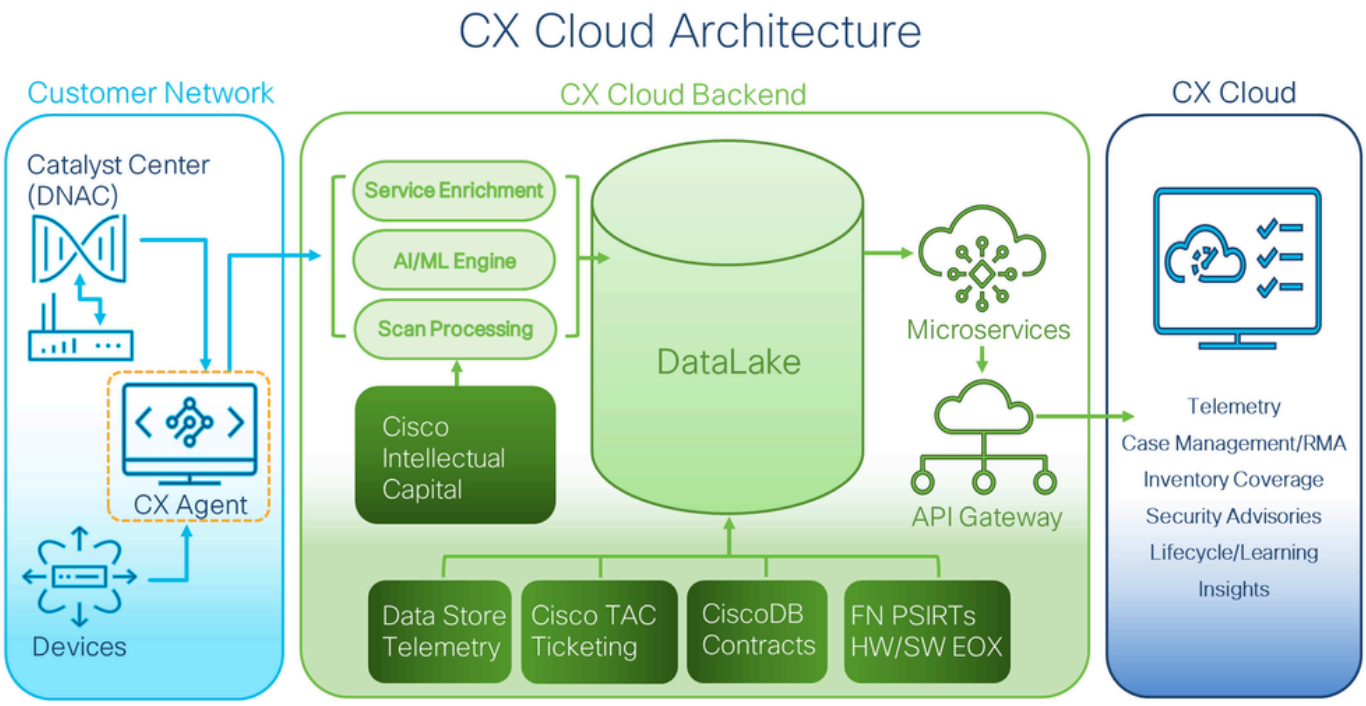
Visão geral do CX Cloud Agent v2.2

Contents

Introdução

Este documento descreve o Cisco Customer Experience (CX) Cloud Agent. O Cisco Cloud Agent (CX) 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.

Este guia é específico do CX Cloud Agent v2.2 e posteriores. Consulte a página Cisco CX Cloud Agent para acessar versões anteriores.



Arquitetura de nuvem CX

Observação: as imagens (e o conteúdo contido neste guia) são apenas para fins de 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 para implantar:

- Qualquer um destes hipervisores:
  - VMware ESXi versão 5.5 ou posterior
  - Oracle Virtual Box 5.2.30 ou posterior
  - Hipervisor Windows versão 2012 a 2022
- O hipervisor pode hospedar uma VM que requer:
  - CPU de 8 núcleos
  - 16 GB de memória/RAM
  - 200 GB de espaço em disco
- Para clientes que usam data centers designados 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.csco.cloud
  - FQDN: ng.acs.agent.us.csco.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.csco.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.csco.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.csco.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:

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

Outras observações:

- 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) e do Cisco DNA Center são 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.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 devem ser usados

Acesso a domínios essenciais

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

Domínios específicos do portal do CX Cloud Agent

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

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

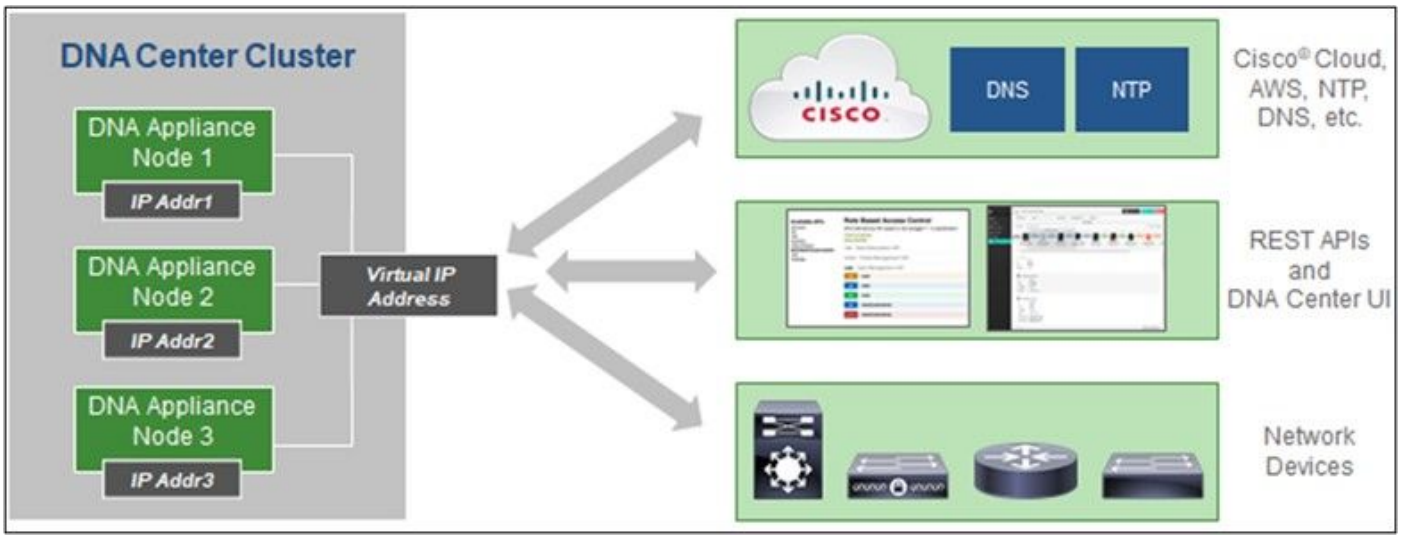
Domínios específicos do CX Cloud Agent OVA

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.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.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 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

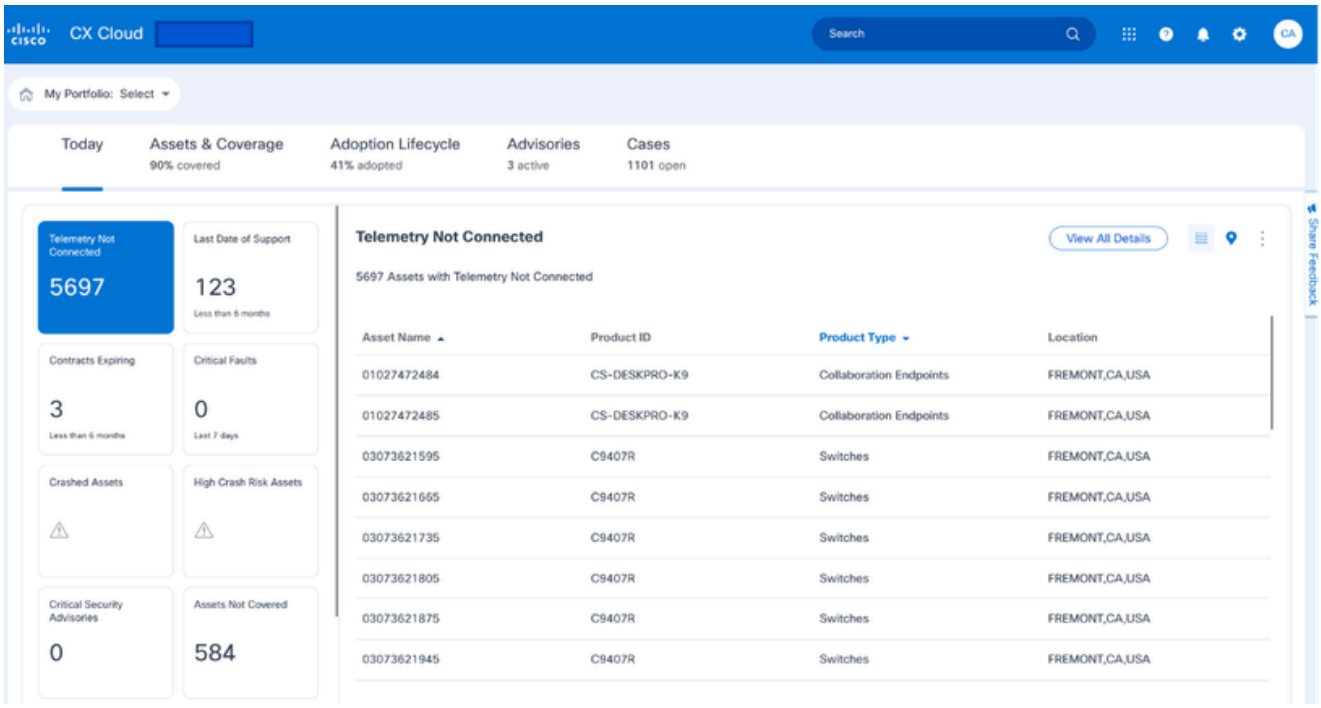
Lista de produtos suportados

Para visualizar a lista de produtos suportados pelo CX Cloud Agent, consulte a Lista de produtos suportados.

Conexão de Origens de Dados

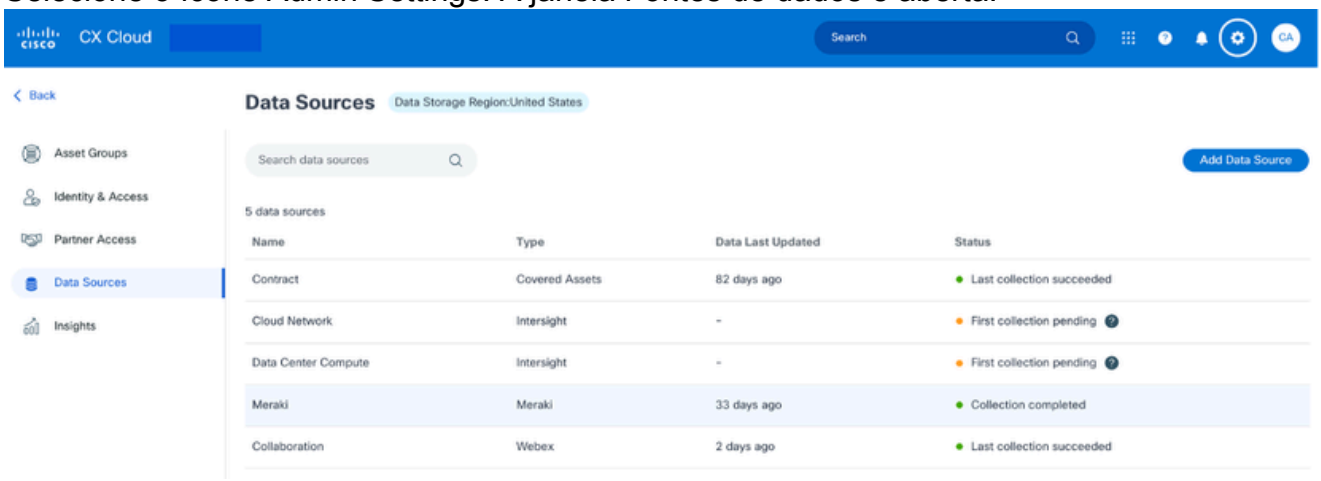
Para conectar origens de dados:

1. Clique em cx.cisco.com para fazer login na CX Cloud.



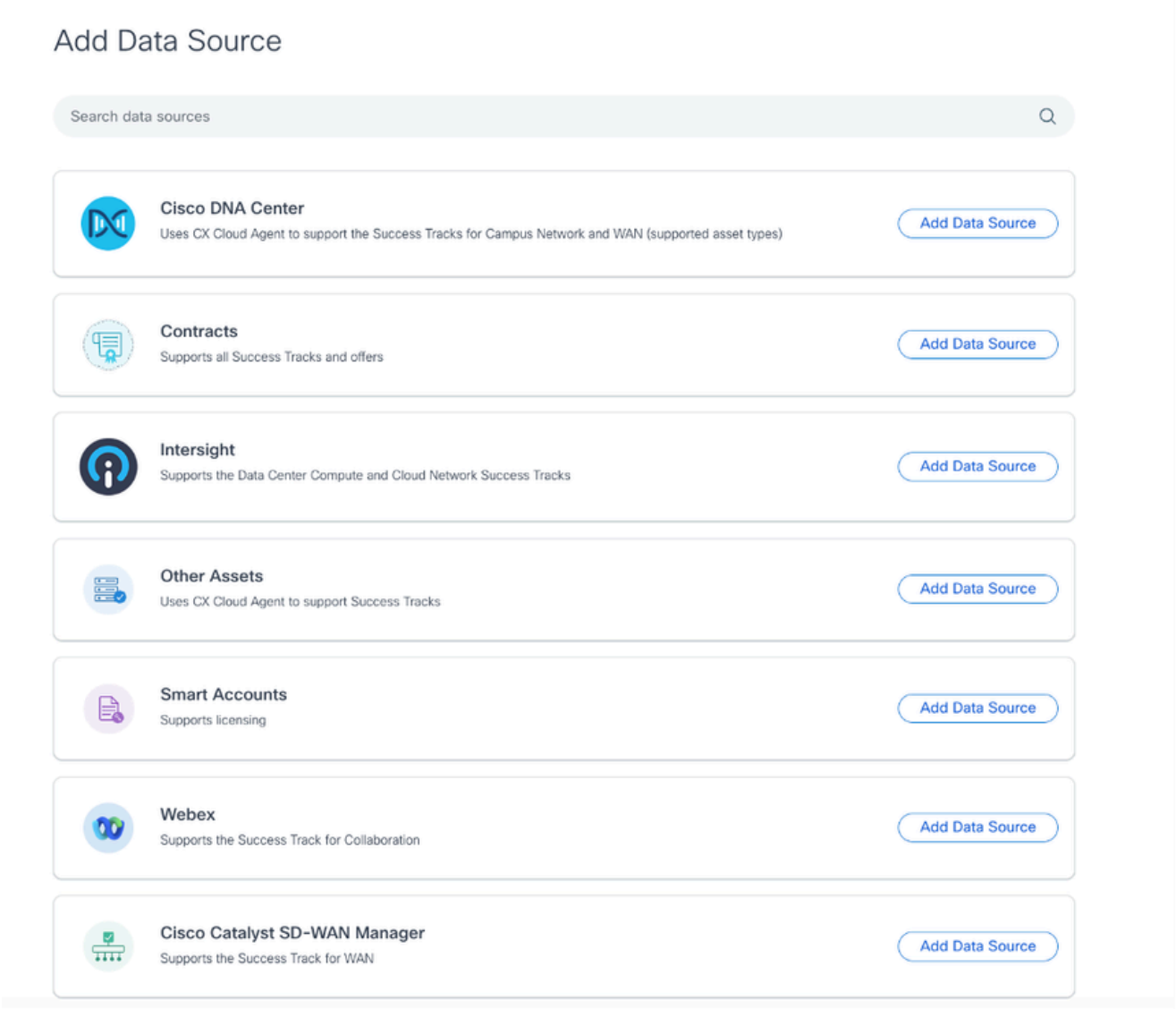
Página inicial do CX Cloud

2. Selecione o ícone Admin Settings. 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 podem variar com base nas assinaturas do cliente.



Adicionar Fonte de Dados

4. Clique em Adicionar fonte de dados para selecionar a fonte de dados aplicável. Se o CX Cloud Agent não tiver sido configurado anteriormente, a janela Setting Up CX Cloud Agent será aberta, onde a configuração deverá ser concluída. Se a configuração estiver concluída, a conexão continuará. Consulte uma das seguintes seções para continuar:

Configurando o CX Cloud Agent

Adicionando o Cisco DNA Center como fonte de dados

Adição de Outros Ativos como Origens de Dados

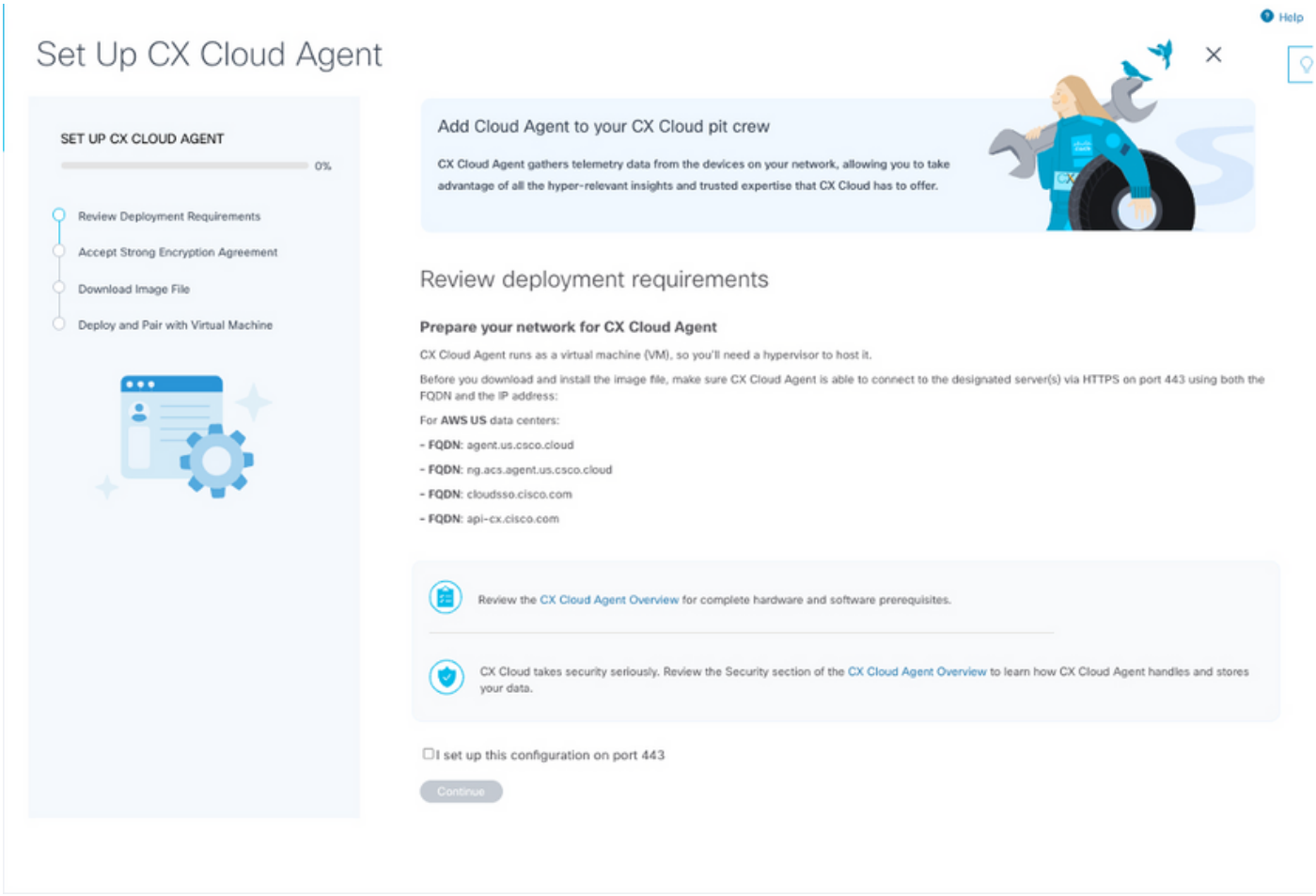
Observação: a opção Outros ativos só estará disponível se a conectividade de dispositivo direto não tiver sido configurada anteriormente.

Configurando o CX Cloud Agent

A configuração do CX Cloud Agent é solicitada durante a conexão de fontes de dados, caso ainda

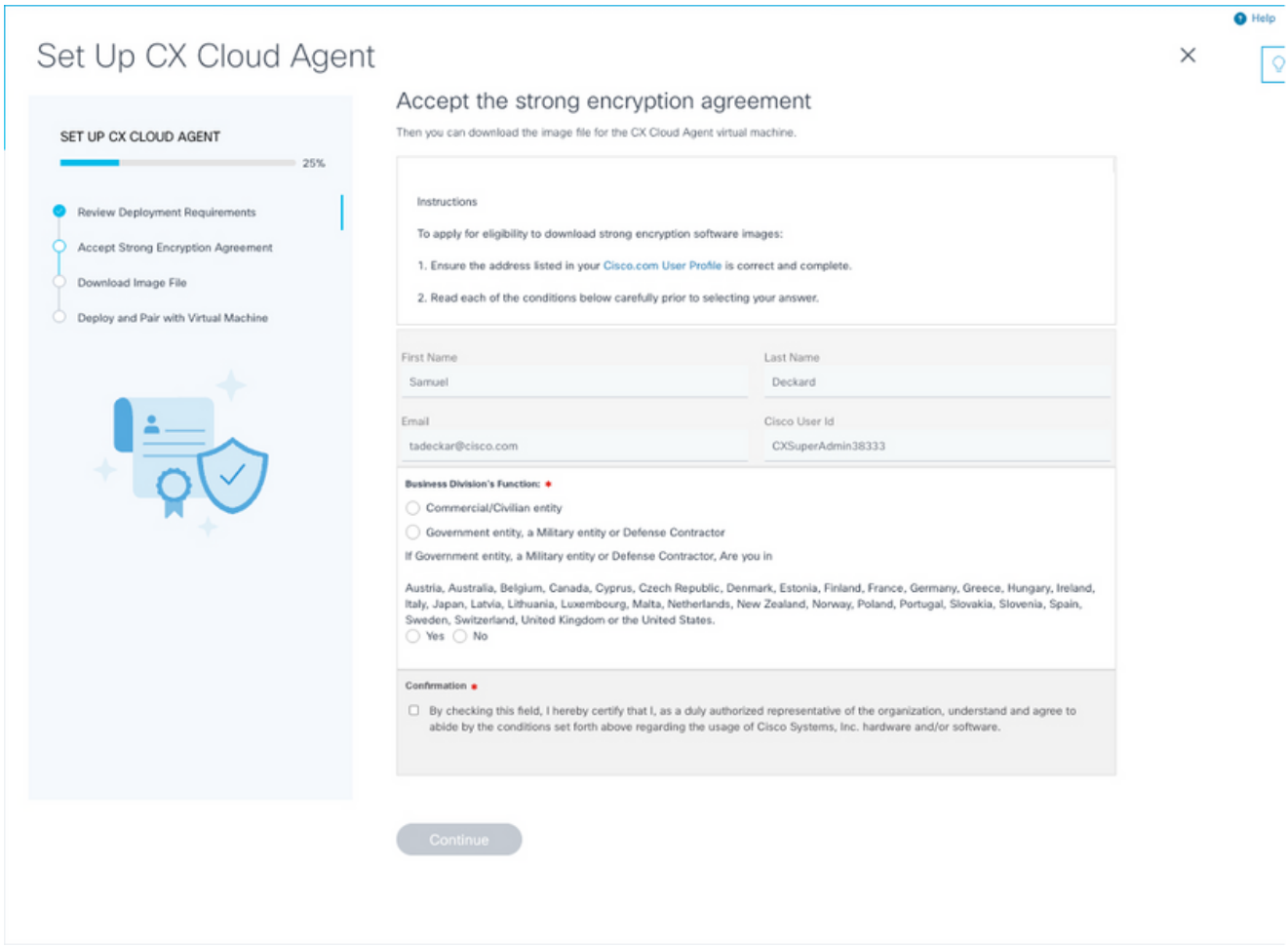
não tenha sido concluída.

Para configurar o CX Cloud Agent:



Analisar os requisitos de implantação

1. Revise a caixa de seleção Review deployment requirements e marque a caixa de seleção I set up this configuration on port 443.
2. Clique em Continuar. A janela Set Up CX Cloud Agent - Accept the strong encryption agreement será aberta.



Contrato de criptografia

3. Verifique as informações pré-preenchidas nos campos Nome, Sobrenome, E-mail e ID de usuário da Cisco.
4. Selecione a Função da Divisão Comercial apropriada.
5. Marque a caixa de seleção Confirmação para concordar com as condições de uso.
6. Clique em Continuar. A janela Set Up CX Cloud Agent - Download image file é exibida.

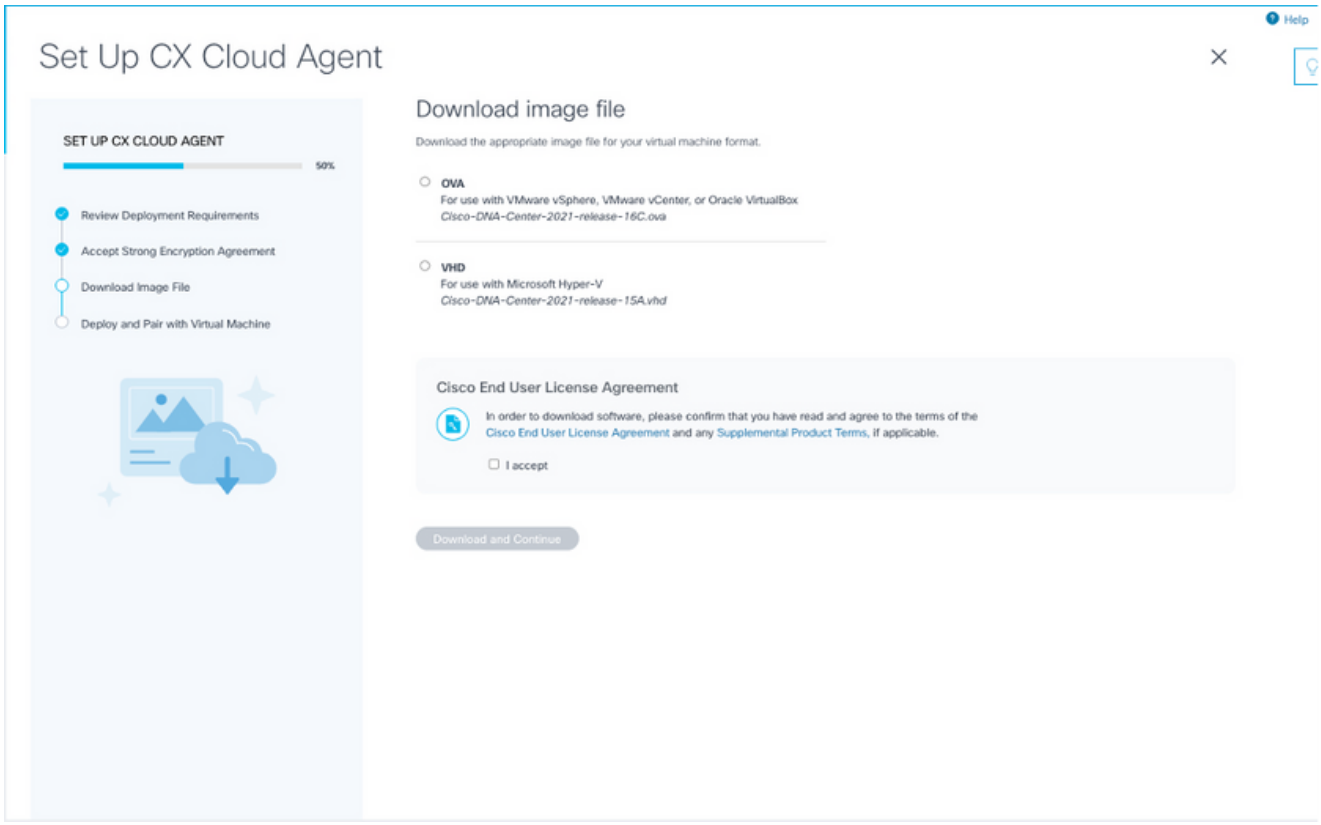


Imagem do download

7. Selecione o formato de arquivo apropriado para fazer o download do arquivo de imagem necessário para a instalação.
8. Marque a caixa de seleção Aceito para concordar com o Contrato de licença de usuário final da Cisco.
9. Clique em Download and Continue. A janela Configurar CX Cloud Agent - Implantar e emparelhar com sua máquina virtual se abre.
10. Consulte Configuração de Rede para obter o código de emparelhamento necessário na próxima seção.

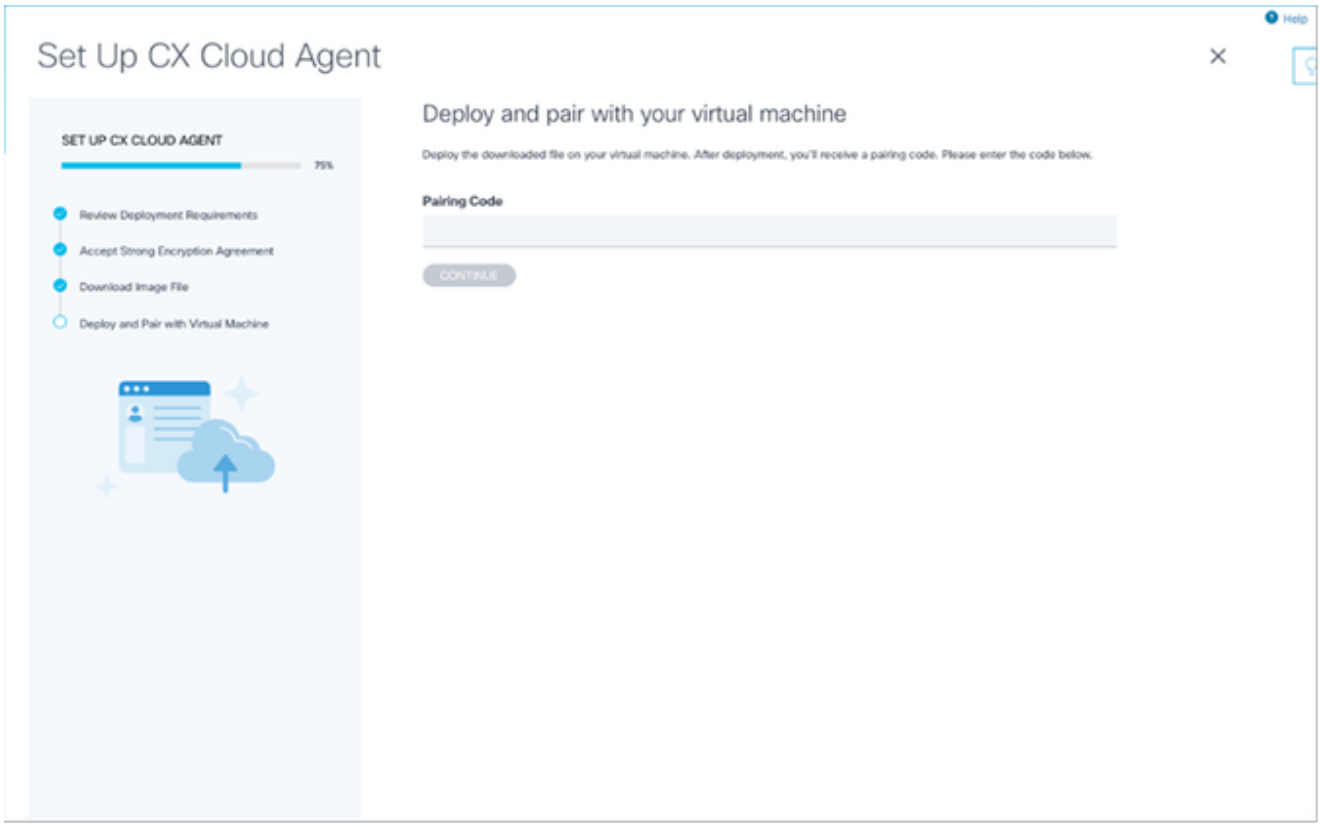
Conexão do CX Cloud Agent com a CX Cloud

É necessário conectar o CX Cloud Agent ao CX Cloud para iniciar a coleta de telemetria, de modo que as informações na interface do usuário possam ser atualizadas para exibir os ativos e as informações atuais. Esta seção fornece detalhes para concluir as diretrizes de conexão e solução de problemas.

Para conectar o CX Cloud Agent ao CX Cloud:

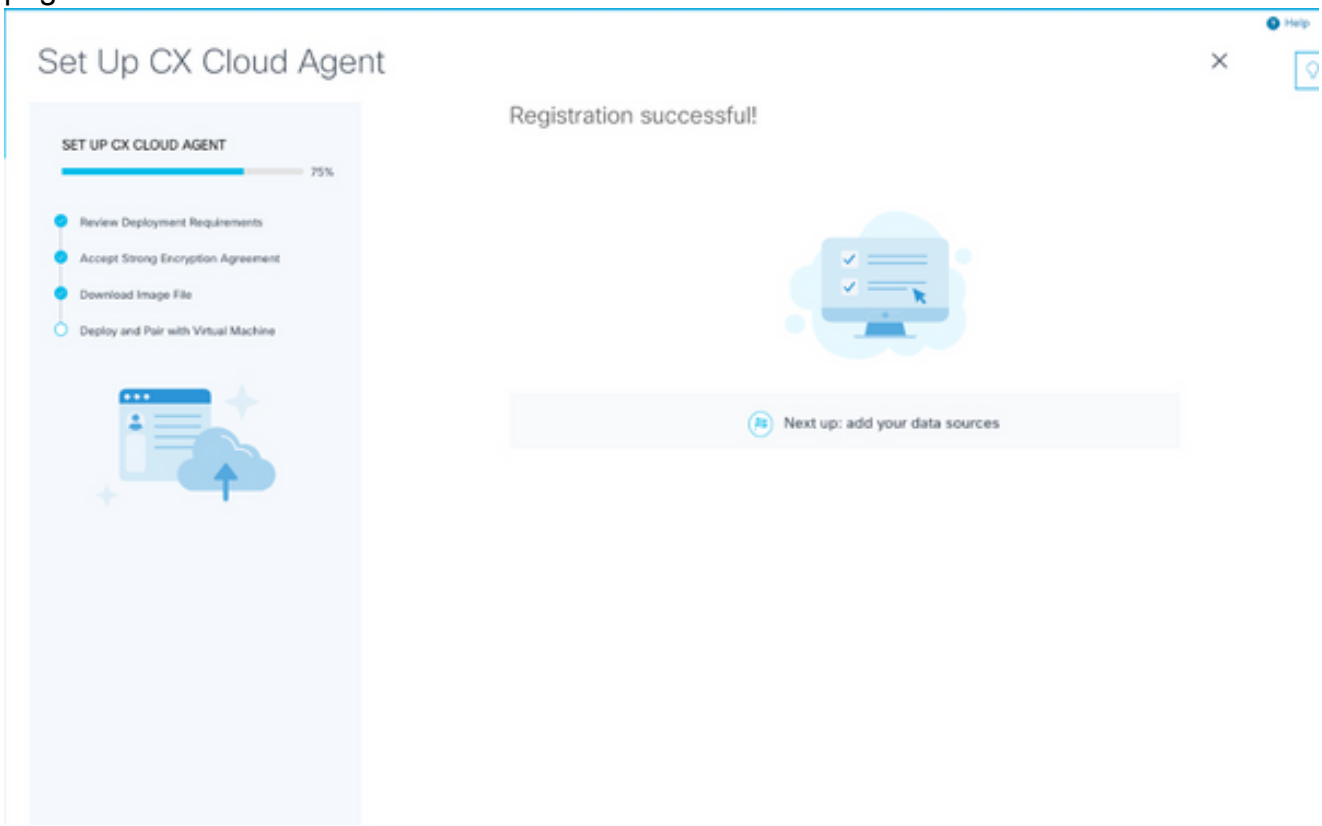
1. Insira o código de emparelhamento fornecido na caixa de diálogo do console ou na interface de linha de comando (CLI) da máquina virtual conectada via agente.

> Observação: o código de emparelhamento é recebido após a implantação do arquivo OVA baixado.



Código de emparelhamento

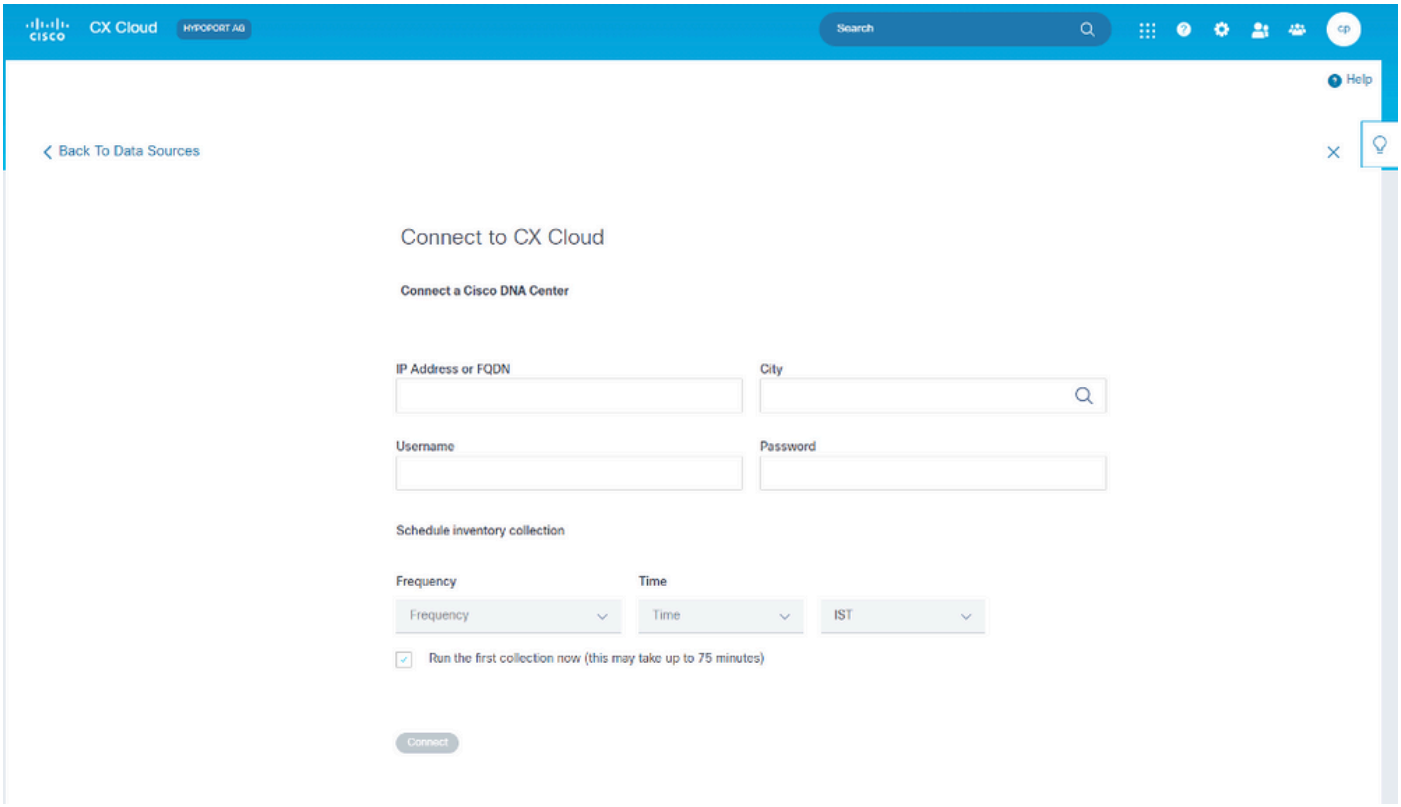
2. Clique em Continuar para registrar o CX Cloud Agent. A janela Set Up CX Cloud Agent - Registration successful é aberta rapidamente antes de navegar automaticamente para a página Add Data Sources.



Registro realizado com sucesso

Adicionando o Cisco DNA Center como uma fonte de dados

Quando o Cisco DNA Center é selecionado na janela de conexão de fontes de dados (consulte a imagem Conectar fontes de dados na seção Conectando fontes de dados), a seguinte janela é aberta:



Conectar-se à nuvem CX

Para adicionar o Cisco DNA Center como fonte de dados:

1. Insira o endereço IP do Cisco DNA Center ou o endereço IP virtual ou FQDN, Cidade (local do Cisco DNA Center), Nome de usuário e Senha.

   Observação: não use um IP de nó de cluster individual.

2. Programe uma coleta de inventário inserindo uma Frequência e Hora para indicar com que frequência o CX Cloud Agent deve executar verificações de rede e atualizar informações em dispositivos conectados.

   Observação: a primeira coleta de inventário pode levar até 75 minutos.

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

Conectado com êxito

4. Clique em Add Another Cisco DNA Center, Done ou Back to Data Sources para voltar à janela Data Sources.

Adição de Outros Ativos como Origens de Dados

Overview

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 também podem conectar o CX Cloud Agent diretamente a outros ativos de hardware em seu ambiente, até 10.000 dispositivos diretamente conectados.

Os usuários podem identificar os dispositivos a serem incorporados na nuvem CX identificando exclusivamente esses dispositivos usando um arquivo de seed ou especificando um intervalo de IP, que deve ser examinado pelo 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.

Note:
O arquivo de seed ou o intervalo de IPs pode ser usado. Não é possível alterar esta seleção após a configuração inicial.

Note:

Um arquivo de seed inicial pode ser substituído por outro arquivo de seed enquanto um intervalo de IP inicial pode ser editado para um novo intervalo de IPs.

Quando Outros Ativos é selecionado na janela de conexão de origens de dados, a seguinte janela é aberta:

Configurar a conexão com a nuvem CX

Para adicionar outros ativos como origens de dados:

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

Protocolos de descoberta

A detecção direta de dispositivos baseada em arquivos de seed e a detecção baseada em intervalo de IPs dependem do SNMP como o protocolo de detecção. Existem versões diferentes de SNMP, mas o CX Cloud Agent oferece suporte a SNMPV2c e SNMP V3 e uma ou ambas as versões podem ser configuradas. As mesmas informações, descritas abaixo em detalhes completos, devem ser fornecidas pelo usuário para concluir a configuração e permitir a conectividade entre o dispositivo gerenciado por SNMP e o gerenciador de serviços SNMP.

O SNMPV2c e o SNMPV3 diferem em termos de segurança e modelo de configuração remota. O SNMPV3 usa um sistema avançado de segurança criptográfica que suporta criptografia SHA para autenticar mensagens e garantir sua privacidade. Recomenda-se que o SNMPv3 seja usado em todas as redes públicas e na Internet para proteger contra riscos e ameaças à segurança. Na nuvem CX, é preferível que o SNMPv3 seja configurado e não o SNMPv2c, exceto para dispositivos herdados mais antigos que não têm suporte integrado para o SNMPv3. Se ambas as versões do SNMP forem configuradas pelo usuário, o CX Cloud Agent tentará, por padrão, se comunicar com cada dispositivo respectivo usando SNMPv3 e reverterá 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 deve ser usado, exceto nos casos de ativos legados individuais que não têm o suporte interno apropriado. Esteja ciente de que o protocolo SSHv1 contém vulnerabilidades fundamentais. 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.

Adicionar dispositivos usando um arquivo de propagação

Sobre o arquivo de propagação

Um arquivo de seed é um arquivo de valores separados por vírgula (csv) em que cada linha representa um registro de dados do sistema. Em um arquivo de seed, cada registro de arquivo de seed corresponde a um dispositivo exclusivo do qual a telemetria deve ser coletada pelo CX 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 tentará se conectar aos dispositivos, mas talvez não consiga processar cada um deles para exibição nas páginas Ativos nos casos em que não seja 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.

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

Coluna do arquivo de propagação	Cabeçalho/Identificador de Coluna	Finalidade da Coluna
R	Endereço IP ou nome de 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 Autenticação segura, o respectivo Algoritmo de autenticação deverá ser fornecido. Nota: MD5 é considerado inseguro e SHA deve ser usado em todos os dispositivos que o suportam.
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.

Coluna do arquivo de propagação	Cabeçalho/Identificador de Coluna	Finalidade da Coluna
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. Nota: As chaves de 56 bits usadas pelo DES são consideradas muito curtas para fornecer segurança criptográfica e que o 3DES deve ser usado em todos os dispositivos que o suportam.
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, será 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 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.

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

Limitações de Processamento de Telemetria para Dispositivos

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

- Alguns dispositivos podem ser exibidos como alcançáveis no Resumo da coleta, mas não são visíveis na página Ativos de nuvem do CX. As limitações de instrumentação de dispositivo impedem o processamento dessa telemetria de dispositivo.

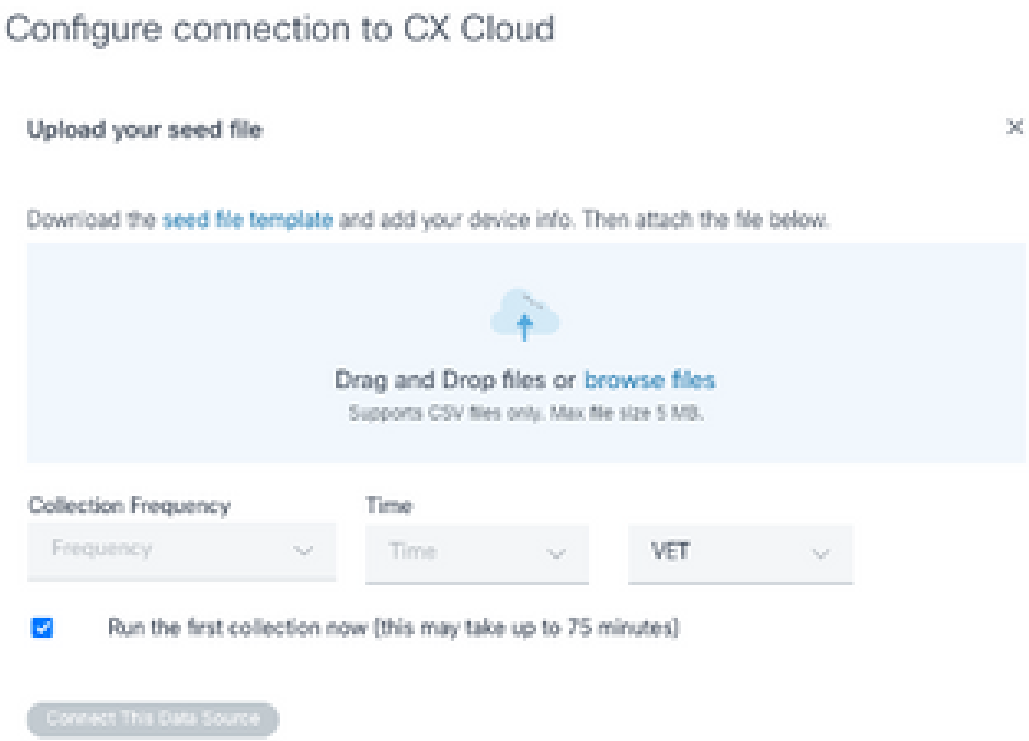
- Os atributos de telemetria podem estar imprecisos ou ausentes na página Ativos de nuvem do CX para dispositivos que não fazem parte do Caminho de sucesso do campus.
- Se um dispositivo do arquivo de seed ou das coleções de intervalos IP também fizer parte do inventário do Cisco DNA Center, o dispositivo será relatado apenas uma vez para a entrada do Cisco DNA Center. A entrada do intervalo de arquivos/ IP de seed não é coletada ou processada para evitar duplicação.

Adicionar dispositivos usando um novo arquivo de propagação

Para adicionar dispositivos usando um novo arquivo de seed:

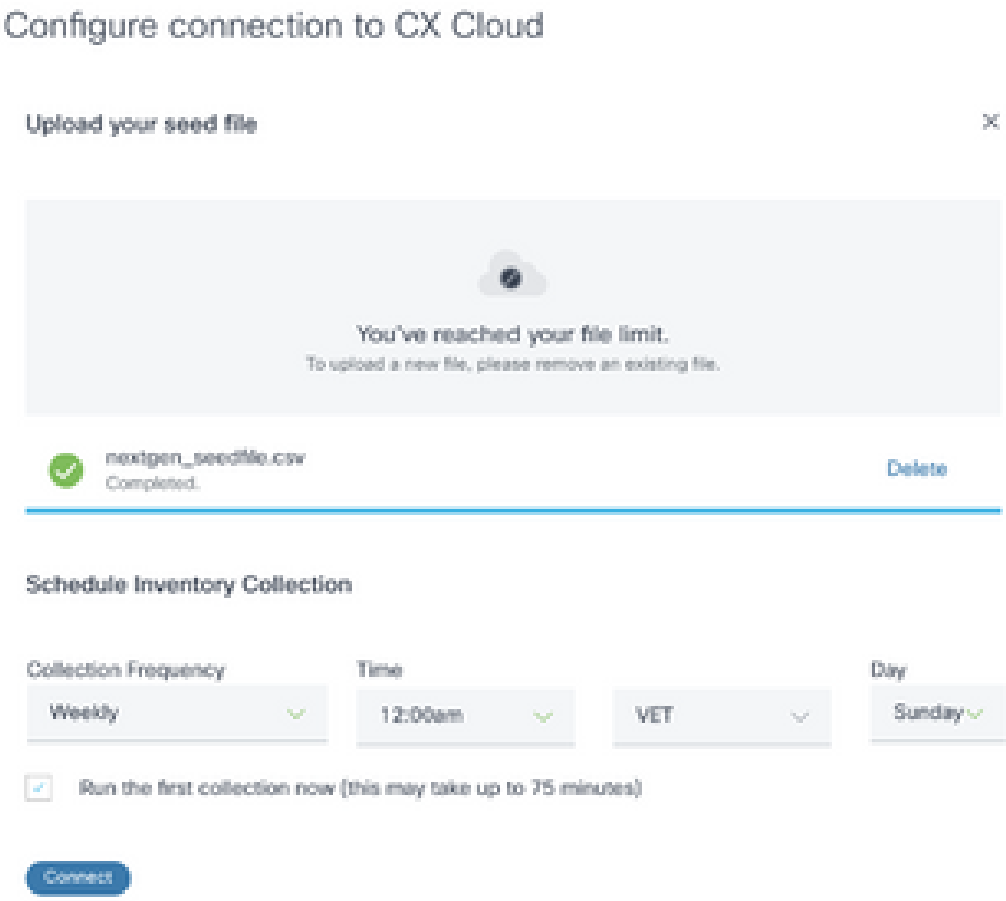
1. Faça o download do modelo de arquivo de seed (PDF) usando o link incorporado neste documento (consulte Sobre o arquivo de seed) ou por meio de um link na janela Configurar conexão com a nuvem CX.

Observação: o link na janela Configurar conexão com a nuvem CX não estará mais disponível depois que o arquivo de seed inicial for baixado.



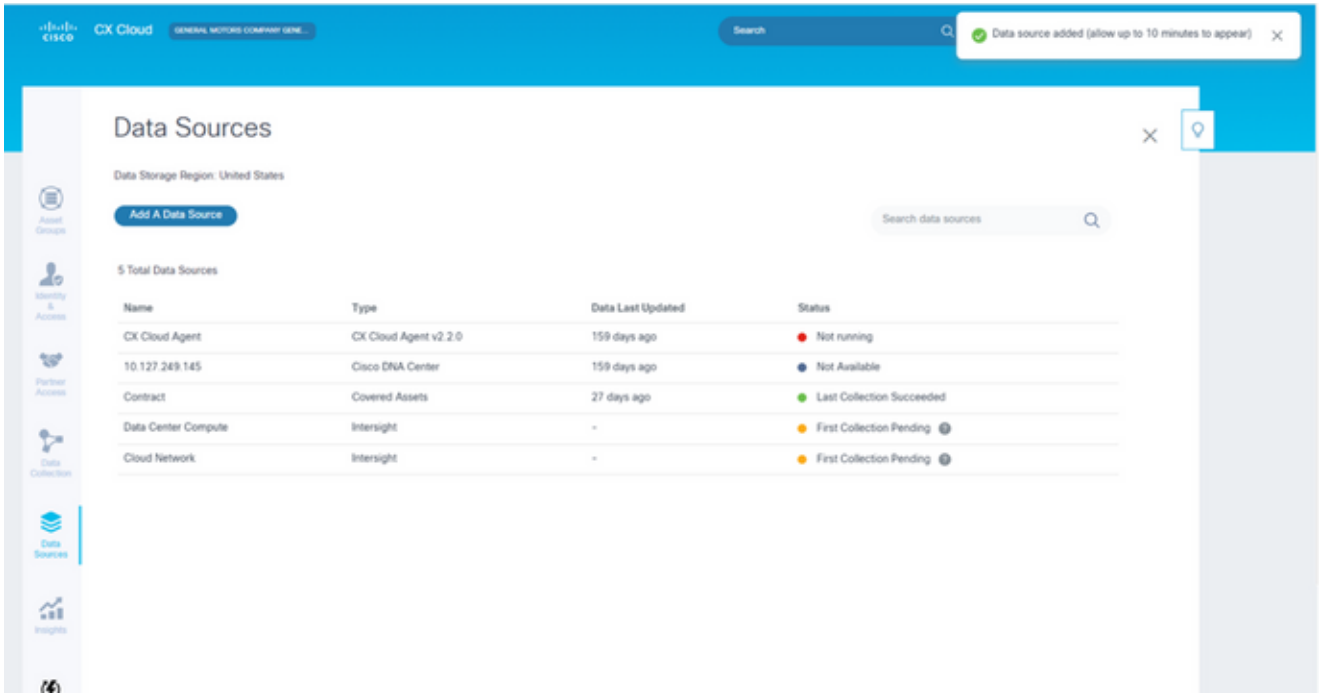
Janela Configurar conexão com a nuvem CX

2. Abra uma planilha do Excel (ou qualquer planilha preferencial) e insira os cabeçalhos conforme mostrado no modelo.
3. Insira os dados manualmente ou importe os dados para o arquivo.
4. Depois de concluir, salve o modelo como um arquivo .csv para importar o arquivo para o CX Cloud Agent.



Janela Carregar arquivo semente

5. Na janela Carregar seu arquivo semente, arraste e solte o arquivo .csv recém-criado ou clique em procurar arquivos e navegue até o arquivo .csv.
6. Preencha a seção Agendar coleta de inventário e clique em Conectar. A janela Fontes de dados é aberta, exibindo uma mensagem de confirmação.
7. Antes de concluir a configuração inicial do CX Cloud, o CX Cloud Agent deve realizar a primeira coleta de telemetria processando o arquivo de seed e estabelecendo conexão com todos os dispositivos identificados. A coleta pode ser iniciada sob demanda ou executada de acordo com uma programação definida aqui. Os usuários podem executar a primeira conexão de telemetria marcando a caixa de seleção Executar a primeira coleta agora. Dependendo do número de entradas especificadas no arquivo de seed e de outros fatores, este processo pode levar um tempo considerável.



Mensagem de confirmação

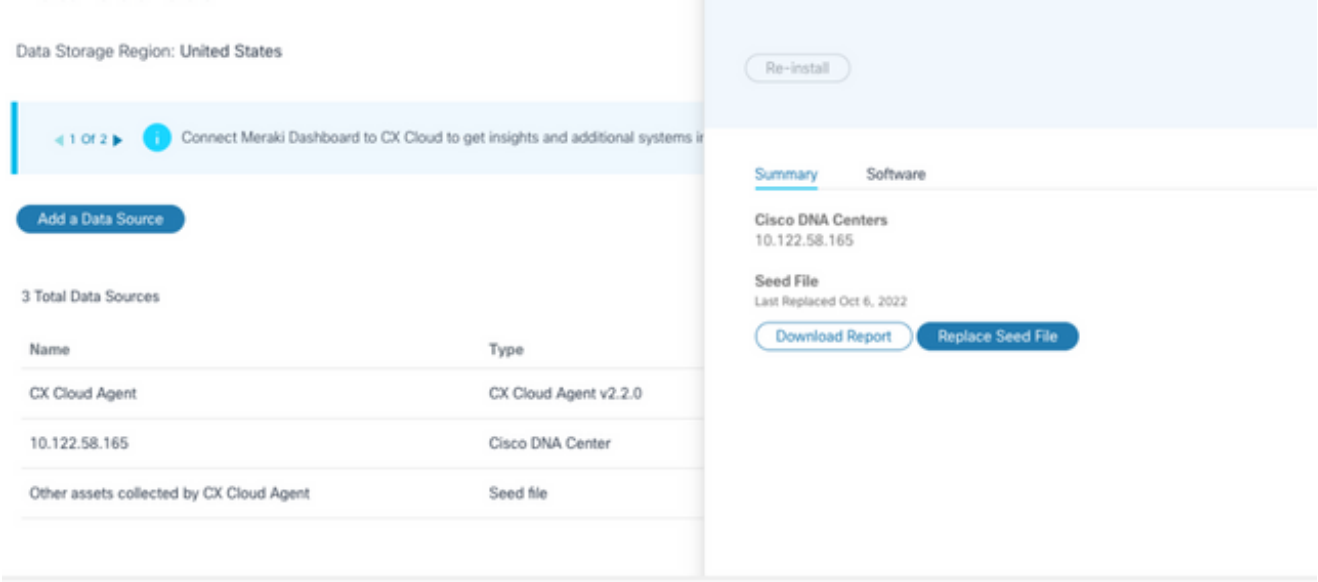
Adicionar dispositivos usando um arquivo de propagação modificado

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.

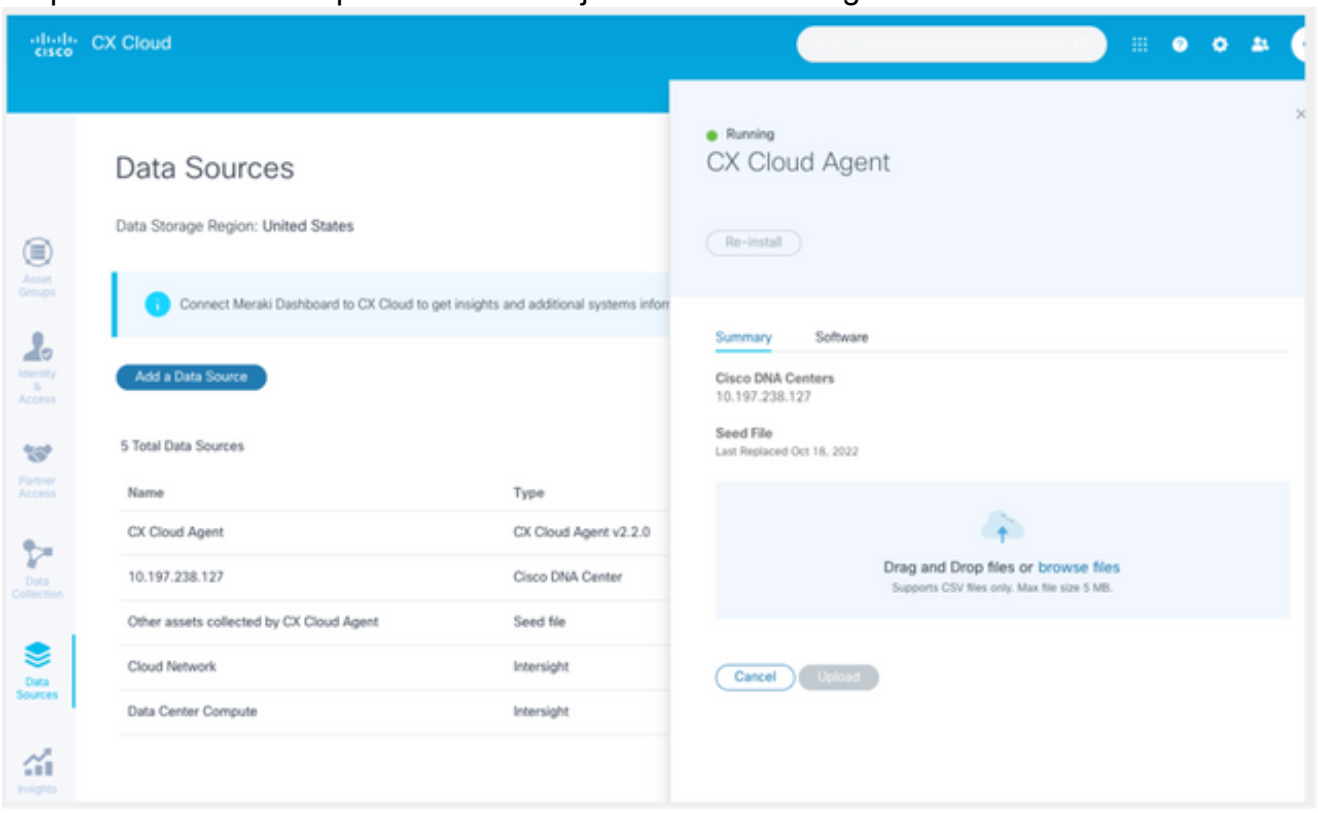
   Observação: para adicionar ativos ao arquivo seed, anexe esses ativos ao arquivo seed criado anteriormente e recarregue o arquivo. Isso é necessário já que o upload de um novo arquivo de seed substitui o arquivo de seed atual. Somente o último arquivo de propagação carregado é usado para descoberta e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

2. Na página Fontes de dados, selecione uma fonte de dados que tenha um Tipo de CX Cloud Agent. Uma janela de detalhes é aberta com as guias Resumo e Software.



Janela Detalhes

3. Clique em Download do relatório para gerar um relatório sobre todos os ativos da fonte de dados selecionada. O relatório fornece informações sobre o Endereço IP do dispositivo, Número de Série, Acessibilidade, Tipo de Comando, Status do Comando e Erro do Comando, se aplicável.
4. Clique em Substituir arquivo semente. A janela CX Cloud Agent é aberta.



Janela do CX Cloud Agent

5. Arraste e solte o arquivo semente modificado na janela ou navegue até o arquivo e adicione-o à janela.
6. Clique em Fazer upload.

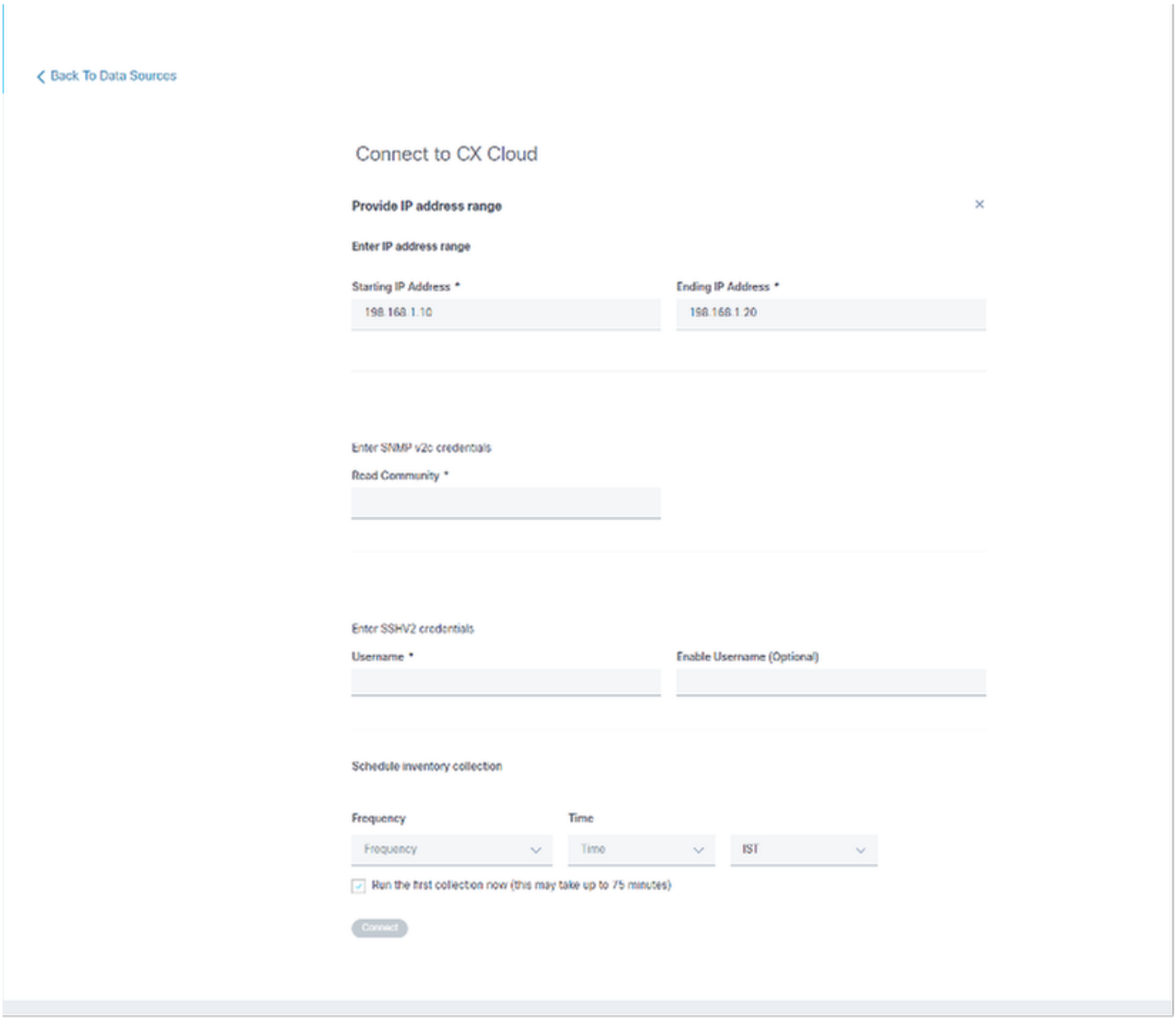
Adicionar dispositivos usando intervalos de IP

Os intervalos de IP permitem que os usuários identifiquem ativos de hardware e, subsequentemente, coletem telemetria desses dispositivos com base em endereços IP. Os dispositivos para coleta de telemetria podem ser identificados exclusivamente especificando-se um único intervalo de IP de nível de rede, que deve 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 devem 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 não será capaz de processar cada um para mostrar na visualização Ativos nos casos em que não for possível 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.



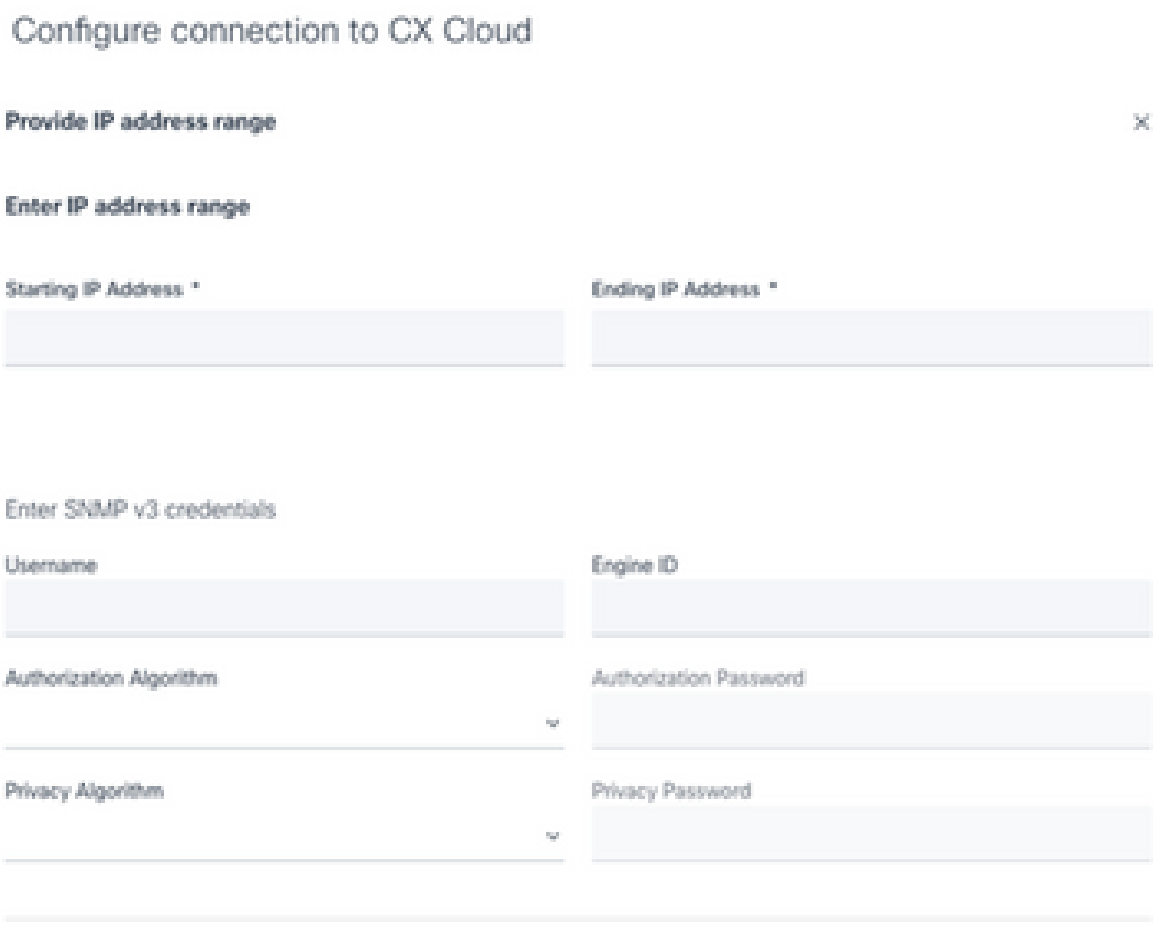
Janela do intervalo de endereços IP iniciais

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.

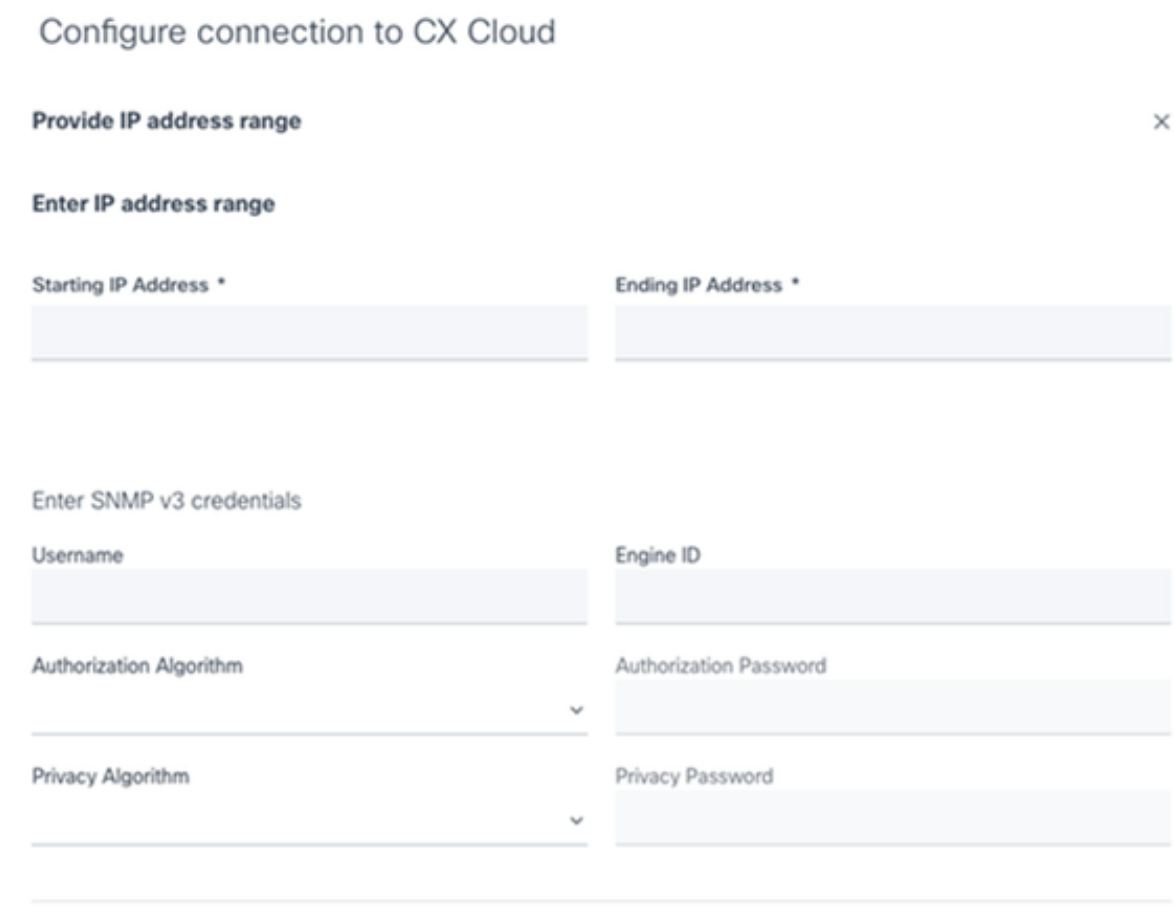
Para adicionar dispositivos usando o intervalo IP:

1. Na janela Configure connection to CX Cloud, selecione a opção Provide an IP Address range.

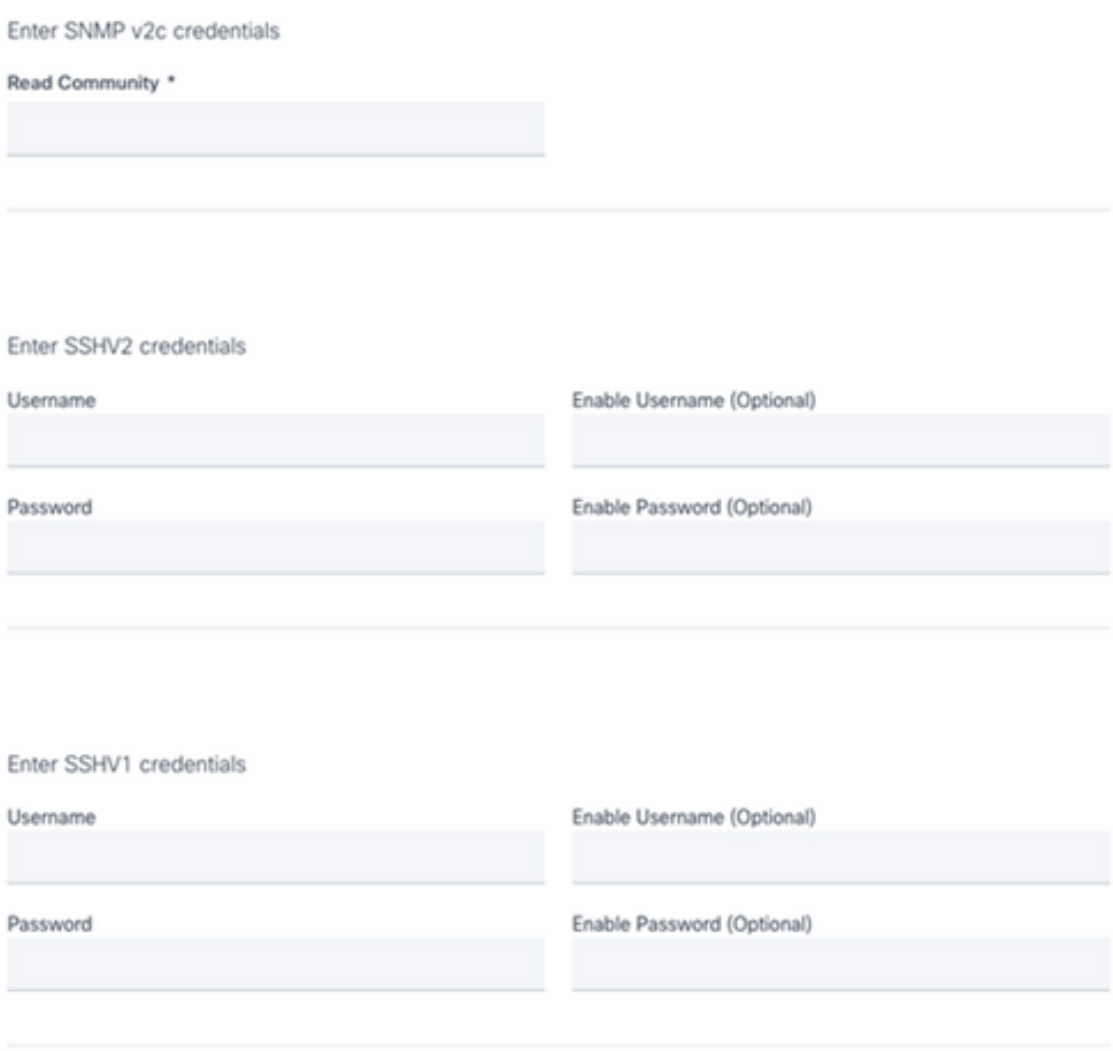


Adicionar dispositivos usando o formulário de endereços IP

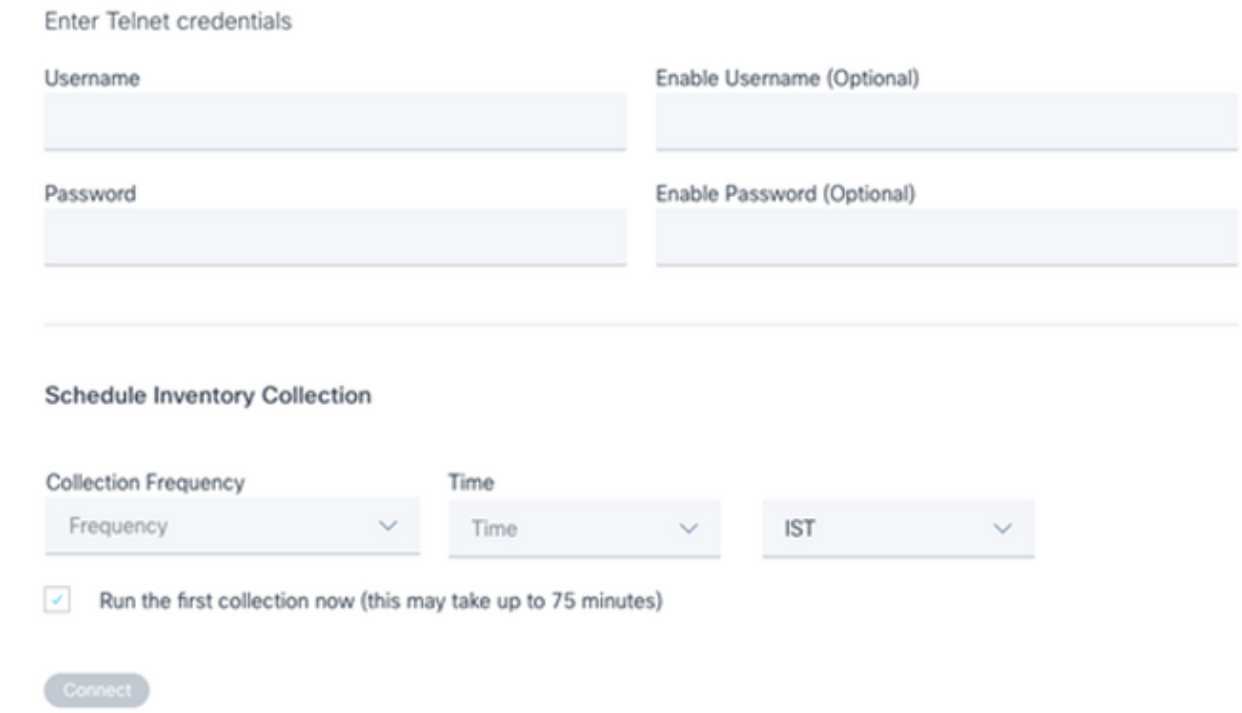
2. Preencha o formulário com as informações relevantes.
3. Várias opções de conexão podem ser selecionadas. As telas a seguir exibem as credenciais de configuração das opções. Consulte Sobre o arquivo de seed para obter uma descrição dos campos de credencial para cada opção de conexão.



Credenciais SNMP v3

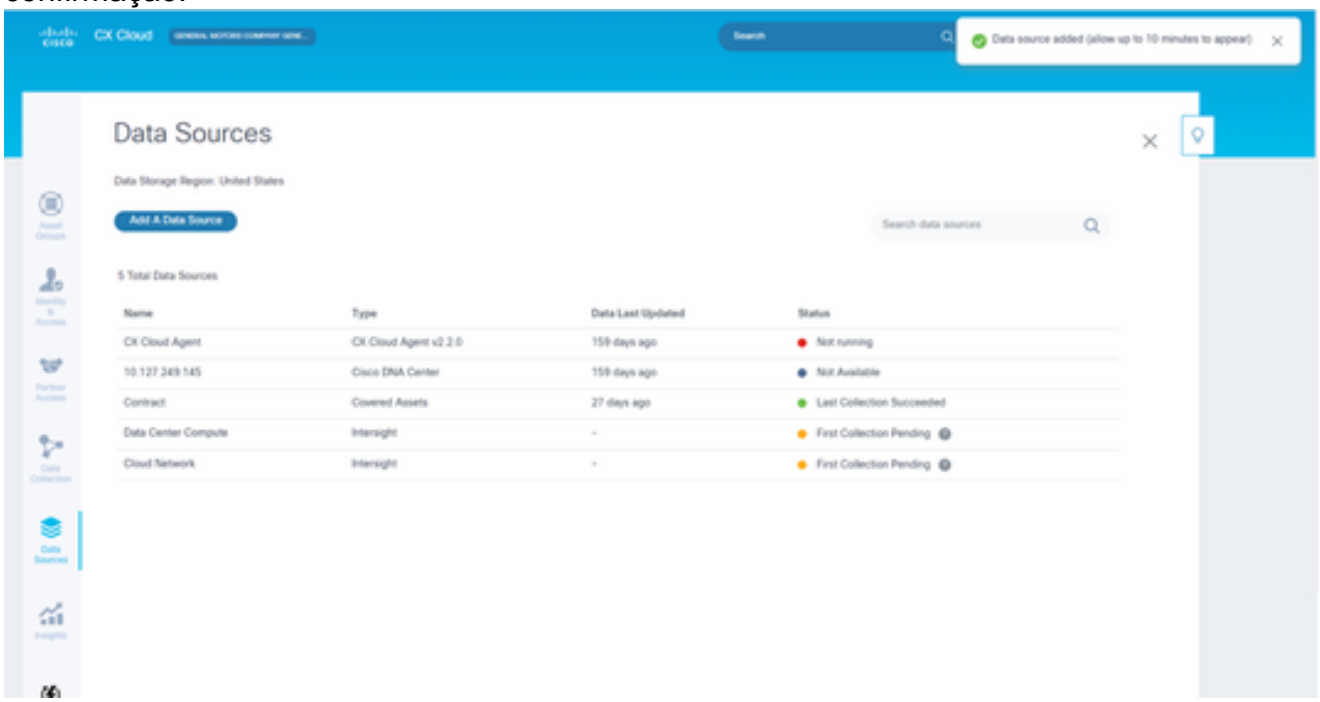


Credenciais SNMP v2, SSHV2 e SSHV1



Credenciais Telnet e programação de verificação de rede

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

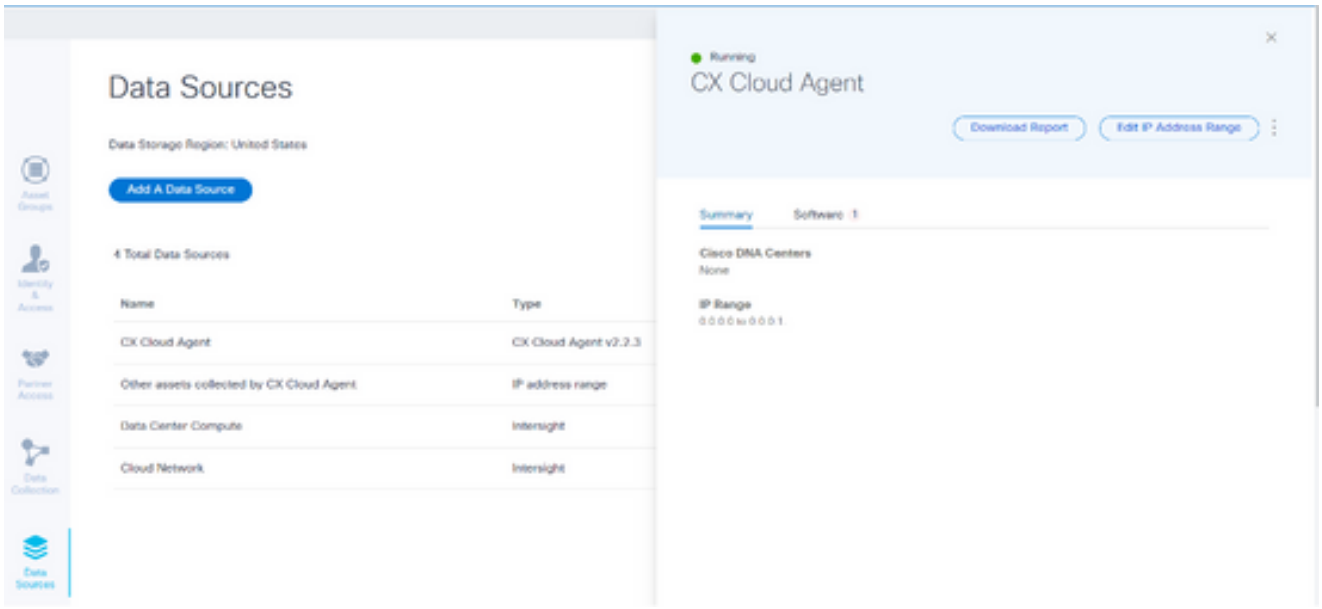


Confirmação

Editando Intervalos IP

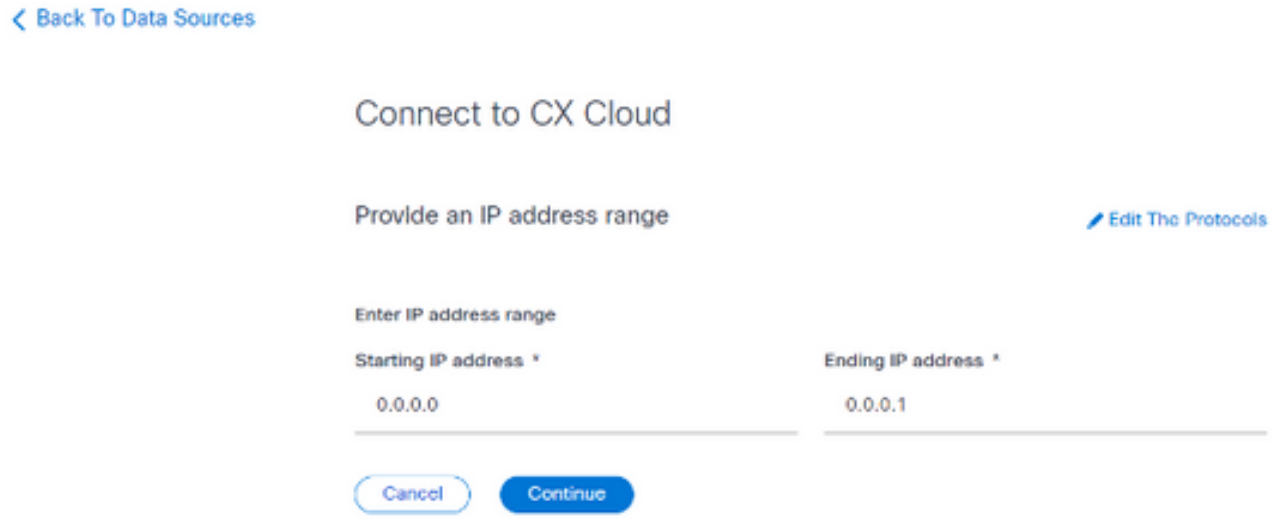
Para editar um intervalo IP;

1. Navegue até a janela Origens de Dados.



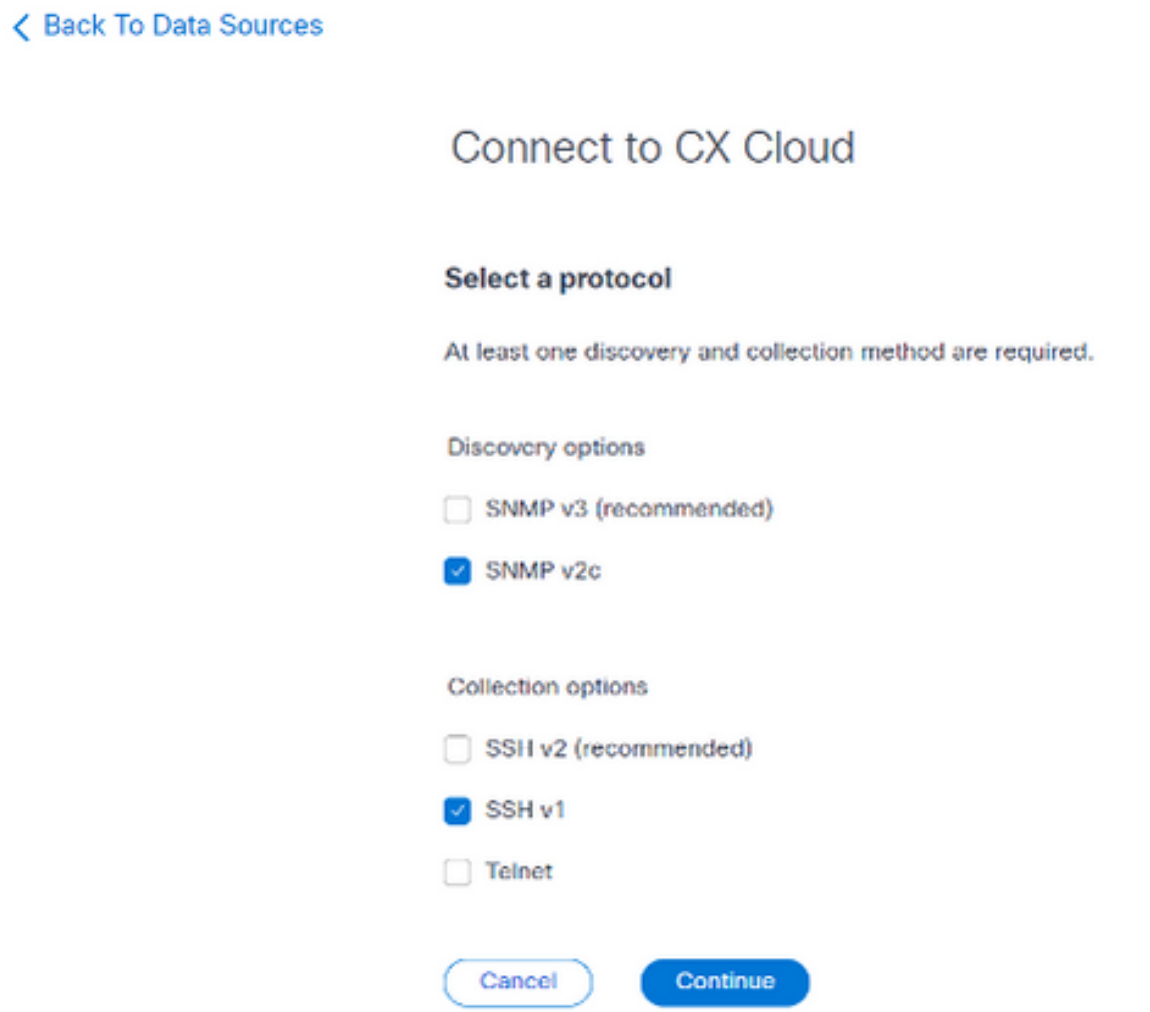
Origem dos dados

2. Clique no CX Cloud Agent que requer a edição do intervalo IP em Data Sources. A janela de detalhes é aberta.
3. Clique em Edit IP Address Range. A janela Connect to CX Cloud é aberta.



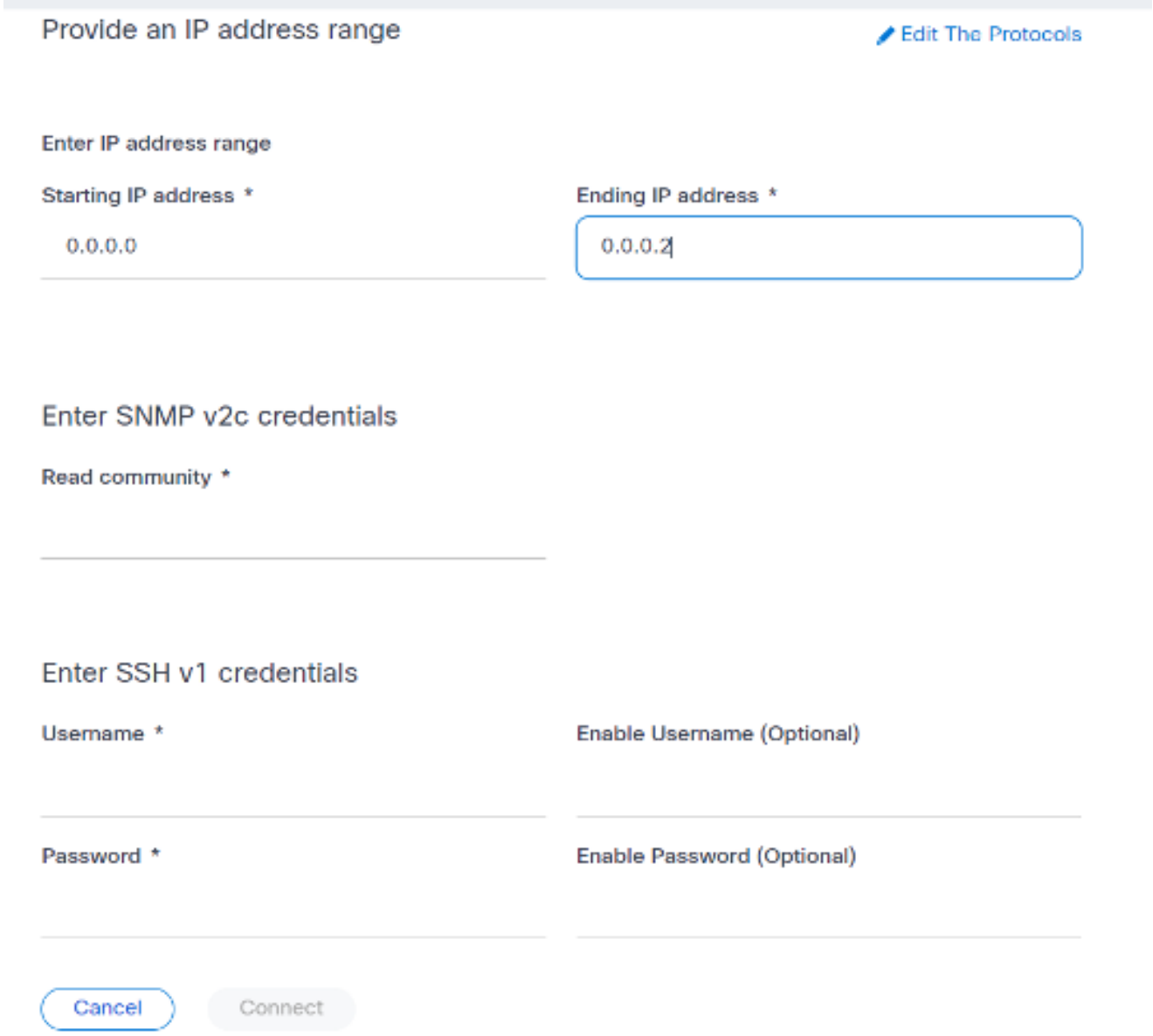
Forneça um intervalo de IPs

4. Atualize os novos IPs nos campos Endereço IP inicial e Endereço IP final.
5. Clique no link Edit the Protocols. A janela Connect to CX Cloud - Select a protocol é aberta.



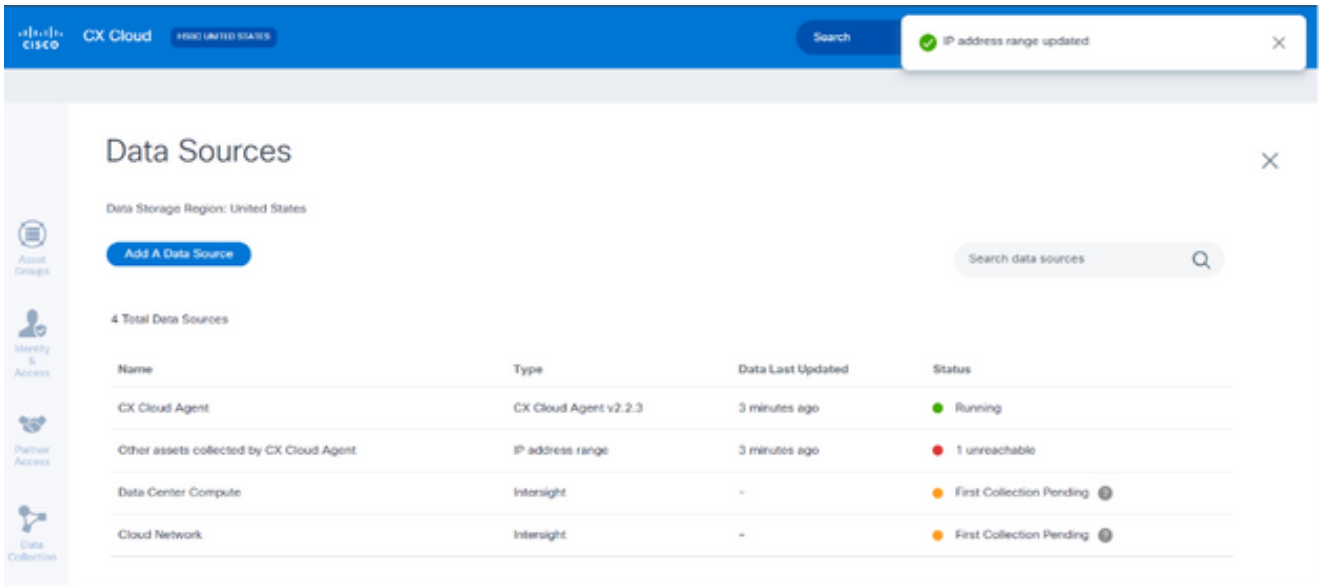
Selecionar um protocolo

6. Selecione os protocolos aplicáveis clicando nas caixas de seleção apropriadas.
7. Clique em Continuar. A janela Provide an IP address range é aberta.



Inserir Credenciais

8. Digite as credenciais de configuração.
9. Clique em Conectar. A janela Fontes de dados é aberta, exibindo uma mensagem de confirmação.



Confirmação

Observação: a mensagem de confirmação não garante que os dispositivos no intervalo editado estejam acessíveis e que as credenciais tenham sido aceitas.

Sobre os dispositivos descobertos de vários controladores

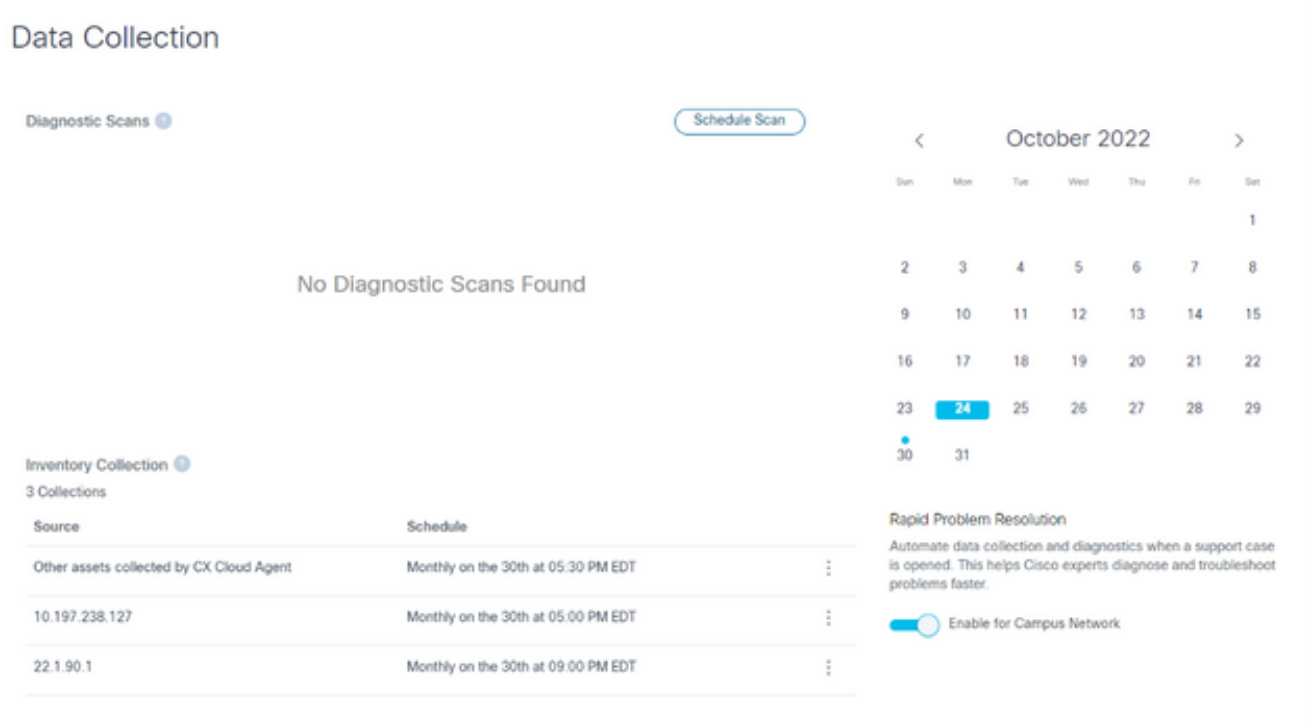
É possível que alguns dispositivos possam ser descobertos pelo Cisco DNA Center e pela conexão direta do dispositivo com o CX Cloud Agent, fazendo com que dados duplicados sejam coletados desses dispositivos. Para evitar a coleta de dados duplicados e ter apenas um controlador para gerenciar os dispositivos, 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

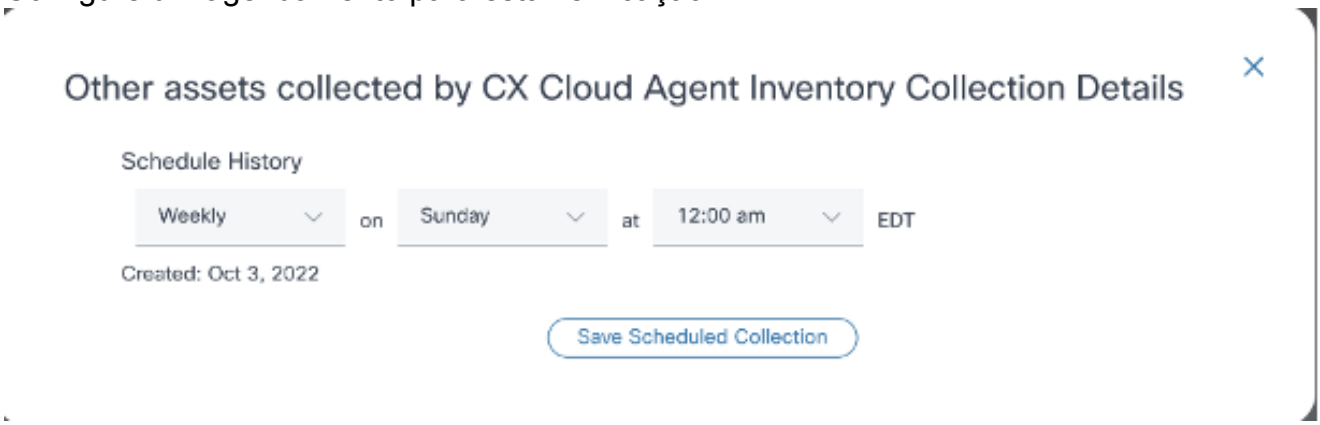
Para programar varreduras de diagnóstico:

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.



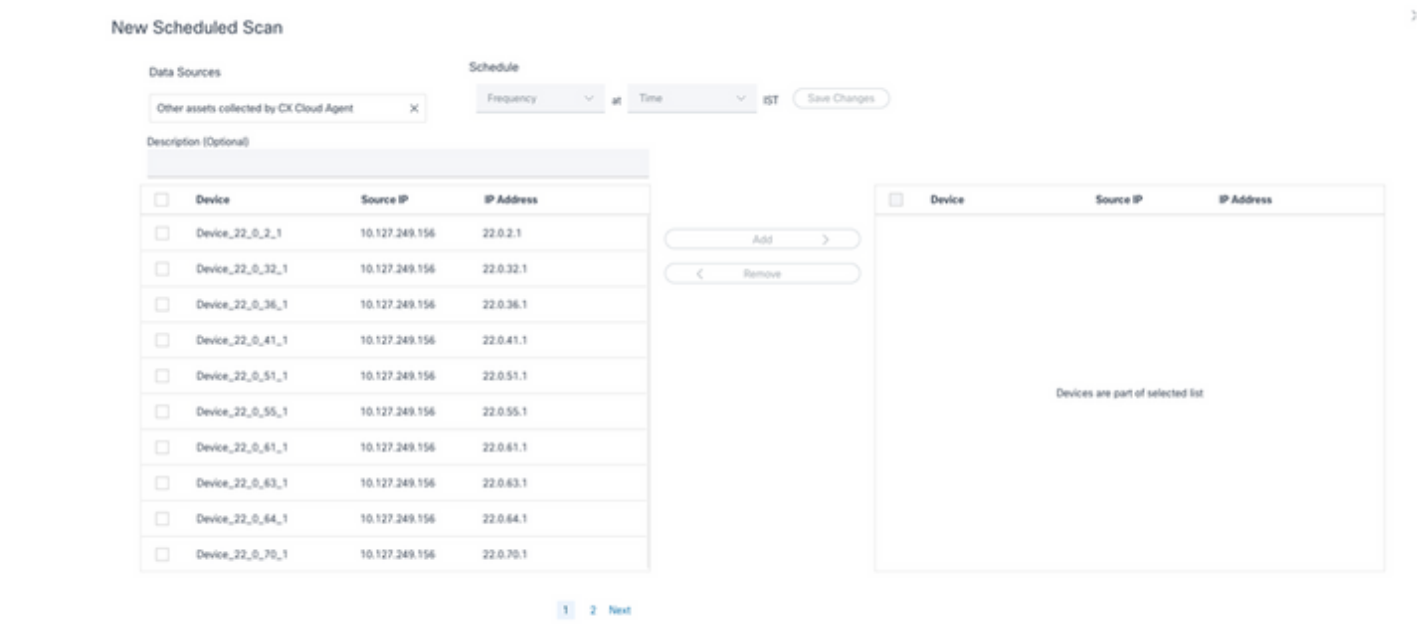
Levantamento de dados

4. Configure um agendamento para esta verificação.



Configurar programação de verificação

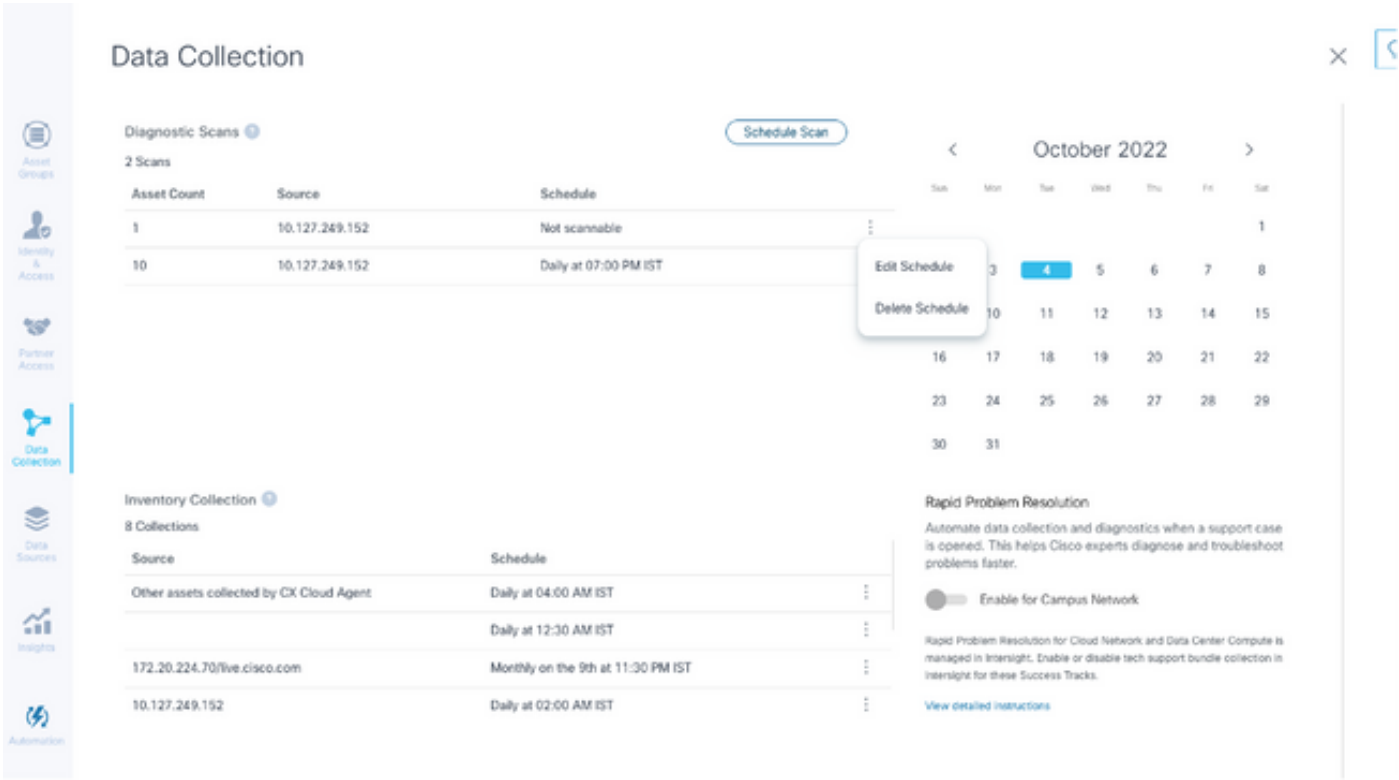
5. Na lista de dispositivos, selecione todos os dispositivos para a verificação e clique em Adicionar.



Agendar uma verificação

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

Os agendamentos Diagnostic Scans e Inventory Collection podem ser editados e excluídos da página Data Collection.



Coleta de dados com opções Editar e Excluir agenda

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

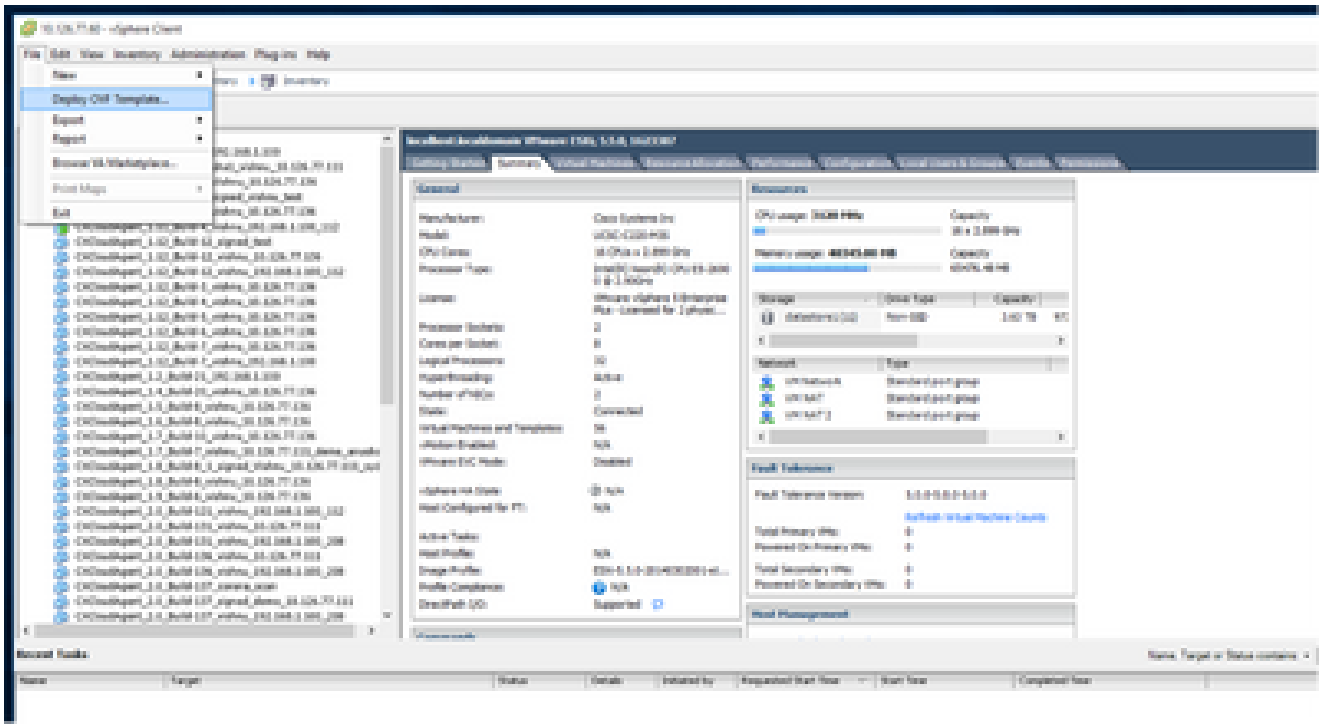
Instalação do Thick Client ESXi 5.5/6.0

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.

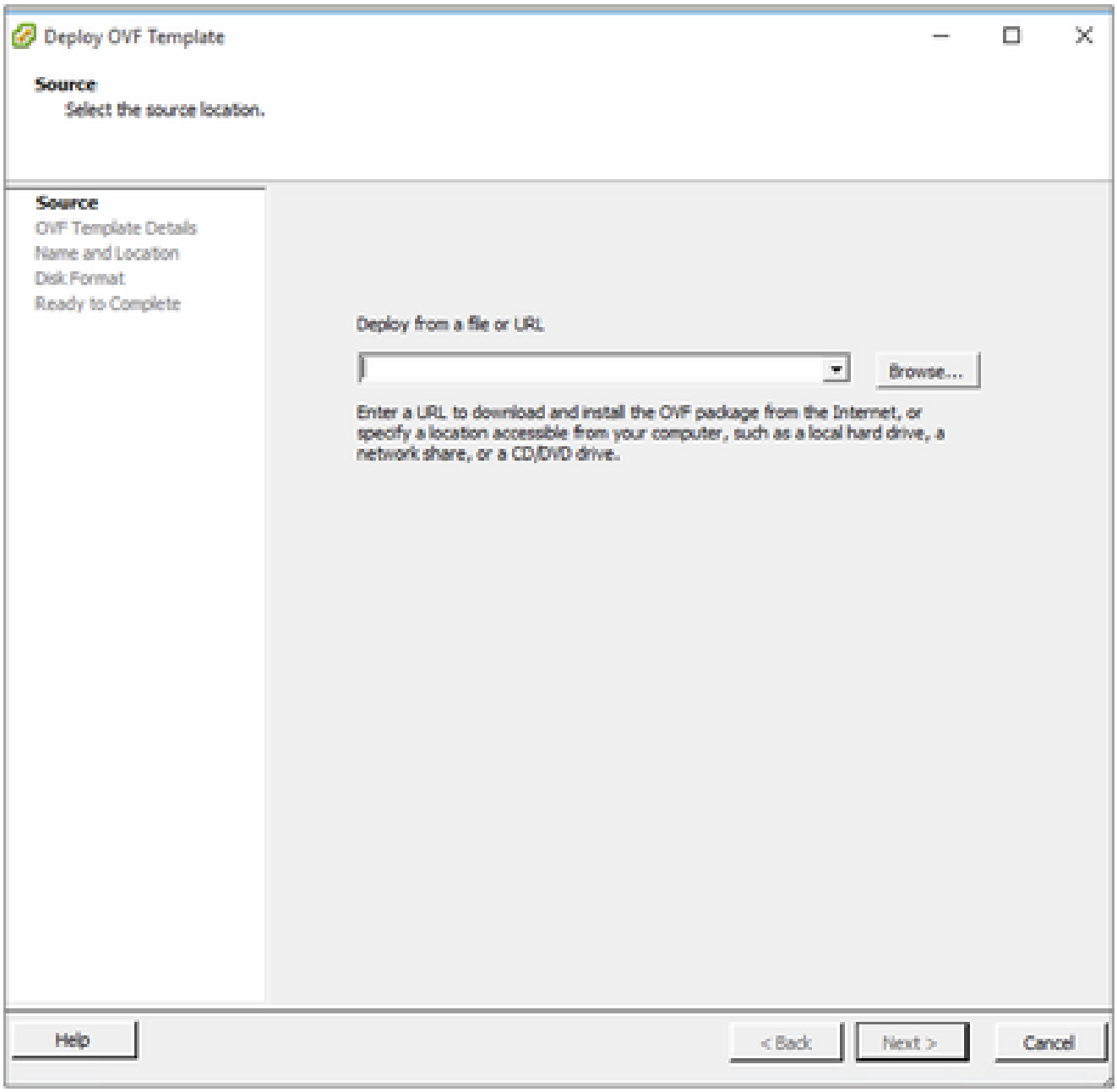
Login

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



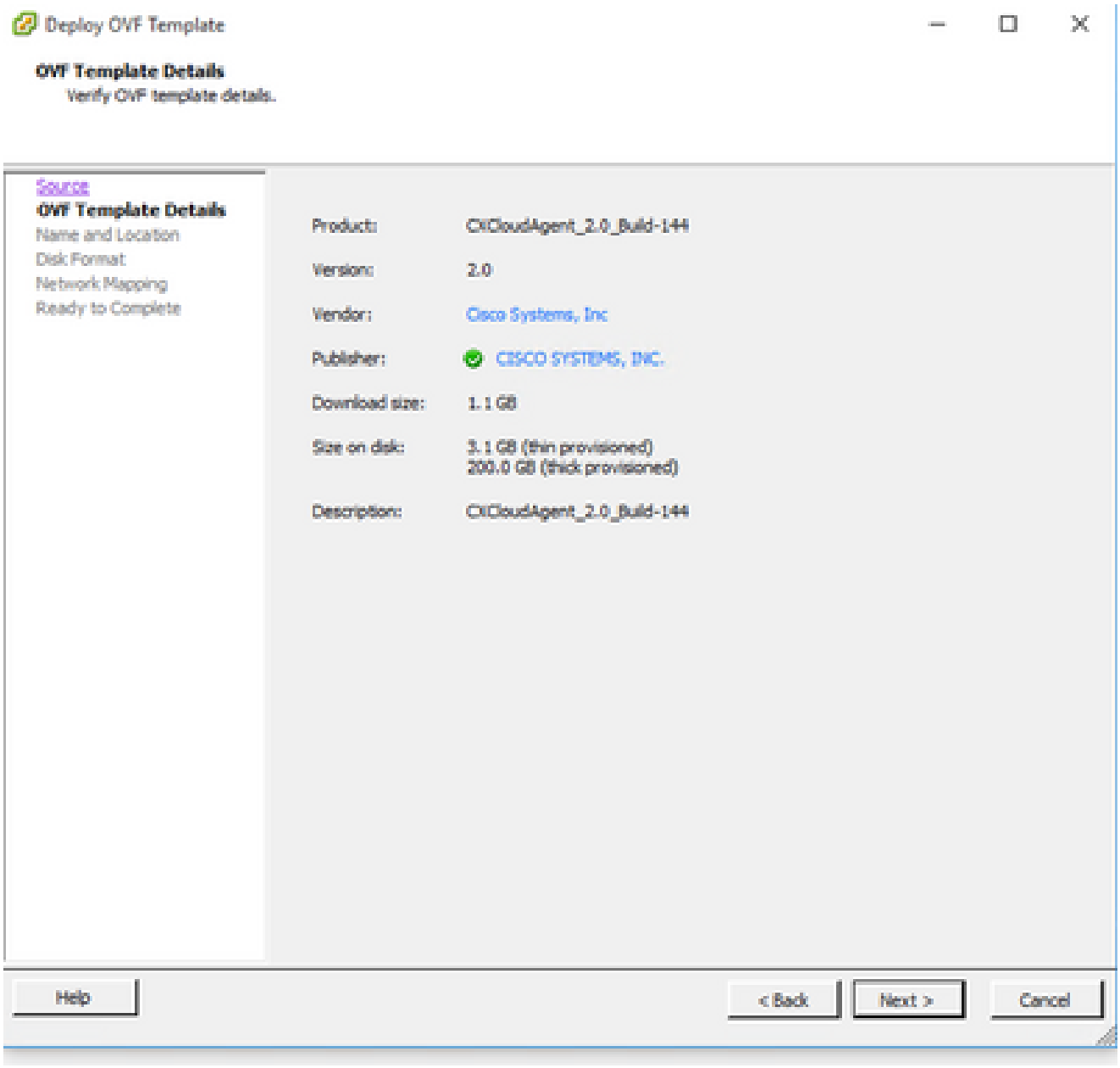
vSphere Client

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



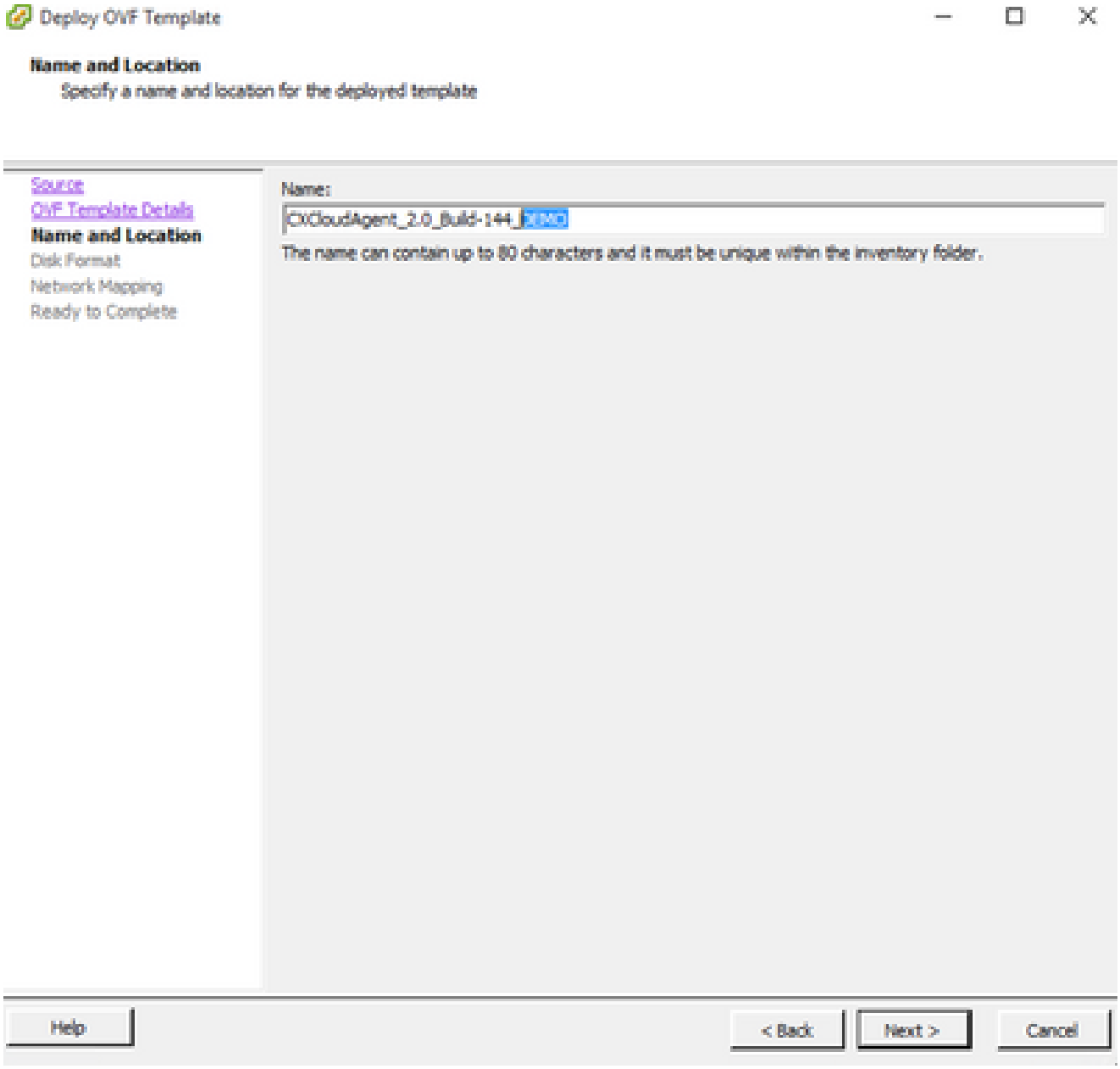
Caminho do OVA

4. Verifique os Detalhes OVF e clique em Avançar.



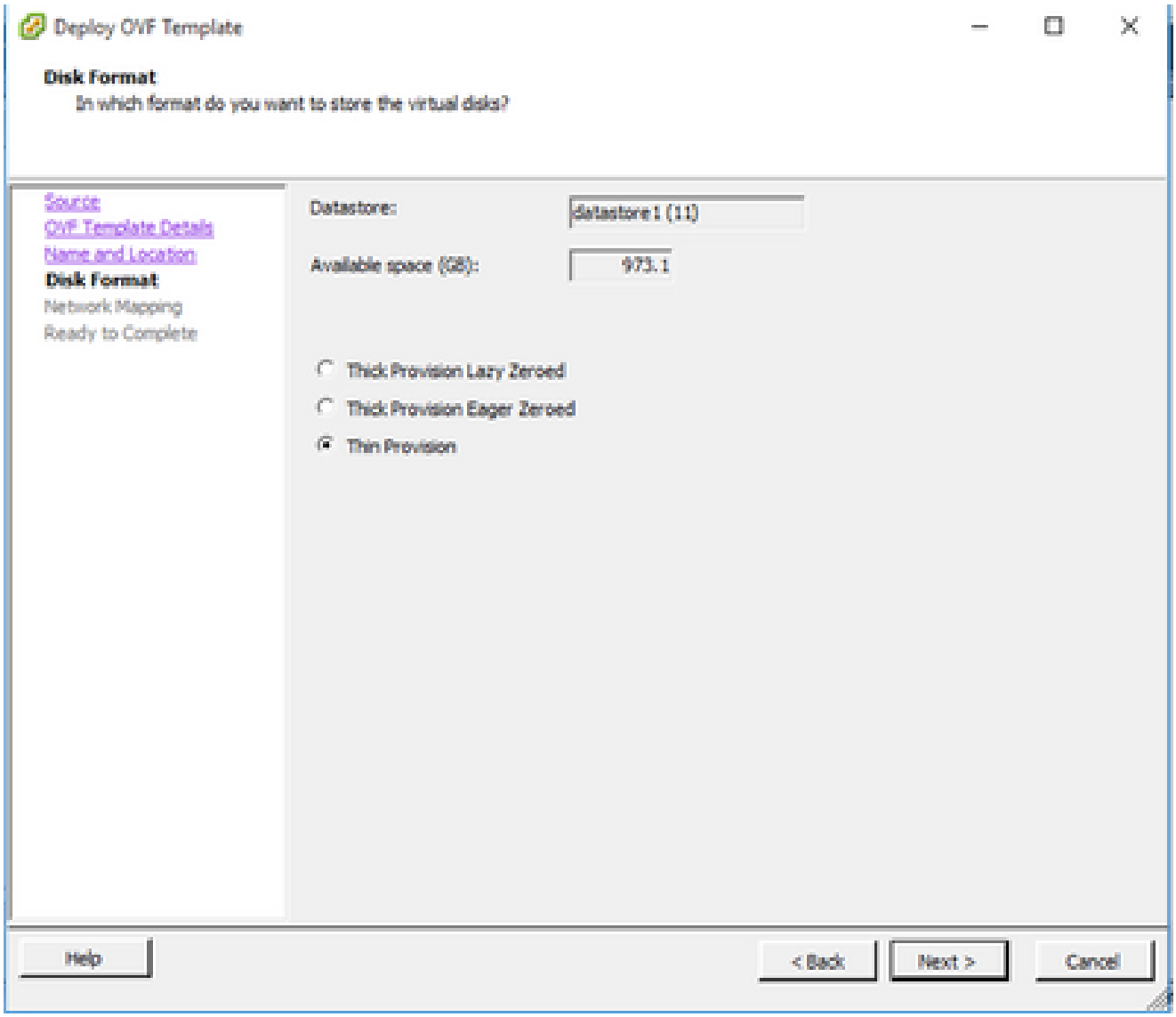
Detalhes do modelo

5. Insira um nome exclusivo e clique em Avançar.



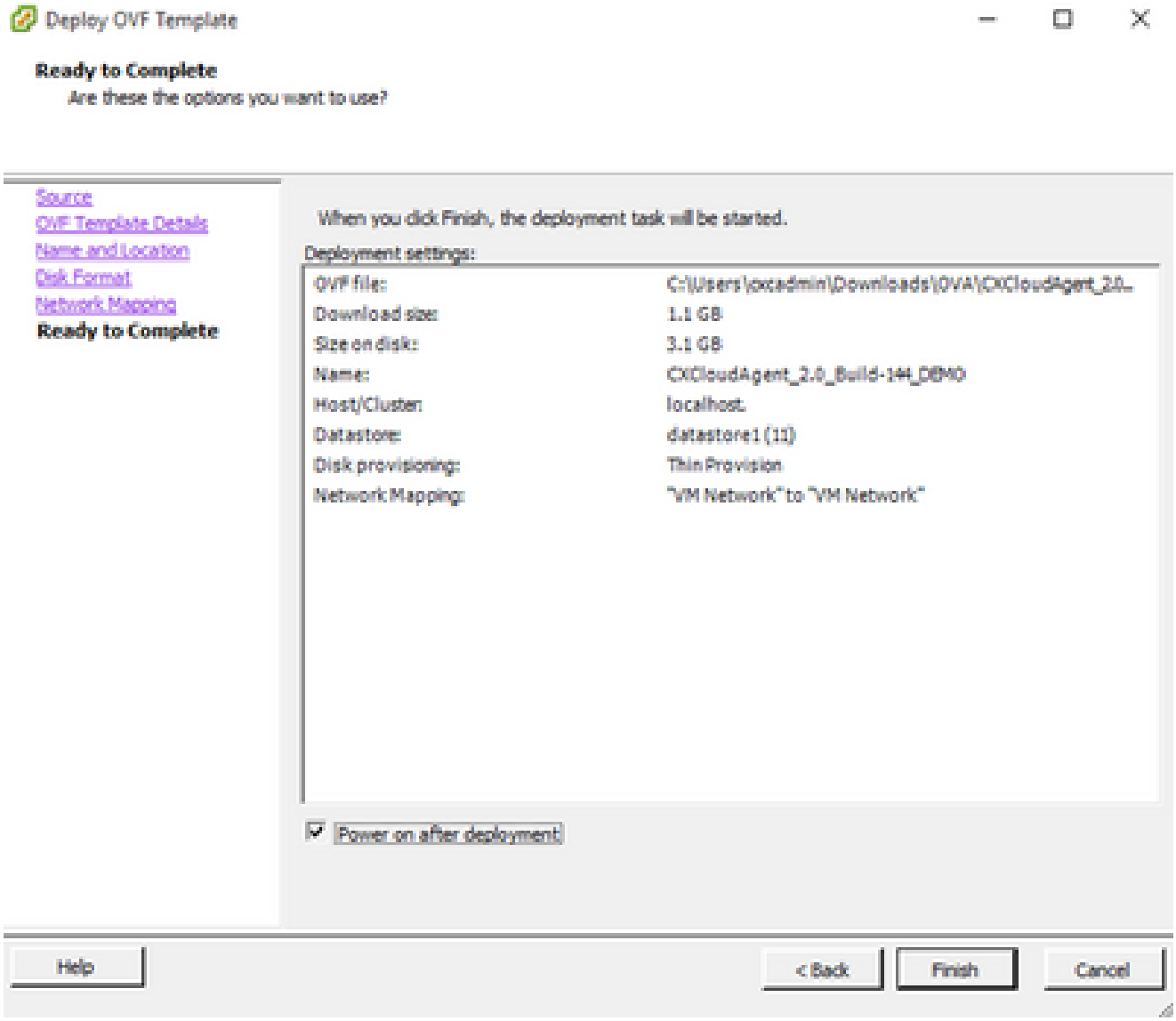
Nome e local

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



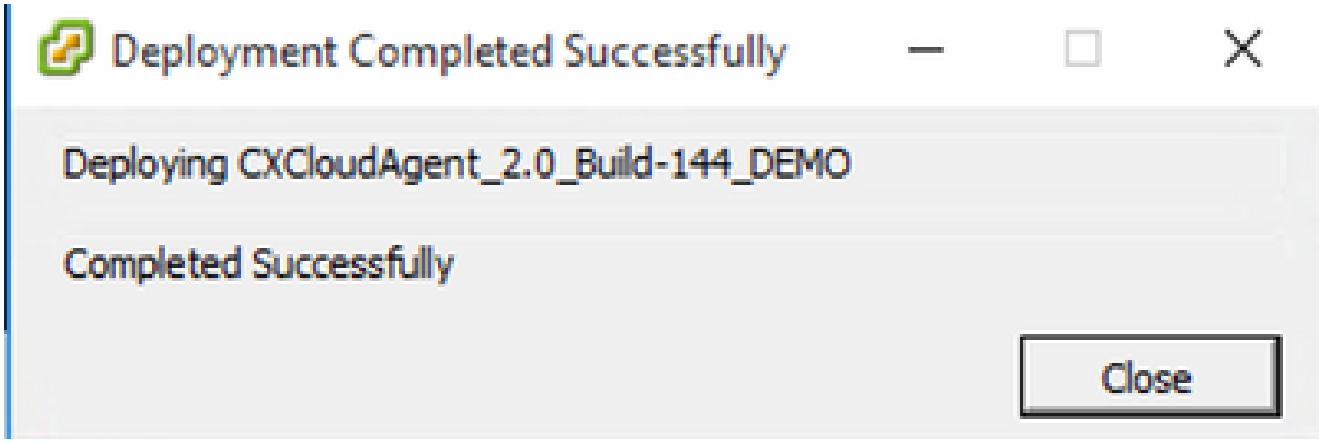
Formato de disco

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



Pronto para concluir

A implantação pode levar vários minutos. WConfirmation é exibido após a implantação bem-sucedida.



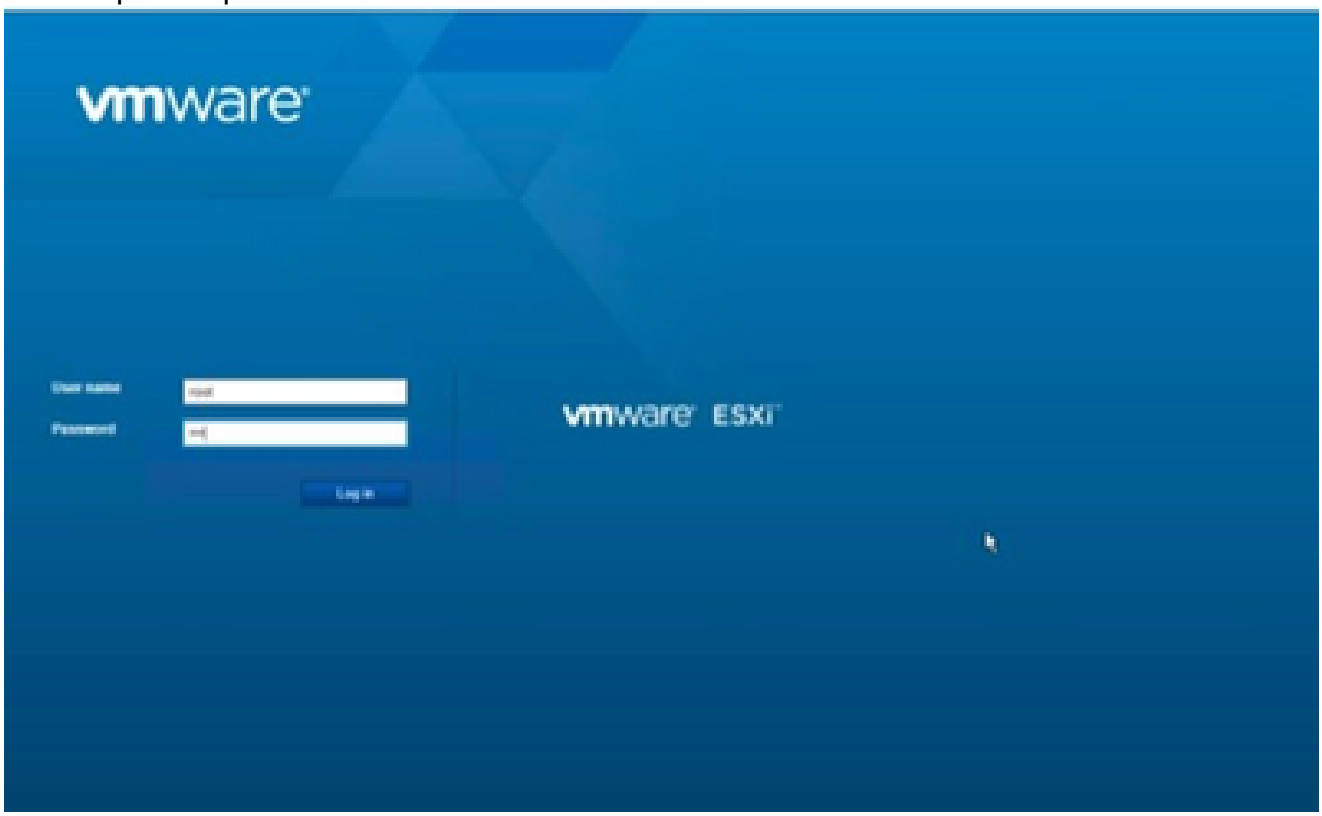
Implantação concluída

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

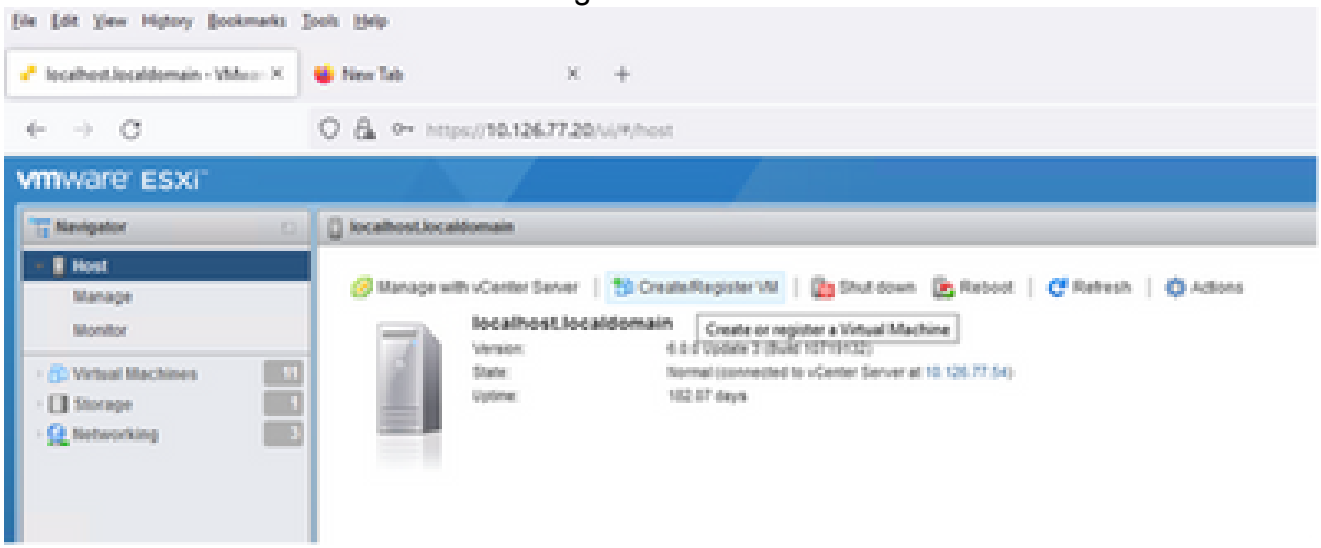
Esse cliente implanta o CX Cloud Agent OVA usando a Web do vSphere.

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



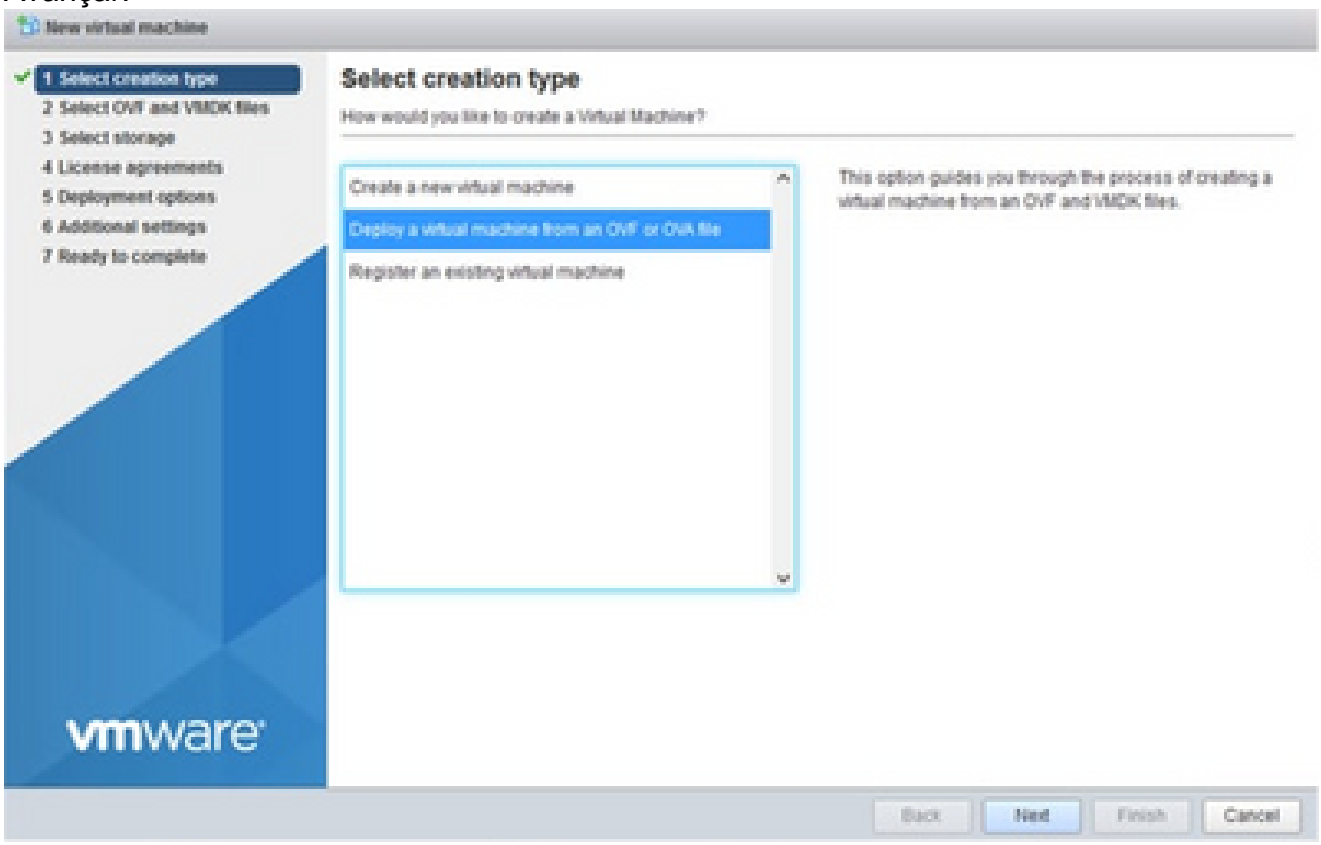
Login no VMware ESXi

2. Selecione Virtual Machine > Create / Register VM.



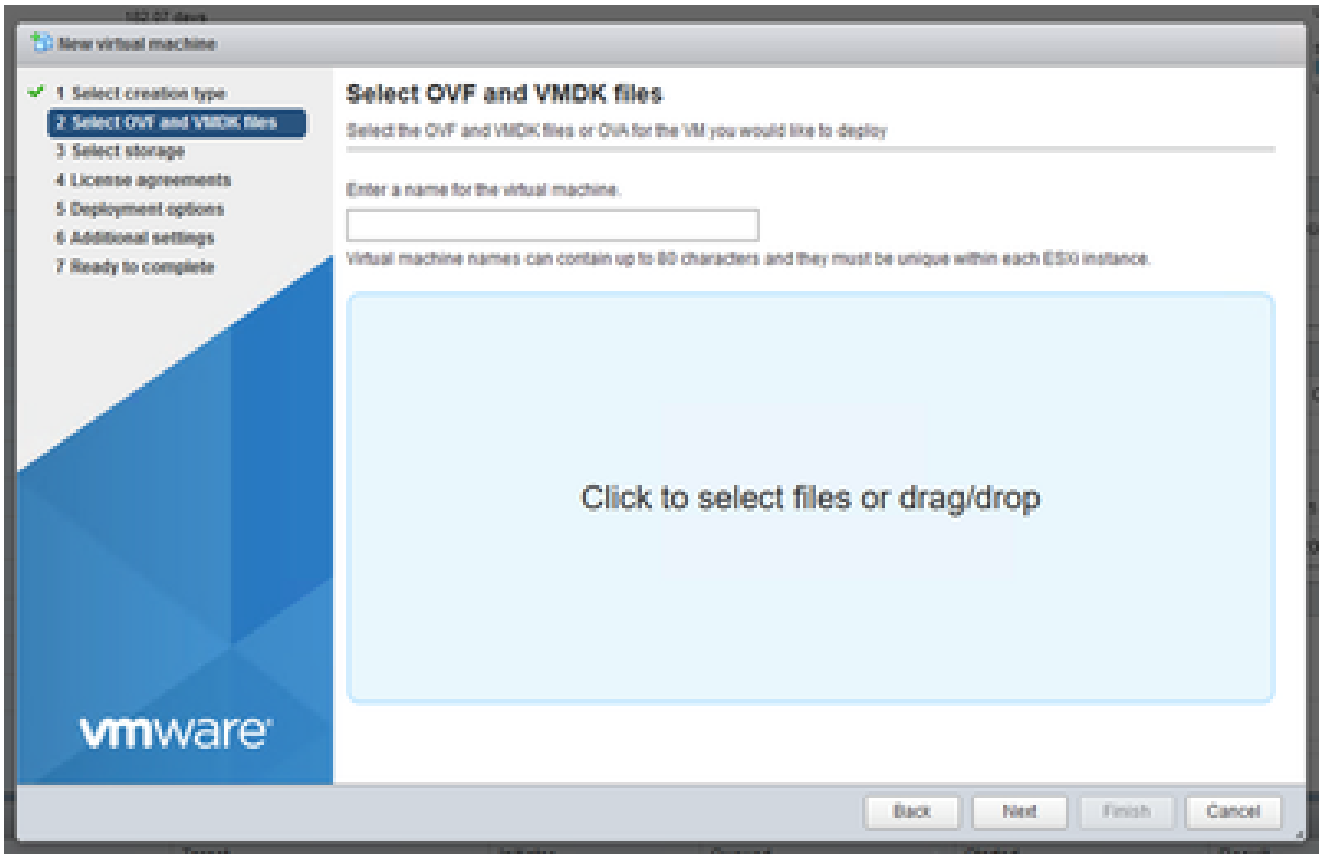
Criar VM

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



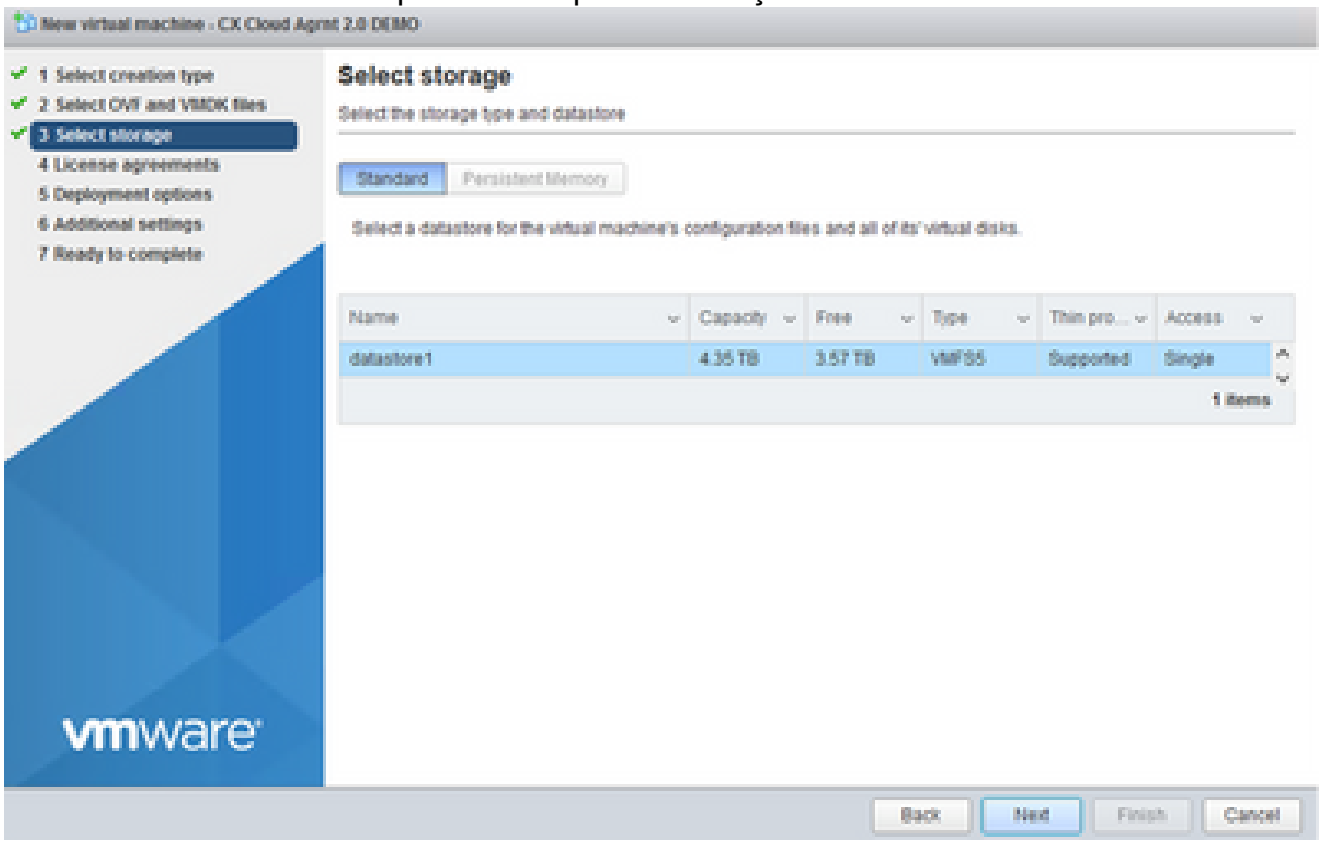
Selecionar Tipo de Criação

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



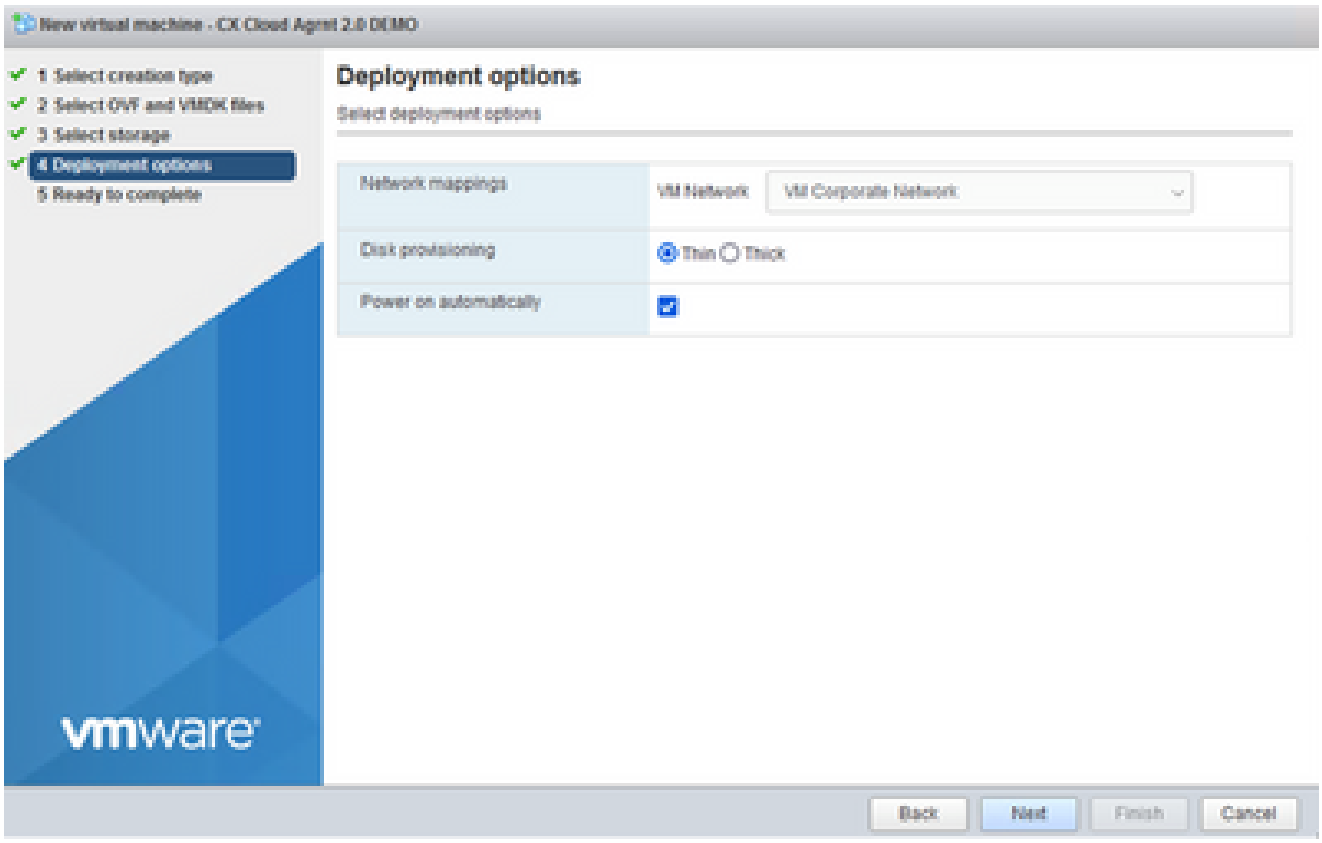
Seleção do OVA

6. Selecione Armazenamento padrão e clique em Avançar.



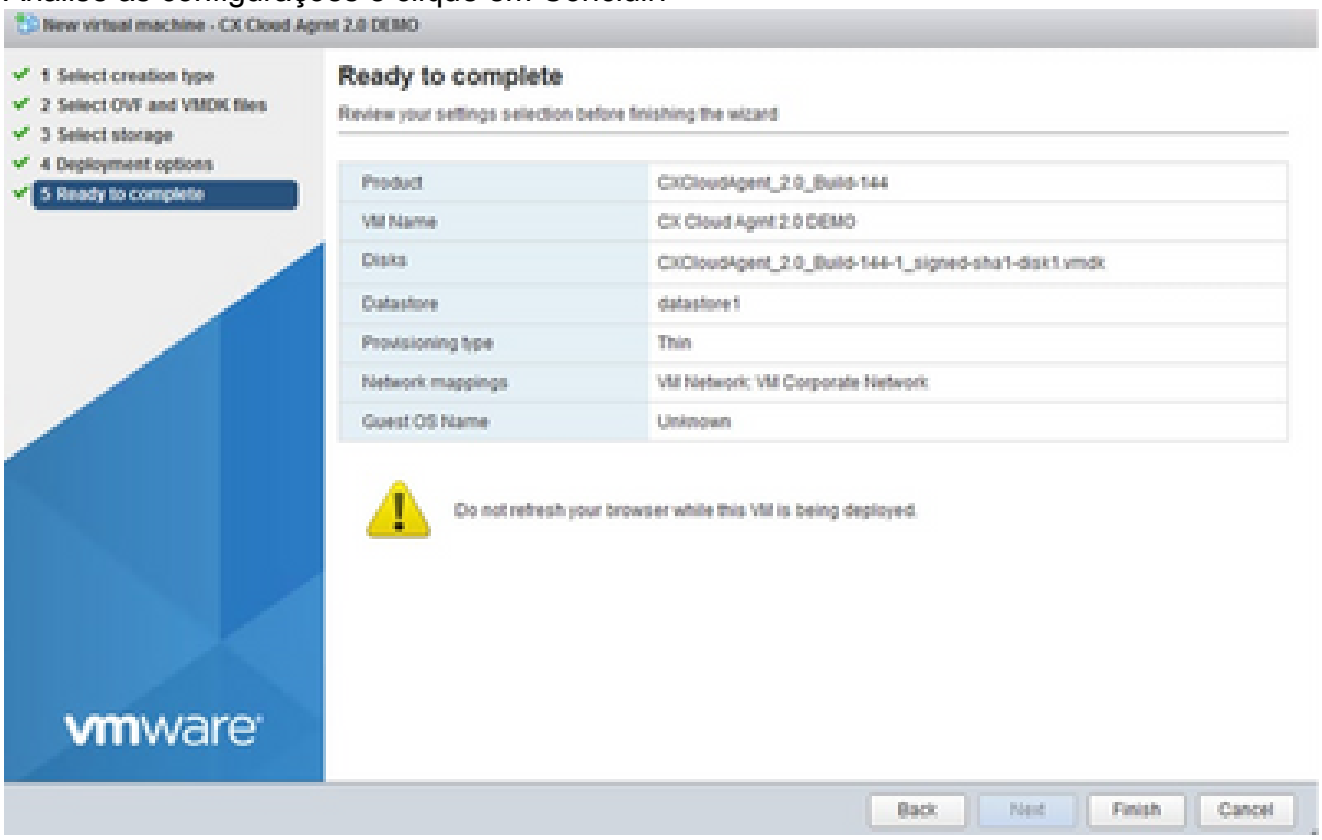
Selecionar armazenamento

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

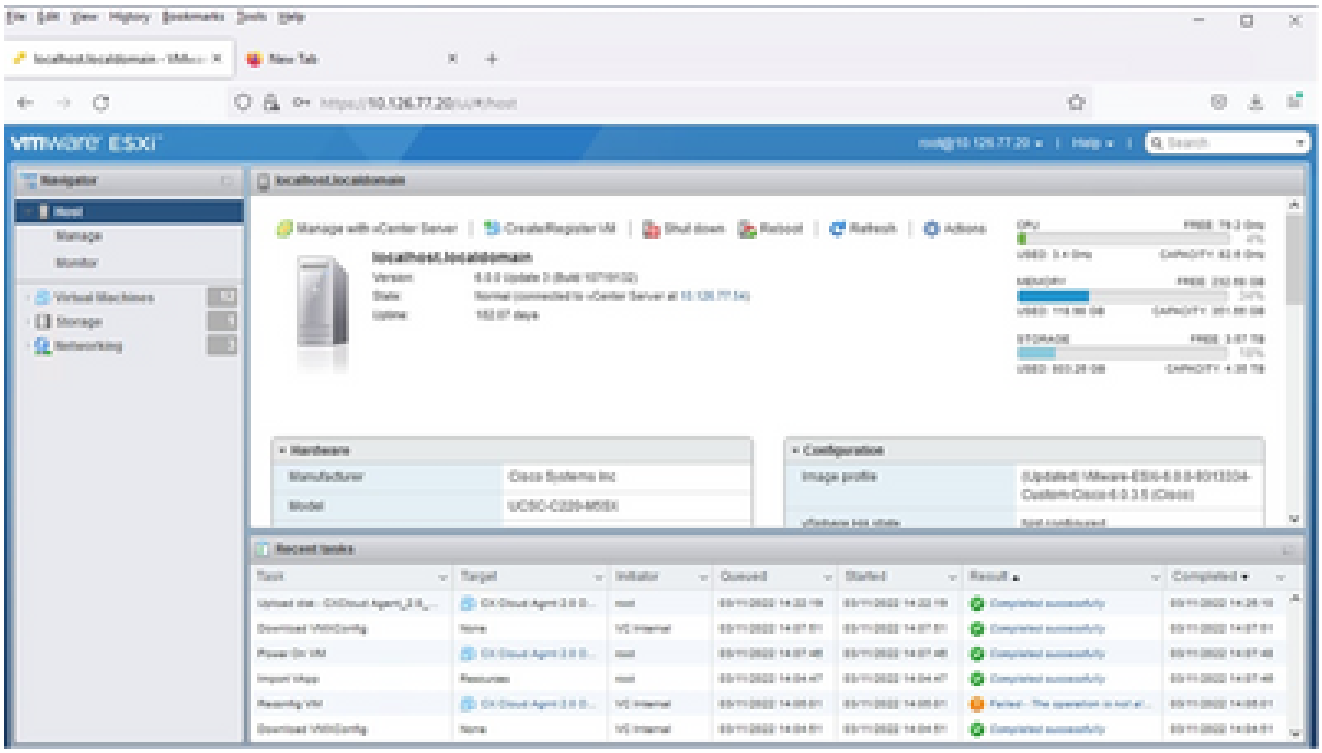


Opções de implantação

8. Analise as configurações e clique em Concluir.

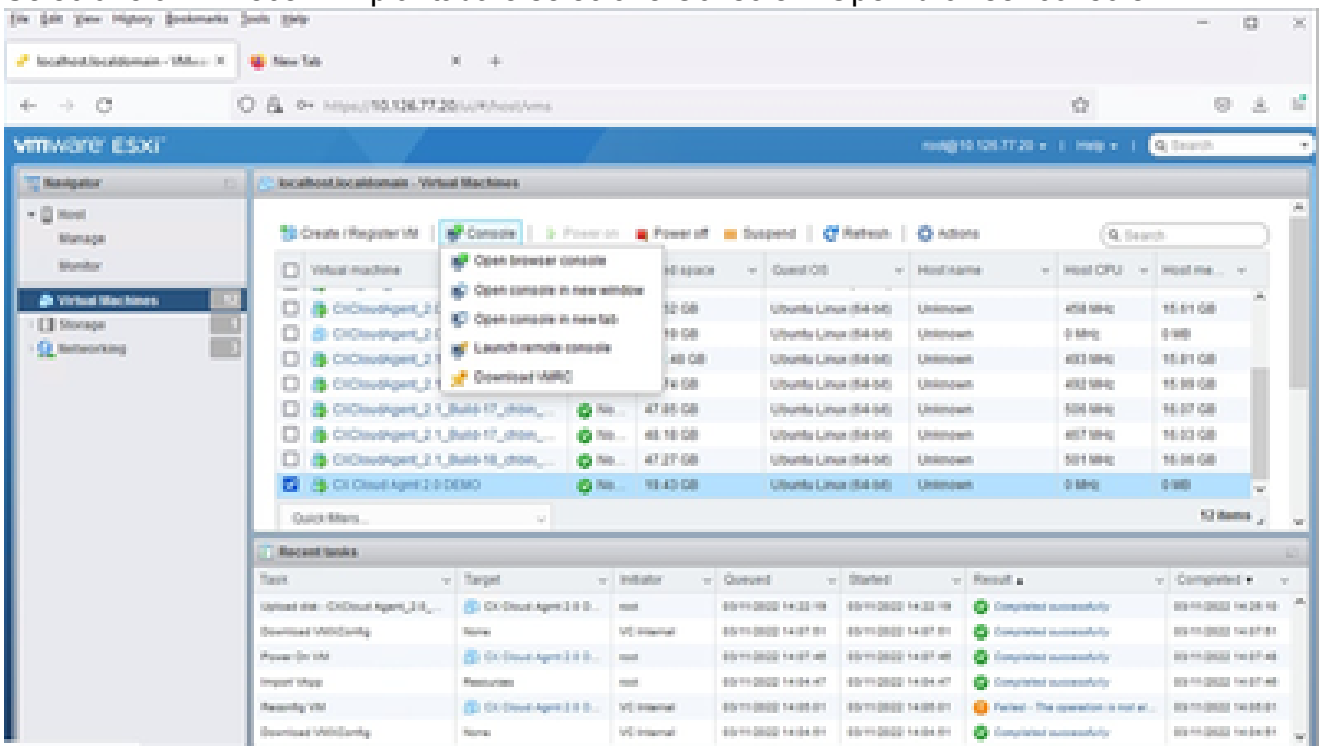


Pronto para concluir



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.

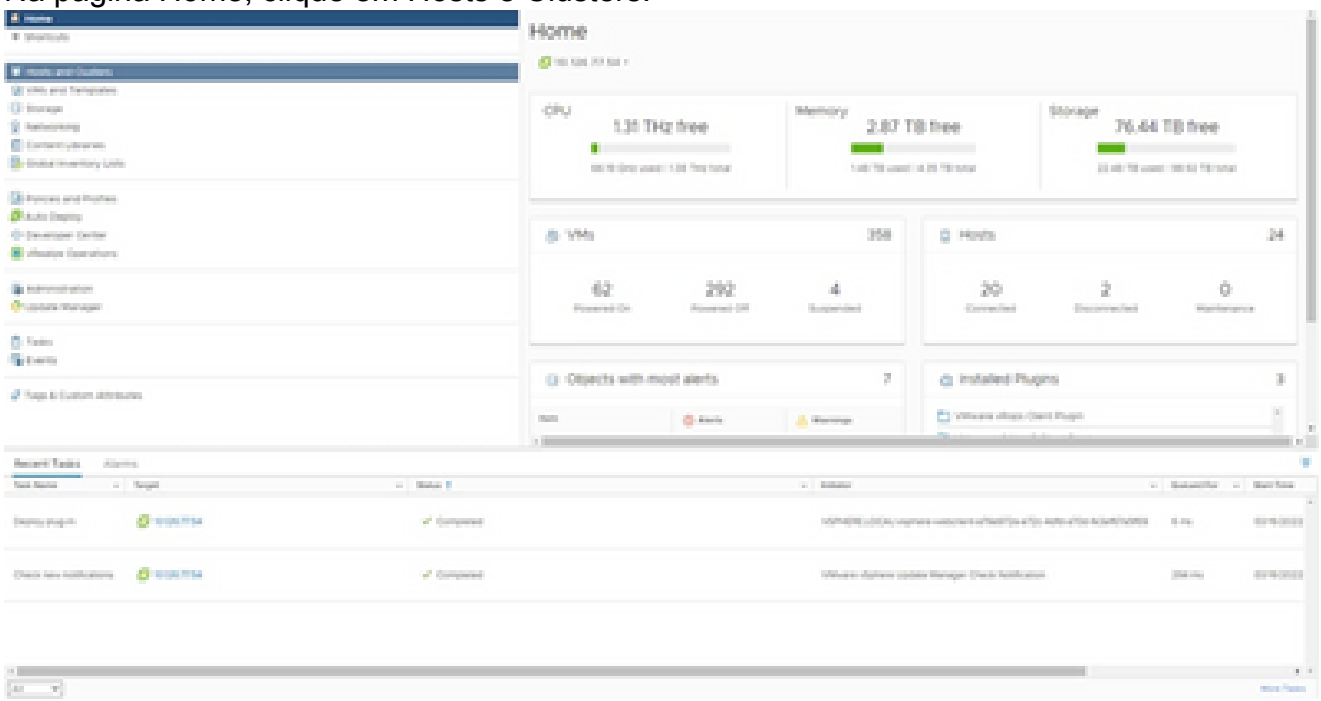
Instalação do Web Client vCenter

Execute o seguinte:

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

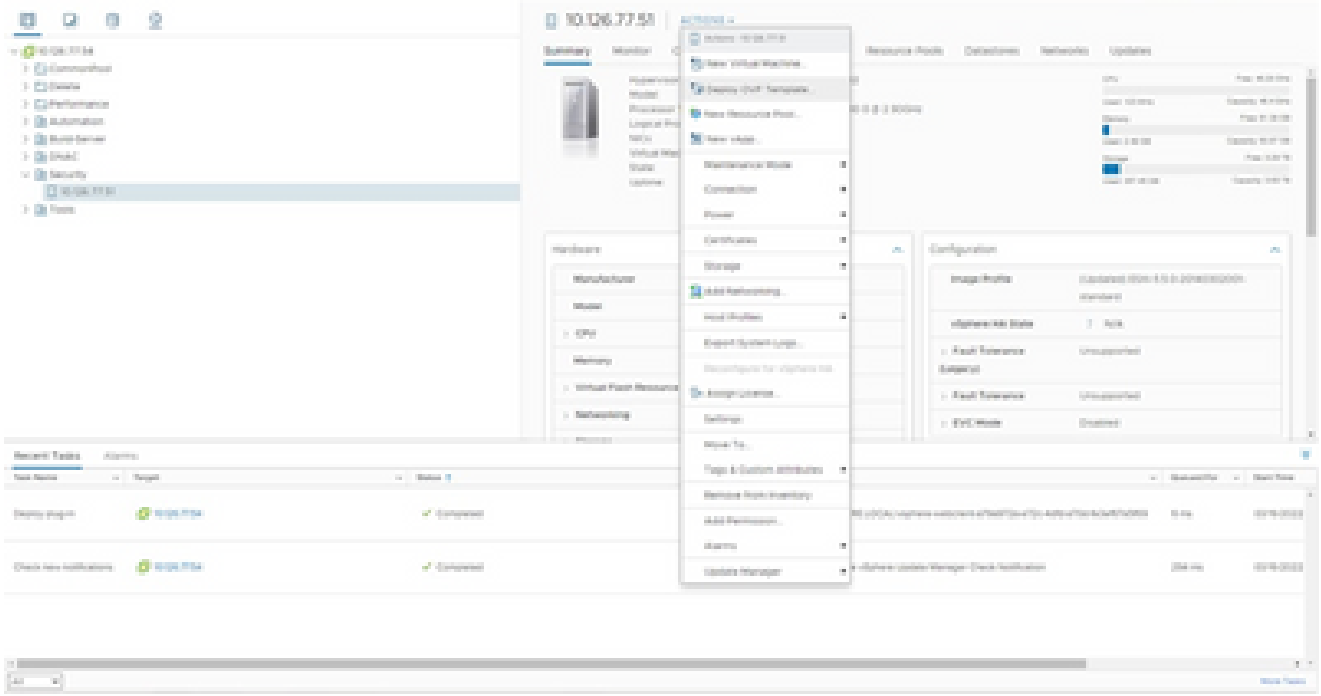
Login

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

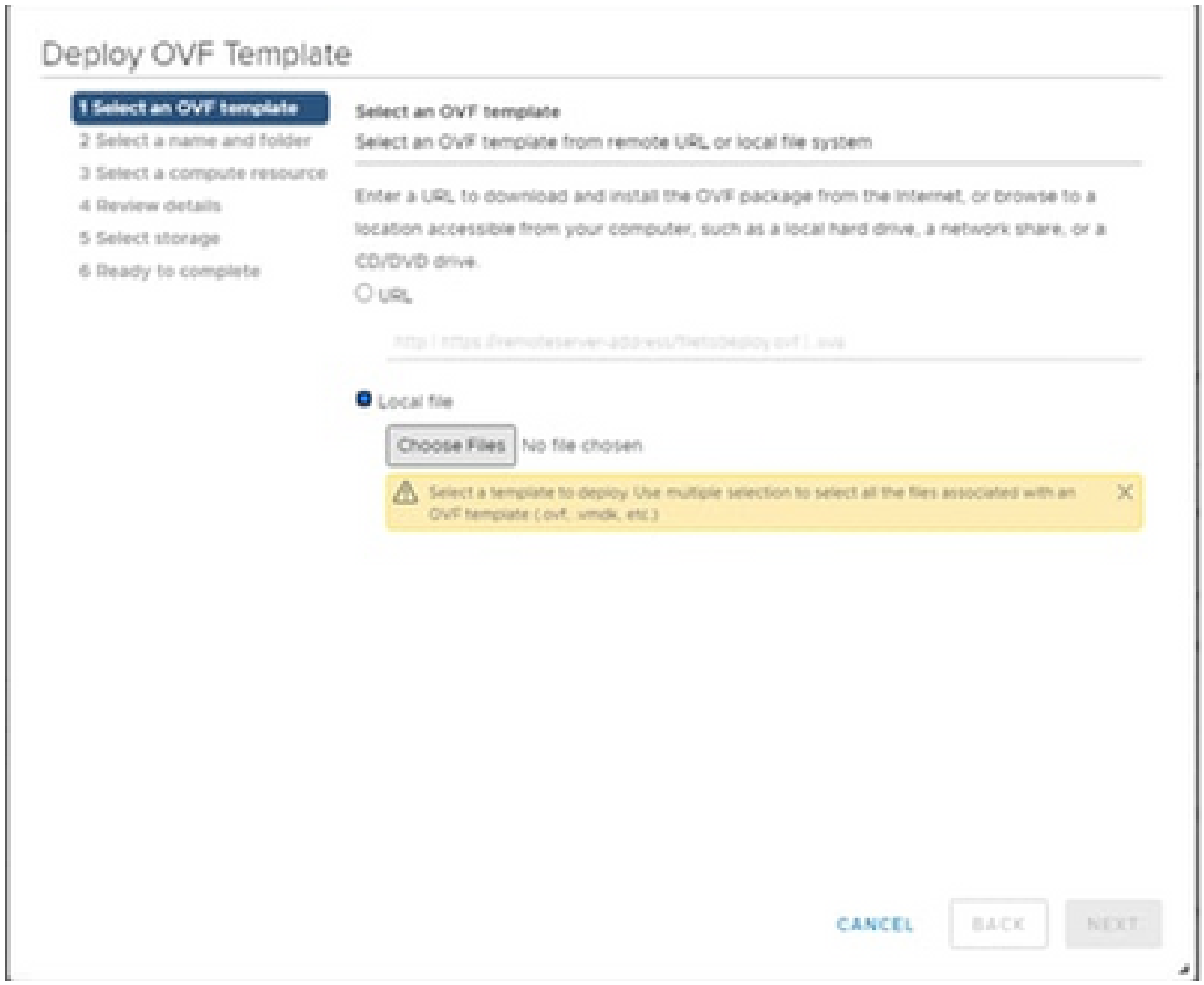


Página inicial

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

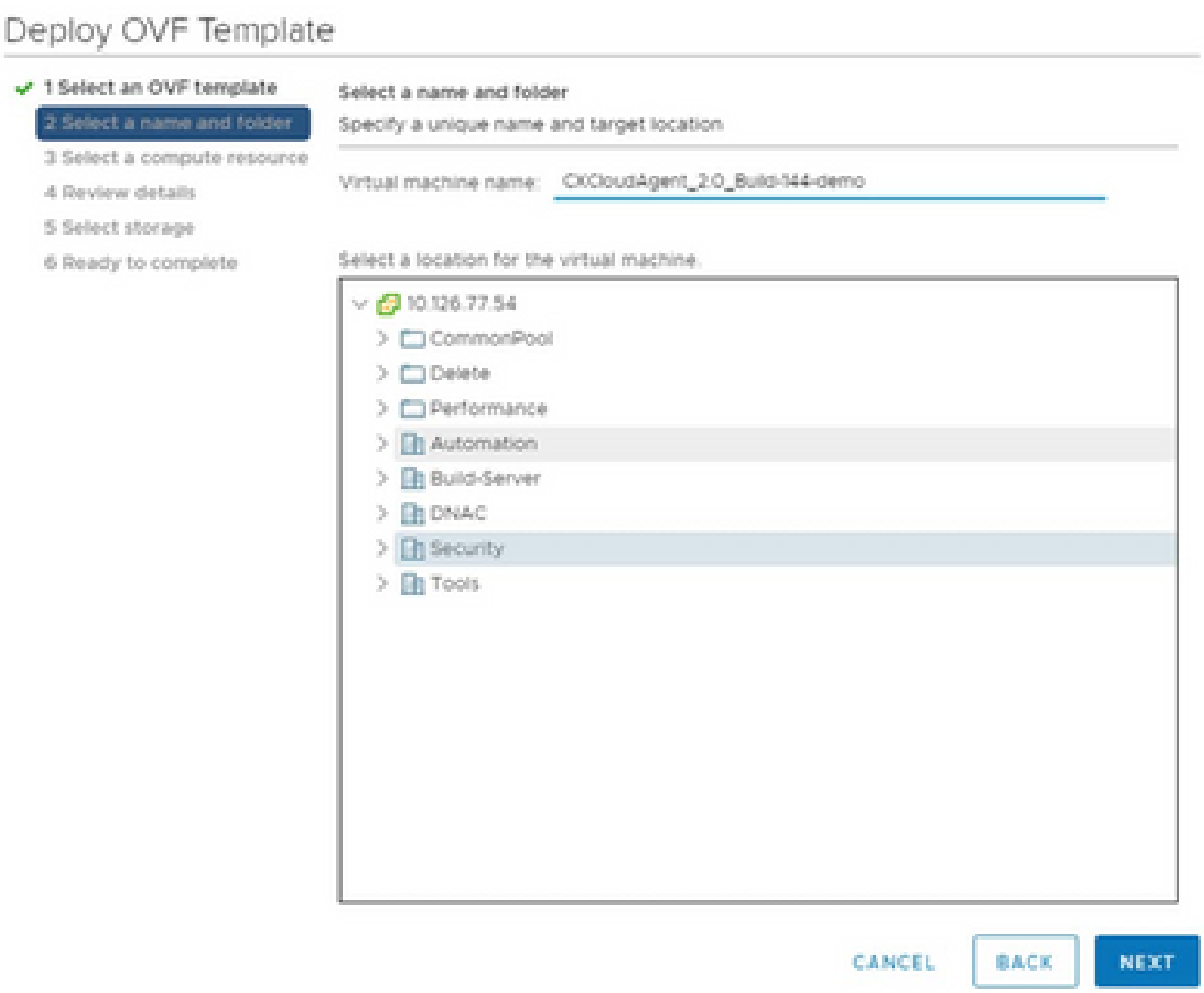


Ações


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete
Select an OVF template
Select an OVF template from remote URL or local file system
Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
URL
Local file
Choose Files
No file chosen
Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)
CANCEL
BACK
NEXT

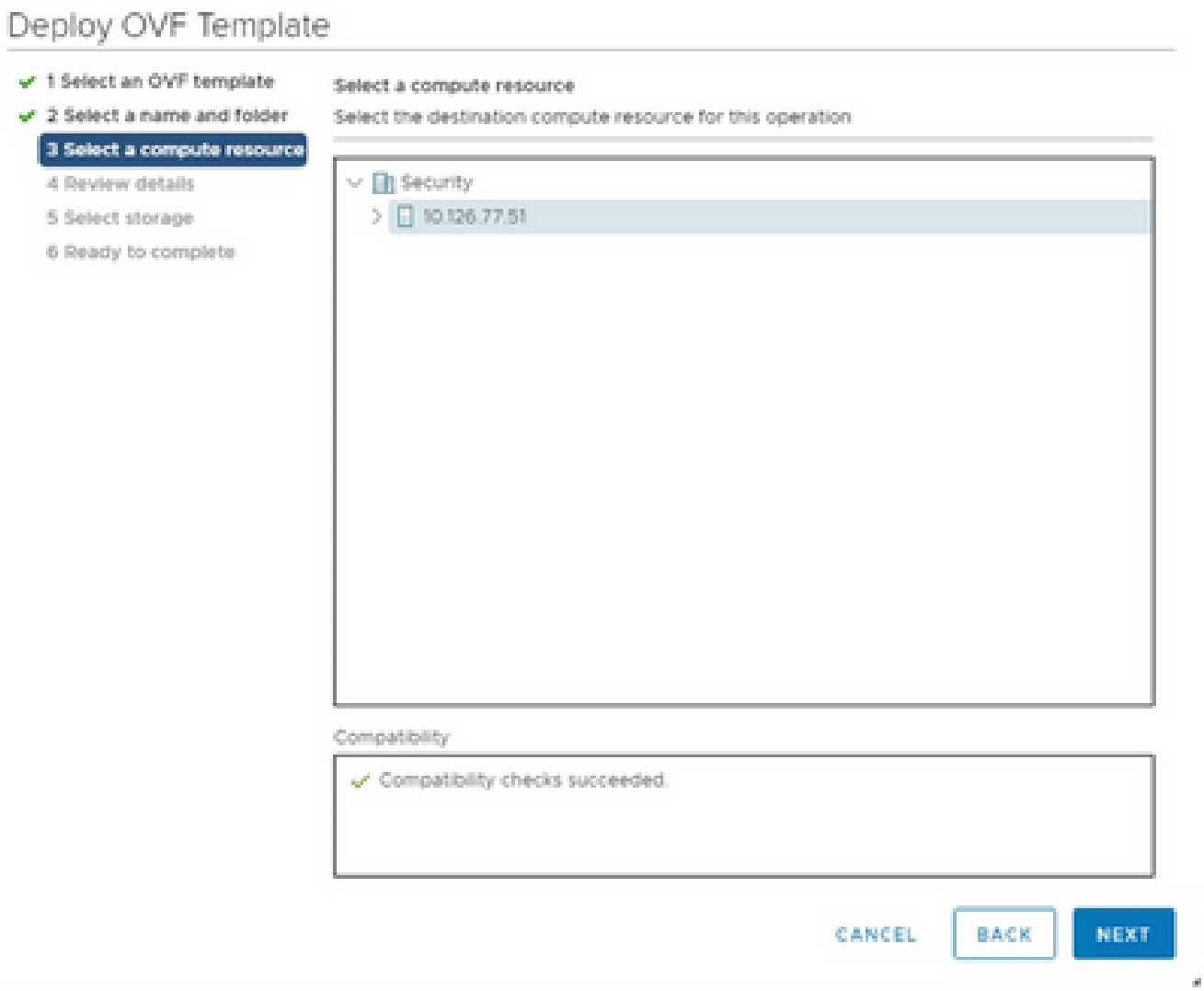
Selecionar modelo

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



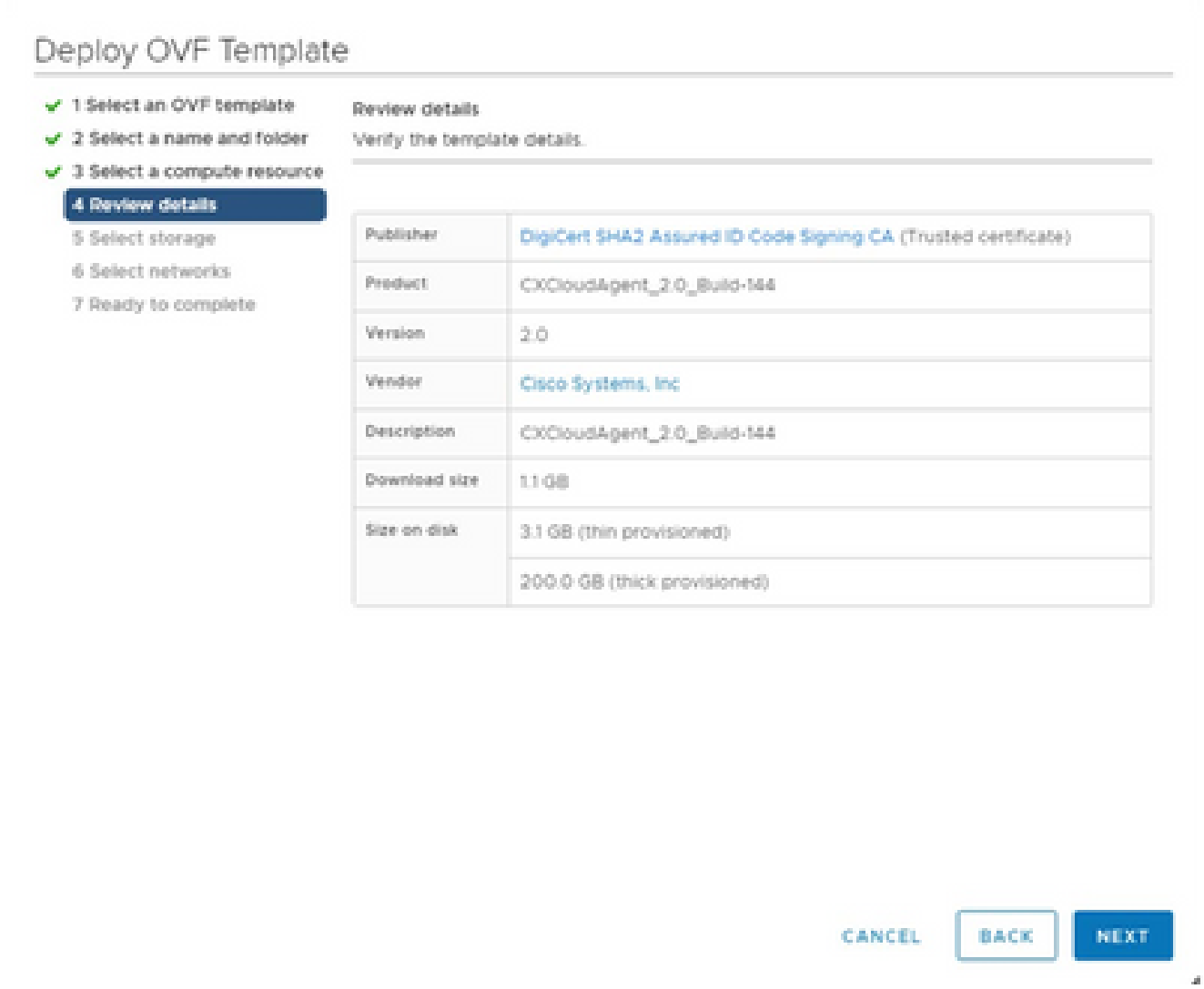
Nome e Pasta

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



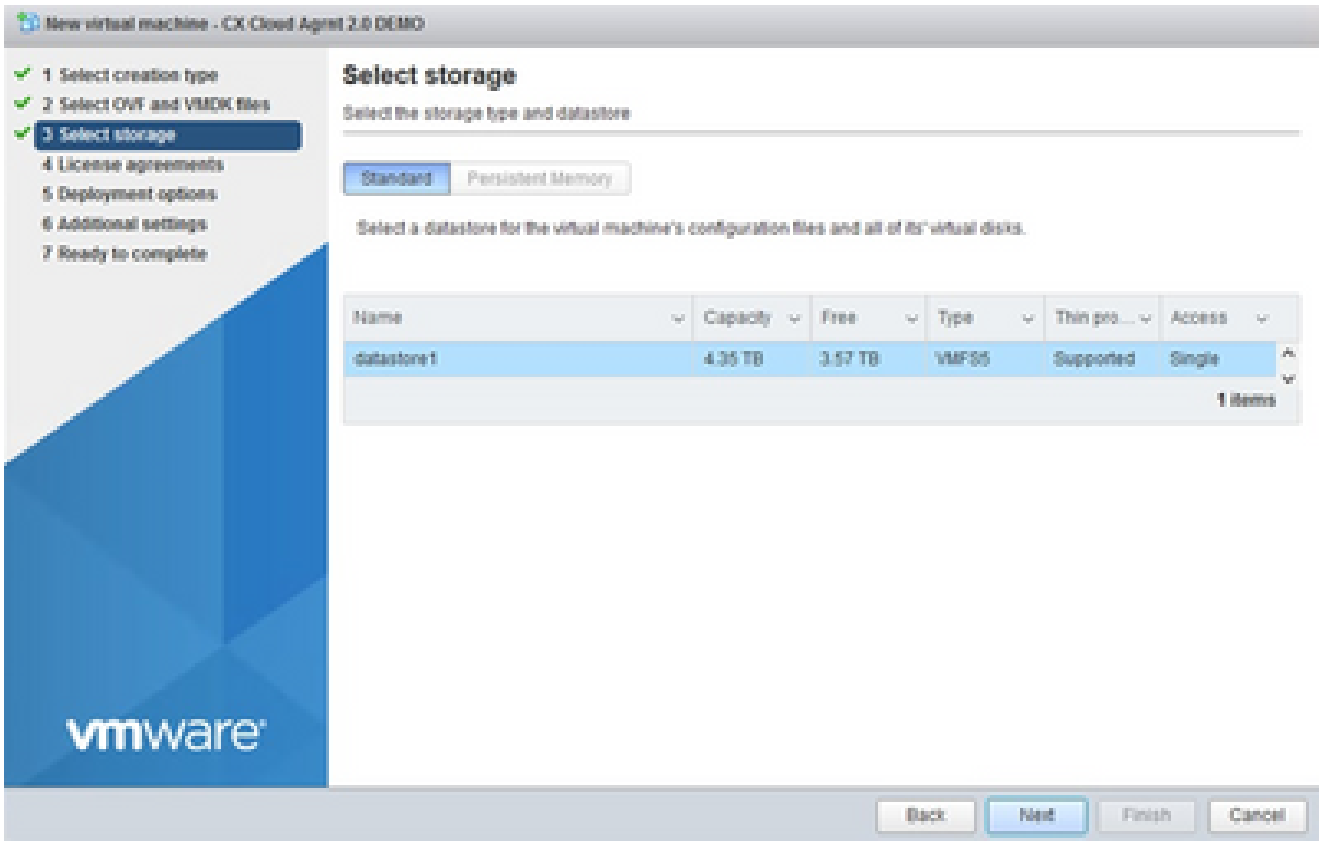
Selecionar Recurso do Computador

8. Analise os detalhes e clique em Avançar.



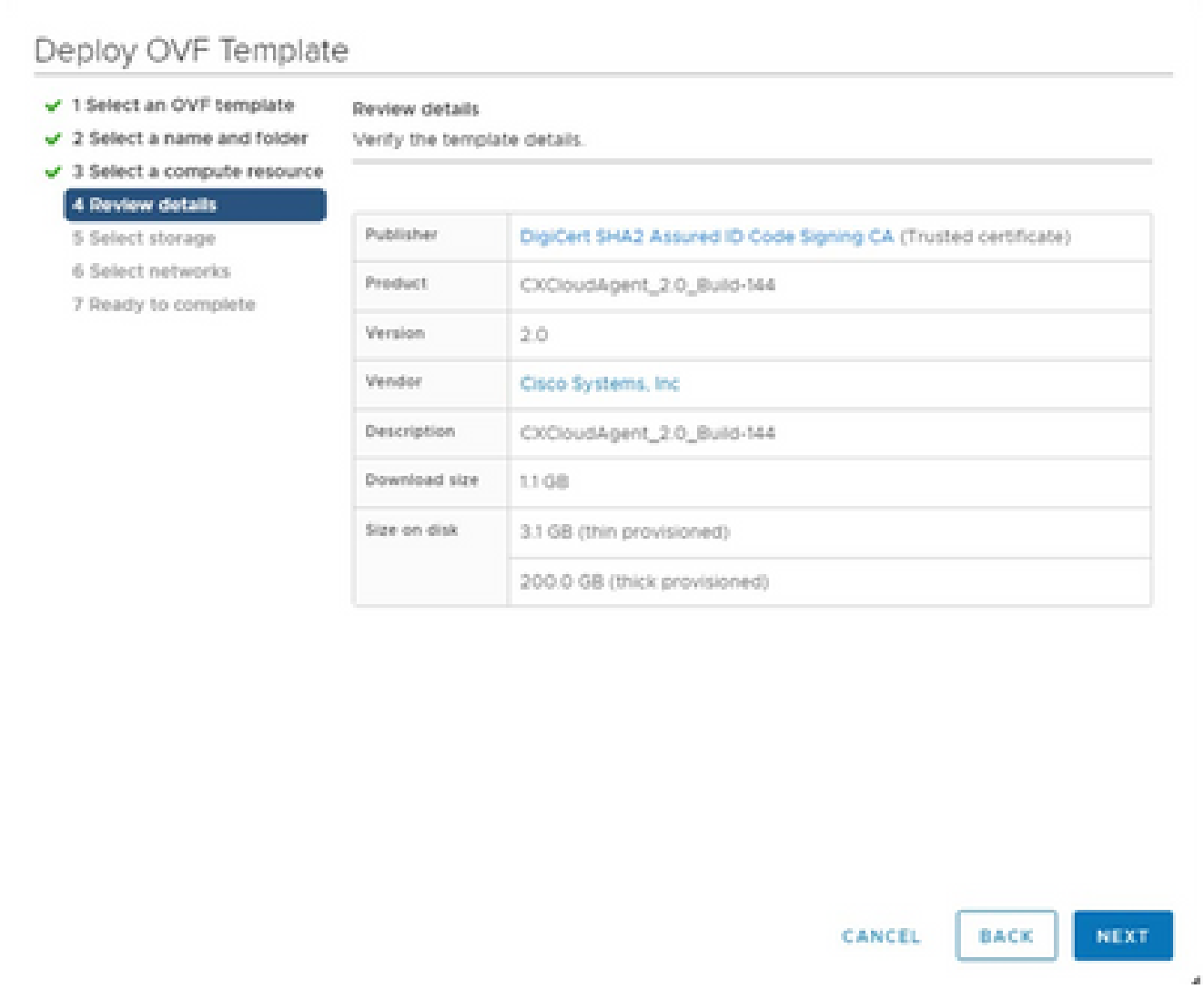
Analisar detalhes

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



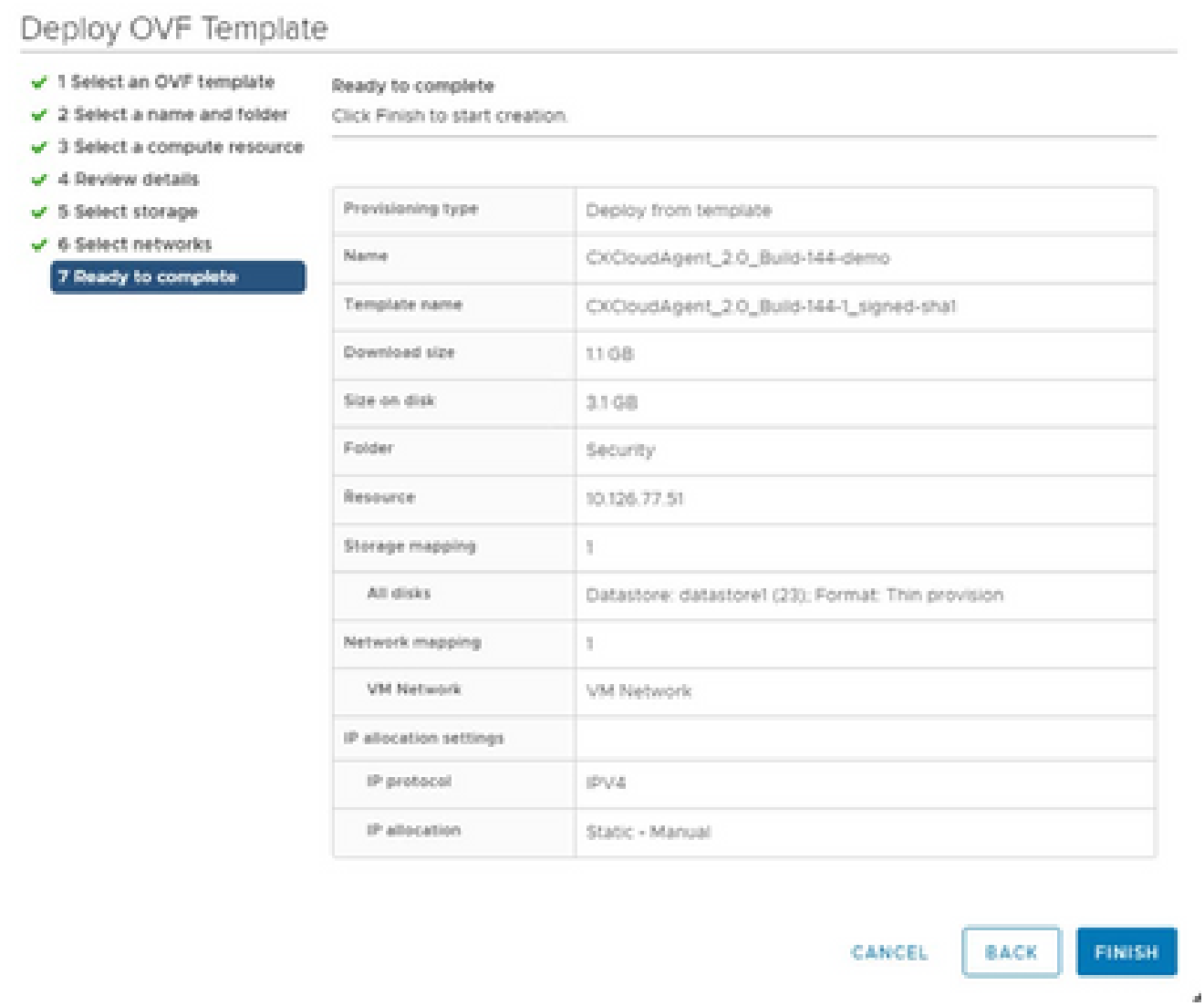
Selecionar armazenamento

10. Clique em Next.



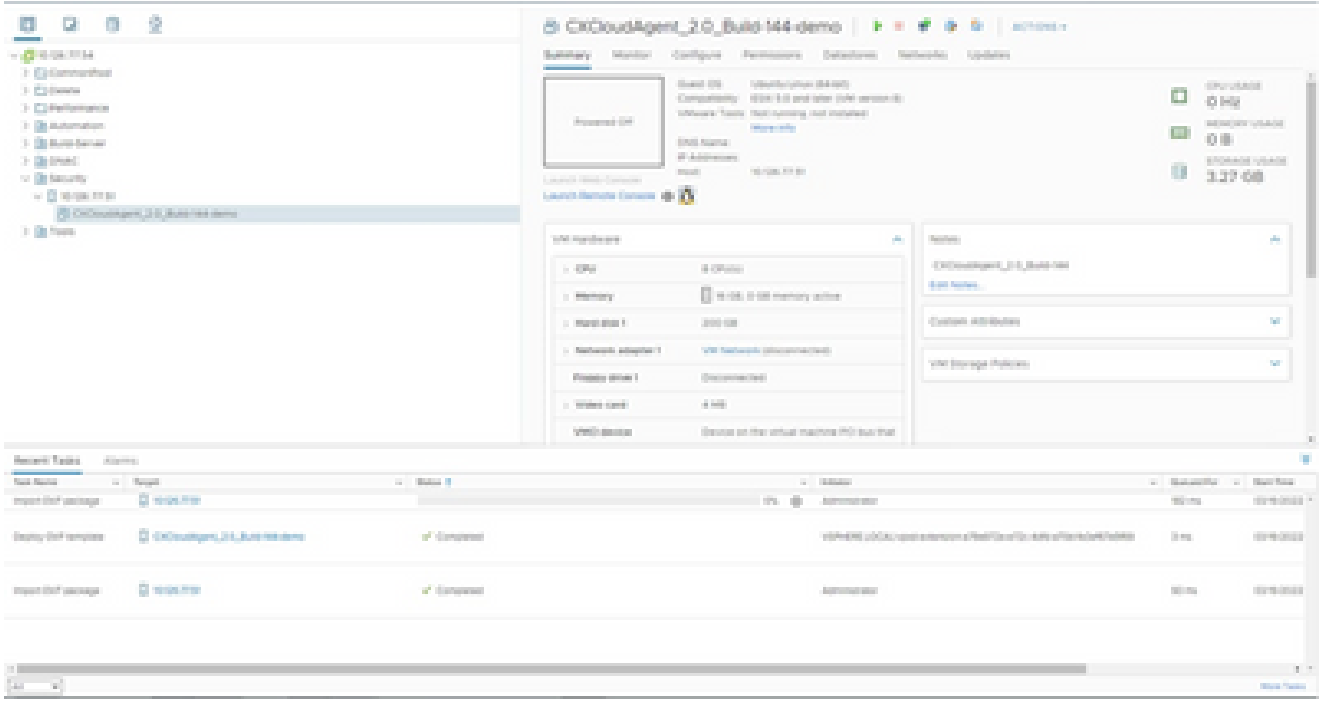
Selecionar rede

11. Clique em Finish.



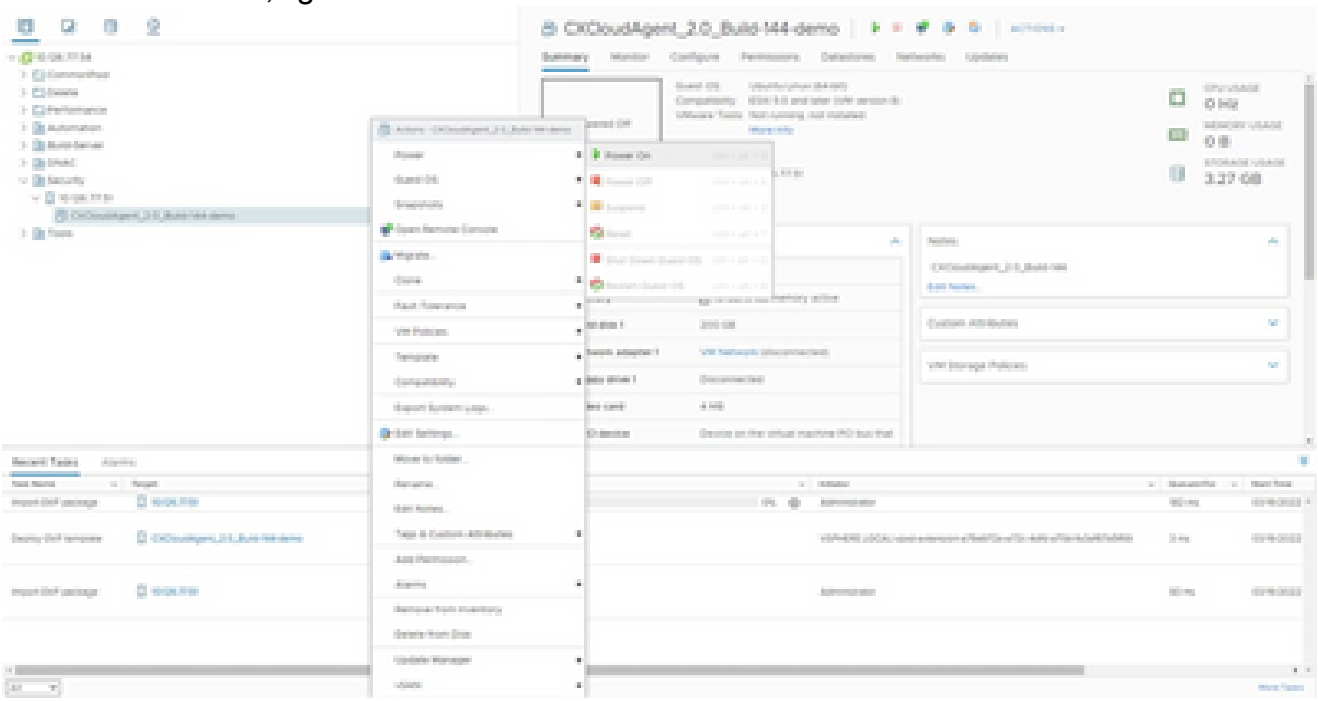
Pronto para concluir

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



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.

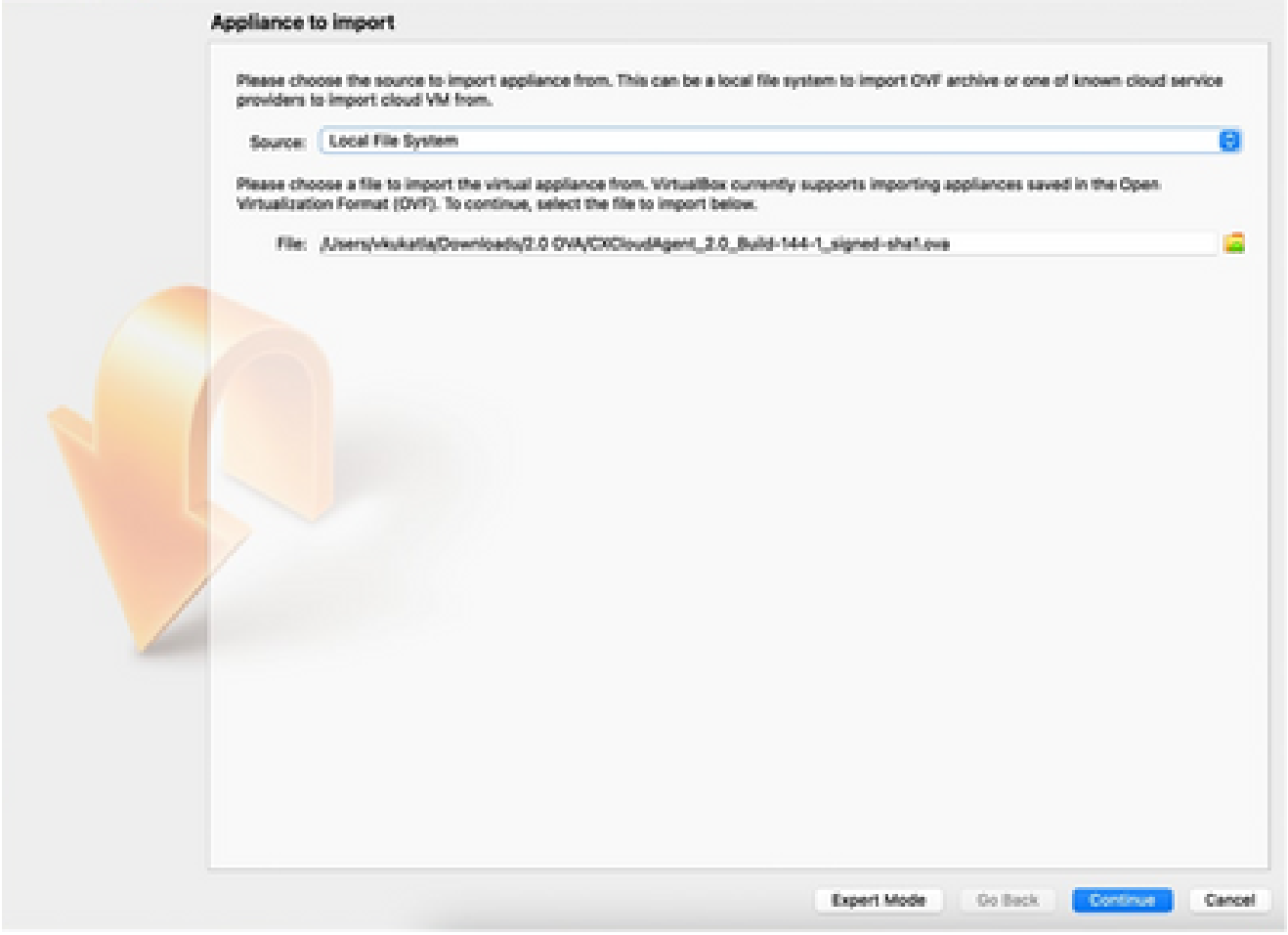
Instalação do Oracle Virtual Box 5.2.30

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.

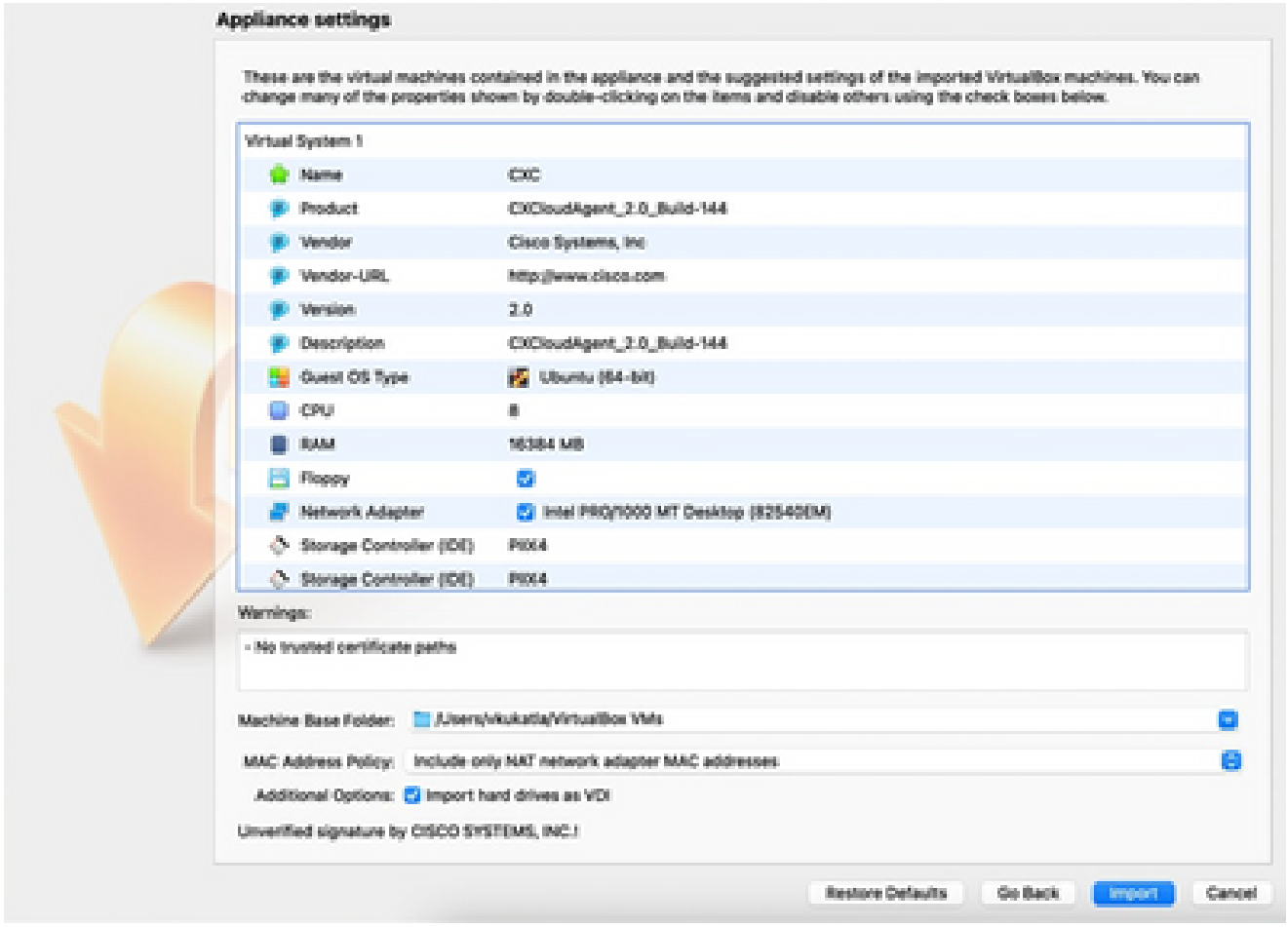
Oracle VM

2. Navegue para importar o arquivo de OVA.



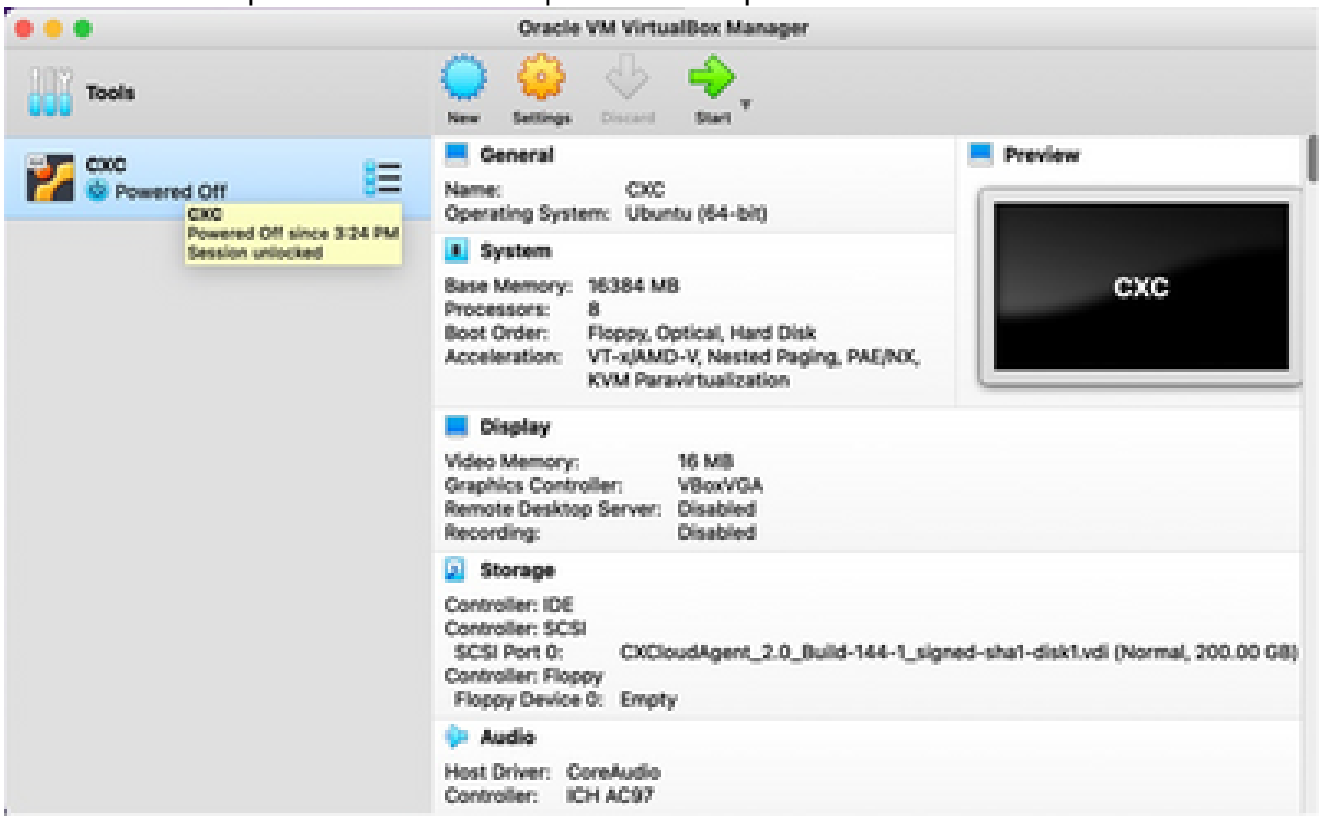
Selecionar arquivo

3. Clique em Importar.

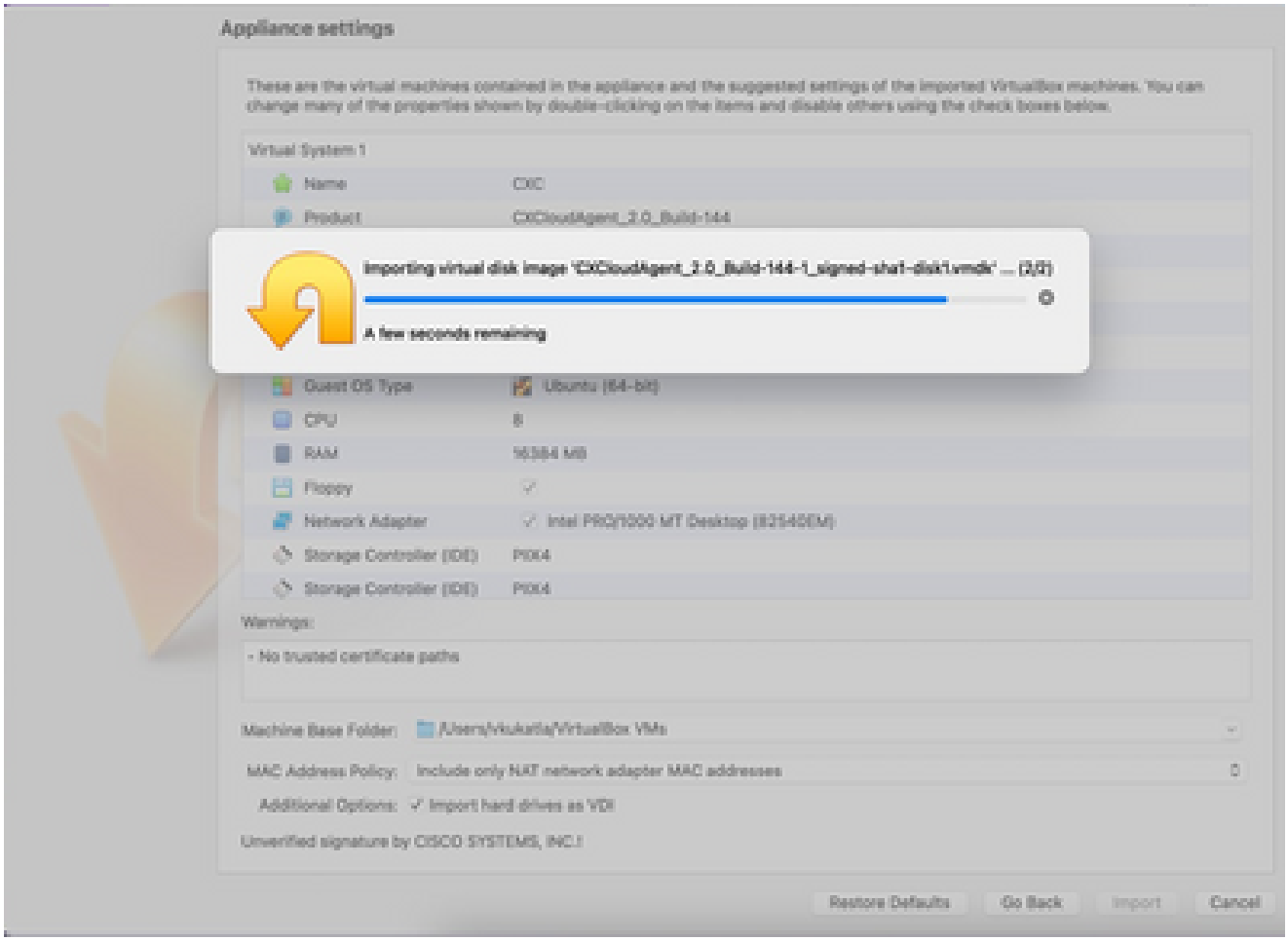


Importar arquivo

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

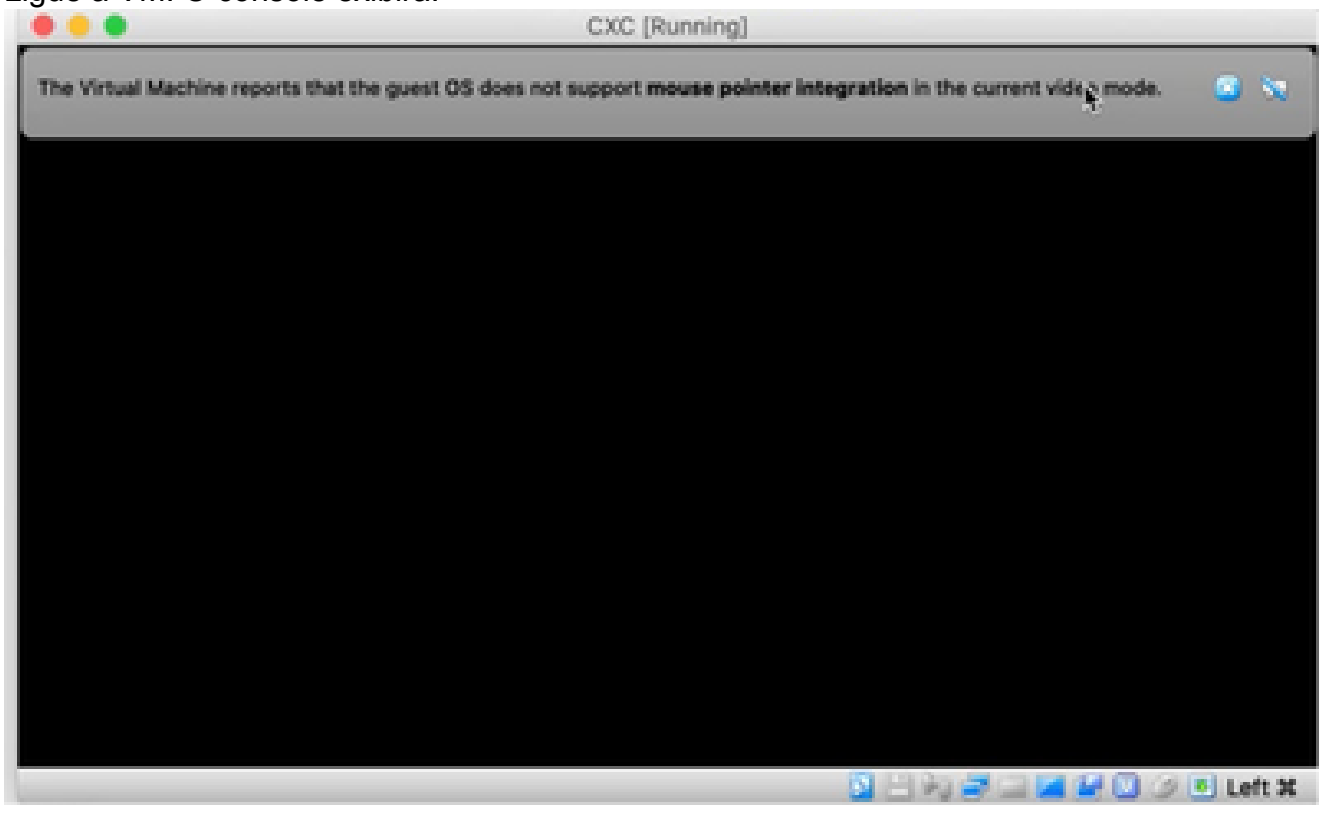


Inicialização do console da VM



Importação em andamento

5. Ligue a VM. O console exibirá.



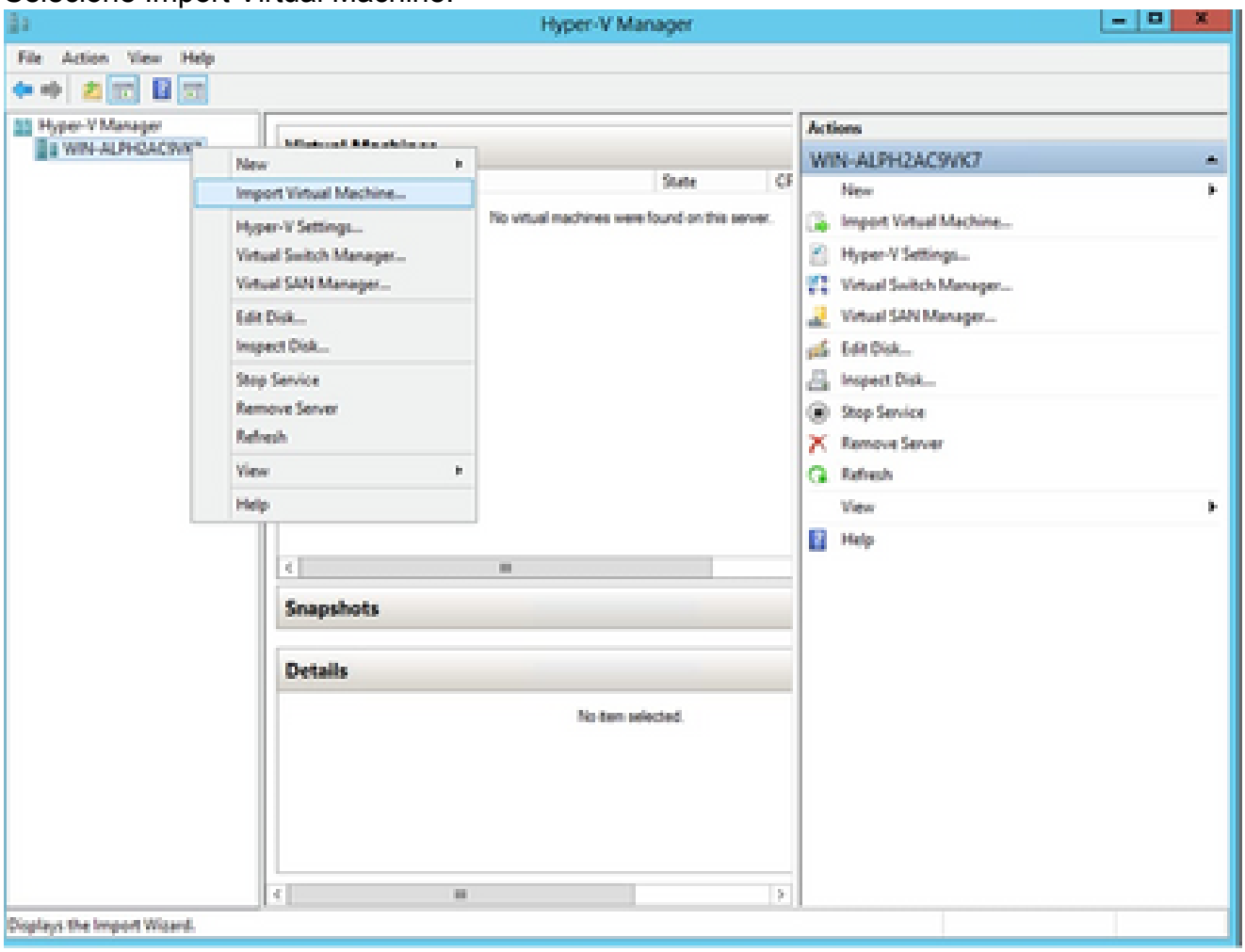
Abrir console

6. Navegue até Network Configuration para continuar com as próximas etapas.

Instalação do Microsoft Hyper-V

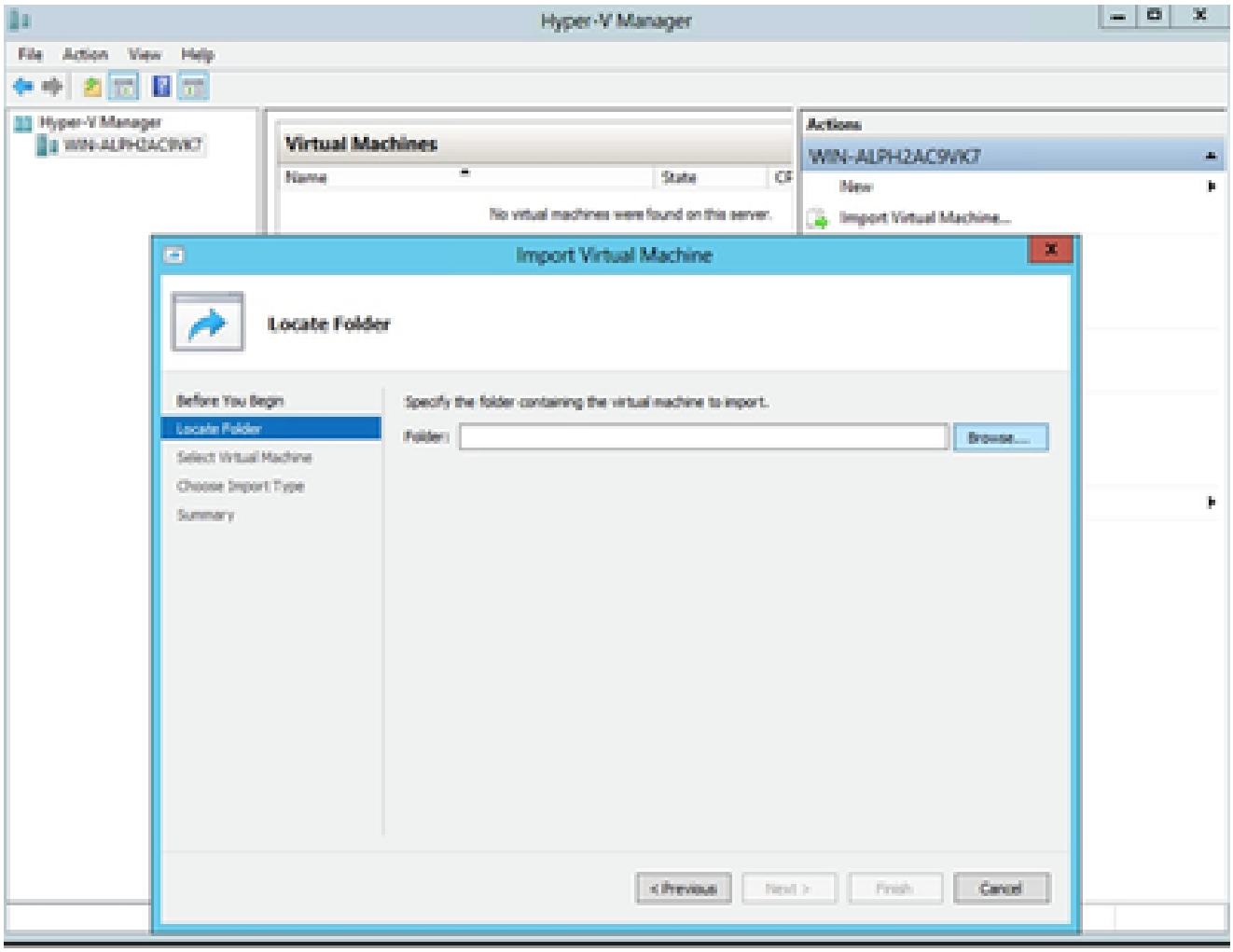
Execute o seguinte:

1. Selecione Import Virtual Machine.



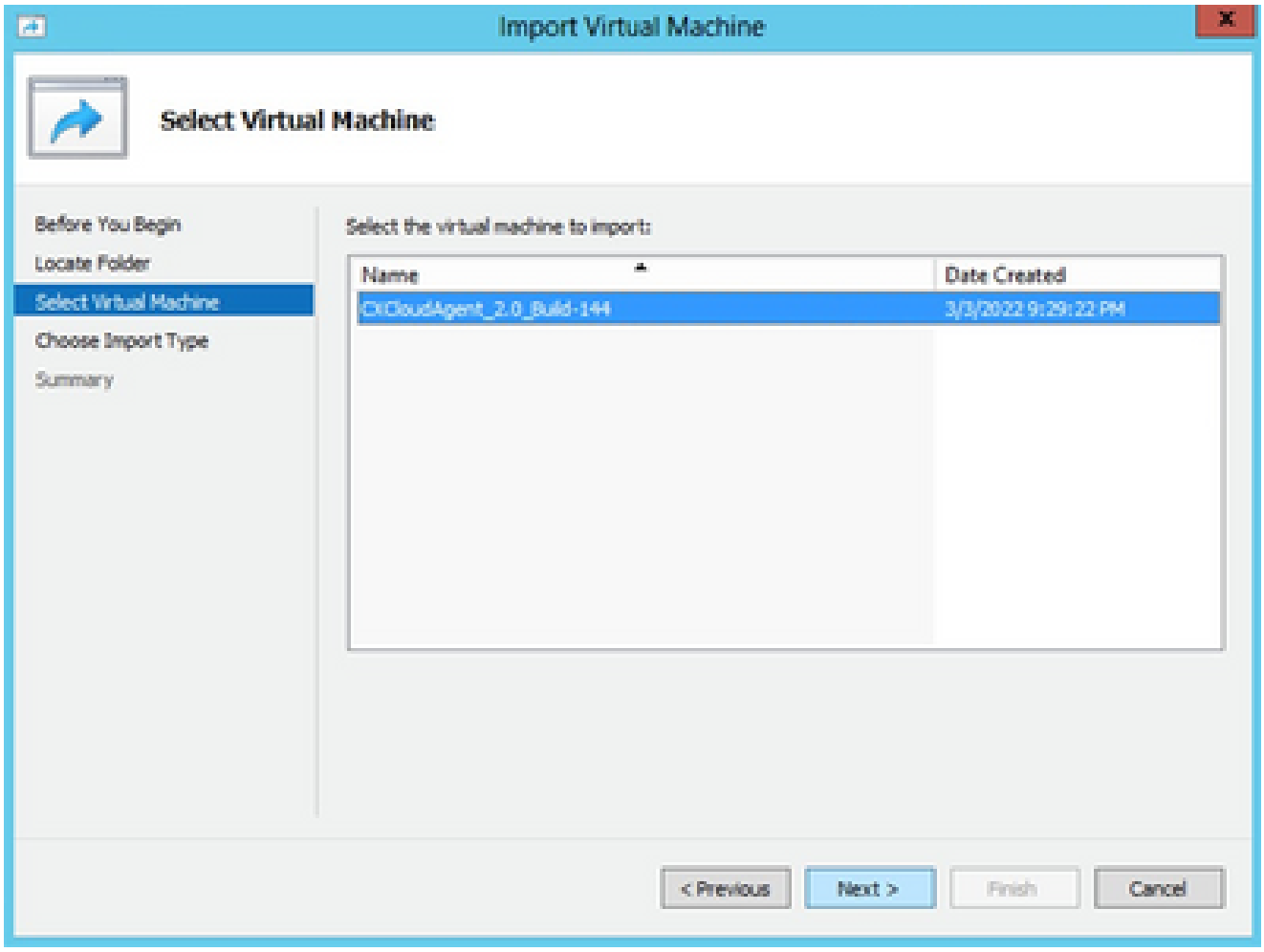
Gerenciador Hyper V

2. Procure e selecione a pasta de download.
3. Clique em Next.



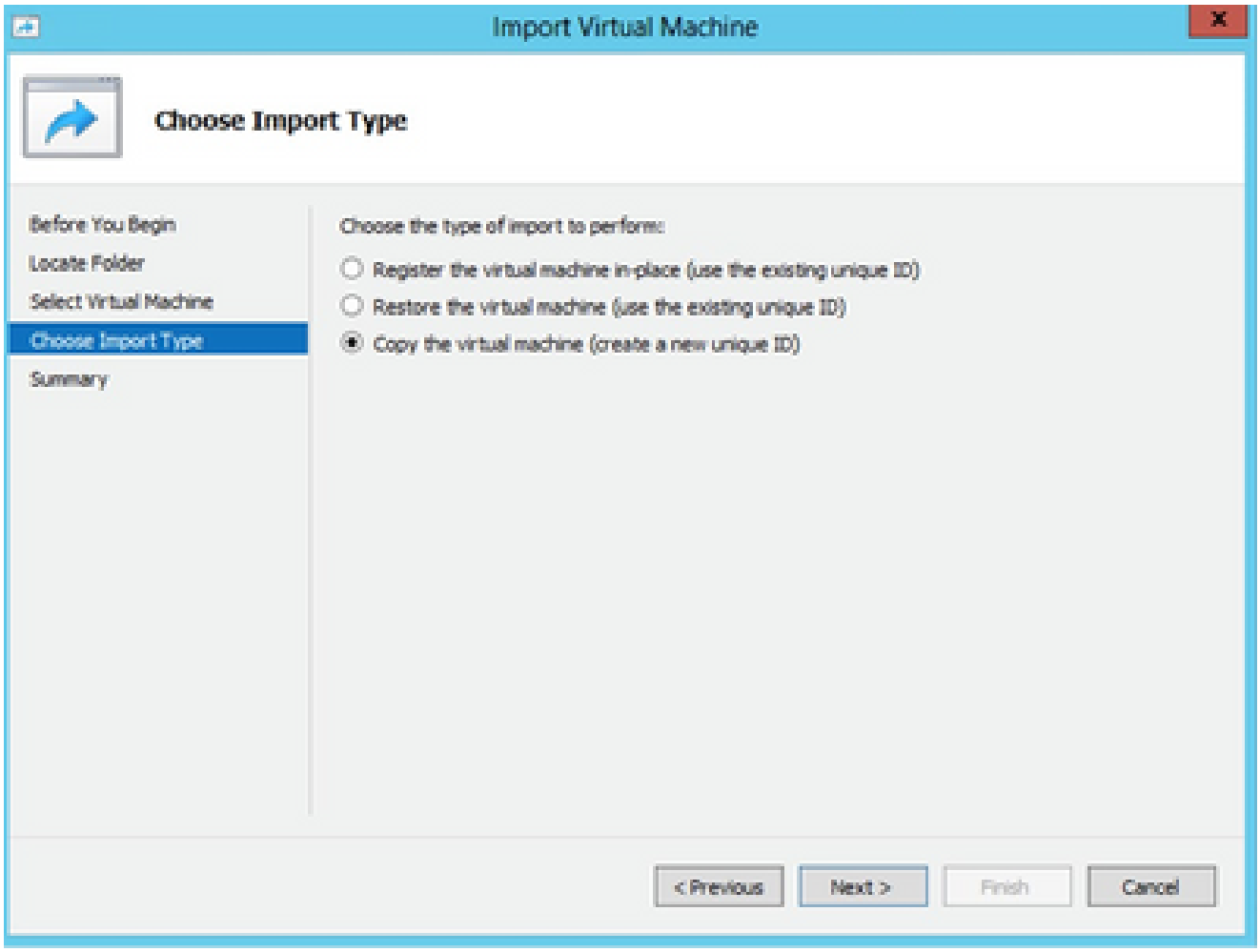
Pasta para importar

4. Selecione a VM e clique em Avançar.



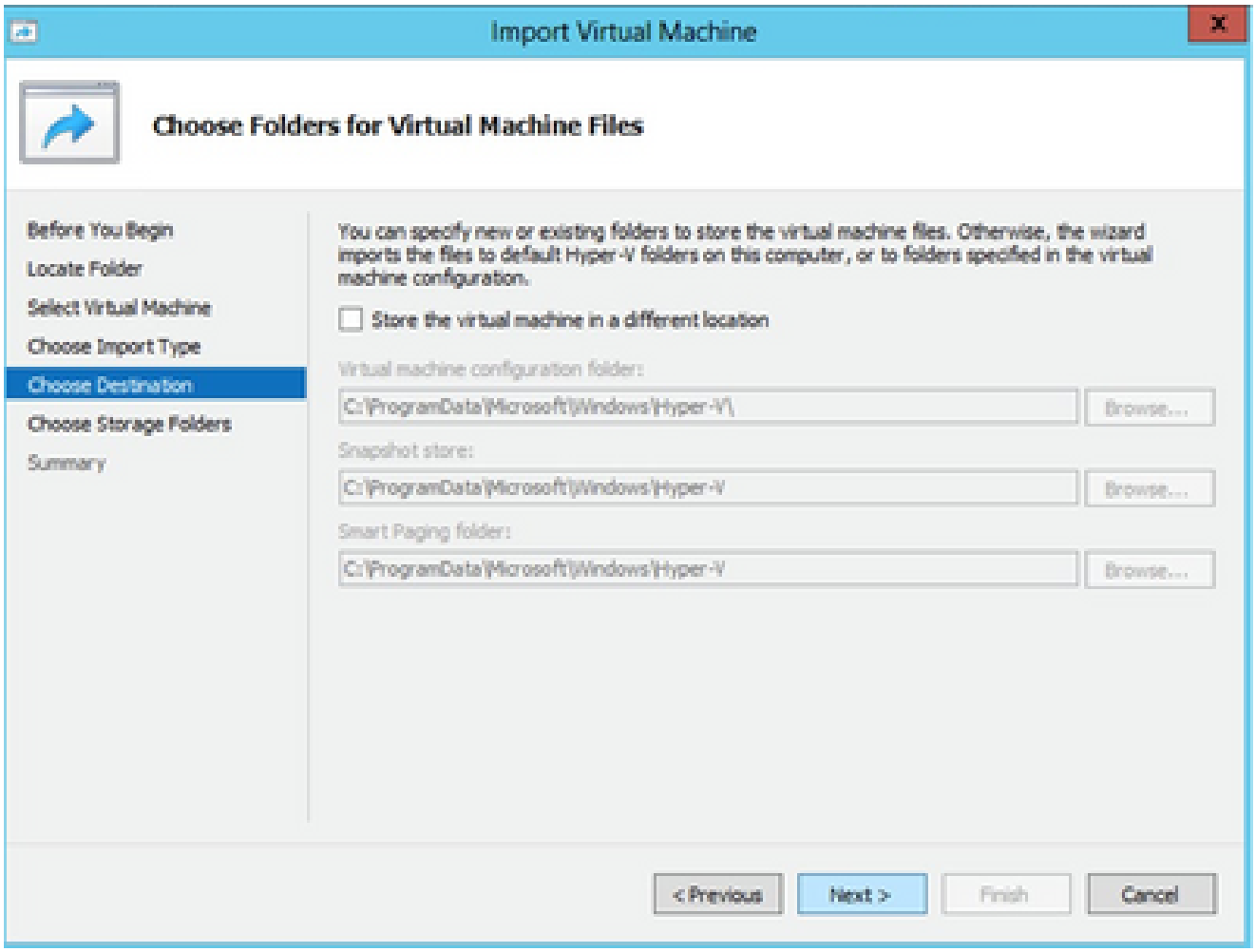
Selecionar VM

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.



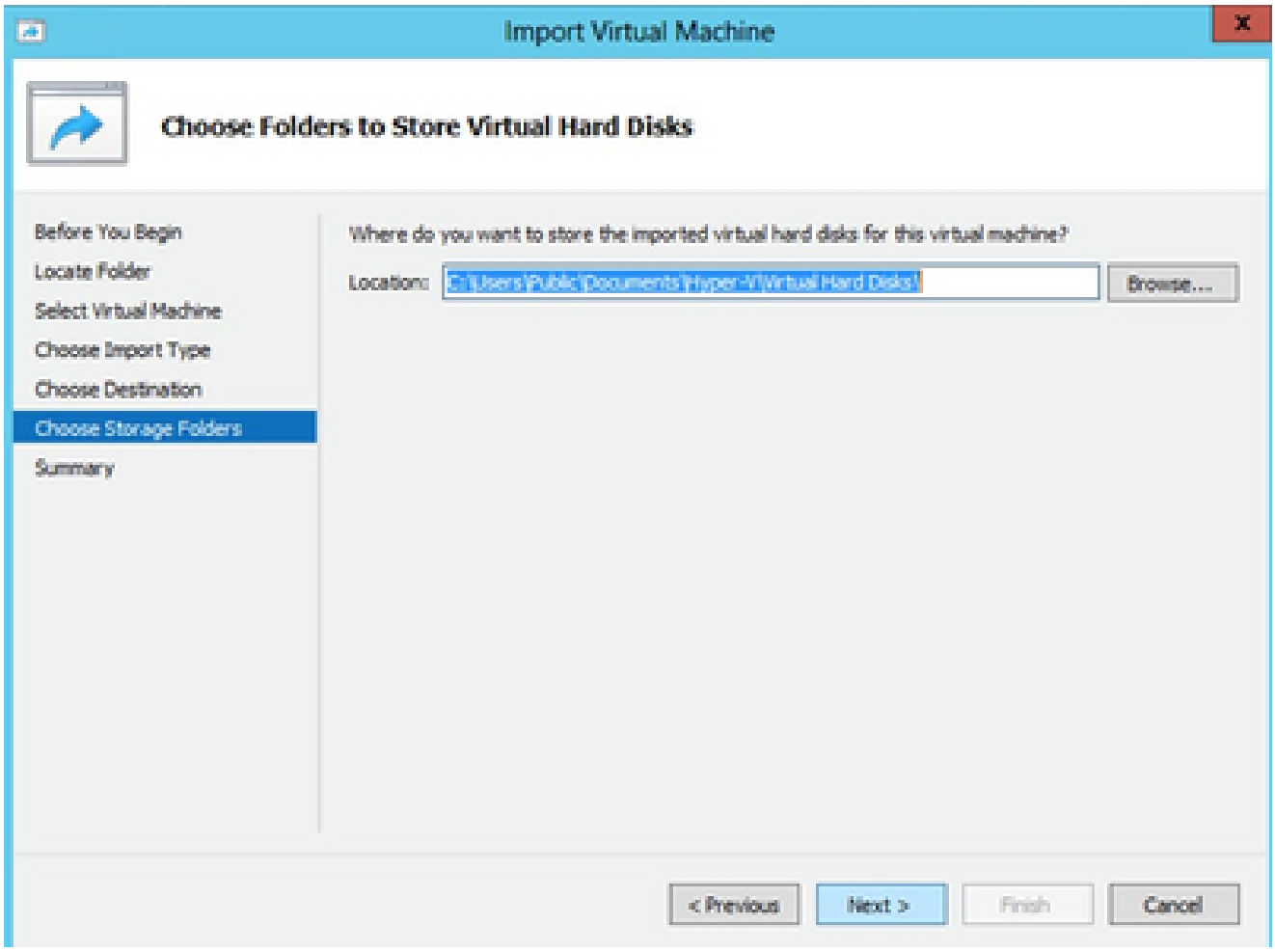
Tipo de importação

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



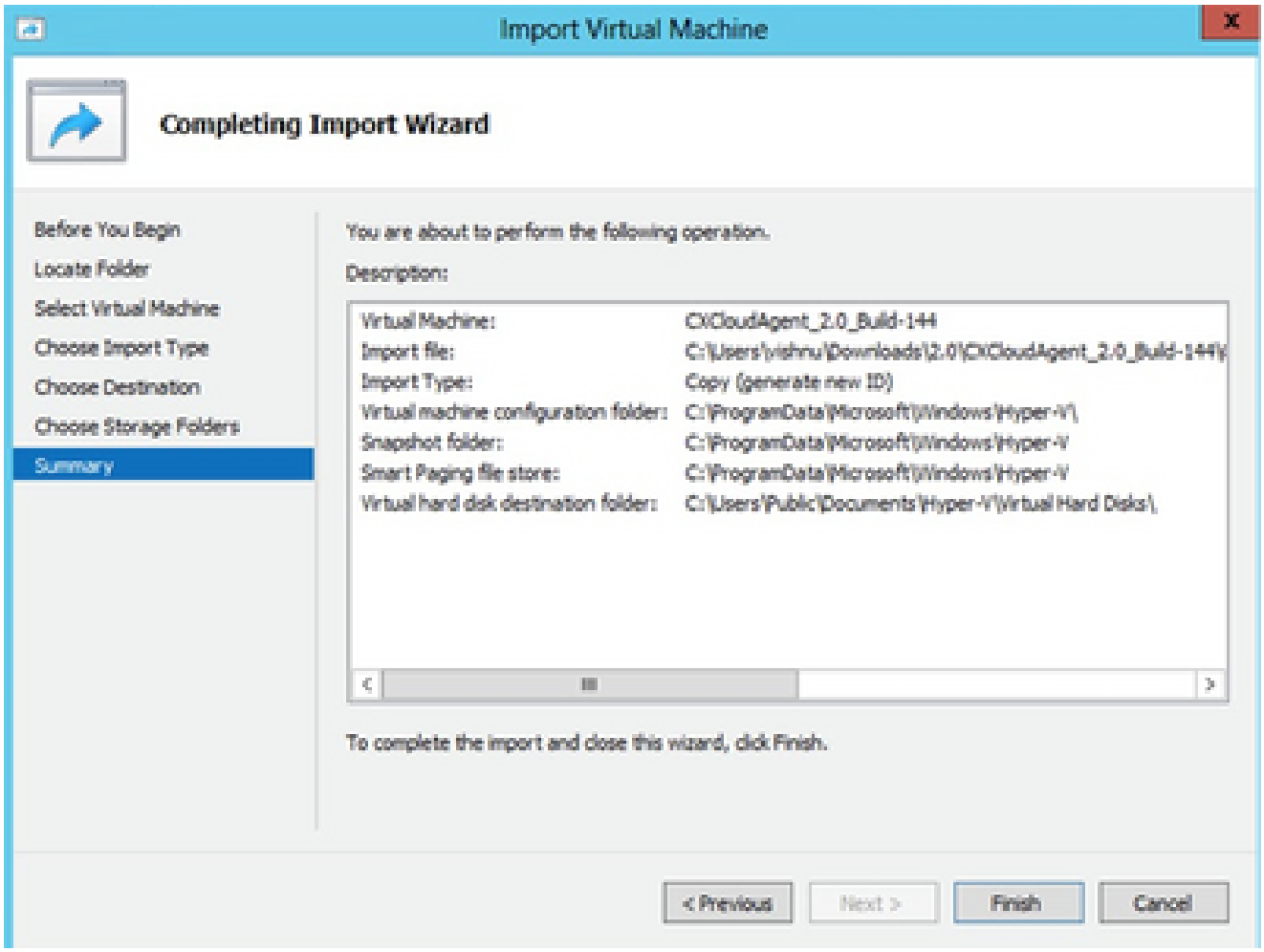
Escolher Pastas para Arquivos de Máquina Virtual

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



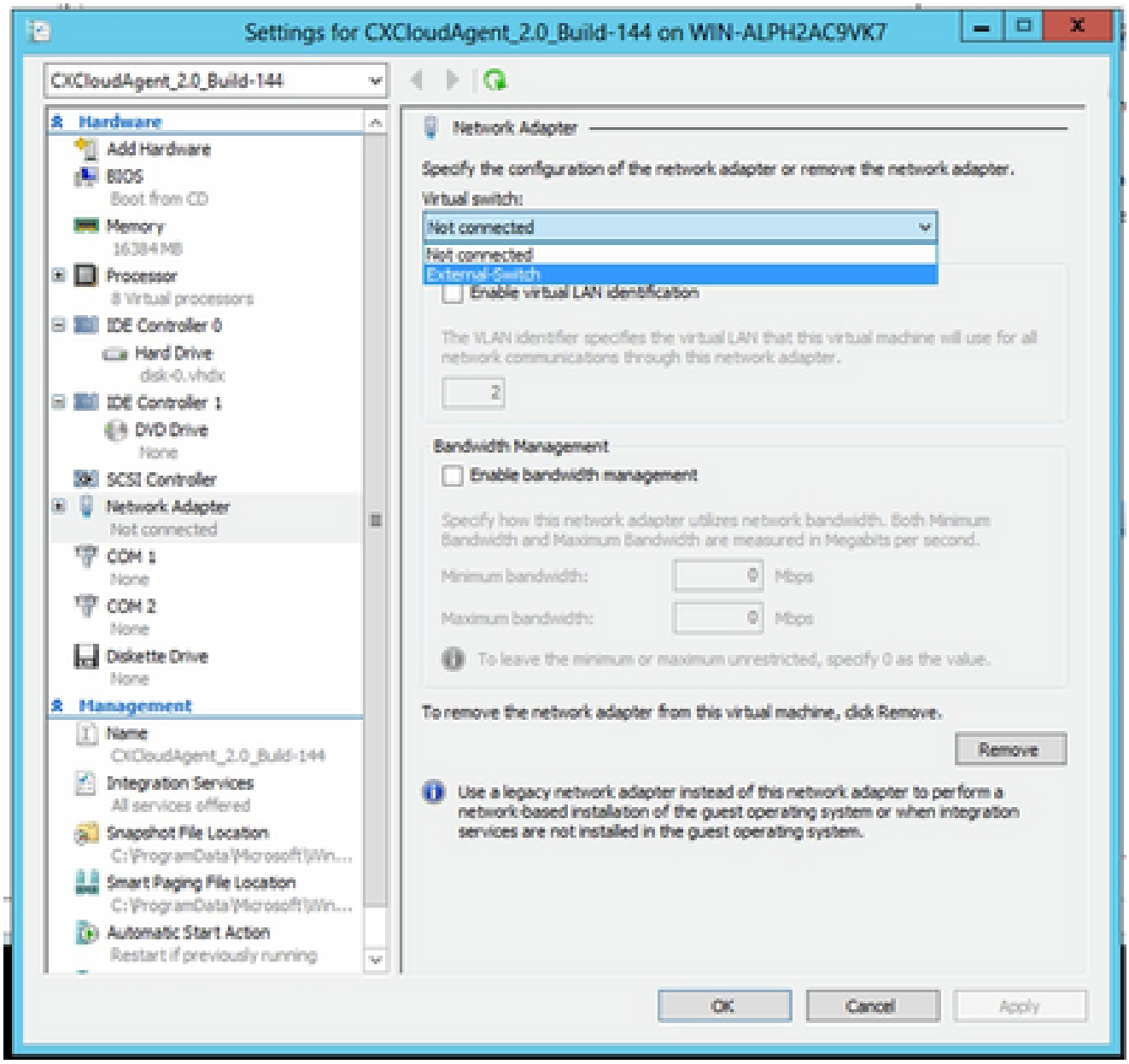
Pasta para armazenar os discos rígidos virtuais

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



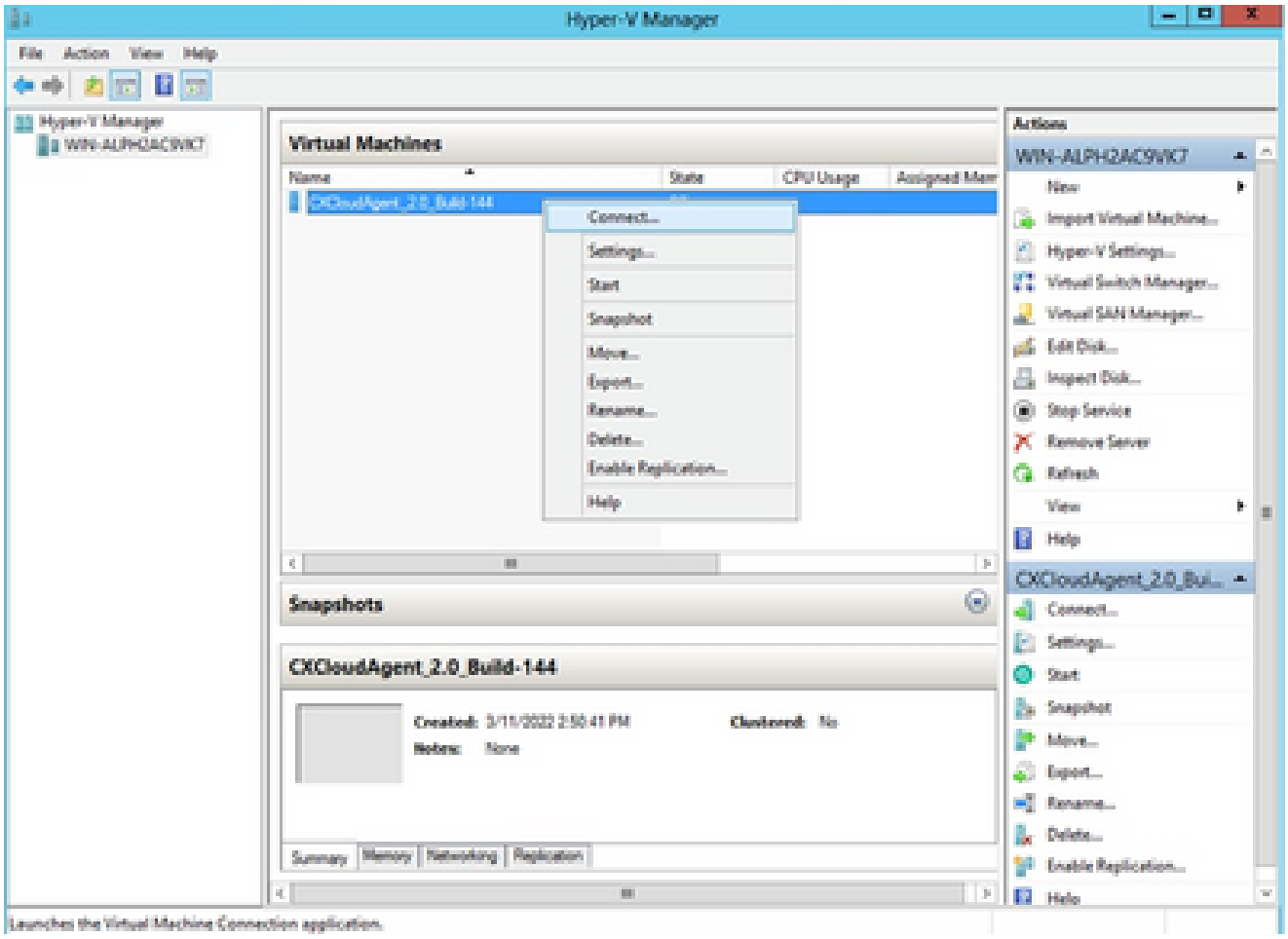
Summary

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. Selecione Connect para iniciar a VM.

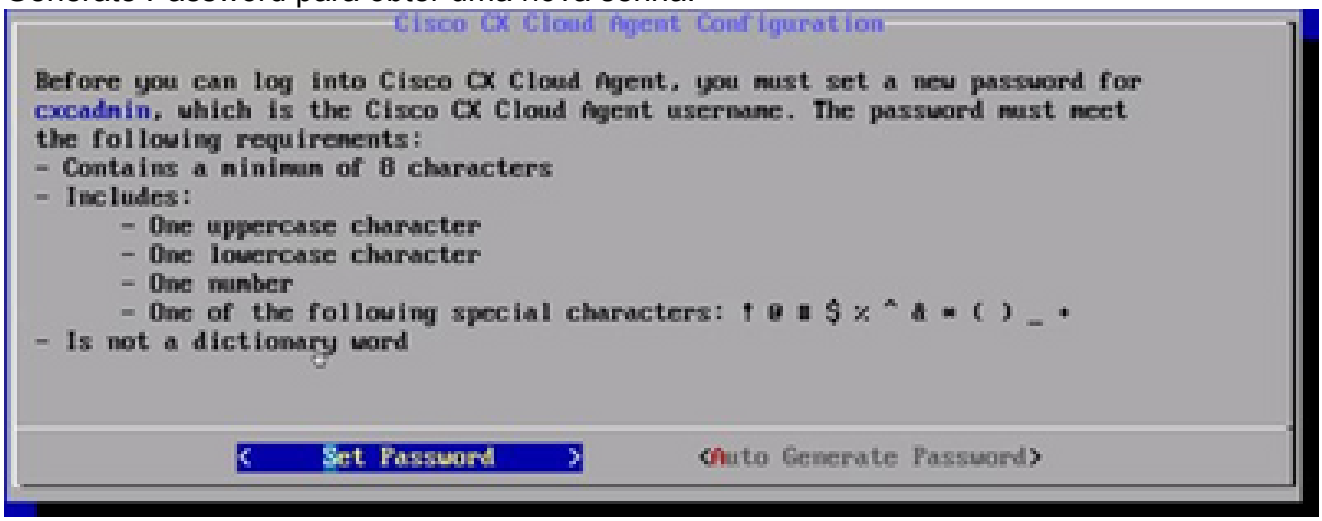


Inicialização da VM

14. Navegue até Network Configuration para continuar com as próximas etapas.

Configuração de rede

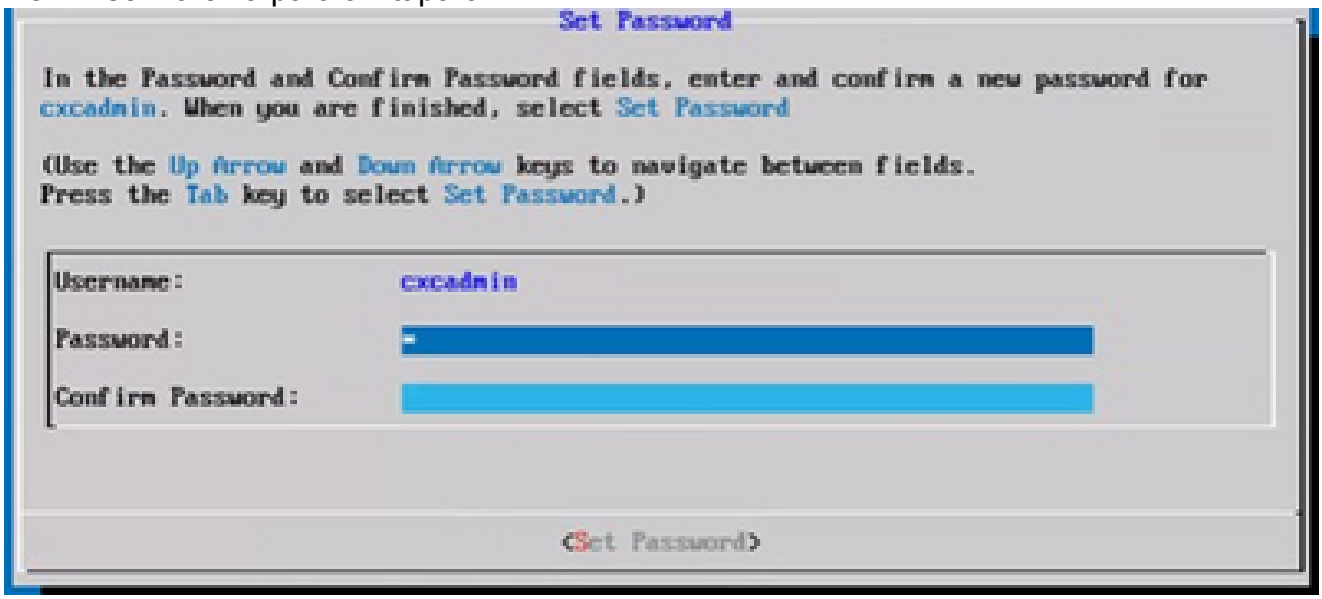
1. Clique em Set Password para adicionar uma nova senha para cxcadmin OU clique em Auto Generate Password para obter uma nova senha.



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.



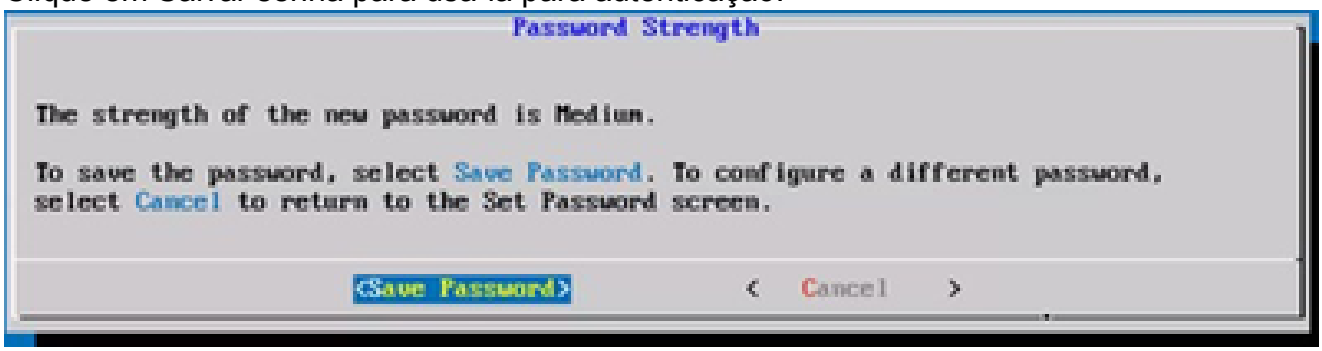
Nova senha

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.

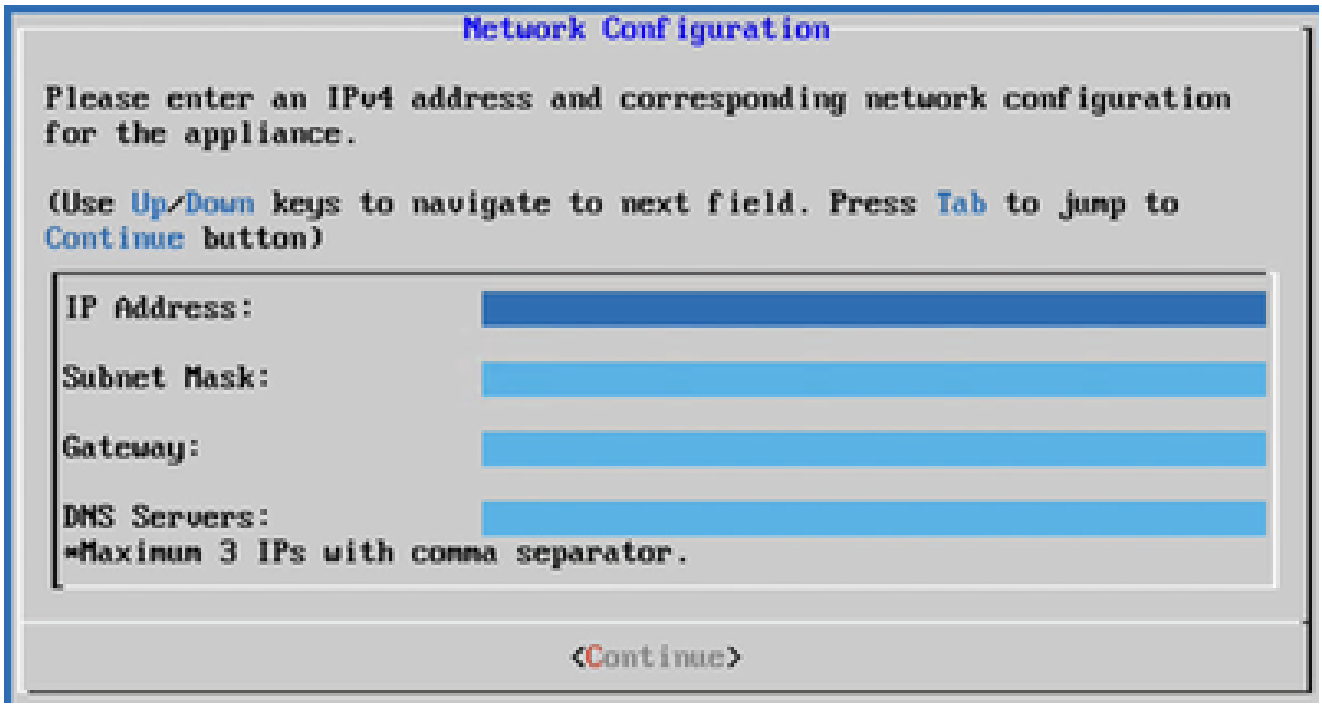
Senha gerada automaticamente

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.

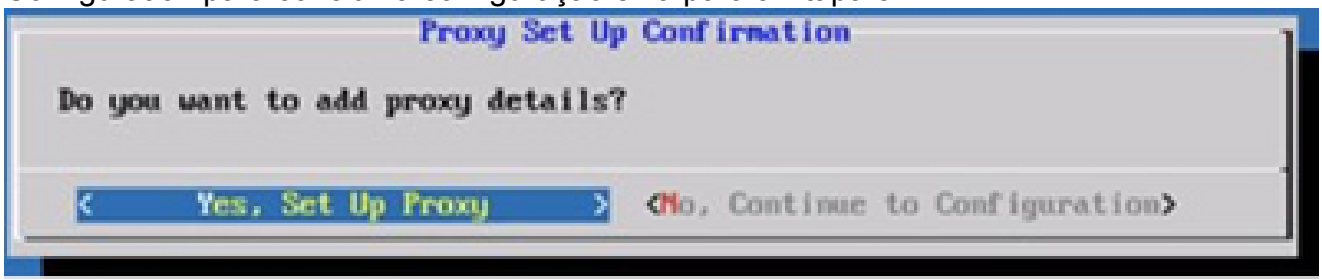


Configuração de rede

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

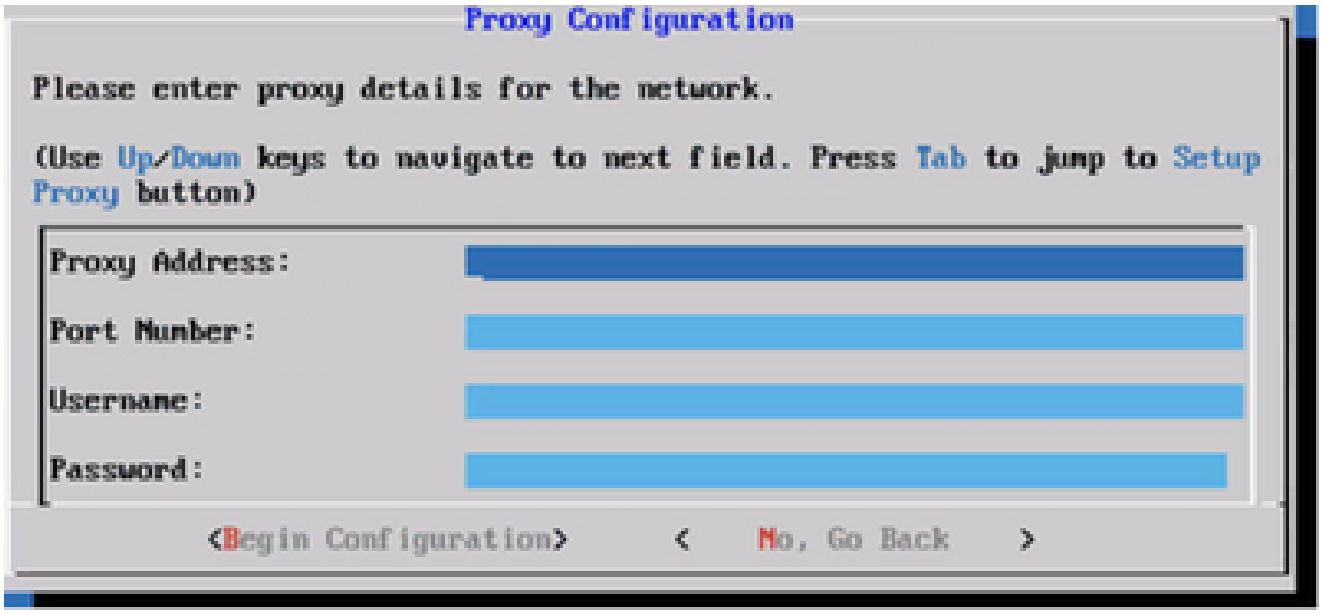
Configuração

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.



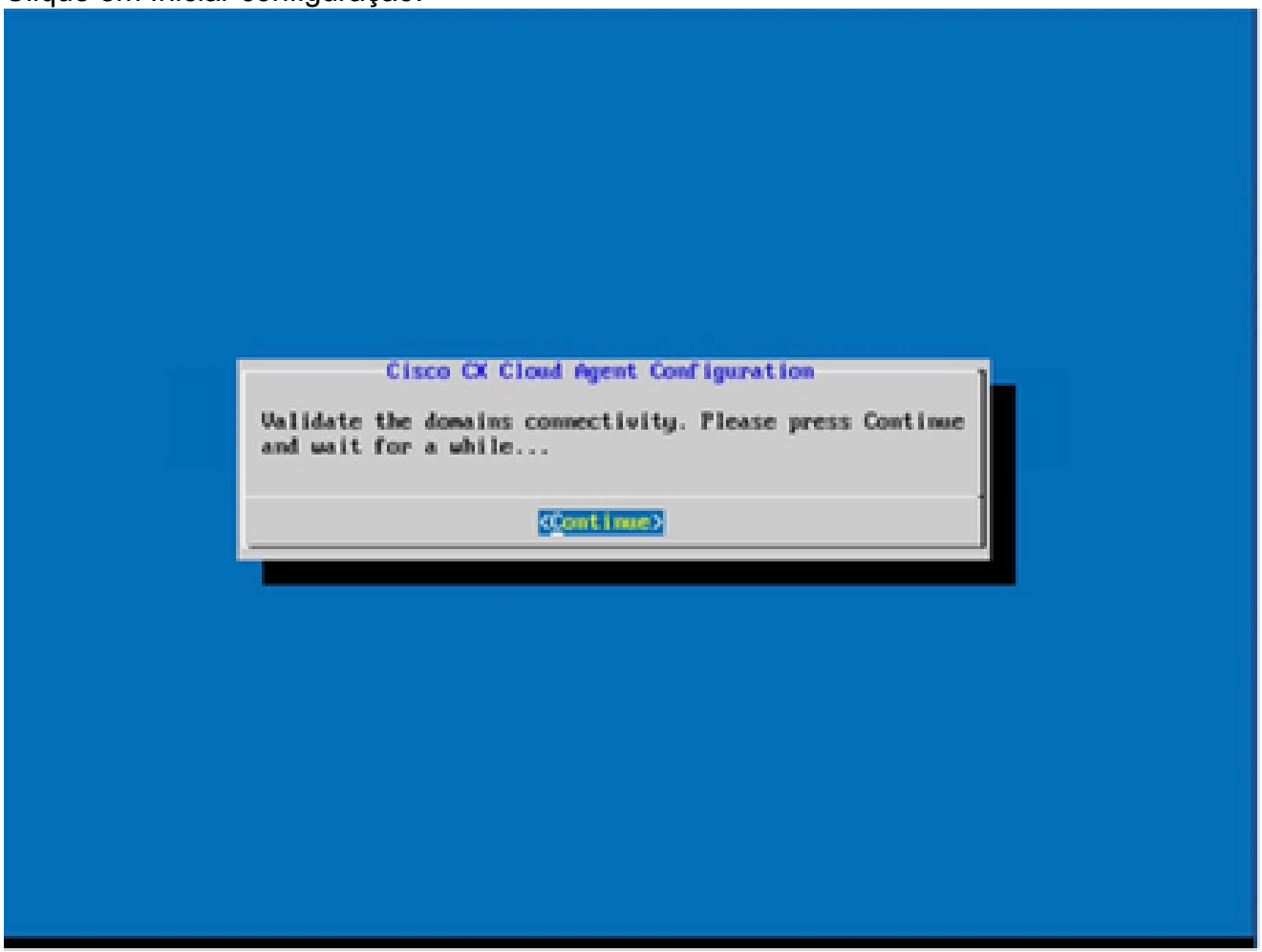
Instalação de proxy

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



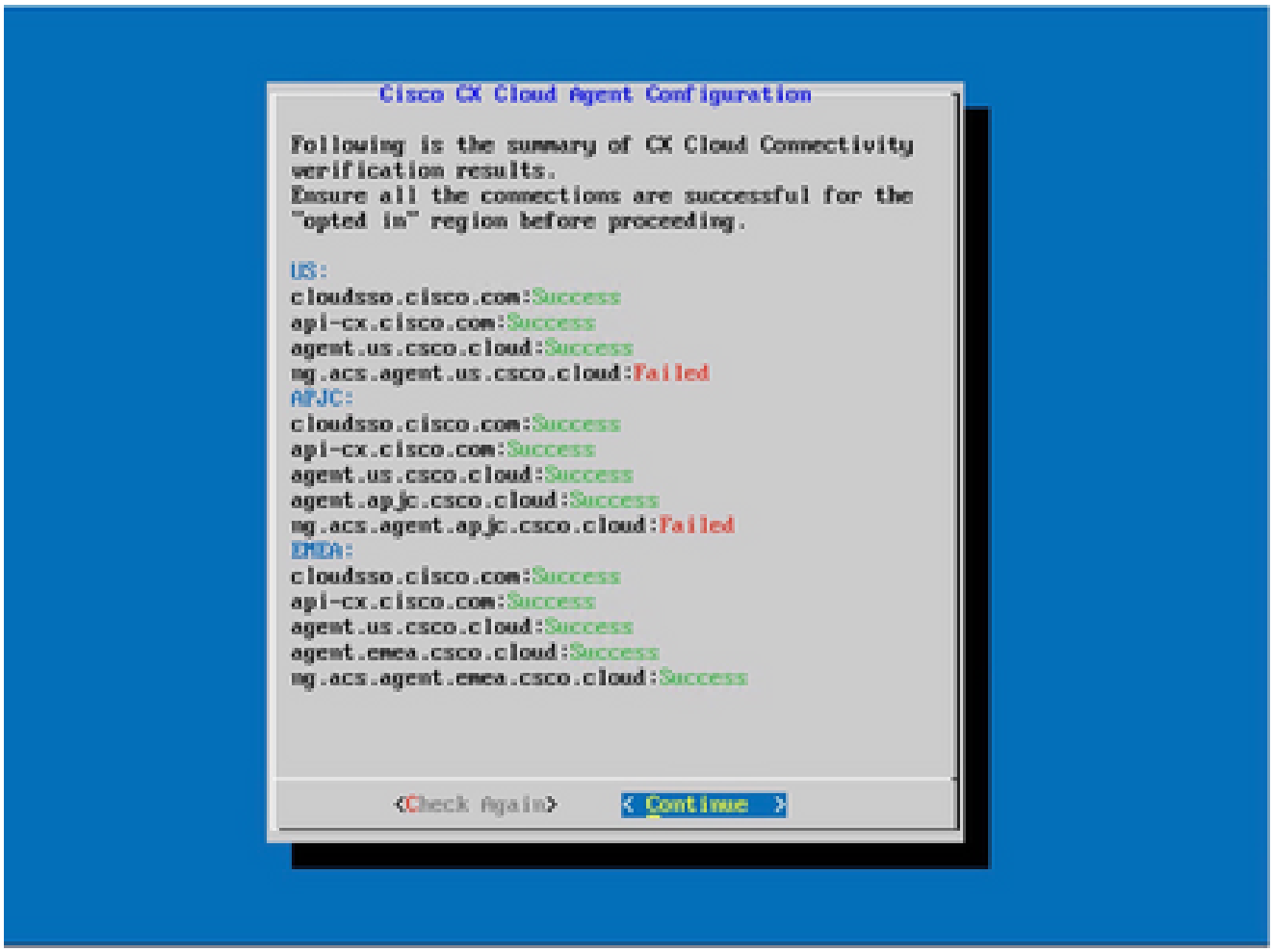
Configuração de proxy

8. Clique em Iniciar configuração.



Configuração inicial

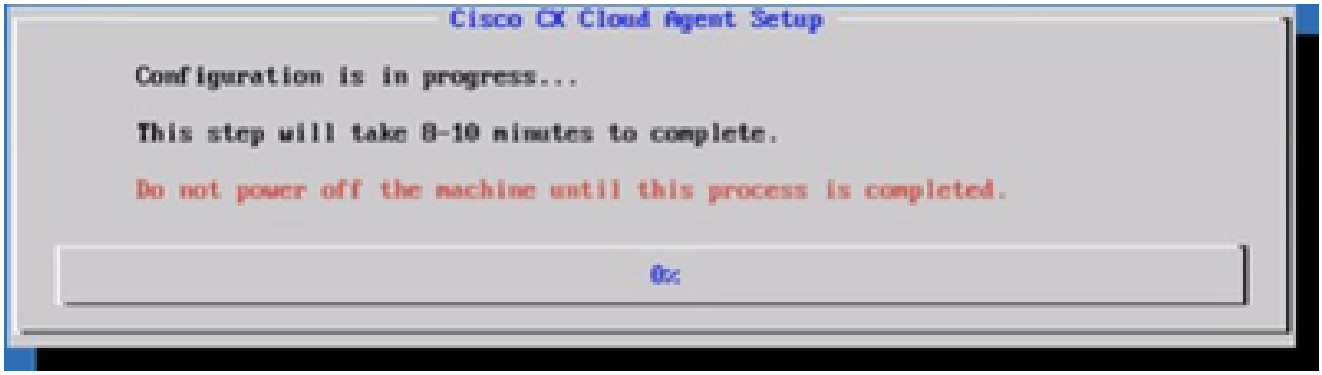
9. Clique em Continuar.



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.

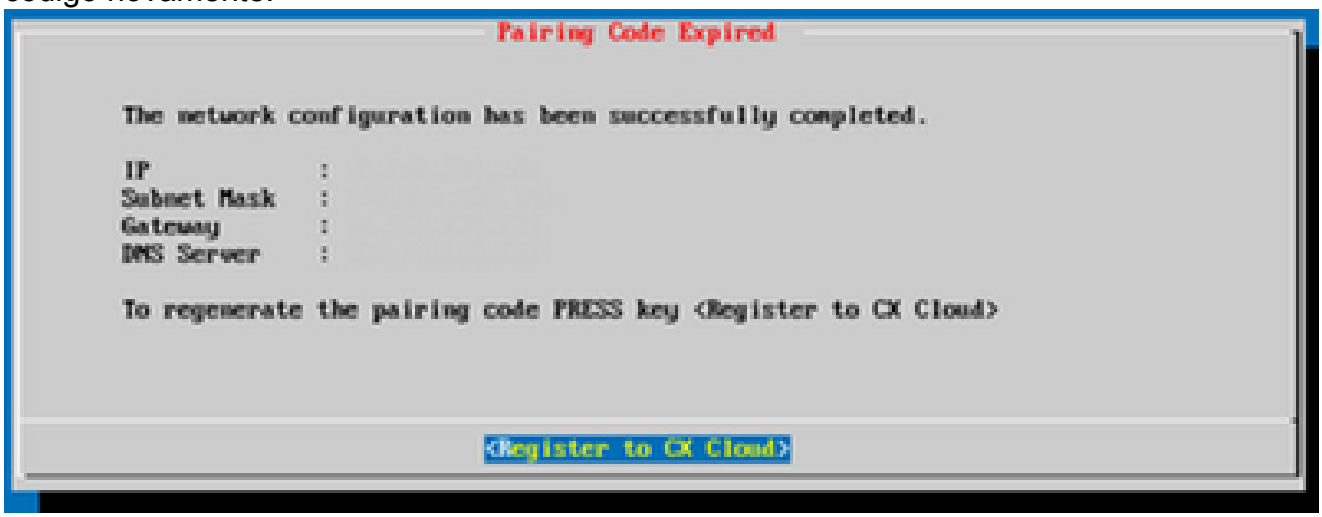


Configuração em andamento

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

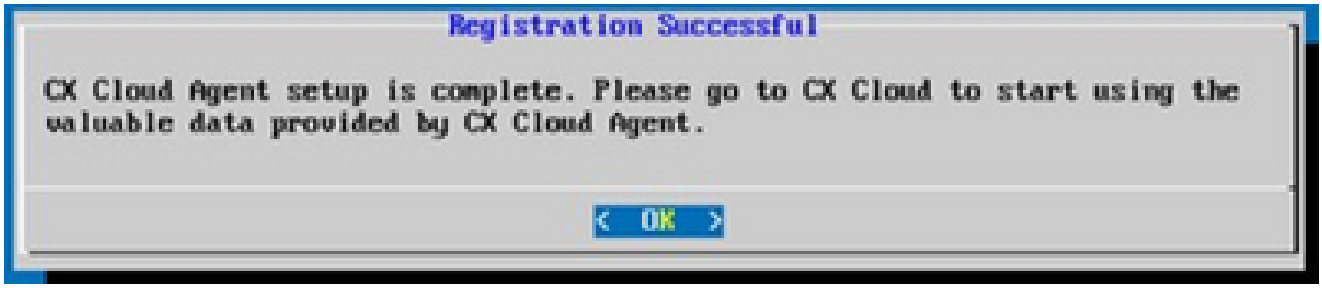
Código de emparelhamento

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



Código expirado

13. Click OK.



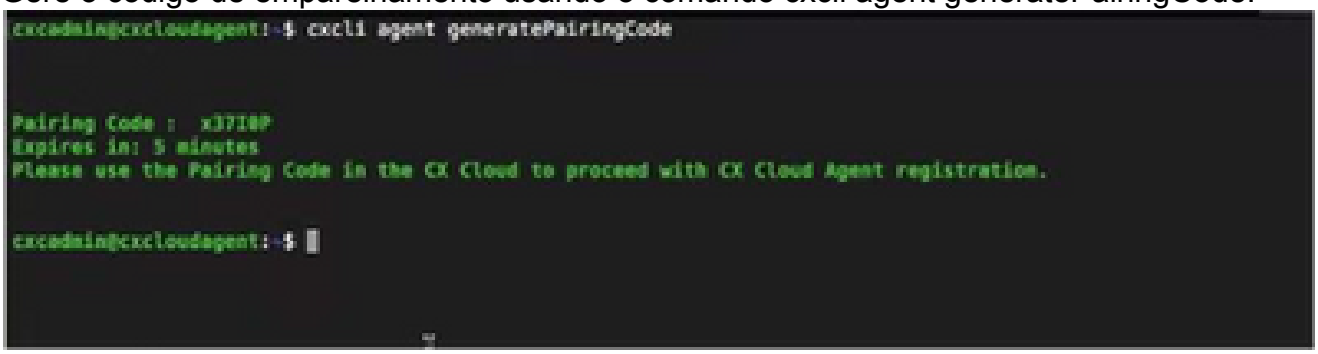
Registro realizado com sucesso

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 logon no Agente de Nuvem via SSH usando a credencial de usuário cxcadmin.
2. Gere o código de emparelhamento usando o comando cxcli agent generatePairingCode.



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

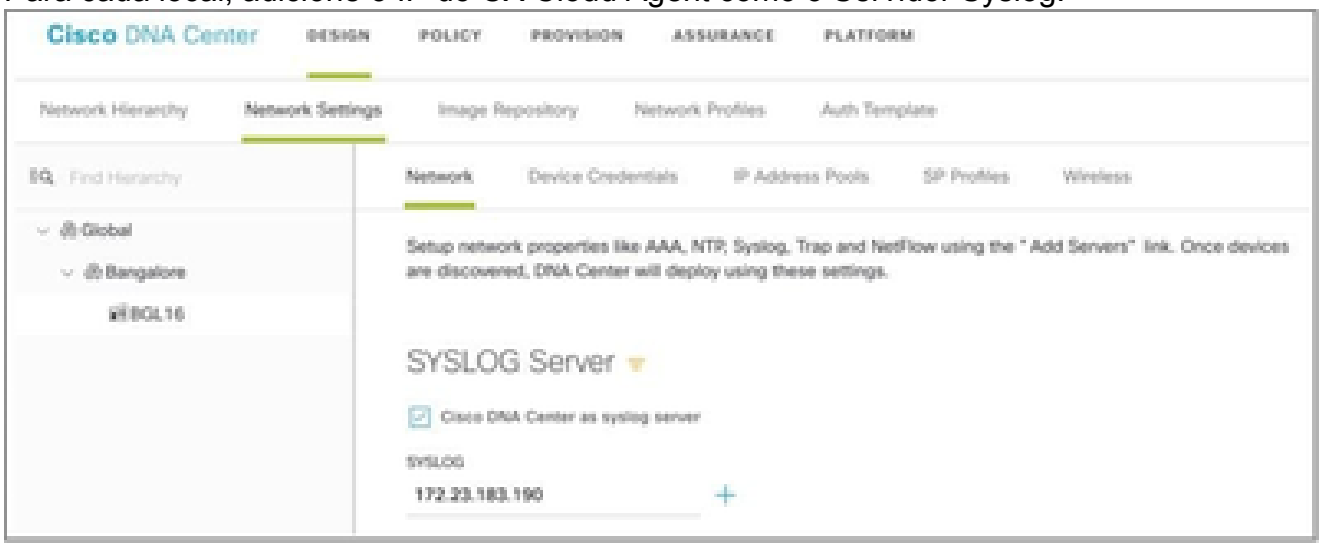
Pré-requisitos

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 as seguintes 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 a documentação a seguir para obter as etapas de configuração específicas.

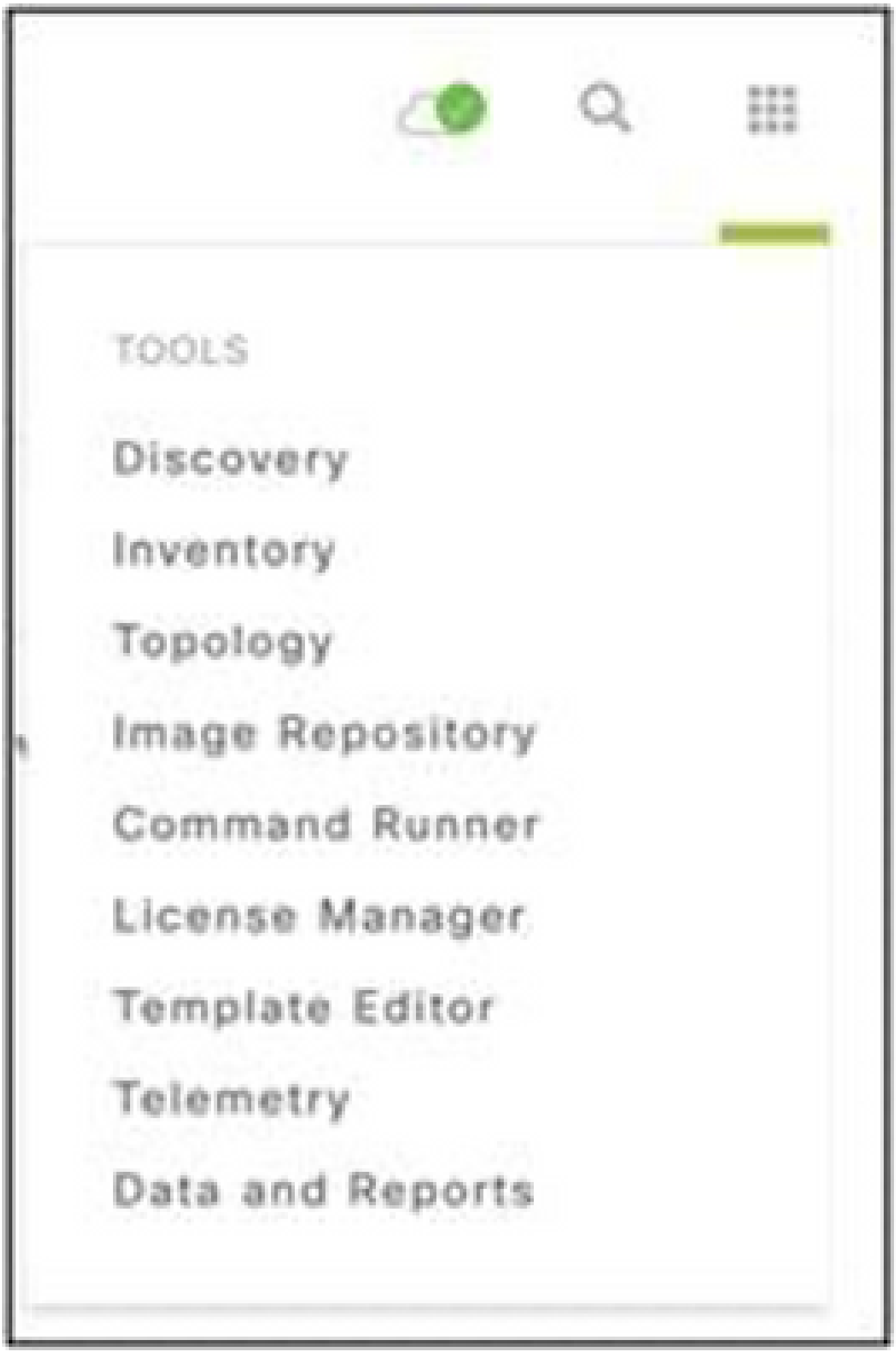
Guia de configuração do IOS-XE

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 as seguintes etapas:

1. Navegue até Ferramentas>Telemetria.


TOOLS
Discovery
Inventory
Topology
Image Repository
Command Runner
License Manager
Template Editor
Telemetry
Data and Reports

Menu Ferramentas

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

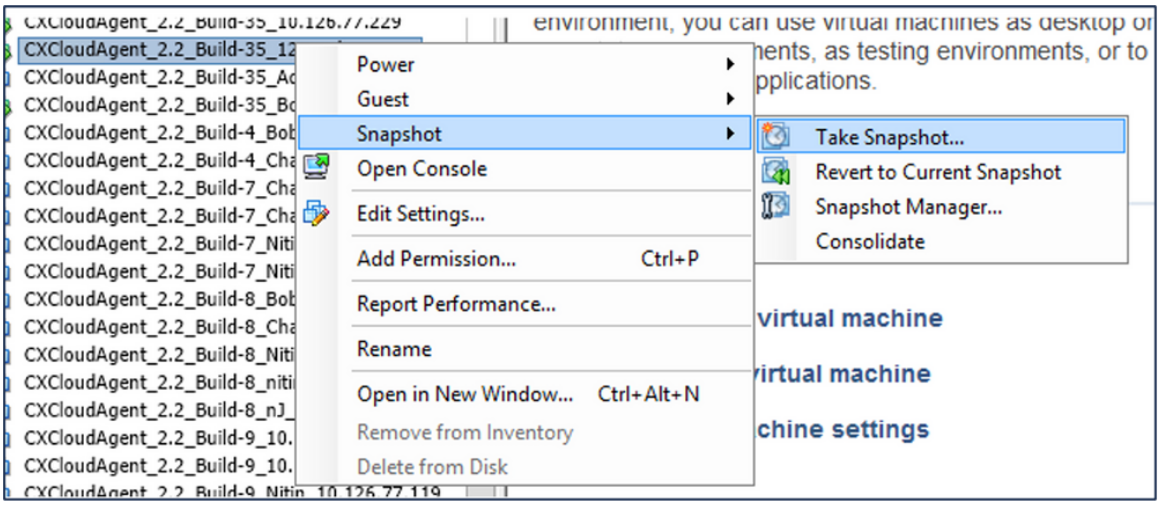
Backup e restauração da VM em nuvem do CX

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.

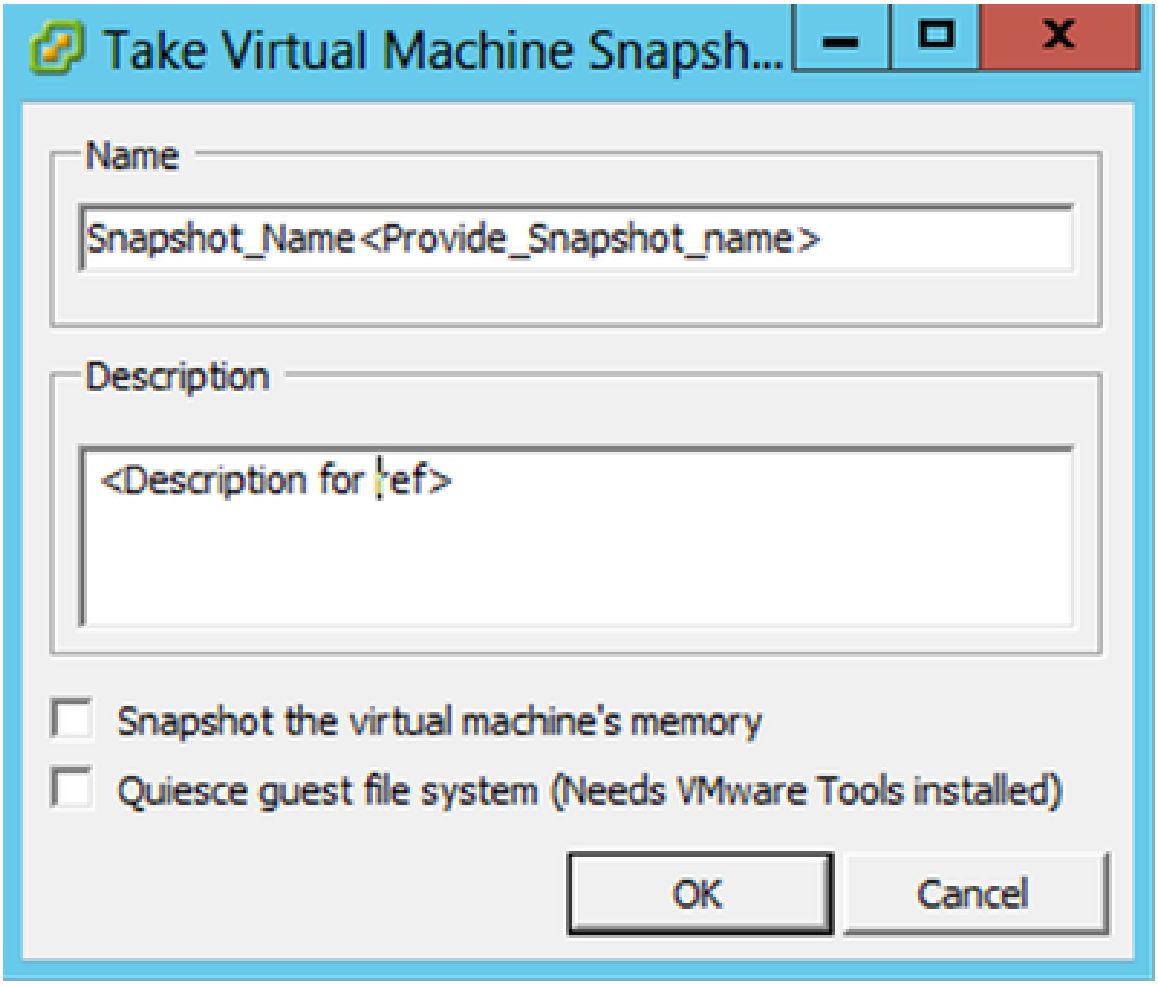
Fazer backup

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



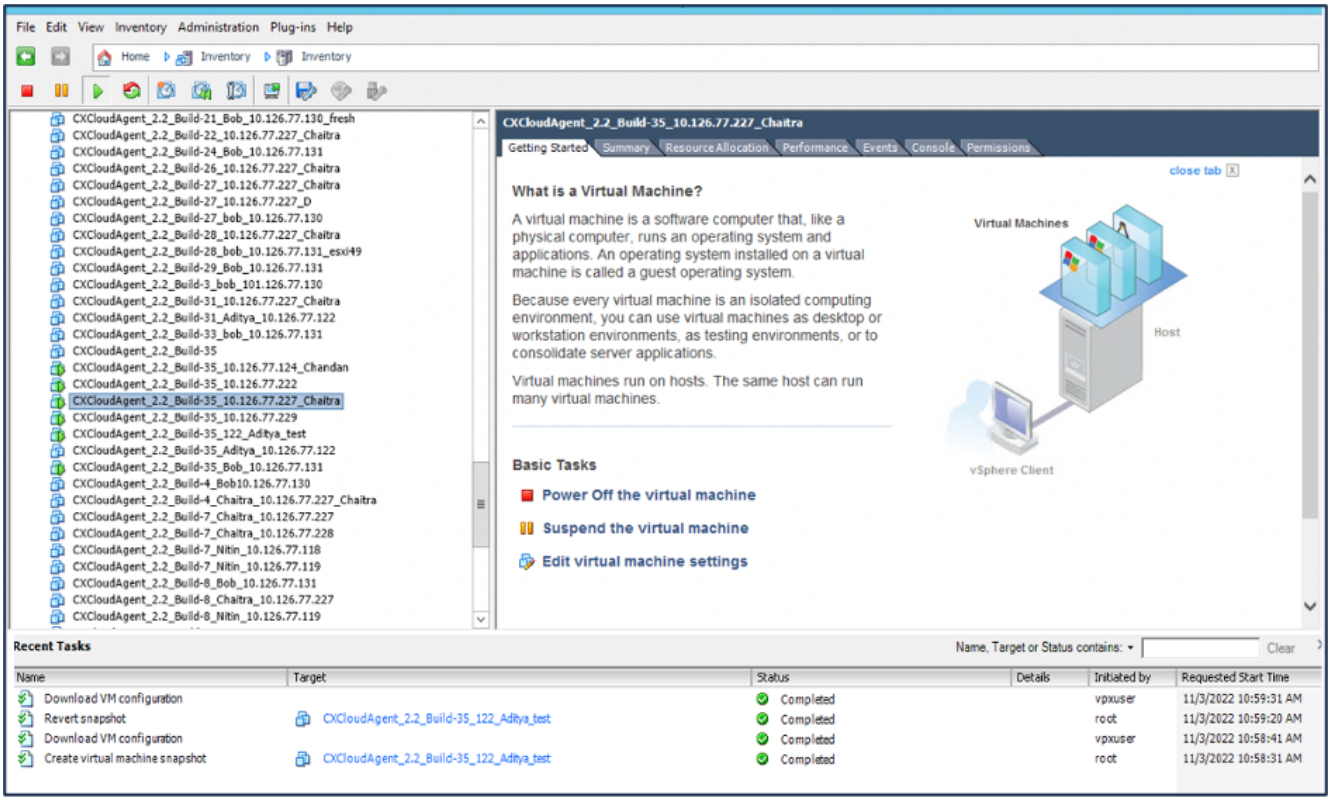
Tirar Instantâneo da Máquina Virtual

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.

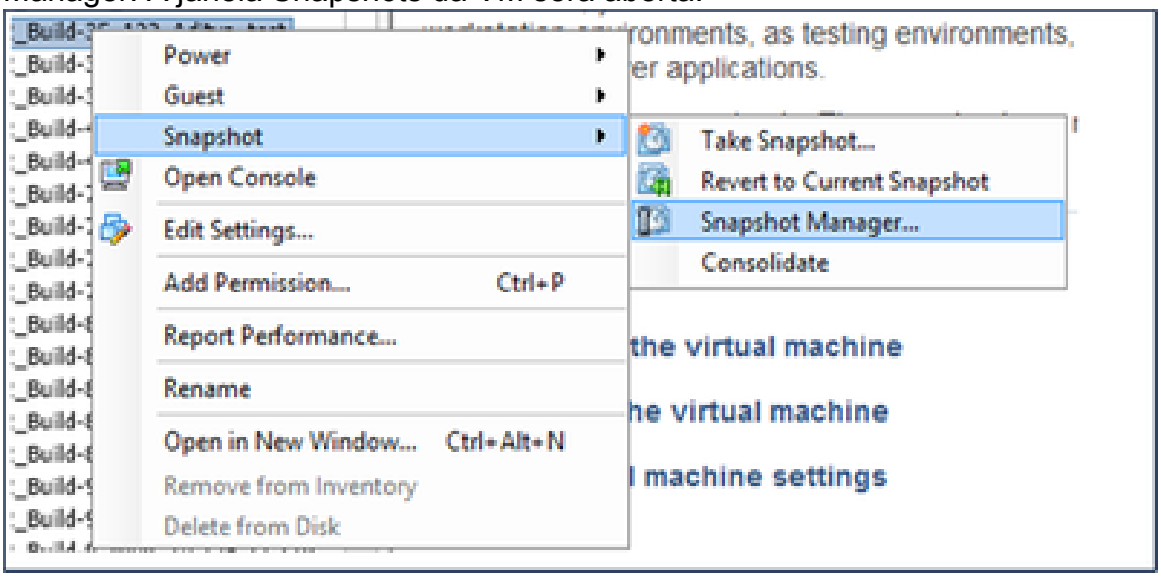


Tarefas Recentes

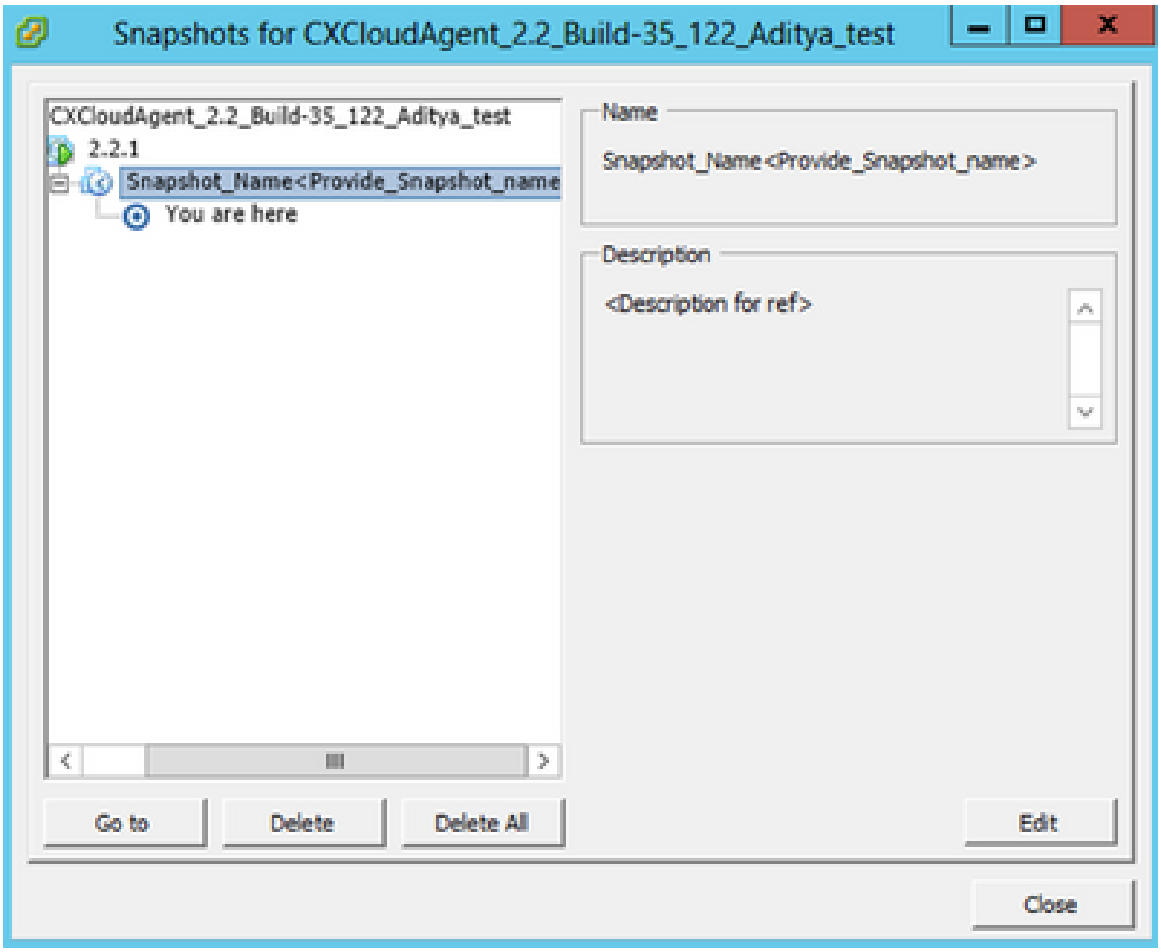
Restaurar

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.

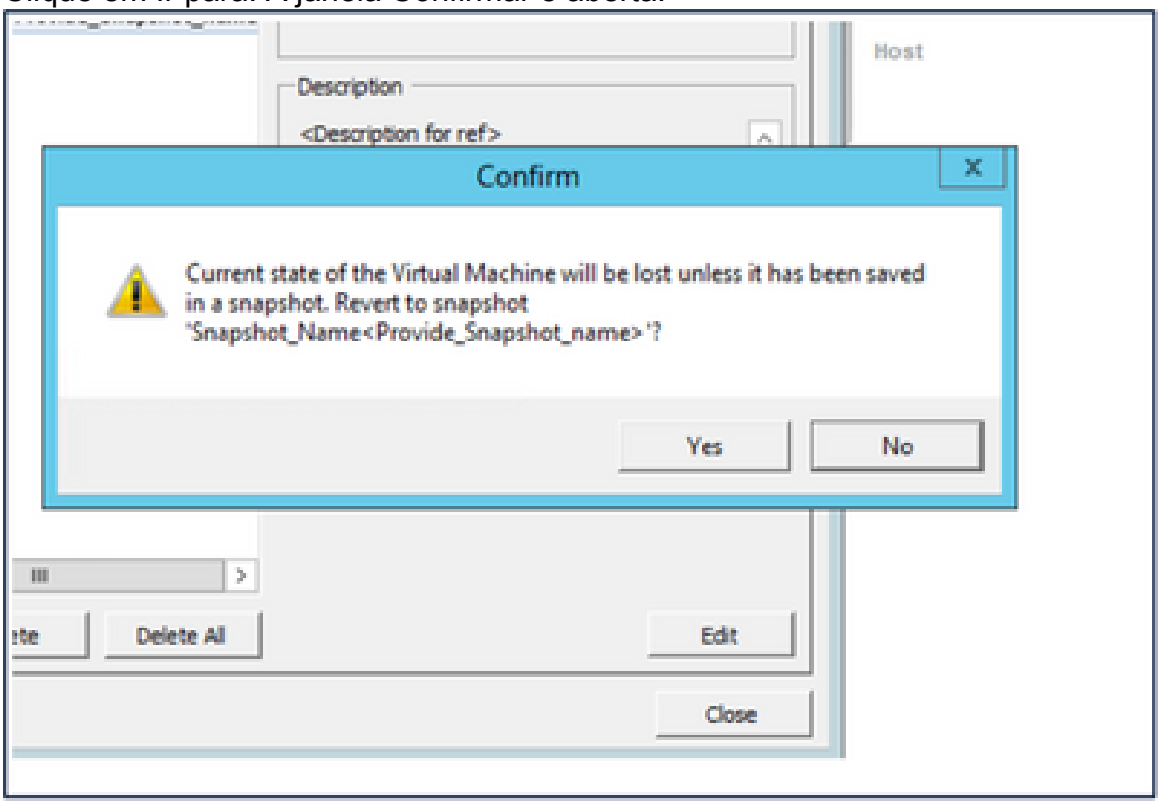


Janela Selecionar VM



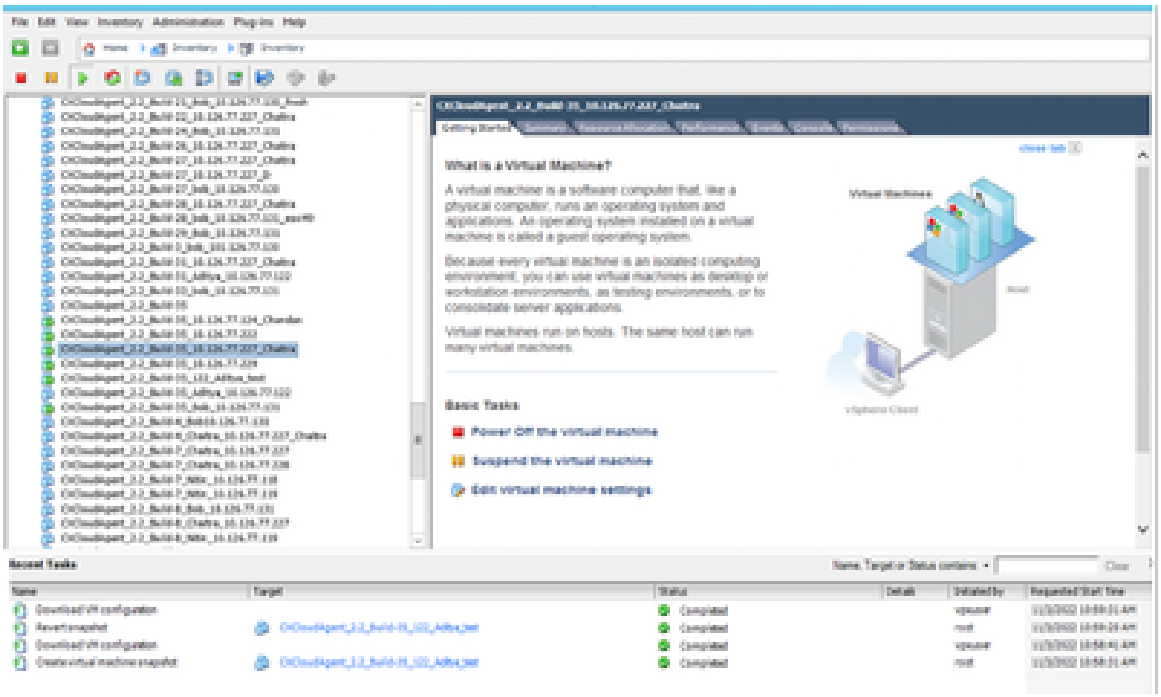
Janela Snapshots

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



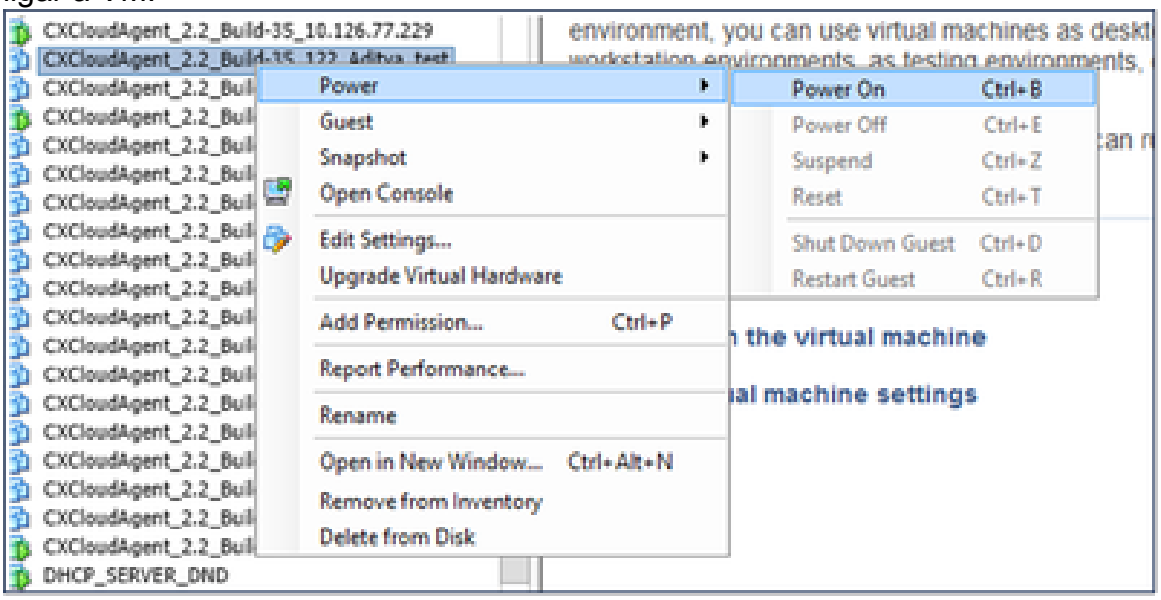
Janela Confirmar

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 (https://swims.cisco.com/abraxas/decrypt). 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 Iot 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, etc. 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 FAQ para definir sua senha do carregador de inicialização (modo de usuário único).
Acesso do usuário	SSH: ·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 descriptografadas usando o portal SWIM por pessoal autorizado
Contas do usuário	· 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 root com esta conta
Política de senha de cxcadmin	·A senha é um hash unidirecional que usa o SHA-256 e é armazenada com segurança · Mínimo de oito (8) caracteres, contendo três das seguintes categorias: maiúsculas, minúsculas, números e caracteres especiais
Política de senha de cxcroot	·A senha de cxcroot é criptografada por RSA/ECB/PKCS1v1_5 ·A frase secreta gerada precisa ser descriptografada no portal do SWIM · 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	· Mínimo de oito caracteres que contêm três das seguintes 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	·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.