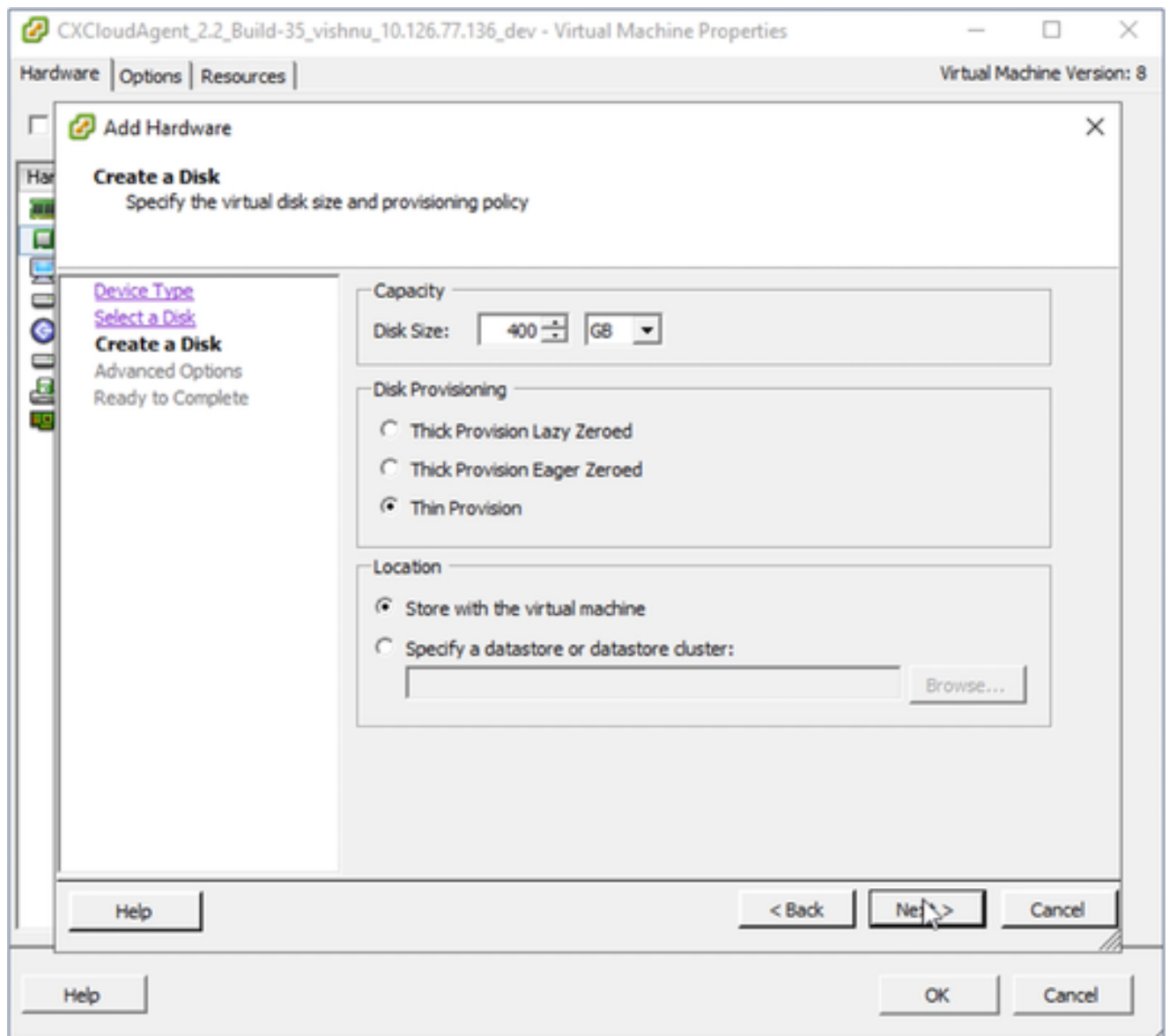
tipo de dispositivo

6. Selecione Hard Disk como o Device Type.
7. Clique em Next.



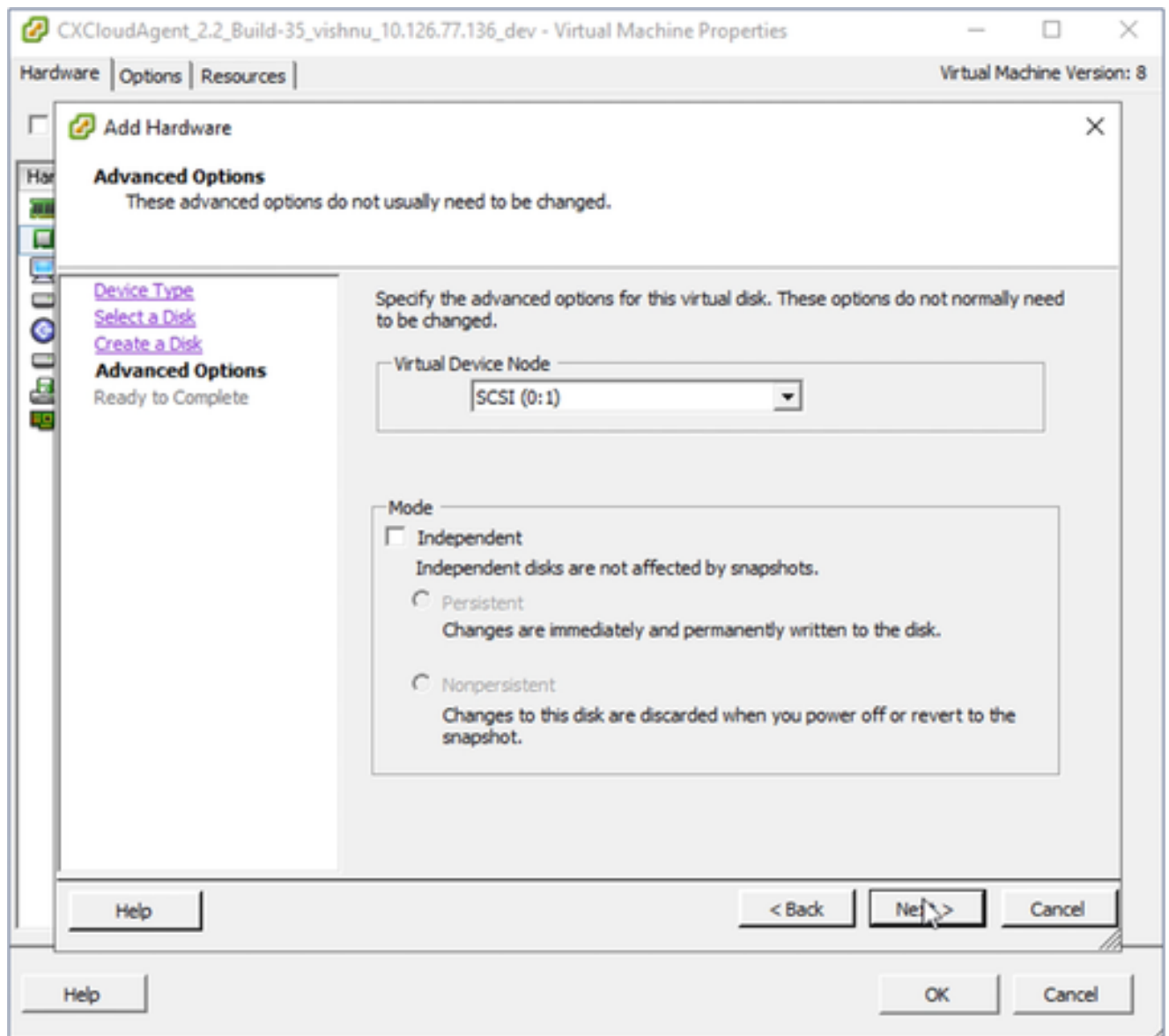
Selecionar disco

8. Selecione o botão de opção Create a new virtual disk e clique em Next.



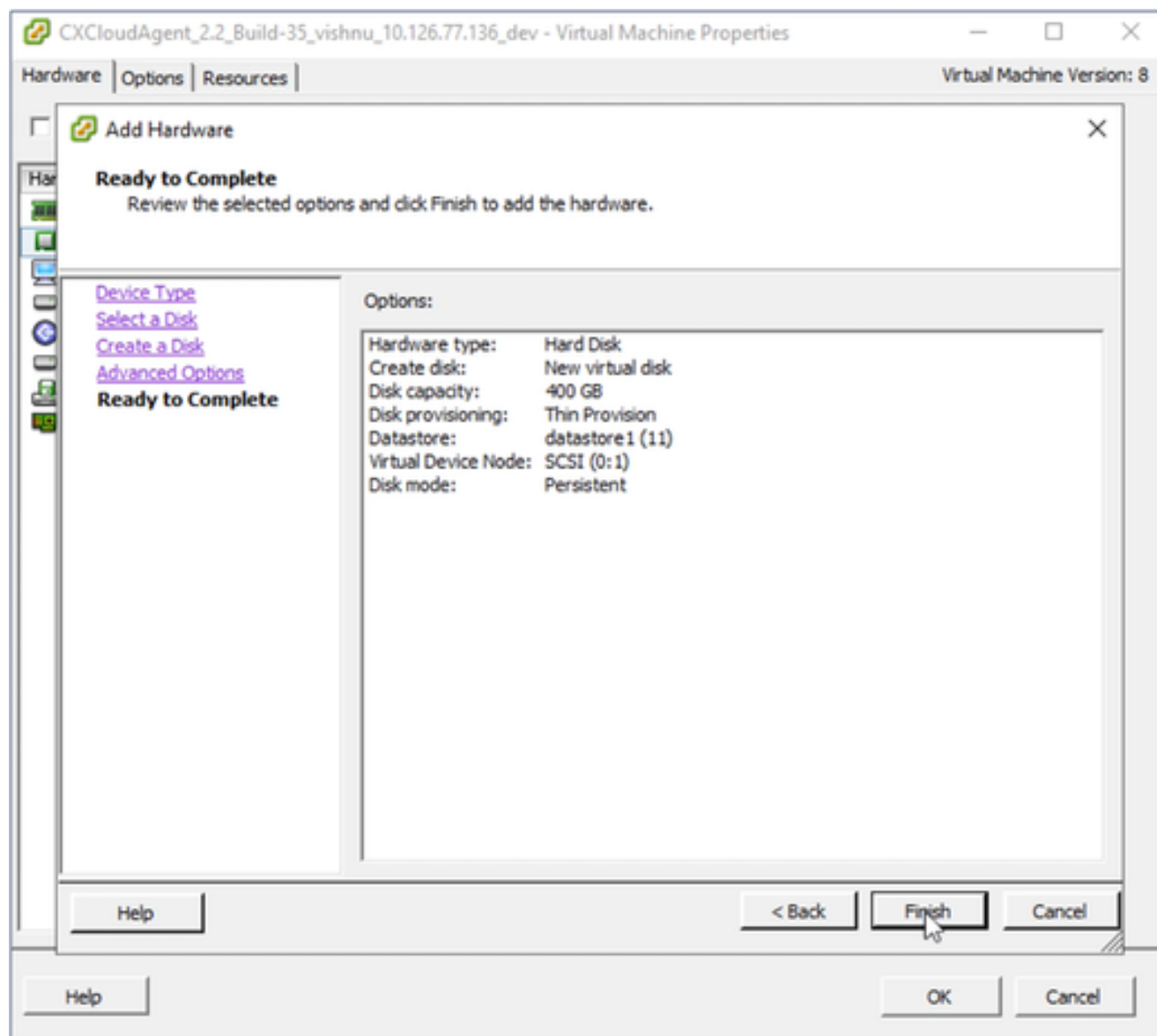
Criar disco

9. Atualize a Capacidade > Tamanho do Disco conforme especificado:  
Pequeno a Médio: 400 GB, (tamanho inicial de 200 GB, aumentando o espaço total para 600 GB)  
Pequeno a Grande: 1000 GB, (tamanho inicial de 200 GB, aumentando o espaço total para 1200 GB)
10. Selecione o botão de opção Thin Provision para Disk Provisioning.
11. Clique em Next. A janela Opções avançadas é exibida.



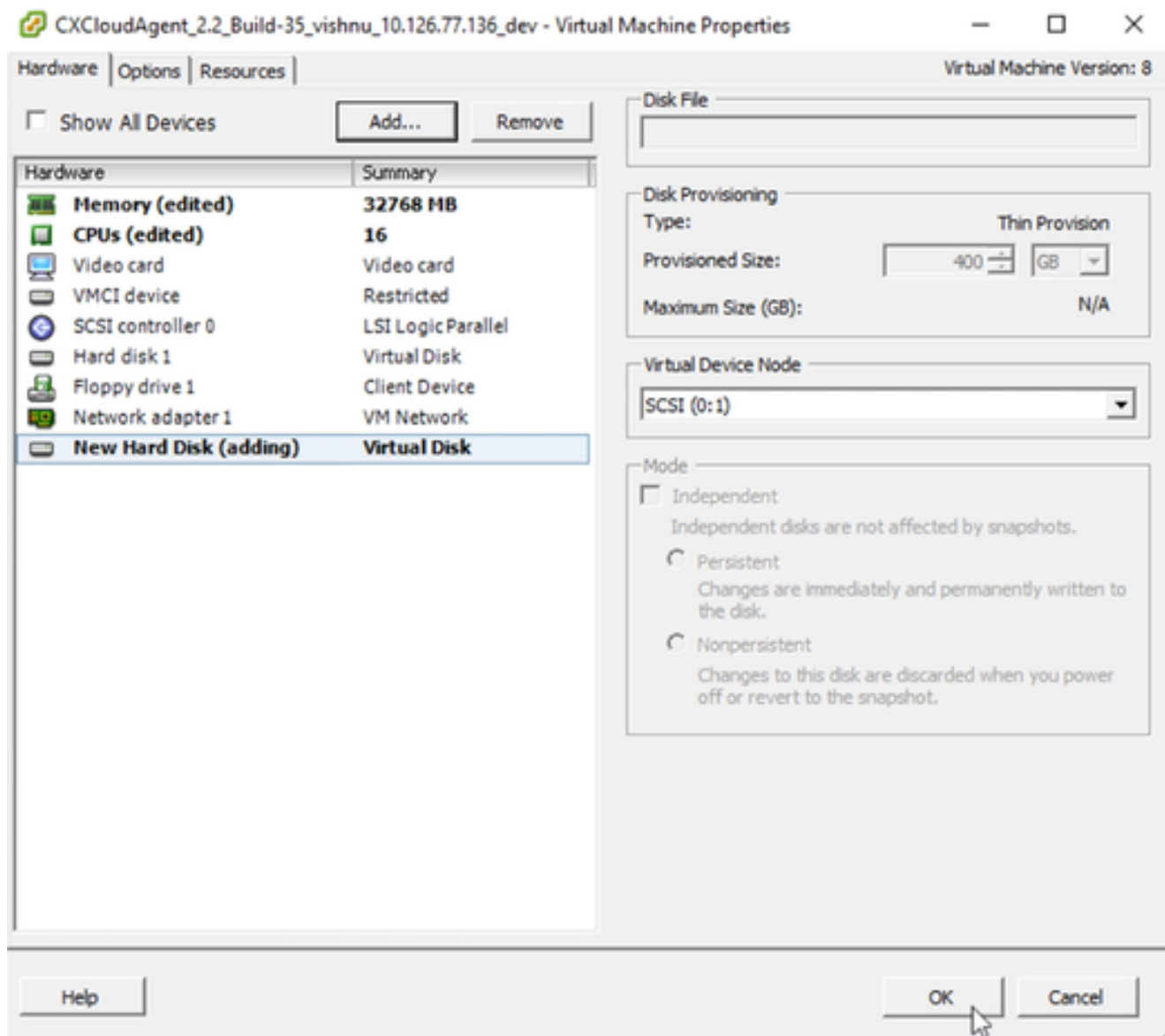
Opções avançadas

12. Não faça alterações. Clique em Avançar para continuar.



Pronto para concluir

13. Clique em Finish.



Hardware

14. Clique em OK para concluir a reconfiguração. A reconfiguração concluída é exibida no painel Tarefas recentes.

10.126.77.60 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Inventory Inventory

10.126.77.60

- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- NAT-Router2.4.4\_vishnu\_1
- NAT-Router2.4.4\_vishnu\_1
- windows-1-test-192.168.77

CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev

Getting Started Summary Resource Allocation Performance Events Console Permissions

close tab

### What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.



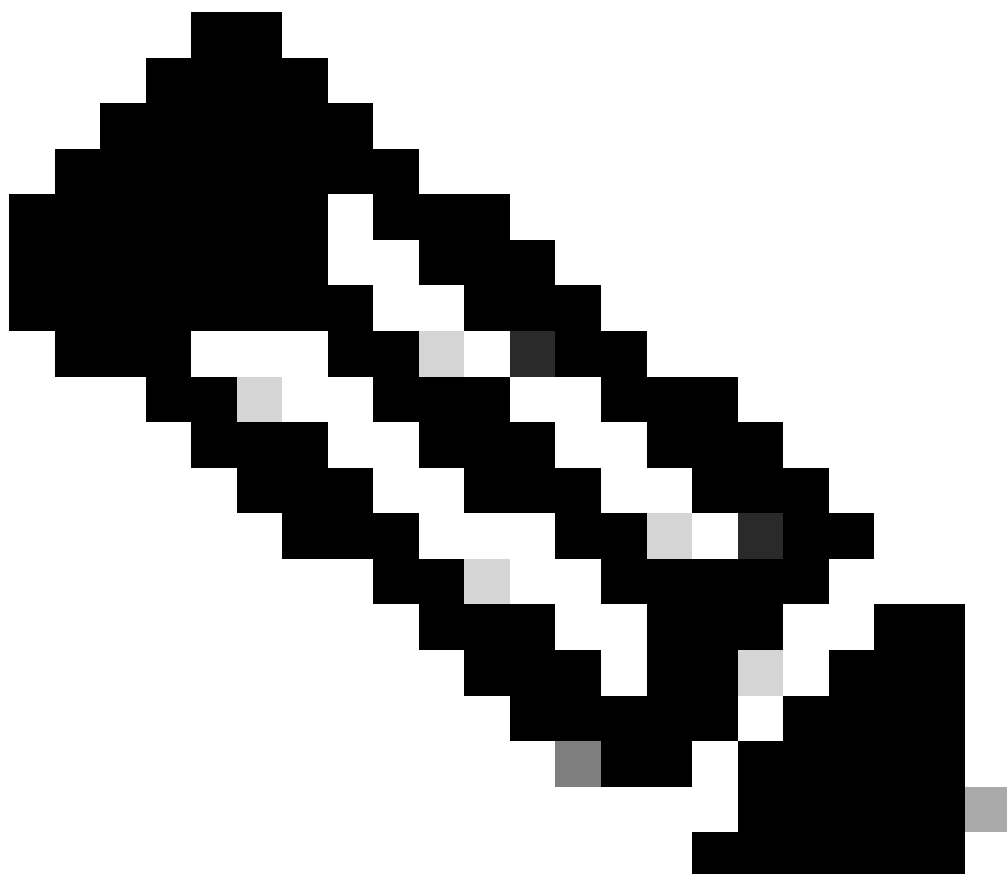
Recent Tasks

Name, Target or Status contains: Clear

| Name                        | Target                                             | Status    | Details | Initiated by |
|-----------------------------|----------------------------------------------------|-----------|---------|--------------|
| Reconfigure virtual machine | CxCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev | Completed |         | root         |
| Power On virtual machine    | CxCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev | Completed |         | root         |

Tasks root

Tarefas Recentes



Note: As alterações de configuração levam aproximadamente cinco minutos para serem concluídas.

---

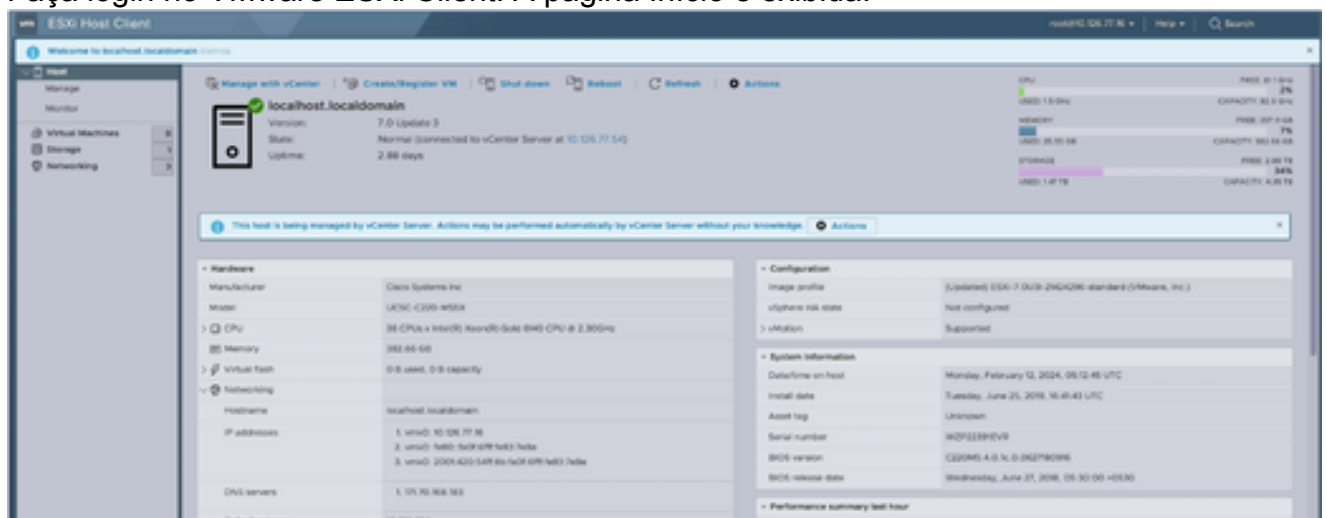
## Reconfiguração usando o cliente da Web ESXi v6.0

Para atualizar as configurações da VM usando o cliente da Web ESXi v6.0:



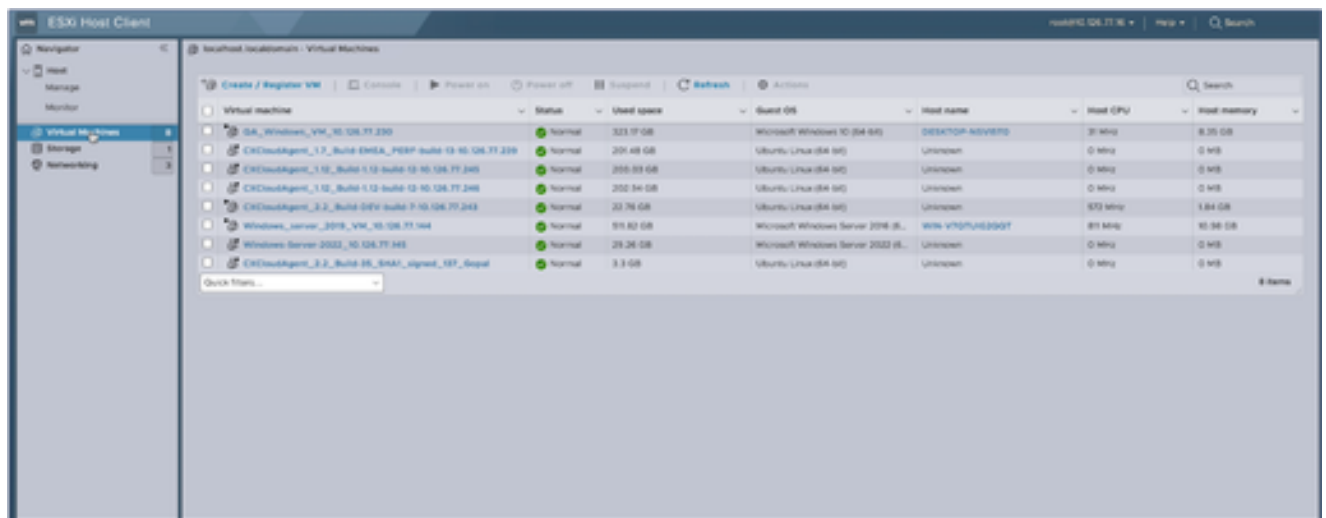
Cliente ESXi

1. Faça login no VMware ESXi Client. A página Início é exibida.



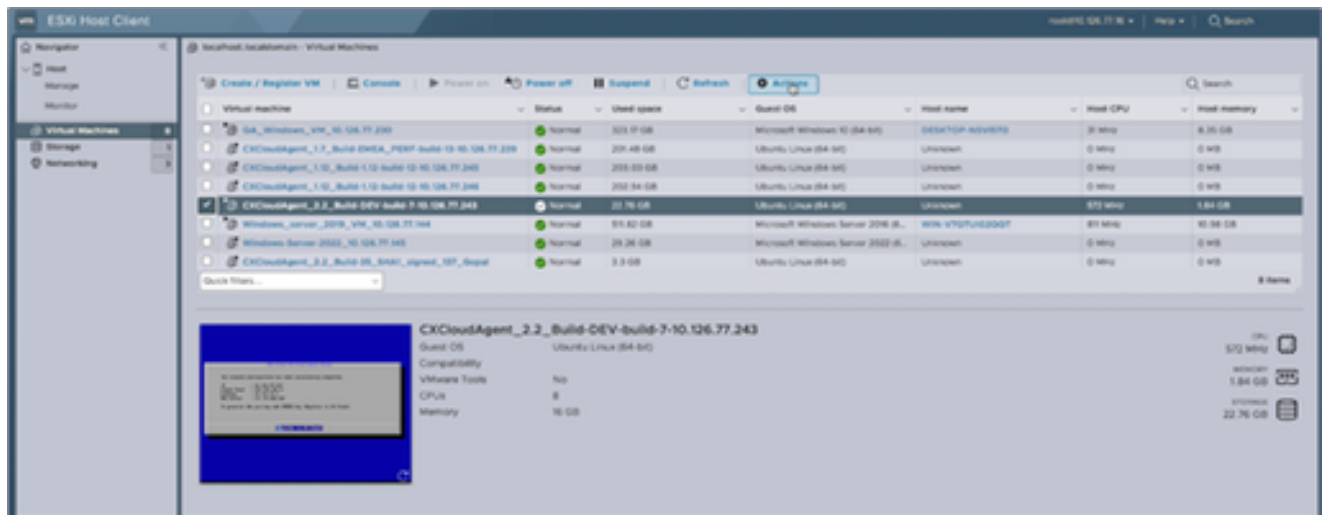
Página inicial do ESXi

2. Clique em Virtual Machine para exibir uma lista de VMs.



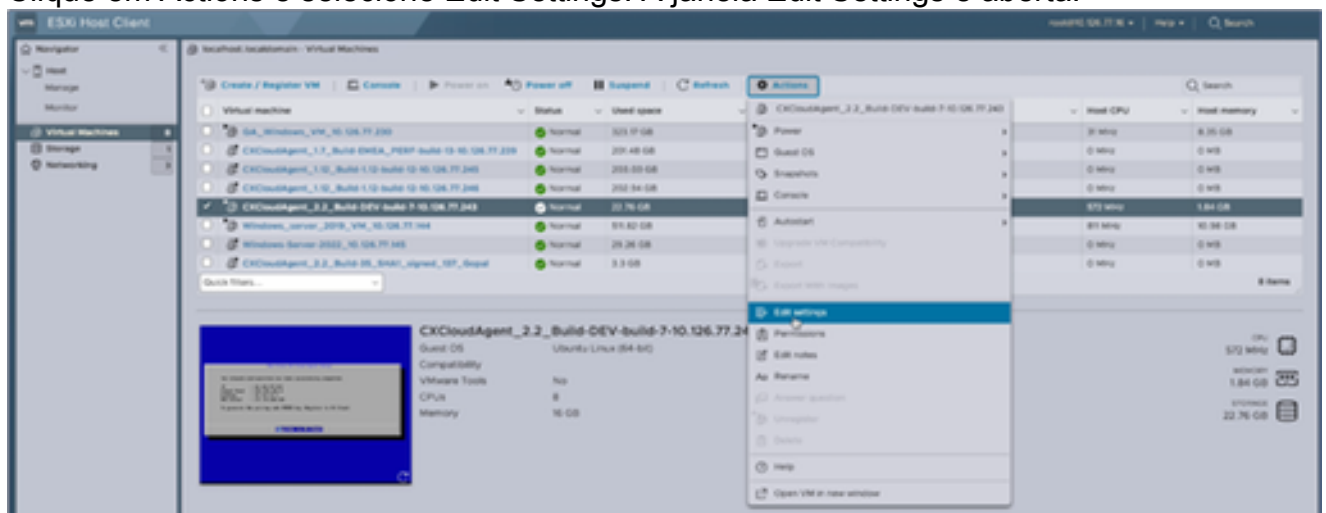
Lista de VMs

### 3. Selecione a VM de destino.

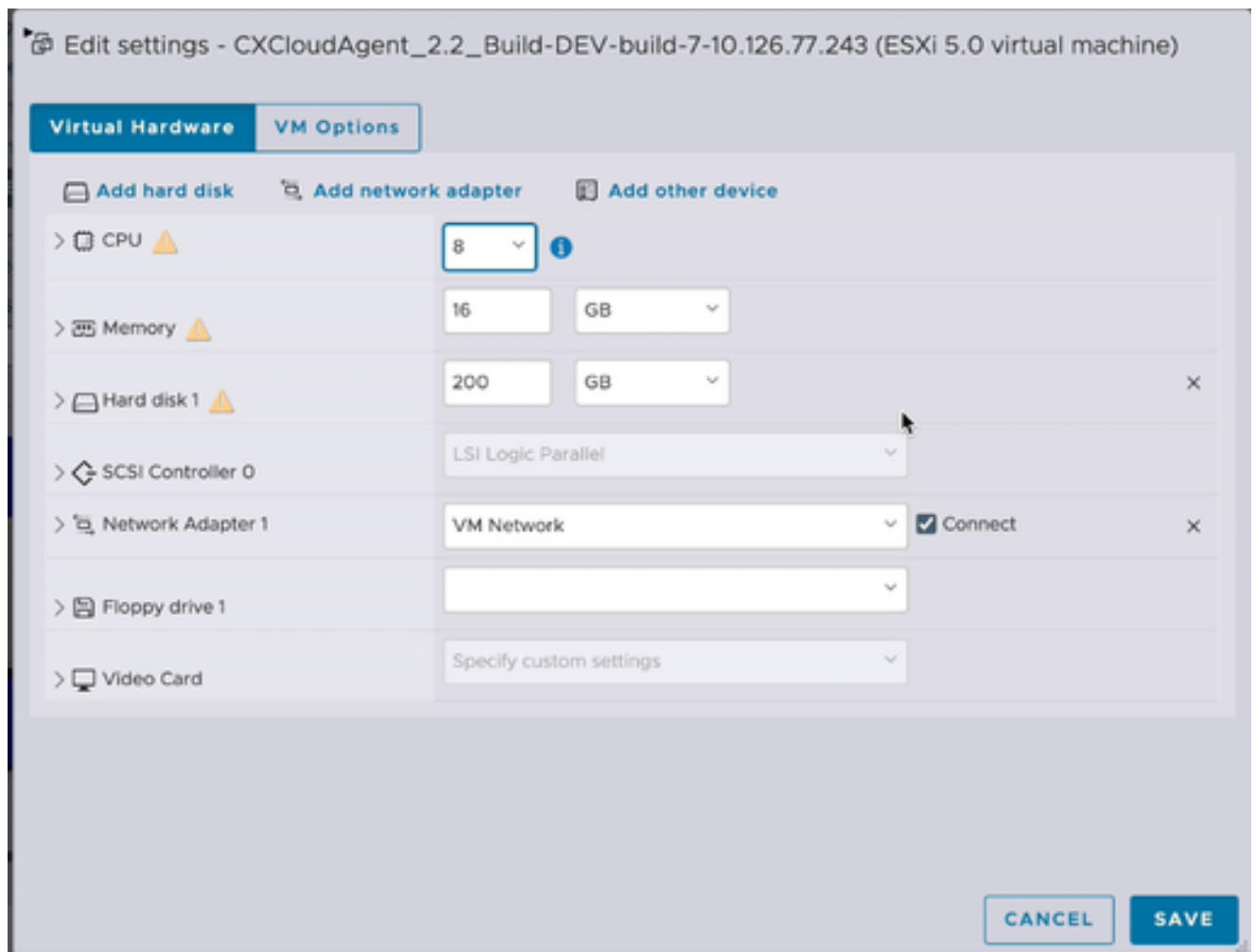


VM de destino

### 4. Clique em Actions e selecione Edit Settings. A janela Edit Settings é aberta.

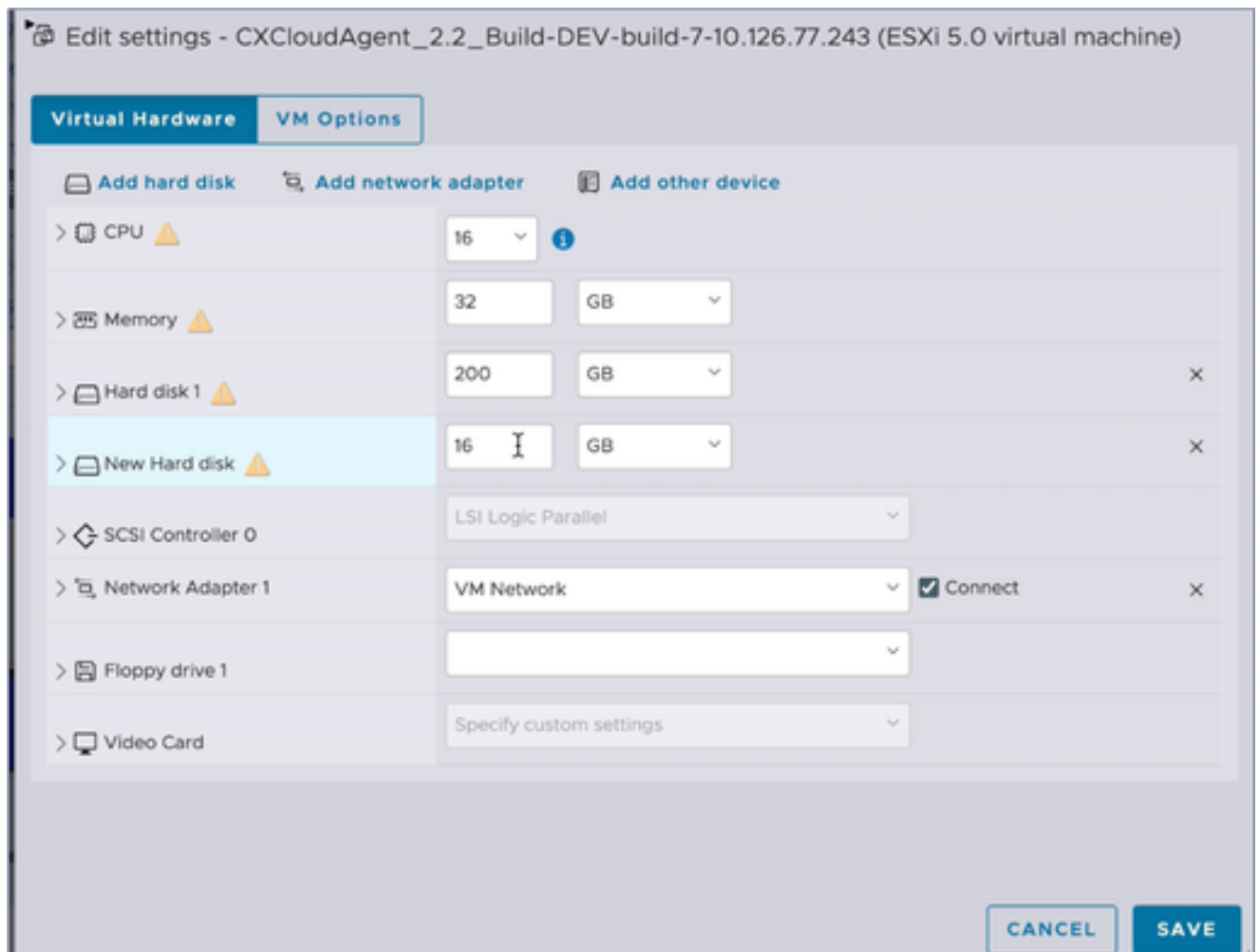


Ações



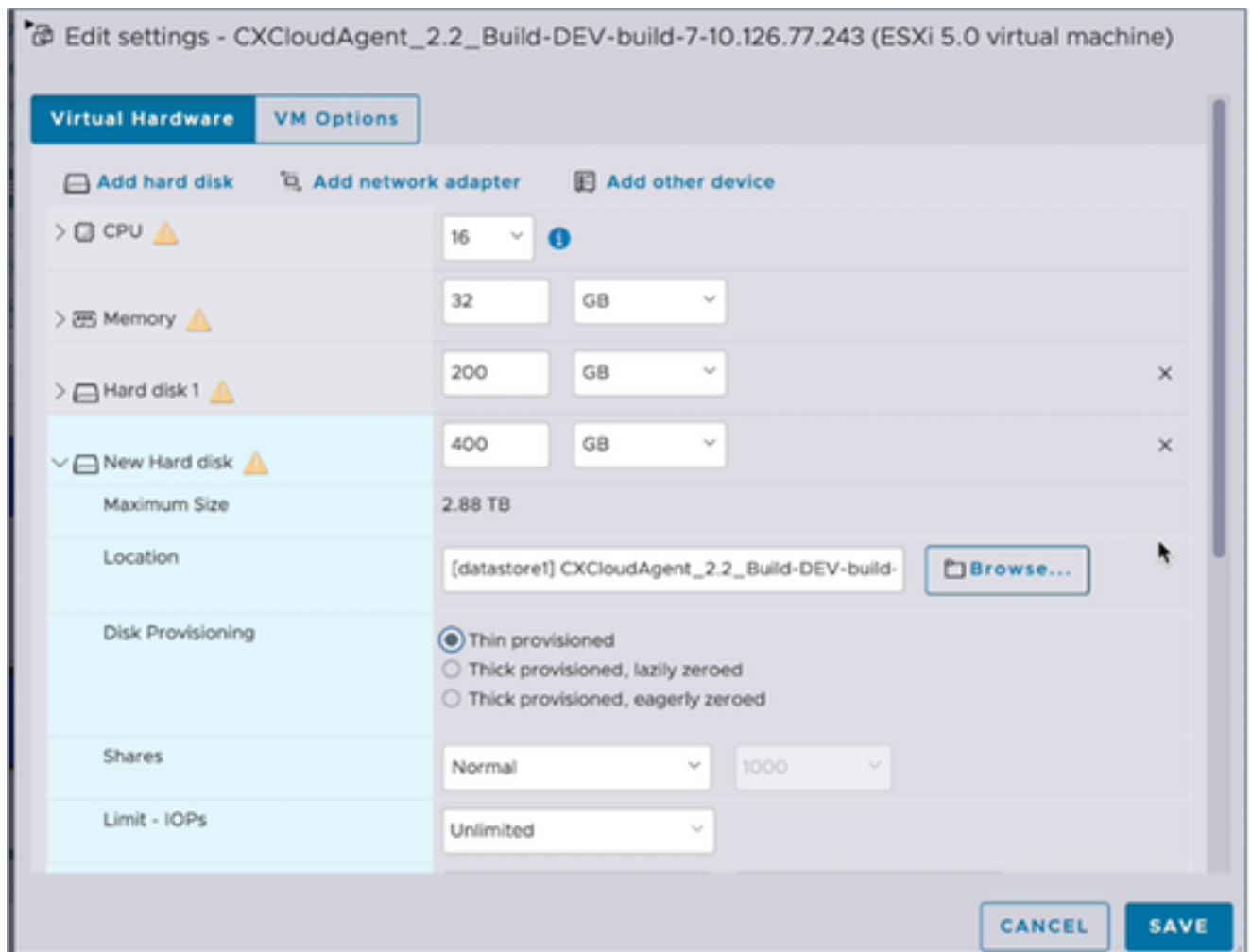
Editar configurações

5. Atualize o valor da CPU conforme especificado:  
Médio: 16 núcleos (8 soquetes \*2 núcleos/soquete)  
Grande: 32 núcleos (16 soquetes \*2 núcleos/soquete)
6. Atualize o valor de Memória conforme especificado:  
Médio: 32 GB  
Grande: 64 GB
7. Clique em Add hard disk > New standard hard disk. A nova entrada do disco rígido é exibida na janela Editar configurações.



Editar configurações

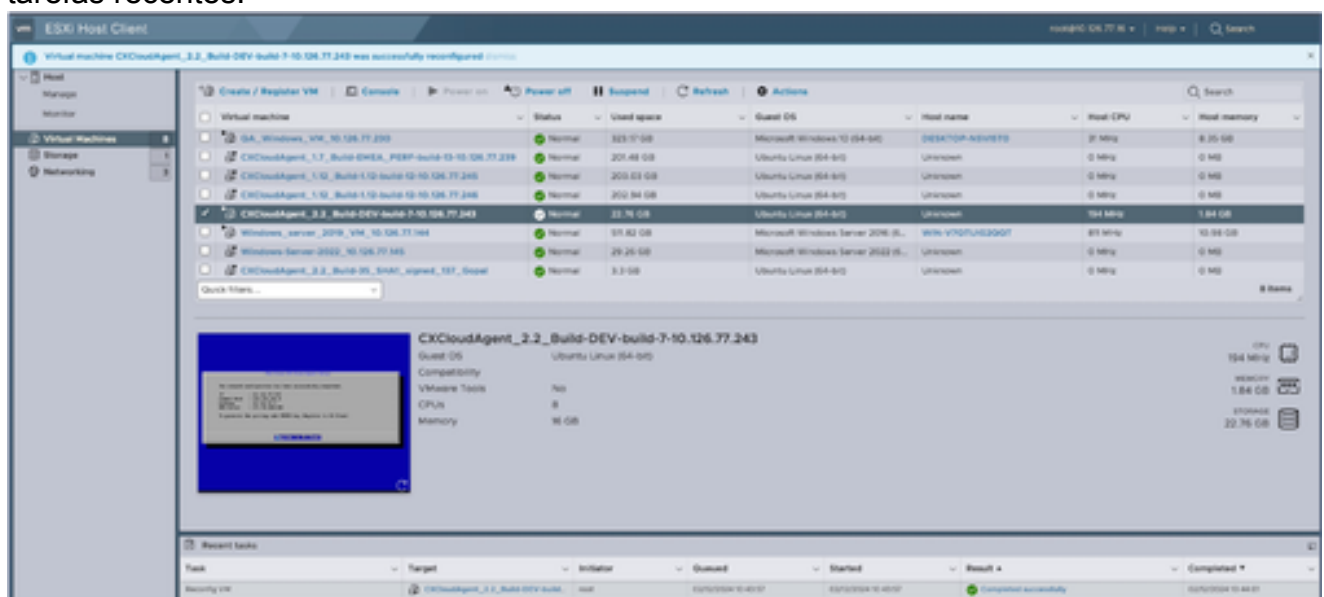
8. Atualize os valores de Novo Disco Rígido conforme especificado:  
Pequeno a Médio: 400 GB, (tamanho inicial de 200 GB, aumentando o espaço total para 600 GB)  
Pequeno a Grande: 1000 GB, (tamanho inicial de 200 GB, aumentando o espaço total para 1200 GB)
9. Clique na seta para expandir Novo disco rígido. As propriedades são exibidas.



Editar configurações

10. Selecione o botão de opção Thin provisioned.

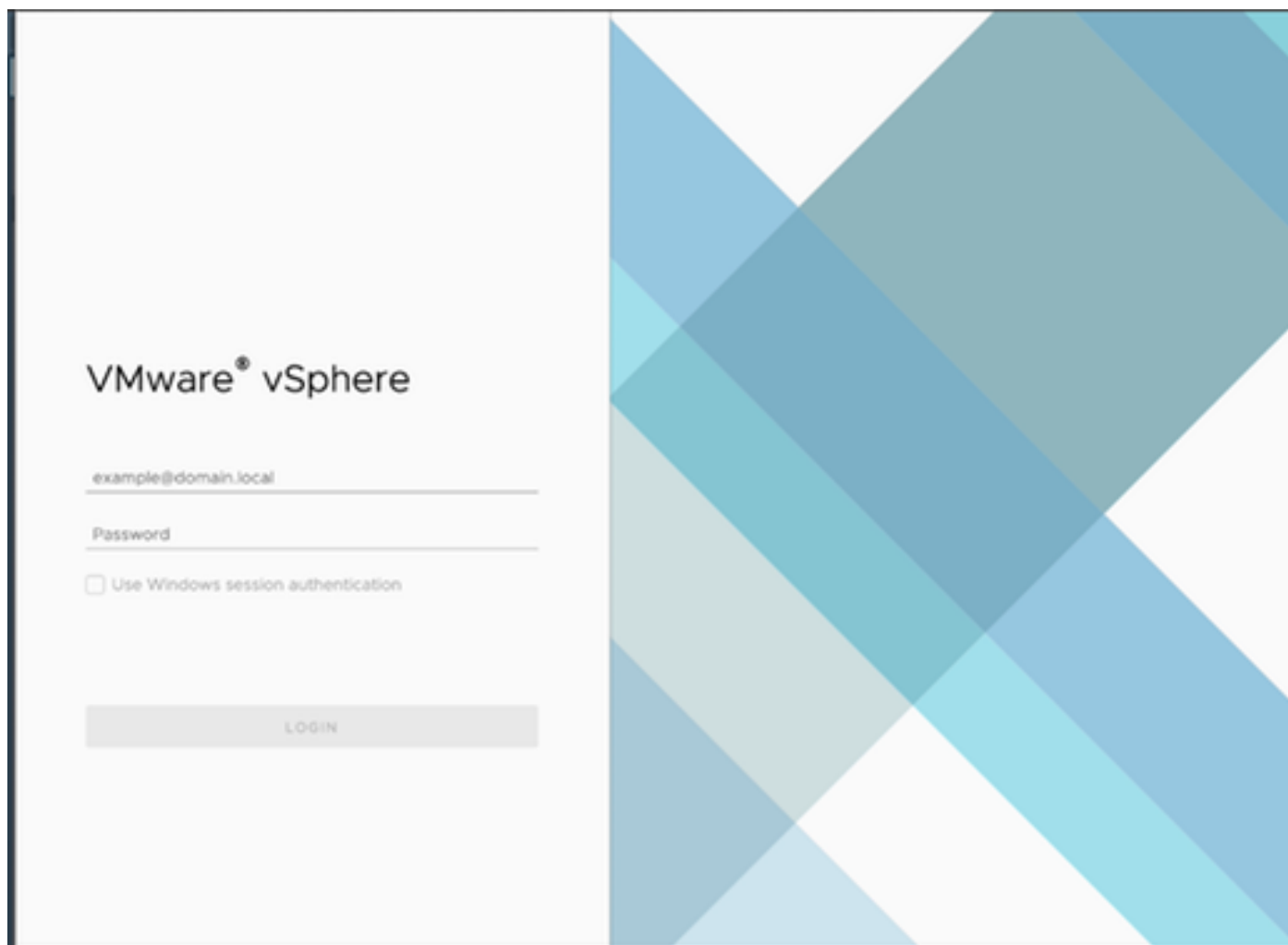
11. Clique em Save para concluir a configuração. A atualização de configuração é exibida nas tarefas recentes.



Tarefas Recentes

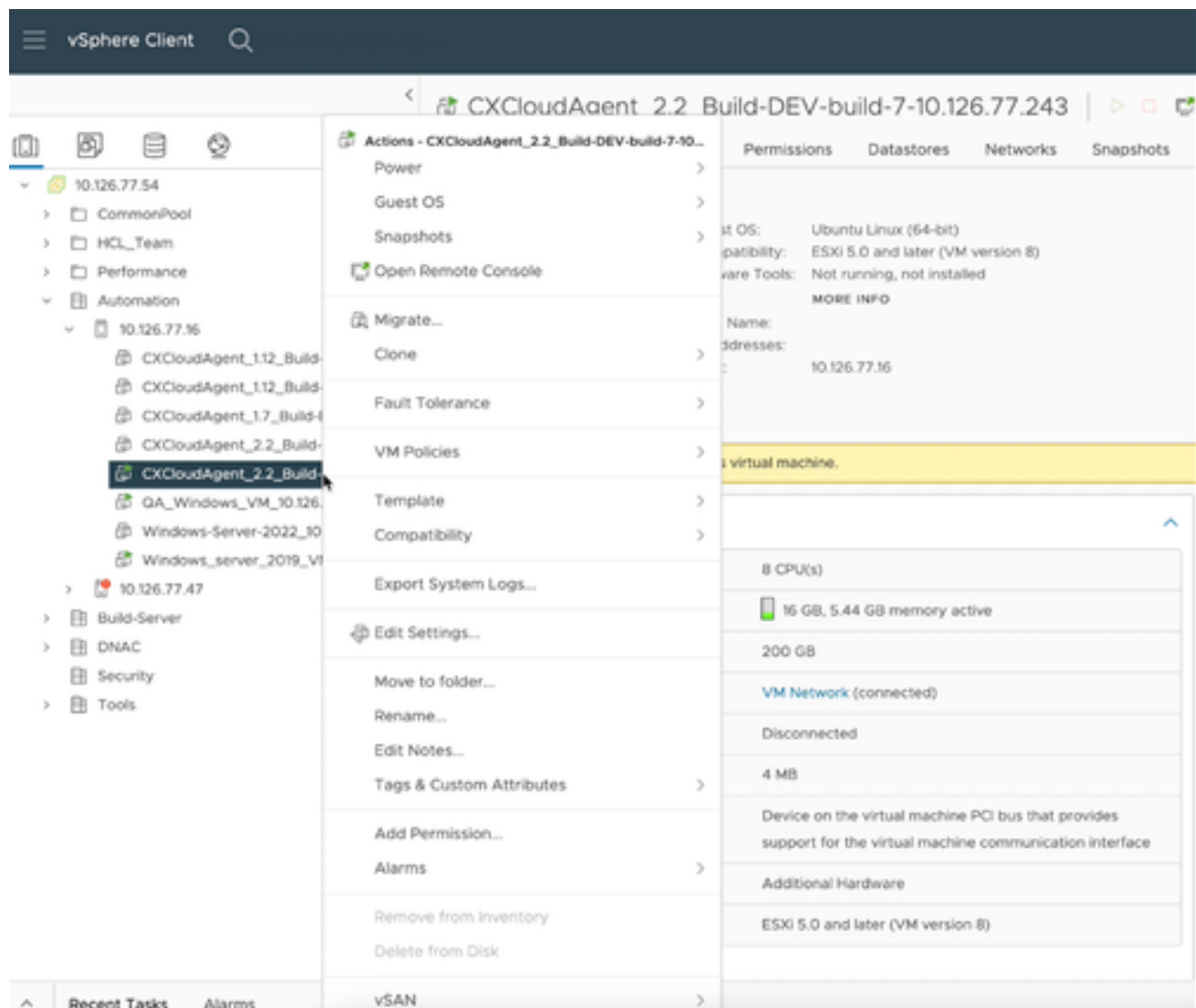
Reconfiguração usando o Web Client vCenter

Para atualizar as configurações da VM usando o Web Client vCenter:



vCenter

1. Faça login no vCenter. A página Início é exibida.



Lista de VMs

2. Clique com o botão direito do mouse na VM de destino e selecione Editar configurações no menu. A janela Edit Settings é aberta.

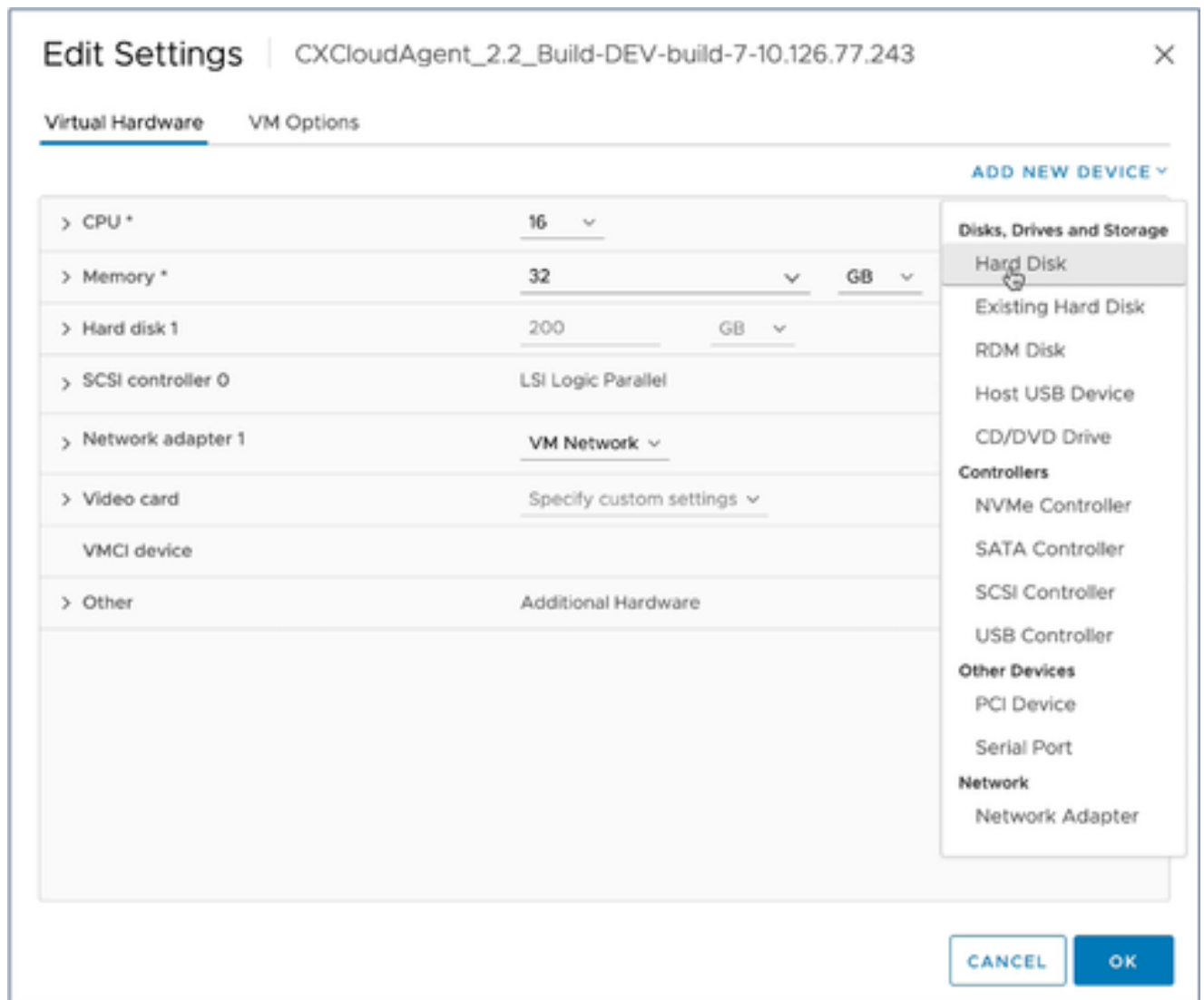
|                                                                                                 |                           |                                               |
|-------------------------------------------------------------------------------------------------|---------------------------|-----------------------------------------------|
| > CPU                                                                                           | 8 ▾                       | ⓘ                                             |
| > Memory                                                                                        | 16 ▾                      | GB ▾                                          |
| > Hard disk 1  | 200                       | GB ▾                                          |
| > SCSI controller 0                                                                             | LSI Logic Parallel        |                                               |
| > Network adapter 1                                                                             | VM Network ▾              | <input checked="" type="checkbox"/> Connected |
| > Video card                                                                                    | Specify custom settings ▾ |                                               |
| VMCI device                                                                                     |                           |                                               |
| > Other                                                                                         | Additional Hardware       |                                               |

CANCEL

OK

Editar configurações

3. Atualize os valores da CPU conforme especificado:  
Médio: 16 núcleos (8 soquetes \*2 núcleos/soquete)  
Grande: 32 núcleos (16 soquetes \*2 núcleos/soquete)
4. Atualize os valores de Memória conforme especificado:  
Médio: 32 GB  
Grande: 64 GB



Editar configurações

5. Clique em Add New Device e selecione Hard Disk. A entrada New Hard disk é adicionada.

Edit Settings | CXCloudAgent\_2.2\_Build-DEV-build-7-10.126.77.243

Virtual Hardware

VM Options

ADD NEW DEVICE

|                     |                                |                         |           |
|---------------------|--------------------------------|-------------------------|-----------|
| > CPU *             | 16                             |                         |           |
| > Memory *          | 32                             |                         | GB        |
| > Hard disk 1       | 200                            |                         | GB        |
| > New Hard disk *   | 16                             |                         | GB        |
| Maximum Size        | 3.02 TB                        |                         |           |
| VM storage policy   | Datastore Default              |                         |           |
| Location            | Store with the virtual machine |                         |           |
| Disk Provisioning   | Thick Provision Lazy Zeroed    |                         |           |
| Sharing             | Unspecified                    |                         |           |
| Shares              | Normal                         | 1000                    |           |
| Limit - IOPs        | Unlimited                      |                         |           |
| Disk Mode           | Dependent                      |                         |           |
| Virtual Device Node | SCSI controller 0              | SCSI(0:1) New Hard disk |           |
| > SCSI controller 0 | LSI Logic Parallel             |                         |           |
| > Network adapter 1 | VM Network                     |                         | Connected |

CANCEL

OK

Editar configurações

6. Atualize a memória do Novo Disco Rígido conforme especificado:
- Pequeno a Médio: 400 GB, (tamanho inicial de 200 GB, aumentando o espaço total para 600 GB)
- Pequeno a Grande: 1000 GB, (tamanho inicial de 200 GB, aumentando o espaço total para 1200 GB)

Edit Settings
CXCloudAgent\_2.2\_Build-DEV-build-7-10.126.77.243

Virtual Hardware
VM Options

ADD NEW DEVICE

|                     |                                |                         |           |
|---------------------|--------------------------------|-------------------------|-----------|
| > CPU *             | 16                             |                         |           |
| > Memory *          | 32                             |                         | GB        |
| > Hard disk 1       | 200                            |                         | GB        |
| > New Hard disk *   | 400                            |                         | GB        |
| Maximum Size        | 3.02 TB                        |                         |           |
| VM storage policy   | Datastore Default              |                         |           |
| Location            | Store with the virtual machine |                         |           |
| Disk Provisioning   | Thin Provision                 |                         |           |
| Sharing             | Unspecified                    |                         |           |
| Shares              | Normal                         | 1000                    |           |
| Limit - IOPs        | Unlimited                      |                         |           |
| Disk Mode           | Dependent                      |                         |           |
| Virtual Device Node | SCSI controller 0              | SCSI(0:1) New Hard disk |           |
| > SCSI controller 0 | LSI Logic Parallel             |                         |           |
| > Network adapter 1 | VM Network                     |                         | Connected |

CANCEL
OK

Editar configurações

- Selecione Thin Provision na lista suspensa Disk Provisioning.
- Clique em OK para concluir a atualização.

## Implantação e configuração de rede

Selecione uma destas opções para implantar o CX Agent:

- [VMware vSphere/vCenter Thick Client ESXi 5.5/6.0](#)
- [Instalação do VMware vSphere/vCenter Web Client ESXi 6.0](#) ou do [Web Client vCenter](#)
- [Oracle Virtual Box 7.0.12](#)
- [Instalação do Microsoft Hyper-V](#)

### Implantação do OVA

Instalação do Thick Client ESXi 5.5/6.0

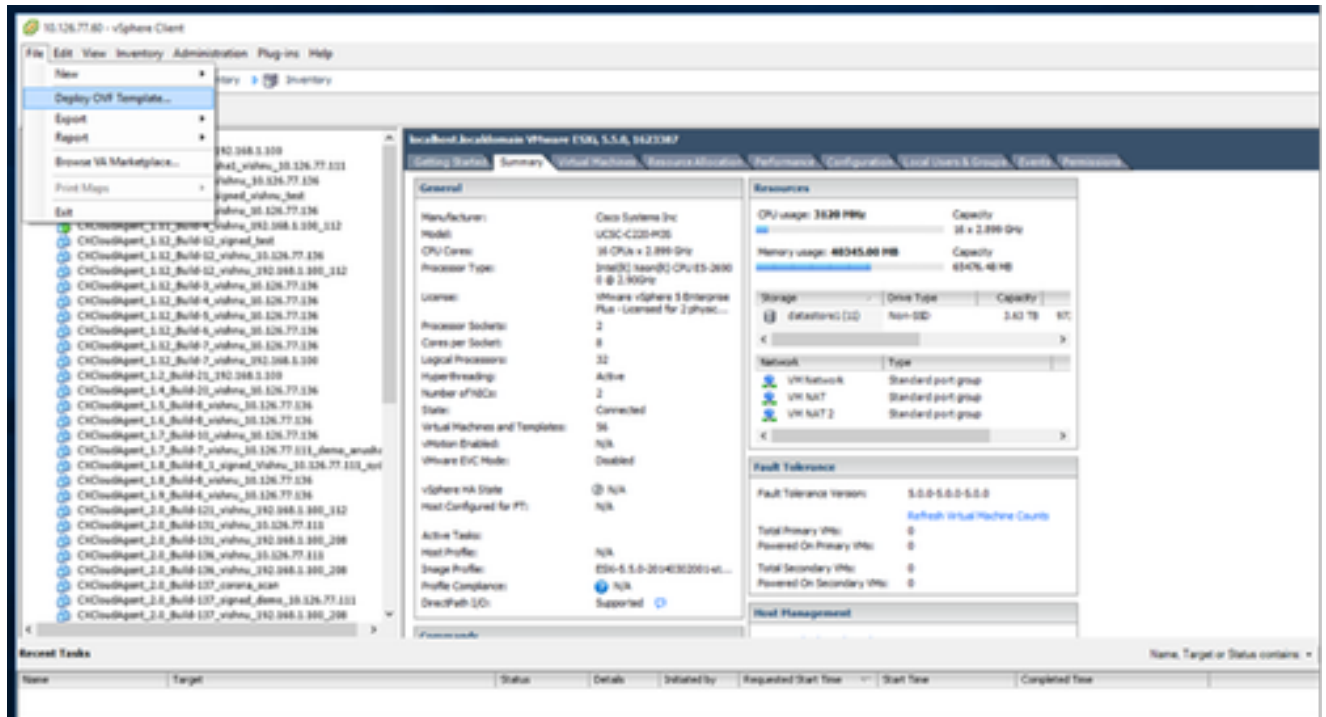
Esse cliente permite a implantação do CX Agent OVA com o uso do cliente thick vSphere.

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



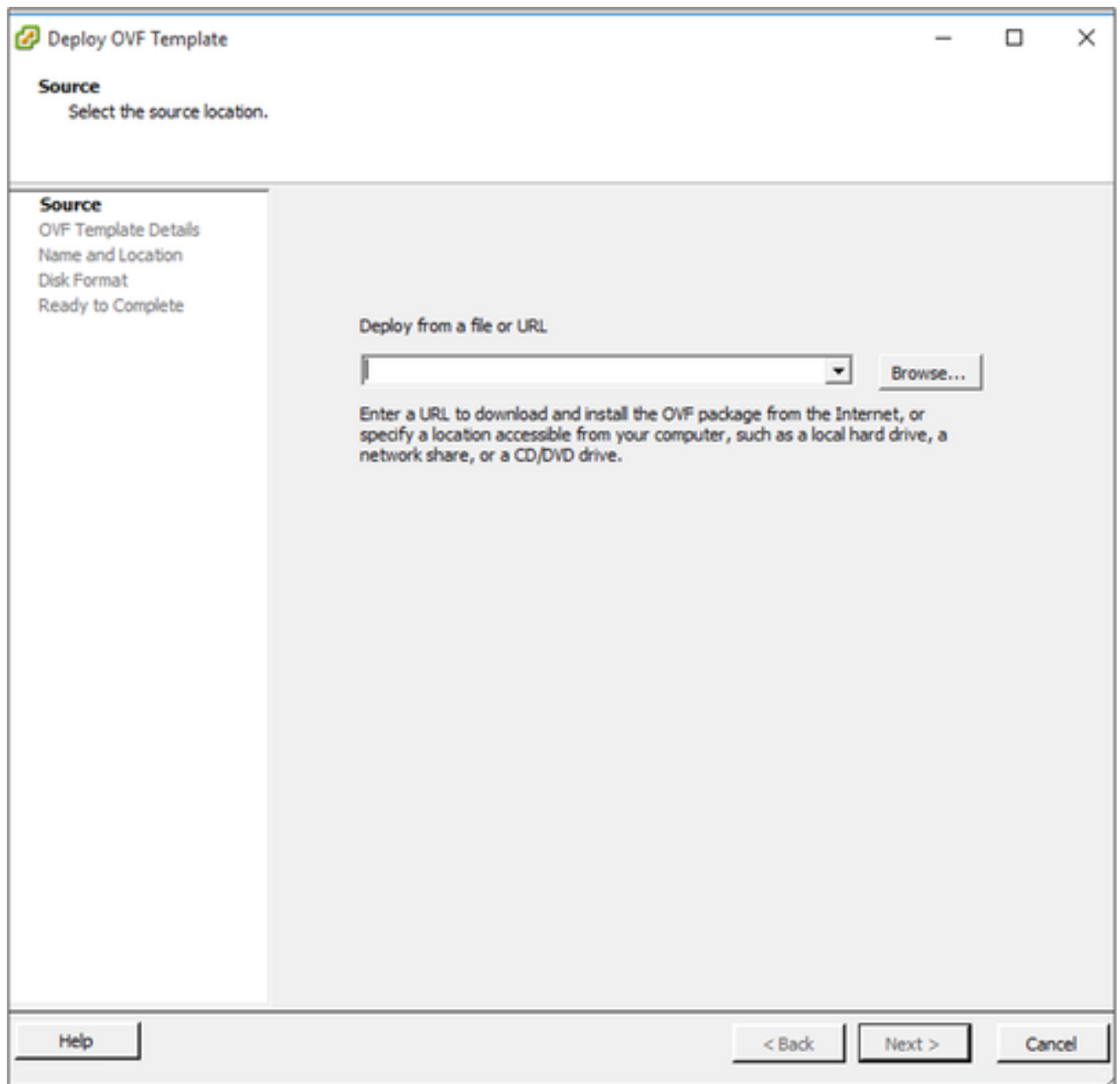
Login

2. No menu, selecione File > Deploy OVF Template.



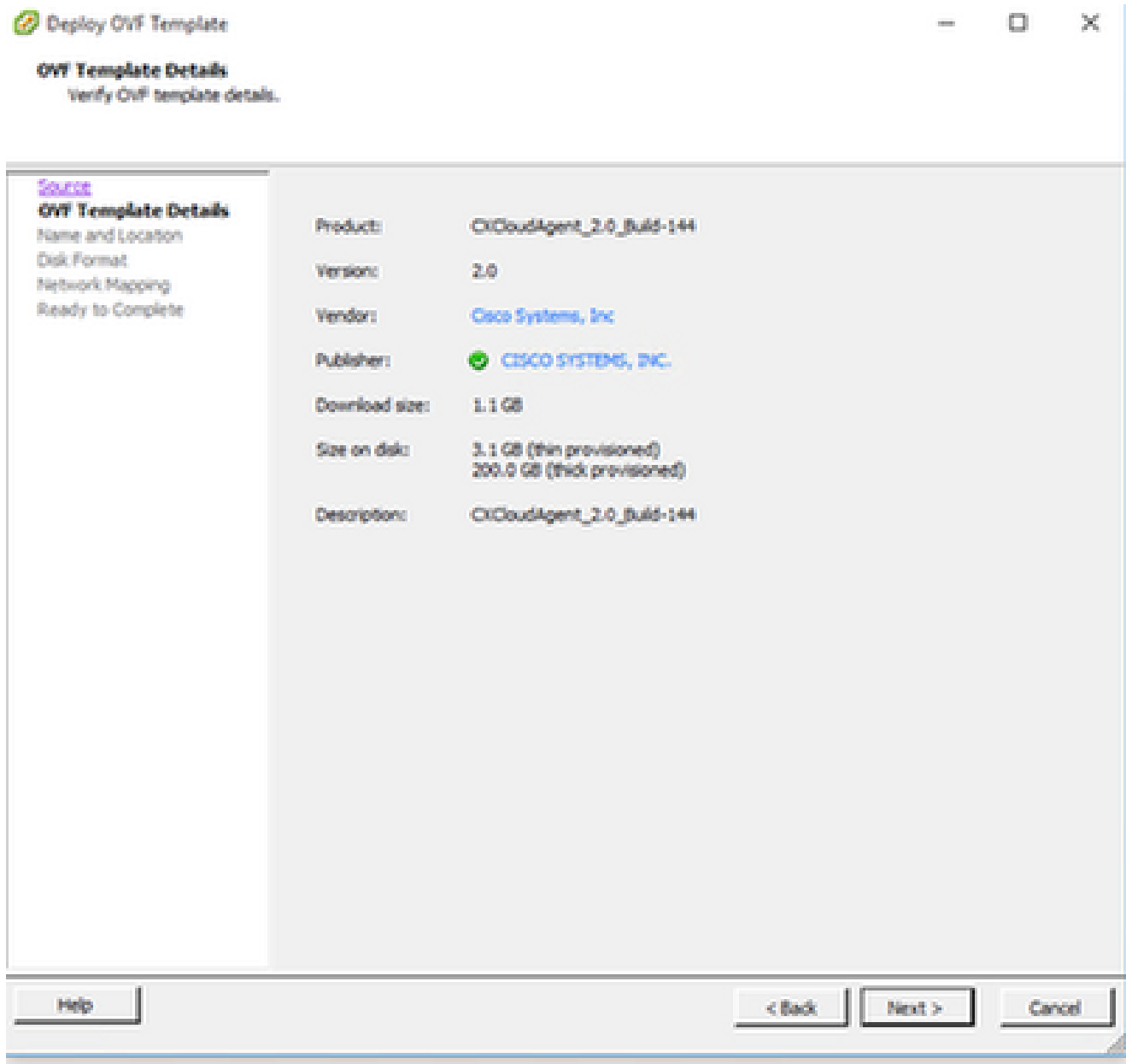
vSphere Client

3. Navegue para selecionar o arquivo OVA e clique em Avançar.



Caminho do OVA

4. Verifique os Detalhes OVF e clique em Avançar.



Detalhes do modelo

5. Insira um nome exclusivo e clique em Avançar.

Deploy OVF Template

**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:  
CXCloudAgent\_2.0\_Build-144\_DEMO

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

Help < Back Next > Cancel

Nome e local

6. Selecione um Formato de disco e clique em Avançar (o provisionamento thin é recomendado).

Deploy OVF Template

**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

Datastore: datastore1 (11)

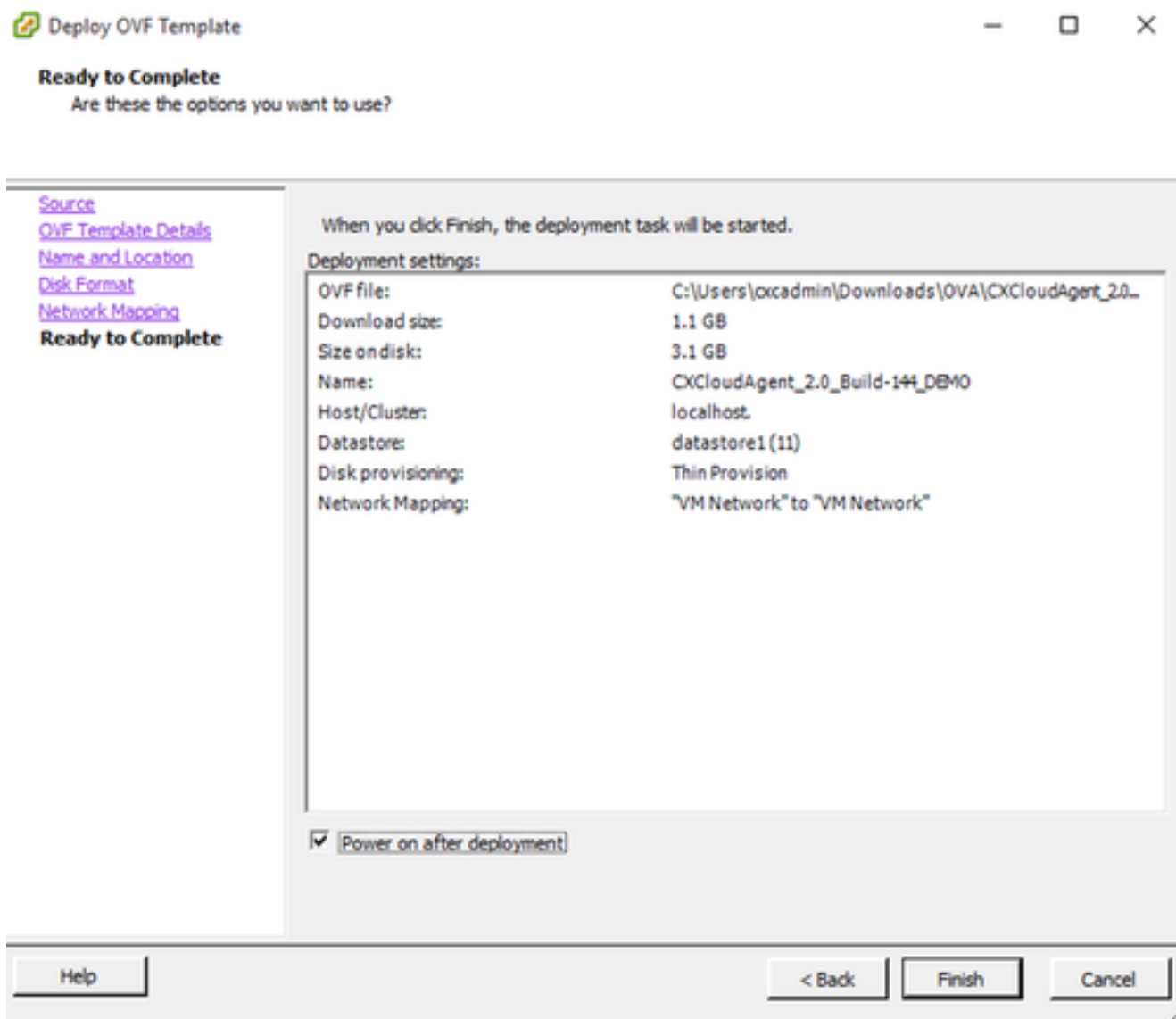
Available space (GB): 973.1

☐ Thick Provision Lazy Zeroed  
☐ Thick Provision Eager Zeroed  
☒ Thin Provision

Help < Back Next > Cancel

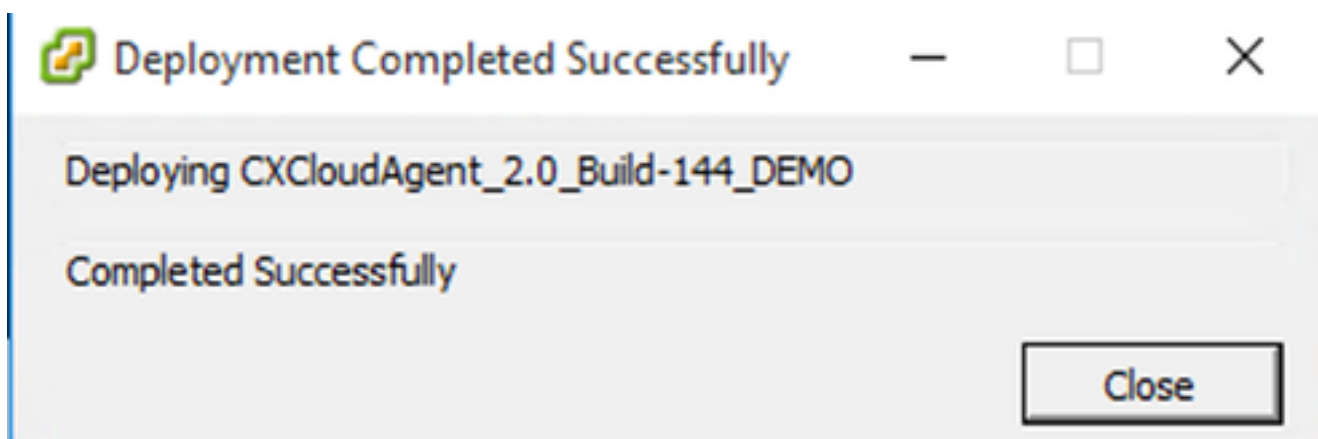
Formato de disco

7. Marque a caixa de seleção Ligar após implantação e clique em Fechar.



Pronto para concluir

A implantação pode levar vários minutos. A confirmação é exibida após a implantação bem-sucedida.



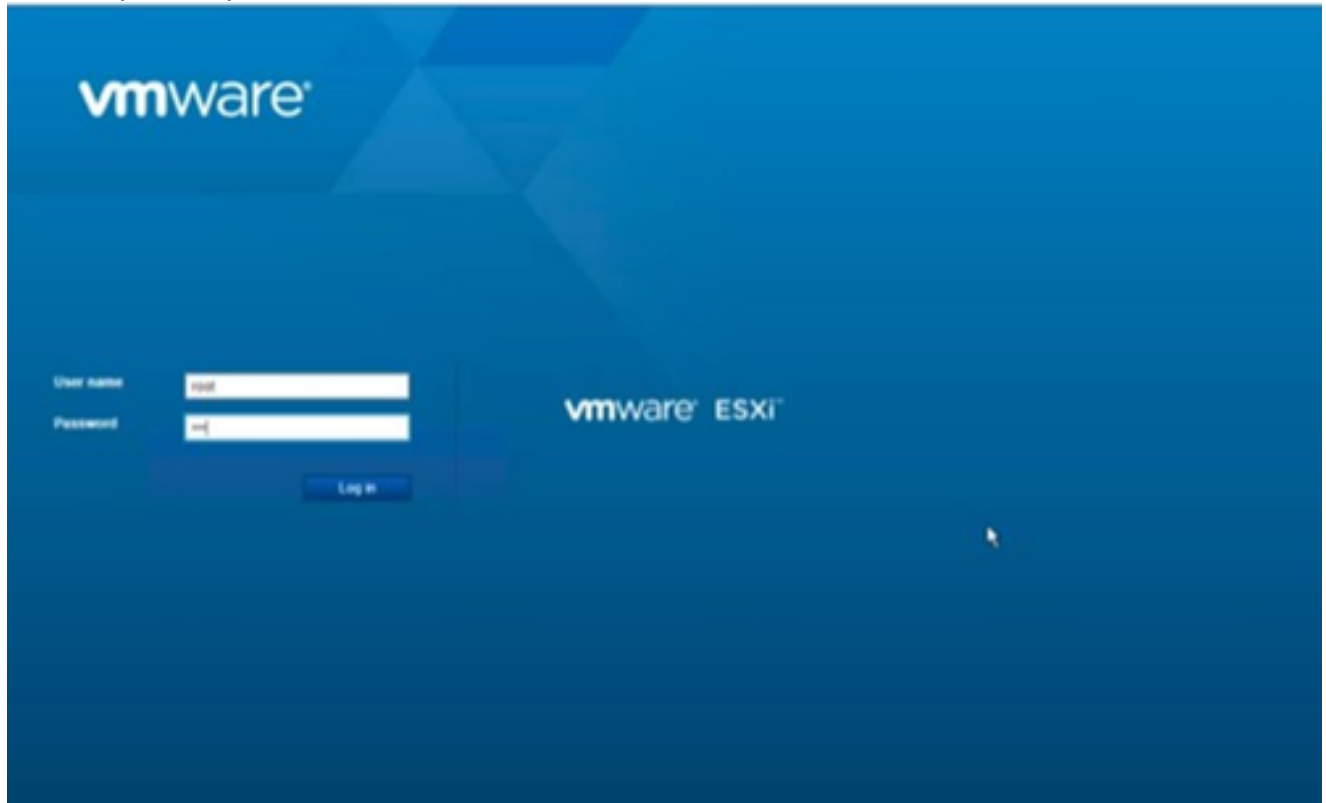
Implantação concluída

8. Selecione a VM implantada, abra o console e vá para [Network Configuration](#) para continuar com as próximas etapas.

## Instalação do Web Client ESXi 6.0

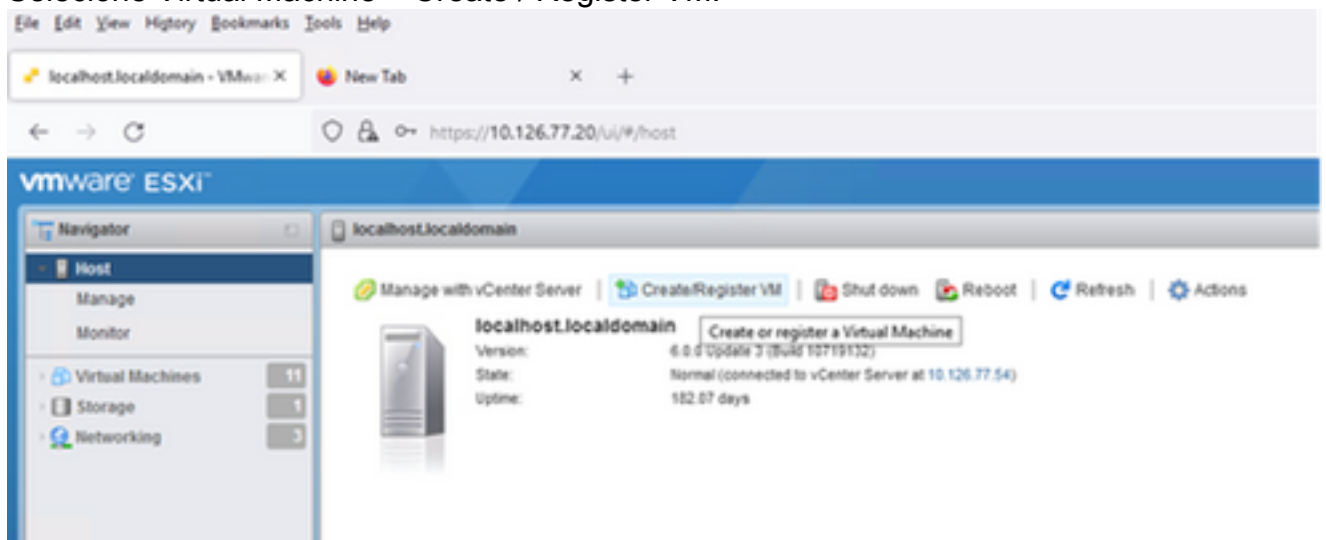
Esse cliente implanta o CX Cloud OVA usando a Web do vSphere.

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



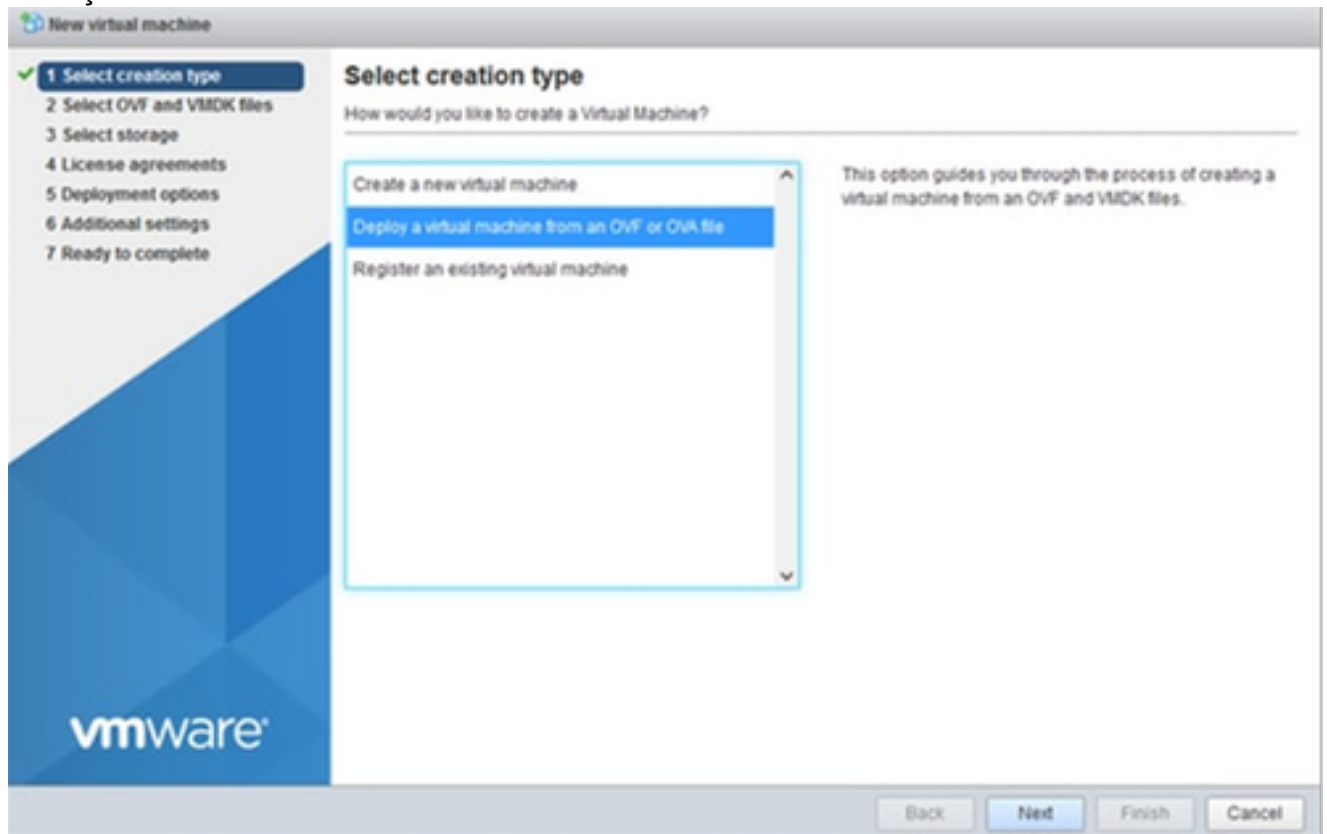
Login no VMware ESXi

2. Selecione Virtual Machine > Create / Register VM.



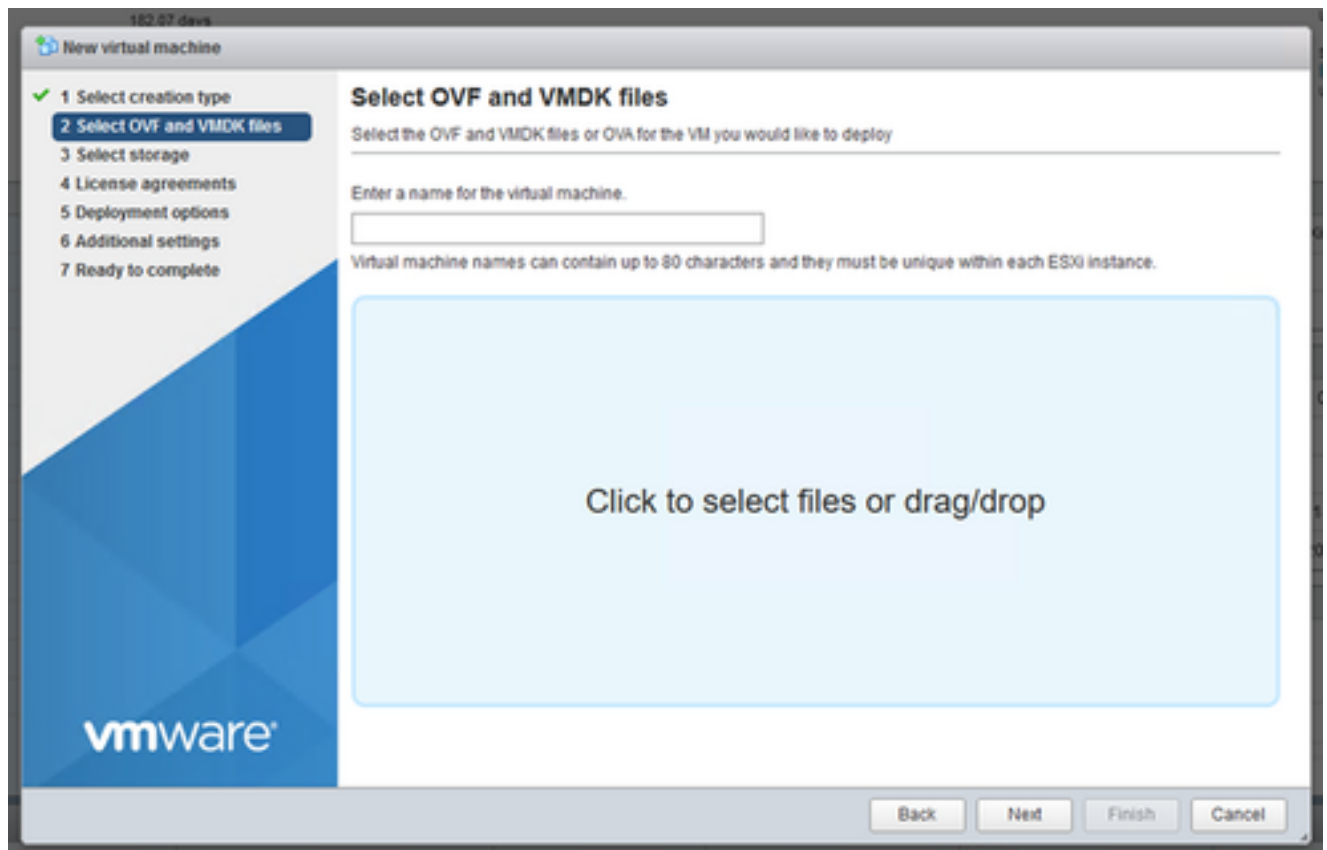
Criar VM

3. Selecione Implantar uma máquina virtual em um arquivo de OVF ou de OVA e clique em Avançar.



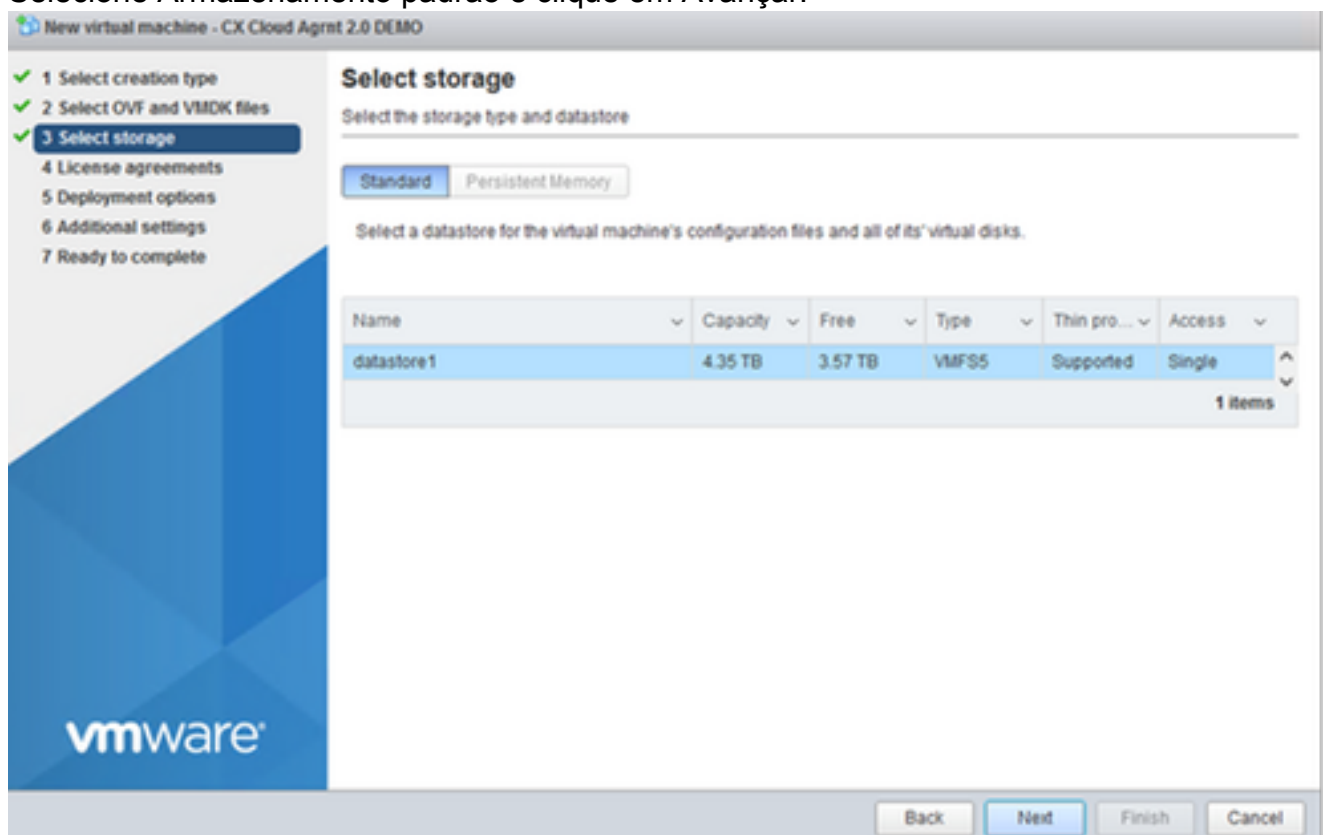
Selecionar Tipo de Criação

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. Selecione Armazenamento padrão e clique em Avançar.



Selecionar armazenamento

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

New virtual machine - CX Cloud Agent 2.0 DEMO

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

### Deployment options

Select deployment options

|                        |                                                                   |
|------------------------|-------------------------------------------------------------------|
| Network mappings       | VM Network: VM Corporate Network                                  |
| Disk provisioning      | <input checked="" type="radio"/> Thin <input type="radio"/> Thick |
| Power on automatically | <input checked="" type="checkbox"/>                               |

Back Next Finish Cancel

Opções de implantação

8. Analise as configurações e clique em Concluir.

New virtual machine - CX Cloud Agent 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

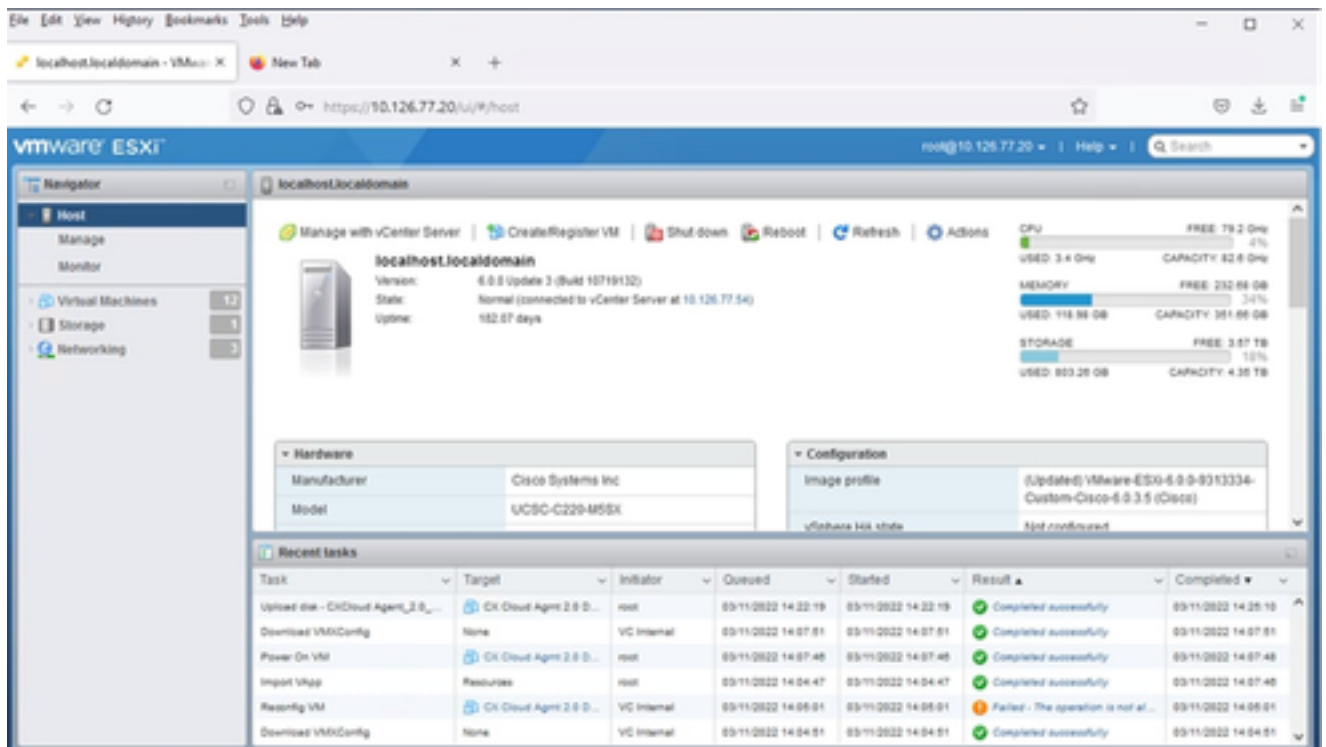
Review your settings selection before finishing the wizard

|                   |                                                     |
|-------------------|-----------------------------------------------------|
| Product           | CXCloudAgent_2.0_Build-144                          |
| VM Name           | CX Cloud Agent 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.

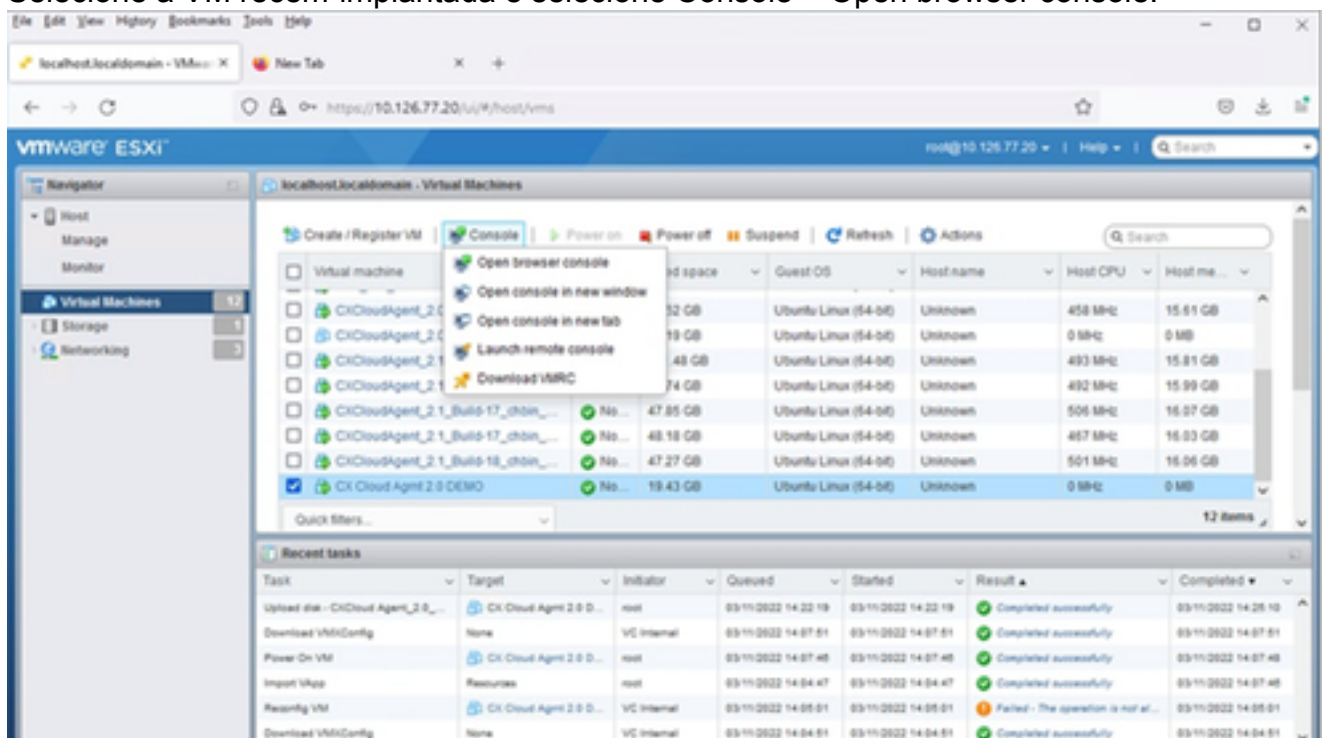
Back Next Finish Cancel

Pronto para concluir



Conclusão realizada com sucesso

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



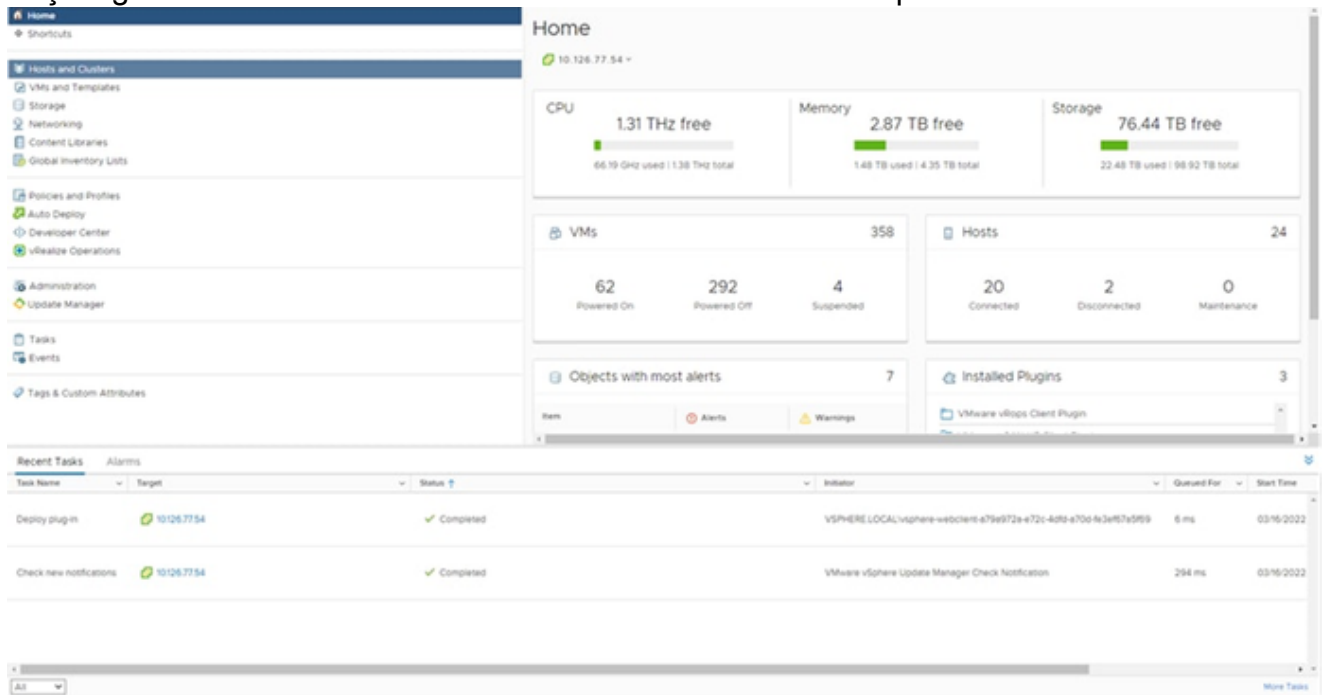
Console

## 10. Navegue até [Network Configuration](#) para continuar com as próximas etapas.

Instalação do Web Client vCenter

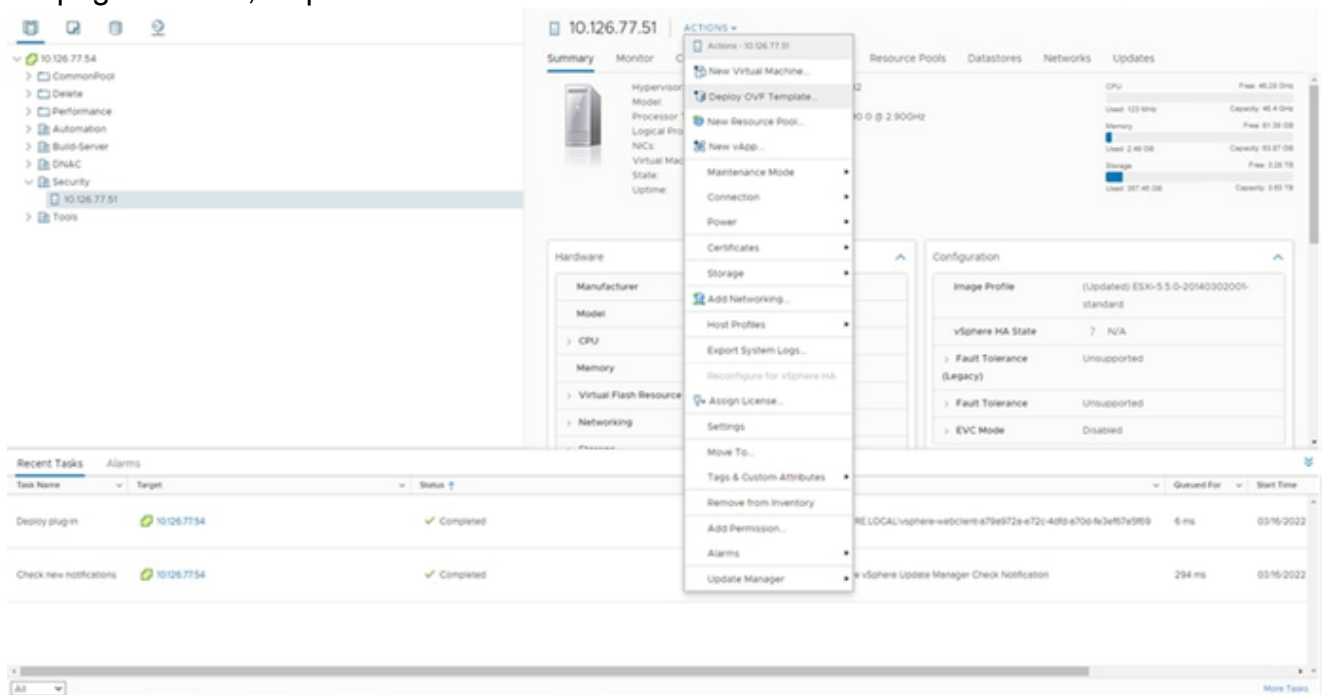
Esse cliente permite a implantação do CX Agent OVA com o uso do Web Client vCenter.

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



Página inicial

2. Na página Home, clique em Hosts e Clusters.



Hosts e clusters

3. Selecione a VM e clique em Action > Deploy OVF Template.

## 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 an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

<http> | <https> | <https://remoteserver-address/filetoinstall.ovf> | [.ova](#)

☒ Local file

Choose Files

No file chosen



Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)



CANCEL

BACK

NEXT

Implantar OVF

4. Adicione o URL diretamente ou navegue para selecionar o arquivo OVA.
5. 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\_2.3\_Build-Demo

Select a location for the virtual machine.

10.126.77.54

CommonPool

M3 - Simulator

M4

M5

HCL\_Team

Performance

Automation

Build-Server

DNAC

Security

Tools

CANCEL

BACK

NEXT

Nome e Pasta

- Insira um nome exclusivo e procure o local, se necessário.
- 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

Build-Server

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

Selecionar recurso de computação

- Selecione um recurso de computação e clique em Avançar.

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details**
- Configuration
- Select storage
- Select networks
- Ready to complete

### Review details

Verify the template details.

|               |                                                          |
|---------------|----------------------------------------------------------|
| Publisher     | TrustID EV Code Signing CA 4 (Trusted certificate)       |
| Product       | CXCloudAgent_2.3_Build-69                                |
| Version       | 2.3                                                      |
| Vendor        | Cisco Systems, Inc                                       |
| Description   | CXCloudAgent_2.3_Build-69                                |
| Download size | 1.4 GB                                                   |
| Size on disk  | Unknown (thin provisioned)<br>1.6 TB (thick provisioned) |

CANCEL
BACK
NEXT

Analisar detalhes

## 9. Analise os detalhes e clique em Avançar.

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Configuration**
- Select storage
- Select networks
- Ready to complete

### Configuration

Select a deployment configuration

☒ Small
 ☐ Medium
 ☐ Large

3 Items

**Description**

The resources consumed by this configuration are: 8 vCPUs 16GB Memory 200GB Storage Typical configuration for DNA installations.

CANCEL
BACK
NEXT

Configuração

## 10. Selecione a Configuração de distribuição e clique em Avançar.

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Configuration
- Select storage**
- Select networks
- Ready to complete

### Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Thick Provision Lazy Zeroed Default

☐ Disable Storage DRS for this

| Name          | Storage Compatibility | Capacity  | Provisioned | Free      | Type   | Cluster |
|---------------|-----------------------|-----------|-------------|-----------|--------|---------|
| datastore1 (- | --                    | 925.25 GB | 8.71 GB     | 916.54 GB | VMFS 5 |         |

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Configuração

11. Selecione Storage > Select virtual disk format na lista suspensa e clique em Next.

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Configuration
- Select storage
- Select networks**
- Ready to complete

### Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| VM Network     | VM Network          |

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Selecionar redes

12. Faça as seleções apropriadas em Select networks e clique em Next.

## Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Configuration
- Select storage
- Select networks
- Ready to complete

## Ready to complete

Review your selections before finishing the wizard

Select a name and folder

Name: CXCloudAgent\_2.3\_Build-Demo  
Template name: CXCloudAgent\_2.3\_Build-69-1\_5h4A1  
Folder: Build-Server

Select a compute resource

Resource: 10.126.77.52

Review details

Download size: 1.4 GB  
Size on disk: Unknown  
Storage mapping: 1  
All disks: Datastore: datastore1 (8); Format: Thin provision

Select storage

Size on disk: Unknown  
Storage mapping: 1  
All disks: Datastore: datastore1 (8); Format: Thin provision

Select networks

Network mapping: 1  
VM Network: VM Network  
IP allocation settings:  
IP protocol: IPV4  
IP allocation: Static - Manual

CANCEL

BACK

FINISH

Pronto para concluir

13. Revise as seleções e clique em Concluir. A página Início é exibida.

vSphere Client

10.126.77.54

CommonHost1

HCL\_Team

Performance

Automation

Build-Server

10.126.77.52

CXCloudAgent\_2.3\_Build-Demo

DNAC

Security

Tools

CXCloudAgent\_2.3\_Build-Demo

Powered Off

Guest OS: Ubuntu Linux (54-bit)

Compatibility: ESXi 5.0 and later (VM version 8)

VMware Tools: Not running, not installed

DNS Name: MORE INFO

IP Addresses: Host: 10.126.77.52

LAUNCH WEB CONSOLE

LAUNCH REMOTE CONSOLE

VM Hardware

CPU: 8 CPU(s)

Memory: 16 GB, 0 GB memory active

Notes

CXCloudAgent\_2.3\_Build-69

Edit Notes...

Summary

Monitor

Configure

Permissions

Datastores

Networks

Snapshots

Updates

SWITCH TO NEW VIEW

CPU USAGE: 0 Hz

MEMORY USAGE: 0 B

STORAGE USAGE: 1.45 KB

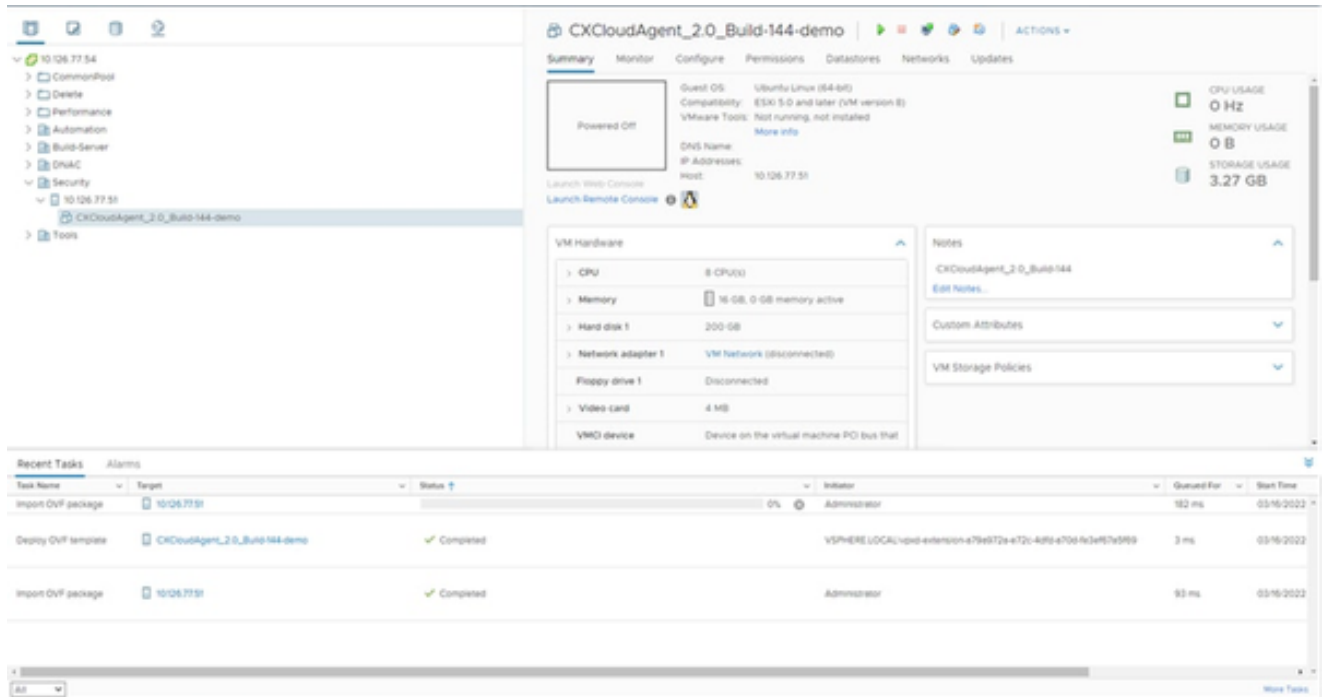
Recent Tasks

Alarms

| Task Name           | Target       | Status    | Details                       | Initiator                      | Elapsed For | Start Time             | Completion Time        |
|---------------------|--------------|-----------|-------------------------------|--------------------------------|-------------|------------------------|------------------------|
| Deploy OVF template | 10.126.77.52 | Completed | Copying Virtual Machine co... | VSPHERE.LOCAL/vspix-extensi... | 6 ms        | 12/15/2023, 3:42:46 AM | 12/15/2023, 3:49:04 AM |
| Import OVF package  | 10.126.77.52 | Completed |                               | vsphere.local/Administrator    | 87 ms       | 12/15/2023, 3:42:19 AM | 12/15/2023, 3:49:04 AM |

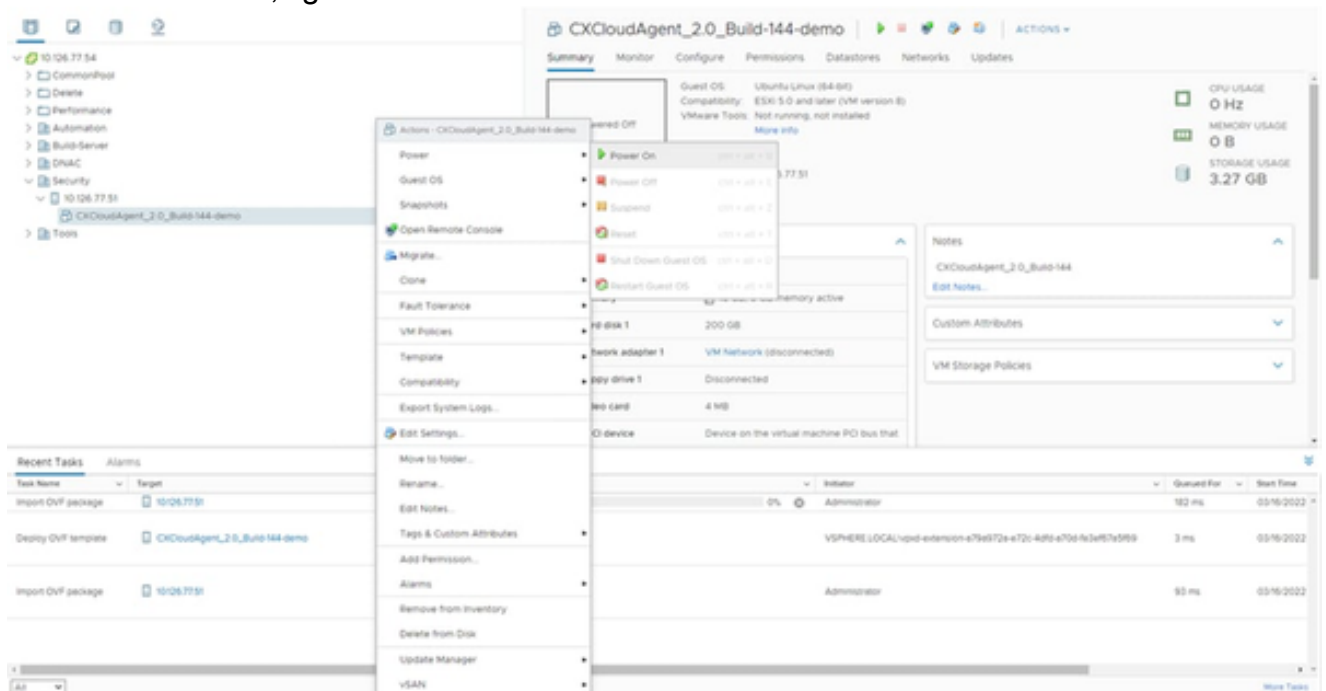
VM adicionada

14. Clique na VM recém-adicionada para exibir o status.



VM adicionada

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



Abrir console

16. Navegue até [Network Configuration](#) para prosseguir com as próximas etapas.

## Instalação do Oracle Virtual Box 7.0.12

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

1. Baixe o CXCloudAgent\_3.1 OVA na caixa de janelas para qualquer pasta.
2. Navegue até a pasta usando a interface de linha de comando.

3. Descompacte o arquivo OVA usando o comando tar -xvf D:\CXCloudAgent\_3.1\_Build-xx.oVA.

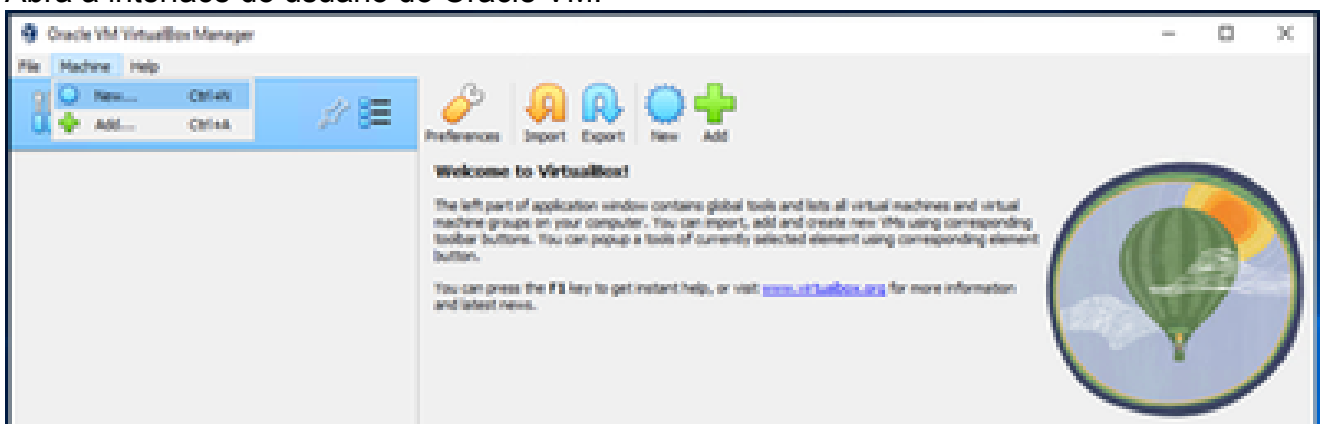
```
D:\>cd CXCAGENT

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

D:\CXCAGENT>_
```

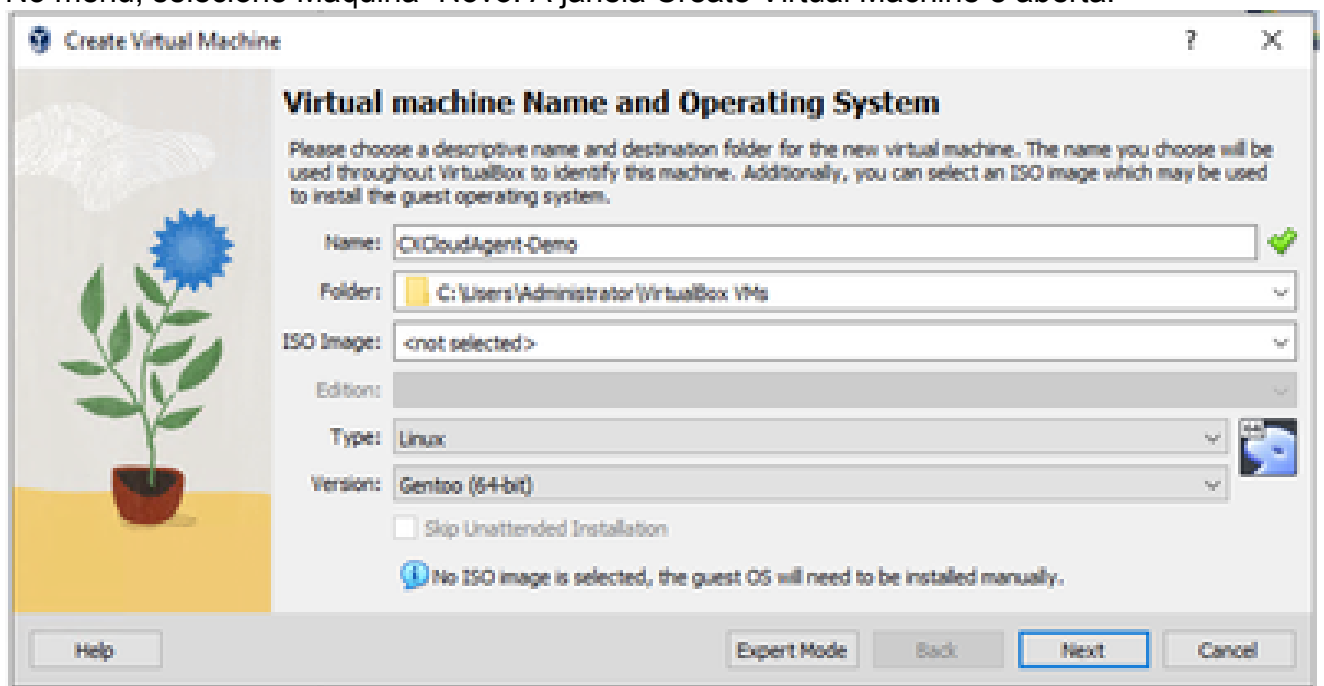
Descompactar arquivo OVA

4. Abra a interface do usuário do Oracle VM.



Oracle VM

5. No menu, selecione Máquina>Novo. A janela Create Virtual Machine é aberta.



Criar Máquina Virtual

6. Insira os seguintes detalhes na janela Nome da máquina virtual e Sistema operacional.

Nome: Nome da VM

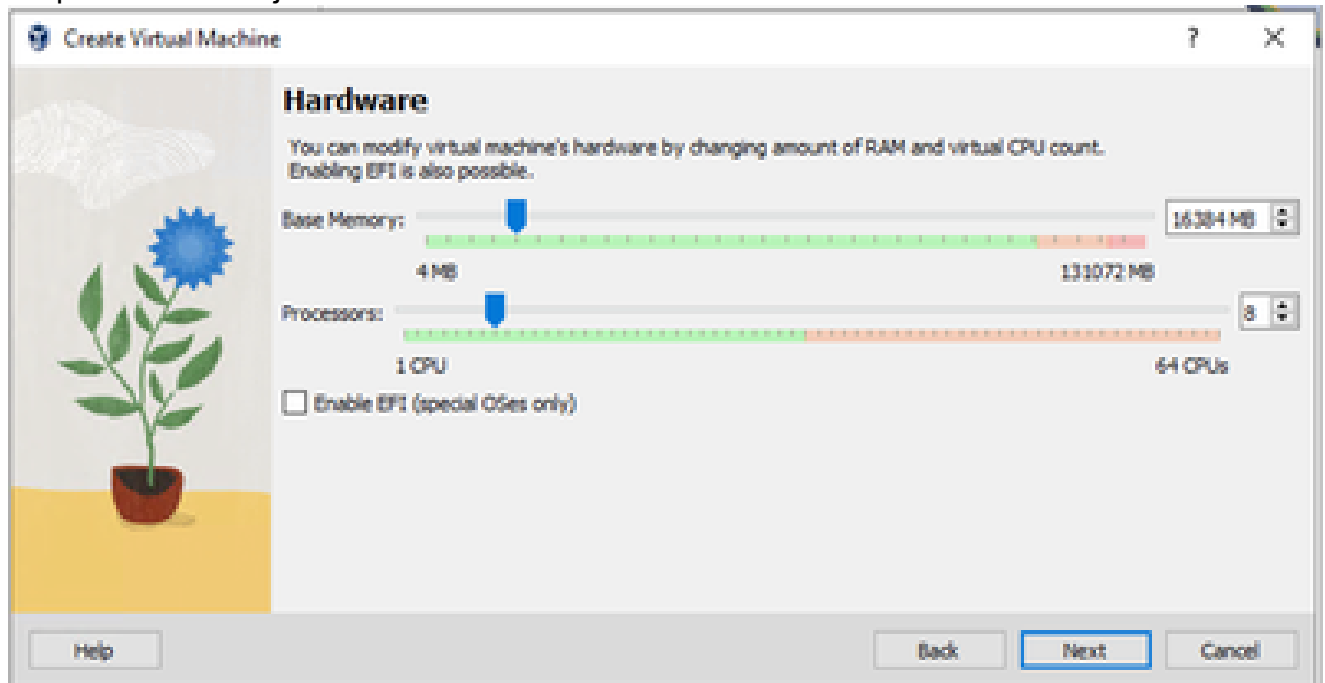
Pasta: Local onde os dados da VM serão armazenados

Imagem ISO: nenhum

Digite: Linux

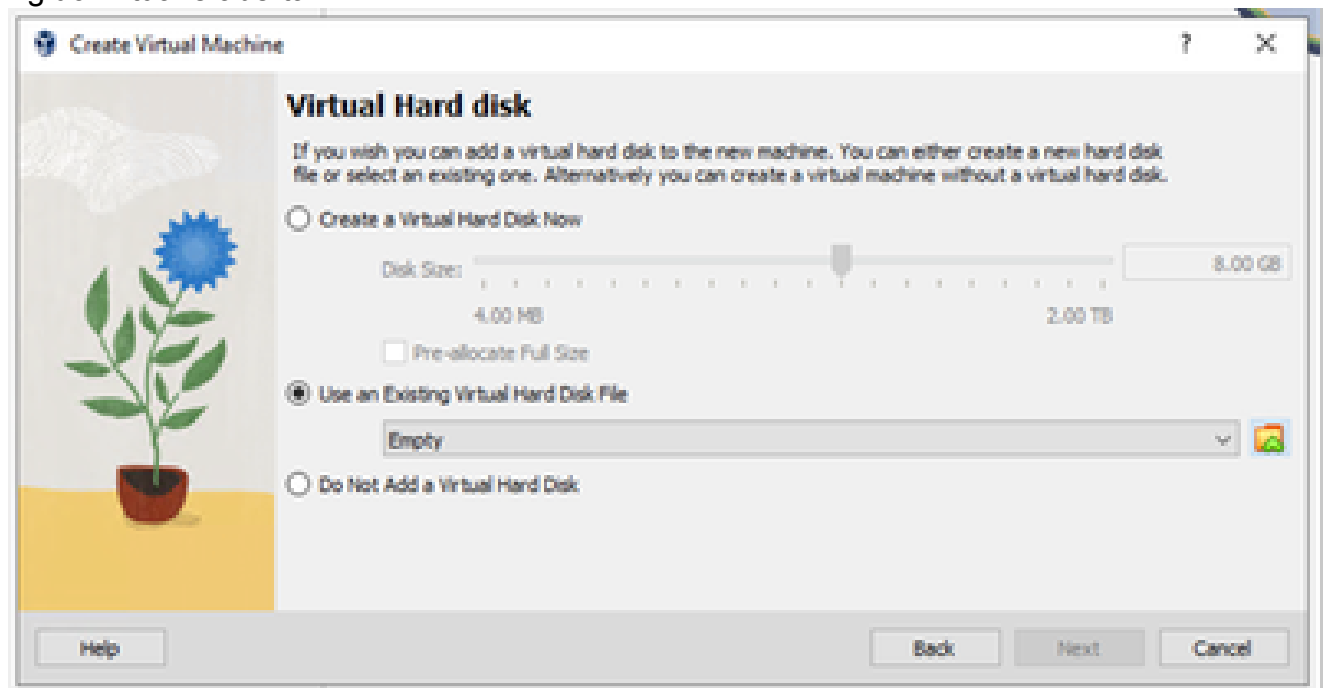
Versão: Gentoo (64 bits)

7. Clique em Next. A janela Hardware se abre.



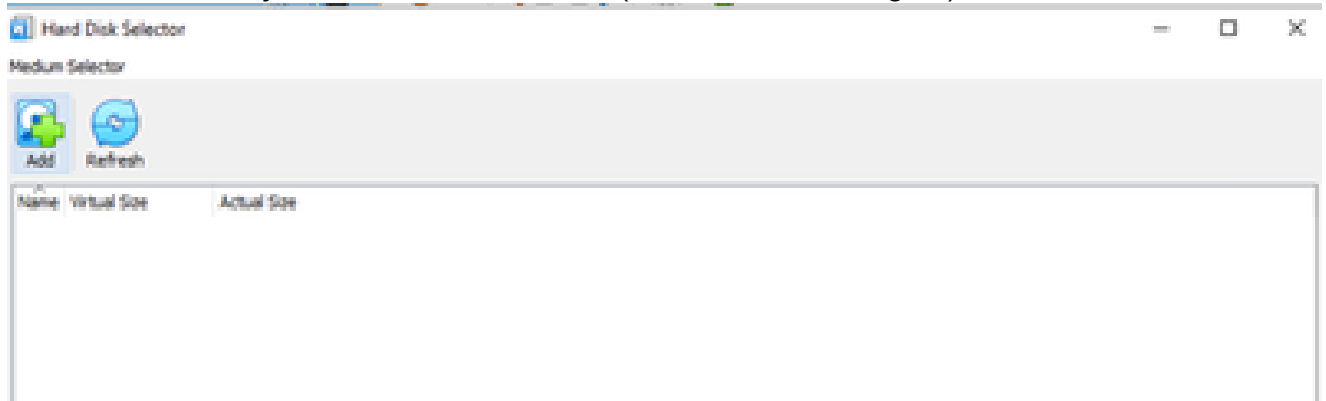
Hardware

8. Insira Base Memory (16384 MB) e Processors (8 CPUs) e clique em Next. A janela Disco rígido virtual é aberta.



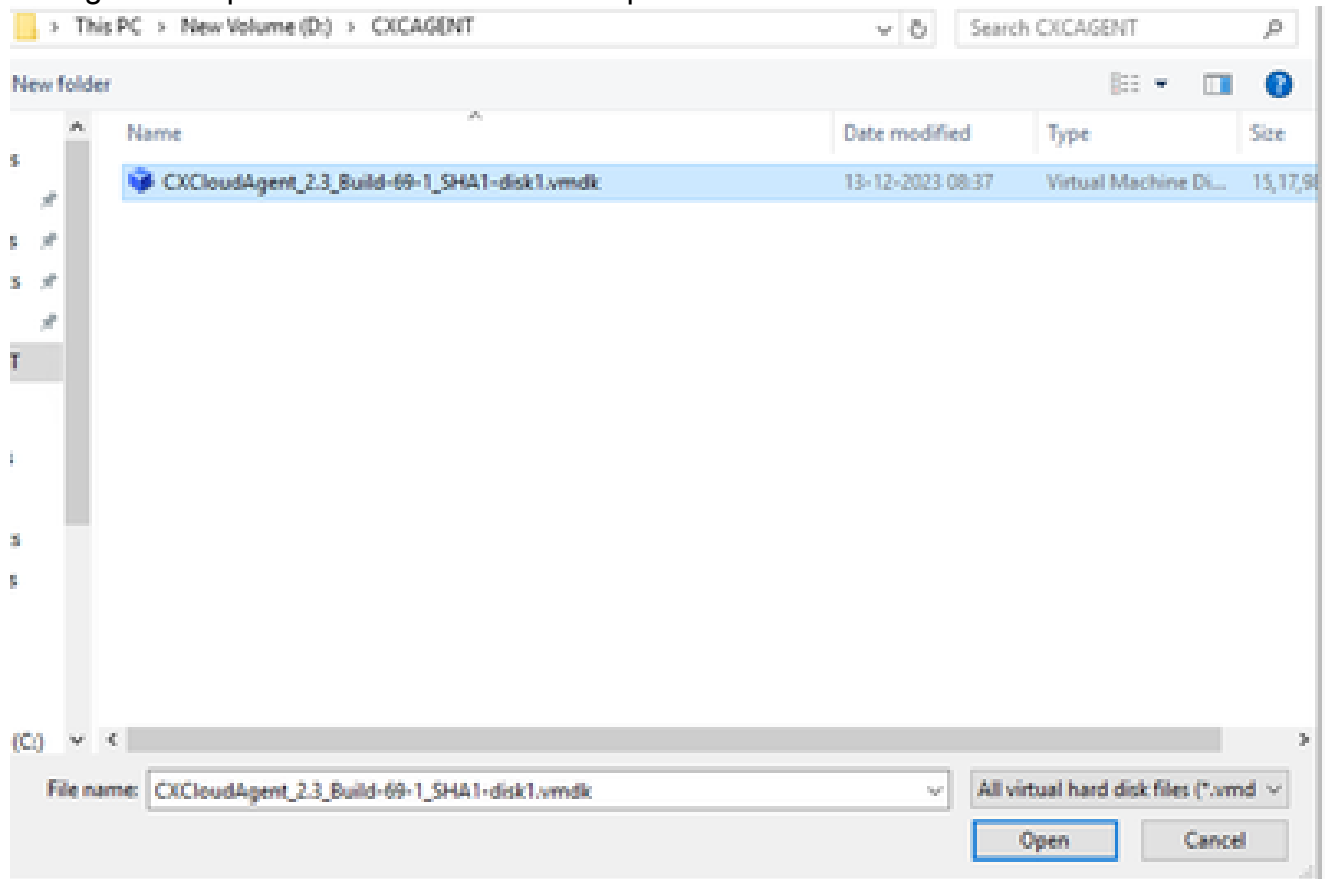
Disco rígido virtual

9. Selecione o botão de opção Usar um arquivo de disco rígido virtual existente e selecione o ícone Procurar. A janela Hard Disk Seletor (Seletor de disco rígido) é aberta.



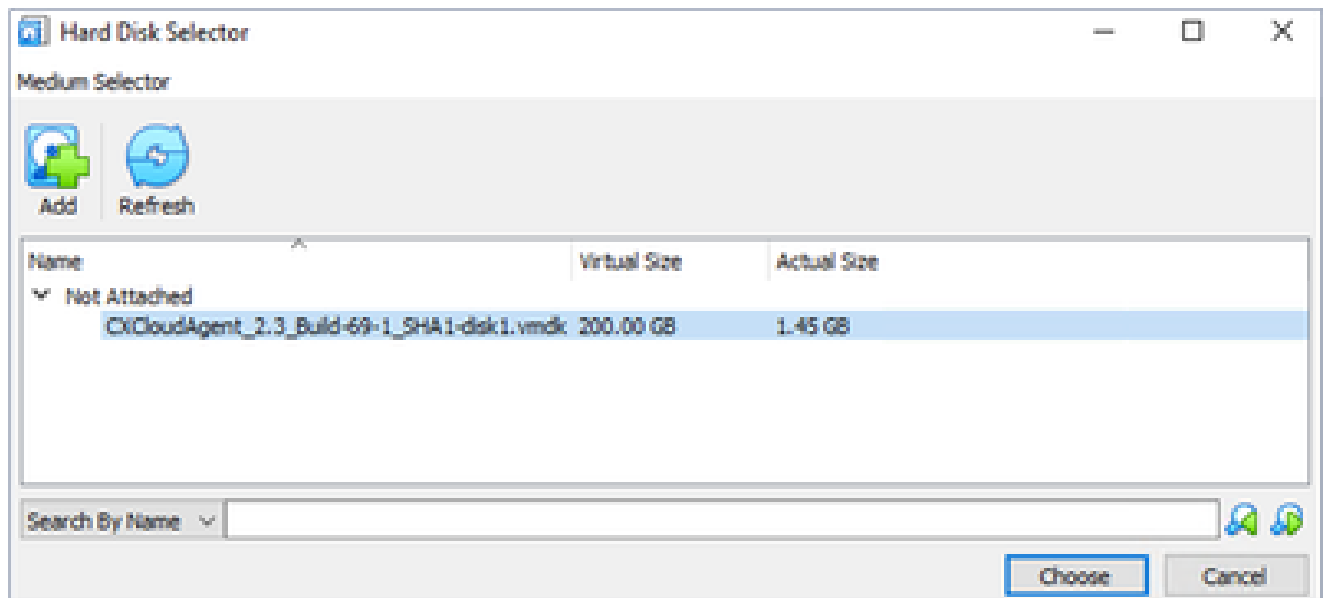
Seletor de disco rígido

10. Navegue até a pasta OVA e selecione o arquivo VMDK.



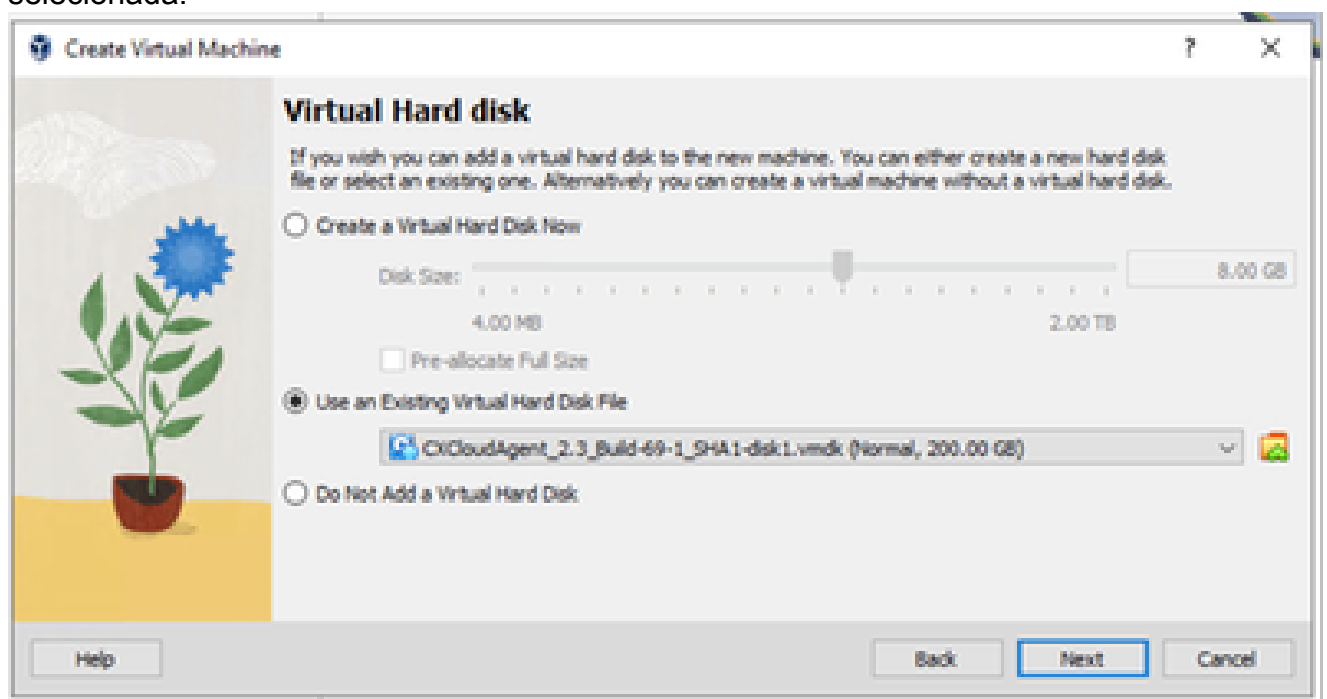
Pasta OVA

11. Clique em Abrir. O arquivo é exibido na janela Hardware Disk Seletor.



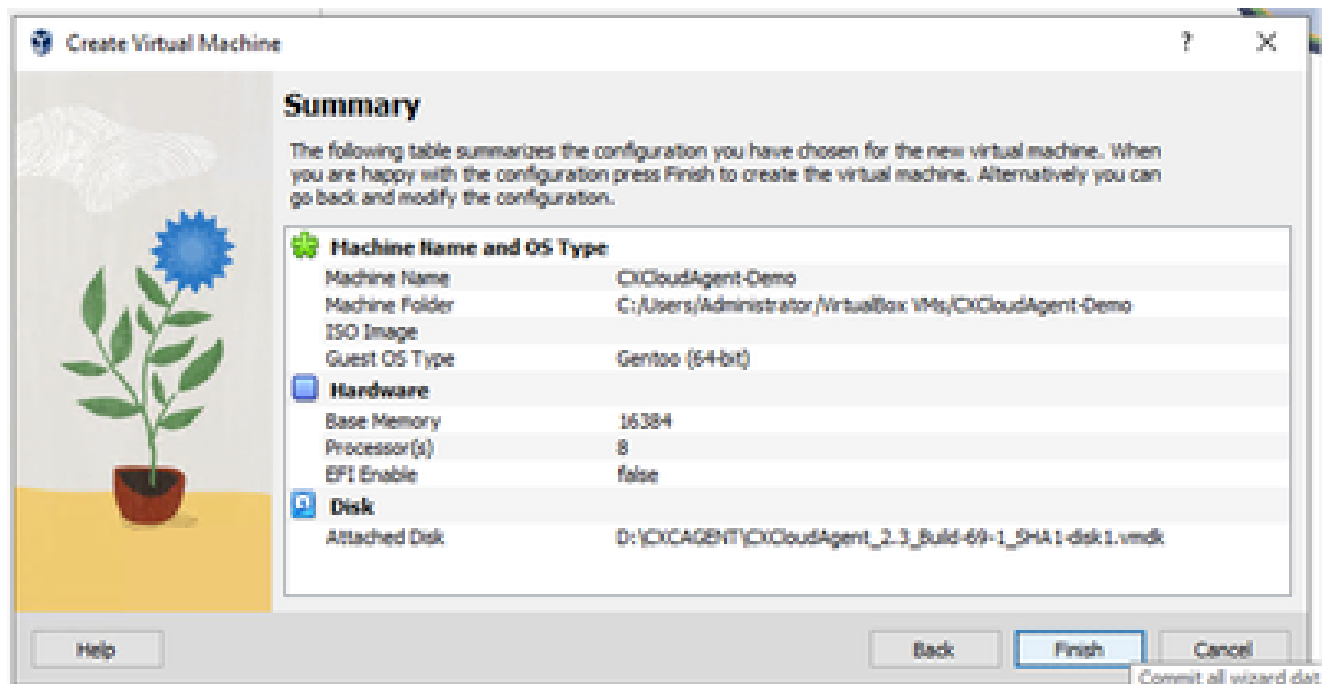
Seletor de disco rígido

12. Clique em Escolher. A janela Disco rígido virtual é aberta. Confirme se a opção exibida está selecionada.



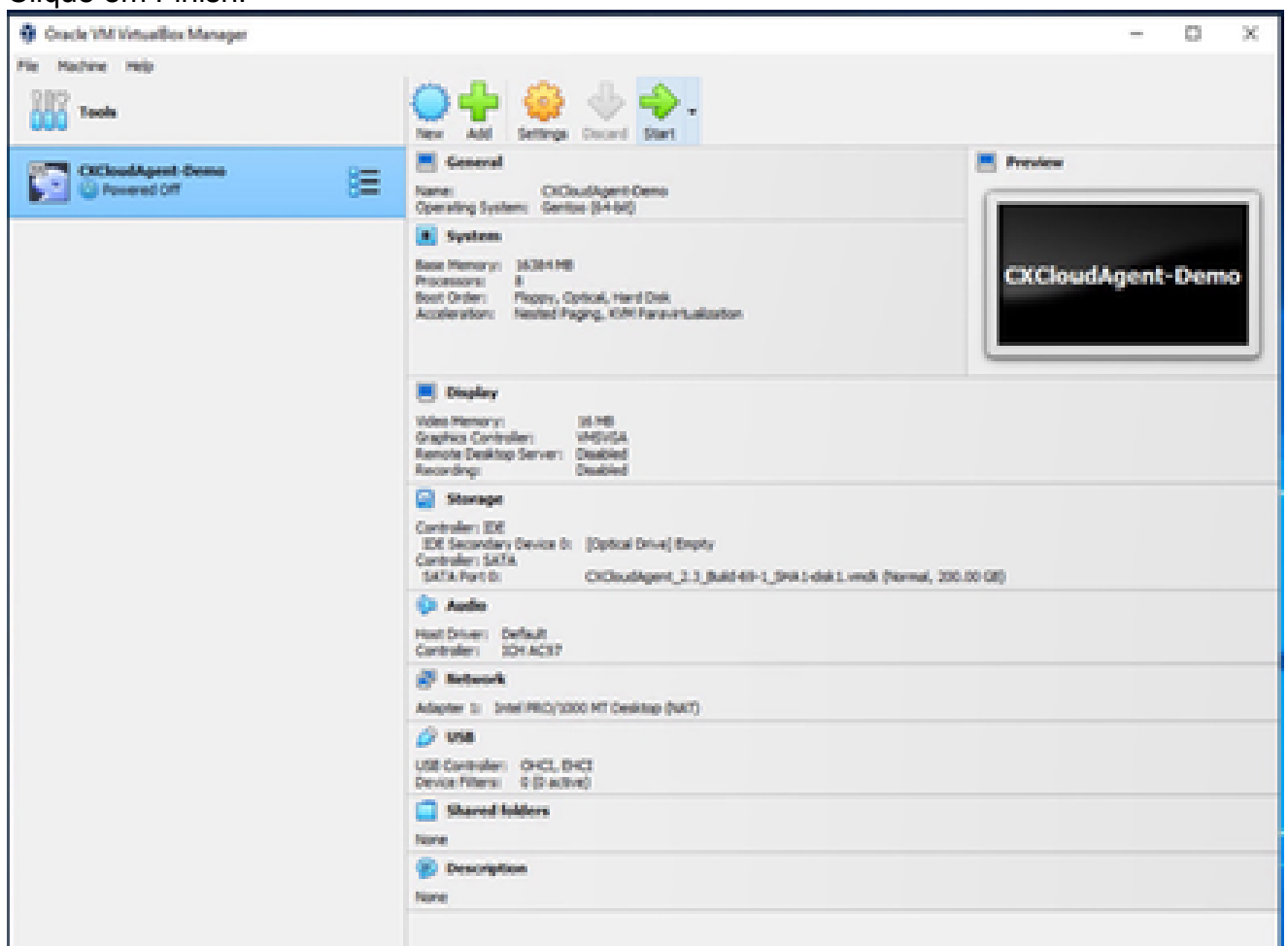
Selecionar arquivo

13. Clique em Next. A janela Resumo é aberta.



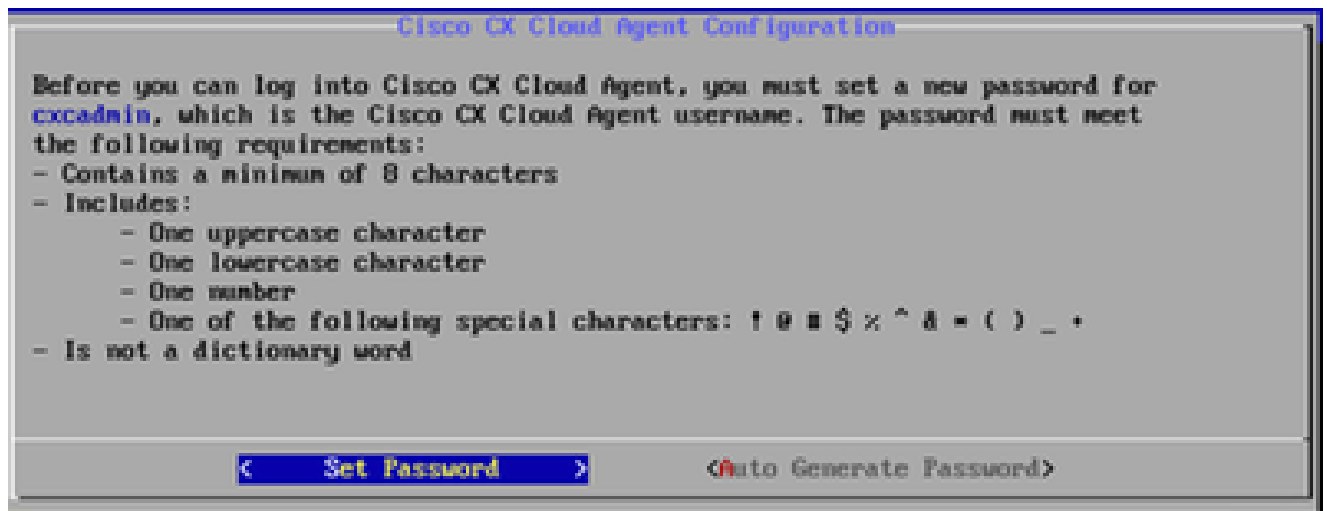
Summary

#### 14. Clique em Finish.



Inicialização do console da VM

#### 15. Selecione a VM implantada e clique em Iniciar. A VM é ligada e a tela do console é exibida para configuração.



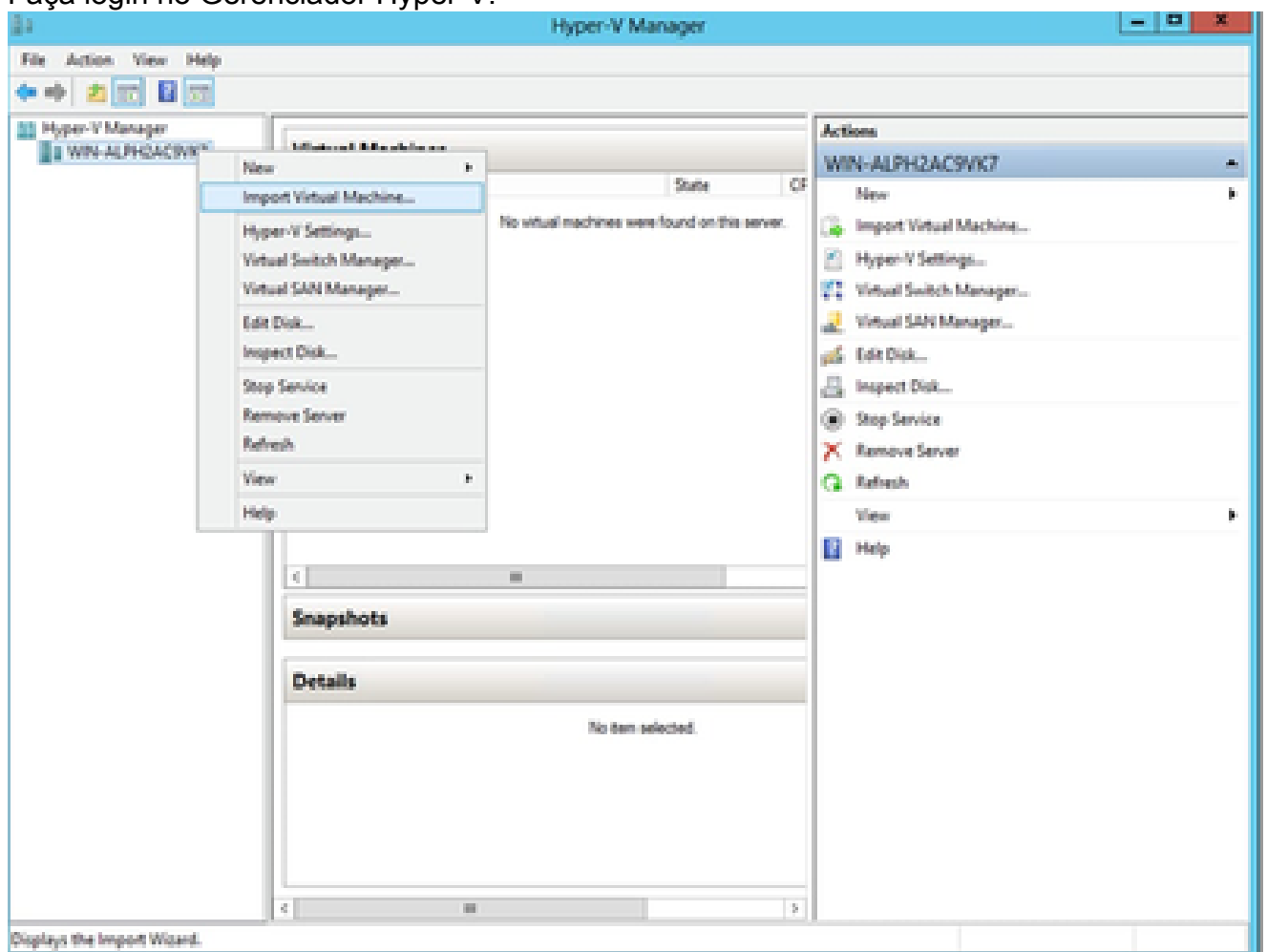
Abrir o console

16. Navegue até [Network Configuration](#) para continuar com as próximas etapas.

## Instalação do Microsoft Hyper-V

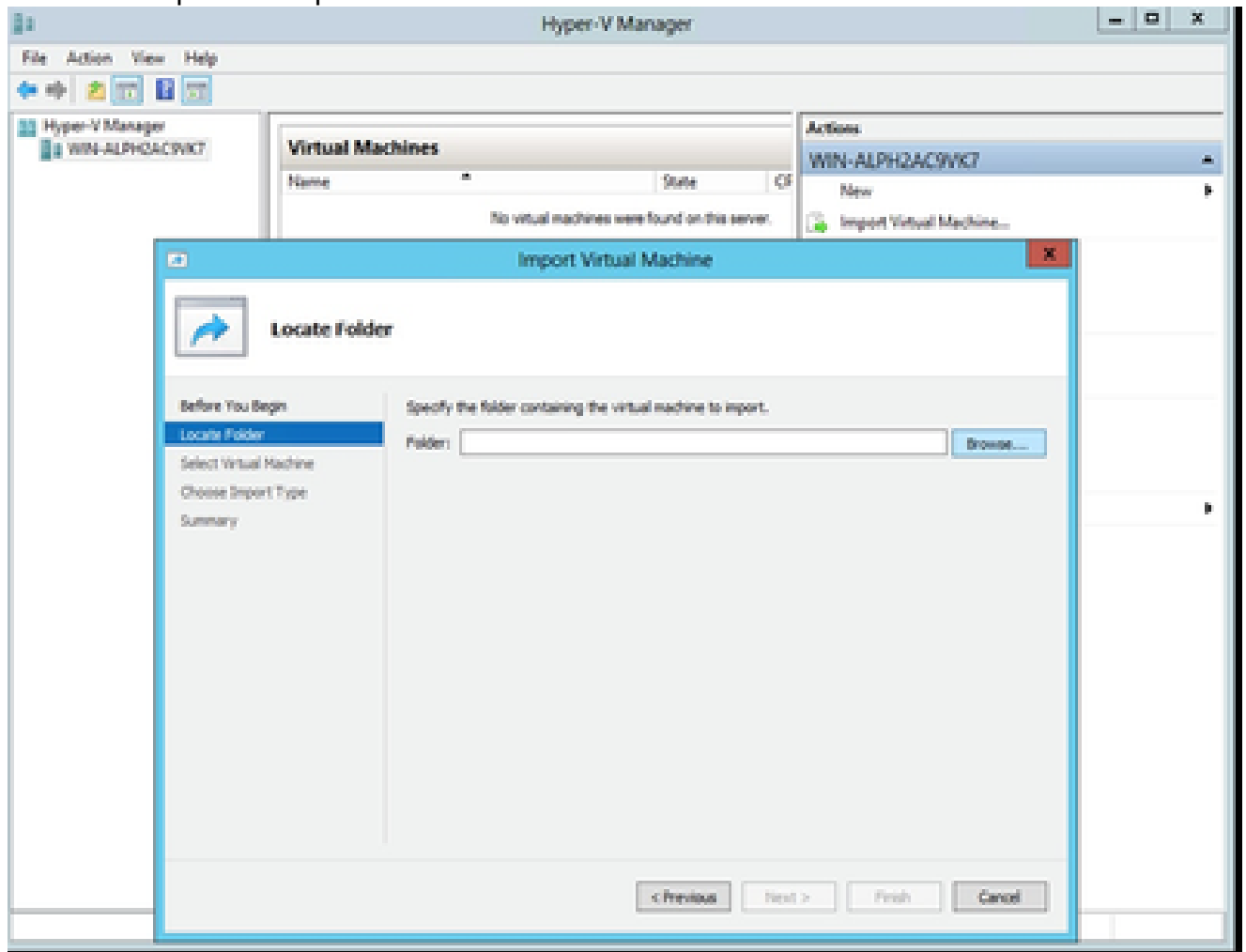
Esse cliente implanta o CX Agent OVA por meio da instalação do Microsoft Hyper-V.

1. Faça login no Gerenciador Hyper-V.



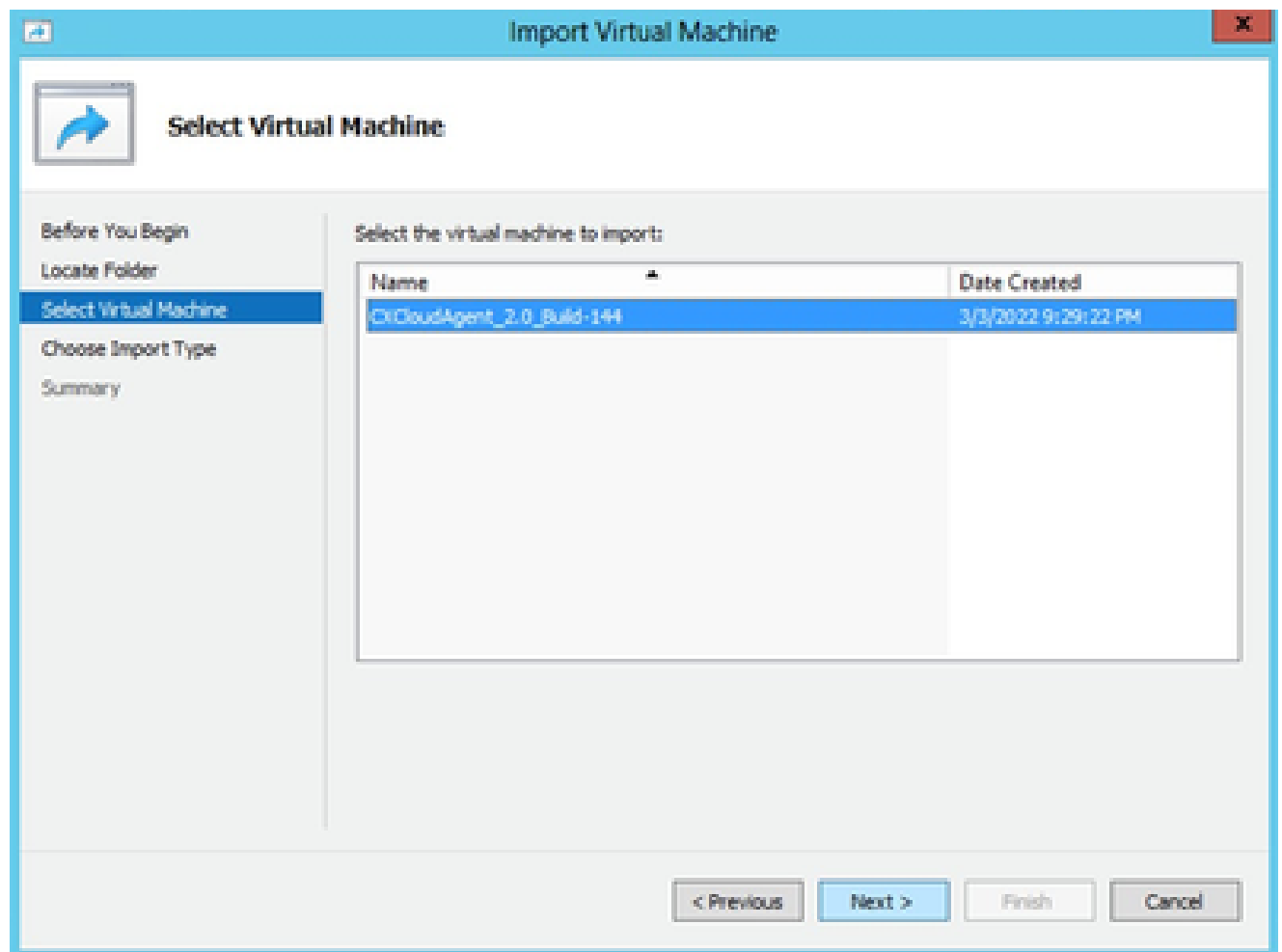
Gerenciador Hyper V

2. Selecione a VM de destino, clique com o botão direito do mouse para abrir o menu e selecione Importar máquina virtual.



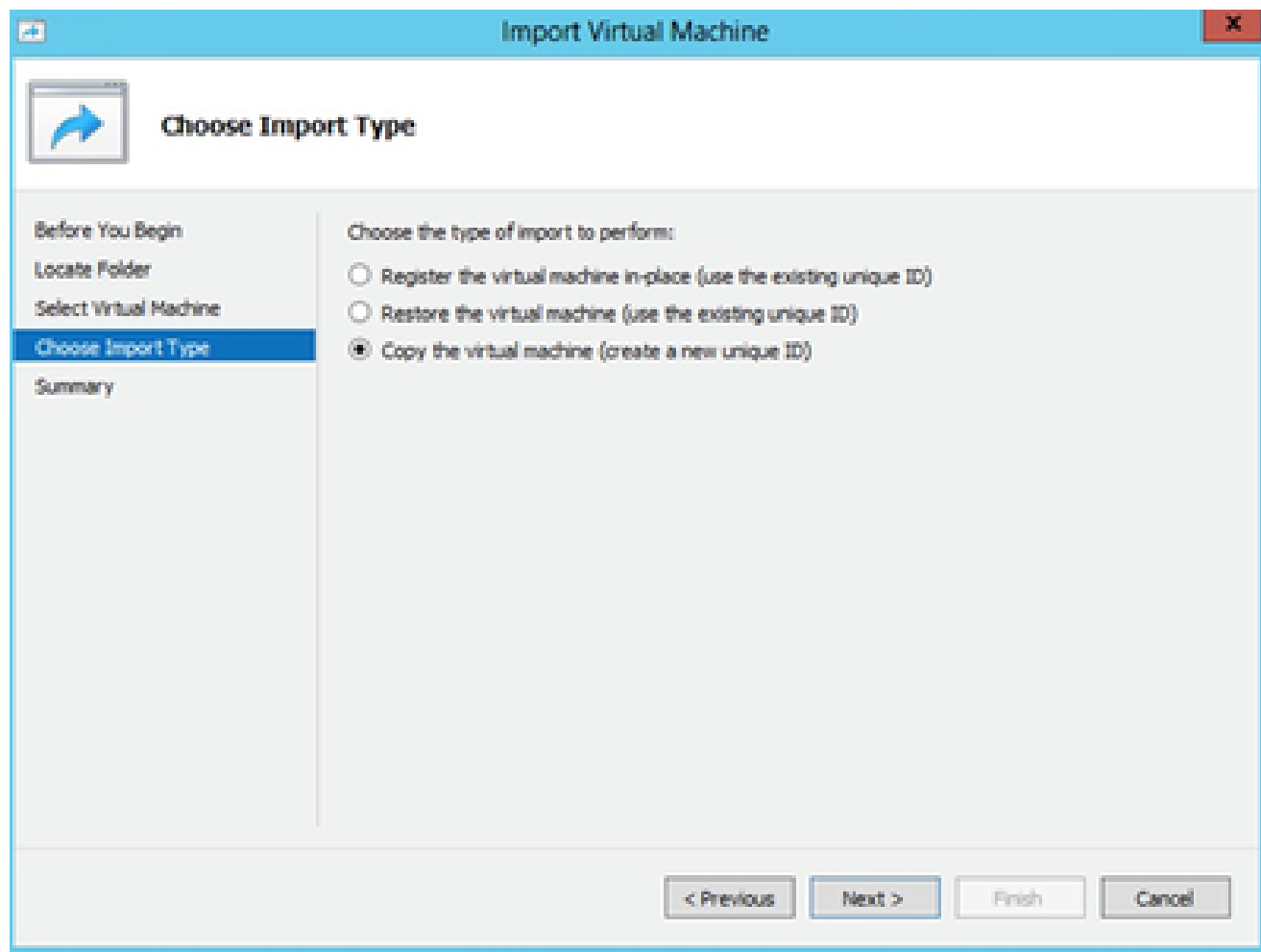
Pasta para importar

3. Procure e selecione a pasta de download e clique em Avançar.



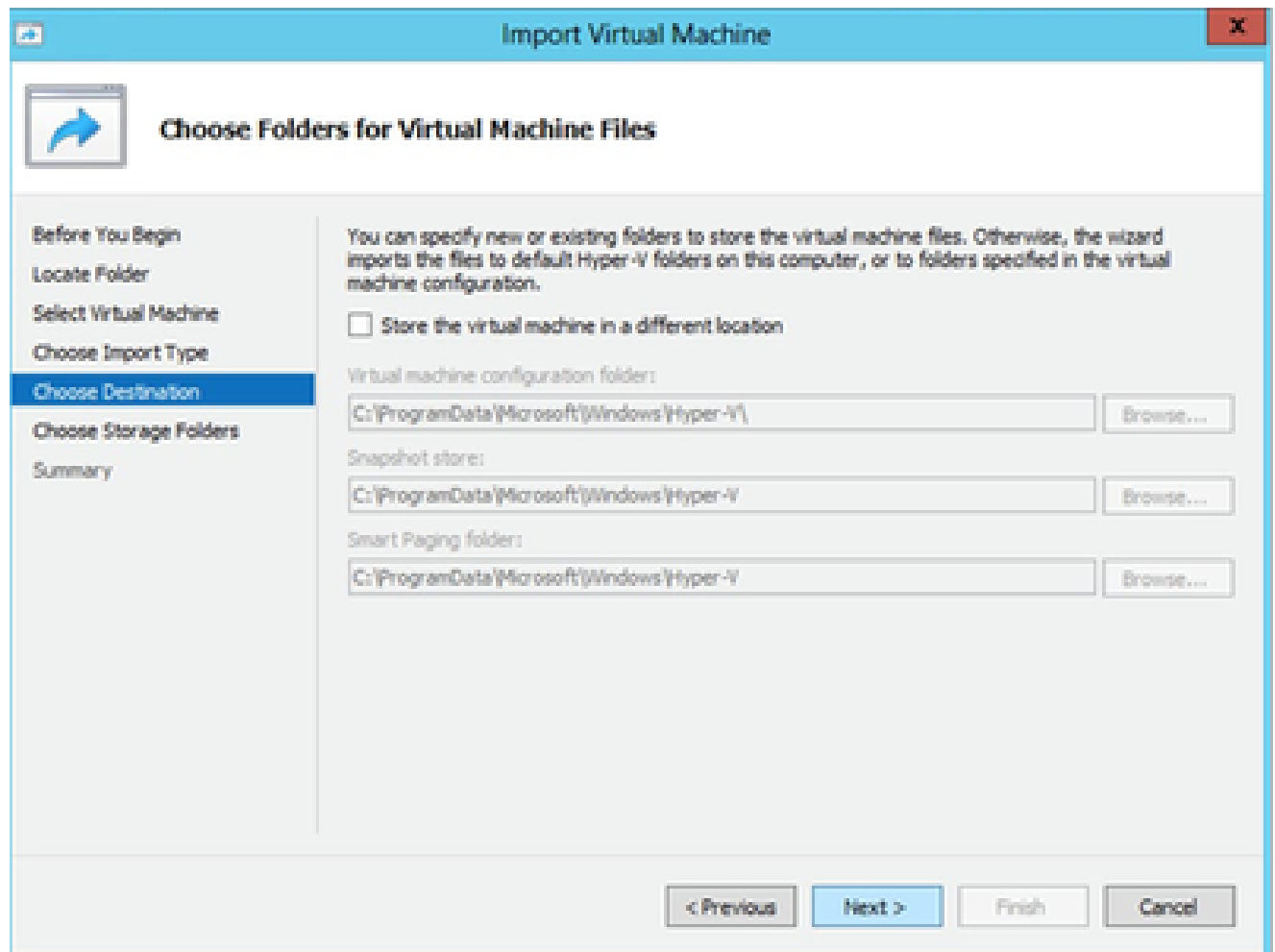
Selecionar VM

4. Selecione a VM e clique em Avançar.



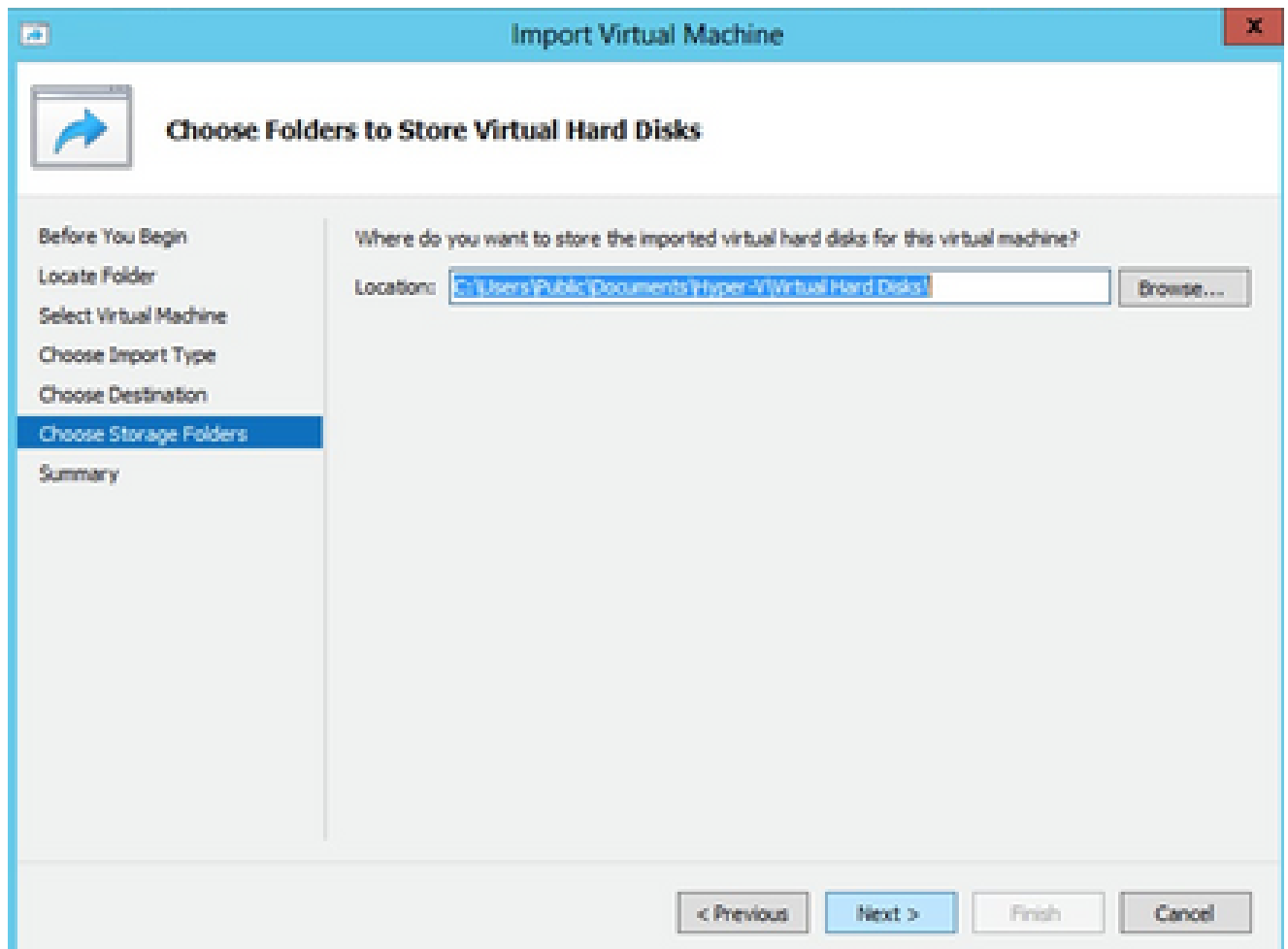
Tipo de importação

5. Selecione o botão de opção Copy the virtual machine (create a new unique ID) (Copiar a máquina virtual (criar uma nova ID exclusiva)) e clique em Next.



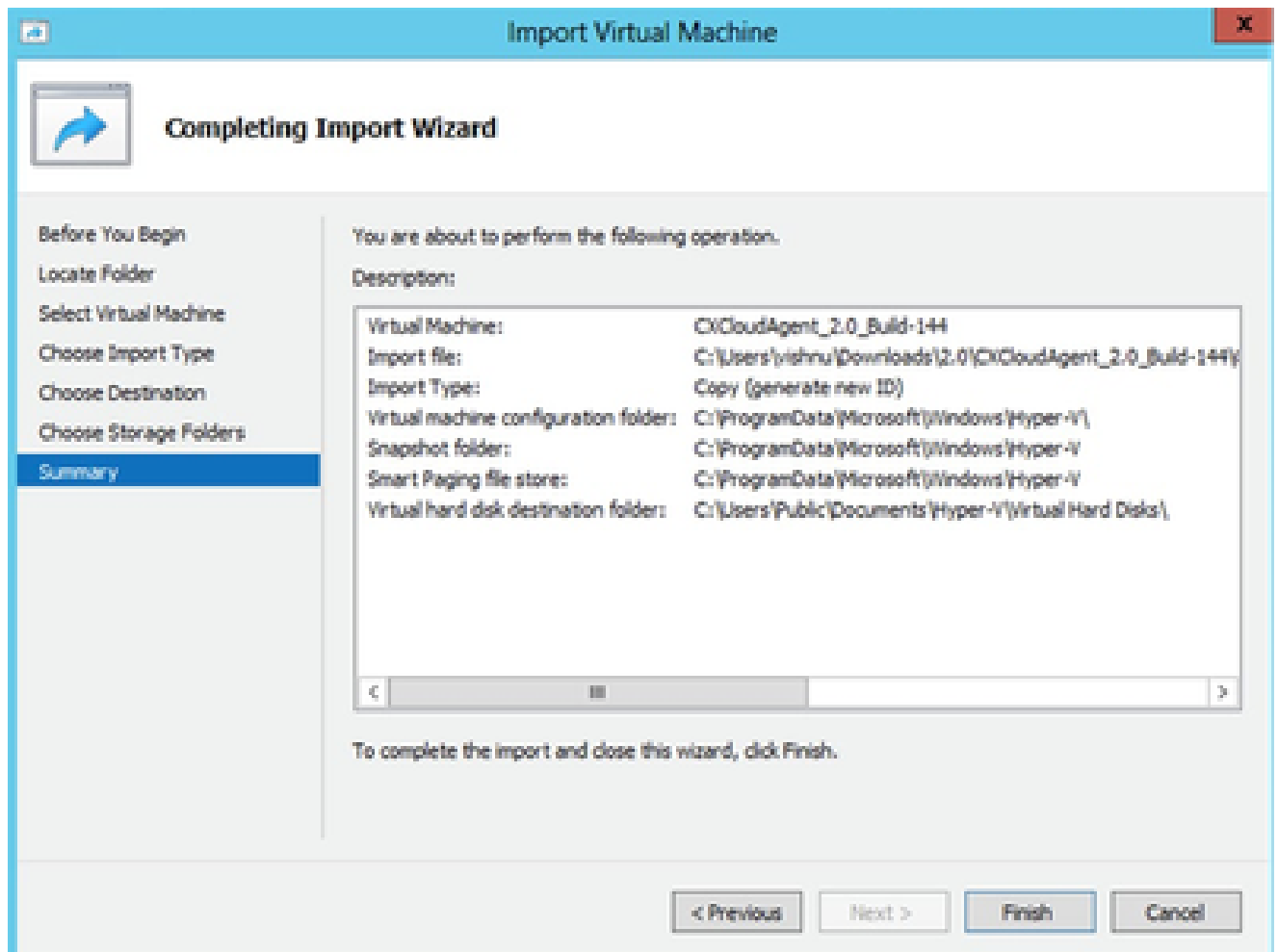
Escolher Pastas para Arquivos de Máquina Virtual

6. Navegue para seleccionar a pasta para arquivos de VM. A Cisco recomenda o uso dos caminhos padrão.
7. Clique em Next.



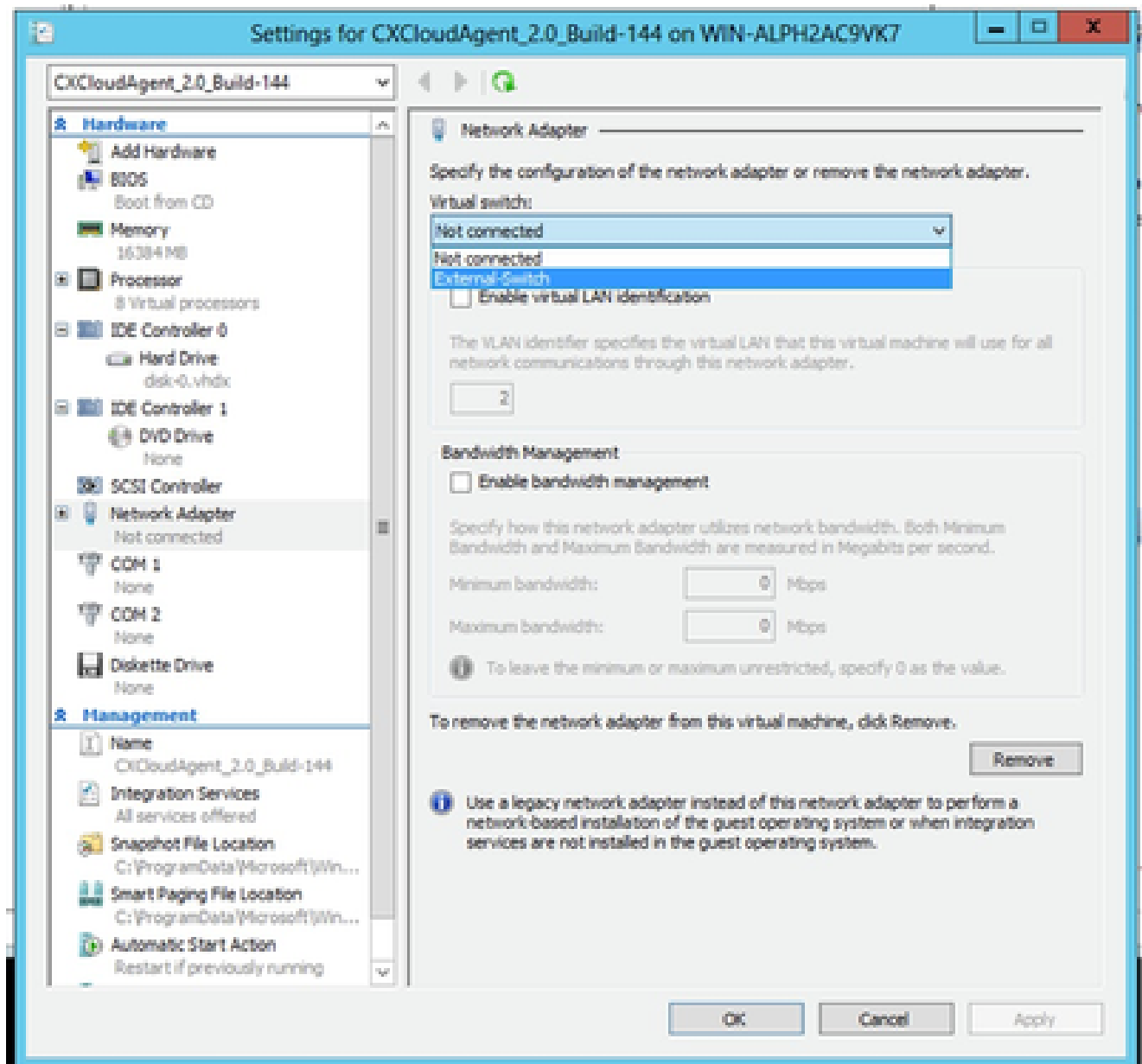
Pasta para armazenar os discos rígidos virtuais

8. Procure e selecione a pasta para armazenar os discos rígidos da VM. A Cisco recomenda o uso dos caminhos padrão.
9. Clique em Next. O resumo da VM é exibido.



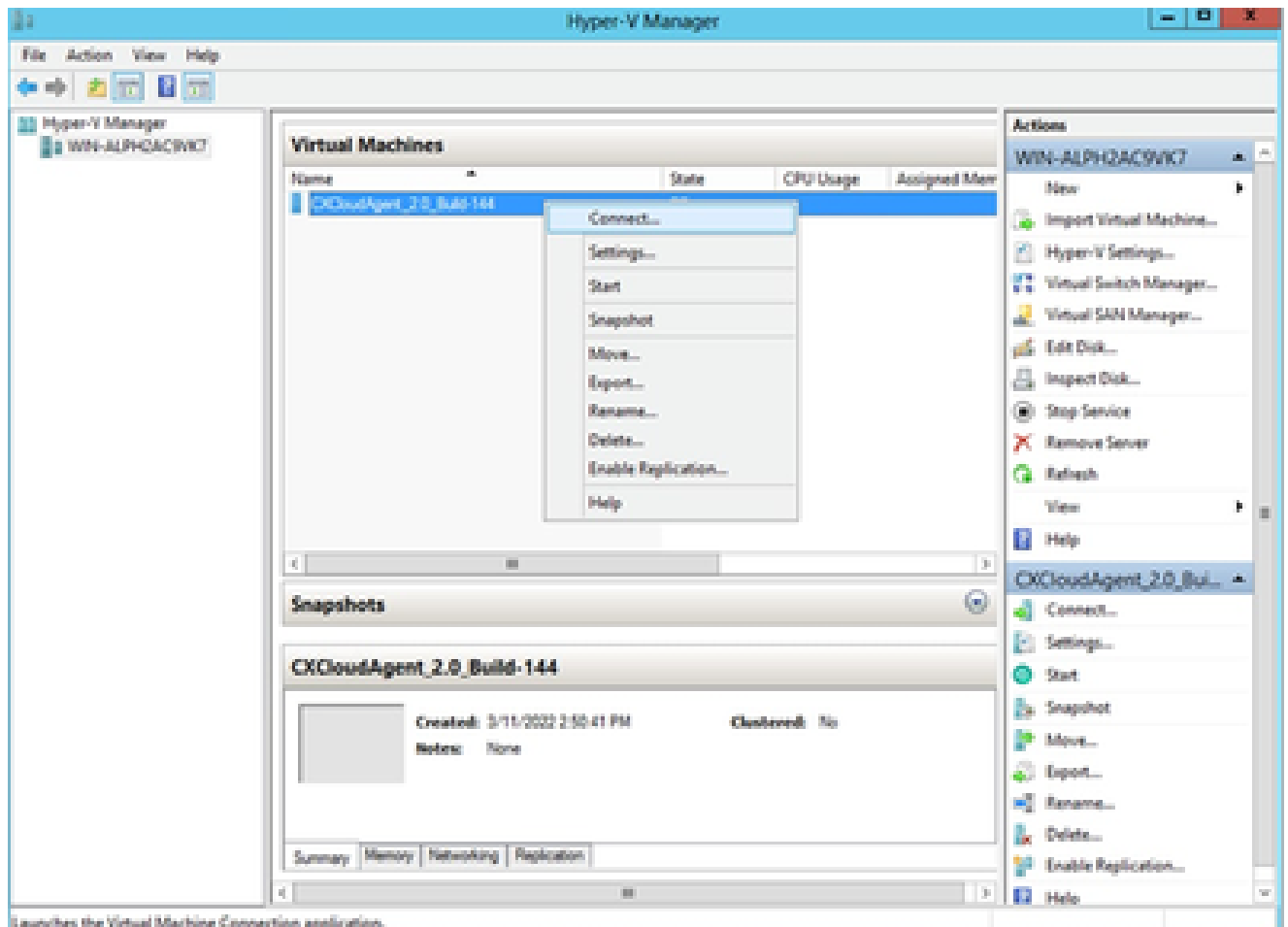
Summary

10. Verifique todas as entradas e clique em Finish.
11. Quando a importação for concluída com êxito, uma nova VM será criada no Hyper-V. Abra as configurações da VM.



Switch Virtual

12. Selecione o Adaptador de rede no painel esquerdo e selecione o Comutador virtual disponível na lista suspensa.

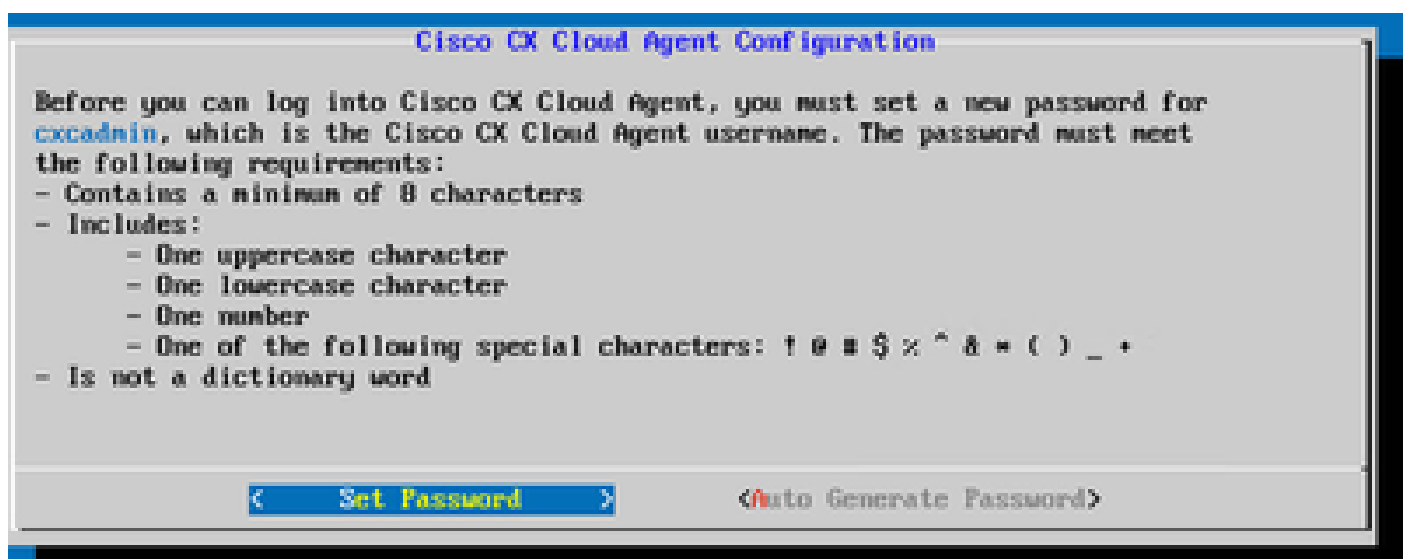


Inicialização da VM

13. Selecione Connect para iniciar a VM.
14. Navegue até [Network Configuration](#) para continuar com as próximas etapas.

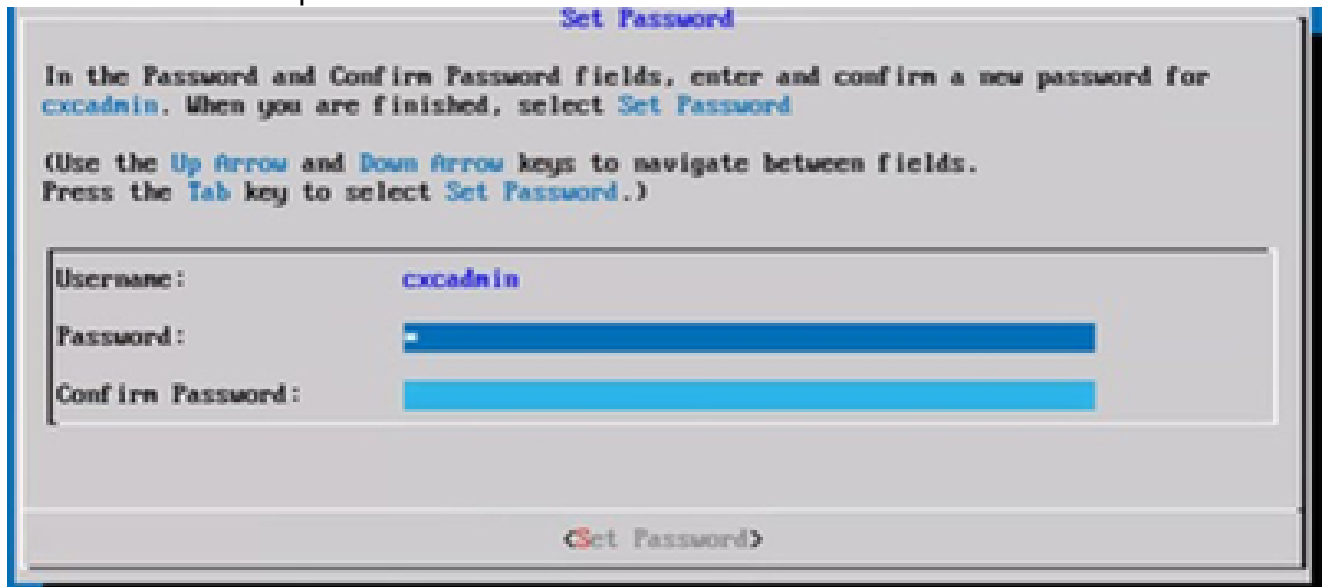
## Configuração de rede

Para definir a senha do CX Cloud Agent para o nome de usuário cxcadmin:



Definir senha

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



The 'Set Password' dialog box contains instructions: 'In the Password and Confirm Password fields, enter and confirm a new password for cxcadmin. When you are finished, select Set Password. (Use the Up Arrow and Down Arrow keys to navigate between fields. Press the Tab key to select Set Password.)'. It features three input fields: 'Username:' with the value 'cxcadmin', 'Password:', and 'Confirm Password:'. The bottom of the dialog has a 'Set Password' button.

Nova senha

2. Se Definir senha estiver selecionado, digite a senha para cxcadmin e confirme. Clique em Definir senha e vá para a Etapa 3.  
OU

Se Gerar senha automaticamente estiver selecionado, copie a senha gerada e armazene-a para uso futuro. Clique em Salvar senha e vá para a Etapa 4.



The 'Autogenerated Password' dialog box displays a password 'XXXXXXXXXX' with the first character masked. It includes instructions: 'Make sure to store this password in a safe place. This password is required to log into Cisco CX Cloud Agent. After you have stored the password in a safe place, select Save Password. To return to the previous screen, select Cancel.' The bottom features a 'Save Password' button and a 'Cancel' button with left and right navigation arrows.

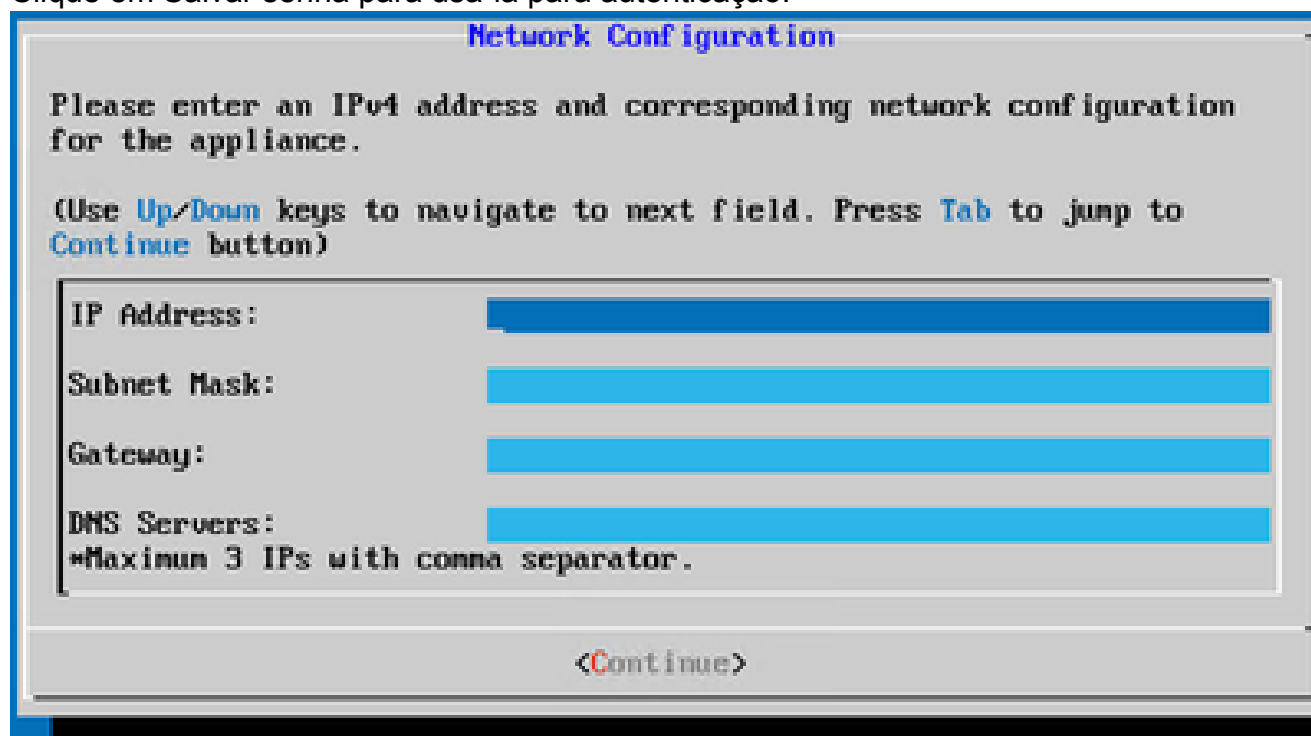
Senha gerada automaticamente



The 'Password Strength' dialog box states: 'The strength of the new password is Medium. To save the password, select Save Password. To configure a different password, select Cancel to return to the Set Password screen.' The bottom features a 'Save Password' button and a 'Cancel' button with left and right navigation arrows.

Salvar senha

3. Clique em Salvar senha para usá-la para autenticação.



The image shows a 'Network Configuration' window. It contains instructions to enter an IPv4 address and network configuration. Below the instructions are four input fields: 'IP Address:', 'Subnet Mask:', 'Gateway:', and 'DNS Servers:'. A note states 'Maximum 3 IPs with comma separator.' At the bottom is a '<Continue>' button.

**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:

Subnet Mask:

Gateway:

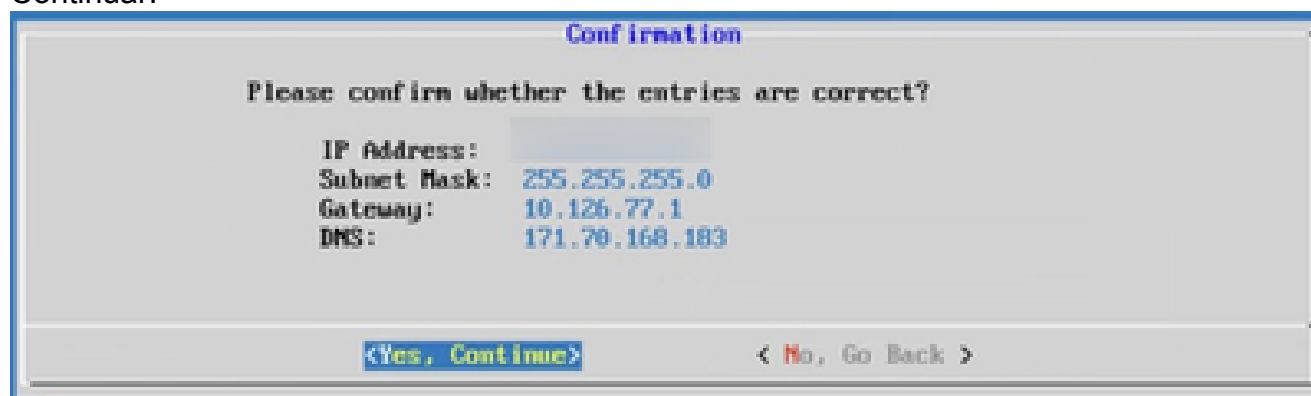
DNS Servers:

\*Maximum 3 IPs with comma separator.

<Continue>

Configuração de rede

4. Insira o endereço IP, a máscara de sub-rede, o gateway e o servidor DNS e clique em Continuar.



The image shows a 'Confirmation' window. It asks the user to confirm the entries. It lists the entered values: IP Address (empty), Subnet Mask (255.255.255.0), Gateway (10.126.77.1), and DNS (171.70.168.183). At the bottom are two buttons: '<Yes, Continue>' and '<No, Go Back>'.

**Confirmation**

Please confirm whether the entries are correct?

IP Address:

Subnet Mask: 255.255.255.0

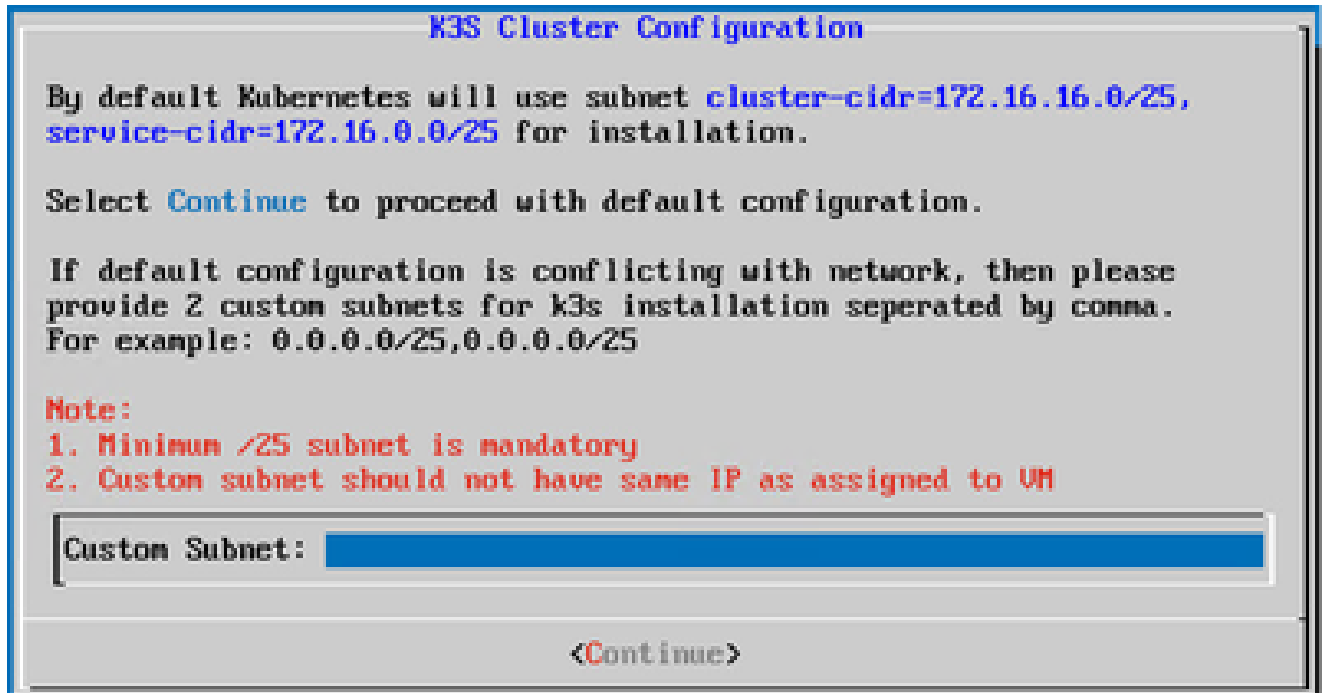
Gateway: 10.126.77.1

DNS: 171.70.168.183

<Yes, Continue>      <No, Go Back>

Confirmação

5. Confirme as entradas e clique em Sim, continuar.



**K3S Cluster Configuration**

By default Kubernetes will use subnet `cluster-cidr=172.16.16.0/25`,  
`service-cidr=172.16.0.0/25` for installation.

Select **Continue** to proceed with default configuration.

If default configuration is conflicting with network, then please  
provide 2 custom subnets for k3s installation seperated by comma.  
For example: `0.0.0.0/25,0.0.0.0/25`

**Note:**

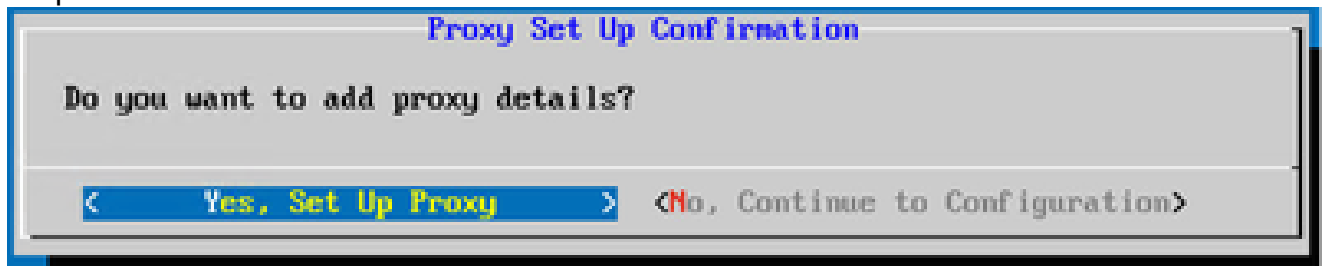
- 1. Minimum `/25` subnet is mandatory
- 2. Custom subnet should not have same IP as assigned to VM

Custom Subnet:

<Continue>

Sub-rede Personalizada

6. Insira o IP da sub-rede personalizada para a configuração de cluster do K3S (se a sub-rede padrão de um cliente entrar em conflito com a rede de seus dispositivos, selecione outra sub-rede personalizada).
7. Clique em Continuar.



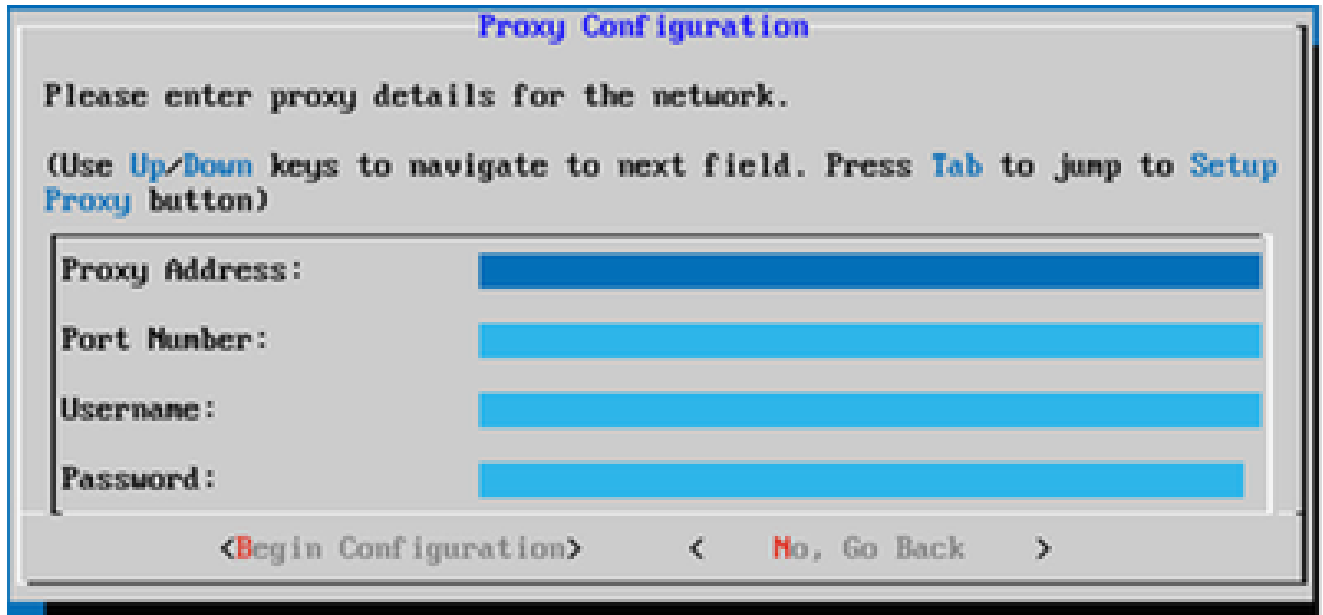
**Proxy Set Up Confirmation**

Do you want to add proxy details?

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

Configuração de proxy

8. Clique em Yes, Set Up Proxy para definir os detalhes do proxy ou clique em No, Continue to Configuration para prosseguir diretamente para a Etapa 11.

A terminal window titled "Proxy Configuration" with a grey background. It contains instructions to enter proxy details and navigate using Up/Down and Tab keys. There are four input fields for Proxy Address, Port Number, Username, and Password. At the bottom, there are three buttons: "<Begin Configuration>", "< No, Go Back >", and ">".

**Proxy Configuration**

Please enter proxy details for the network.

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

Proxy Address:

Port Number:

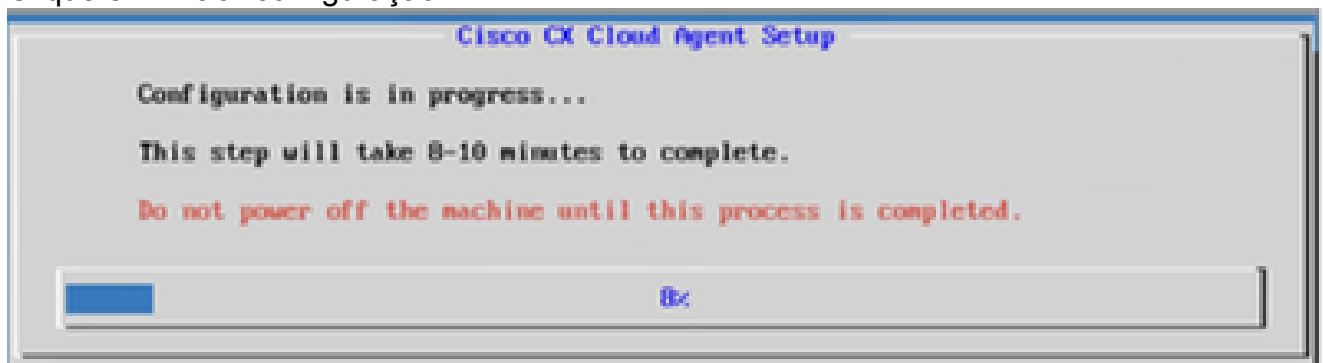
Username:

Password:

<Begin Configuration>      < No, Go Back >

Configuração de proxy

9. Digite o endereço do proxy, o número da porta, o nome do usuário e a senha.
10. Clique em Iniciar configuração.

A terminal window titled "Cisco CX Cloud Agent Setup" with a grey background. It displays a progress bar and instructions that configuration is in progress and will take 8-10 minutes. A warning in red text says not to power off the machine until the process is completed. At the bottom, there is a button labeled "<Back".

**Cisco CX Cloud Agent Setup**

Configuration is in progress...

This step will take 8-10 minutes to complete.

Do not power off the machine until this process is completed.

<Back

Configuração do Agente de Nuvem CX

A terminal window titled "Cisco CX Cloud Agent Configuration" with a grey background. It contains instructions to validate domain connectivity and press Continue. At the bottom, there is a button labeled "<Continue>".

**Cisco CX Cloud Agent Configuration**

Validate the domains connectivity. Please press Continue and wait for a while...

<Continue>

Configuração do agente de nuvem CX

11. Clique em Continuar.

## Cisco CX Cloud Agent Configuration

Following is the summary of CX Cloud Connectivity verification results.

Ensure all the connections are successful for the "opted in" region before proceeding.

### US:

cloudsso.cisco.com: Success  
api-cx.cisco.com: Success  
agent.us.cisco.cloud: Success  
ng.acs.agent.us.cisco.cloud: Success

### APJC:

cloudsso.cisco.com: Success  
api-cx.cisco.com: Success  
agent.us.cisco.cloud: Success  
agent.apjc.cisco.cloud: Success  
ng.acs.agent.apjc.cisco.cloud: Success

### EMEA:

cloudsso.cisco.com: Success  
api-cx.cisco.com: Success  
agent.us.cisco.cloud: Success  
agent.emea.cisco.cloud: Success  
ng.acs.agent.emea.cisco.cloud: Success

<Check Again>

< Continue >

A configuração continua

12. Clique em Continuar para continuar com a configuração para o alcance de domínio bem-sucedido. A configuração pode levar vários minutos para ser concluída.

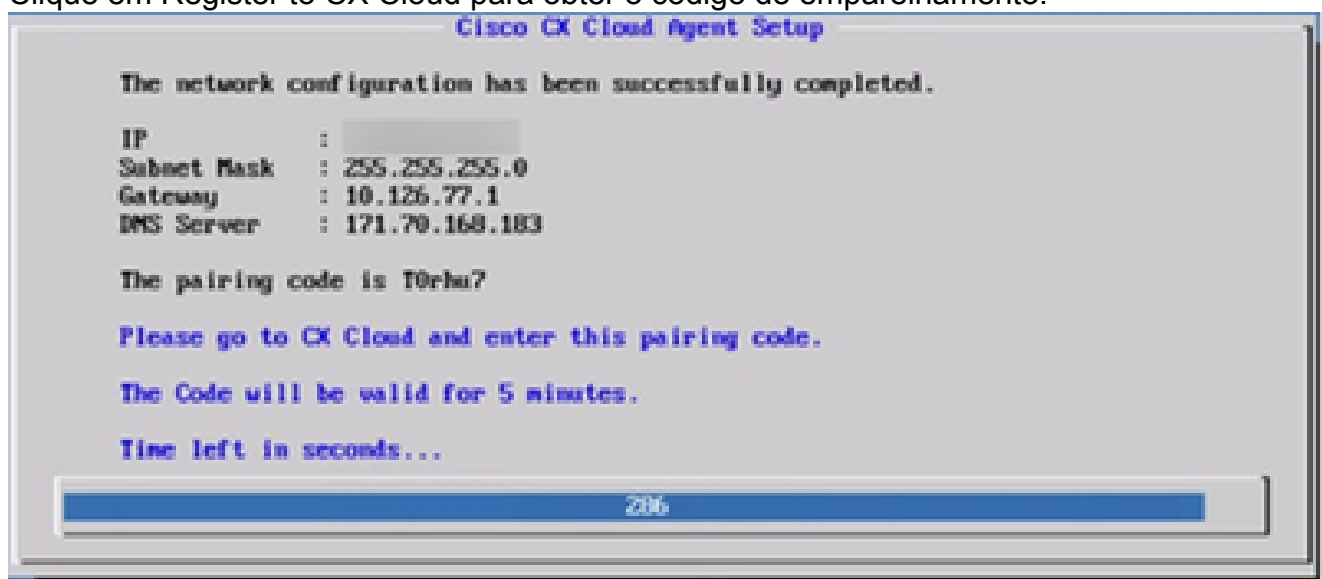


Note: Se os domínios não puderem ser acessados com êxito, o cliente deverá corrigir a acessibilidade do domínio fazendo alterações em seu firewall para garantir que os domínios estejam acessíveis. Clique em Verificar novamente quando o problema de acessibilidade dos domínios for resolvido.



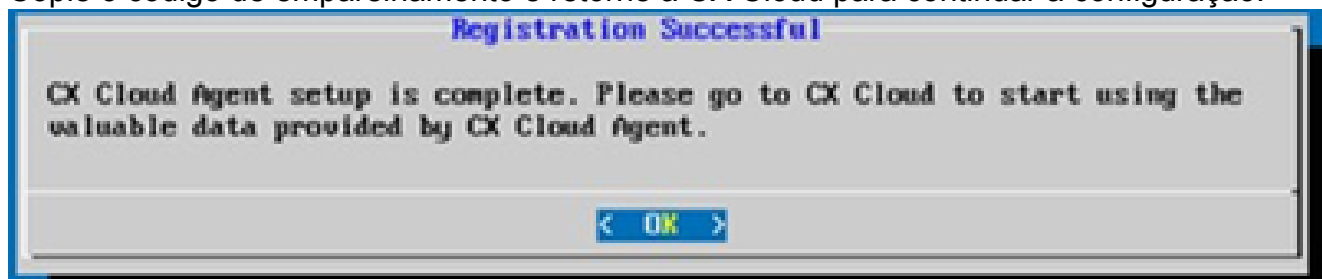
Registrar-se na CX Cloud

13. Clique em Register to CX Cloud para obter o código de emparelhamento.



Código de emparelhamento

14. Copie o código de emparelhamento e retorne à CX Cloud para continuar a configuração.



Registro realizado com sucesso



Note: Se o código de emparelhamento expirar, clique em Register to CX Cloud para gerar um novo código de emparelhamento (Etapa 13).

15. Clique em OK.

## 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 : x3710P
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 código de emparelhamento e retorne à CX Cloud para continuar a configuração.

## Configurando dispositivos para encaminhar syslog para o CX Cloud Agent

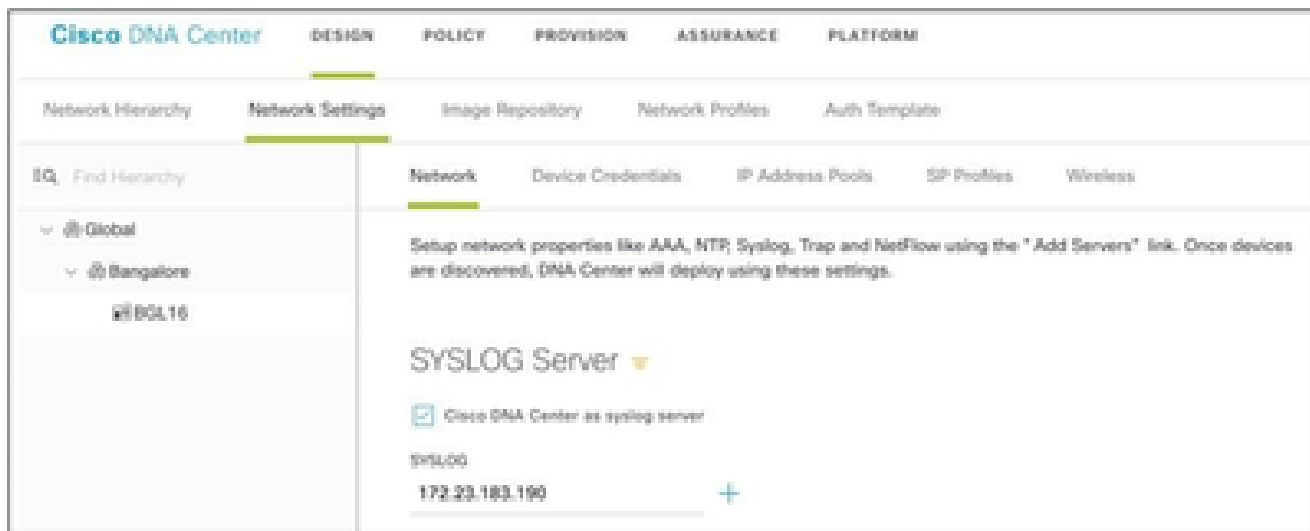
### Pré-requisitos

As versões suportadas do Cisco Catalyst Center são 2.1.2.0 a 2.2.3.5, 2.3.3.4 a 2.3.3.6, 2.3.5.0 e o Cisco Catalyst Center Virtual Appliance

### Definir Configuração De Encaminhamento De Syslog

Para configurar o encaminhamento de syslog para o agente CX no Cisco Catalyst Center, execute estas etapas:

1. Inicie o Cisco Catalyst Center.
2. Vá para Design > Configurações de rede > Rede.
3. Para cada site, adicione o IP do agente CX como o Servidor Syslog.



Servidor Syslog

 **Note:** Uma vez configurados, todos os dispositivos associados àquele site são configurados para enviar syslog com nível crítico para o CX 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 de servidor syslog é atualizada, todos os dispositivos associados a esse site são automaticamente definidos para o nível crítico padrão.

## Configurando outros ativos (coleta direta de dispositivos) para encaminhar o Syslog ao agente CX

Os dispositivos devem ser configurados para enviar mensagens de Syslog ao agente CX para usar o recurso de gerenciamento de falhas do CX Cloud.

 **Note:** O CX Agent relata apenas informações de syslog dos ativos de Nível 2 do Campus Success Track para o CX Cloud. Outros ativos são impedidos de ter seu syslog configurado para o CX Agent e não têm seus dados de syslog relatados no CX Cloud.

## Servidores Syslog existentes com capacidade de encaminhamento

Execute as instruções de configuração para o software do servidor syslog e adicione o endereço IP do agente CX como um novo destino.

 **Note:** Ao encaminhar syslogs, certifique-se de que o endereço IP origem da mensagem de syslog original seja preservado.

## Servidores Syslog existentes sem capacidade de encaminhamento OU sem servidor Syslog

Configure cada dispositivo para enviar syslogs diretamente para o endereço IP do agente do CX. Consulte esta documentação para obter as etapas de configuração específicas.

[Guia de configuração do Cisco IOS® XE](#)

[Guia de configuração do controlador sem fio AireOS](#)

## Habilitando configurações de syslog de nível de informação para o Cisco Catalyst Center

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

1. Navegue até Ferramentas>Telemetria.



## TOOLS

Discovery

Inventory

Topology

Image Repository

Command Runner

License Manager

Template Editor

Telemetry

Data and Reports

2. Selecione e expanda a Exibição de Site e selecione um site da hierarquia de sites.



Visualização do local

3. Selecione o site necessário e selecione todos os dispositivos usando a caixa de seleção Nome do dispositivo.
4. Selecione Visibilidade ideal na lista suspensa Ações.



Ações

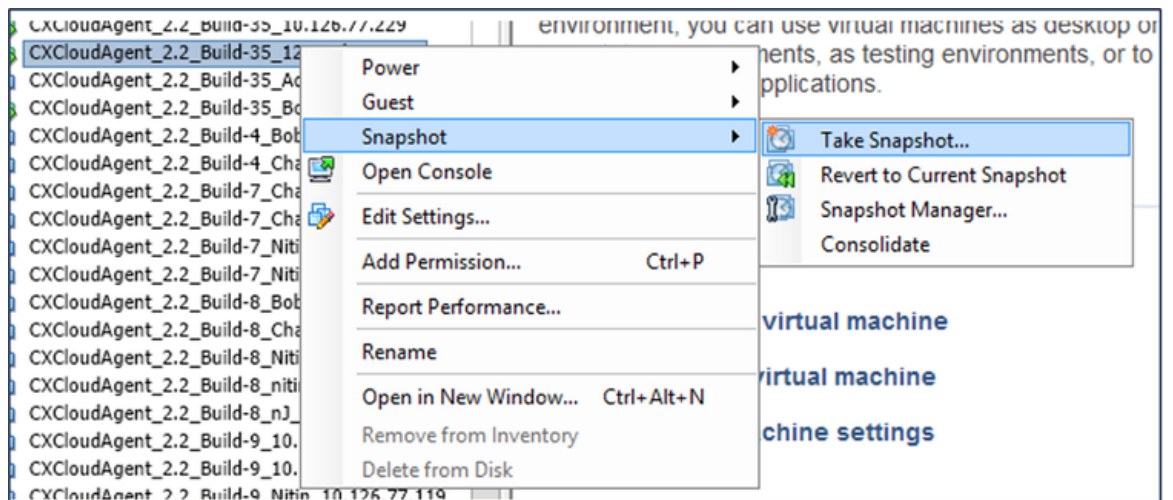
## Backup e restauração da VM em nuvem do CX

É recomendável preservar o estado e os dados de uma VM do agente CX em um point-in-time específico usando o recurso de instantâneo. Esse recurso facilita a restauração da máquina virtual em nuvem do CX para o horário específico em que o instantâneo é tirado.

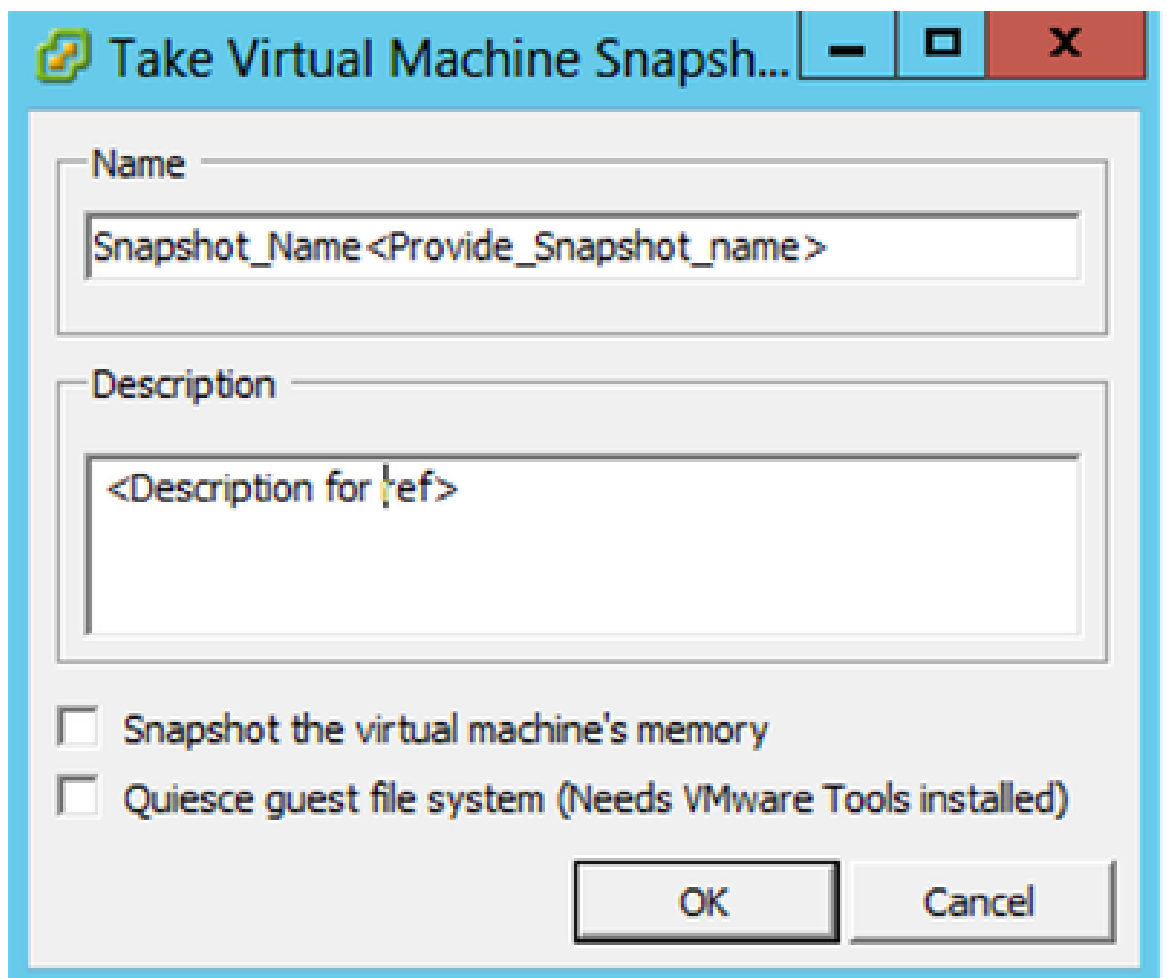
### Backup da VM de nuvem CX

Para fazer backup da máquina virtual em nuvem do CX:

1. Clique com o botão direito do mouse na VM e selecione Snapshot > Take Snapshot. A janela Tirar instantâneo da máquina virtual se abre.



Selecionar VM



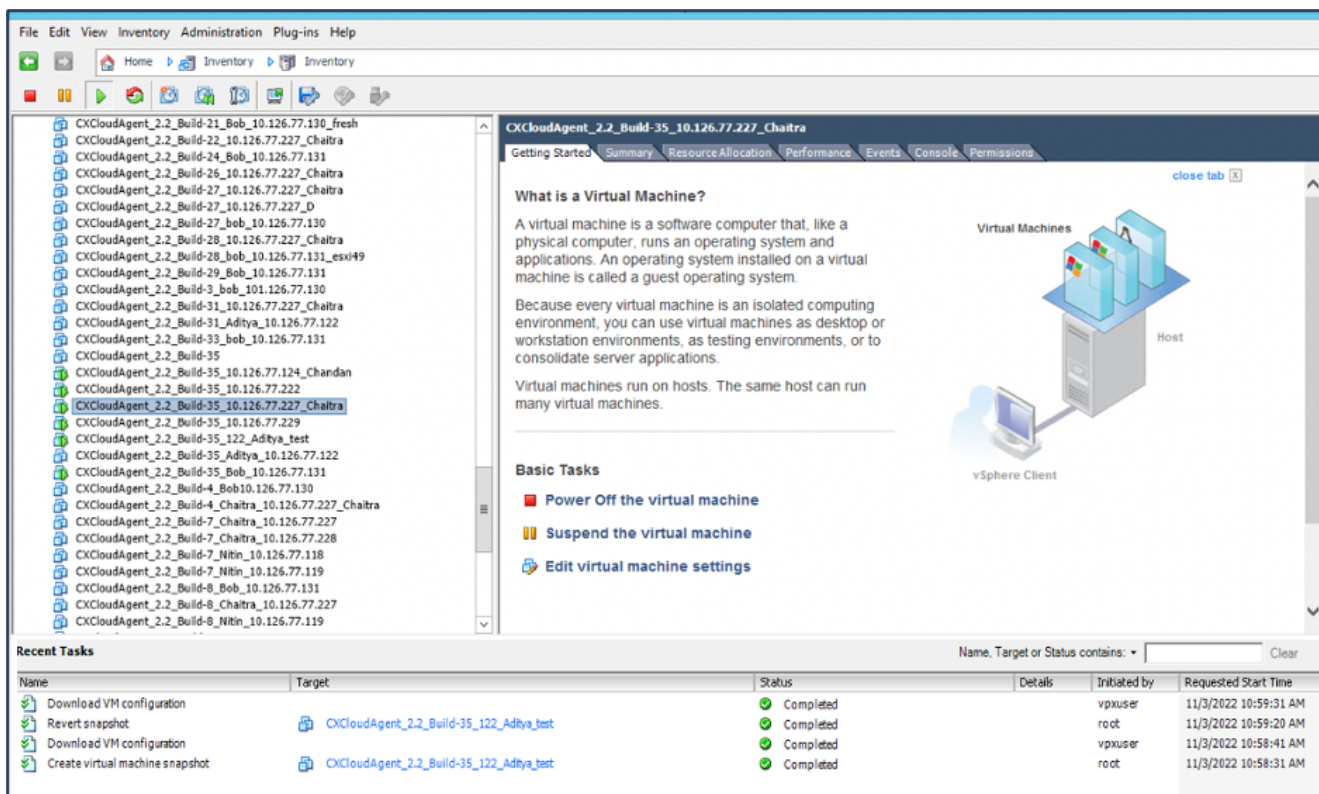
Tirar Instantâneo da Máquina Virtual

2. Insira Name e Description.



Note: Verifique se a caixa de seleção Instantâneo da memória da máquina virtual está desmarcada.

3. Clique em OK. O status Criar instantâneo da máquina virtual é exibido como Concluído na lista Tarefas recentes.

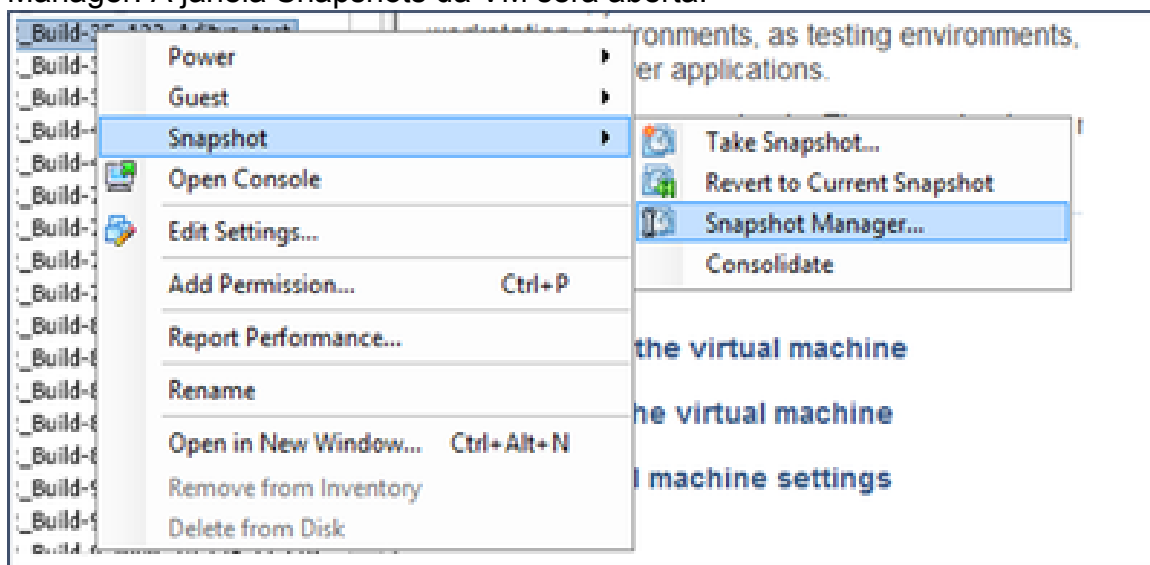


Tarefas Recentes

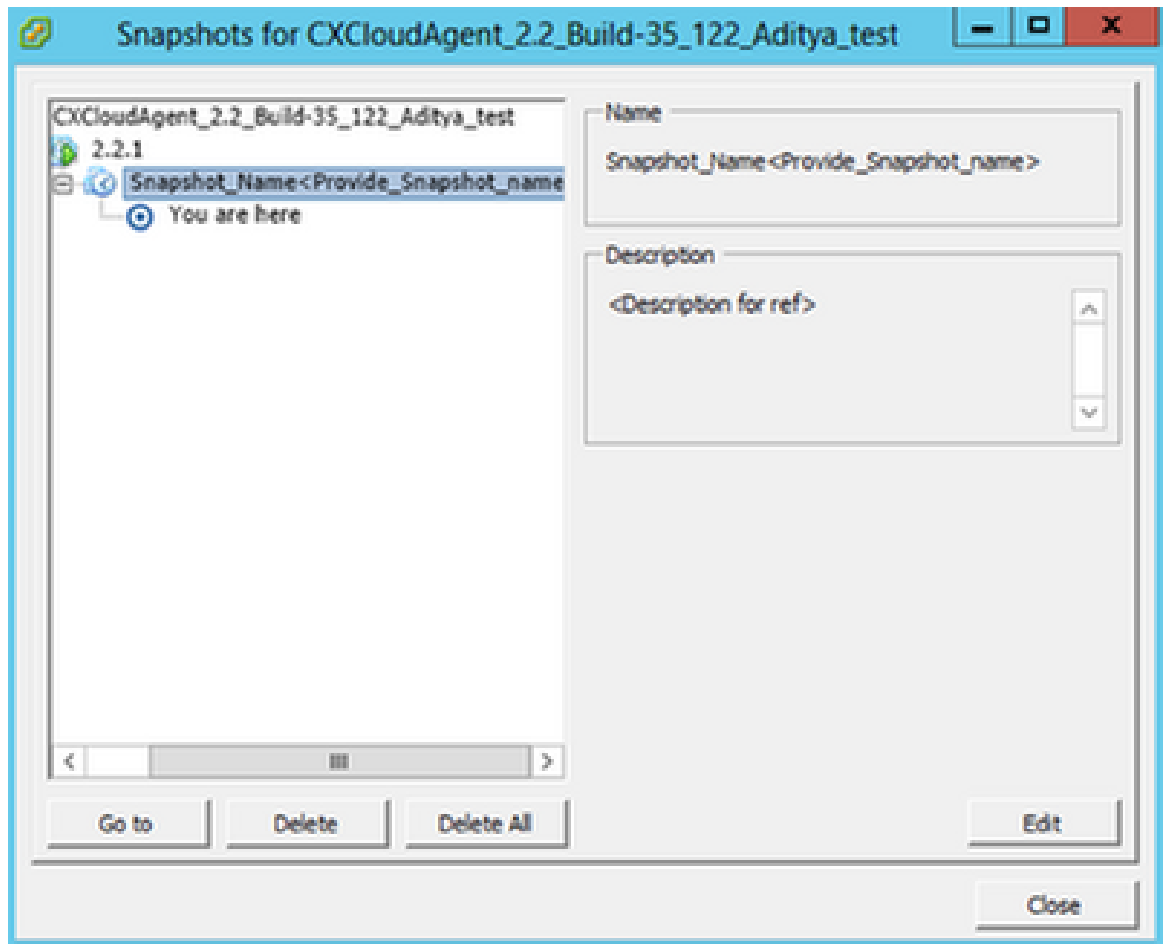
## Restaurando a VM em nuvem do CX

Para restaurar a máquina virtual em nuvem do CX:

1. Clique com o botão direito do mouse na VM e selecione Snapshot > Snapshot Manager. A janela Snapshots da VM será aberta.

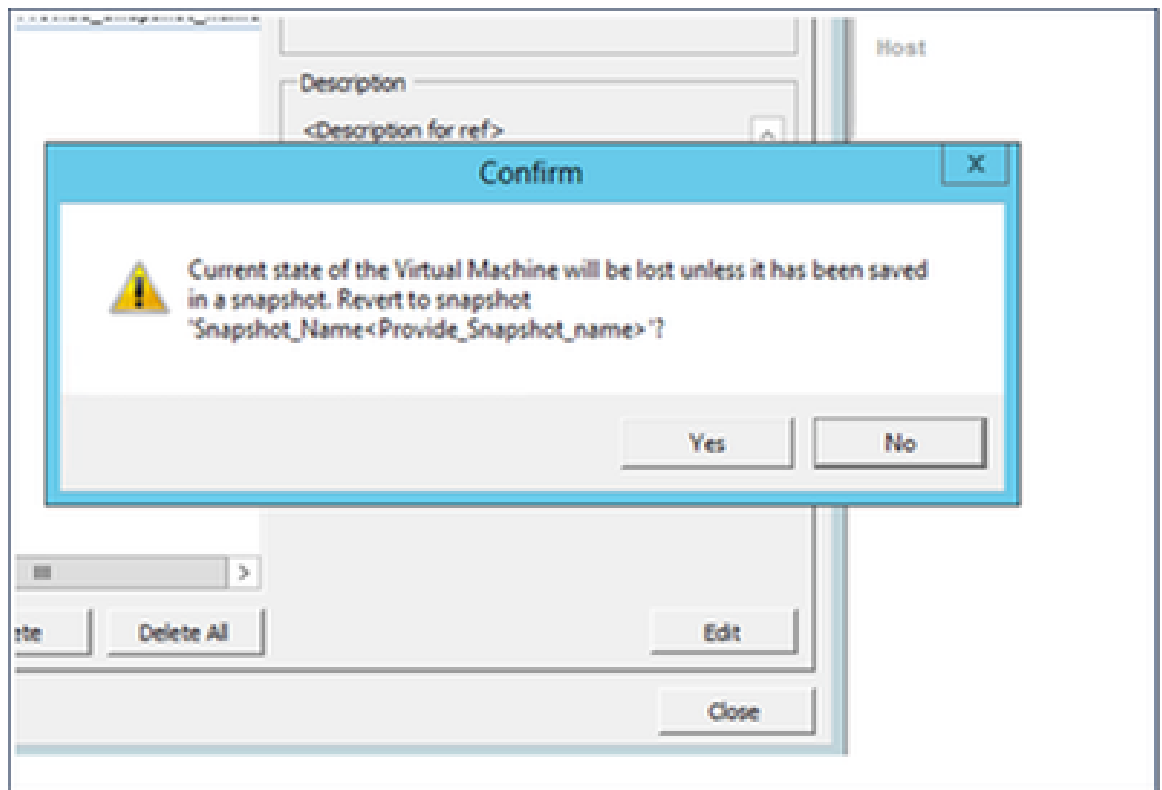


Janela Selecionar VM



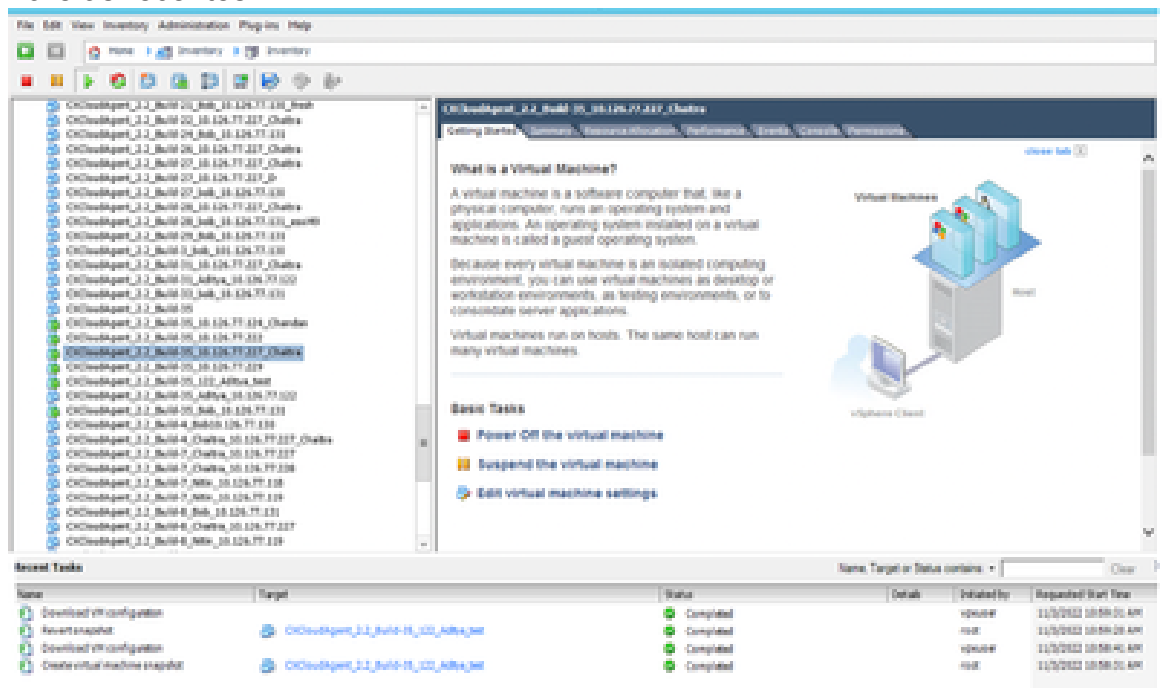
Janela Snapshots

2. Clique em Ir para. A janela Confirmar é aberta.



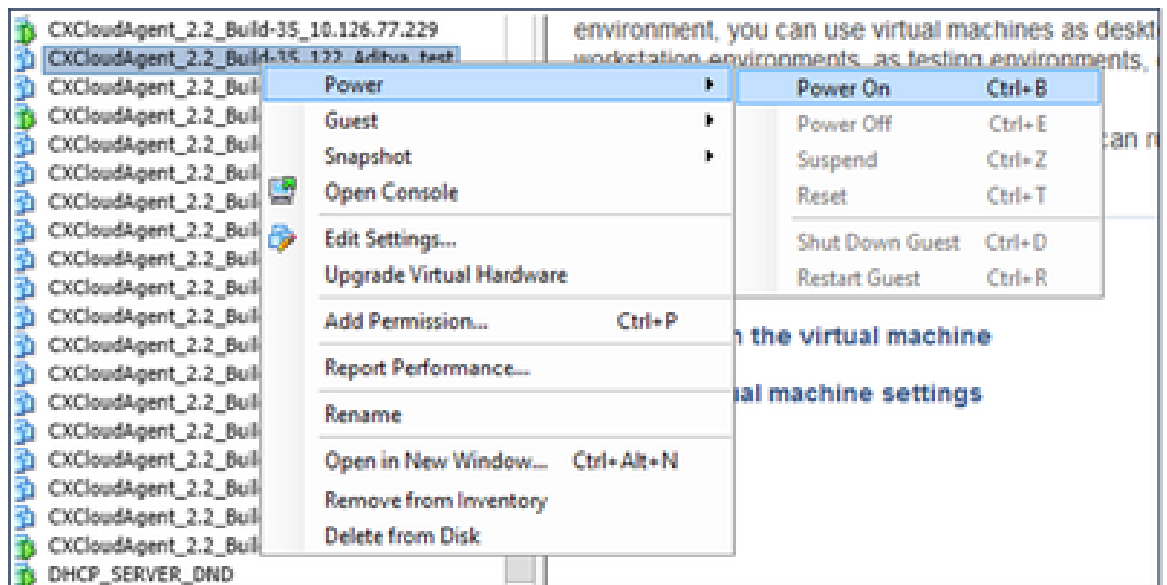
Confirmar janela

3. Clique em Sim. O status Reverter instantâneo é exibido como Concluído na lista Tarefas recentes.



Tarefas Recentes

4. Clique com o botão direito do mouse na VM e selecione Power > Power On para ligar a VM.



## Security

O agente CX garante ao cliente segurança de ponta a ponta. A conexão entre o CX Cloud e o CX Agent é TLS protegida. O usuário SSH padrão do Agente de Nuvem é limitado para executar somente operações básicas.

### Segurança física

Implante a imagem OVA do CX 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 esta [FAQ](#) para definir esta senha do carregador de inicialização (modo de usuário único).

### Segurança da conta

Durante a implantação, a conta de usuário cxcadmin é criada. Os usuários são forçados a definir uma senha durante a configuração inicial. cxcadmin usuário/credenciais são usados para acessar as APIs do agente CX e para se conectar ao dispositivo por SSH.

os usuários cxcadmin têm acesso restrito 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. os usuários cxcadmin podem criar um usuário cxcroot usando o utilitário chamado remoteaccount. os usuários cxcroot podem obter privilégios de root.

### Segurança de rede

A VM do agente CX 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 autentique e se comunique com o agente CX.

- Ações com privilégios do root no dispositivo usando o ssh.

os usuários cxcadmin podem criar o usuário cxcroot usando um utilitário chamado remotesaccount. Este utilitário exibe uma senha criptografada RSA/ECB/PKCS1v1\_5 que pode ser descriptografada somente no portal SWIM ([DECRYPT Request Form](#)). Somente o pessoal autorizado tem acesso a esse portal. os usuários cxcroot podem obter privilégios de root usando essa senha descriptografada. A frase secreta é válida apenas por dois dias. Os usuários cxcadmin devem recriar a conta e obter a senha do portal SWIM após a expiração da senha.

## Blindagem

O CX Agent Appliance segue os padrões de fortalecimento do Centro de Segurança da Internet.

## Segurança de dados

O aplicativo CX Agent não armazena informações pessoais do cliente. O aplicativo de credenciais do dispositivo (executado como um dos pods) armazena credenciais de servidor criptografadas dentro do banco de dados protegido. Os dados coletados não são armazenados de nenhuma forma dentro do dispositivo, exceto temporariamente quando estão sendo processados. Os dados de telemetria são carregados na nuvem CX assim que possível após a coleta ser concluída e são imediatamente excluídos do armazenamento local após a confirmação de que o carregamento foi bem-sucedido.

## Transmissão de Dados

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

## Registros e monitoramento

Os registros não contêm nenhuma forma de dados de informações pessoais identificáveis (PII). Os logs de auditoria capturam todas as ações confidenciais de segurança executadas no dispositivo CX Cloud Agent.

## Comandos de telemetria da Cisco

O CX Cloud recupera a telemetria de ativos usando as APIs e os comandos listados nos [comandos de telemetria da Cisco](#). Este documento categoriza os comandos com base em sua aplicabilidade ao inventário do Cisco Catalyst Center, Diagnostic Bridge, Intersight, Compliance Insights, Falhas e todas as outras fontes de telemetria coletadas pelo CX Agent.

As informações confidenciais na telemetria de ativos são mascaradas antes de serem

transmitidas para a nuvem. O agente CX mascara os dados confidenciais de todos os ativos coletados que enviam telemetria diretamente ao agente CX. Isso inclui senhas, chaves, strings de comunidade, nomes de usuário e assim por diante. Os controladores fornecem mascaramento de dados para todos os ativos gerenciados pelo controlador antes de transferir essas informações para o agente CX. Em alguns casos, a telemetria de ativos gerenciados por controlador pode ser ainda mais anônima. Consulte a [documentação de suporte do produto](#) correspondente para obter mais informações sobre como tornar a telemetria anônima (por exemplo, a seção [Anonimizar Dados](#) do Guia do Administrador do Cisco Catalyst Center).

Embora a lista de comandos de telemetria não possa ser personalizada e as regras de mascaramento de dados não possam ser modificadas, os clientes podem controlar quais acessos à nuvem de telemetria CX de ativos especificando fontes de dados conforme discutido na [documentação de suporte do produto](#) para dispositivos gerenciados por controlador ou na seção Conectando fontes de dados deste documento (para outros ativos coletados pelo agente CX).

## 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. Os usuários devem consultar as <a href="#">FAQ</a> para definir sua senha do carregador de inicialização (modo de usuário único).                                                                                                                                                                                                            |
| Acesso do usuário             | SSH: <ul style="list-style-type: none"><li>· O acesso ao dispositivo usando o usuário de cxcadmin exige as credenciais criadas durante a instalação.</li><li>· O acesso ao dispositivo usando o usuário cxcroot requer que as credenciais sejam descriptografadas usando o portal SWIM por pessoal autorizado.</li></ul>                                                                                                                           |
| Contas do usuário             | <ul style="list-style-type: none"><li>· cxcadmin: conta de usuário padrão criada; O usuário pode executar comandos de aplicativos do CX Agent usando cxcli e tem privilégios mínimos no dispositivo; O usuário de cxcroot e a senha criptografada são gerados com o usuário de cxcadmin.</li><li>· cxcroot: cxcadmin pode criar este usuário usando o utilitário remoteaccount; O usuário pode obter privilégios do root com essa conta.</li></ul> |
| Política de senha de cxcadmin | <ul style="list-style-type: none"><li>· A senha é um hash unidirecional que usa o SHA-256 e é armazenada com segurança.</li><li>· Mínimo de oito (8) caracteres, contendo três destas categorias: maiúsculas,</li></ul>                                                                                                                                                                                                                            |

|                                   |                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <p>minúsculas, números e caracteres especiais.</p>                                                                                                                                                                                                                                                                    |
| Política de senha de cxcroot      | <ul style="list-style-type: none"> <li>· A senha de cxcroot é criptografada por RSA/ECB/PKCS1v1_5</li> <li>· A frase secreta gerada precisa ser descriptografada no portal do SWIM.</li> <li>· O usuário e a senha do cxcroot são válidos por dois dias e podem ser regenerados usando o usuário cxcadmin.</li> </ul> |
| Política de senha de login de ssh | <ul style="list-style-type: none"> <li>· Mínimo de oito caracteres que contenham três destas categorias: maiúsculas, minúsculas, números e caracteres especiais.</li> <li>· Cinco tentativas de login com falha bloqueiam a caixa por 30 minutos; A senha expira em 90 dias.</li> </ul>                               |
| Portas                            | <p>Portas de entrada abertas – 514 (Syslog) e 22 (ssh)</p>                                                                                                                                                                                                                                                            |
| Segurança de dados                | <ul style="list-style-type: none"> <li>· Não há informações de cliente armazenadas.</li> <li>· Não há dados de dispositivo armazenados.</li> <li>· As credenciais do servidor Cisco Catalyst Center são criptografadas e armazenadas no banco de dados.</li> </ul>                                                    |

### 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.