

Visão geral do CX Cloud Agent v2.4

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos de implantação](#)

[Acesso a domínios essenciais](#)

[Domínios específicos do portal do CX Cloud Agent](#)

[Domínios específicos do CX Cloud Agent OVA](#)

[Versão com suporte do Cisco DNA Center](#)

[Navegadores compatíveis](#)

[Lista de produtos suportados](#)

[Atualizando/instalando o CX Cloud Agent v2.4](#)

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

[Atualize o CX Cloud Agent v2.4](#)

[Adicionando o CX Cloud Agent](#)

[Adicionando o Cisco DNA Center como fonte de dados](#)

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

[Protocolos de descoberta](#)

[Protocolos de conectividade](#)

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

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

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

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

[Adicionar 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 as VMs do CX Cloud 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 5.2.30](#)

[Instalação do Microsoft Hyper-V](#)

[Configuração de rede](#)

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

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

[Pré-requisitos](#)

[Definir Configuração De Encaminhamento De Syslog](#)

[Configurar outros ativos para encaminhar o Syslog ao CX Cloud Agent](#)

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

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

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

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

[Fazer backup](#)

[Restaurar](#)

[Security](#)

[Segurança física](#)

[Segurança da conta](#)

[Segurança de rede](#)

[Autenticação](#)

[Blindagem](#)

[Segurança de dados](#)

[Transmissão de Dados](#)

[Registros e monitoramento](#)

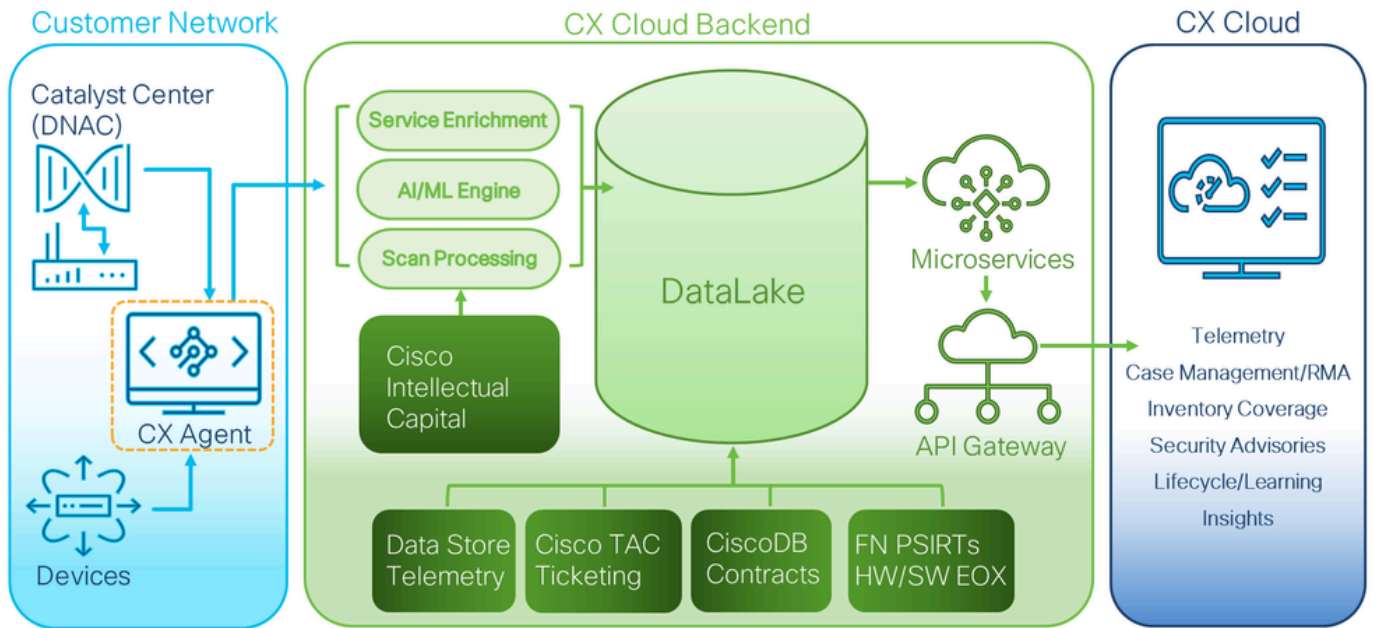
[Comandos de telemetria da Cisco](#)

[Resumo de segurança](#)

Introdução

Este documento descreve o Cisco Customer Experience (CX) Cloud Agent. O CX Cloud 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 Cloud Agent permite a transformação da Inteligência Artificial (AI)/Aprendizagem Automática (ML) de dados de configuração ativa em insights proativos e preditivos exibidos na nuvem CX.

CX Cloud Architecture



Arquitetura de nuvem CX

Este guia é específico do CX Cloud Agent v2.4. Consulte a página [Cisco CX Cloud Agent](#) para acessar versões anteriores.



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

Pré-requisitos

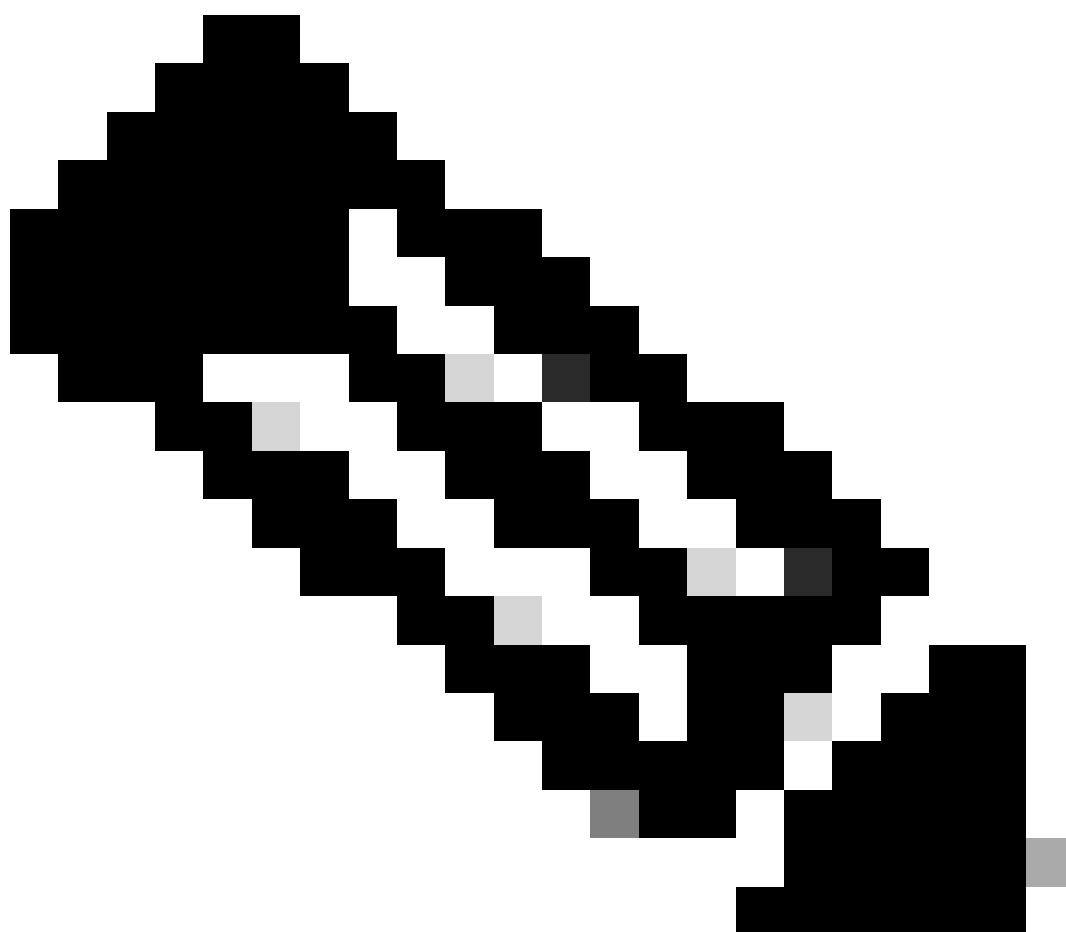
O CX Cloud Agent é executado como máquina virtual (VM) e está disponível para download como Open Virtual Appliance (OVA) ou um Virtual Hard Disk (VHD).

Requisitos de implantação

- Um dos seguintes hipervisores é necessário para uma nova instalação:
 - VMware ESXi versão 5.5 ou posterior
 - Oracle Virtual Box 5.2.30 ou posterior
 - Hipervisor Windows versão 2012 a 2022
- As configurações na tabela a seguir são necessárias para a implantação da VM:

Tipo de implantação do agente de nuvem CX	Número de núcleos da CPU	RAM	Disco rígido	*Número máximo de ativos diretamente conectados ao CX Cloud Agent
OVA pequeno	8C	16 GB	200 GB	10,000
ÓVULOS médios	16 C	32 GB	600 GB	20,000
ÓVULOS GRANDES	32 C	64 GB	1.200 GB	50,000 :

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



Observação: o Flexible OVA/Patch 2.4 para configurações médias e grandes está disponível apenas para VMs VMware ESXi. O Oracle VirtualBox e o Windows Hyper-V não podem ser usados para configurações médias e grandes.

- Para clientes que usam data centers designados nos EUA como a região de dados principal para armazenar dados da nuvem CX, o CX Cloud Agent deve ser capaz de se conectar aos servidores mostrados aqui, usando o Fully Qualified Domain Name (FQDN) e usando HTTPS na porta TCP 443:
 - FQDN: agent.us.cisco.cloud
 - FQDN: ng.acs.agent.us.cisco.cloud
 - FQDN: cloudsso.cisco.com
 - FQDN: api-cx.cisco.com
- Para clientes que usam data centers designados na Europa como a região de dados principal para armazenar dados da nuvem CX: o CX Cloud Agent deve ser capaz de se conectar a ambos os servidores mostrados aqui, usando o FQDN e usando HTTPS na porta TCP 443:
 - FQDN: agent.us.cisco.cloud
 - FQDN: agent.emea.cisco.cloud
 - FQDN: ng.acs.agent.emea.cisco.cloud
 - FQDN: cloudsso.cisco.com
 - FQDN: api-cx.cisco.com
- Para clientes que usam data centers designados do Pacífico Asiático como a região de dados principal para armazenar dados da nuvem CX: o CX Cloud Agent deve ser capaz de se conectar aos dois servidores mostrados aqui, usando o FQDN e usando HTTPS na porta TCP 443:
 - FQDN: agent.us.cisco.cloud
 - FQDN: agent.apjc.cisco.cloud
 - FQDN: ng.acs.agent.apjc.cisco.cloud
 - FQDN: cloudsso.cisco.com
 - FQDN: api-cx.cisco.com
- Para clientes que usam 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 necessária apenas para registrar o CX Cloud Agent com a 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.
- 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	<u>All regions:</u> cloudsso.cisco.com api-cx.cisco.com agent.us.cisco.cloud DNA Center <u>AMER region:</u> ng.acs.agent.us.cisco.cloud <u>EMEA region:</u> agent.emea.cisco.cloud ng.acs.agent.emea.cisco.cloud <u>APJC region:</u> agent.apjc.cisco.cloud ng.acs.agent.apjc.cisco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers	Bi-directional to Cisco AWS regional data centers and DNA 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 será detectado automaticamente se o DHCP (Dynamic Host Configuration Protocol) estiver habilitado no ambiente da VM; caso contrário, um endereço IPv4, uma máscara de sub-rede, um endereço IP do gateway padrão e um endereço IP do servidor DNS (Domain Name Service) deverão estar disponíveis.
- Somente IPv4 é suportado.
- As versões certificadas do Cisco DNA Center para Cluster de HA (High Availability, nó único) são 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x e o Cisco Catalyst Center Virtual Appliance e o Cisco DNA Center Virtual Appliance.
- Se a rede tiver interceptação SSL, permita listar o endereço IP do CX Cloud Agent.
- Para todos os ativos diretamente conectados, é necessário o nível de privilégio SSH 15.
- Use apenas os nomes de host fornecidos; endereços IP estáticos não podem ser usados.

Acesso a domínios essenciais

Para iniciar a jornada da nuvem do CX, os usuários precisam de acesso a esses domínios. Use apenas os nomes de host fornecidos; não use endereços IP estáticos.


Domínios específicos do portal do CX Cloud Agent

Principais domínios	Outros domínios
cisco.cloud	cloudfront.net
	eum-appdynamics.com

split.io	appdynamics.com
	tiqcdn.com
	jquery.com

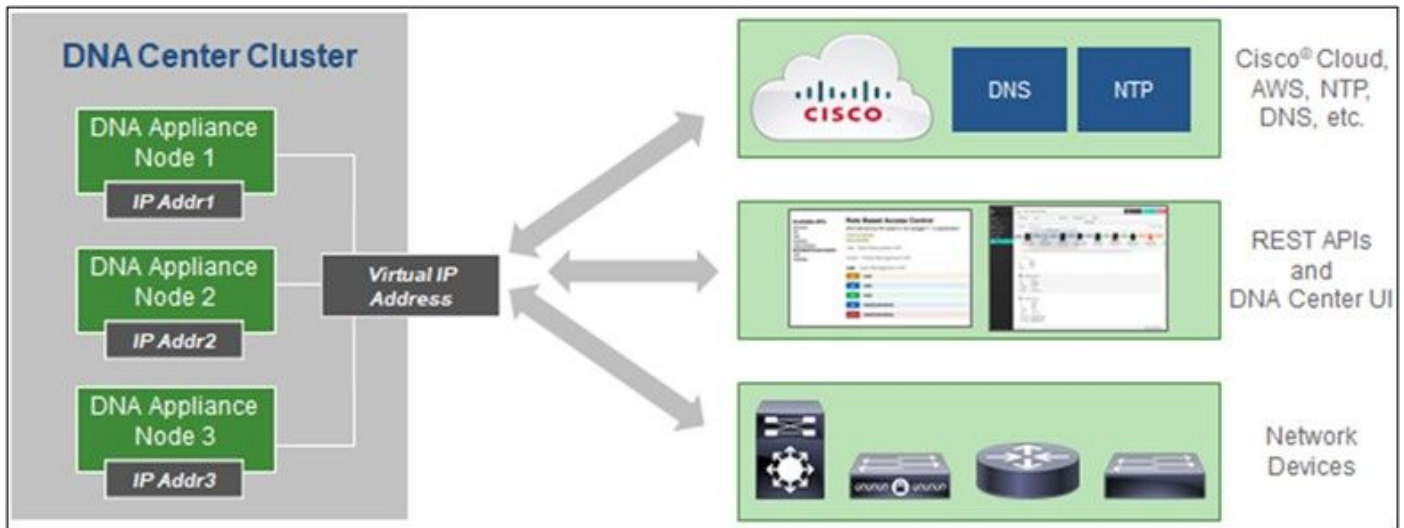
Domínios específicos do CX Cloud Agent OVA

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

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

Versão com suporte do Cisco DNA Center

As versões de nó único e cluster HA do Cisco DNA Center são 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x e o Cisco Catalyst Center Virtual Appliance e o Cisco DNA 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 visualizar a lista de produtos suportados pelo CX Cloud Agent, consulte a [Lista de produtos suportados](#).

Atualizando/instalando o CX Cloud Agent v2.4

- Os clientes atuais que estiverem fazendo o upgrade para a nova versão devem consultar [Upgrade CX Cloud Agent v2.4](#).
- Os novos clientes que implementarem uma nova instalação flexível do OVA v2.4 devem consultar [Adicionando o CX Cloud Agent como fonte de dados](#).

Atualização de VMs existentes para configurações grandes e médias

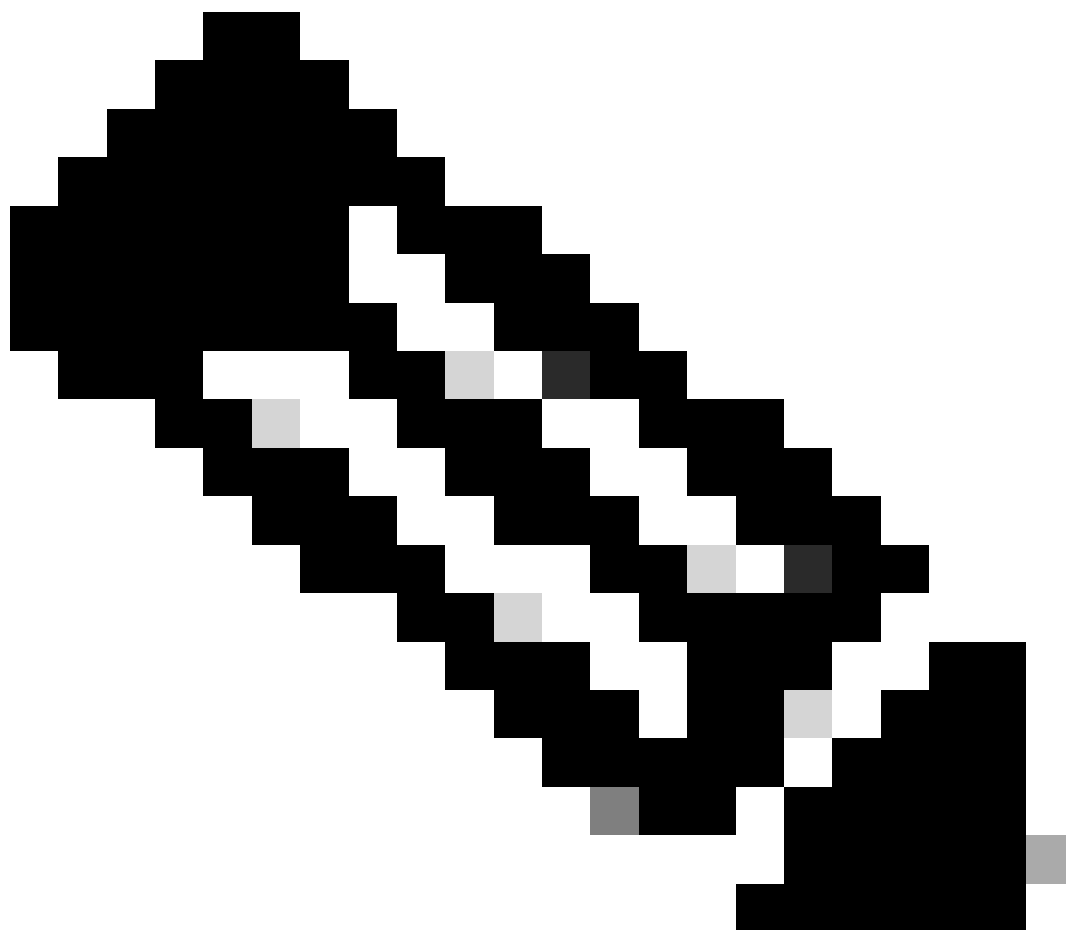
Os clientes podem atualizar sua configuração de VM existente para médio ou grande usando as opções de OVA flexível com base no tamanho e na complexidade da rede.

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

Atualize o CX Cloud Agent v2.4

Os clientes que executam o CX Cloud Agent v2.3.x ou superior podem seguir as etapas desta

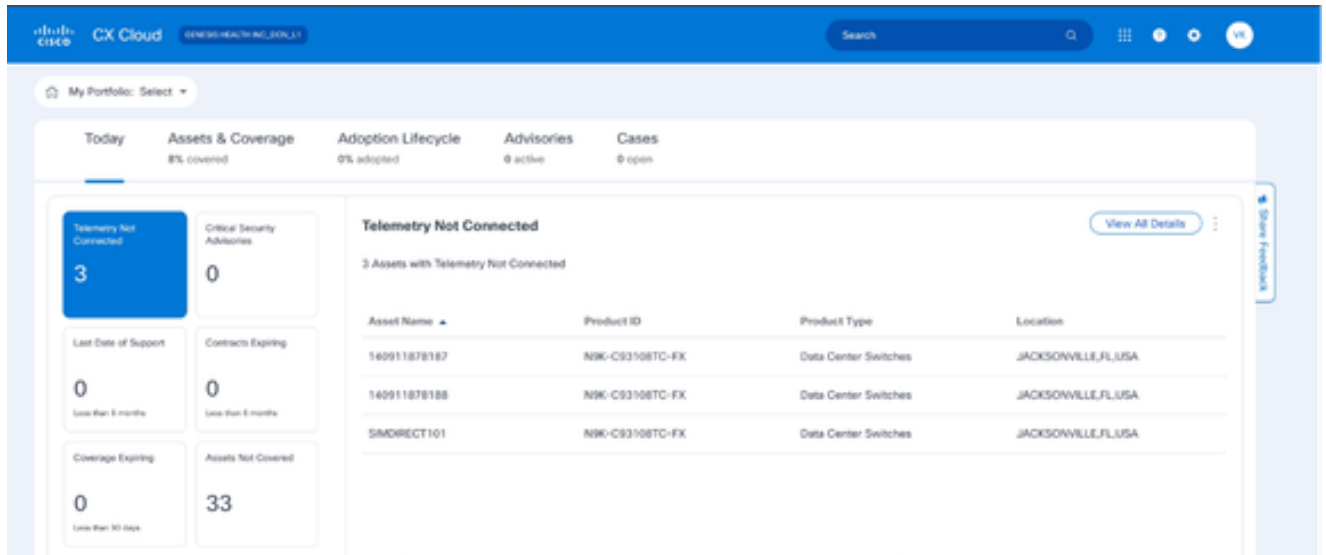
seção para atualizar diretamente para a v2.4.



Observação: os clientes no CX Cloud Agent v2.2.x devem atualizar para v2.3.x antes de atualizar para v2.4 ou instalar o v2.4 como uma nova instalação OVA.

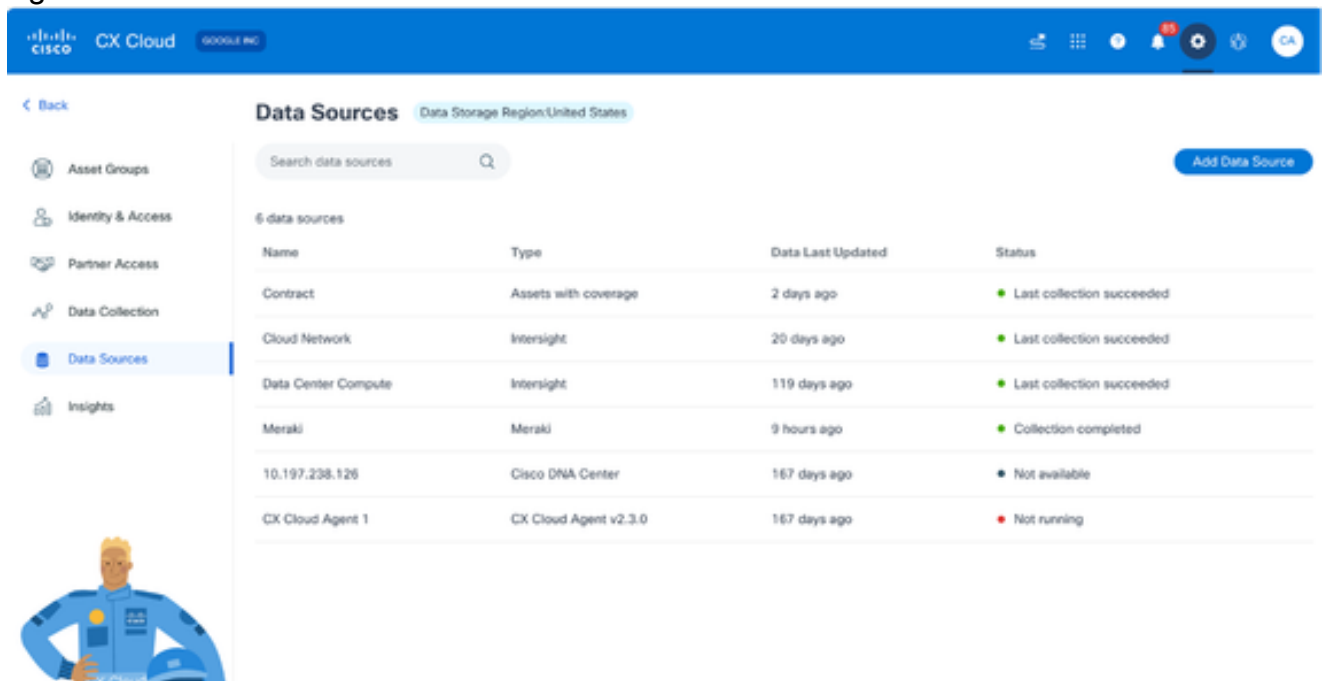
Para instalar a atualização do CX Cloud Agent v2.4 a partir do CX Cloud:

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



Página inicial do CX Cloud

2. Clique no ícone Admin Center. A janela Fontes de dados é aberta exibindo o CX Cloud Agent como uma fonte de dados existente.



Origem dos dados

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

The screenshot shows the Cisco CX Cloud interface. On the left, a navigation menu includes 'Asset Groups', 'Identity & Access', 'Partner Access', 'Data Collection', 'Data Sources', and 'Insights'. The 'Data Sources' section is active, displaying a table with 6 data sources. The table has columns for 'Name' and 'Type'. The data sources listed are: Contract (Assets with co), Cloud Network (Intersight), Data Center Compute (Intersight), Collaboration (Webex), 100.1.1.1 (Cisco DNA Ce), and CX Cloud Agent 1 (CX Cloud Agen). On the right, the 'CX Cloud Agent 1' details are shown. It is currently 'Running'. There are buttons for 'Download Report' and 'Replace Seed File'. Below this, there are tabs for 'Seed File', 'Cisco DNA Centers', and 'Software'. The 'Software' tab is selected, showing '1 assets reachable' and '146 assets unreachable'. The collection schedule is 'Daily at 01:00 AM EST'.

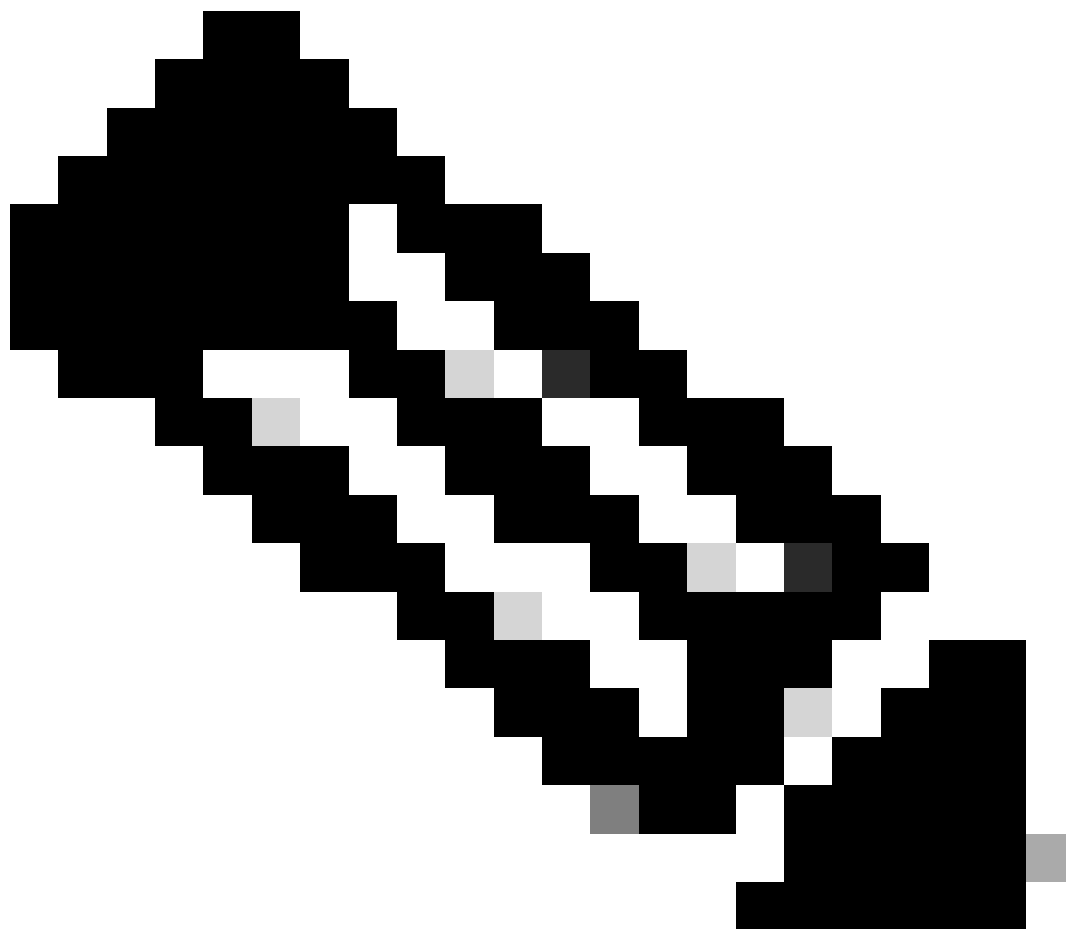
Exibição de Detalhes de Fontes de Dados

4. Clique na guia Software.

The screenshot shows the Cisco CX Cloud interface with the 'Software' tab selected for 'CX Cloud Agent 1'. The status is 'Not running'. There is a 'Replace Seed File' button. Below, there are tabs for 'Seed File', 'Cisco DNA Centers', and 'Software'. The 'Software' tab is selected, showing 'Choose a software version to update to: 2.4.0' with a dropdown arrow and a 'View release notes' link. There is a checked 'Install Now' checkbox and an 'Install Update' button.

Exibição de Detalhes do Agente de Nuvem CX

5. Selecione a versão 2.4.0 do software na lista suspensa Escolha uma versão de software para atualizar.
6. Clique em Install Update para instalar o CX Cloud Agent v2.4.0.

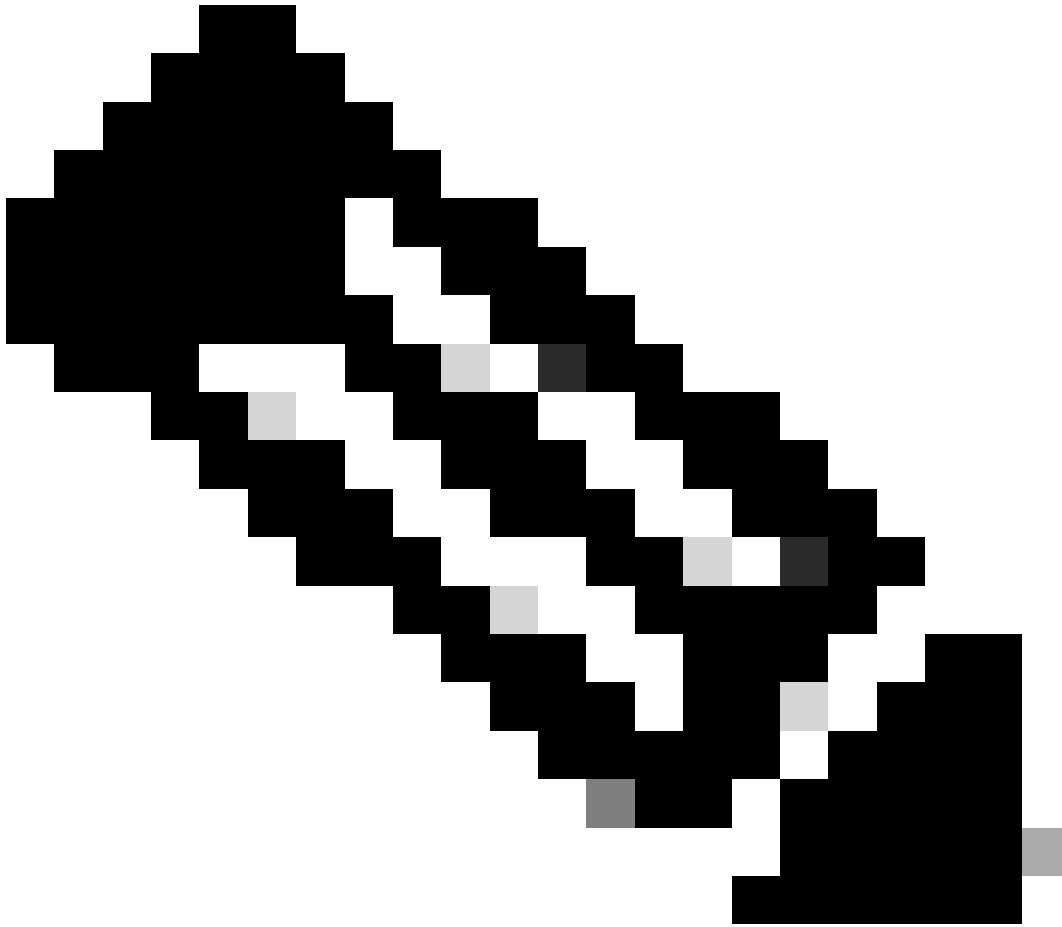


Observação: os clientes podem agendar a atualização para mais tarde desmarcando a caixa de seleção Instalar agora, que exibe as opções de agendamento.

Adicionando o CX Cloud Agent

Os clientes podem adicionar até vinte (20) instâncias do CX Cloud Agent na nuvem CX.

Para adicionar um CX Cloud Agent:



Observação: repita as etapas a seguir para adicionar instâncias adicionais do CX Cloud Agent como uma fonte de dados.

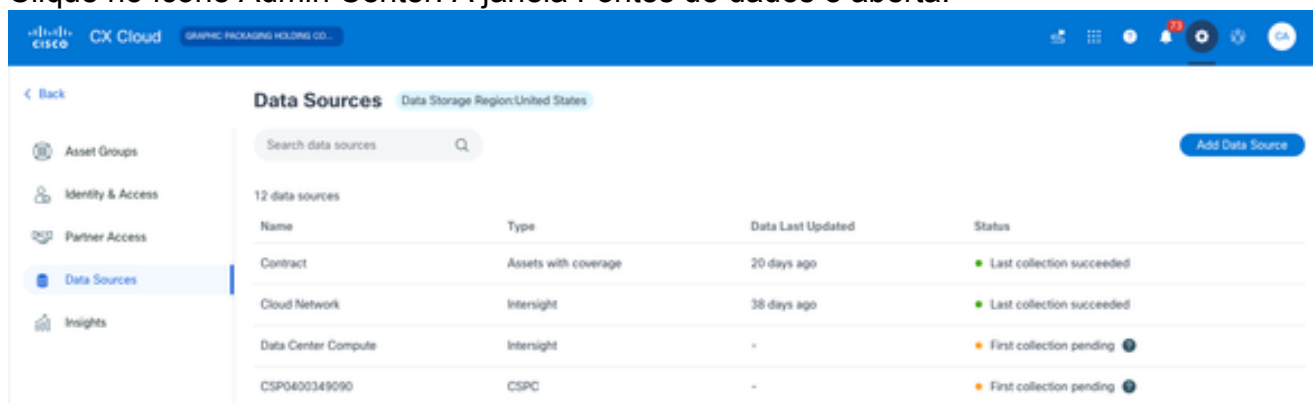
1. Faça login no [CX Cloud](#). A página Início é exibida.

The screenshot displays the Cisco CX Cloud dashboard. At the top, there is a navigation bar with the Cisco logo, 'CX Cloud', and a search bar. Below the navigation bar, there is a 'My Portfolio' section with a dropdown menu. The main content area is divided into several sections:

- Today**: A summary section with five cards: 'Assets & Coverage' (8% covered), 'Adoption Lifecycle' (0% adopted), 'Advisories' (0 active), and 'Cases' (0 open).
- Telemetry Not Connected**: A section with a blue card showing '3' and a 'View All Details' button. Below this is a table with 3 assets.
- Critical Security Advisories**: A card showing '0'.
- Contracts Expiring**: A card showing '0' with a note 'Less than 6 months'.
- Coverage Expiring**: A card showing '0' with a note 'Less than 30 days'.
- Assets Not Covered**: A card showing '33'.

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
SMDIRECT101	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA

2. Clique no ícone Admin Center. A janela Fontes de dados é aberta.











Origem dos dados

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

Add Data Source

Search data sources Q

-  **Cisco Catalyst SD-WAN Manager**
Supports the Success Track for WAN [Add Data Source](#)
-  **Cisco DNA Center**
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types) [Add Data Source](#)
-  **Contracts**
Supports assets associated with a contract [Add Data Source](#)
-  **CX Cloud Agent**
Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks [Add Data Source](#)
-  **Firewall Management Center**
Supports Cisco Secure Firewall [Add Data Source](#)
-  **Intersight**
Supports the Data Center Compute and Cloud Network Success Tracks [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](#)

Adicionar Fonte de Dados

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

Set Up CX Cloud Agent
0% complete

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

Review deployment requirements
Prepare your network for CX Cloud Agent

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

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

For **AWS US** centers:

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

Review the CX Cloud Agent Overview for complete hardware and software prerequisites.

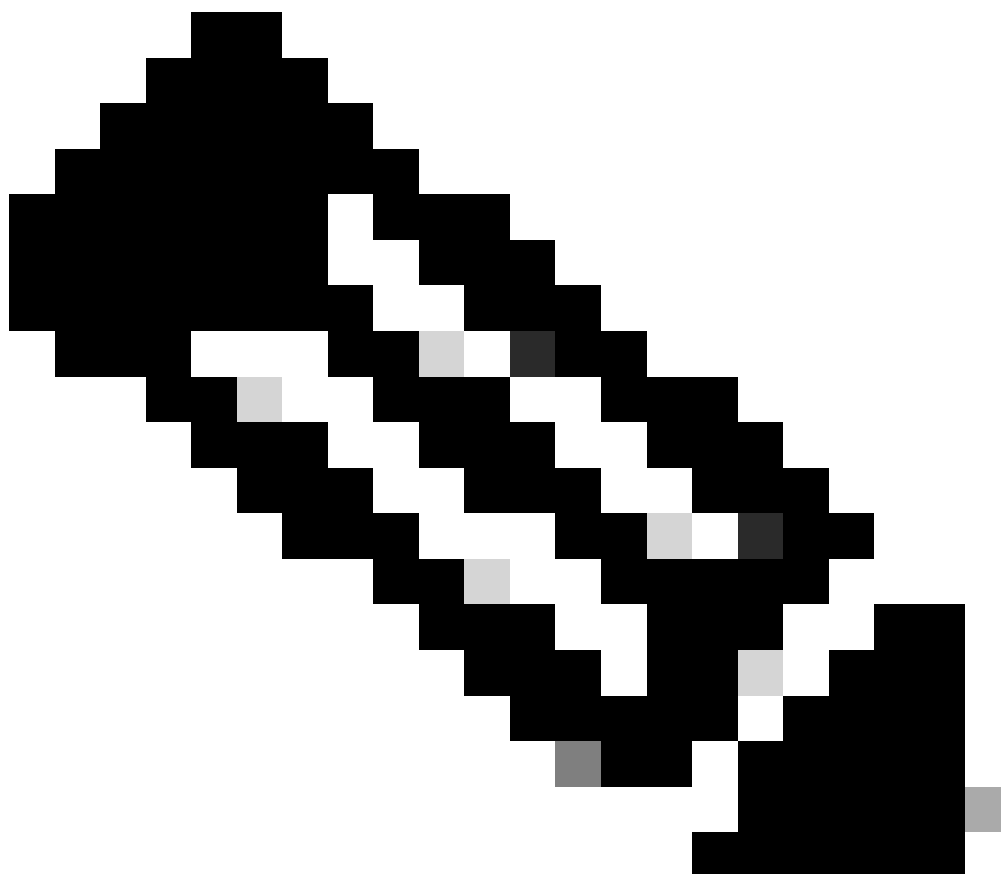
CX Cloud takes security seriously. Review the Security section of the CX Cloud Agent Overview to learn how CX Cloud Agent handles and stores your data.

I set up this configuration on port 443

[Download on Cisco.com](#)

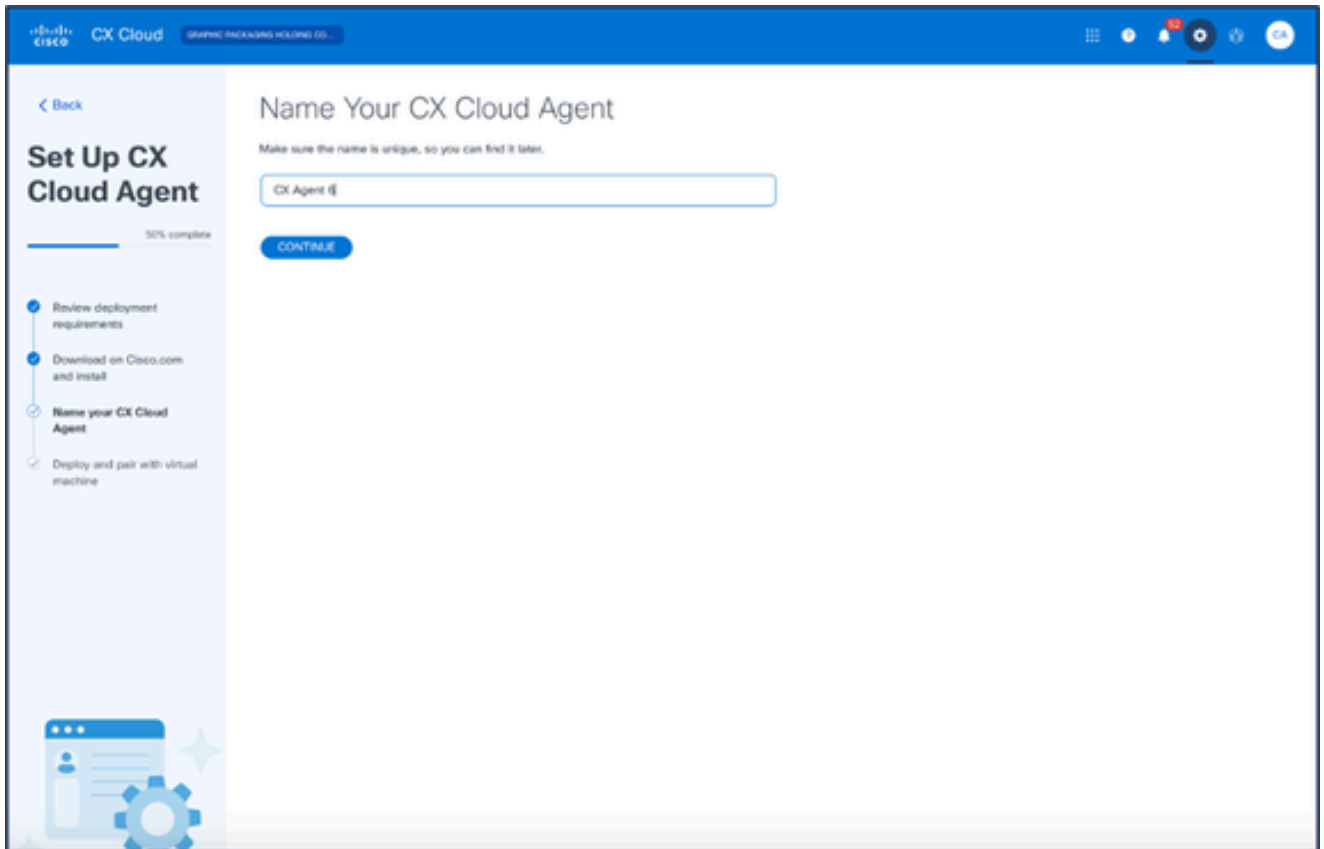
Configurar o CX Cloud Agent

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 página Download de software é aberta.
7. Faça o download do arquivo OVA do CX Cloud Agent v2.4.



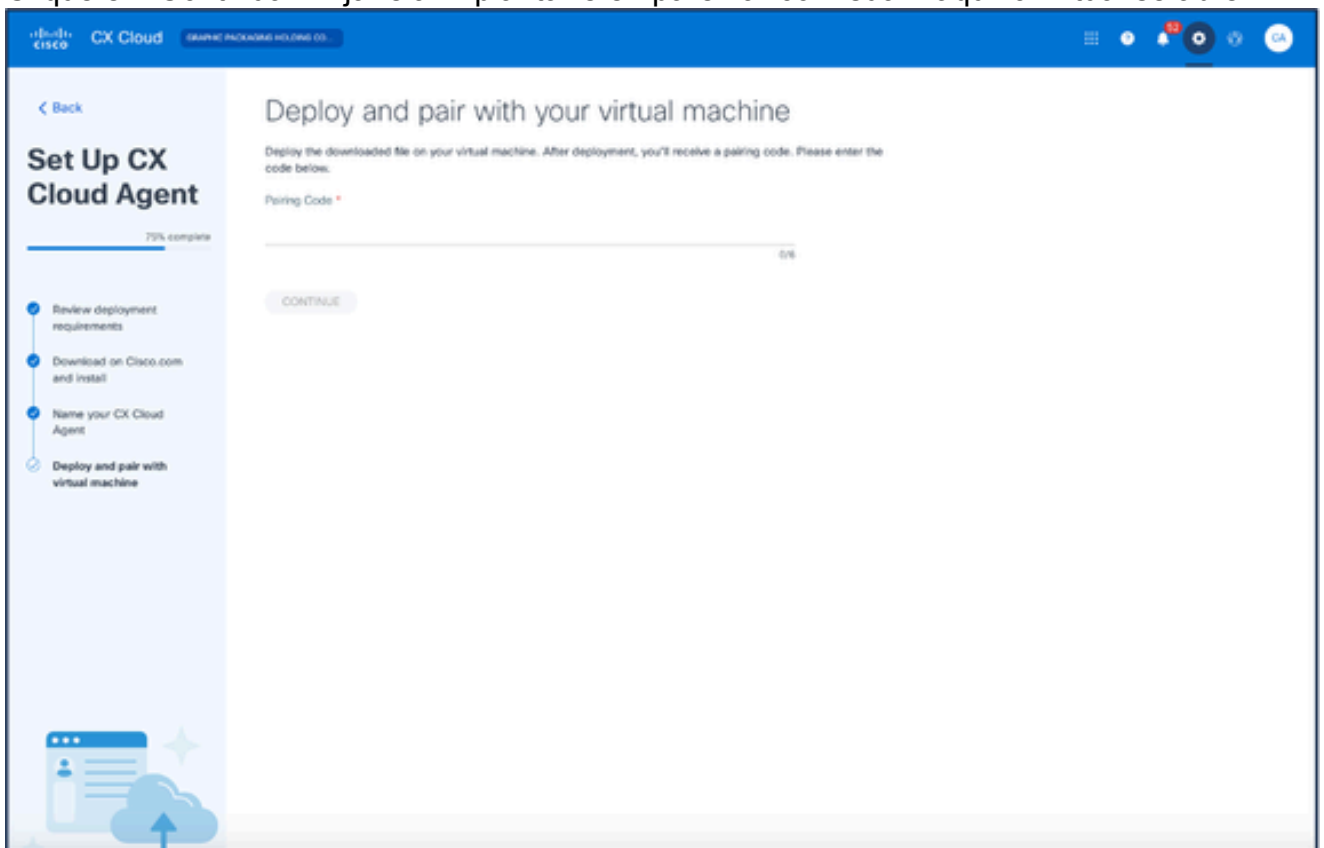
Observação: um código de emparelhamento, necessário para concluir a configuração do CX Cloud Agent, é gerado após a implantação do arquivo OVA.

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



Nomeie seu agente de nuvem do CX

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



Implante e emparelhe com sua máquina virtual

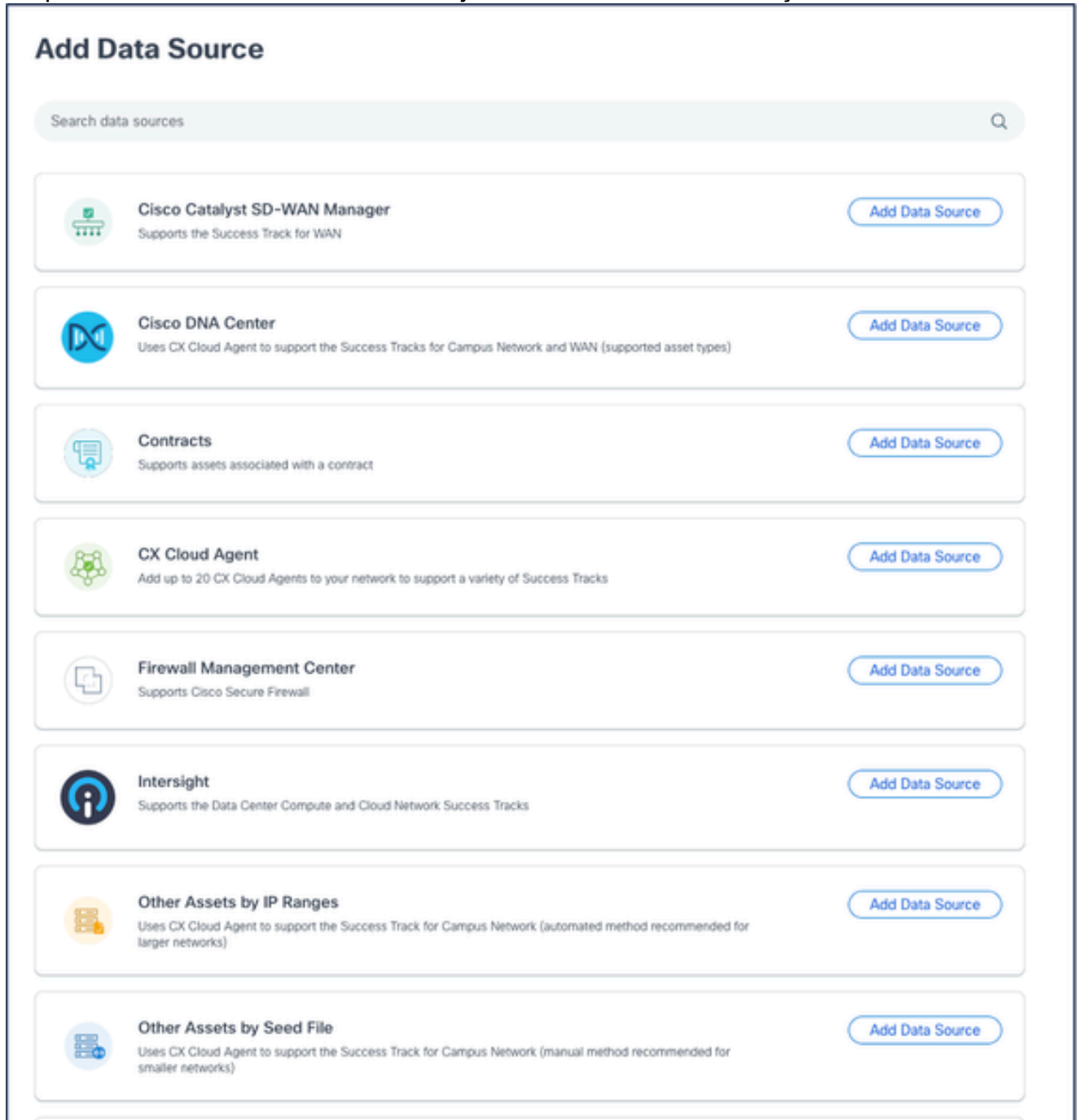
10. Insira o código de emparelhamento recebido após a implantação do arquivo OVA baixado.

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

Adicionando o Cisco DNA Center como fonte de dados

Para adicionar o Cisco DNA Center como fonte de dados:

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



Add Data Source

Search data sources

- Cisco Catalyst SD-WAN Manager**
Supports the Success Track for WAN
- Cisco DNA Center**
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)
- Contracts**
Supports assets associated with a contract
- CX Cloud Agent**
Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks
- Firewall Management Center**
Supports Cisco Secure Firewall
- Intersight**
Supports the Data Center Compute and Cloud Network Success Tracks
- Other Assets by IP Ranges**
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)
- Other Assets by Seed File**
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

Adicionar Fonte de Dados

2. Clique em Adicionar fonte de dados na opção Cisco DNA Center.

Which CX Cloud Agent Do You Want to Connect to?

Select option ▼



Selecionar CX Cloud Agent

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

Connect to CX Cloud

Connect a Cisco DNA Center (2 of 2)

IP Address or FQDN *

City * ▼

Username *

Password *

Schedule inventory collection

Frequency ▼ Select time ▼ AM ▼ Time Zone ▼

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

Conectar-se à nuvem CX

5. Digite o seguinte no Conectar um Cisco DNA Center:

- Endereço IP virtual ou FQDN (isto é, endereço IP do Cisco DNA Center),
- Cidade (ou seja, a localização do Cisco DNA Center),
- Nome de usuário
- Senha
- Frequência, Hora e Fuso Horário para indicar com que frequência o CX Cloud Agent deve executar verificações de rede nas seções Agendar Coleta de Inventário.
Observação: marque a caixa de seleção Executar a primeira coleta agora para executar a coleta agora.

6. Clique em Conectar. Uma confirmação é exibida com o endereço IP do Cisco DNA Center.

Adição de Outros Ativos como Origens de Dados

A coleta de telemetria foi estendida a dispositivos não gerenciados pelo Cisco DNA Center, permitindo que os clientes visualizem e interajam com análises e informações derivadas da telemetria para uma variedade maior de dispositivos. Após a configuração inicial do CX Cloud Agent, os usuários têm a opção de configurar o CX Cloud Agent para se conectar a mais 20 Cisco DNA Centers 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 pode ser examinado pelo CX Cloud Agent. Ambas as abordagens dependem do Simple Network Management Protocol (SNMP) para fins de descoberta (SNMP) 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:

- Carregue um arquivo de seed usando um modelo de arquivo de seed.
- Forneça 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 CX Cloud Agent oferece suporte a SNMPV2c e SNMP V3 e uma ou ambas as versões podem ser configuradas. As mesmas informações, descritas em seguida 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 integrado para o SNMPv3. Se ambas as

versões do SNMP forem configuradas pelo usuário, o CX Cloud Agent poderá, por padrão, tentar se comunicar com cada dispositivo respectivo usando SNMPv3 e reverter para 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 pode 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. Na ausência de 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 (nomes de usuário e senhas) enviadas através do telnet não são criptografadas e, portanto, vulneráveis a comprometimento, sem segurança adicional.

Limitação 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. As limitações de instrumentação do dispositivo impedem o processamento de telemetria de tais dispositivos.
- Se um dispositivo do arquivo de seed ou das coleções de intervalos IP também fizer parte do inventário do Cisco DNA Center, o dispositivo será relatado apenas uma vez para a entrada do Cisco DNA Center. Os respectivos dispositivos dentro da entrada do intervalo de IP/arquivo de seed são ignorados para evitar duplicação.


Adicionando outros ativos usando um arquivo de propagação

Um arquivo de seed 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 a partir do qual a telemetria pode ser coletada pelo CX Cloud 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 CX Cloud Agent pode tentar se conectar aos dispositivos, mas não pode processar cada um para ser exibido nas páginas Ativos nos casos em que não é possível 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.

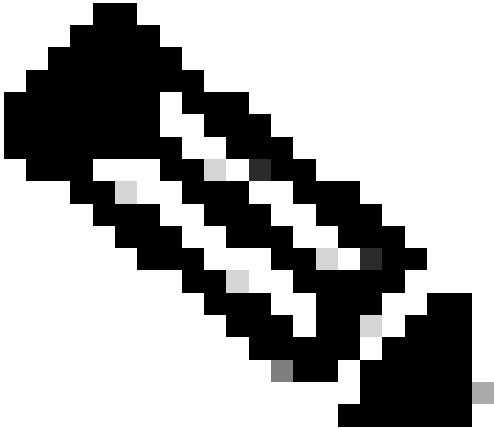
É importante que o formato do arquivo semente de exemplo, incluindo os cabeçalhos das colunas, não seja alterado de forma alguma. Clique no link fornecido para visualizar um arquivo de seed em formato PDF. Este PDF é apenas para referência e pode ser usado para criar um arquivo de seed que precisa ser salvo no formato .csv.

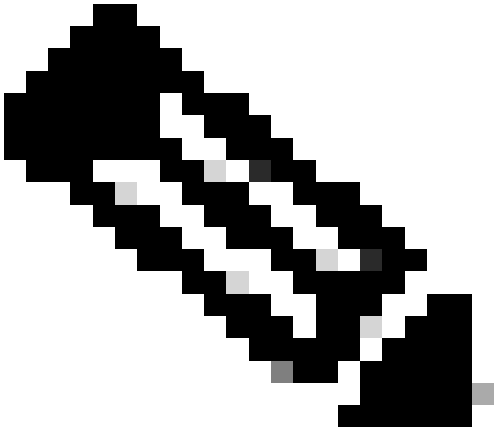
Clique neste [link](#) para exibir um arquivo de seed que pode ser usado para criar um arquivo de seed no formato .csv.

 Observação: este PDF é apenas para referência e pode ser usado para criar um arquivo de seed que precisa ser salvo no formato .csv.

Esta tabela 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 host	Forneça um endereço IP ou nome de host válido e exclusivo do dispositivo.
B	versão do protocolo SNMP	O protocolo SNMP é exigido pelo CX Cloud 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 : os valores podem ser MD5 ou SHA	O protocolo SNMPv3 permite a autenticação através do algoritmo MD5 ou SHA. Se o dispositivo estiver configurado com

Coluna do arquivo de propagação	Cabeçalho/Identificador de Coluna	Finalidade da Coluna
		<p data-bbox="826 293 1458 371">Autenticação segura, o respectivo Algoritmo de autenticação deverá ser fornecido.</p>  <p data-bbox="922 965 1461 1084">Observação: MD5 é considerado inseguro e SHA pode ser usado em todos os dispositivos que o suportam.</p>
F	snmpv3AuthPassword : 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	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.

Coluna do arquivo de propagação	Cabeçalho/Identificador de Coluna	Finalidade da Coluna
		 <p data-bbox="922 846 1461 1093">Observação: as chaves de 56 bits usadas pelo DES são consideradas muito curtas para fornecer segurança criptográfica e que o 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 exclusiva que representa o dispositivo, especifique a ID do mecanismo se configurada manualmente no dispositivo	O EngineID SNMPv3 é um ID exclusivo que representa cada dispositivo. Essa ID do mecanismo é enviada como referência durante a coleta dos conjuntos de dados SNMP pelo CX Cloud Agent. Se o cliente configurar o EngineID manualmente, o respectivo EngineID precisará ser fornecido.
J	cliProtocol: os valores podem ser 'telnet', 'sshv1', 'sshv2'. Se vazio, pode ser definido como 'sshv2' por padrão	A CLI tem a finalidade de interagir diretamente com o dispositivo. O CX Cloud Agent usa esse protocolo para a coleta de CLI para um dispositivo específico. Esses dados de coleta de CLI são usados para ativos e outros relatórios de insights na nuvem CX. O SSHv2 é recomendado; na ausência de outras

Coluna do arquivo de propagação	Cabeçalho/Identificador de Coluna	Finalidade da Coluna
		medidas de segurança de rede, os protocolos SSHv1 e Telnet não fornecem segurança de transporte adequada.
K	cliPort : número da 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.
I	cliUser : Nome 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.)	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 Cloud 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

Coluna do arquivo de propagação	Cabeçalho/Identificador de Coluna	Finalidade da Coluna
R	Suporte futuro (sem necessidade de entradas)	Reservado para uso futuro
S	Suporte futuro (sem necessidade de entradas)	Reservado para uso futuro

Adicionar outros ativos usando um novo arquivo de propagação

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.

The screenshot shows the 'Add Data Source' page in the Cisco CX Cloud interface. At the top, there is a search bar labeled 'Search data sources'. Below it, there is a list of seven data source options, each with an icon, a title, a brief description, and an 'Add Data Source' button.

- Cisco Catalyst SD-WAN Manager**: Supports the Success Track for vWAN
- Cisco DNA Center**: Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)
- Contracts**: Supports assets associated with a contract
- CX Cloud Agent**: Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks
- Intersight**: Supports the Data Center Compute and Data Center Network Success Tracks
- Other Assets by IP Ranges**: Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)
- Other Assets by Seed File**: Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

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 CX Cloud Agent

3. Selecione o CX Cloud 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](#)

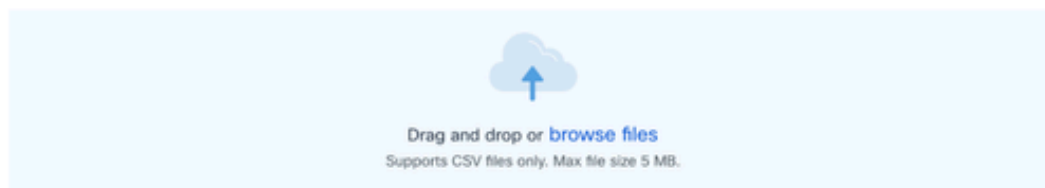


Continuar

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

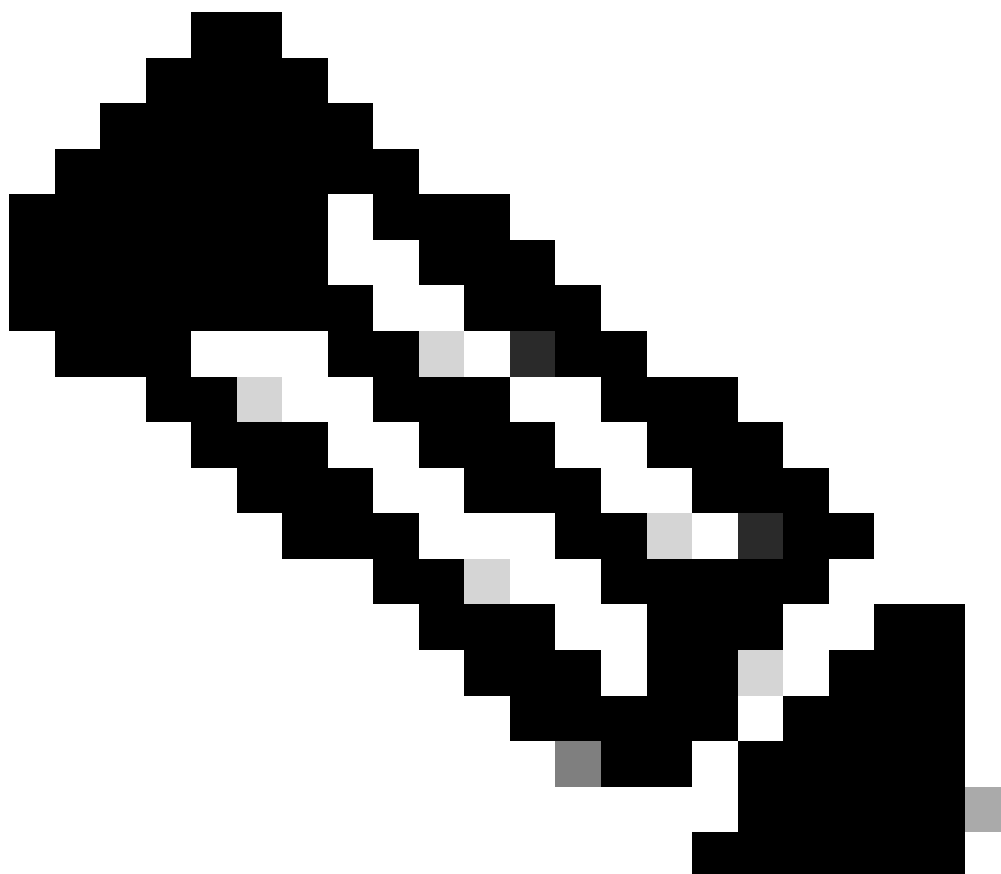
Frequency	Select time	Time Zone	
Frequency ▾	12:00 ▾	AM ▾	Europe/Amsterdam (... ▾

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 Cloud Agent.
7. Arraste e solte ou clique em procurar arquivos para carregar o arquivo .csv.
8. Conclua a seção Agendar coleta de inventário.




Observação: antes da conclusão da configuração inicial do CX Cloud, o CX Cloud Agent deve executar 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.

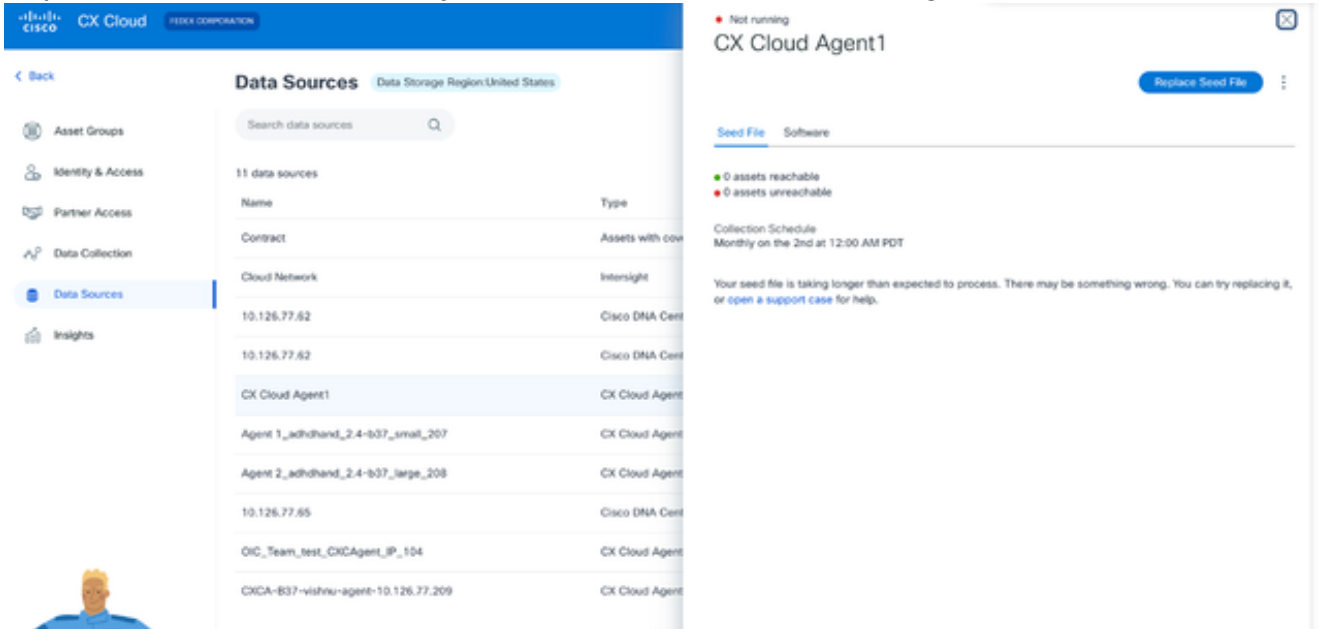
Adicionar outros ativos usando um arquivo de propagação modificado

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

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

 Observação: para adicionar ativos ao arquivo seed, anexe esses ativos ao arquivo 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 CX Cloud Agent que requer um arquivo semente atualizado. A janela de detalhes do CX Cloud Agent é aberta.

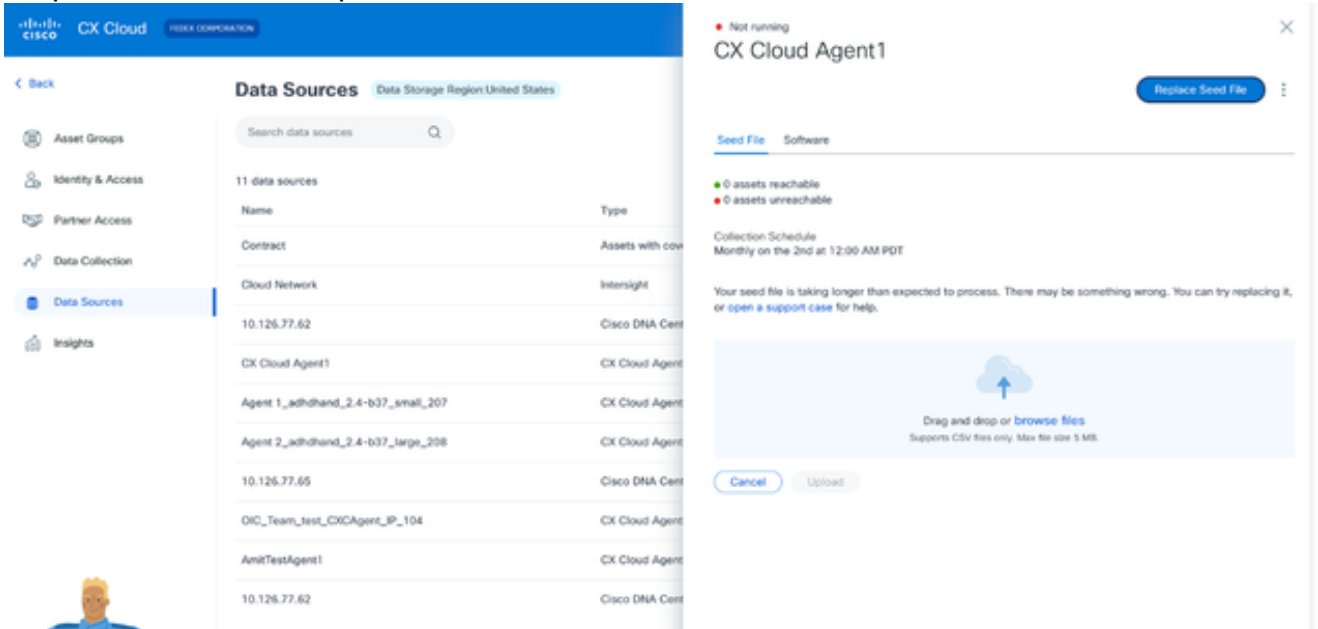


The screenshot shows the Cisco CX Cloud interface. On the left, the 'Data Sources' page is visible, listing 11 data sources. The 'CX Cloud Agent1' source is highlighted. On the right, the 'CX Cloud Agent1' details modal is open, showing a 'Replace Seed File' button and a message indicating that the seed file is taking longer than expected to process.

Name	Type
Contract	Assets with cov
Cloud Network	Intersight
10.126.77.62	Cisco DNA Cent
10.126.77.62	Cisco DNA Cent
CX Cloud Agent1	CX Cloud Agent
Agent 1_adhdhand_2.4-b37_small_207	CX Cloud Agent
Agent 2_adhdhand_2.4-b37_large_208	CX Cloud Agent
10.126.77.65	Cisco DNA Cent
OIC_Team_test_CXCAGENT_IP_104	CX Cloud Agent
CXCA-B37-vishnu-agent-10.126.77.209	CX Cloud Agent

Janela Detalhes do agente de nuvem CX

3. Clique em Substituir arquivo semente.



The screenshot shows the same Cisco CX Cloud interface as before. The 'CX Cloud Agent1' details modal is open, and the 'Replace Seed File' dialog is displayed. The dialog prompts the user to 'Drag and drop or browse files' and includes a 'Cancel' button and an 'Upload' button.

janela do CX Cloud Agent

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

Adicionar outros ativos usando intervalos de IP

Os intervalos de IP permitem que os usuários identifiquem ativos de hardware e, subsequentemente, colem 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 CX Cloud Agent 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 Cloud Agent não tentará se comunicar com um dispositivo que tenha esse endereço IP, nem coletará telemetria desse dispositivo.
- Inserir *.*.*.* permite que o CX Cloud Agent 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 CX Cloud Agent tentará se conectar aos dispositivos, mas talvez não seja capaz de 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 Cloud Agent.

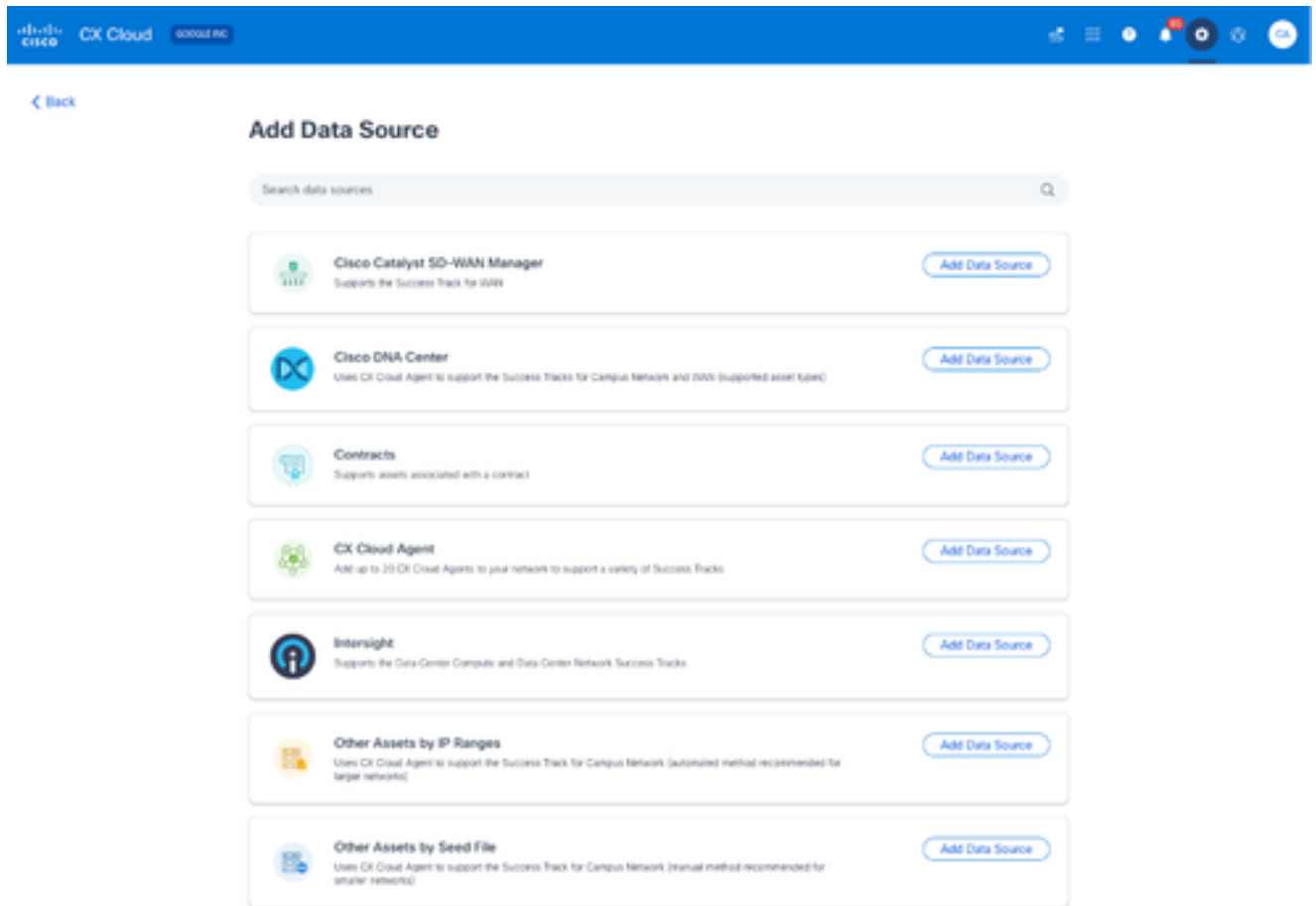
Adicionar dispositivos usando um intervalo de IPs exige que os usuários especifiquem todas as credenciais aplicáveis por meio da interface de usuário da configuração. Os campos visíveis variam de acordo com os protocolos selecionados nas janelas anteriores. Se várias seleções forem feitas para o mesmo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

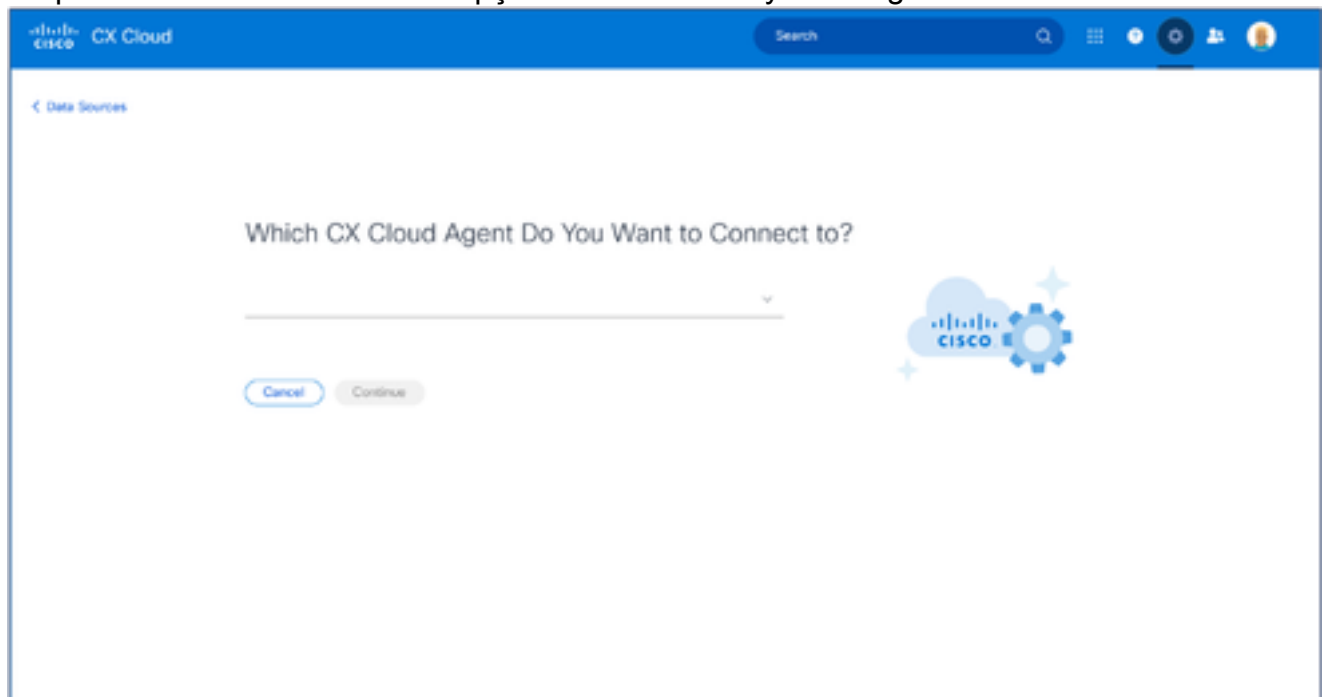
Para adicionar dispositivos usando o intervalo IP:

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



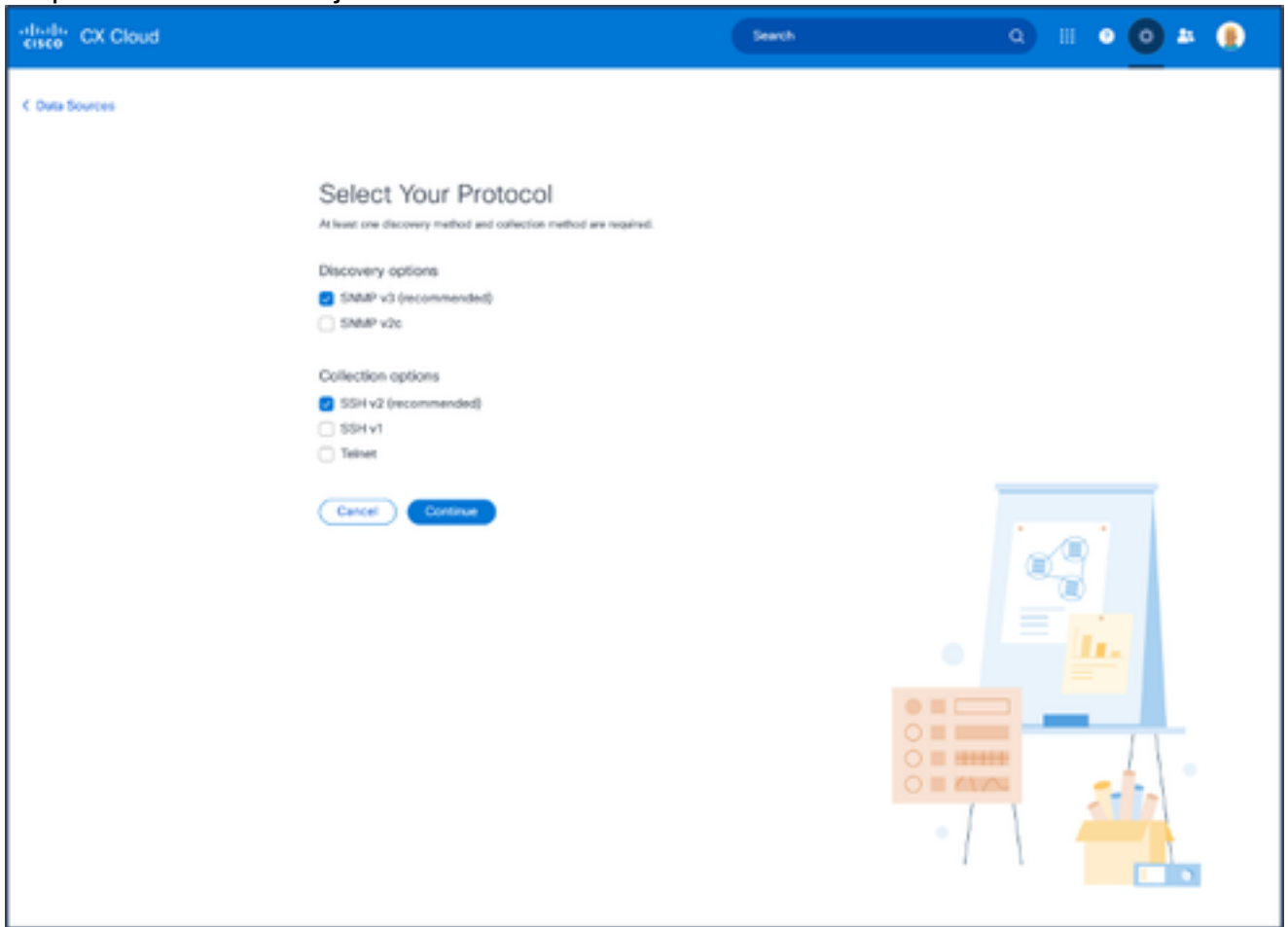
Adicionar Fontes de Dados

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



Selecionar CX Cloud Agent

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



Selecione seu protocolo

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

CISCO CX Cloud Search

← Data Sources

Provide Discovery Details

[Edit protocol](#)

Starting IP address: 198.89.09.2 Ending IP address: 198.89.09.10

SNMP v3 credentials

Username: Manager1505 Engine ID: 1uto50102

Authorization algorithm: MD5 Authorization password: *****

Privacy algorithm: DES Authorization password: *****

SSH v2 credentials

Username: Manager1505 Enable username (optional): 1uto50102


Password: MD5 Enable password (optional): *****

Schedule Inventory Collection

Frequency: Weekly Time: 12:00 AM PST Day: Tuesday

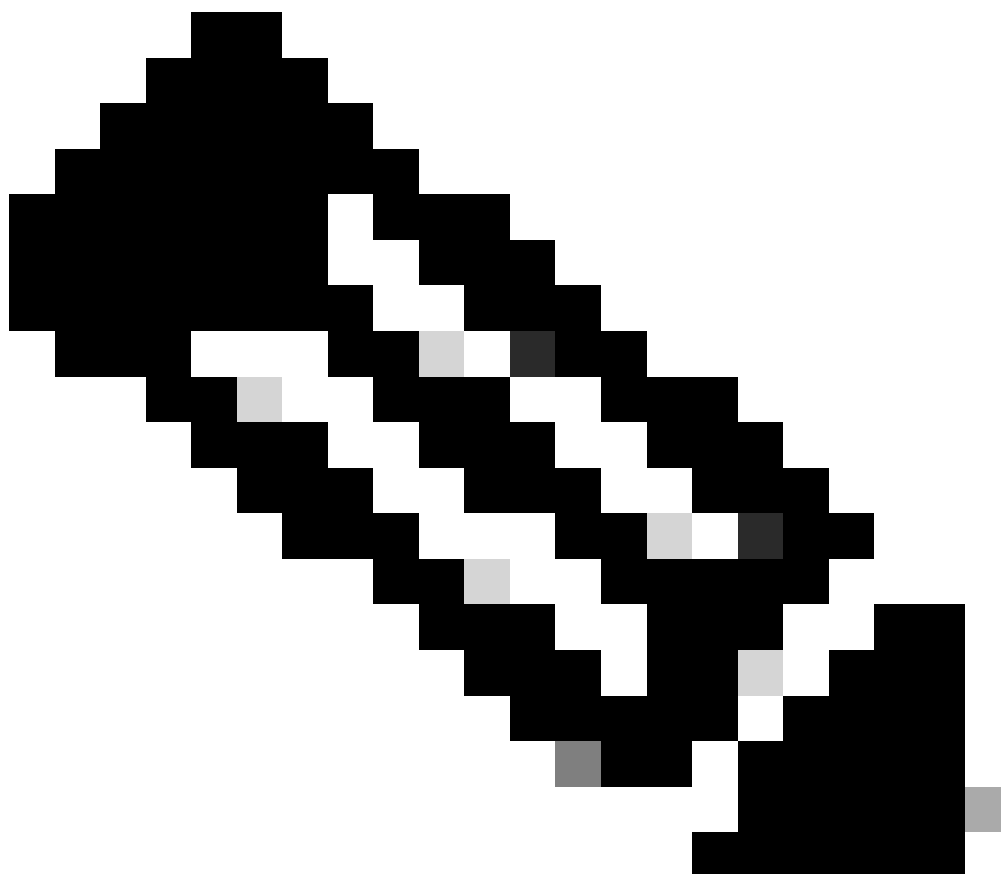
Run the first collection now (may take up to 75 minutes)

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



Seções Fornecer detalhes da descoberta e Agendar coleta de inventário

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



Observação: para adicionar outro intervalo de IP para o CX Cloud Agent selecionado, clique em Add Another IP Range para voltar para a janela Set Your Protocol e repita as etapas nesta seção.

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

Search

My Portfolio

Account

Asset Groups

Identity & Access

Partner Access

Data Collection

Data Sources

Data Sources Region: United States

Search data sources

4 data sources

Name	Type	Date 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
475.92.988.3	Catalyst Center	1 month ago	Reachable
Meraki	Meraki - L1	23 hours ago	Last update succeeded

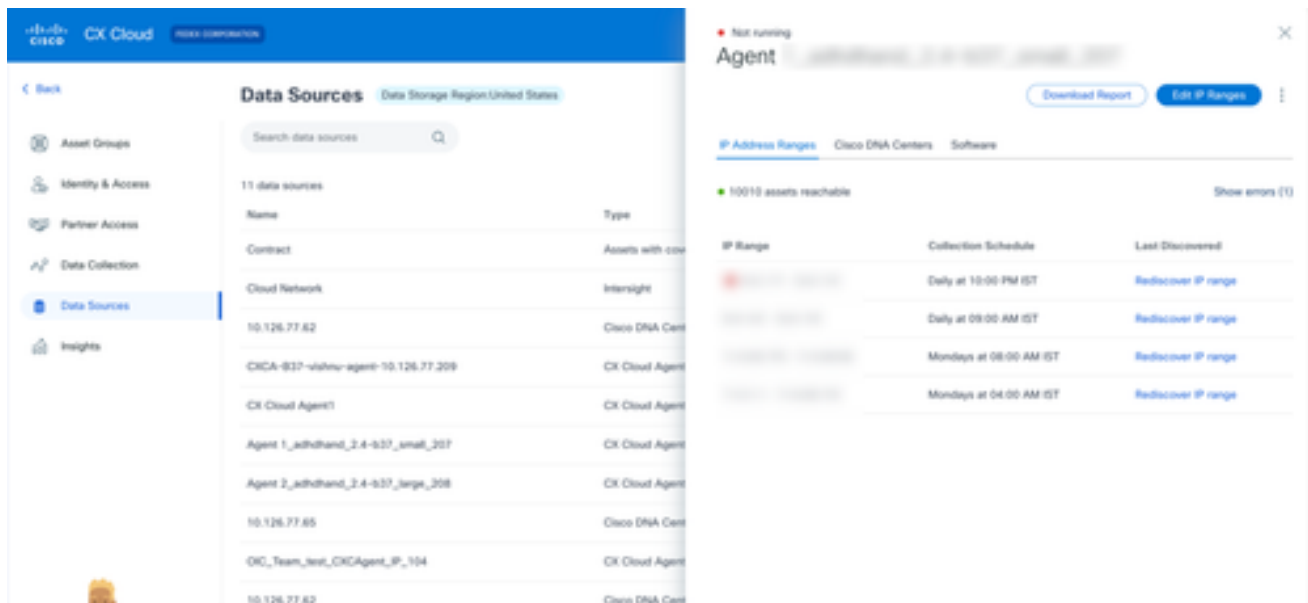
Your IP ranges are being processed. It may take up to an hour to complete.

Mensagem de confirmação

Editando Intervalos IP

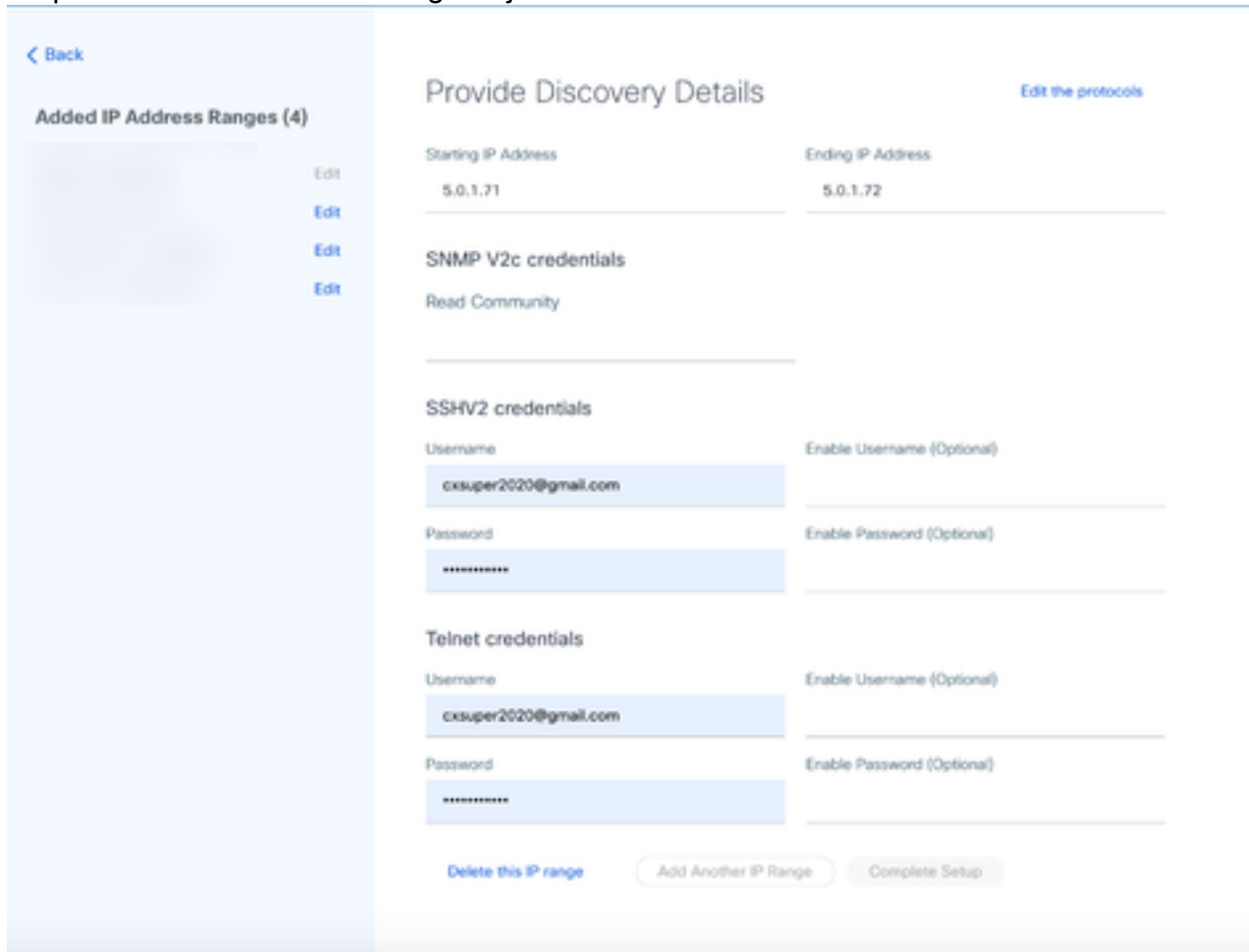
Para editar um intervalo IP;

1. Navegue até a janela Origens de Dados.
2. Clique no CX Cloud Agent que requer a edição do intervalo IP em Data Sources. A janela de detalhes é aberta.



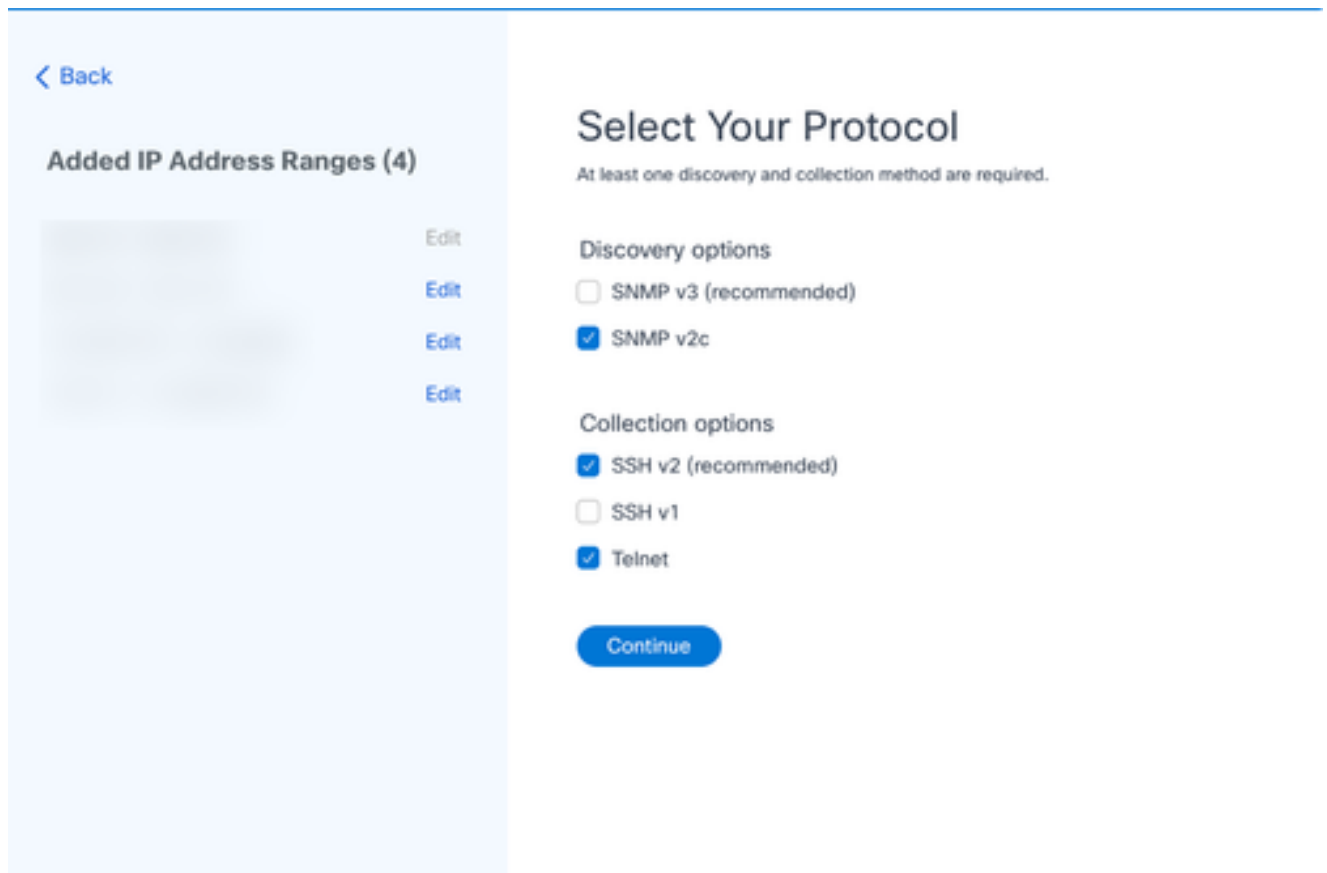
Origem dos dados

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



Fornecer Detalhes da Descoberta

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



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.

[< Back](#)

Added IP Address Ranges (4)

Edit
Edit
Edit
Edit

Provide Discovery Details [Edit the protocols](#)

Starting IP Address: 5.0.1.71 | Ending IP Address: 5.0.1.72

SNMP V2c credentials

Read Community

SSHV2 credentials

Username: | Enable Username (Optional)

Password: | Enable Password (Optional)

Telnet credentials

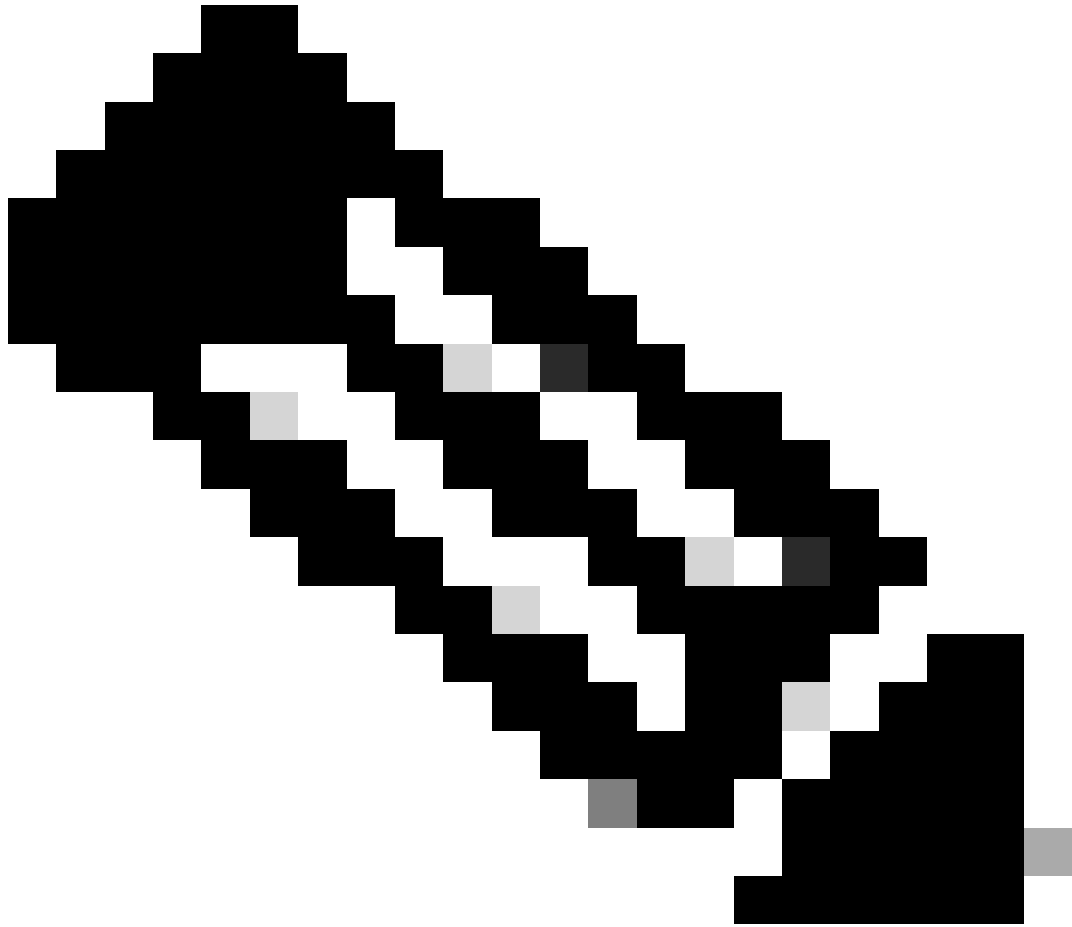
Username: | Enable Username (Optional)

Password: | Enable Password (Optional)

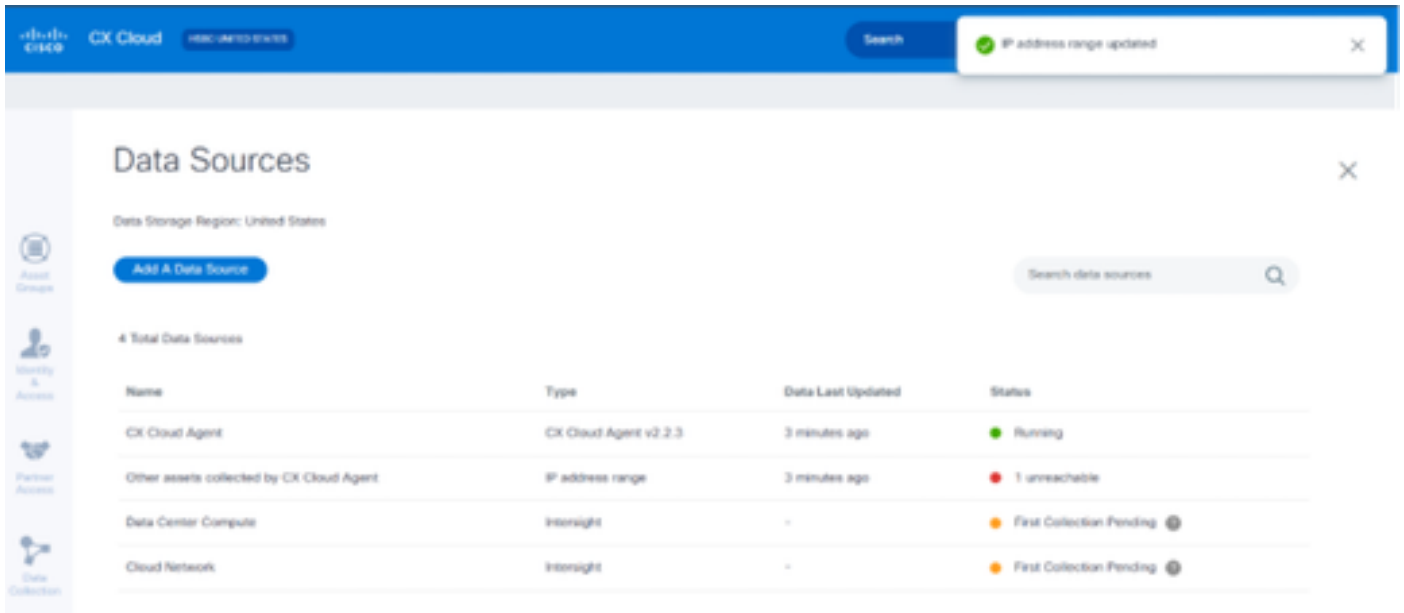
[Delete this IP range](#) | [Add Another IP Range](#) | [Complete Setup](#)

Fornecer Detalhes da Descoberta

6. Edite os detalhes conforme necessário e clique em Concluir Configuração. A janela Fontes de dados é aberta, exibindo uma mensagem confirmando a adição de intervalos de endereços IP recém-adicionados.



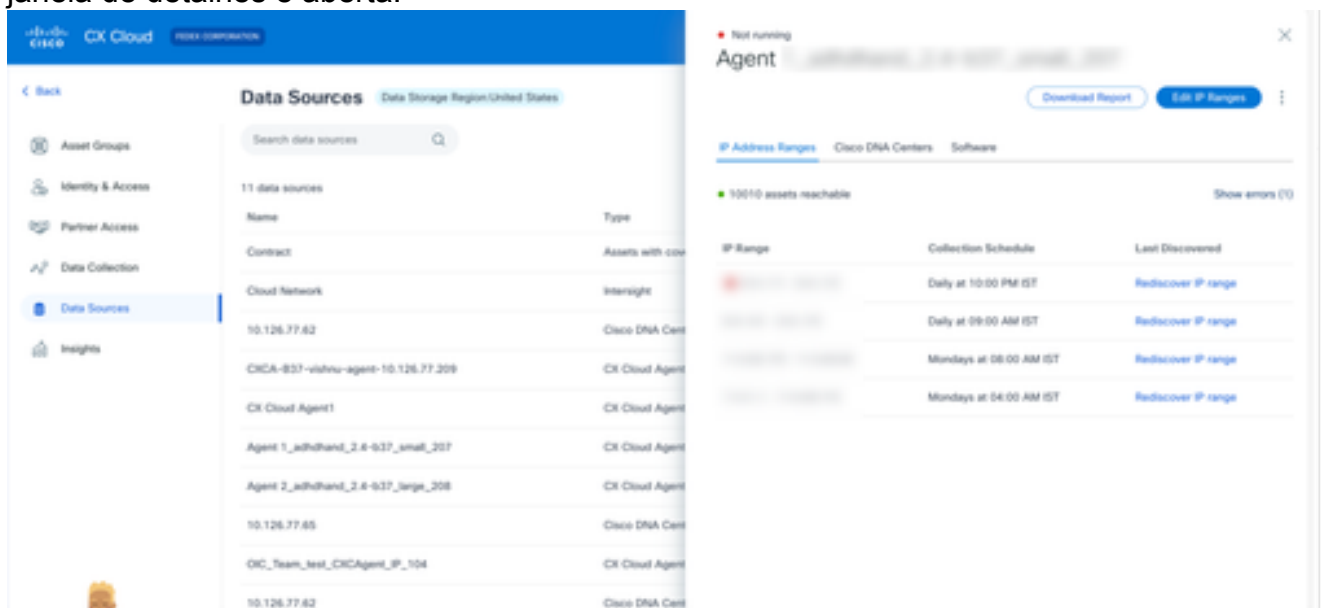
Observação: esta mensagem de confirmação não verifica se os dispositivos dentro do intervalo modificado estão acessíveis ou se suas credenciais são aceitas. Essa confirmação ocorre quando o cliente inicia o processo de descoberta.



Excluindo intervalo de IPs

Para excluir um intervalo IP:

1. Navegue até a janela Origens de Dados.
2. Selecione o respectivo CX Cloud 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.

< Back

Added IP Address Ranges (4)

Edit

Edit

Edit

Edit

Provide Discovery Details

[Edit the protocols](#)

Starting IP Address: 5.0.1.71

Ending IP Address: 5.0.1.72

SNMP V2c credentials

Read Community

SSHV2 credentials

Username: cxsuper2020@gmail.com

Enable Username (Optional)

Password:

Enable Password (Optional)

Telnet credentials

Username: cxsuper2020@gmail.com

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.



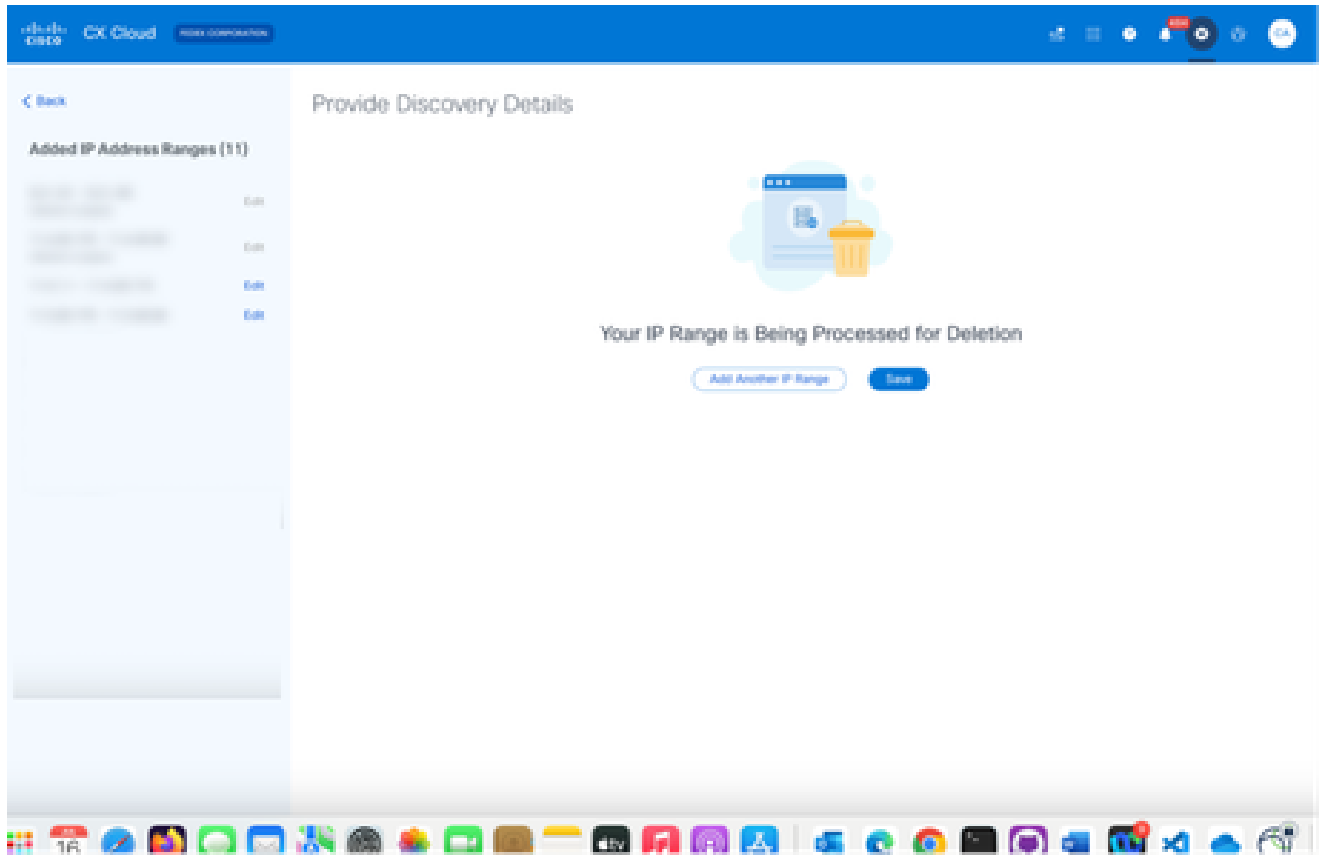
Delete This IP Range

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

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

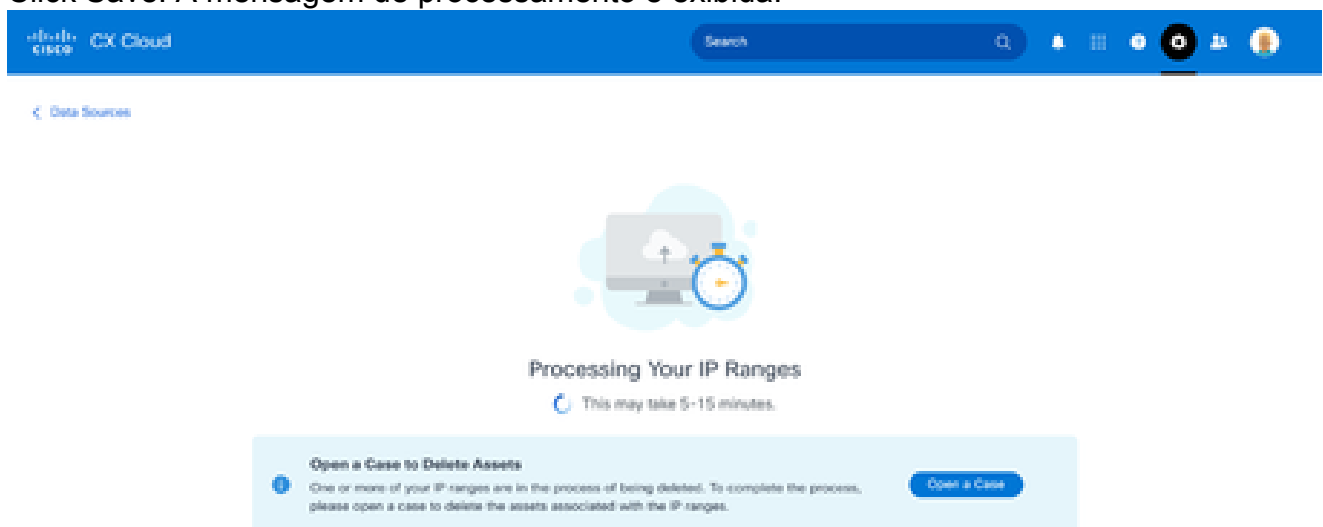
Confirmação - Excluir mensagem

5. Clique em Excluir.



Exclusão de intervalo de IPs

6. Click Save. 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

É possível que alguns dispositivos possam ser descobertos pelo Cisco DNA Center e pela conexão direta do dispositivo com o CX Cloud Agent, 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 CX Cloud Agent gerencia os dispositivos.

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

Programando verificações de diagnóstico

Os clientes podem programar varreduras de diagnóstico sob demanda na nuvem CX.



Observação: a Cisco recomenda programar verificações 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 não se sobreponham. A execução simultânea de várias varreduras de diagnóstico pode retardar o processo de varredura e resultar potencialmente em falhas.

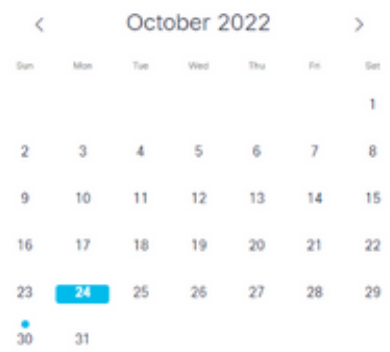
Para programar varreduras de diagnóstico:

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 3

Schedule Scan



No Diagnostic Scans Found

Inventory Collection 3

3 Collections

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

Rapid Problem Resolution

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

Enable for Campus Network

Levantamento de dados

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

Schedule
Frequency at Time IST Save Changes

Description (Optional)

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

Add Remove

Device	Source IP	IP Address
Devices are part of selected list		

1 2 Next

Agendar uma 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.

Data Collection

Diagnostic Scans 2 Scans

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

Schedule Scan

October 2022

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

Edit Schedule Delete Schedule

Inventory Collection 8 Collections

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

Rapid Problem Resolution

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

Enable for Campus Network

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

View detailed instructions

Coleta de Dados com Opções de Editar e Excluir Programação

Atualizando as VMs do CX Cloud 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.

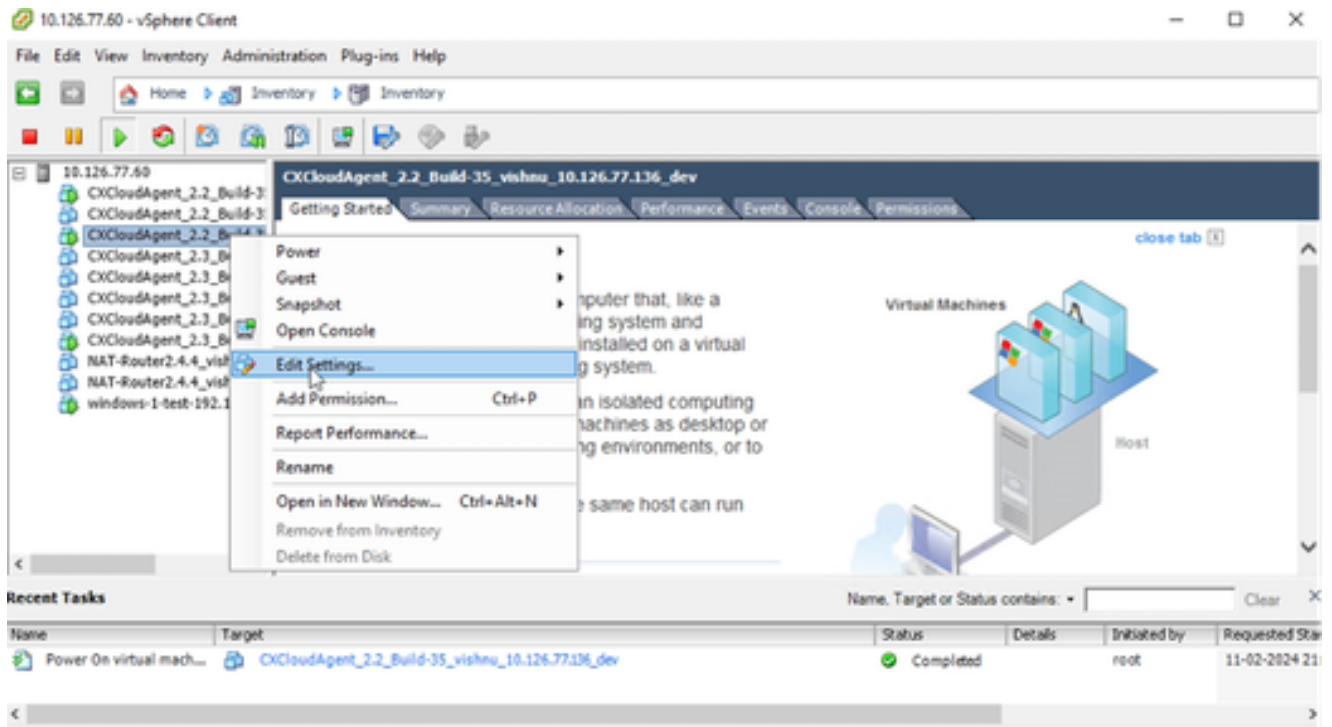
Reconfiguração usando o VMware vSphere Thick Client

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



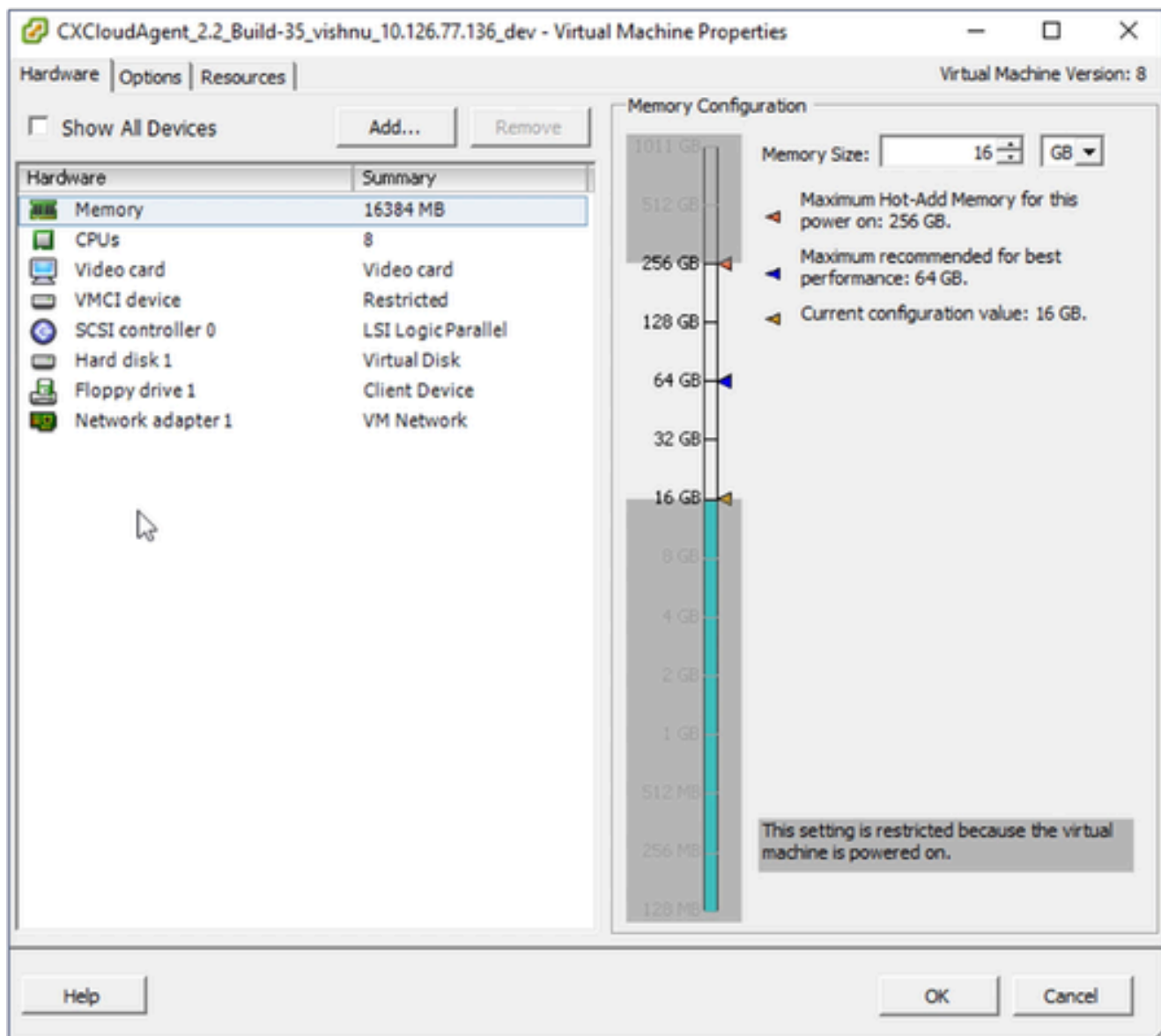
vSphere Client

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



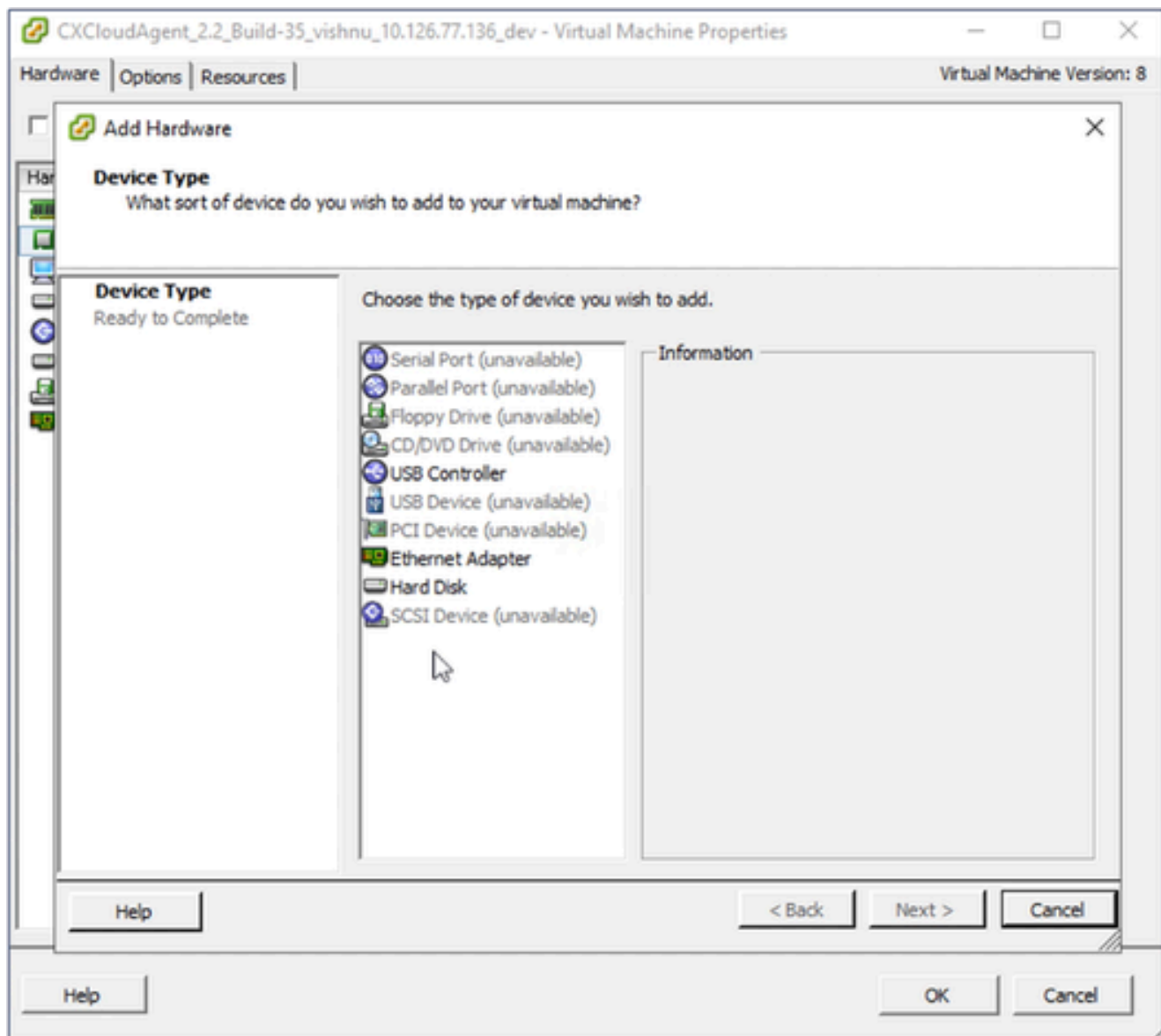
Editar configurações

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.



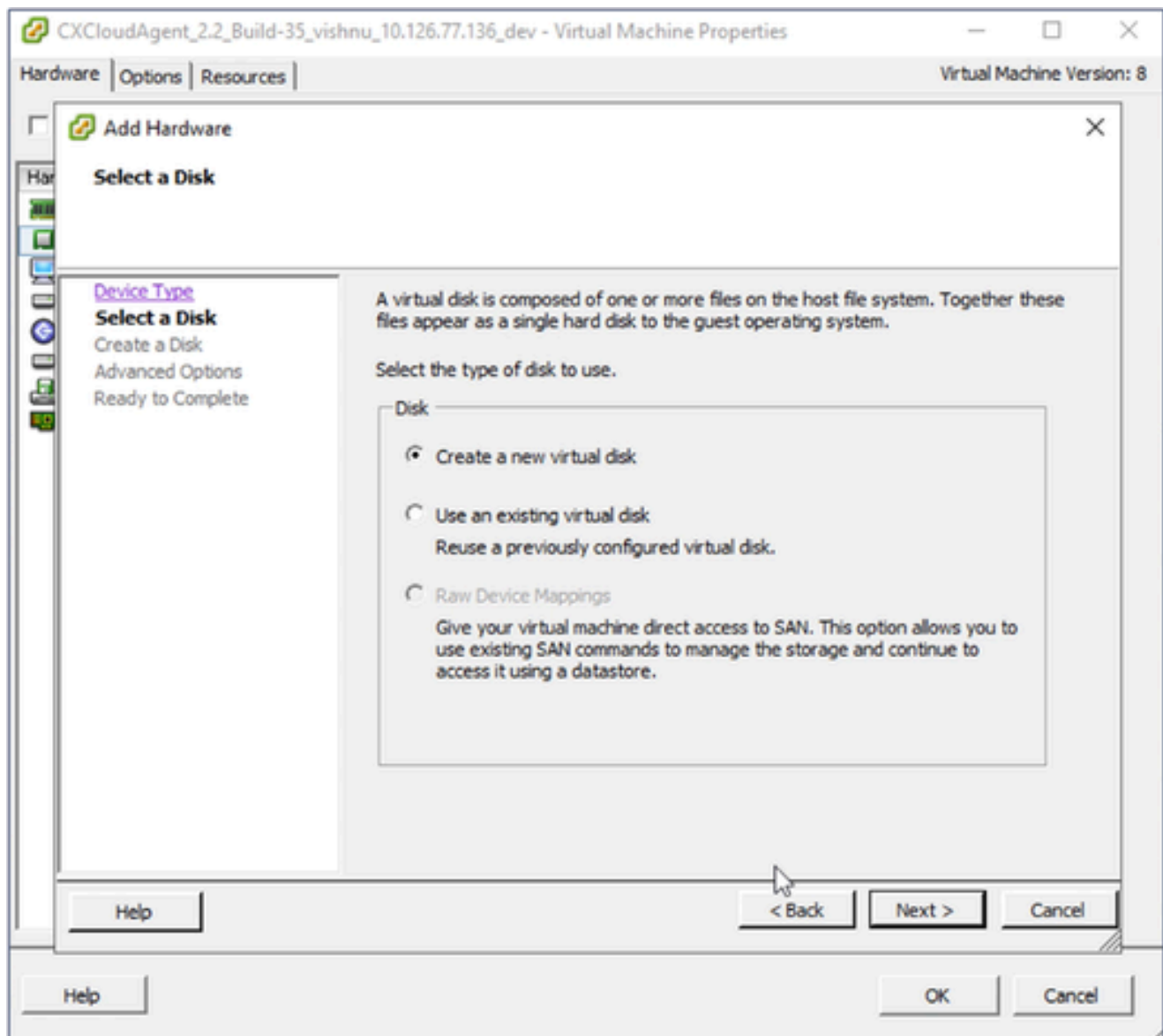
Propriedades da VM

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.



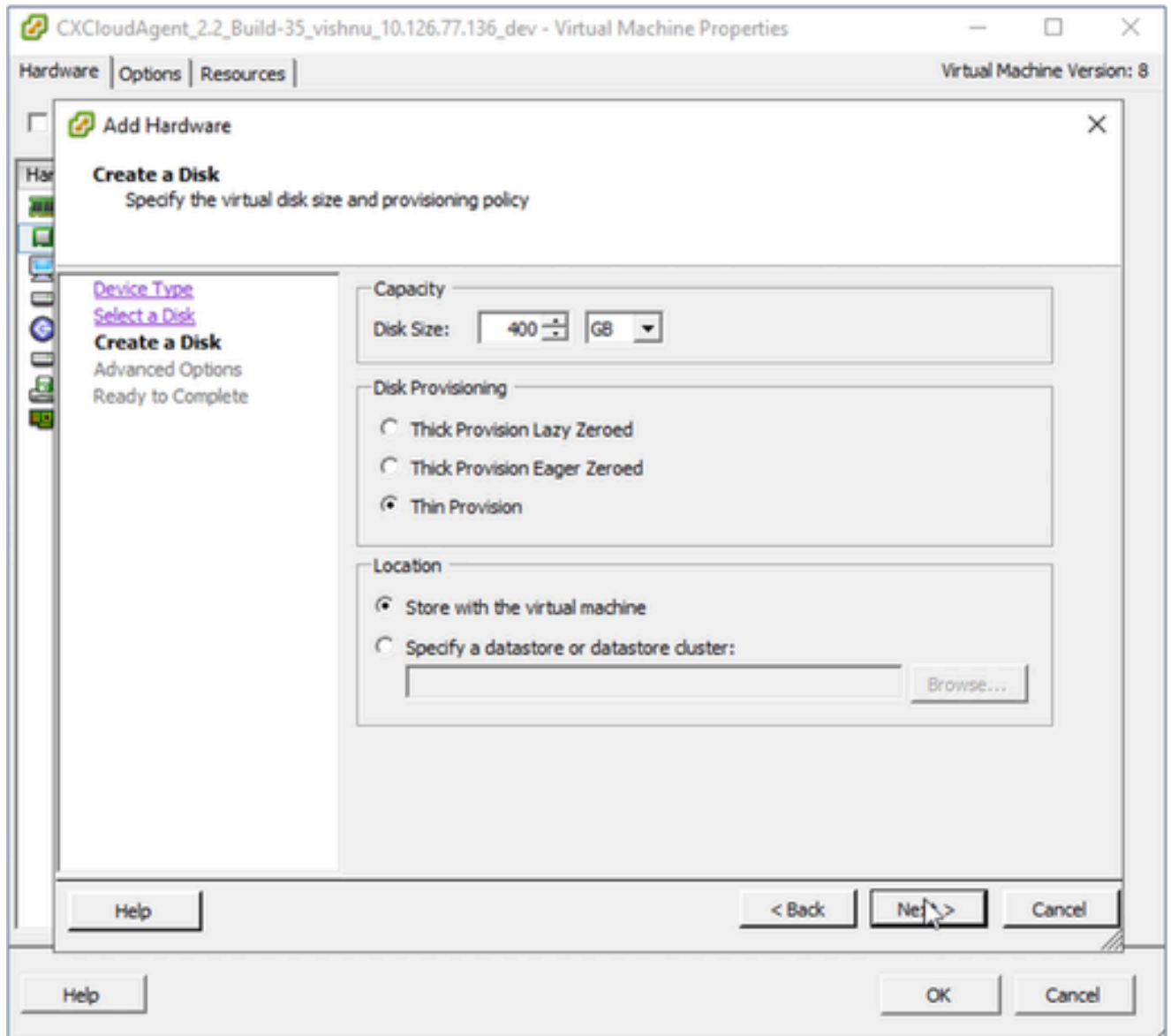
tipo de dispositivo

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



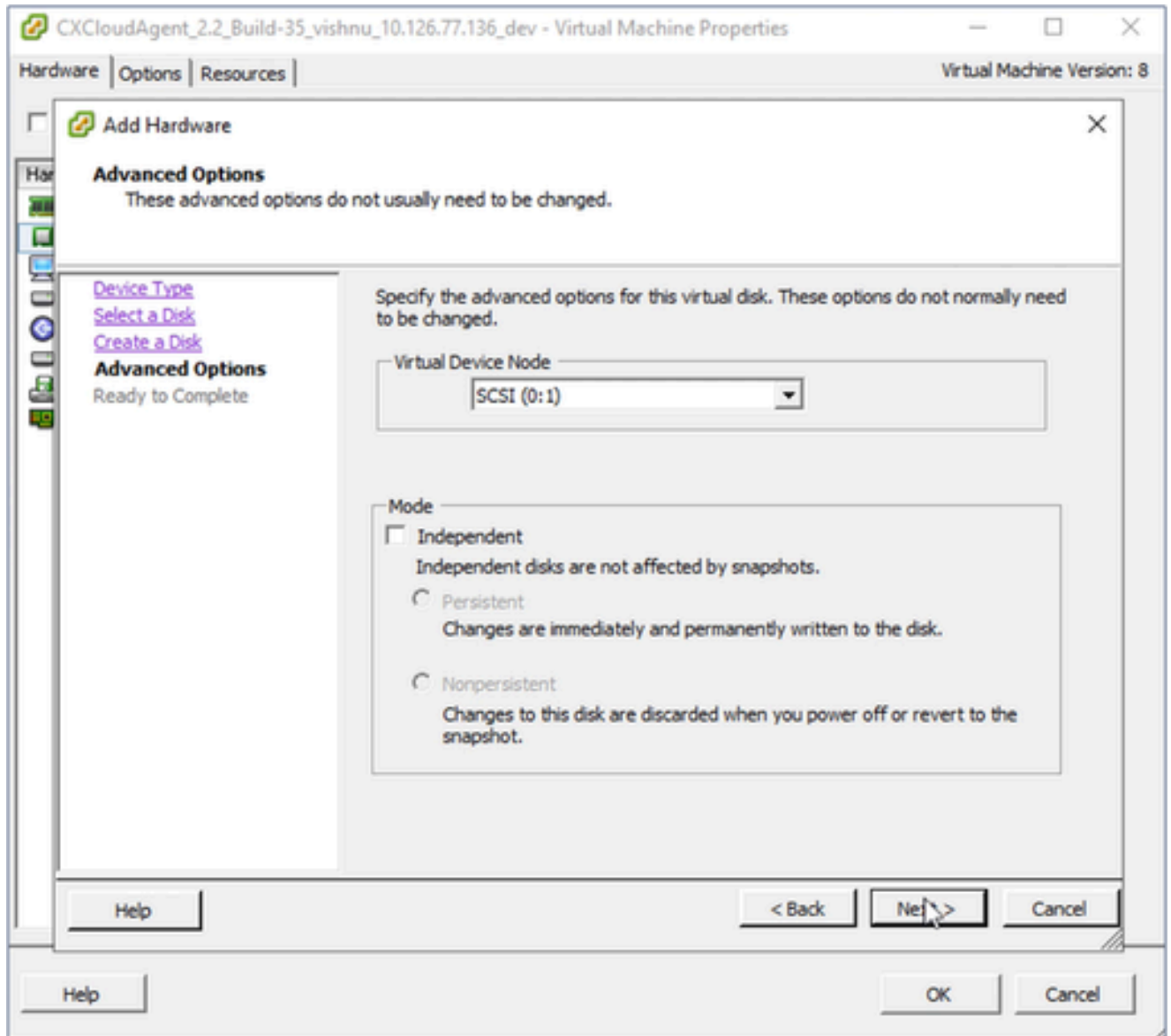
Selecionar disco

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



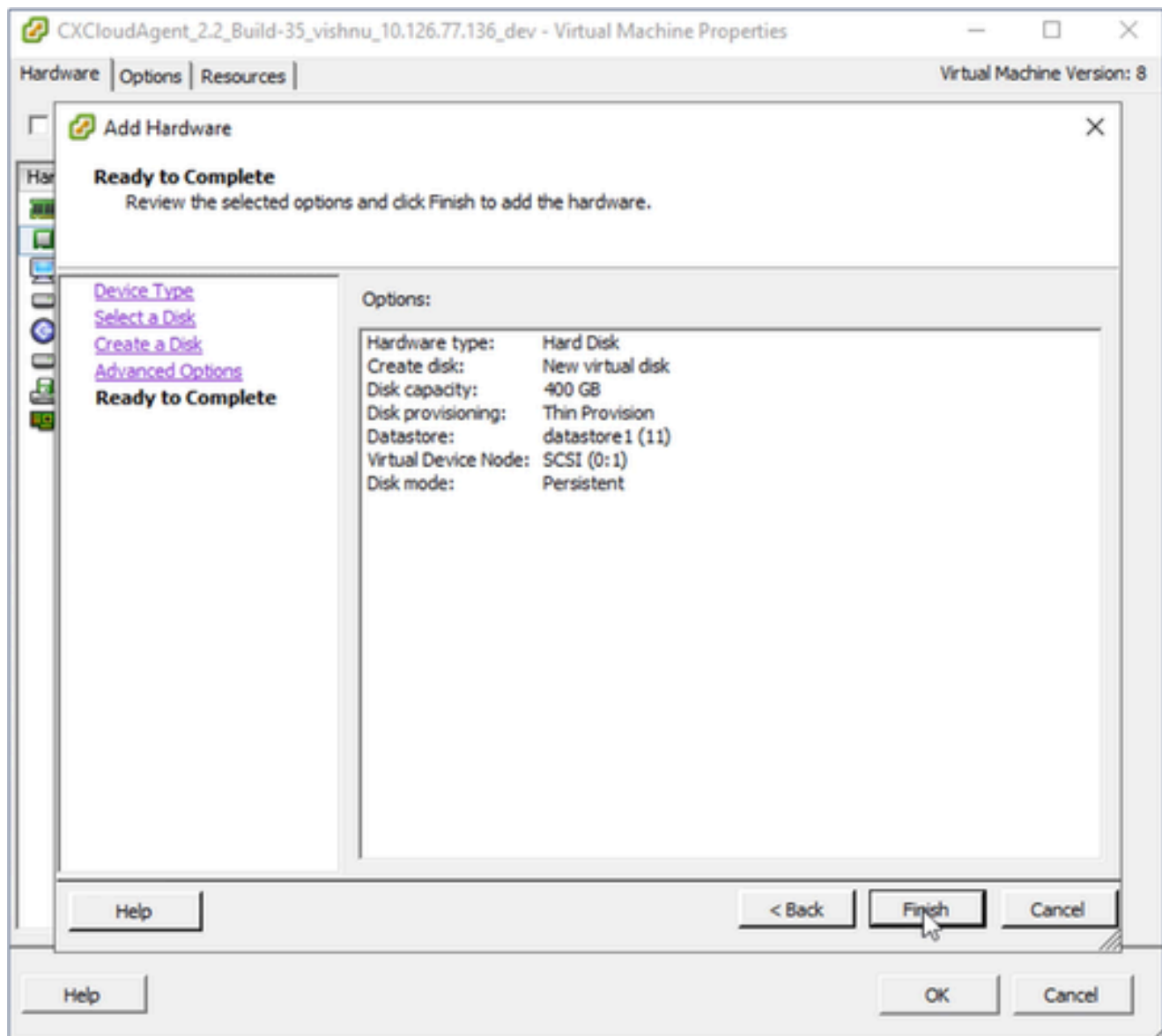
Criar disco

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.



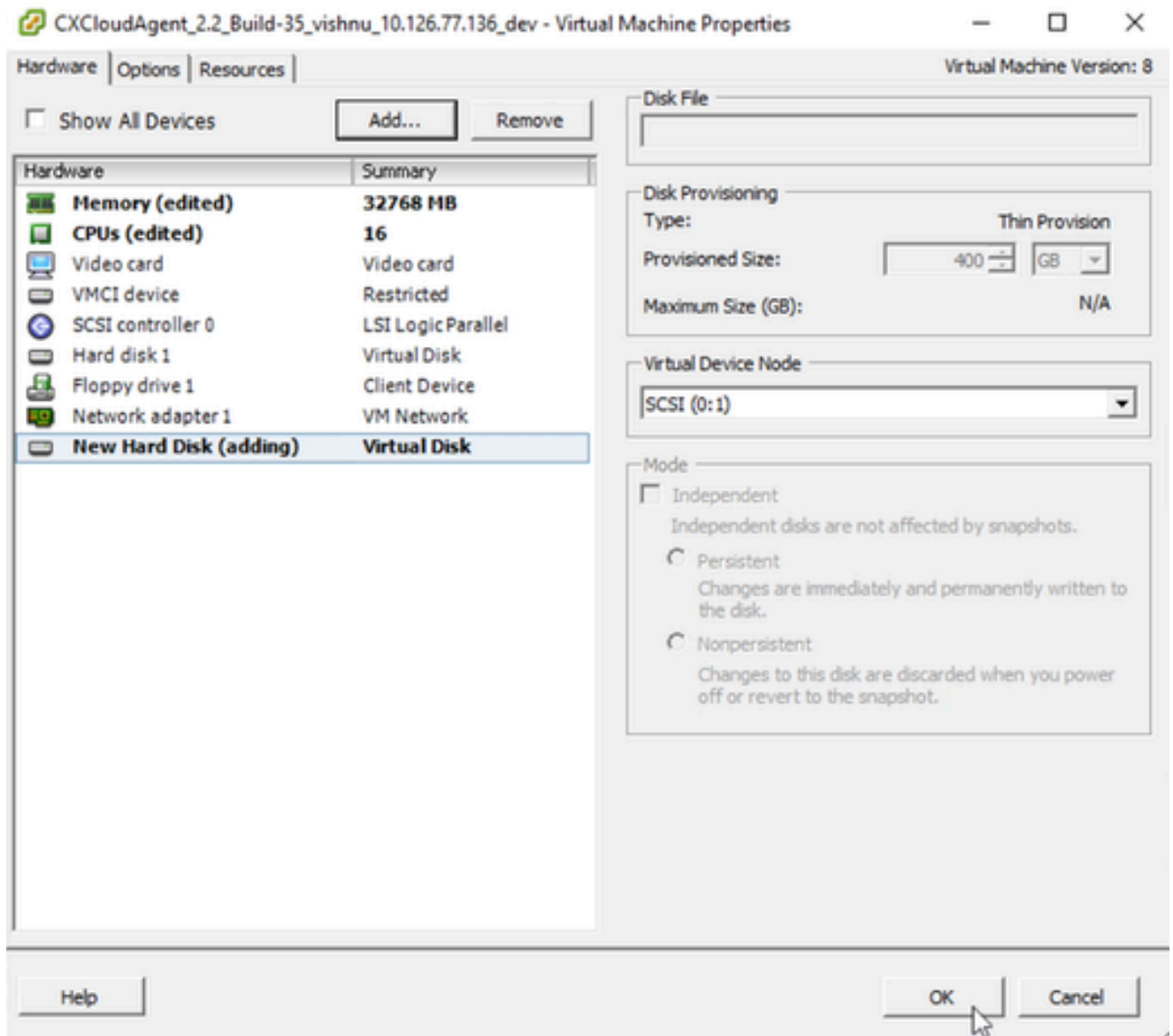
Opções avançadas

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-3
- CXCloudAgent_2.2_Build-3
- CXCloudAgent_2.2_Build-3
- CXCloudAgent_2.3_Build-7
- CXCloudAgent_2.3_Build-7
- CXCloudAgent_2.3_Build-7
- CXCloudAgent_2.3_Build-7
- CXCloudAgent_2.3_Build-7
- NAT-Router2.4.4_vishnu_1
- NAT-Router2.4.4_vishnu_1
- windows-test-192.168.77

CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev

Getting Started Summary Resource Allocation Performance Events Console Permissions

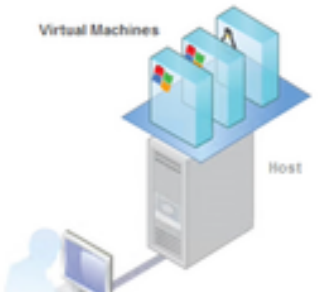
close tab

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.



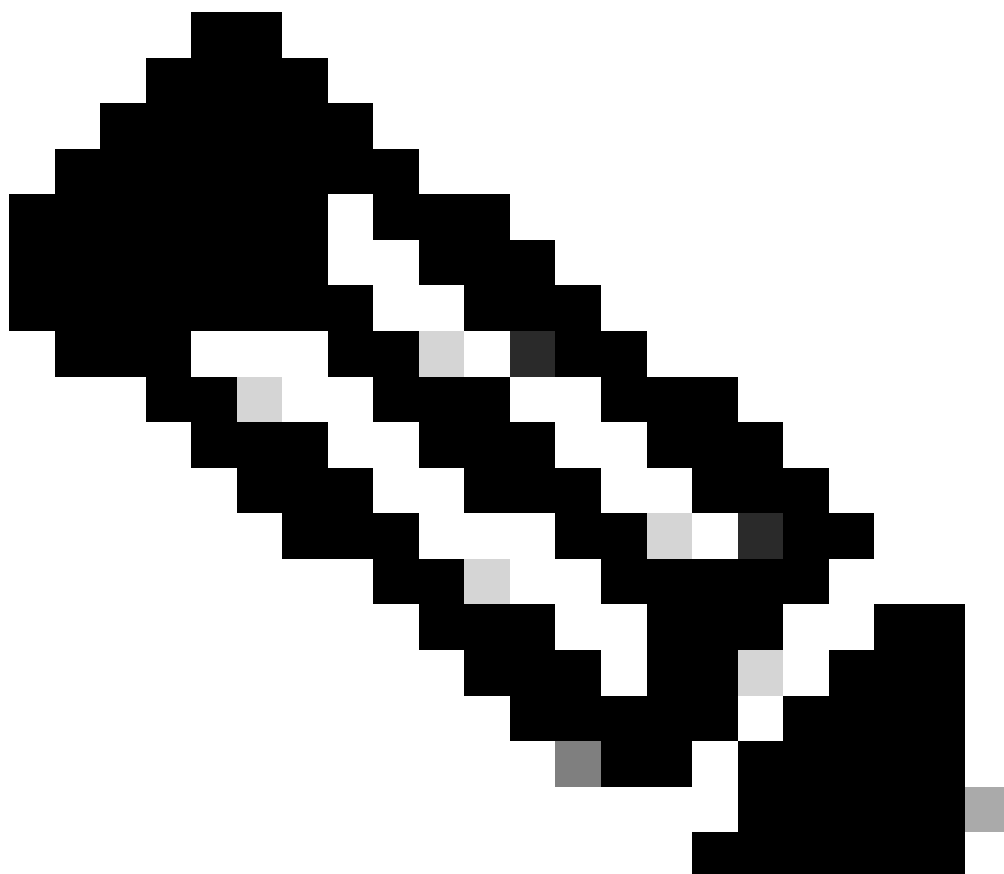
Recent Tasks

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



Observação: as alterações de configuração levam aproximadamente cinco minutos para serem concluídas.

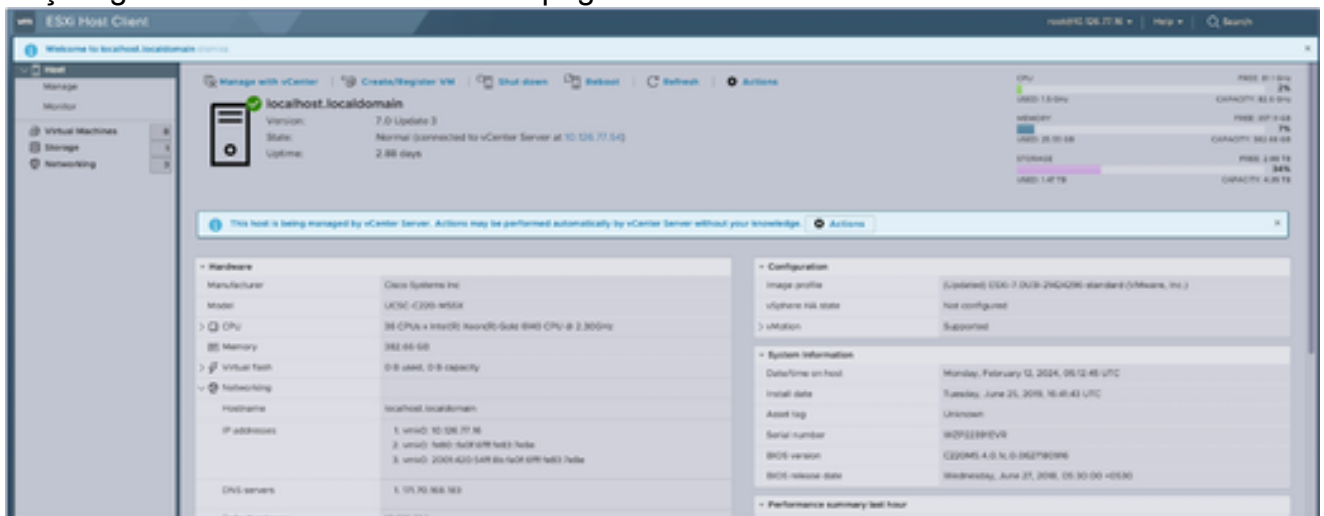
Reconfiguração usando o cliente da Web ESXi v6.0

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



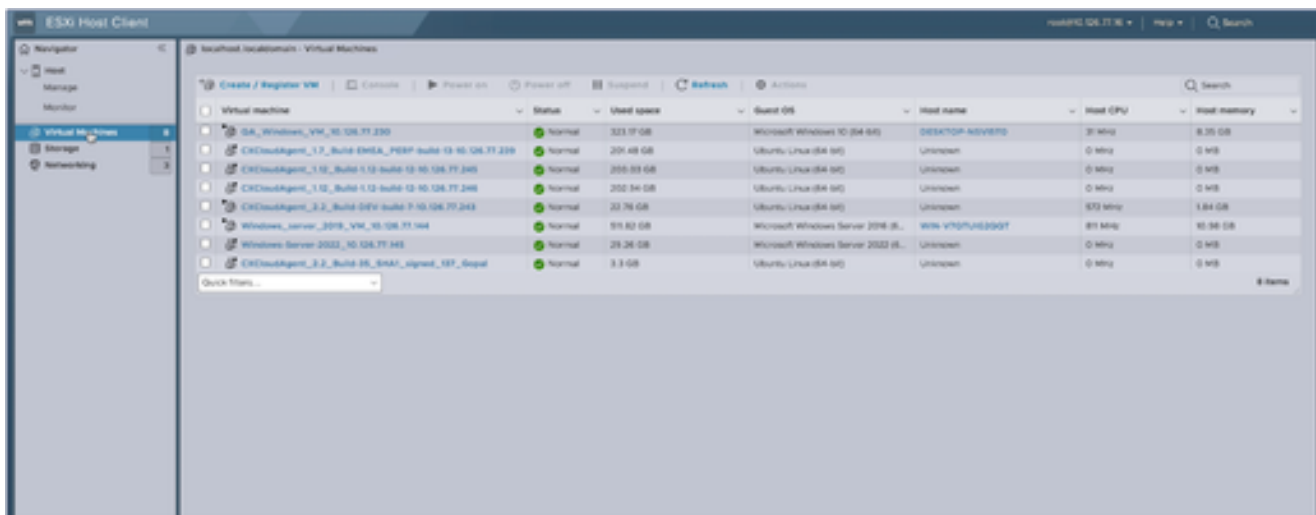
Cliente ESXi

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



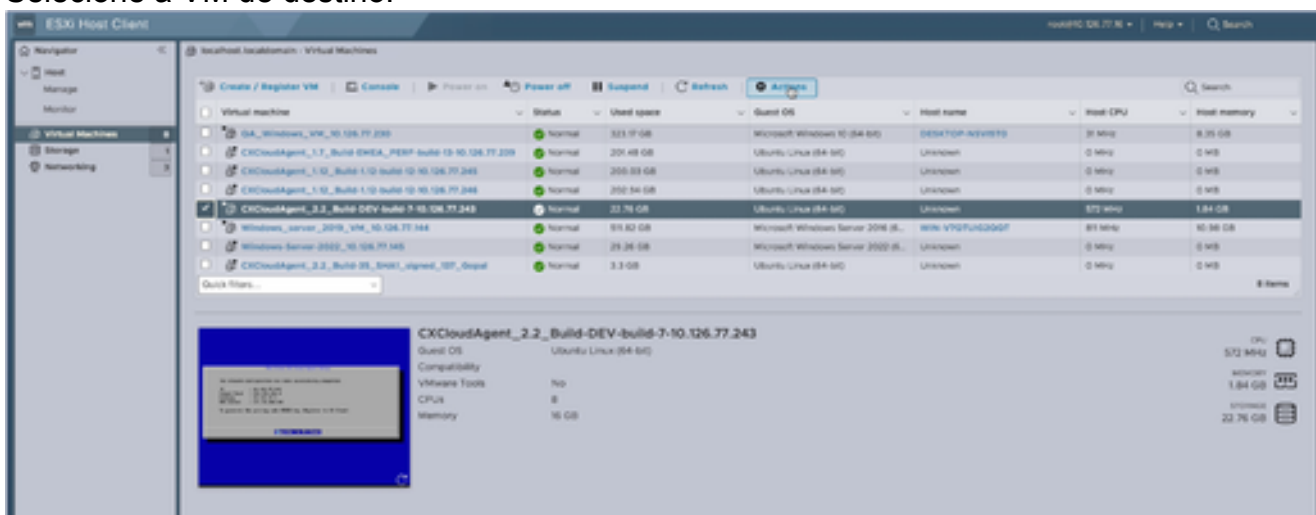
Página inicial do ESXi

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



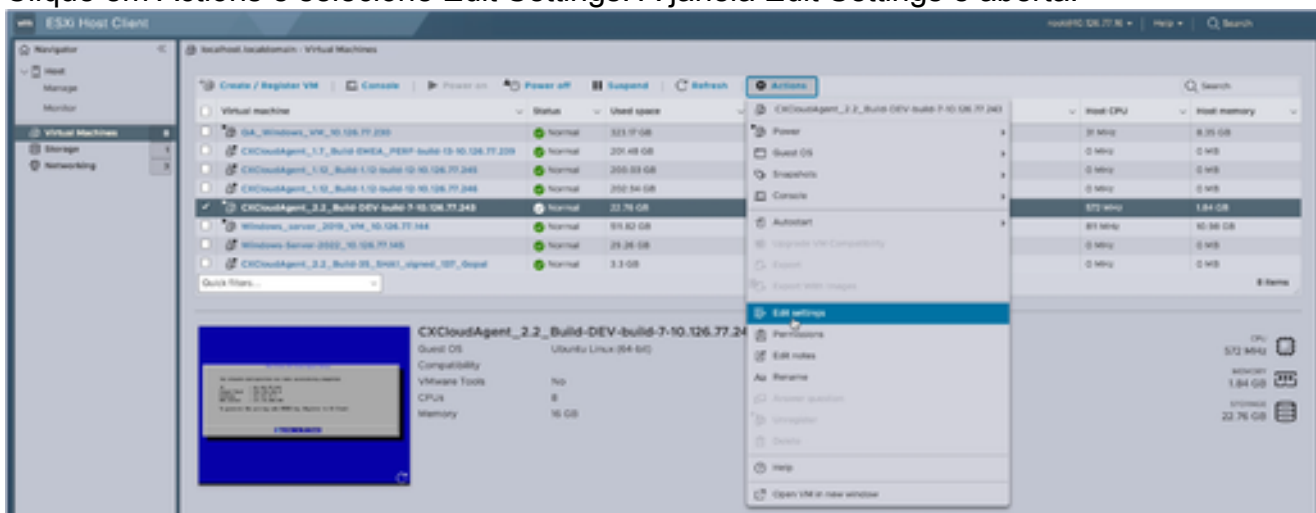
Lista de VMs

3. Selecione a VM de destino.

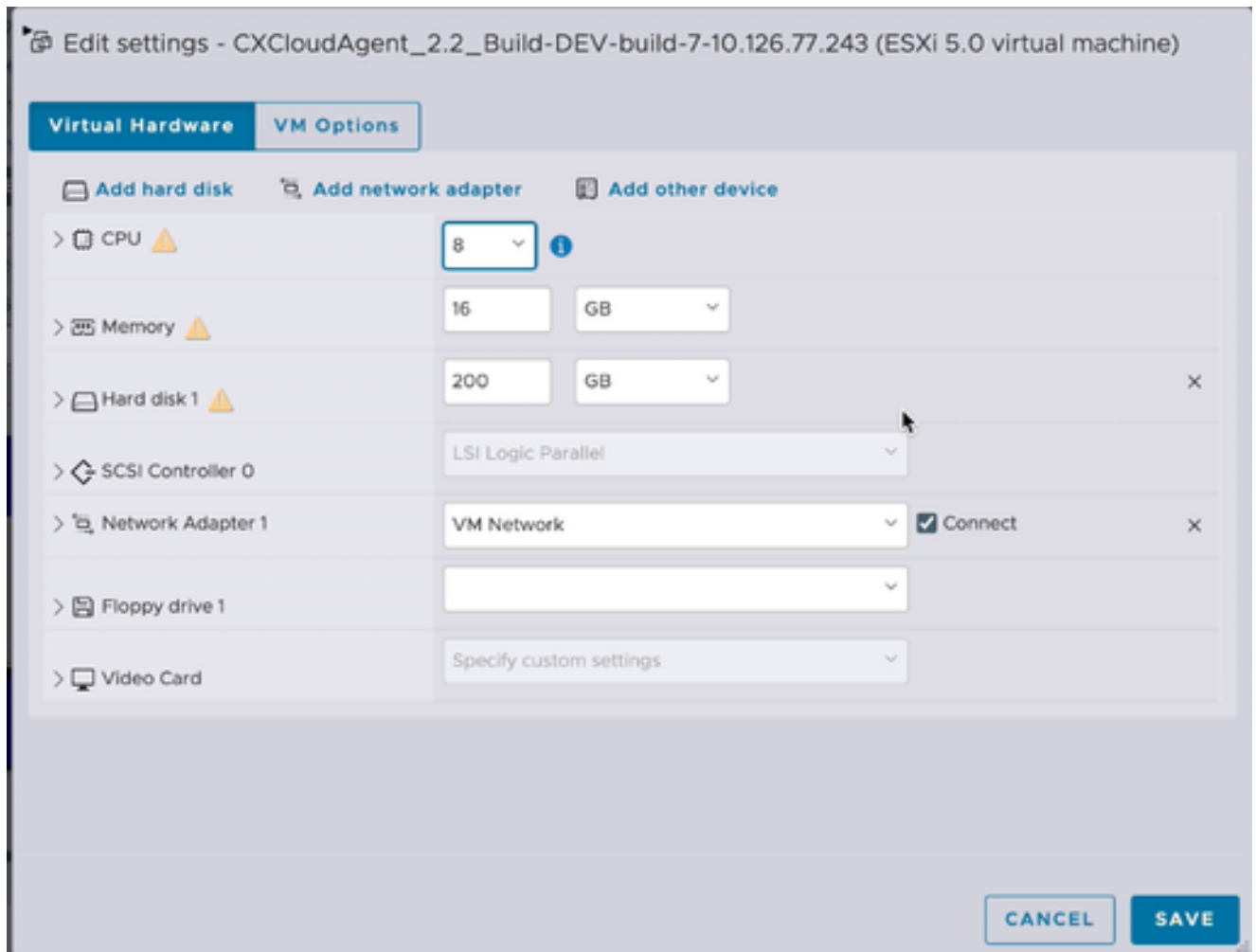


VM de destino

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

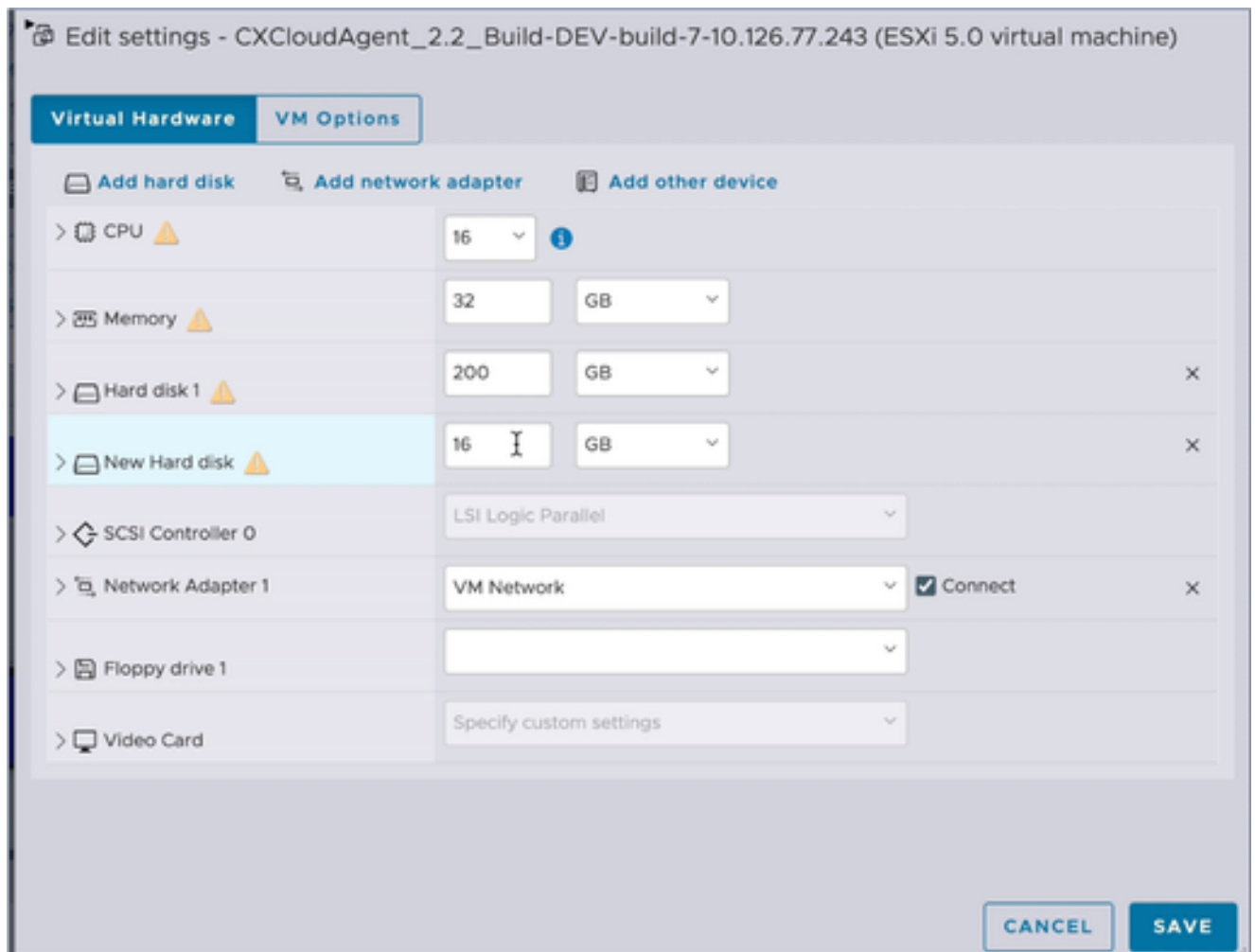


Ações



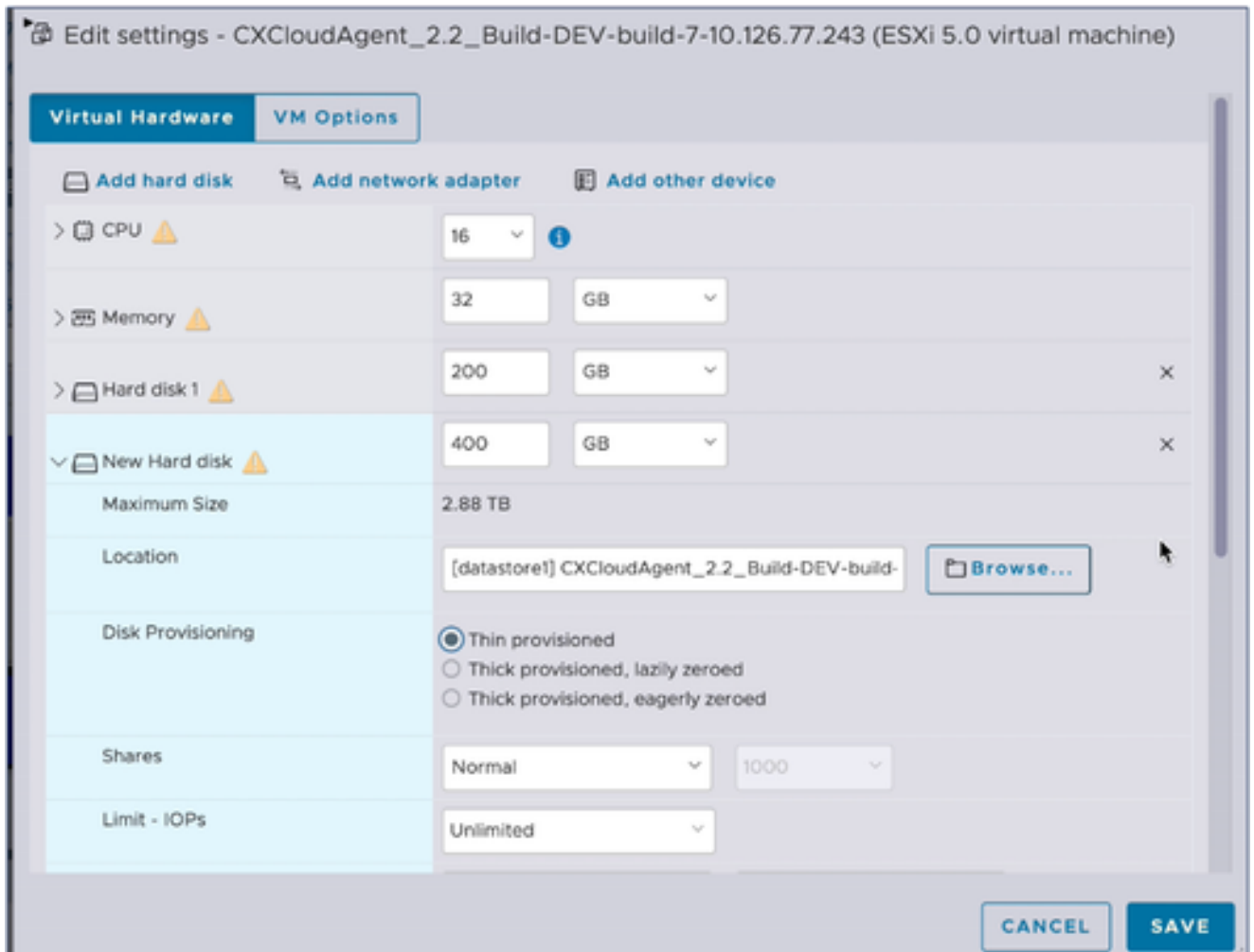
Editar configurações

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.



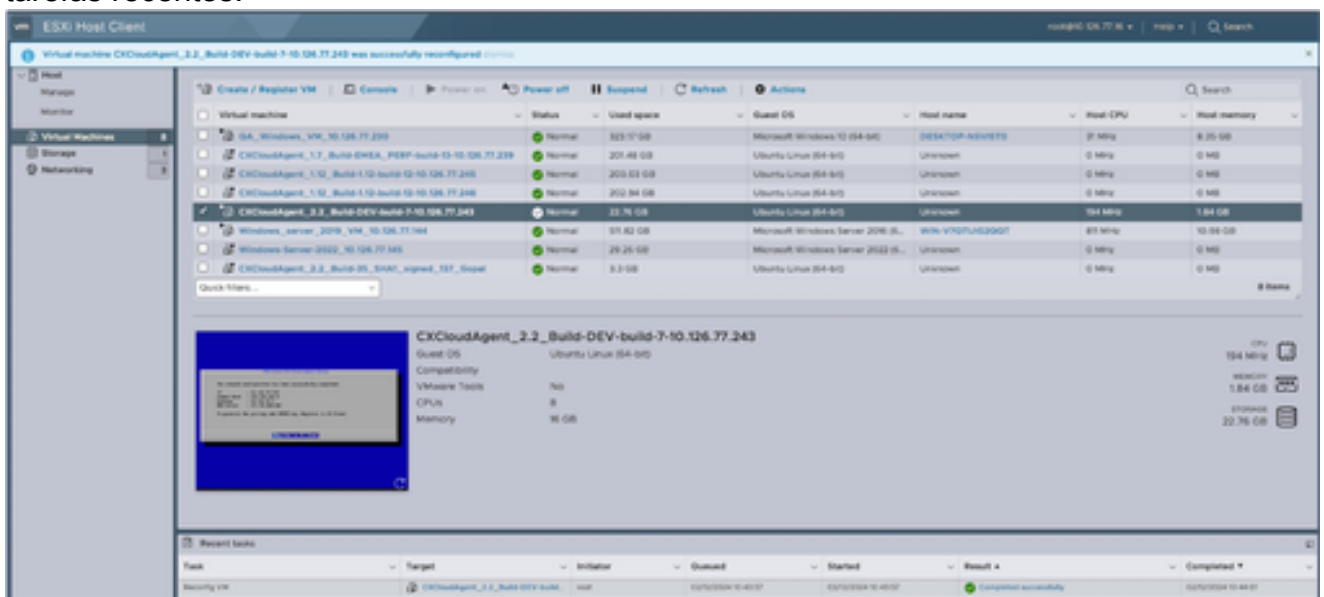
Editar configurações

- 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)
- Clique na seta para expandir Novo disco rígido. As propriedades são exibidas.



Editar configurações

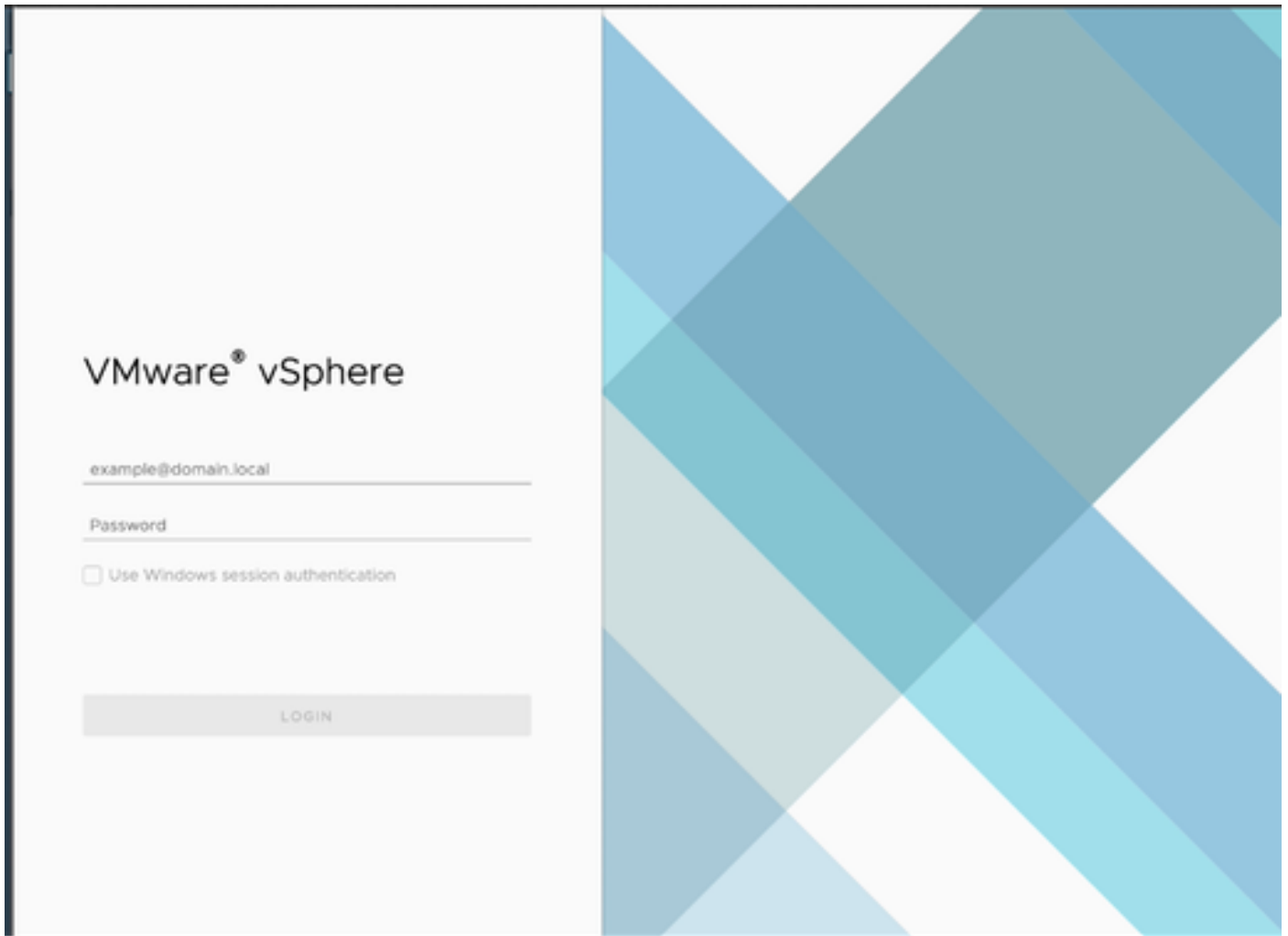
10. Selecione o botão de opção Thin provisioned.
11. Clique em Save para concluir a configuração. A atualização de configuração é exibida nas tarefas recentes.



Tarefas Recentes

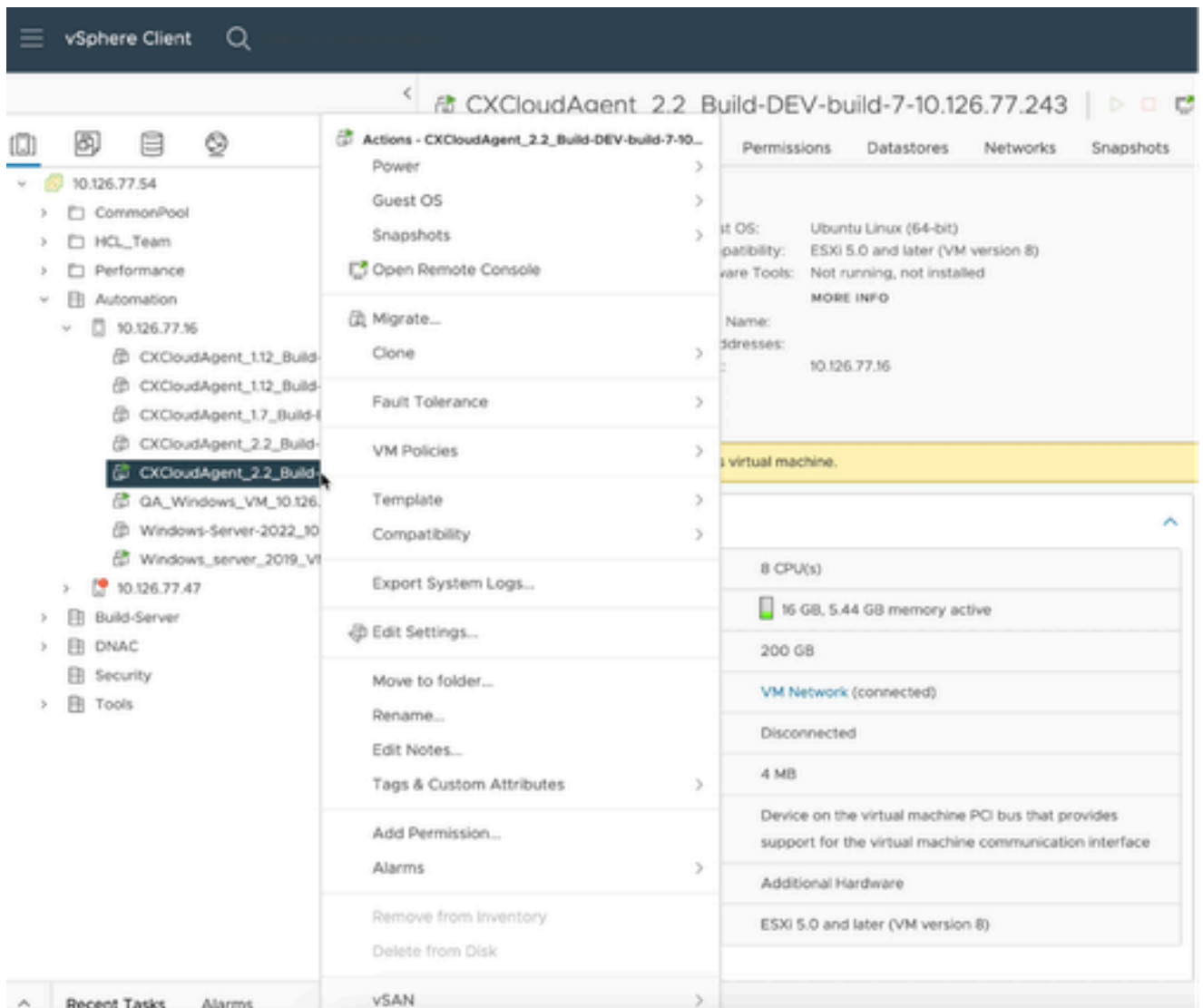
Reconfiguração usando o Web Client vCenter

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

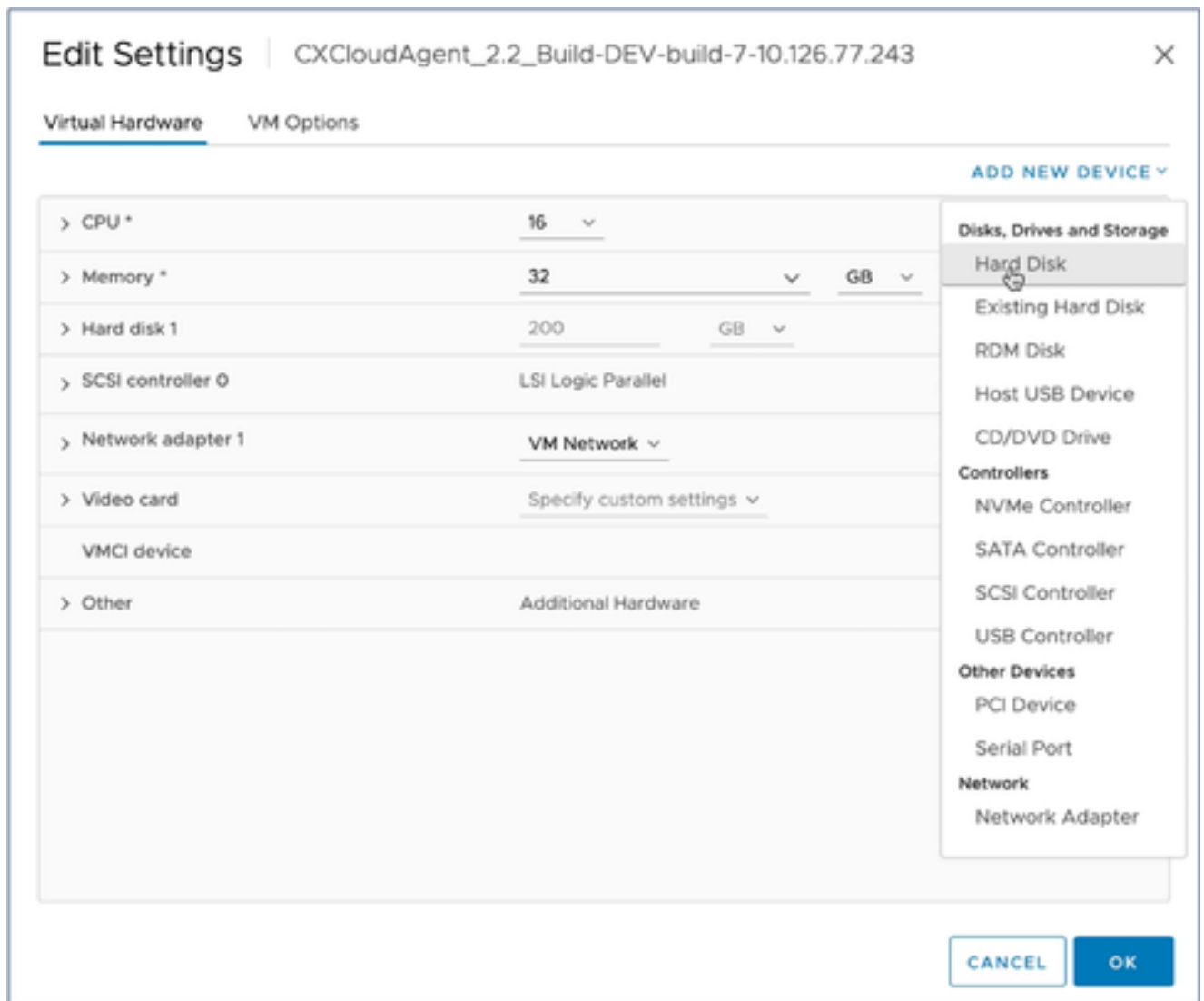
2. Clique com o botão direito do mouse na VM de destino e selecione Editar configurações no menu. A janela Edit Settings é aberta.

> 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

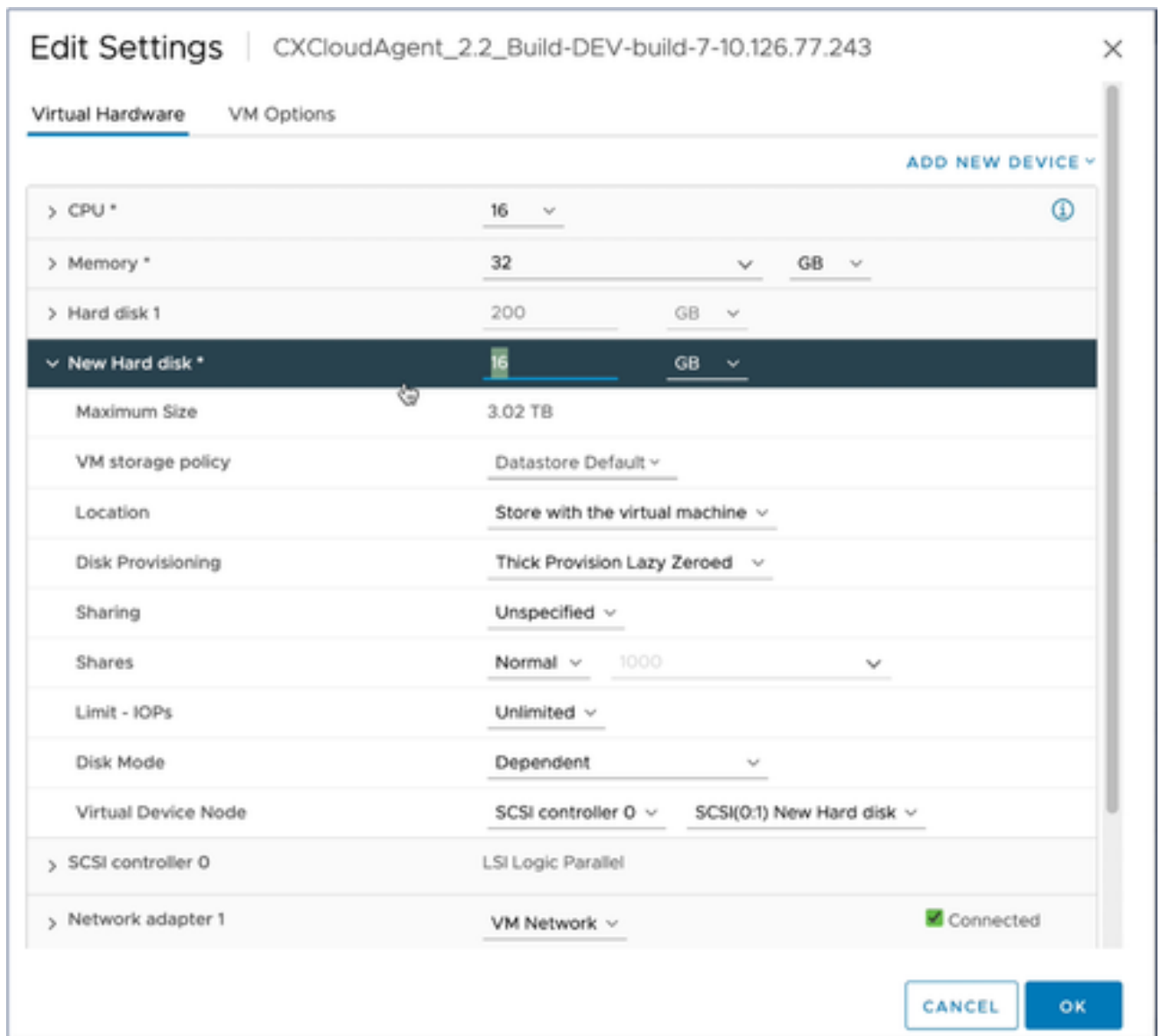
Editar configurações

3. Atualize os valores de 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.



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)

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

CANCEL

OK

Editar configurações

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

Implantação e configuração de rede

Selecione qualquer uma destas opções para implantar o CX Cloud Agent:

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

Implantação do OVA

Instalação do Thick Client ESXi 5.5/6.0

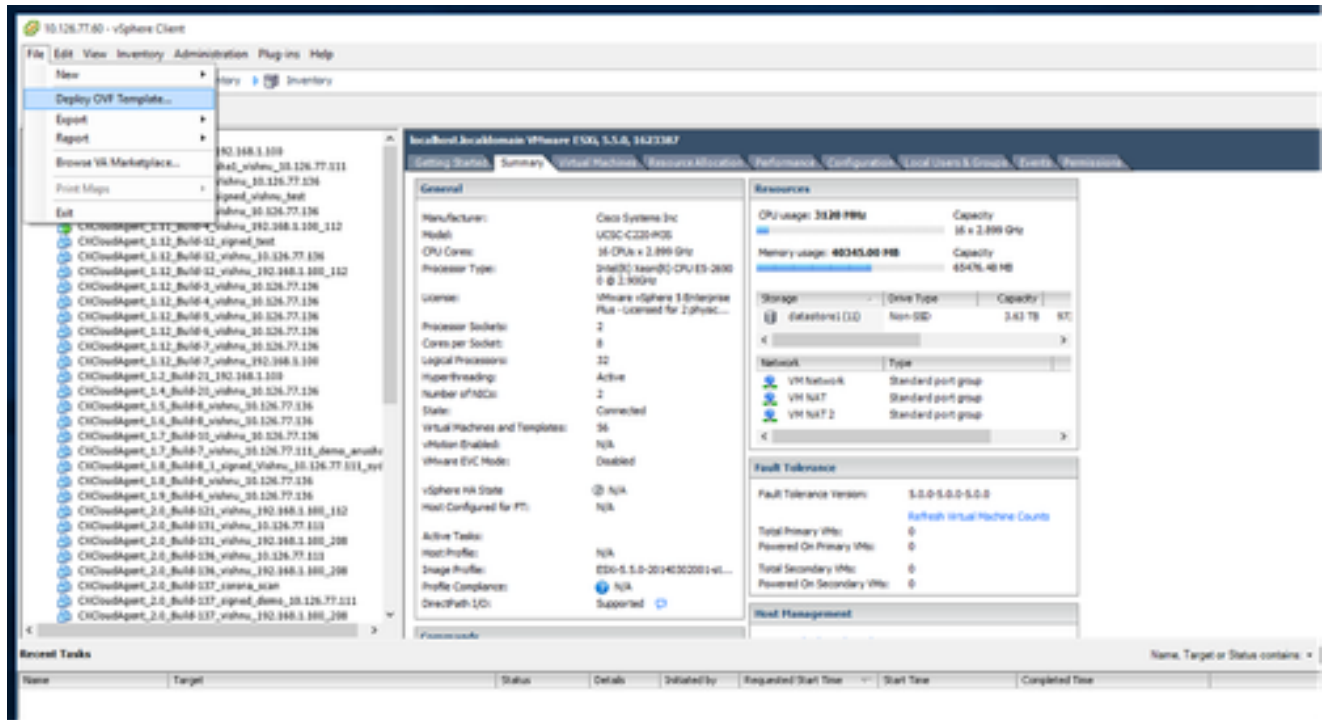
Esse cliente permite a implantação do CX Cloud Agent OVA com o uso do cliente thick vSphere.

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



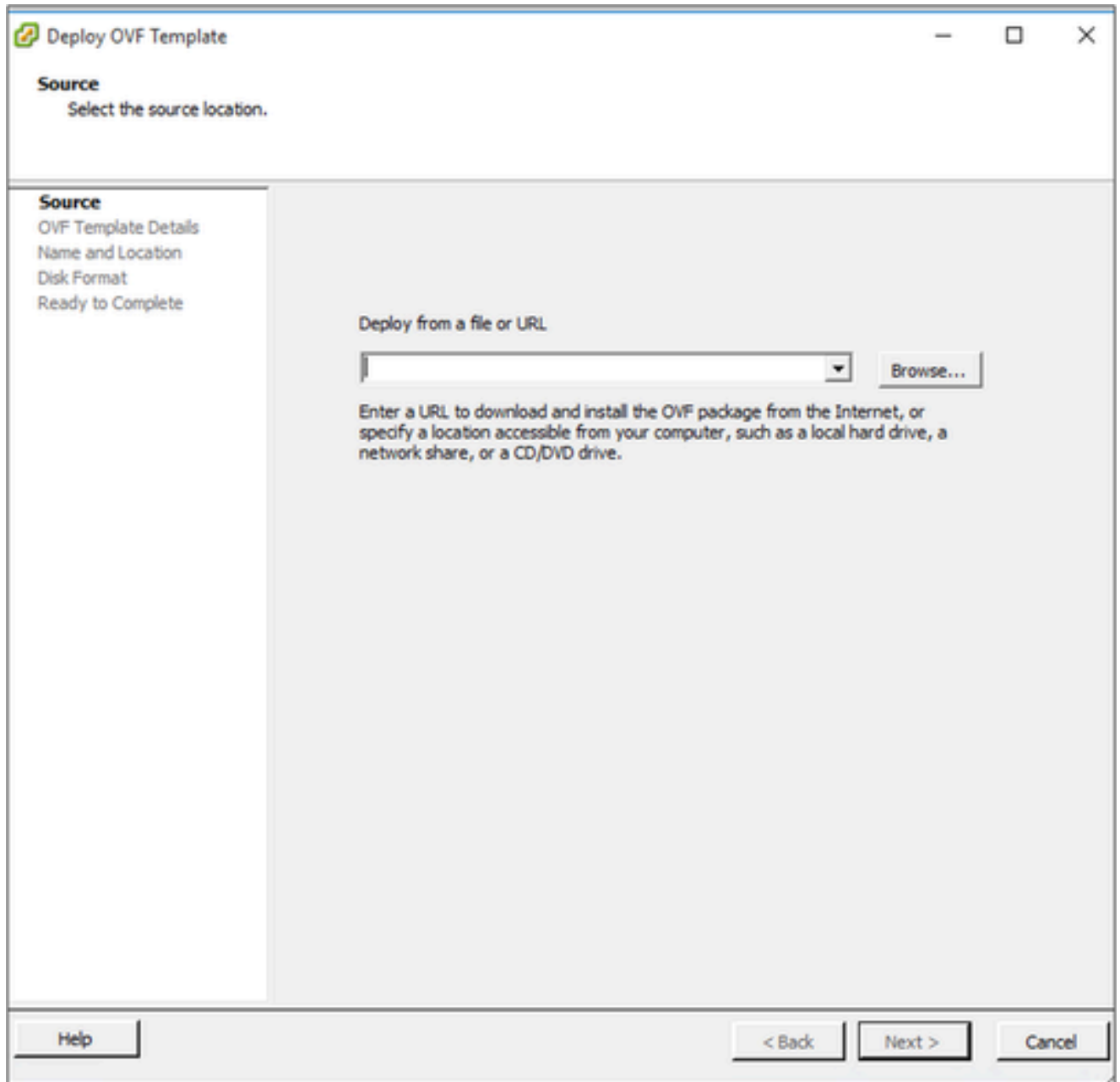
Login

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.

OVF Template Details

Verify OVF template details.

SOURCE

OVF Template Details

Name and Location
Disk Format
Network Mapping
Ready to Complete

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

Help < Back Next > Cancel

Detalhes do modelo

5. Insira um nome exclusivo e clique em Avançar.

Name and Location

Specify a name and location for the deployed template

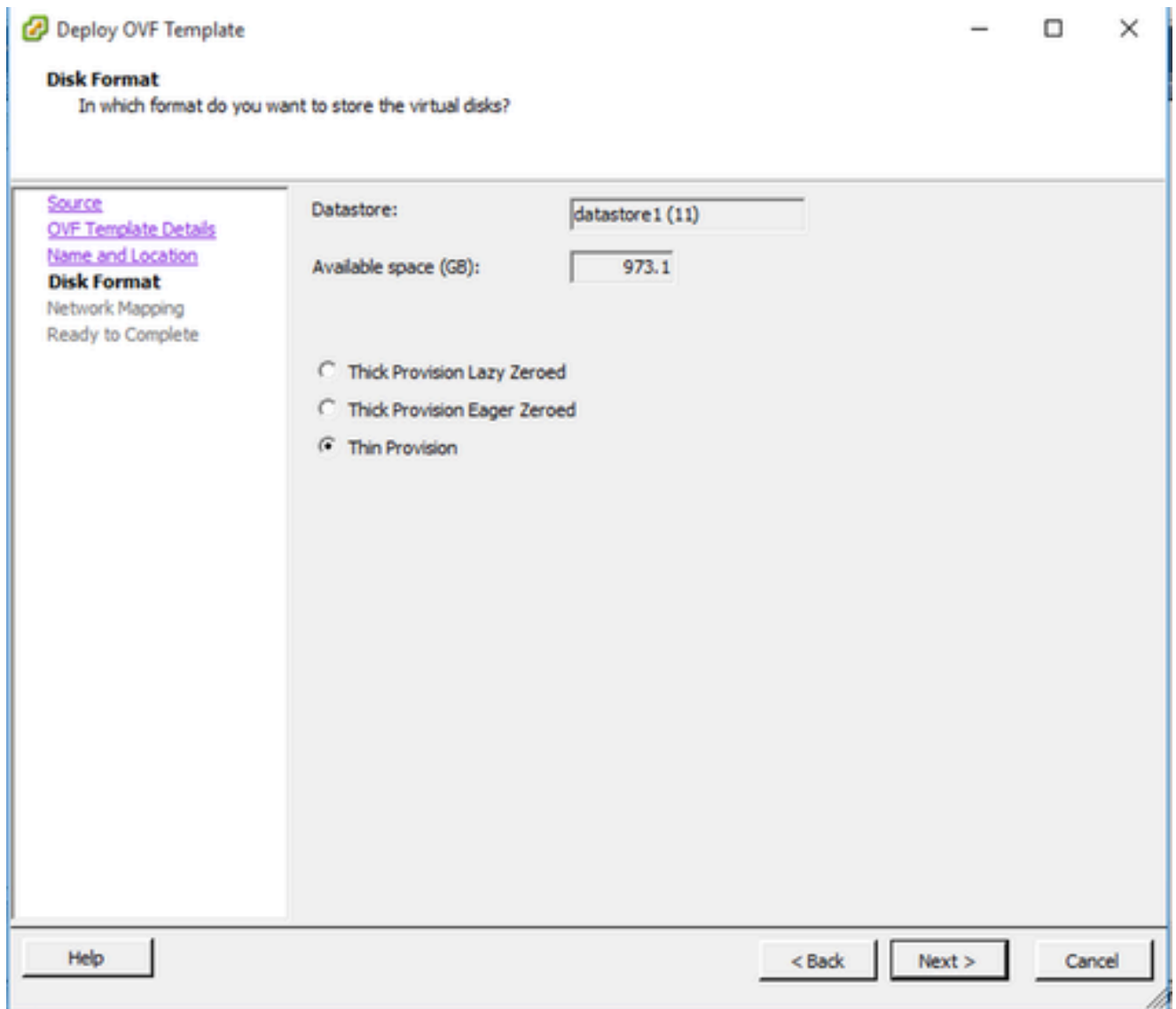
[Source](#)
[OVF Template Details](#)
Name and Location
Disk Format
Network Mapping
Ready to Complete

Name:

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

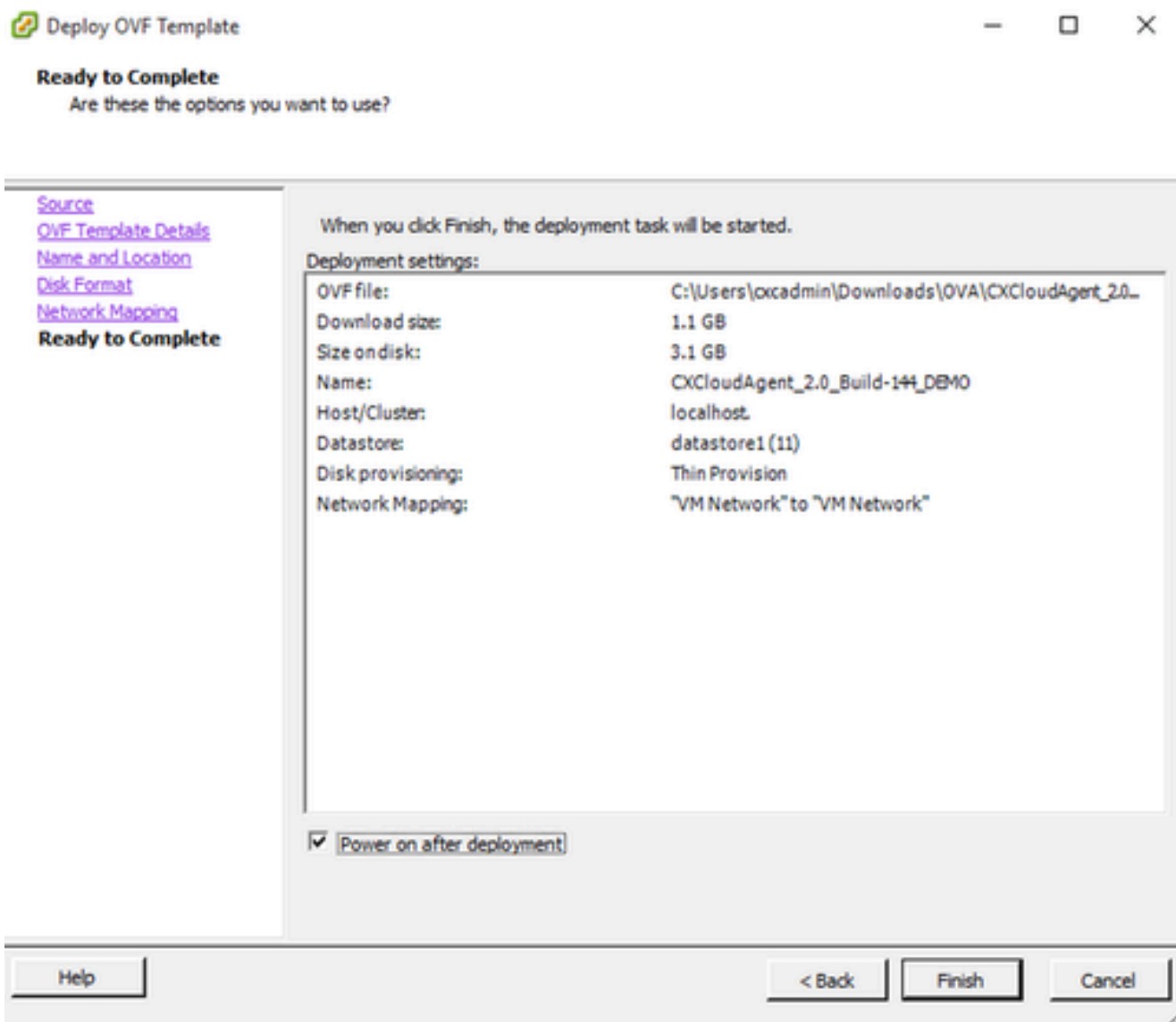
Nome e local

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



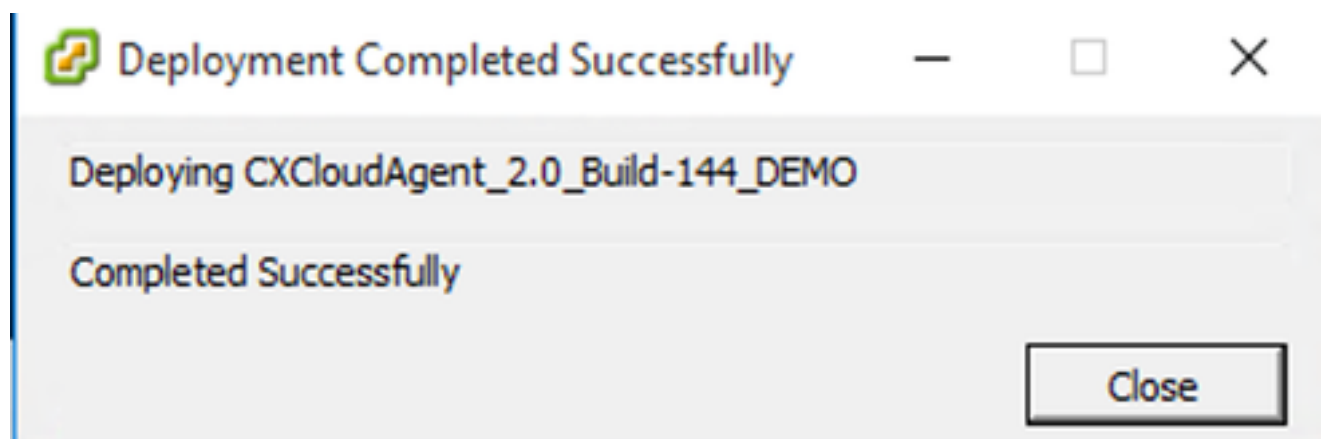
Formato de disco

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

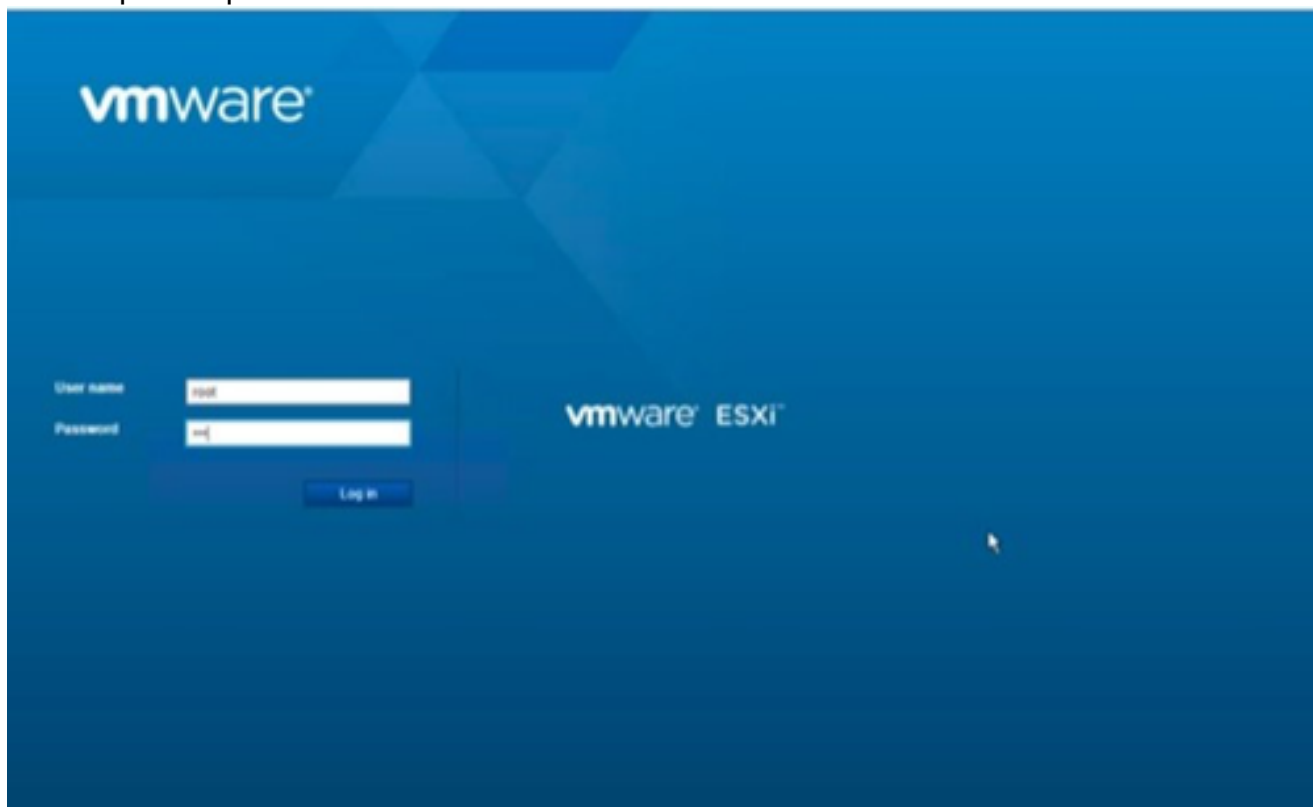
8. Selecione a VM implantada, abra o console e vá para [Network Configuration](#) para continuar

com as próximas etapas.

Instalação do Web Client ESXi 6.0

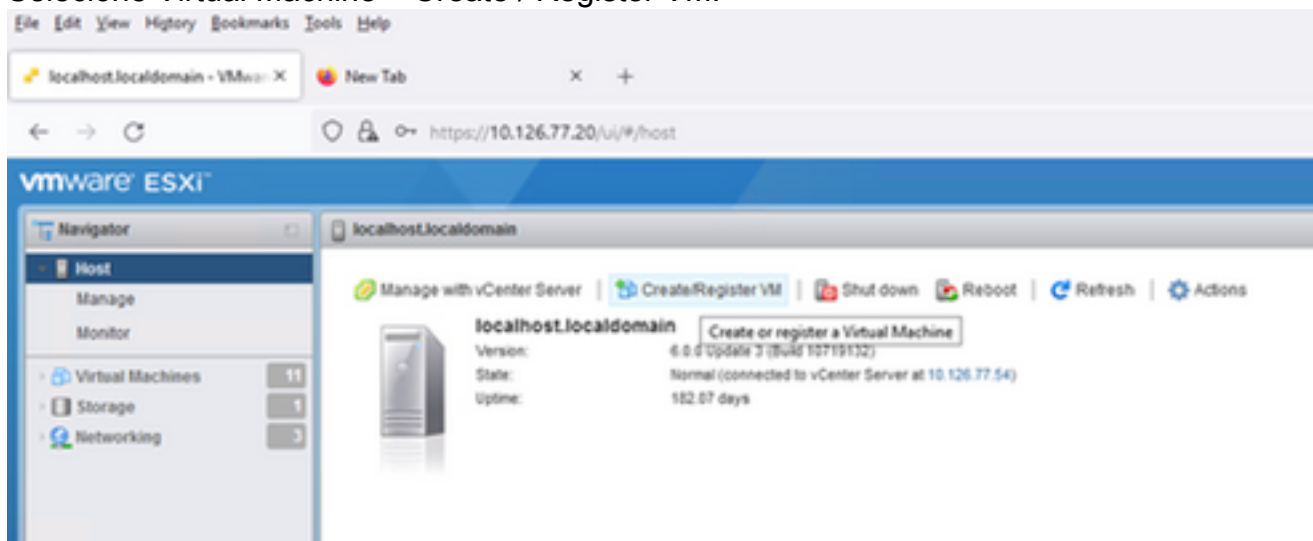
Esse cliente implanta o CX Cloud Agent OVA usando a Web do vSphere.

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



Login no VMware ESXi

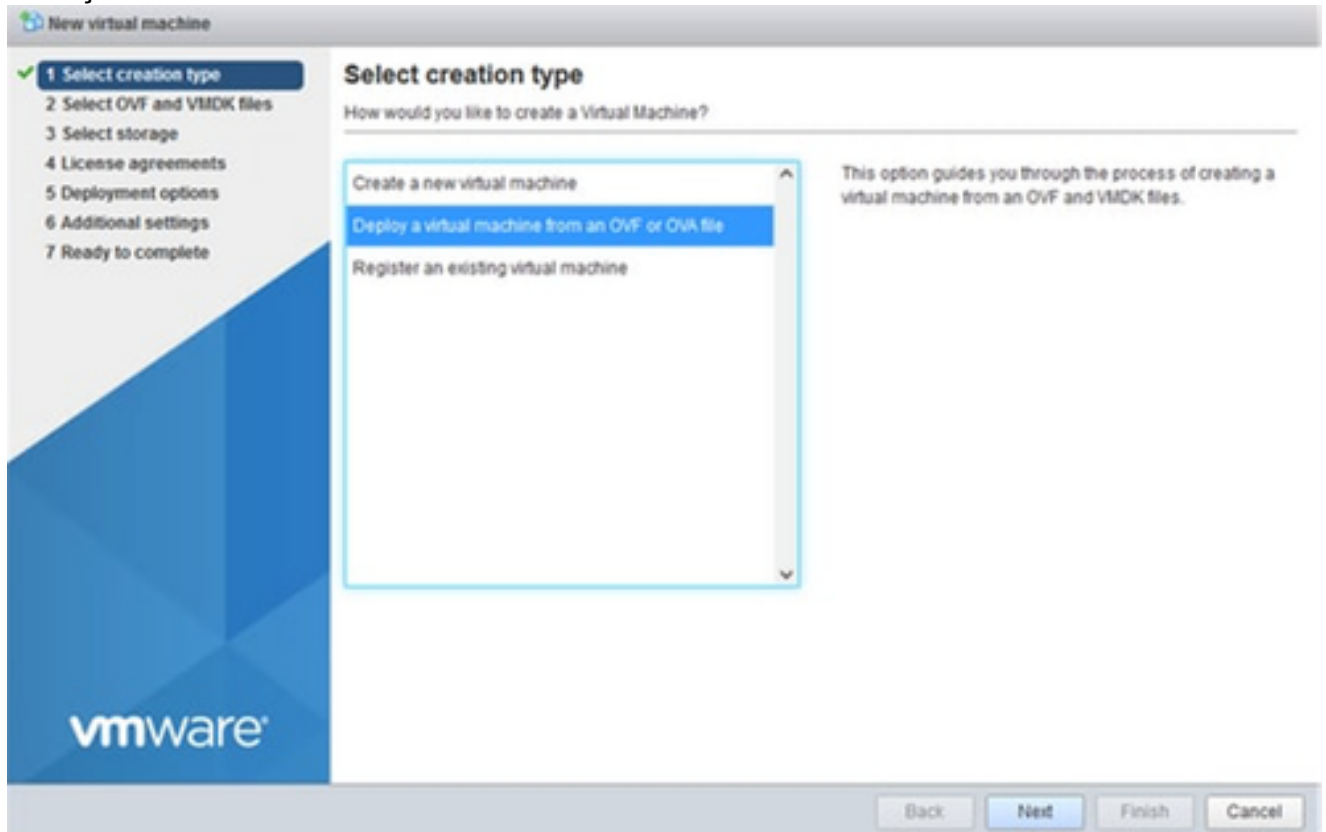
2. Selecione Virtual Machine > Create / Register VM.



Criar VM

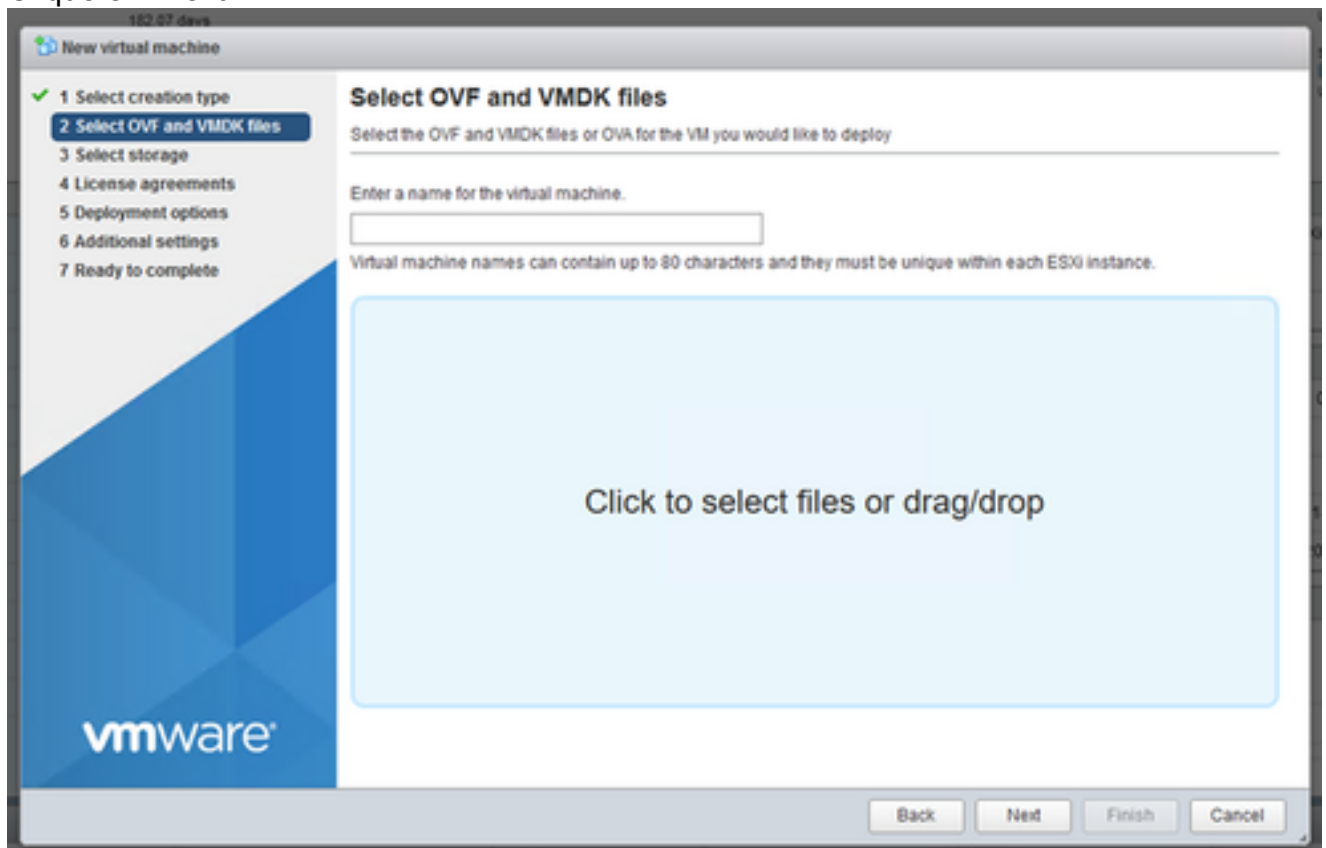
3. Selecione Implantar uma máquina virtual em um arquivo de OVF ou de OVA e clique em

Avançar.



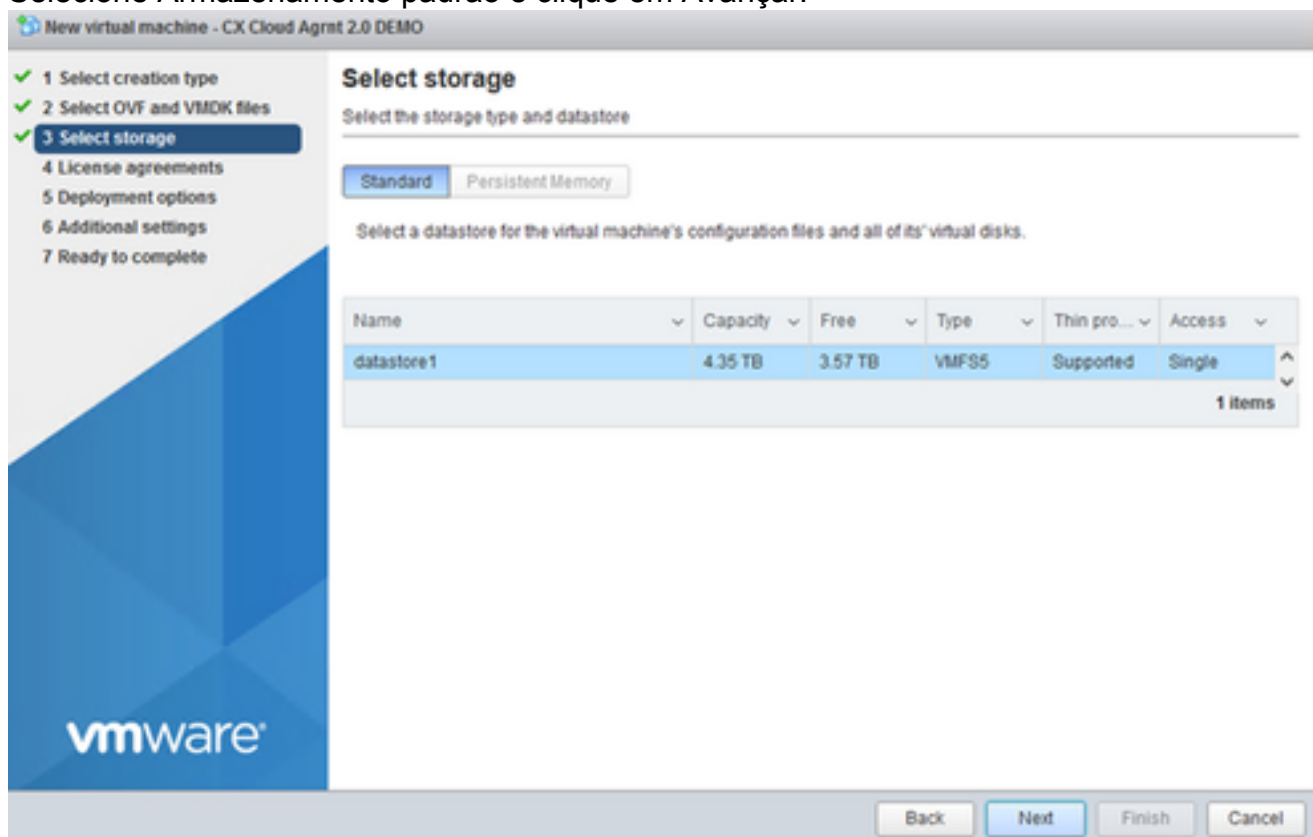
Selecionar Tipo de Criação

4. Insira o nome da VM, procure para selecionar o arquivo ou arraste e solte o arquivo OVA baixado.
5. Clique em Next.



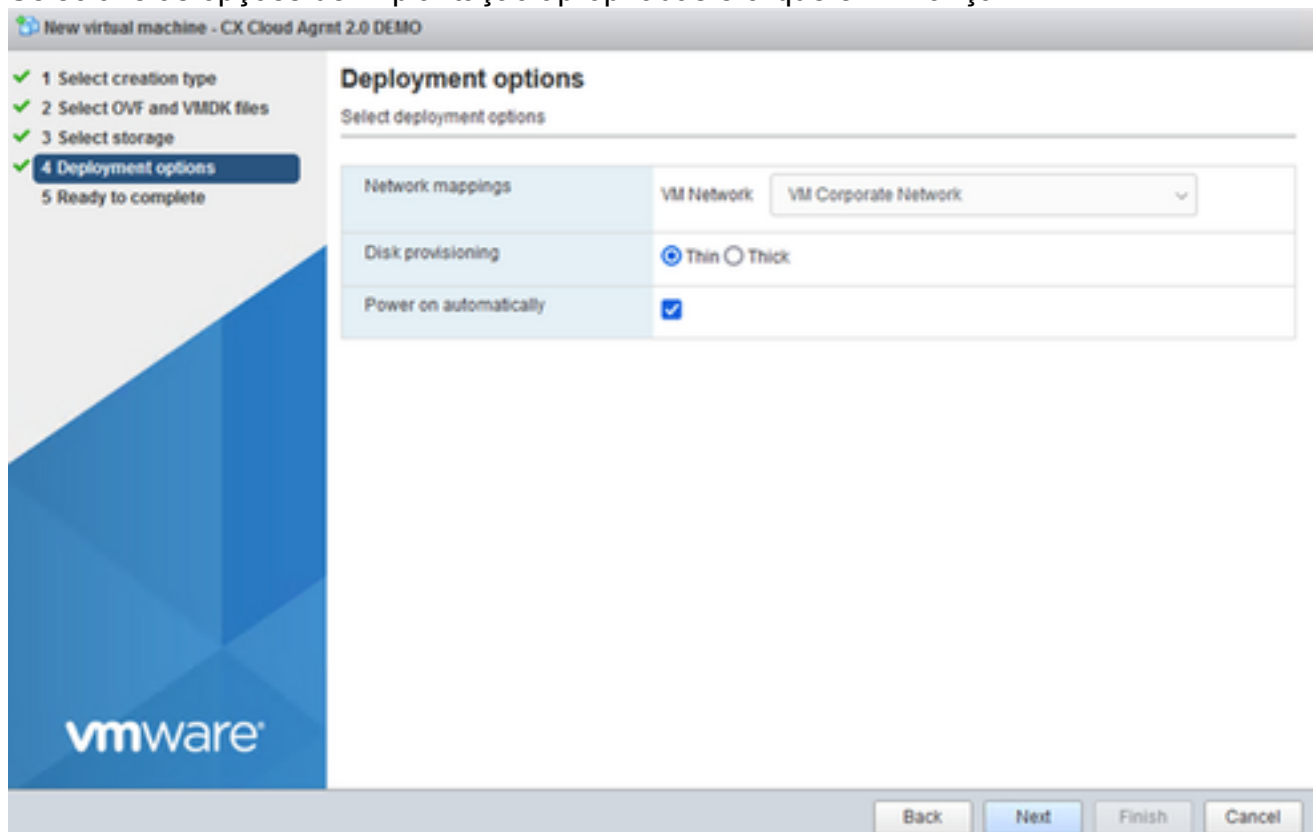
Seleção do OVA

6. Selecione Armazenamento padrão e clique em Avançar.



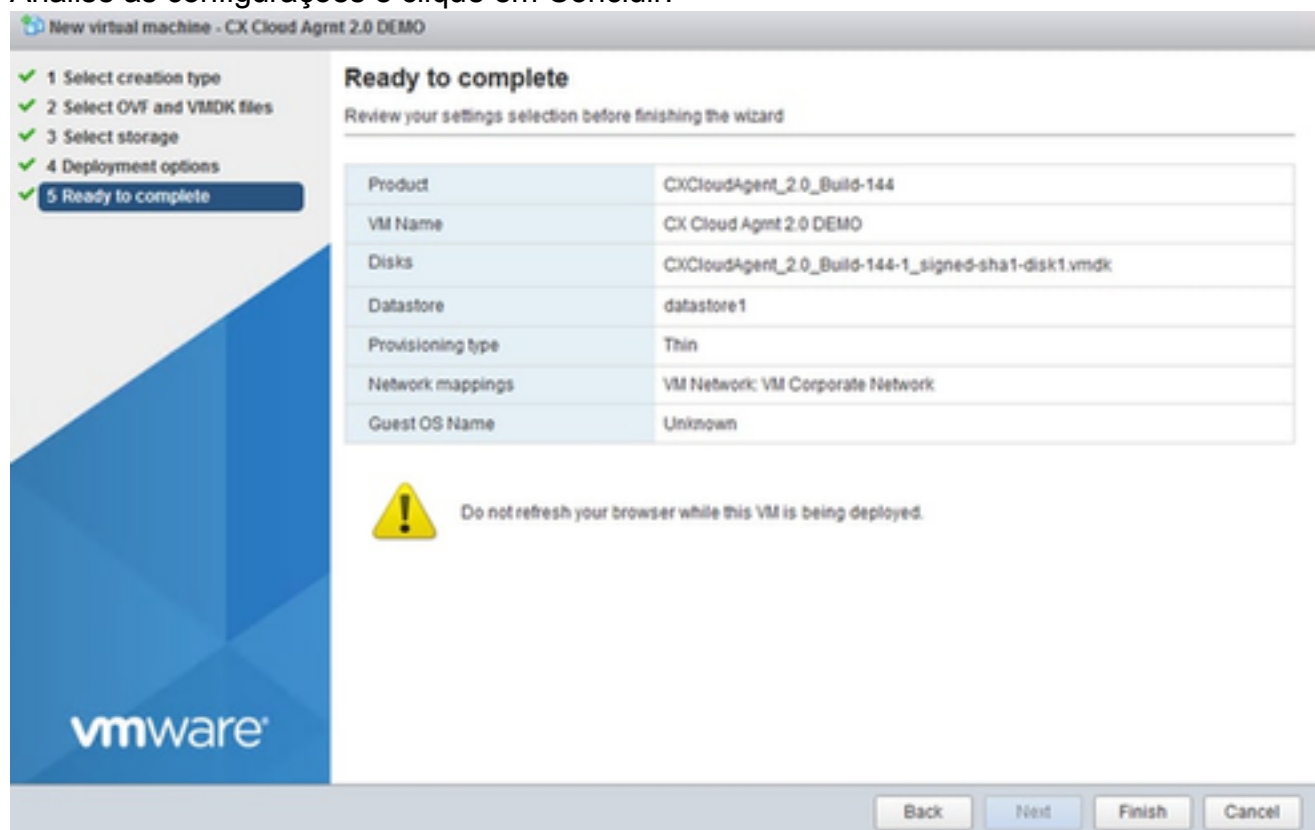
Selecionar armazenamento

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

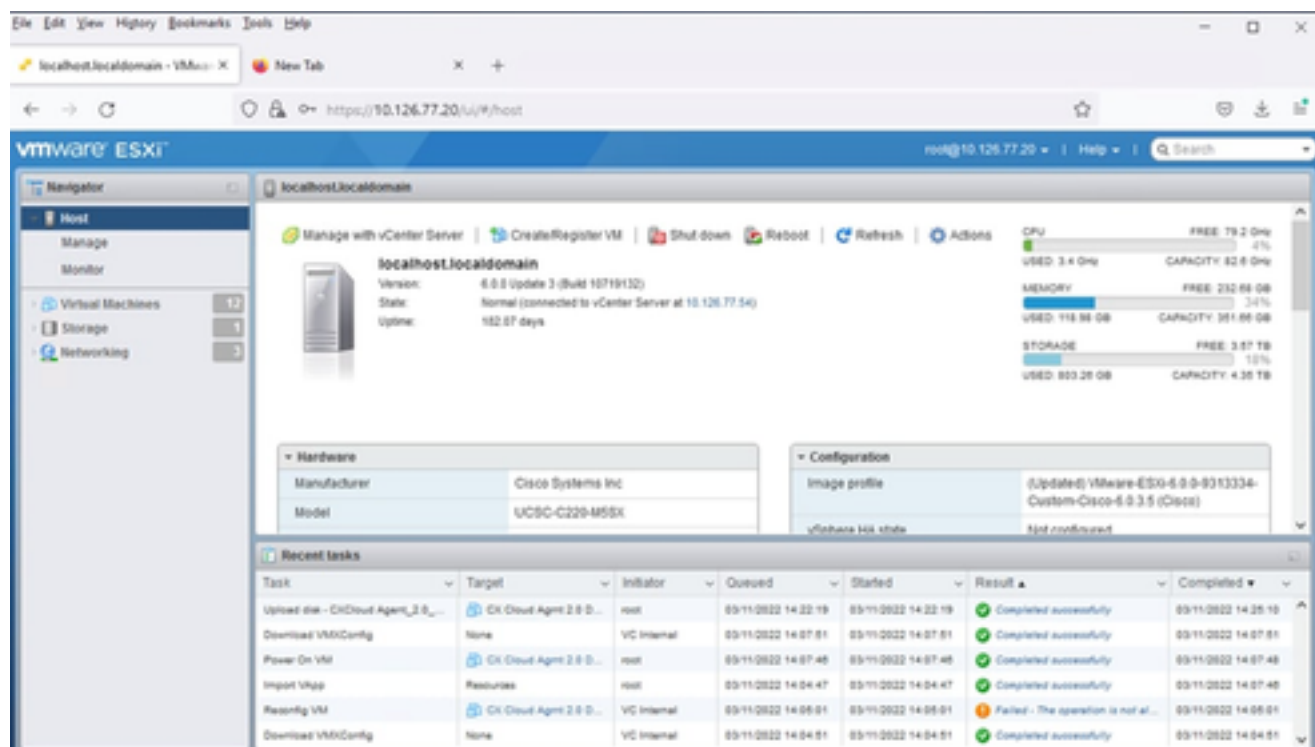


Opções de implantação

8. Analise as configurações e clique em Concluir.

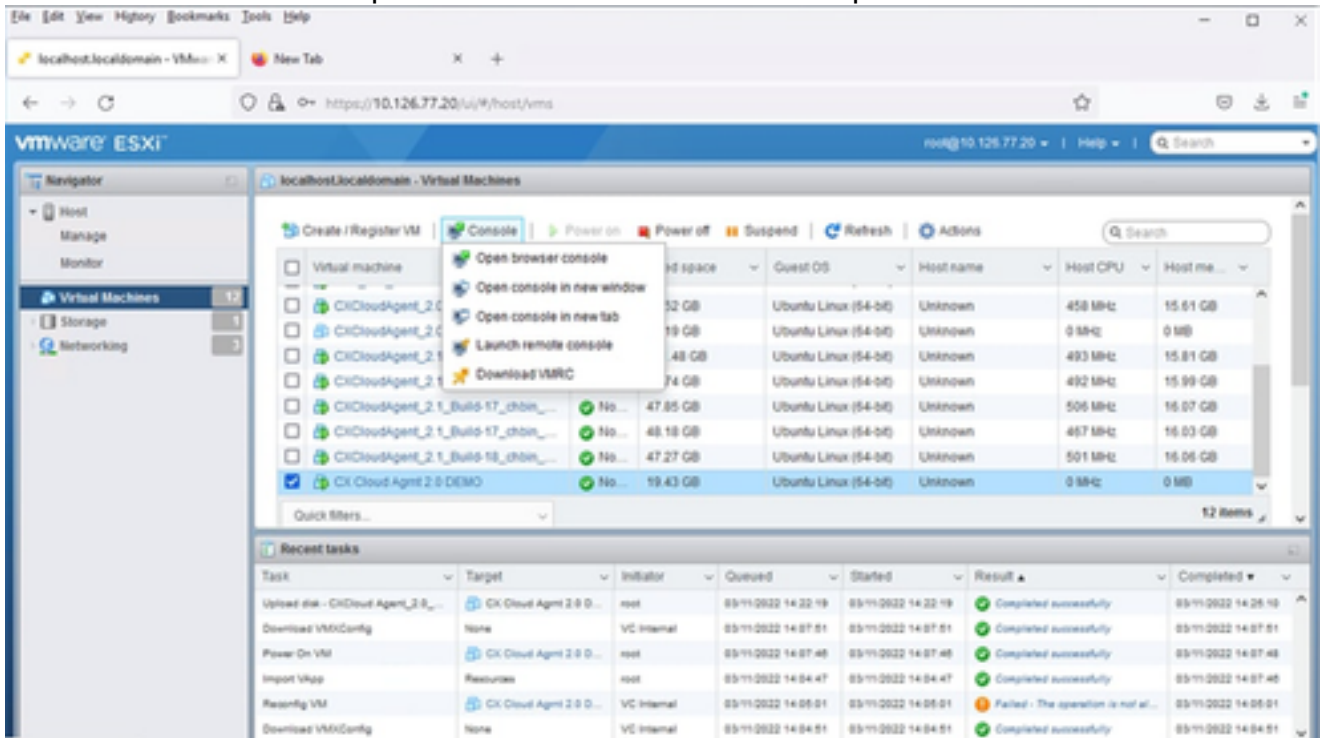


Pronto para concluir



Conclusão realizada com sucesso

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



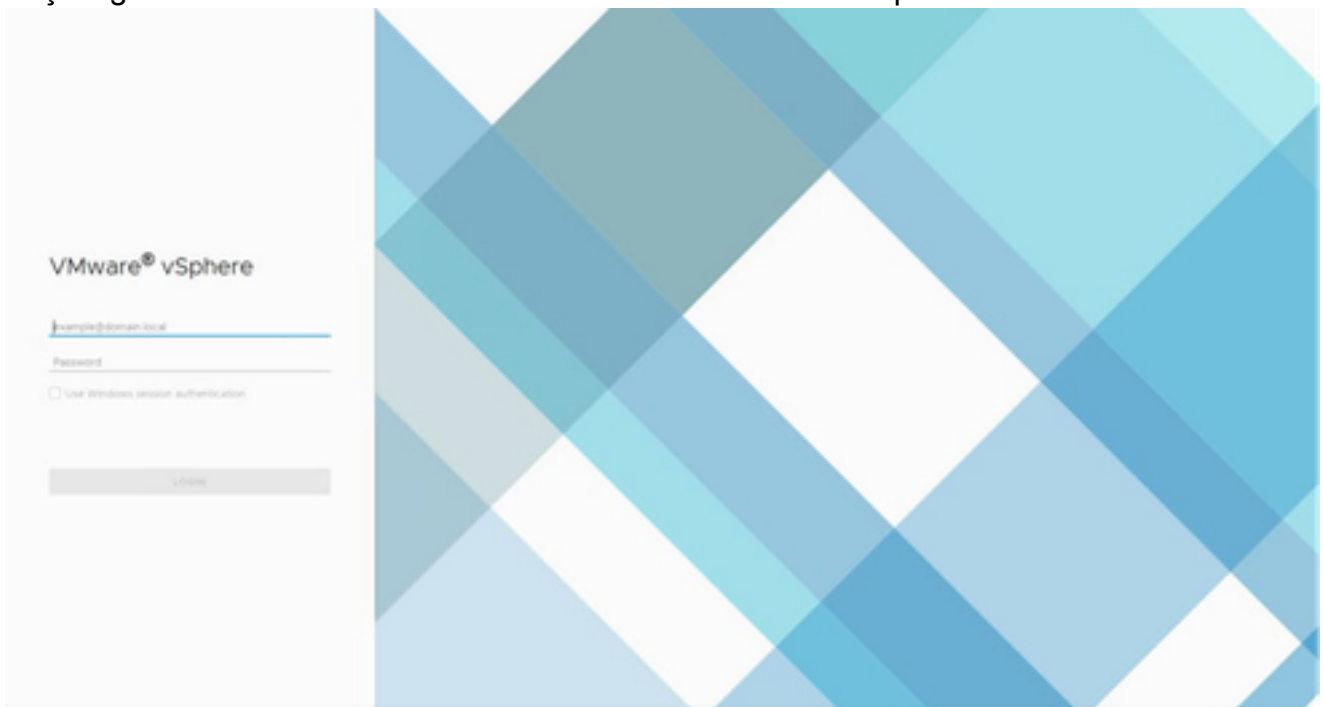
Console

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

Instalação do Web Client vCenter

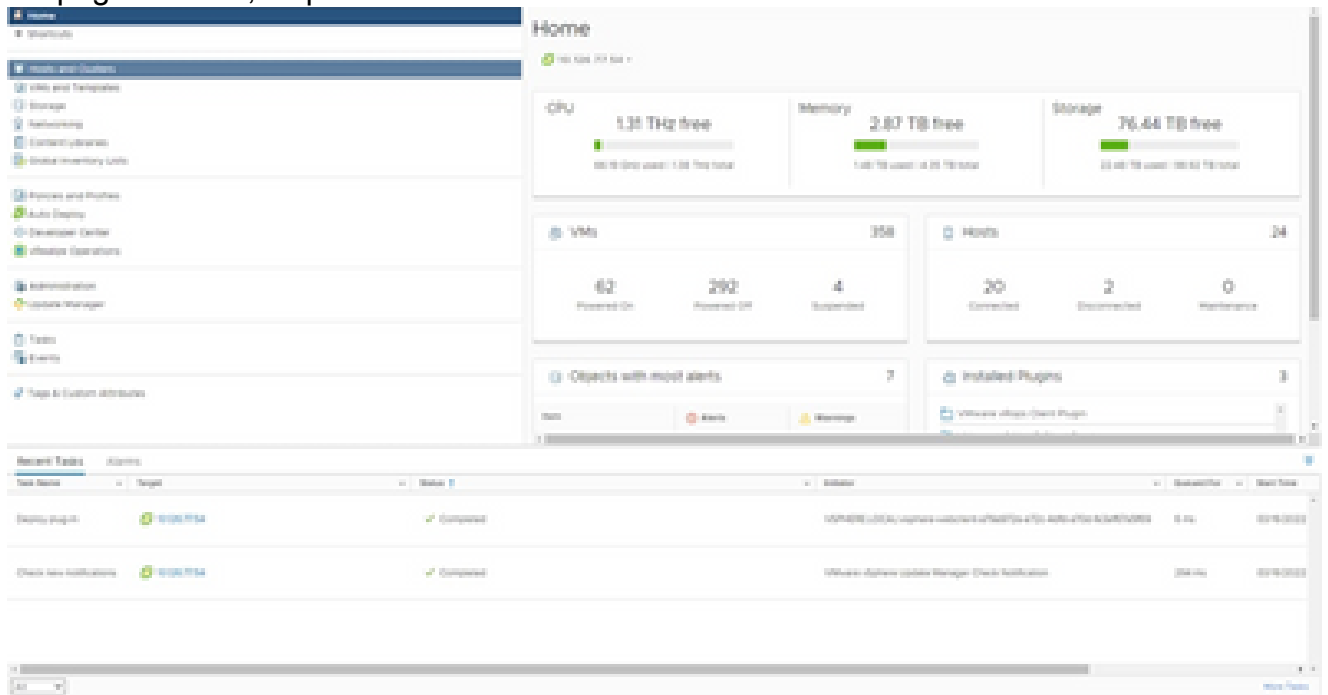
Execute estas etapas:

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



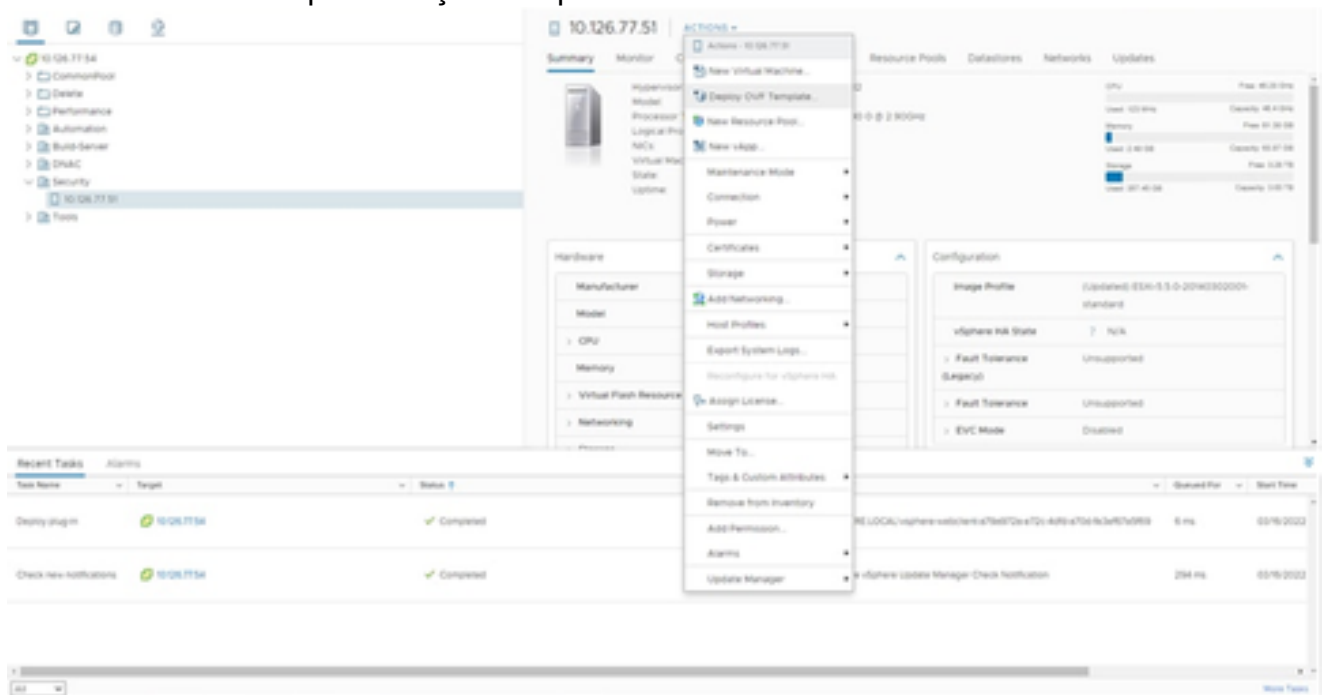
Login

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



Página inicial

3. Selecione a VM e clique em Ação > Implantar modelo de OVF.



Ações

Deploy OVF Template

- Select an OVF template**
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- 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

Local file

No file chosen

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

Selecionar modelo

- Adicione o URL diretamente ou navegue para selecionar o arquivo OVA e clique em Avançar.
- 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 name and folder

Specify a unique name and target location

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

Select a location for the virtual machine.

10.126.77.54

- > CommonPool
- > Delete
- > Performance
- > Automation
- > Build-Server
- > DNAC
- > Security
- > Tools

CANCEL

BACK

NEXT

Nome e Pasta


7. Selecione um recurso de computação e clique em Avançar.


Deploy OVF Template

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

Select a compute resource

Select the destination compute resource for this operation

▼  Security

>  10.126.77.51

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

Selecionar Recurso do Computador

8. Analise os detalhes e clique em Avançar.

Deploy OVF Template

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

Review details

Verify the template details.

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

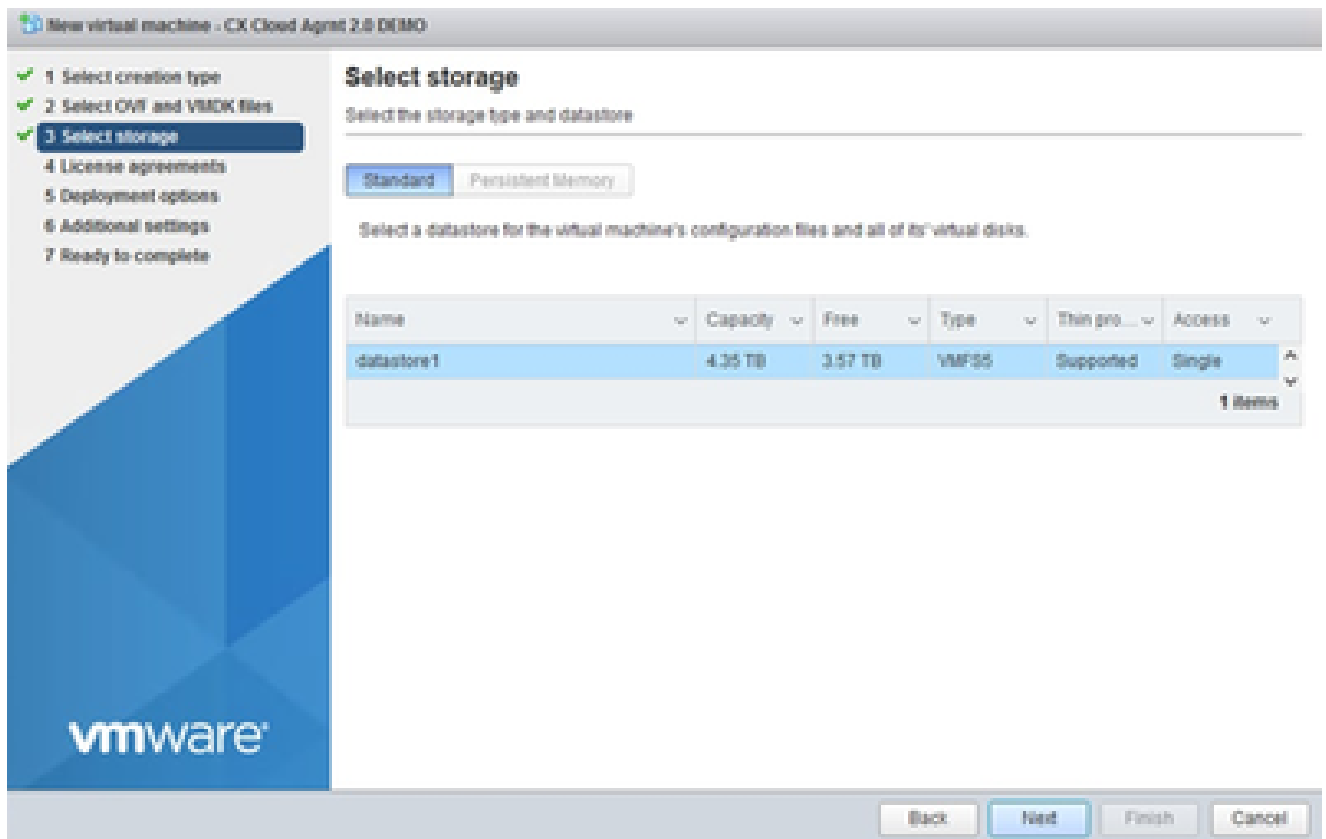
CANCEL

BACK

NEXT

Analisar detalhes

9. Selecione o formato de disco virtual e clique em Avançar.



Selecionar armazenamento

10. Clique em Next.

Deploy OVF Template

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

Review details

Verify the template details.

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

CANCEL

BACK

NEXT

Selecionar rede

11. Clique em Finish.

Deploy OVF Template

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

Ready to complete
Click Finish to start creation.

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

CANCEL

BACK

FINISH

Pronto para concluir

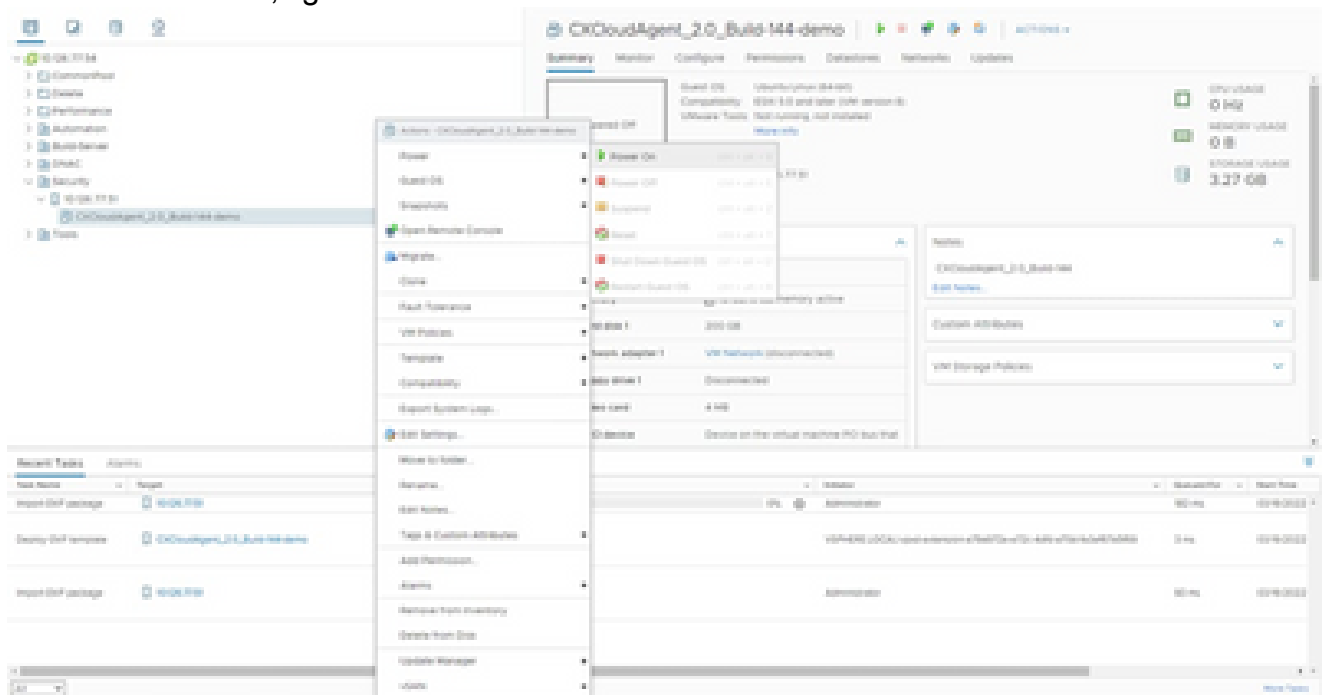
12. Clique no nome da VM recém-adicionada para exibir o status.

The screenshot shows the vSphere interface for a newly created VM named "CxCloudAgent_2.0_Build-144-demo". The VM is currently in a "Powered Off" state. The interface displays various hardware settings such as CPU (0 CPUs), Memory (16 GB), Hard disk 1 (200 GB), Network adapter 1 (VM Network), Floppy disk 1 (Disconnected), Video card (4 MB), and VMX device (Device on the virtual machine PC bus that). A "Recent Tasks" table at the bottom shows the deployment task as "Completed".

Task Name	Progress	Status	Message	Start Time	End Time
Import OVF template	100%	Completed		12/19/2022	12/19/2022
Deploy OVF template	100%	Completed	VMX: VMX file created successfully	12/19/2022	12/19/2022
Import OVF template	100%	Completed		12/19/2022	12/19/2022

VM adicionada

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



Abrir console

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

Instalação do Oracle Virtual Box 5.2.30

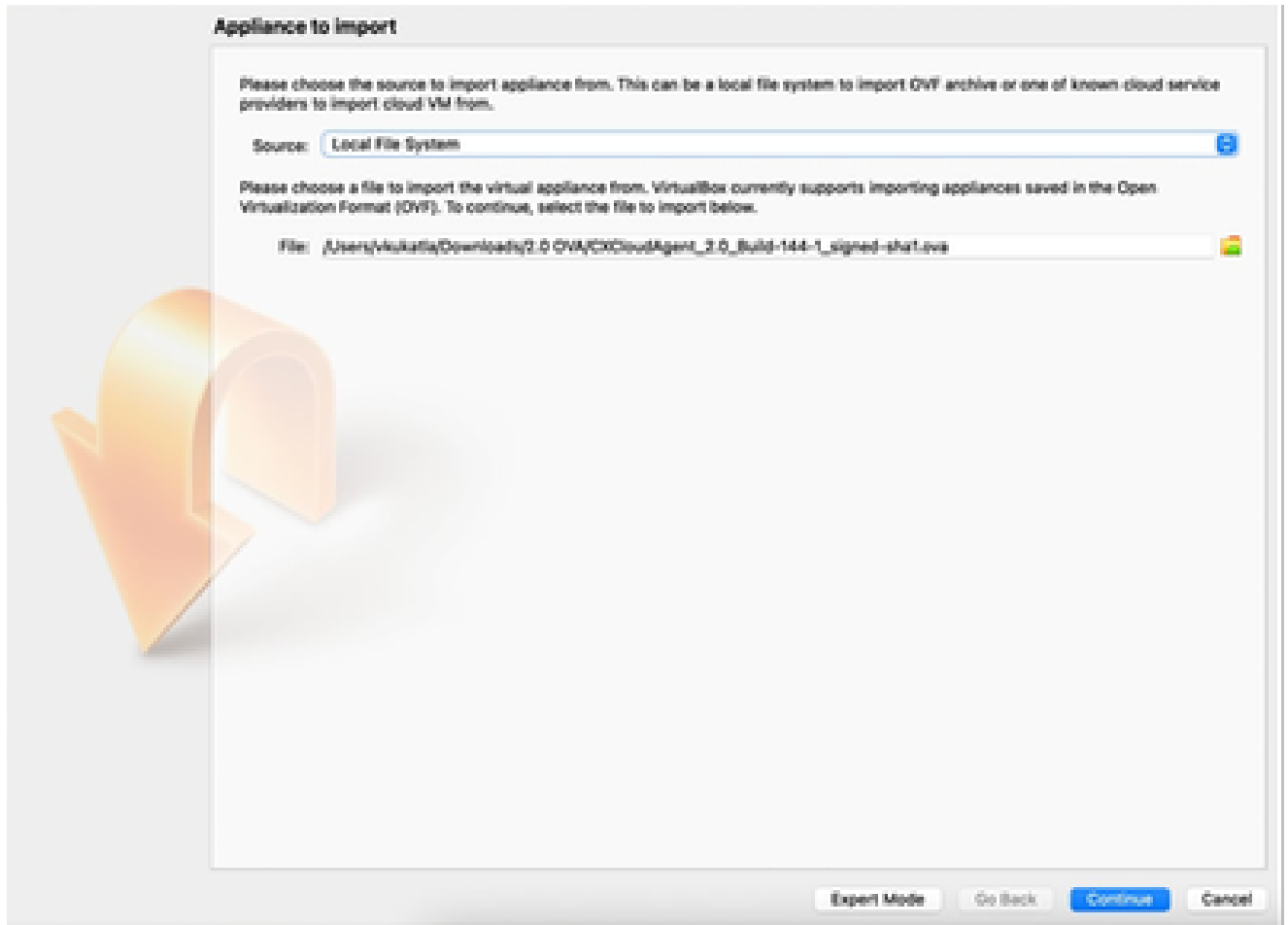
Esse cliente implanta o CX Cloud Agent OVA por meio do Oracle Virtual Box.

1. Abra a interface do usuário do Oracle VM e selecione File> Import Appliance.



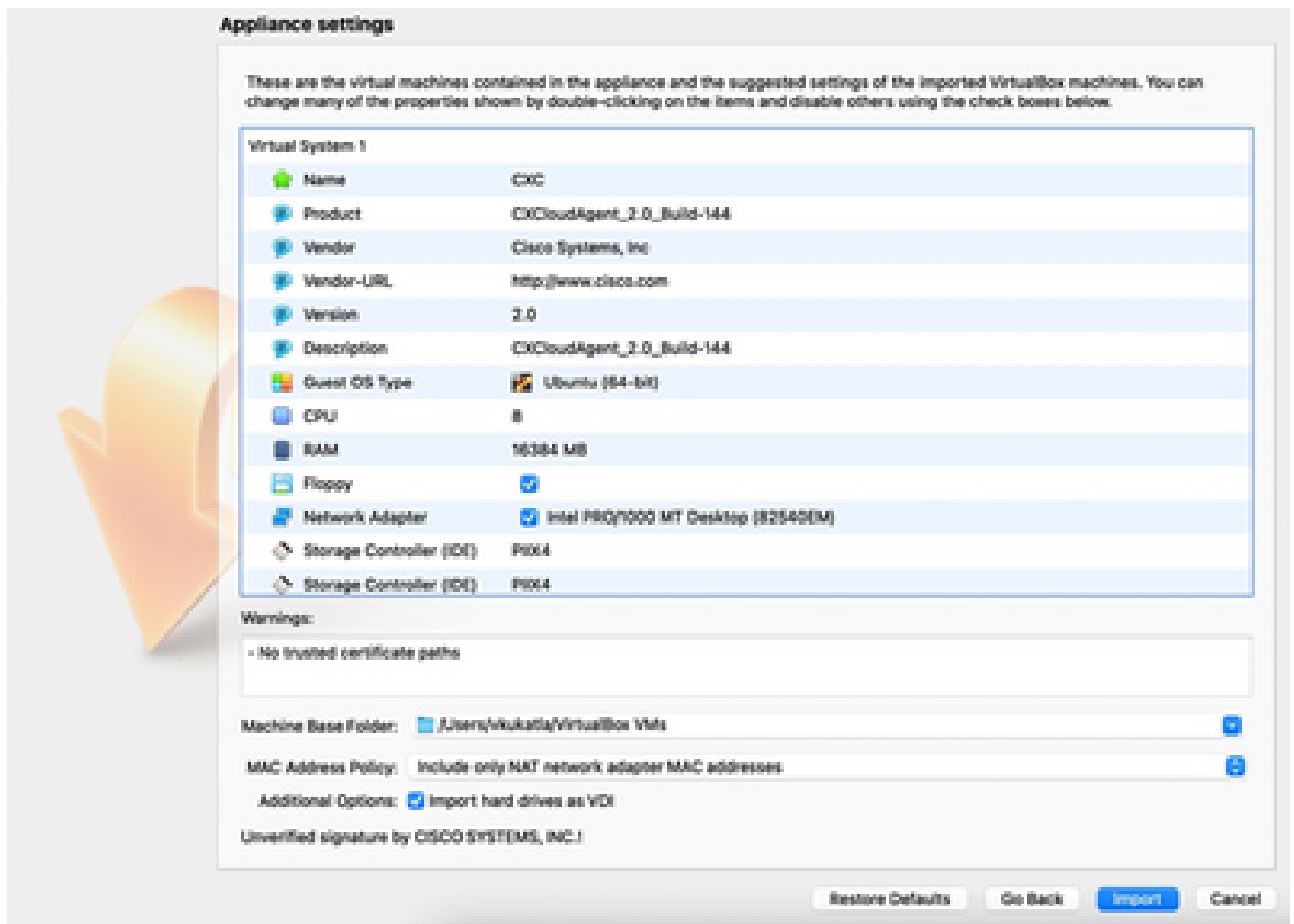
Oracle VM

2. Navegue para importar o arquivo de OVA.



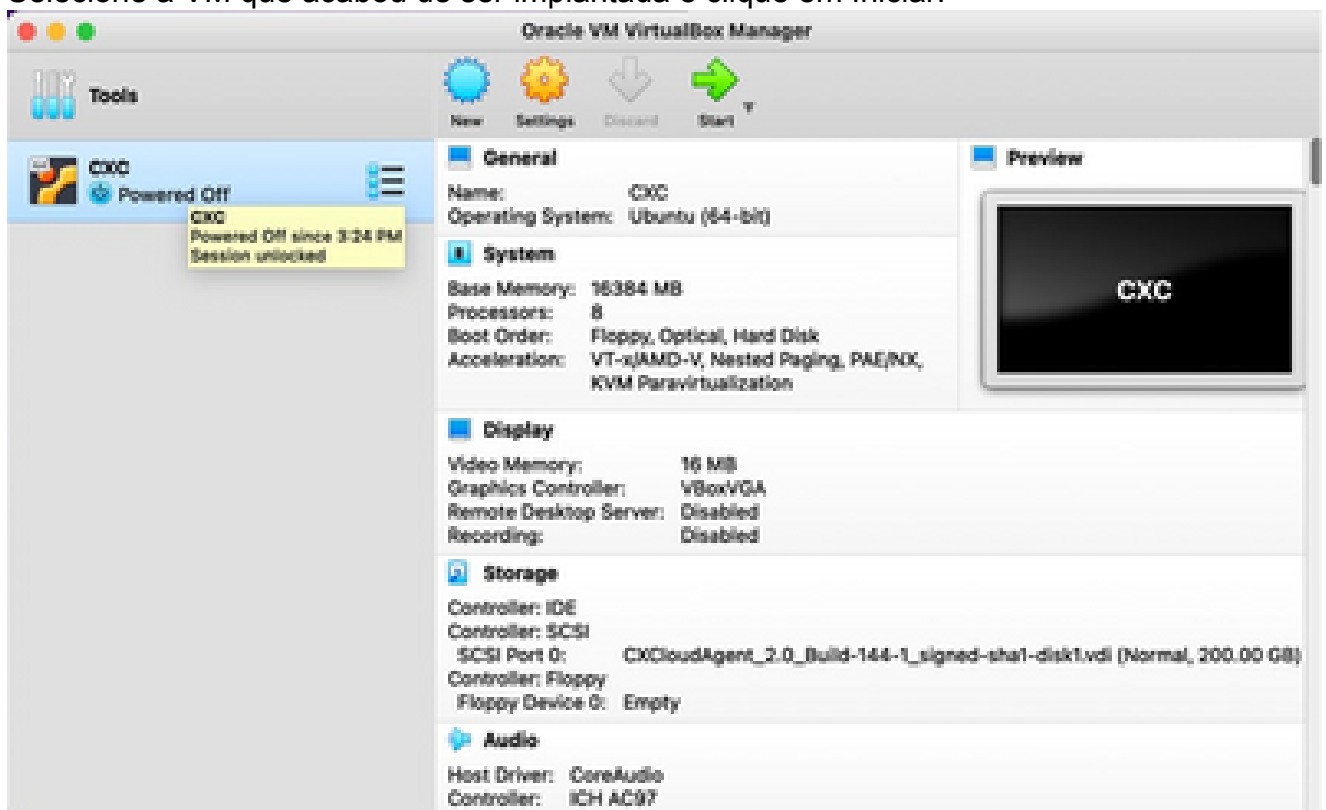
Selecionar arquivo

3. Clique em Importar.

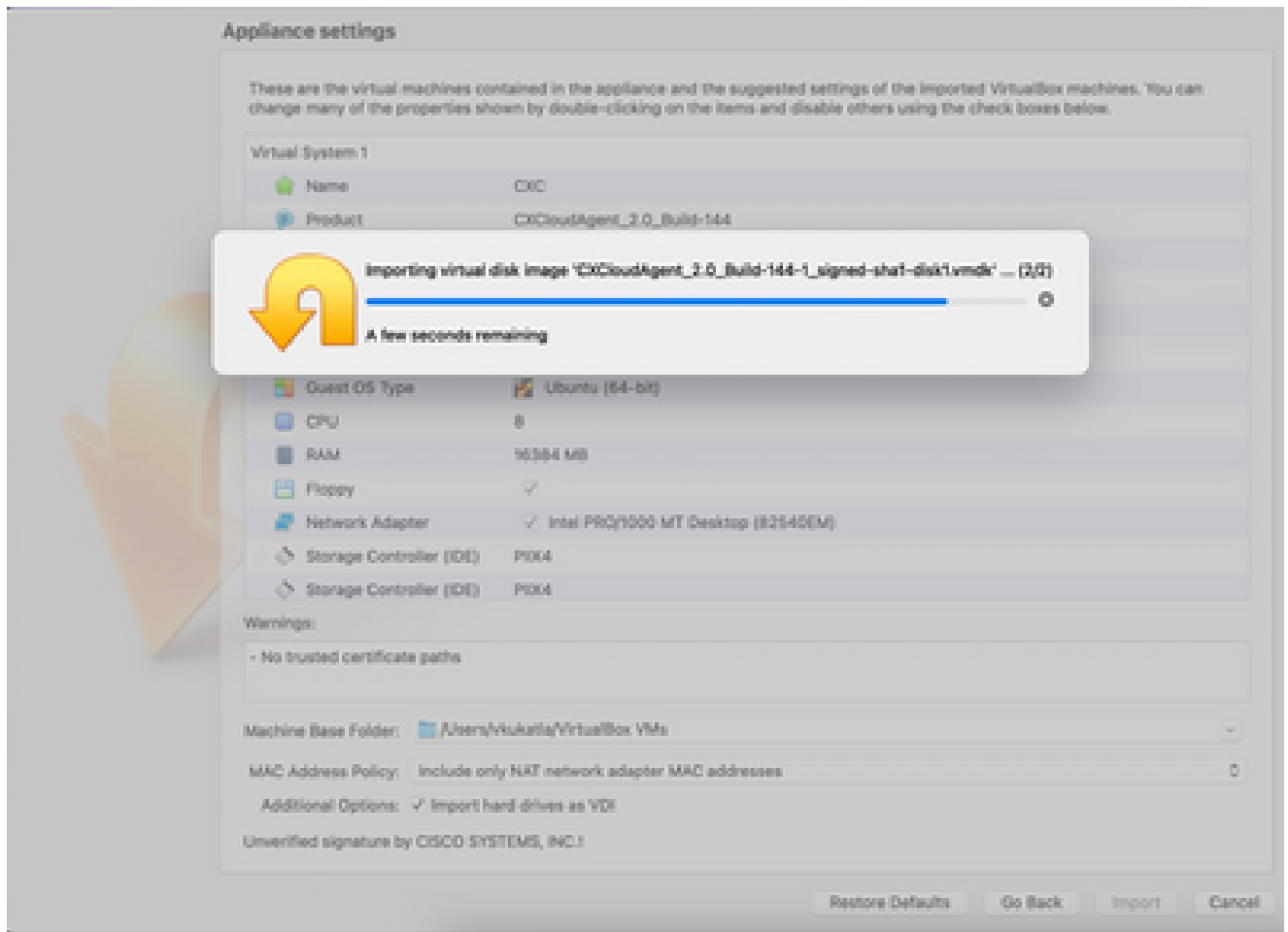


Importar arquivo

4. Selecione a VM que acabou de ser implantada e clique em Iniciar.



Inicialização do console da VM



Importação em andamento

5. Ligue a VM. O console exibirá.



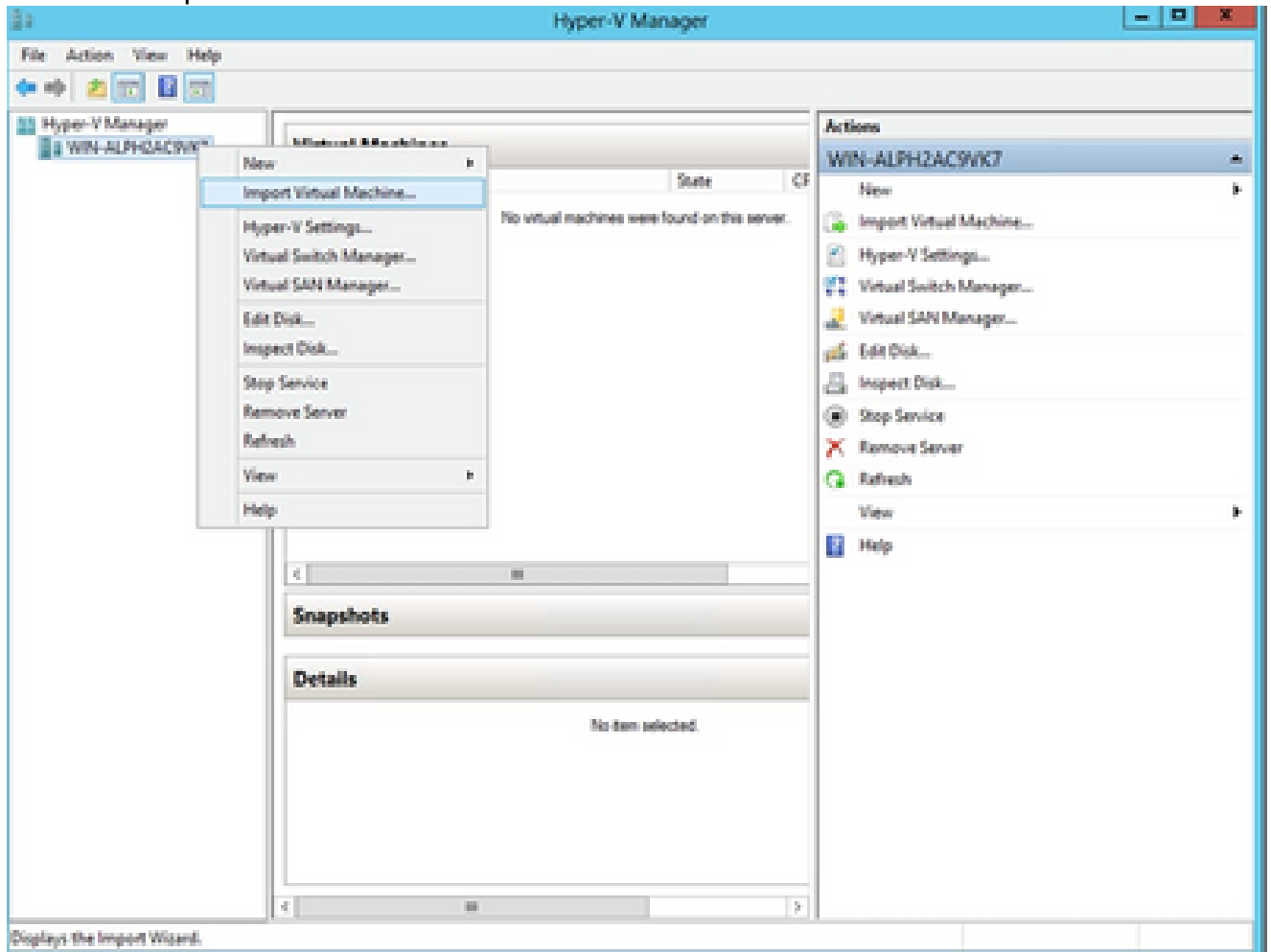
Abrir console

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

Instalação do Microsoft Hyper-V

Execute estas etapas:

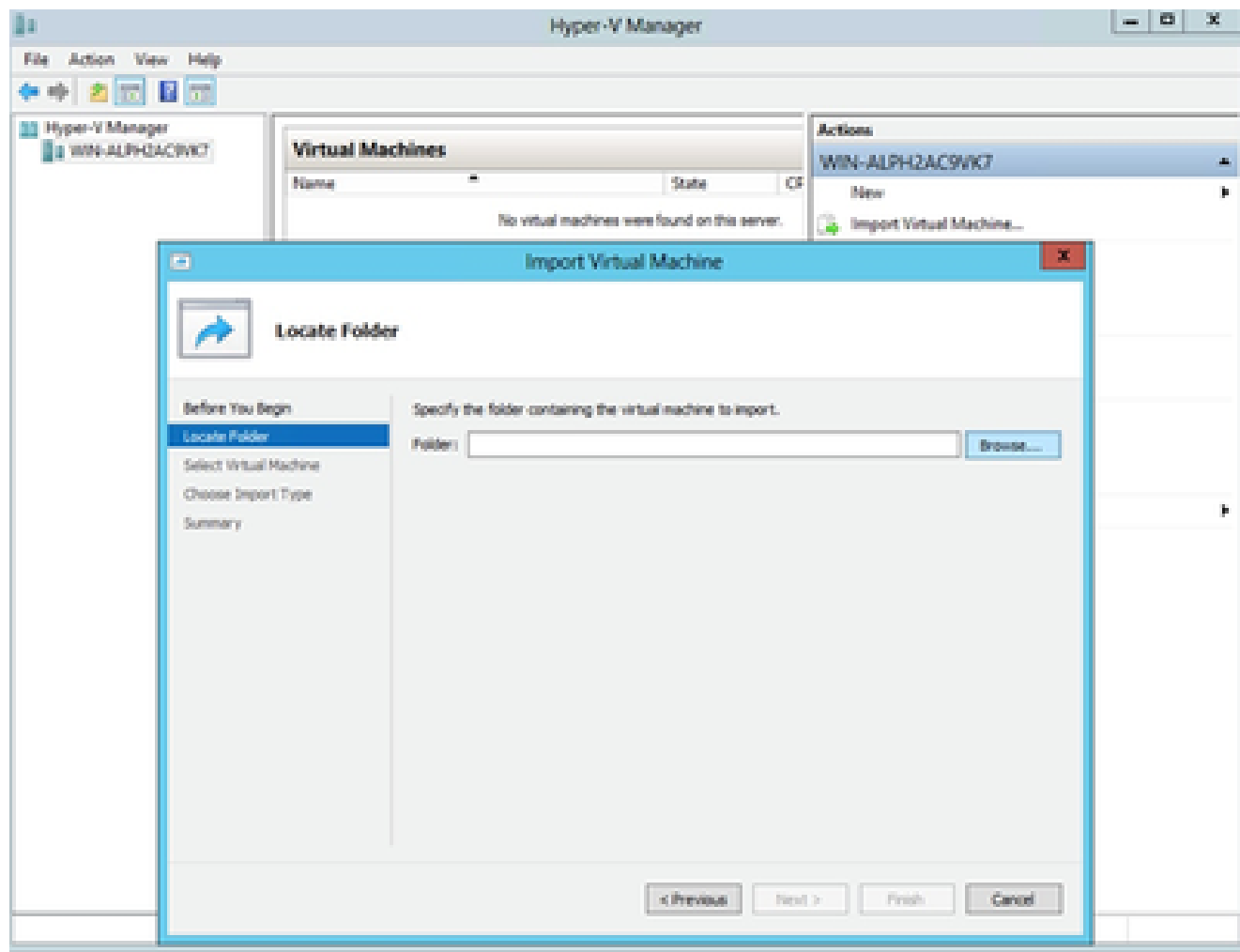
1. Selecione Import Virtual Machine.



Gerenciador Hyper V

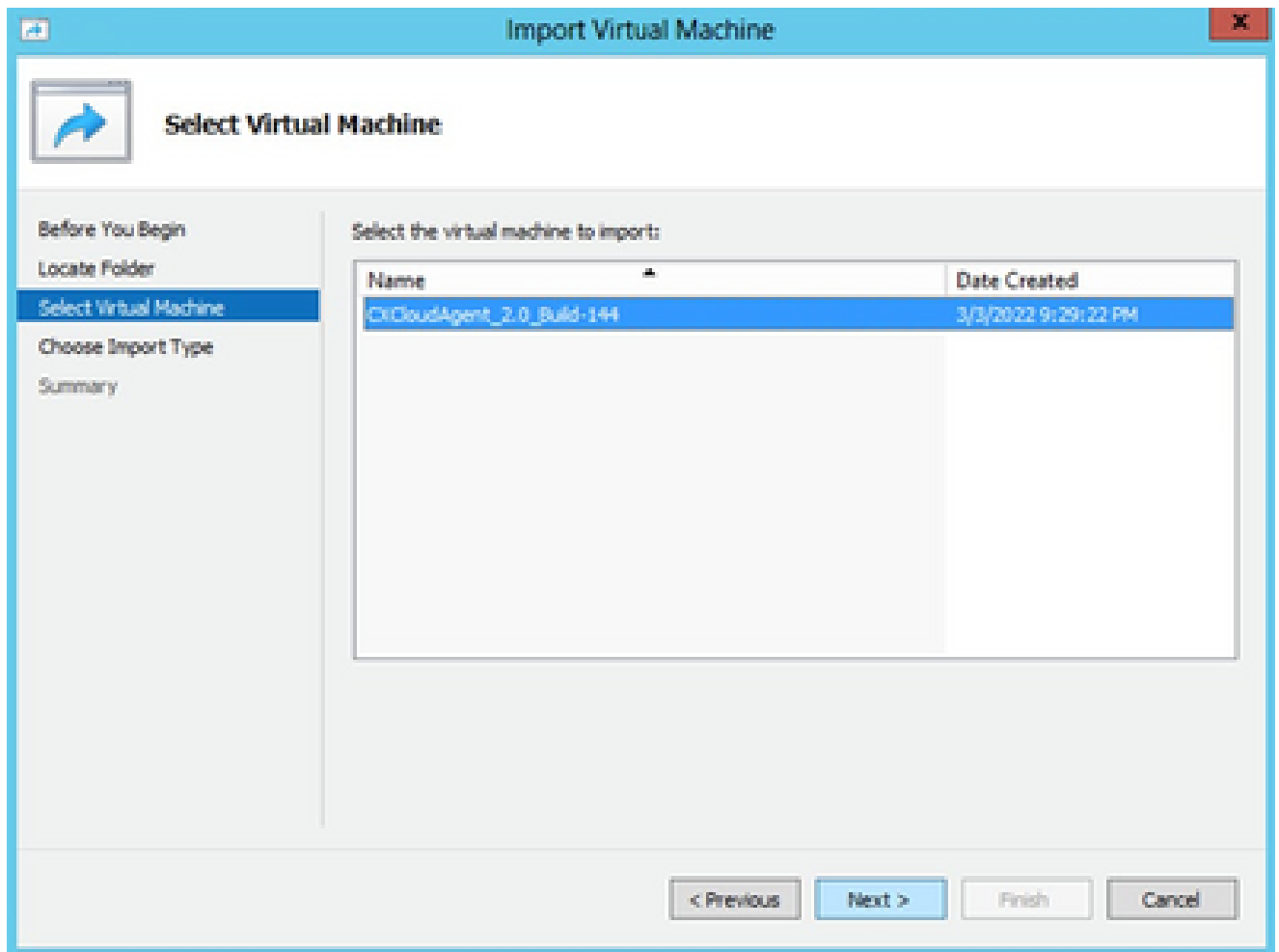
2. Procure e selecione a pasta de download.

3. Clique em Next.



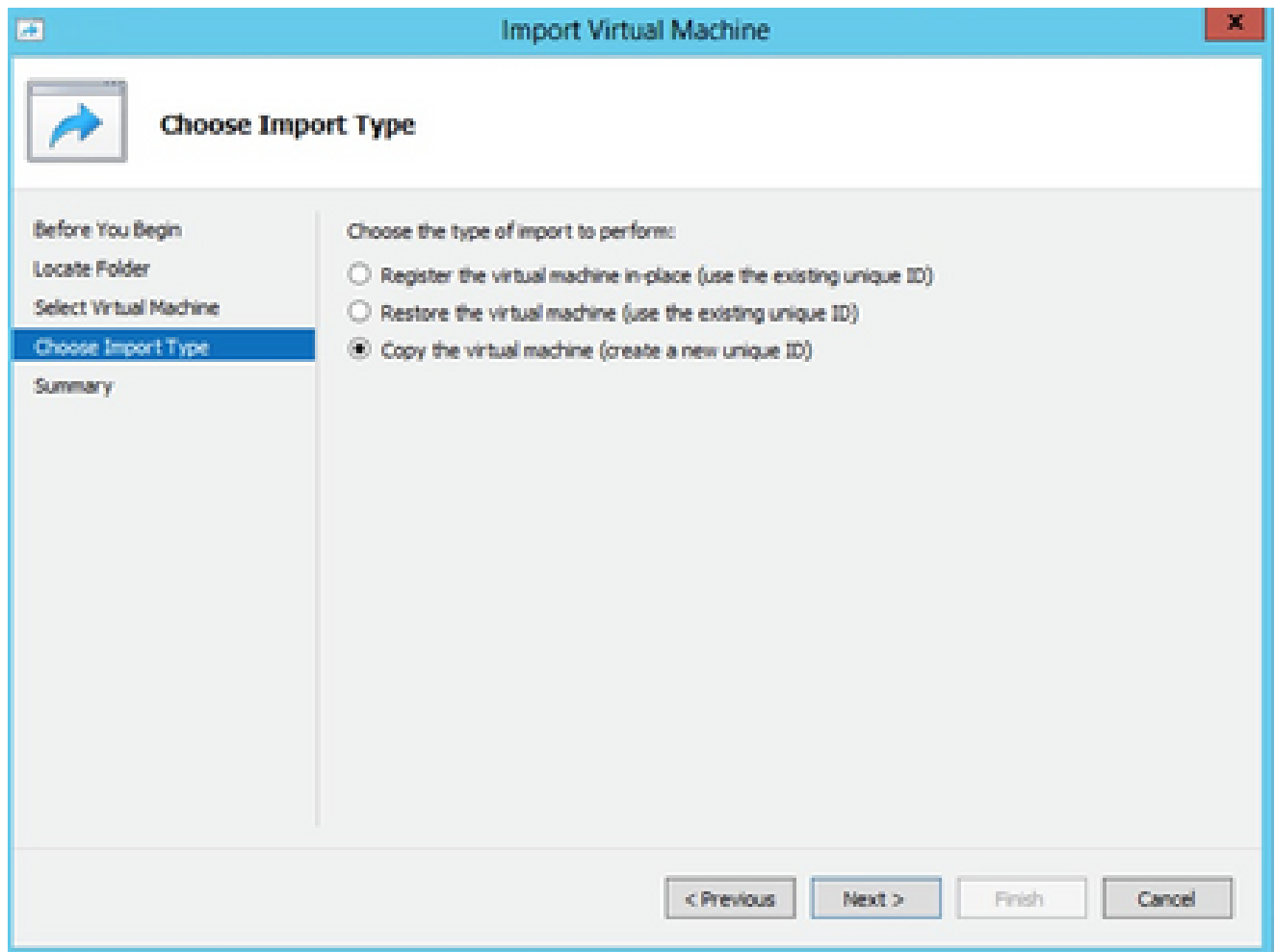
Pasta para importar

4. Selecione a VM e clique em Avançar.



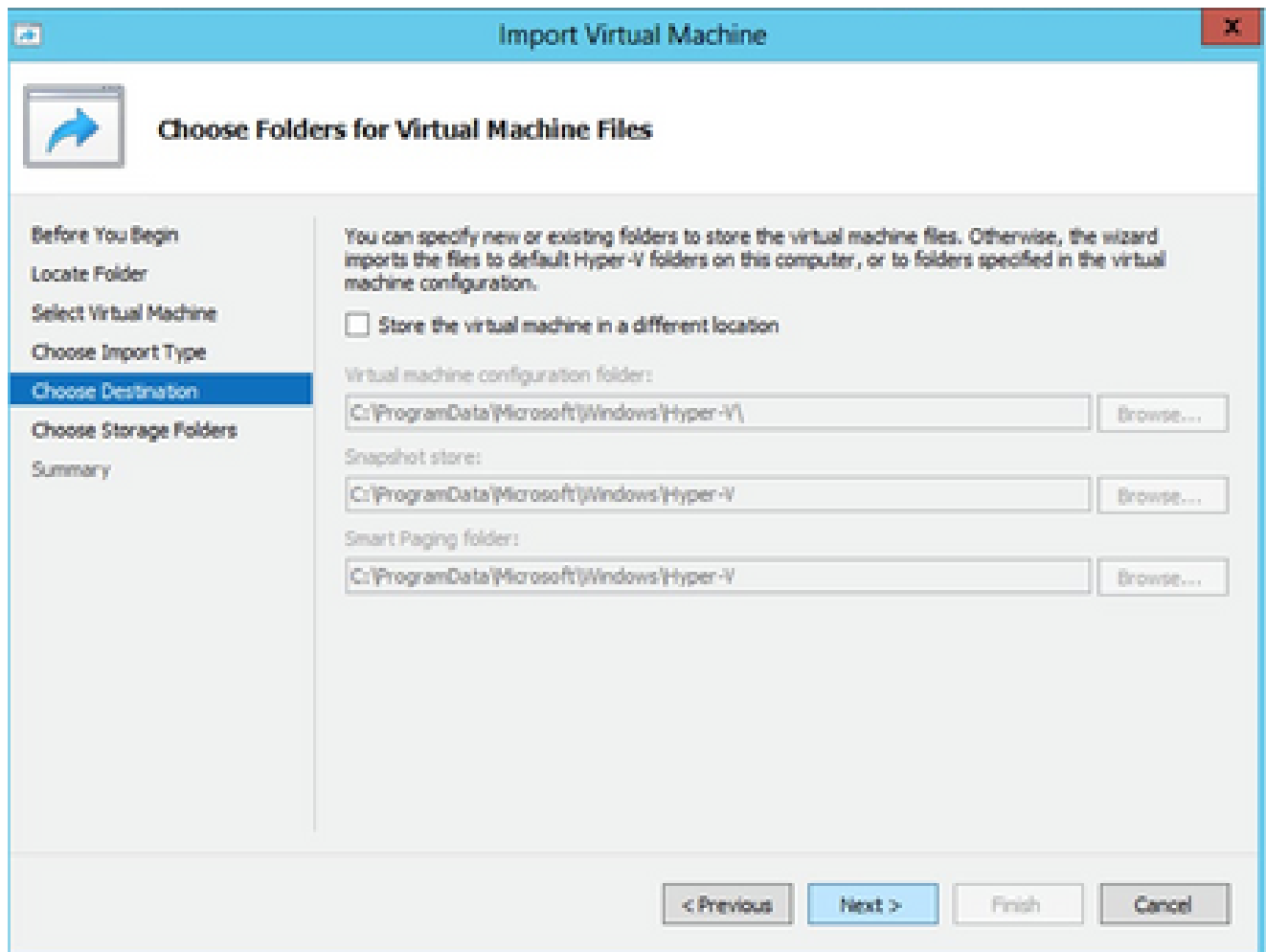
Selecionar VM

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.



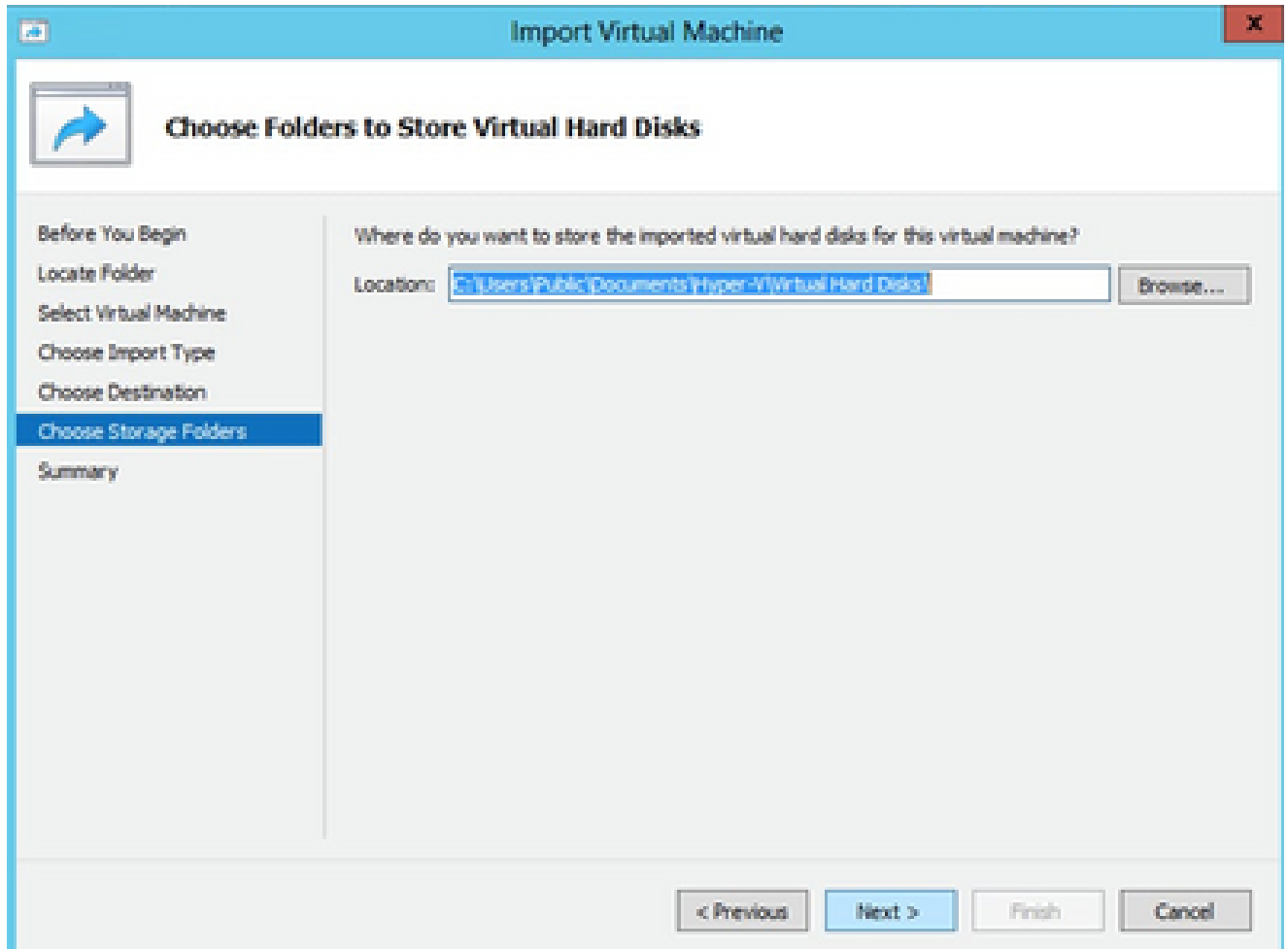
Tipo de importação

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



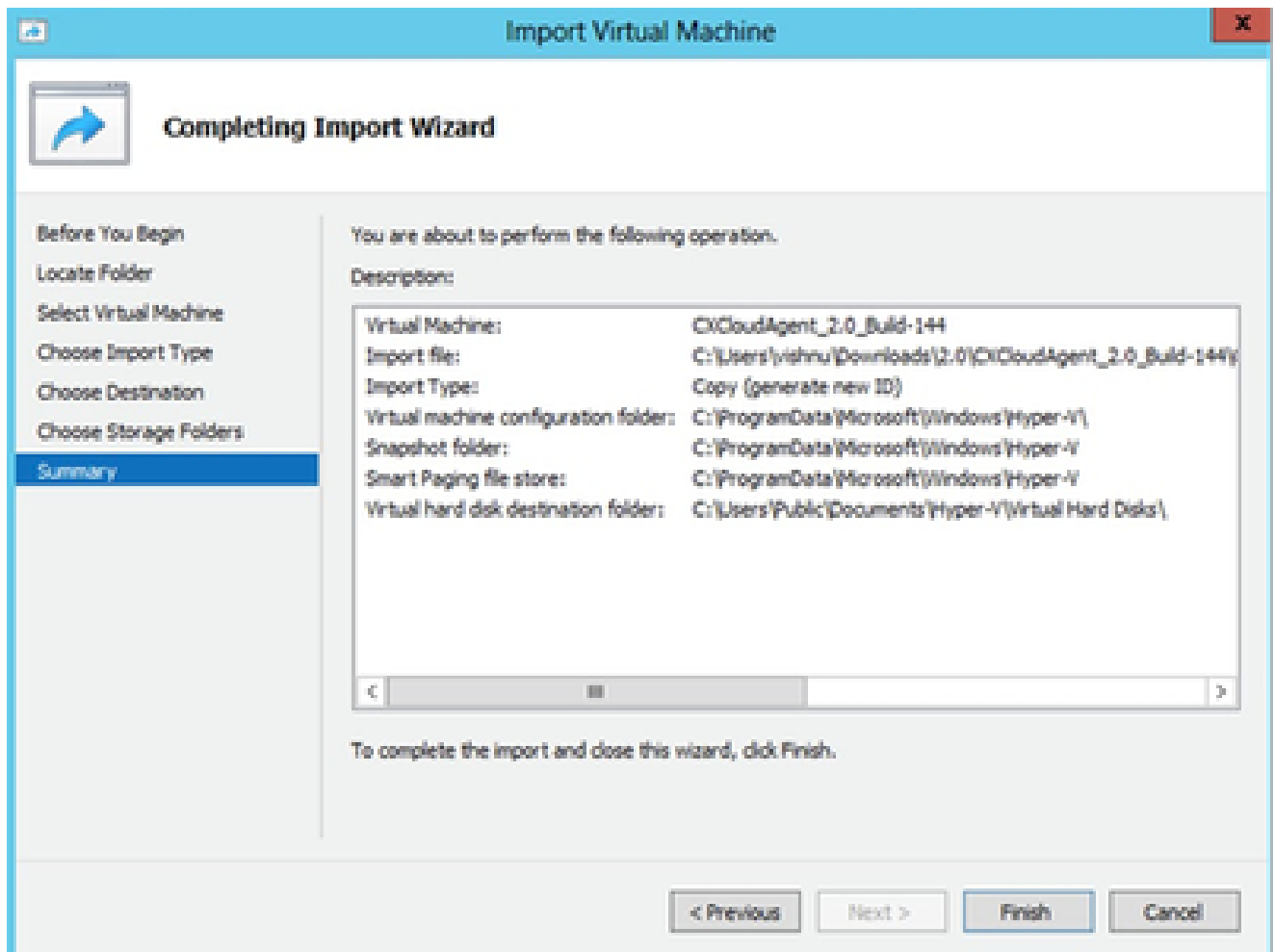
Escolher Pastas para Arquivos de Máquina Virtual

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



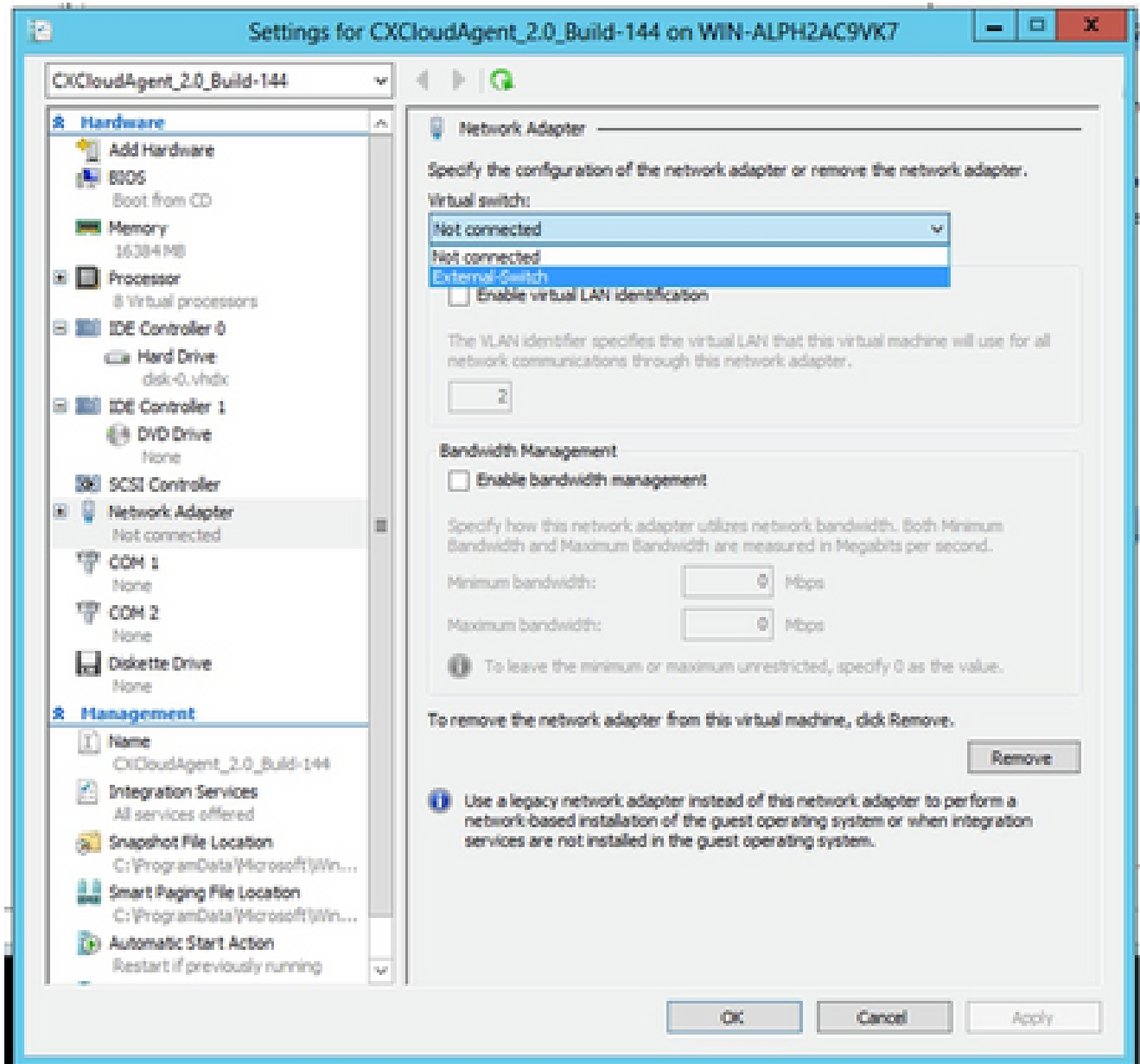
Pasta para armazenar os discos rígidos virtuais

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



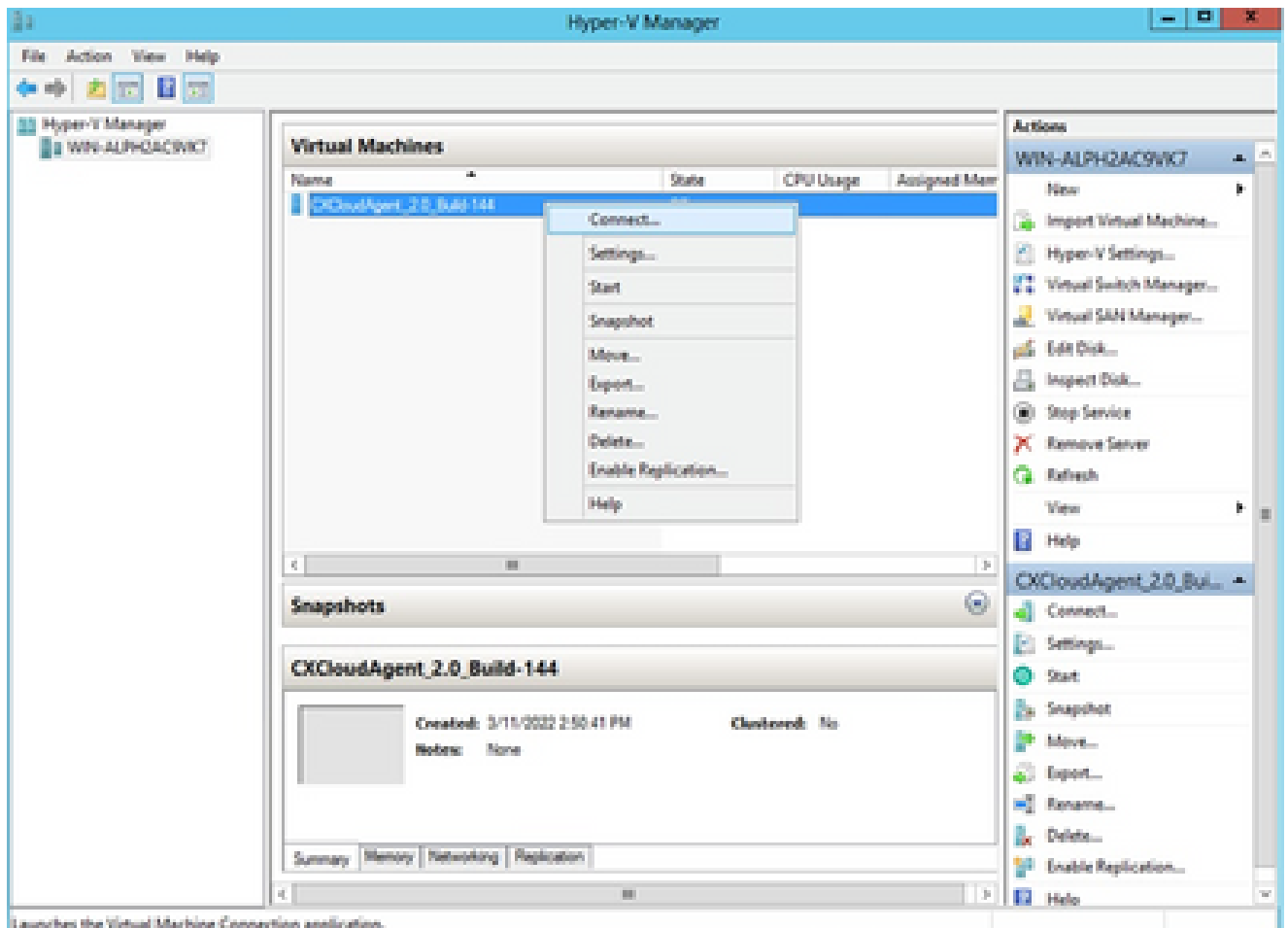
Summary

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



Switch Virtual

13. Seleccione Connect para iniciar a VM.



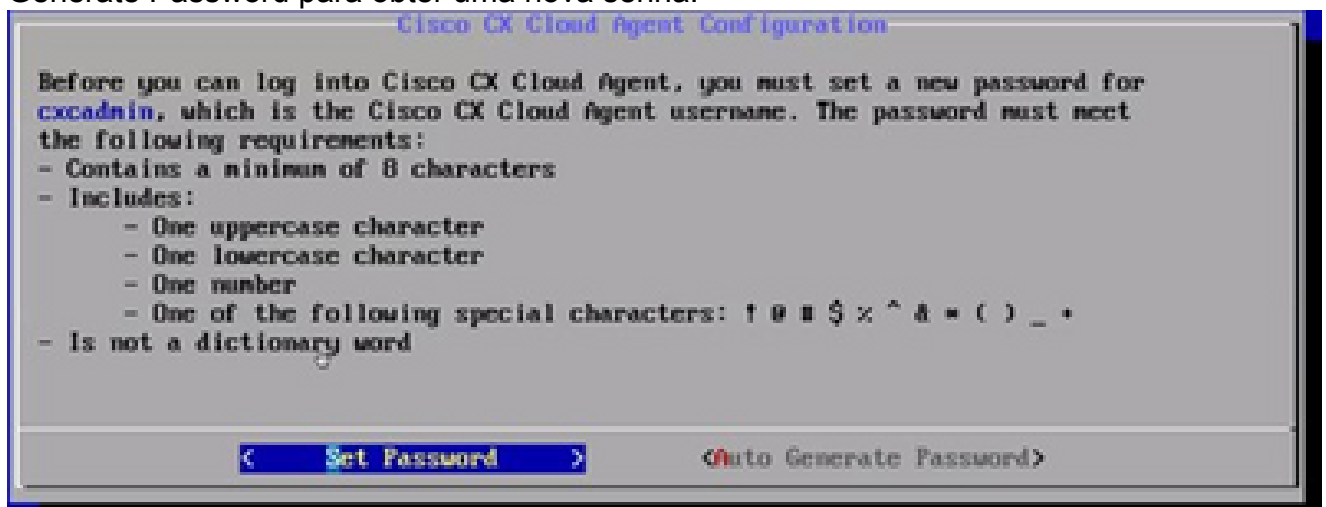
Launches the Virtual Machine Connection application.

Inicialização da VM

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

Configuração de rede

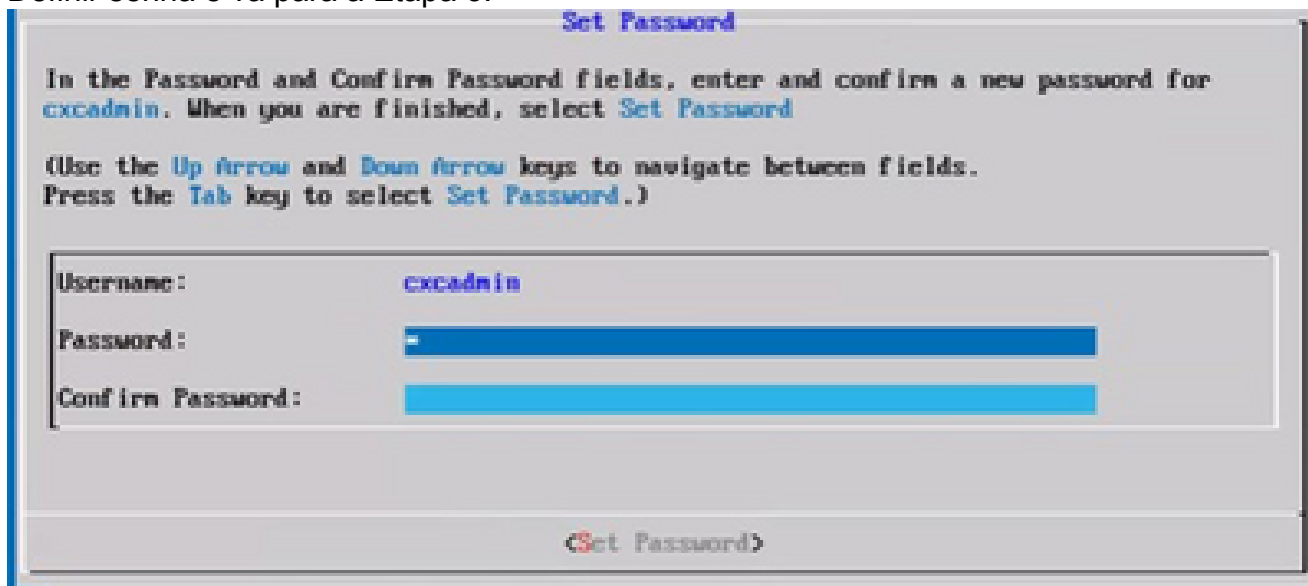
1. Clique em Set Password para adicionar uma nova senha para cxcadmin OU clique em Auto Generate Password para obter uma nova senha.



Definir senha

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

Definir senha e vá para a Etapa 3.



Nova senha

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.



Senha gerada automaticamente

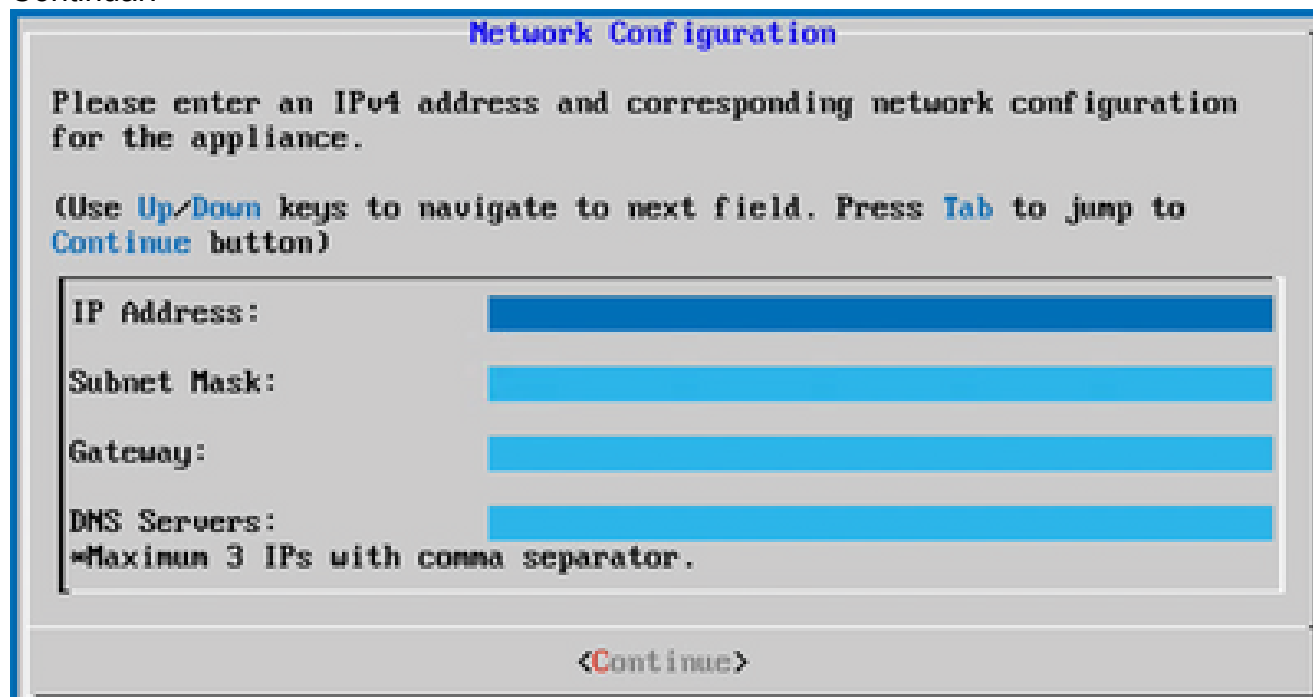
3. Clique em Salvar senha para usá-la para autenticação.



Salvar senha

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

Continuar.



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:

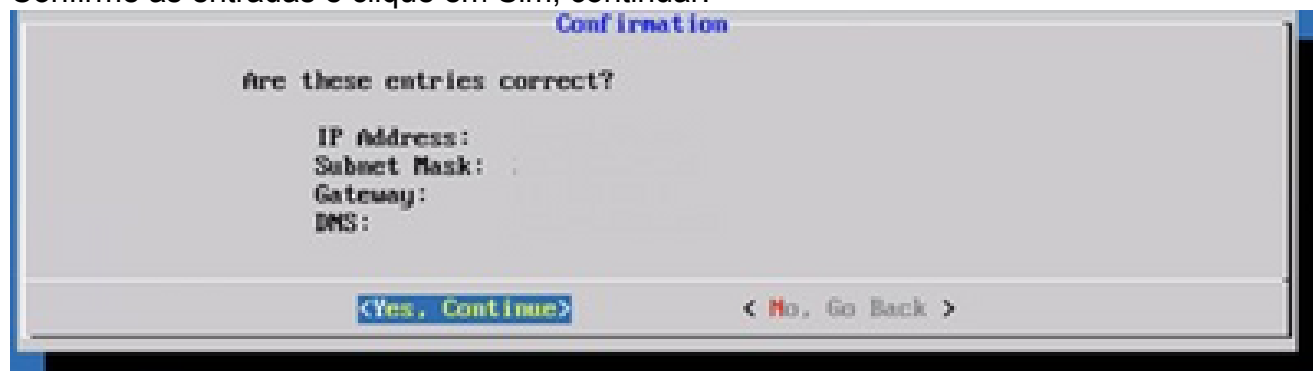
DNS Servers:

Maximum 3 IPs with comma separator.

<Continue>

Configuração de rede

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



Confirmation

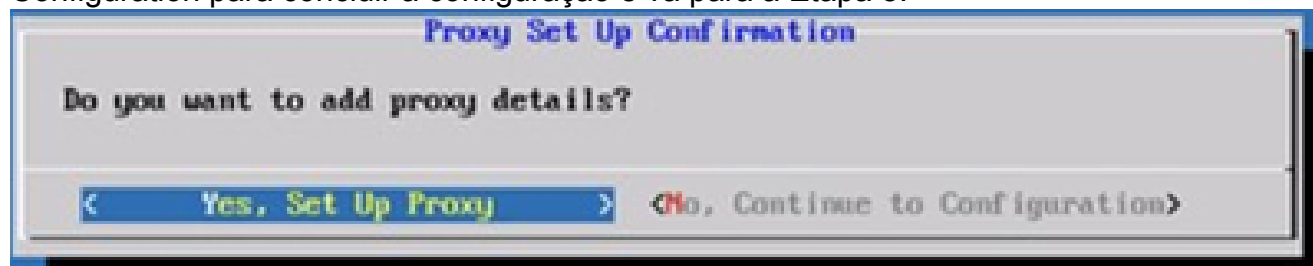
Are these entries correct?

IP Address:
Subnet Mask: .
Gateway:
DNS:

<Yes, Continue> **<No, Go Back >**

Configuração

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



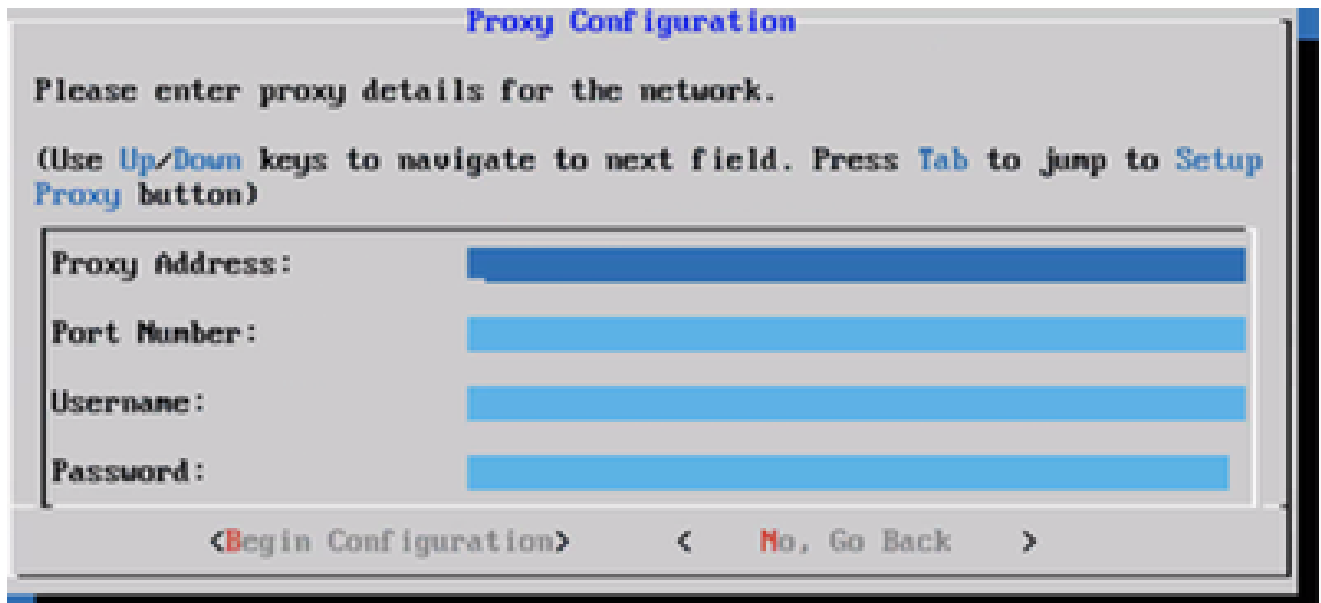
Proxy Set Up Confirmation

Do you want to add proxy details?

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

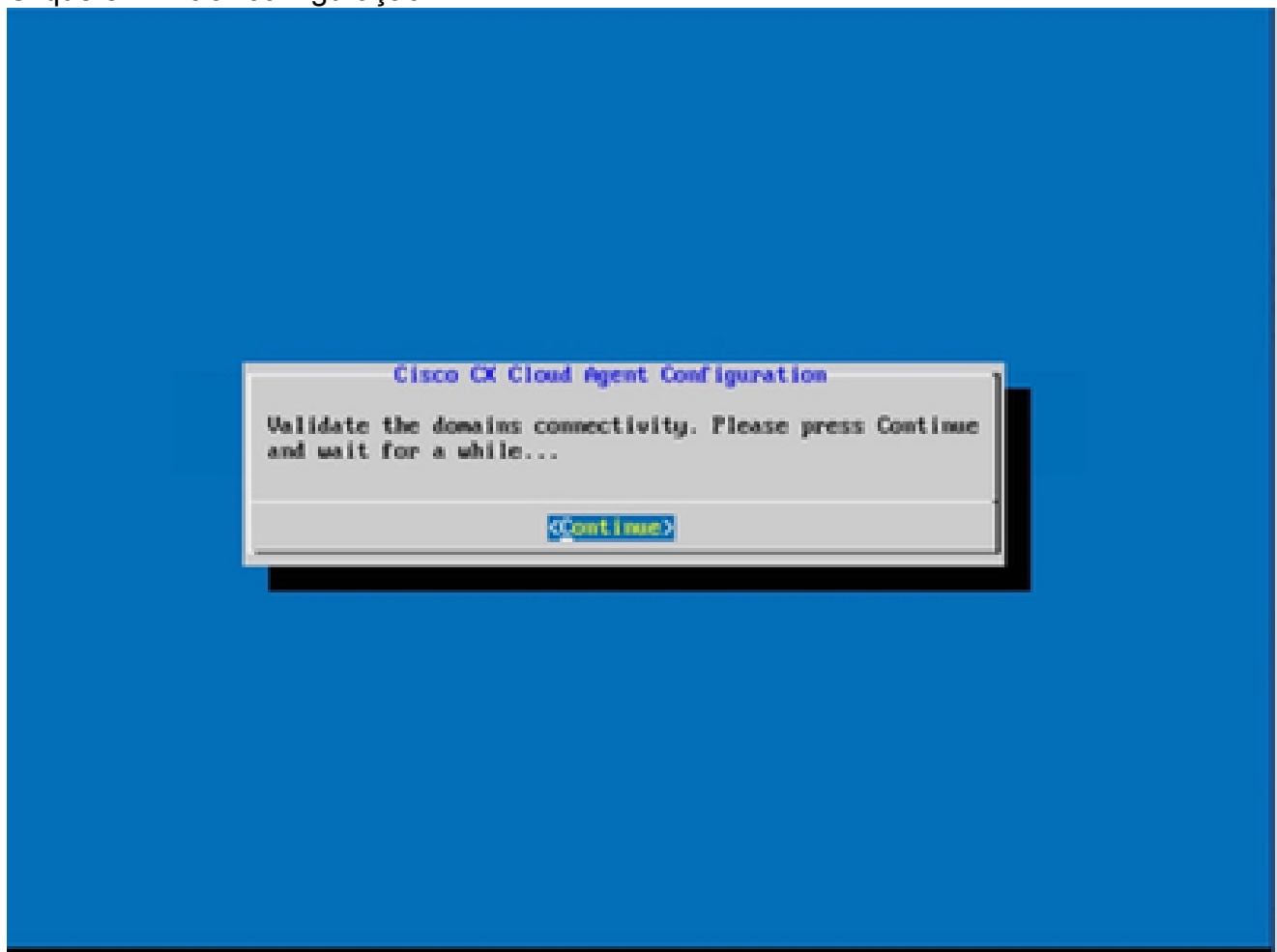
Instalação de proxy

7. Digite o endereço do proxy, o número da porta, o nome do usuário e a senha.



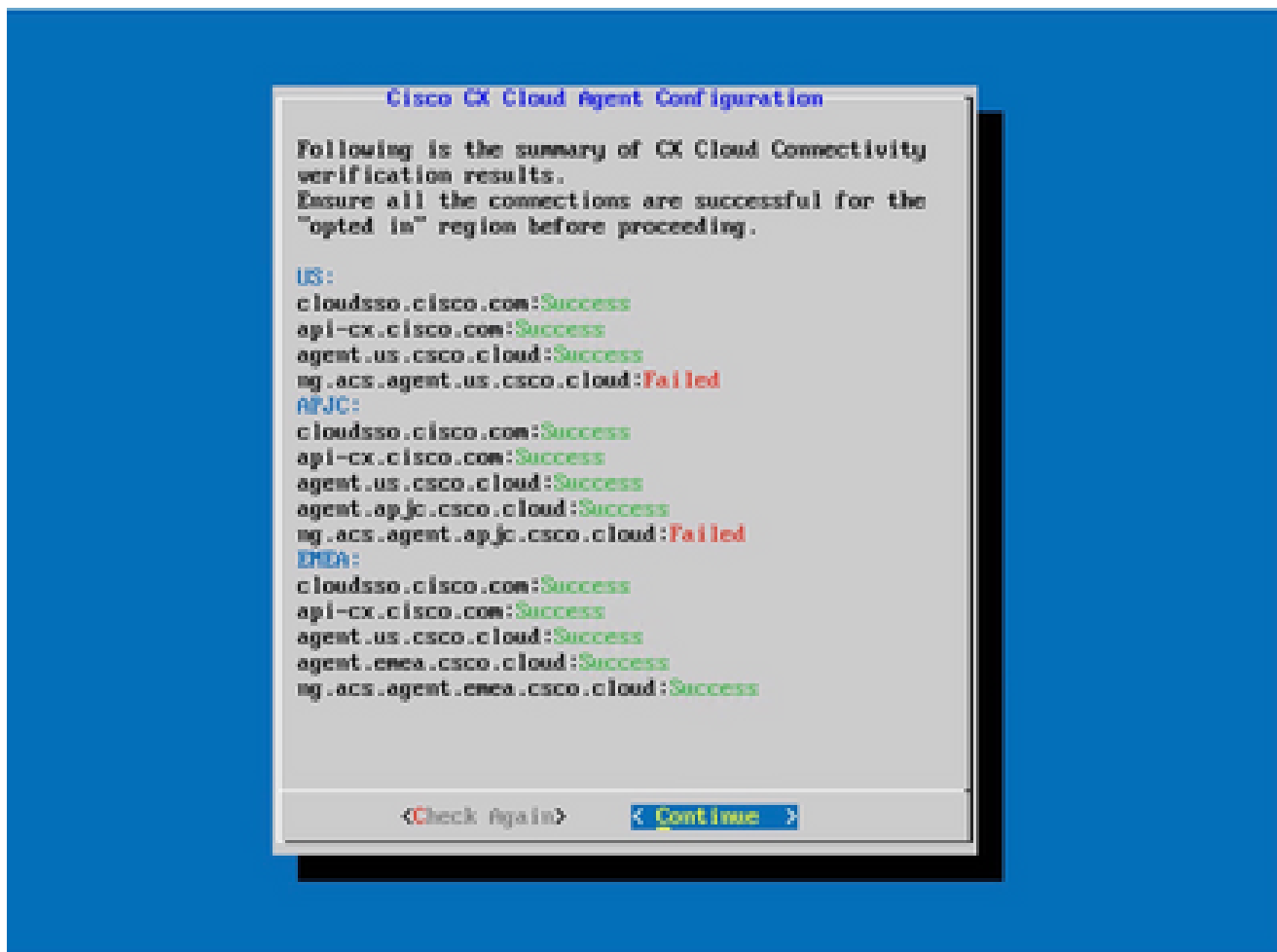
Configuração de proxy

8. Clique em Iniciar configuração.




Configuração inicial

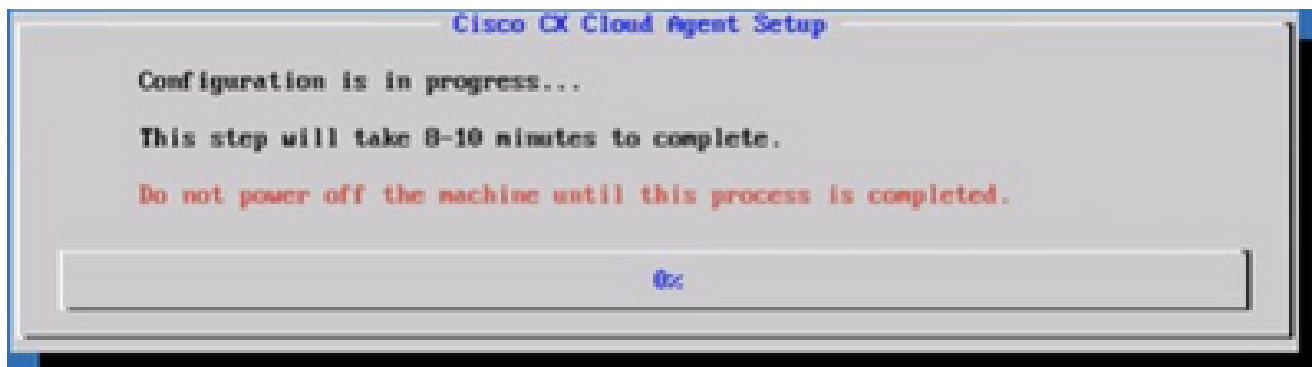
9. Clique em Continuar.



A configuração continua

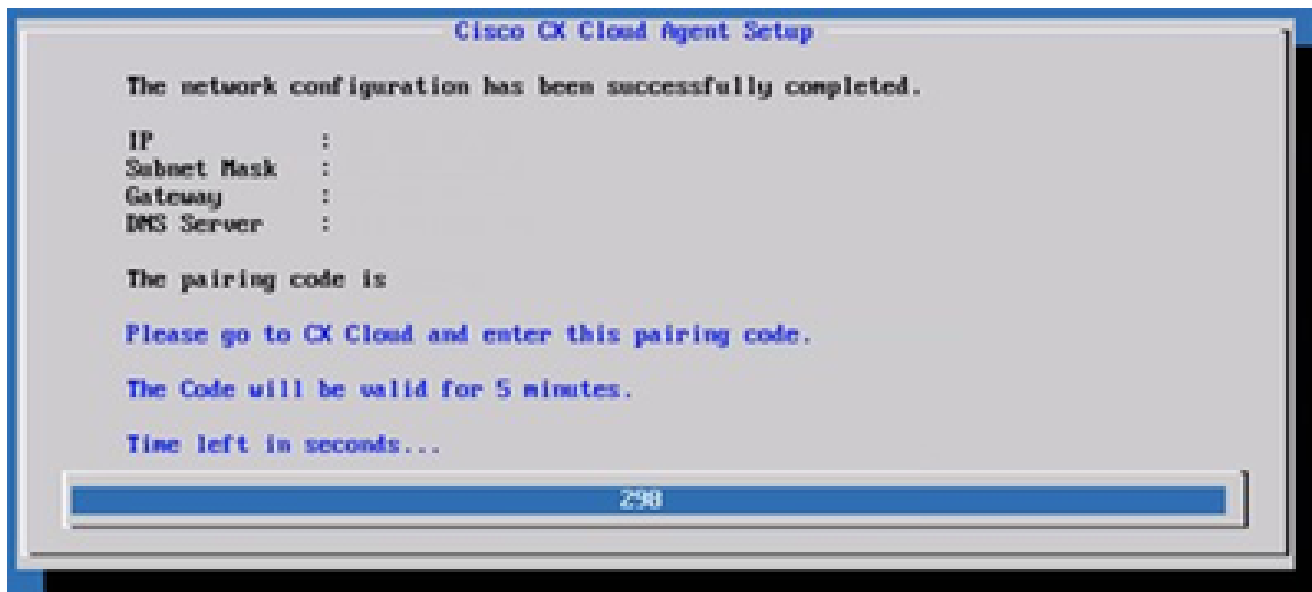
10. Clique em Continuar para continuar com a configuração para o alcance de domínio bem-sucedido. A configuração pode levar vários minutos para ser concluída.

 **Observação:** 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.



Configuração em andamento

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



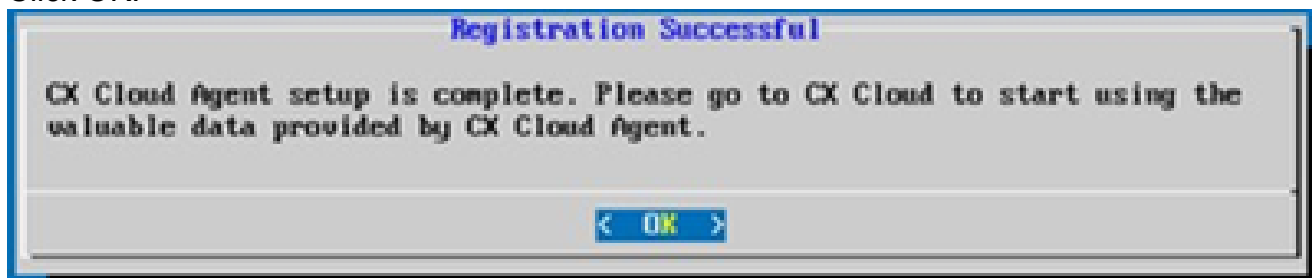
Código de emparelhamento

12. Se o código de emparelhamento expirar, clique em Register to CX Cloud para obter o código novamente.



Código expirado

13. Click OK.



Registro realizado com sucesso

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 : xJ7I8P
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.

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

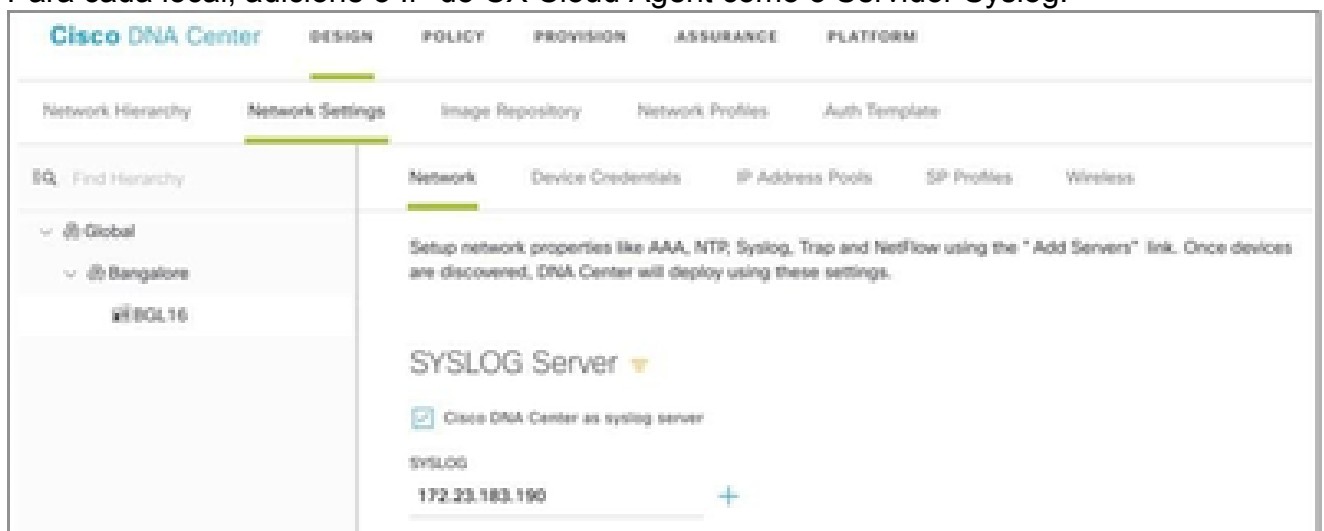
Pré-requisitos

As versões compatíveis do Cisco DNA 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 DNA Center Virtual Appliance


Definir Configuração De Encaminhamento De Syslog

Para configurar o encaminhamento de syslog para o CX Cloud Agent no Cisco DNA Center, execute estas etapas:

1. Inicie o Cisco DNA Center.
2. Vá para Design > Configurações de rede > Rede.
3. Para cada local, adicione o IP do CX Cloud Agent como o Servidor Syslog.




Servidor Syslog

 **Notas:**

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


Configurar outros ativos para encaminhar o Syslog ao CX Cloud Agent

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

 **Observação:** somente os dispositivos Nível 2 do Campus Success são qualificados para configurar outros ativos para encaminhar syslog.

Servidores Syslog existentes com capacidade de encaminhamento

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

 **Observação:** 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 CX Cloud Agent. 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](#)

Habilitar Configurações de Syslog de Nível de Informação

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

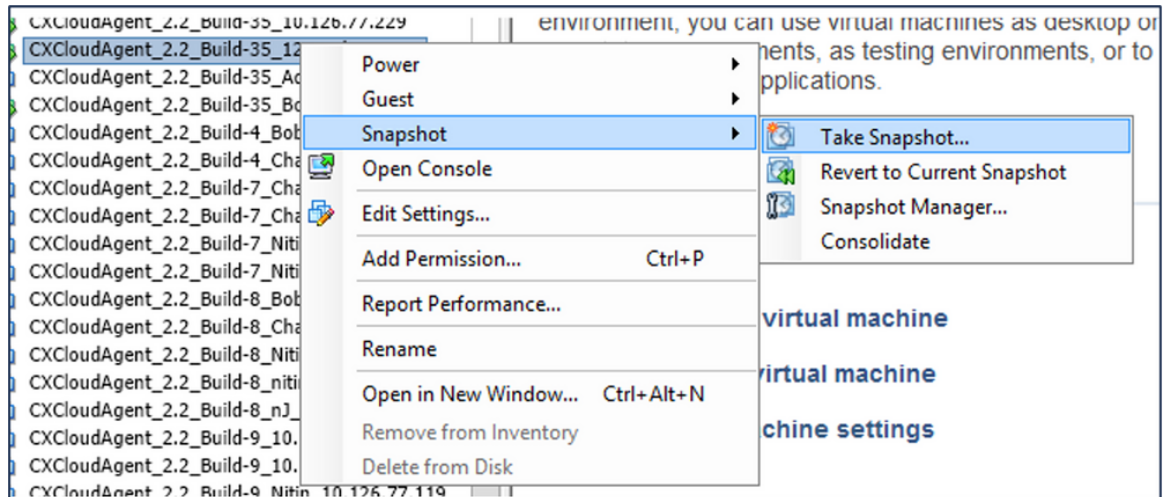
Backup e restauração da VM em nuvem do CX

É recomendável preservar o estado e os dados de uma VM do CX Cloud Agent 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.

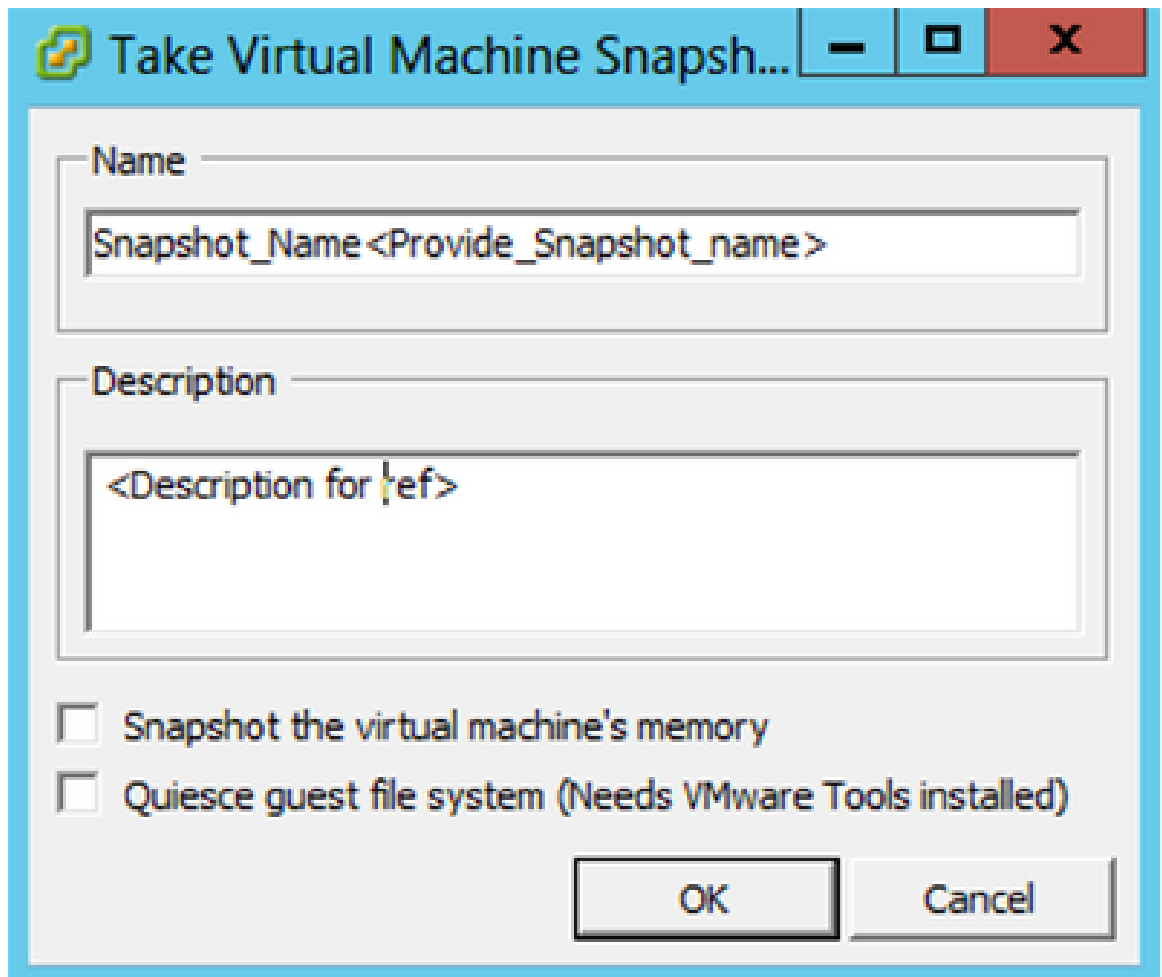
Fazer backup

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

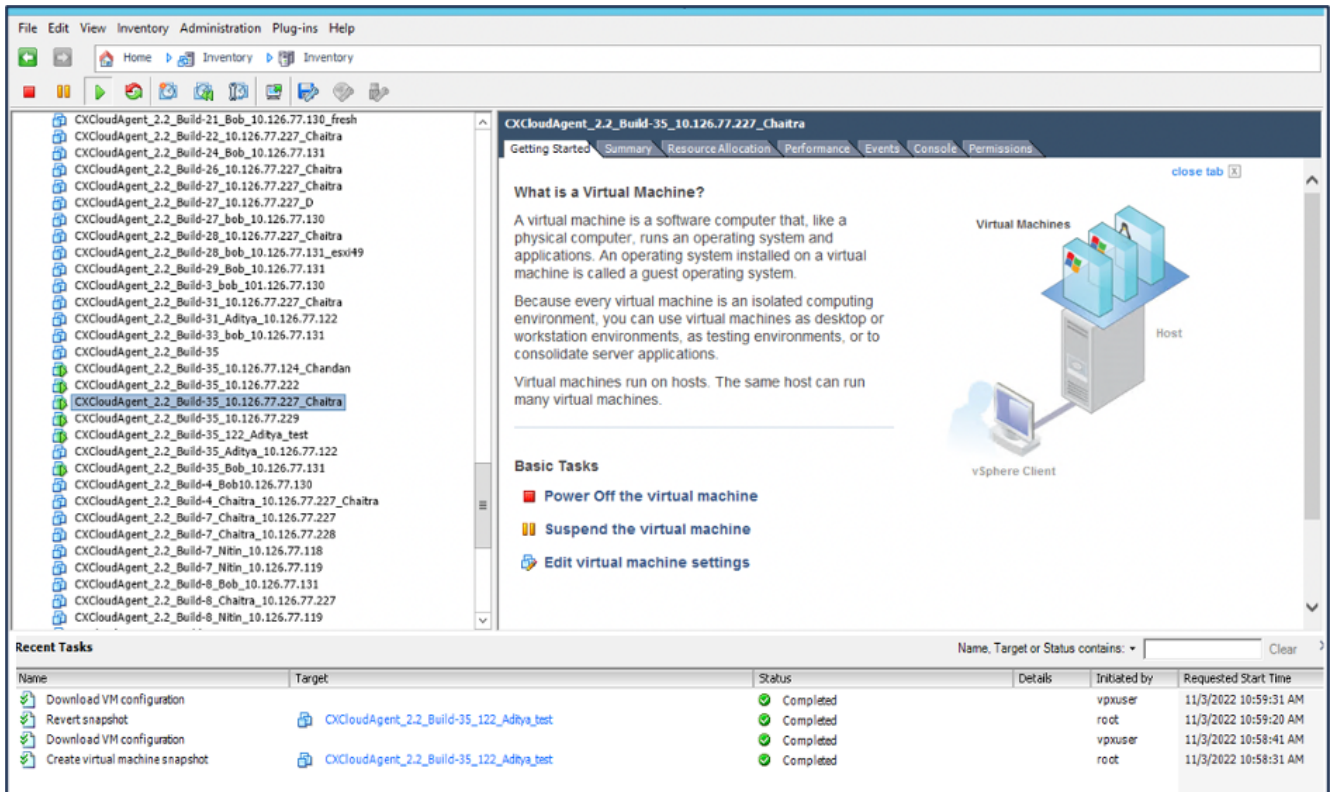


Tirar Instantâneo da Máquina Virtual

2. Insira Name e Description.

 Observação: 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.

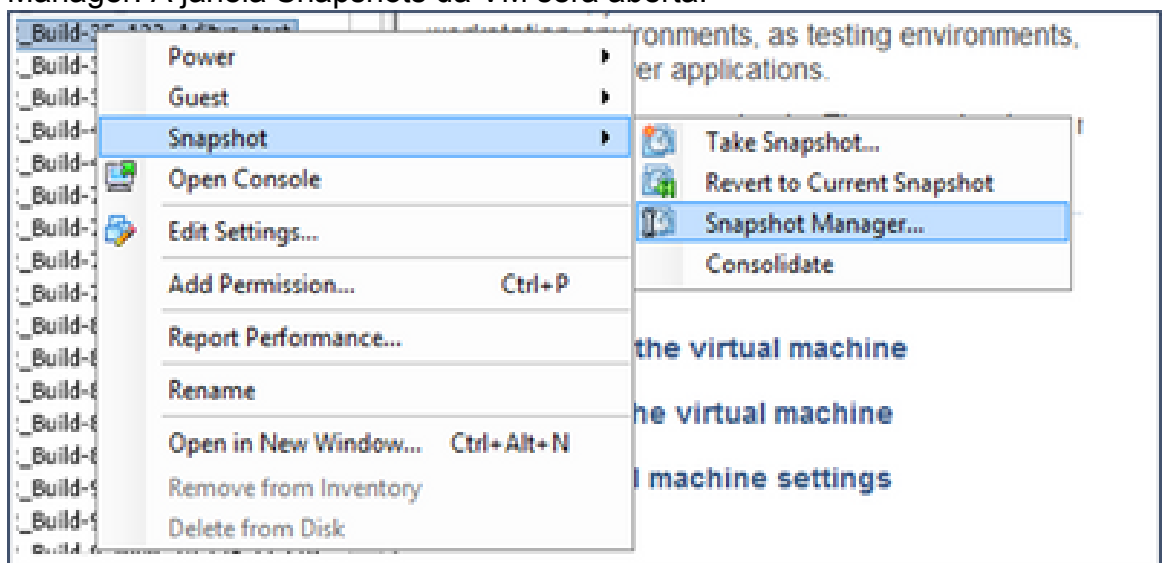


Tarefas Recentes

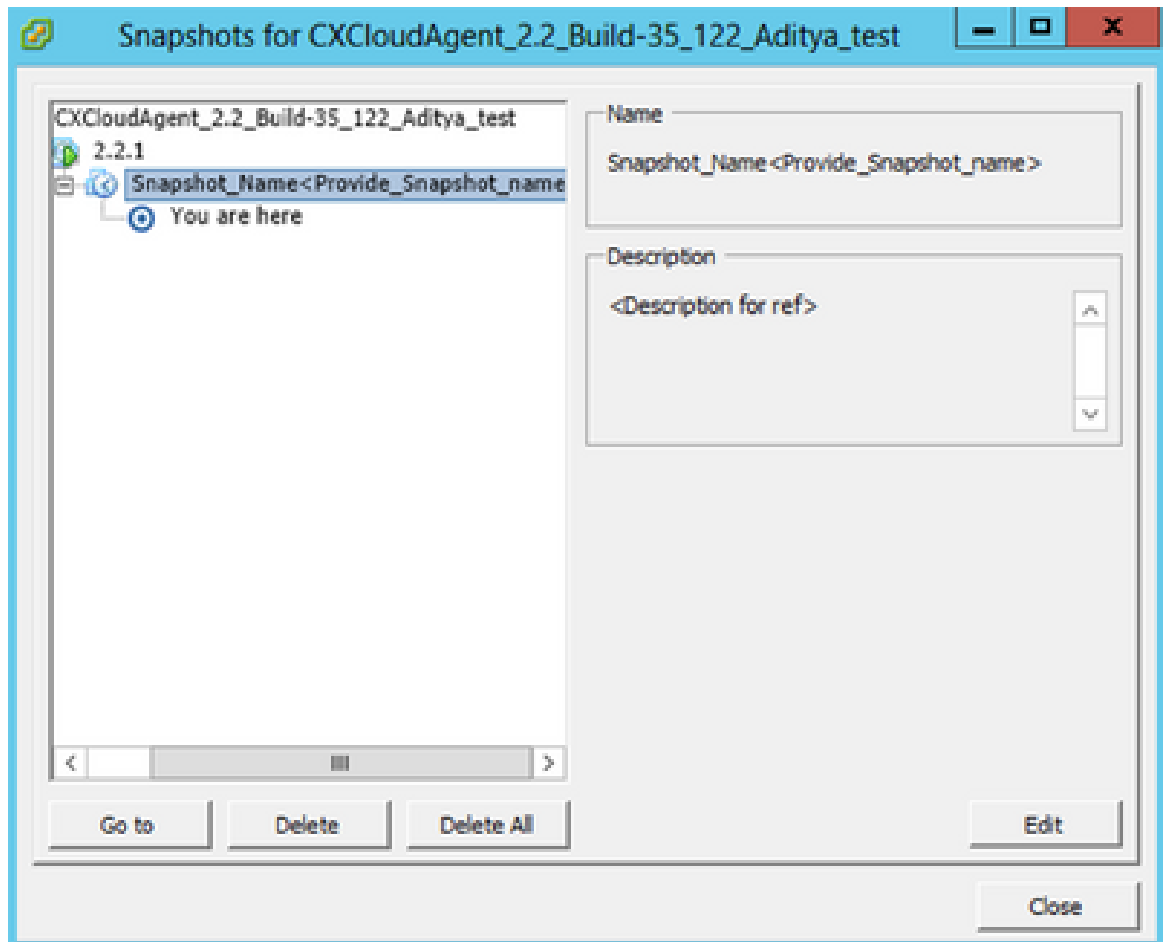
Restaurar

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.

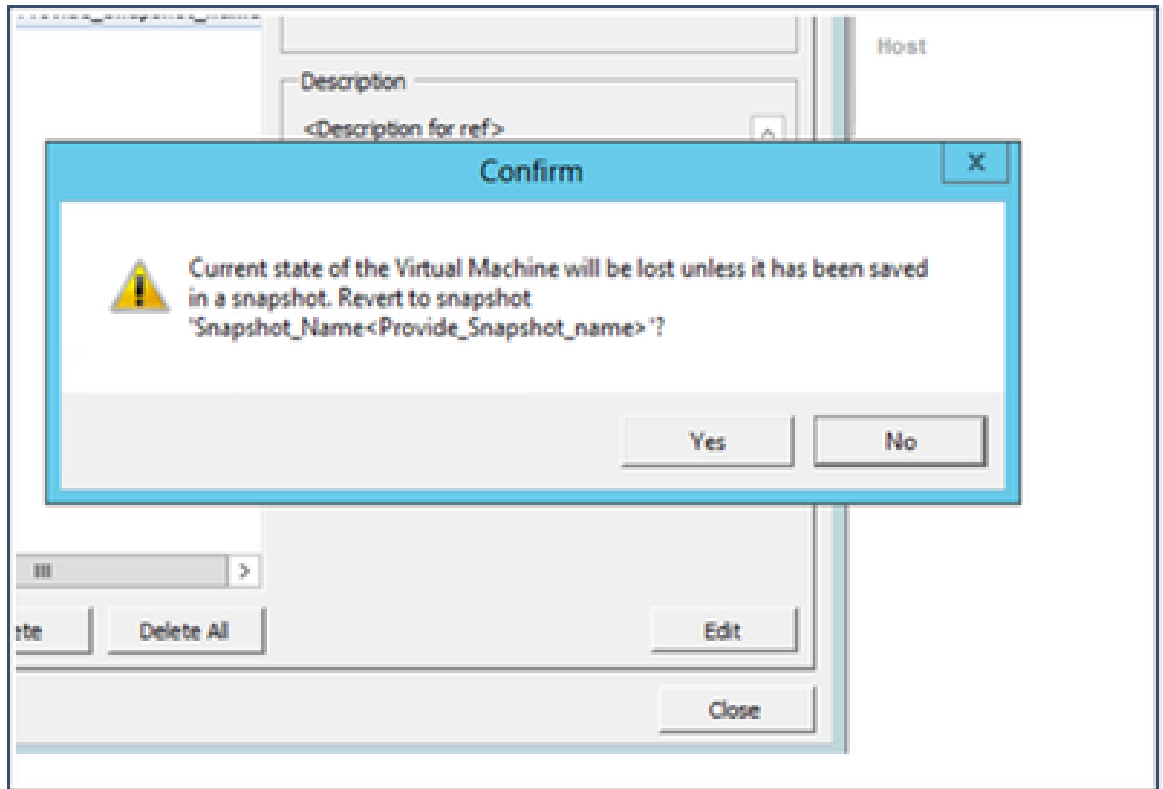


Janela Selecionar VM



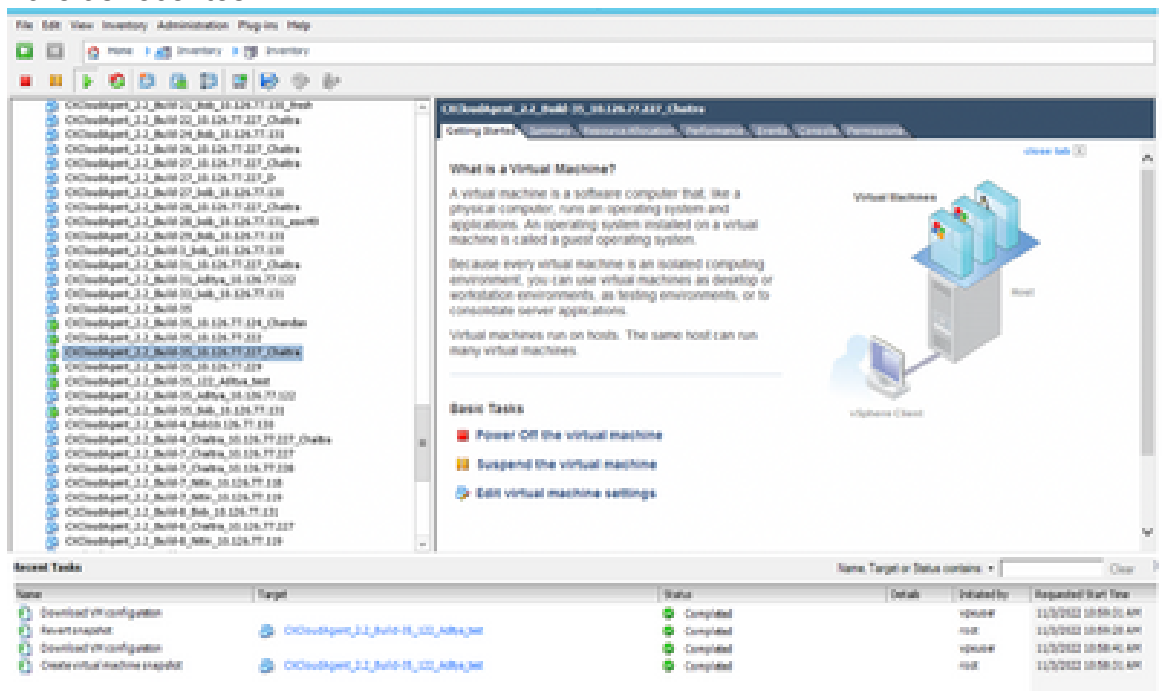
Janela Snapshots

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



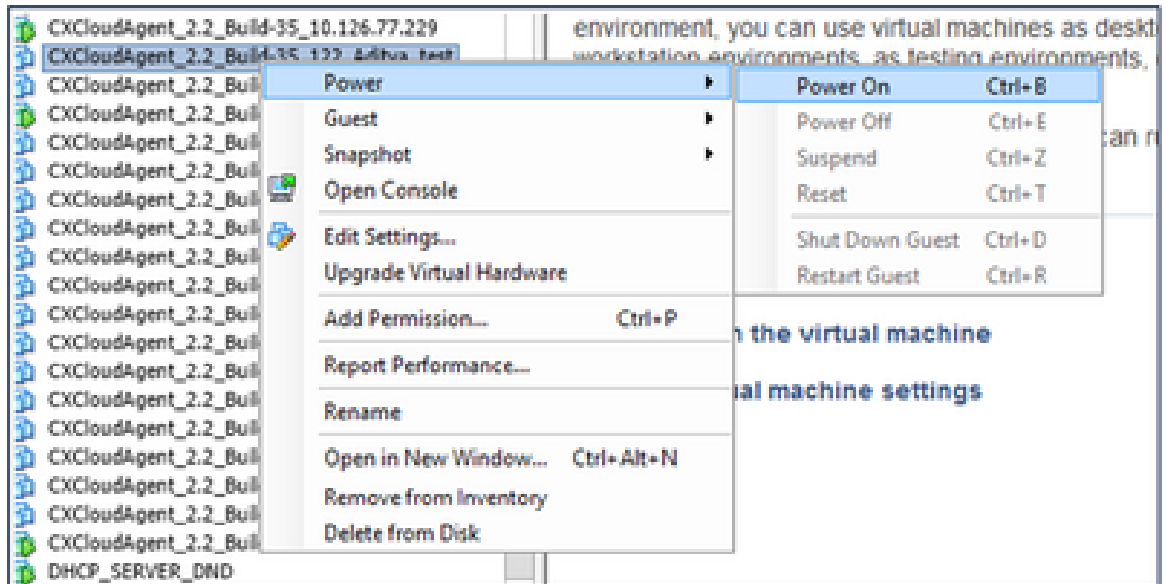
Confirmar janela

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 CX Cloud Agent garante ao cliente uma segurança completa. A conexão entre o CX Cloud e o CX Cloud 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 Cloud Agent em uma empresa de servidores VMware segura. O OVA é compartilhado de forma segura pelo Cisco Software Download Center. A senha do bootloader (modo de usuário individual) é definida com uma senha aleatoriamente exclusiva. Os usuários devem consultar 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 user/credentials são usados para acessar as APIs do CX Cloud Agent e para se conectar ao dispositivo por SSH.

os usuários cxcadmin têm acesso restrito com os privilégios mínimos. A senha de 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 raiz.

Segurança de rede

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

Autenticação

Autenticação baseada em senha: o dispositivo mantém um único usuário (cxcadmin) que permite que o usuário autentique e se comunique com o CX Cloud Agent.

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

os usuários cxcadmin podem criar o usuário cxcroot usando um utilitário chamado remoteaccount. Este utilitário exibe uma senha criptografada RSA/ECB/PKCS1v1_5 que pode ser descriptografada somente no portal SWIM ([DECRYPT Request Form](#)). Somente pessoal autorizado tem acesso a este portal. usuários cxcroot podem obter privilégios de root usando esta senha descriptografada. A senha é válida somente por dois dias. Os usuários cxcadmin devem recriar a conta e obter a senha do portal SWIM após a expiração da senha.

Blindagem

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

Segurança de dados

O dispositivo do CX Cloud Agent não armazena as 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 DNA Center, Diagnostic Bridge, Intersight, Compliance Insights, Falhas e todas as outras fontes de telemetria coletadas pelo CX Cloud Agent.

As informações confidenciais na telemetria de ativos são mascaradas antes de serem transmitidas para a nuvem. O CX Cloud Agent mascara os dados confidenciais de todos os ativos coletados que enviam telemetria diretamente ao CX Cloud Agent. 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 CX Cloud Agent. 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 [Dados Anônimos](#) do Guia do Administrador do Cisco DNA 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 de telemetria do CX Cloud 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 CX Cloud Agent).

Resumo de segurança

Recursos de segurança	Descrição
Senha do bootloader	A senha do bootloader (modo de usuário individual) é definida com uma senha aleatoriamente exclusiva. Os usuários devem consultar as FAQ para definir sua senha do carregador de inicialização (modo de usuário único).
Acesso do usuário	SSH: <ul style="list-style-type: none"> · O acesso ao dispositivo usando o usuário de cxcadmin exige as credenciais criadas durante a instalação. · O acesso ao dispositivo usando o usuário cxcroot requer que as credenciais sejam descritografadas usando o portal SWIM por pessoal autorizado.
Contas do usuário	<ul style="list-style-type: none"> · cxcadmin: conta de usuário padrão criada; o usuário pode executar comandos do aplicativo CX Cloud Agent usando cxcli e tem menos privilégios no dispositivo; o usuário cxcroot e sua senha criptografada são gerados usando o usuário cxcadmin. · cxcroot: cxcadmin pode criar este usuário usando o utilitário remoteaccount; O usuário pode obter privilégios de raiz com esta conta.
Política de senha de cxcadmin	· A senha é um hash unidirecional que usa o SHA-256 e é armazenada com segurança.

	<ul style="list-style-type: none"> · Mínimo de oito (8) caracteres, contendo três destas categorias: maiúsculas, minúsculas, números e caracteres especiais.
Política de senha de cxcroot	<ul style="list-style-type: none"> · A senha de cxcroot é criptografada por RSA/ECB/PKCS1v1_5 · A frase secreta gerada precisa ser descriptografada no portal do SWIM. · O usuário e a senha do cxcroot são válidos por dois dias e podem ser regenerados usando o usuário cxcadmin.
Política de senha de login de ssh	<ul style="list-style-type: none"> · Mínimo de oito caracteres que contêm três destas categorias: maiúsculas, minúsculas, números e caracteres especiais. · Cinco tentativas de login com falha bloqueiam a caixa por 30 minutos; a senha expira em 90 dias.
Portas	Portas de entrada abertas – 514 (Syslog) e 22 (ssh)
Segurança de dados	<ul style="list-style-type: none"> · Não há informações de cliente armazenadas. · Não há dados de dispositivo armazenados. · Credenciais do servidor Cisco DNA Center criptografadas e armazenadas no banco de dados.

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.