

Guía general del agente CX v3.1

Contenido

[Introducción](#)

[Prerequisites](#)

[Acceso a dominios críticos](#)

[Dominios específicos del portal de agentes CX](#)

[Dominios específicos de OVA del agente CX](#)

[Versiones compatibles con Catalyst Center](#)

[Navegadores admitidos](#)

[Lista de productos admitidos](#)

[Actualización/Instalación de CX Agent v3.1](#)

[Actualización de VM existentes a configuraciones grandes y medianas](#)

[Actualización a CX Agent v3.1](#)

[Actualizaciones automáticas](#)

[Actualizaciones manuales](#)

[Adición de un agente CX](#)

[Configuración de CX Agent para BCS/LCS](#)

[Prerequisites](#)

[Configuración del agente CX](#)

[Configuración de funciones RADKit](#)

[Integración del cliente RADKit a través de CLI](#)

[Configuración de Vault para agentes CX existentes](#)

[Configuración de HashiCorp Vault en la interfaz de usuario de la nube CX](#)

[Integración de CX Agent con HashiCorp Vault a través de CLI](#)

[Prerequisites](#)

[Integración con HashiCorp Vault](#)

[Integración de HashiCorp Vault](#)

[Inhabilitación de la Integración de HashiCorp Vault](#)

[Esquema de credenciales del dispositivo HashiCorp Vault](#)

[Configuración de credenciales de dispositivos en HashiCorp Vault \(primera vez\)](#)

[Adición de más credenciales a HashiCorp Vault](#)

[Archivo inicial de nube CX con credenciales predeterminadas](#)

[Adición de Catalyst Center como origen de datos](#)

[Agregar SolarWinds® como origen de datos](#)

[Adición de otros recursos como orígenes de datos](#)

[Protocolos de detección](#)

[Protocolos de conectividad](#)

[Limitaciones del procesamiento de telemetría para dispositivos](#)

[Adición de otros activos mediante un archivo simiente](#)

[Adición de otros activos mediante un nuevo archivo simiente](#)

[Adición de otros activos mediante un archivo simiente modificado](#)



[Credenciales por Defecto para el Archivo Inicial](#)

[Adición de otros activos mediante rangos de IP](#)

[Adición de otros recursos por intervalos de IP](#)

[Edición de rangos IP](#)

[Eliminando intervalo IP](#)

[Acerca de los dispositivos detectados desde varios controladores](#)

[Programación de análisis de diagnóstico](#)

[Actualización de VM de agente CX a configuraciones medianas y grandes](#)

[Reconfiguración mediante VMware vSphere Thick Client](#)

[Reconfiguración mediante el cliente web ESXi v6.0](#)

[Reconfiguración mediante Web Client vCenter](#)

[Implementación y configuración de red](#)

[Implementación de OVA](#)

[Instalación de ThickClient ESXi 5.5/6.0](#)

[Instalación de WebClient ESXi 6.0](#)

[Instalación de WebClient vCenter](#)

[Instalación de Oracle Virtual Box 7.0.12](#)

[Instalación de Microsoft Hyper-V](#)

[Configuración de red](#)

[Enfoque alternativo para generar código de emparejamiento mediante CLI](#)

[Configuración de dispositivos para reenviar Syslog a CX Cloud Agent](#)

[Prerequisites](#)

[Configurar la configuración de Syslog Forward](#)

[Configuración de otros recursos \(recopilación directa de dispositivos\) para reenviar el registro del sistema al agente CX](#)

[Servidores Syslog existentes con capacidad de reenvío](#)

[Servidores Syslog existentes sin capacidad de reenvío O sin servidor Syslog](#)

[Habilitación de la Configuración de Syslog de Nivel de Información para Cisco Catalyst Center](#)

[Copia de seguridad y restauración de la VM en la nube CX](#)

[Respaldo de la VM en la nube CX](#)

[Restauración de la VM en la nube CX](#)

[Security](#)

[Seguridad Física](#)

[Seguridad de cuentas](#)

[Seguridad de redes:](#)

[Autenticación](#)

[Endurecimiento](#)

[Seguridad de datos](#)

[Transmisión de datos](#)

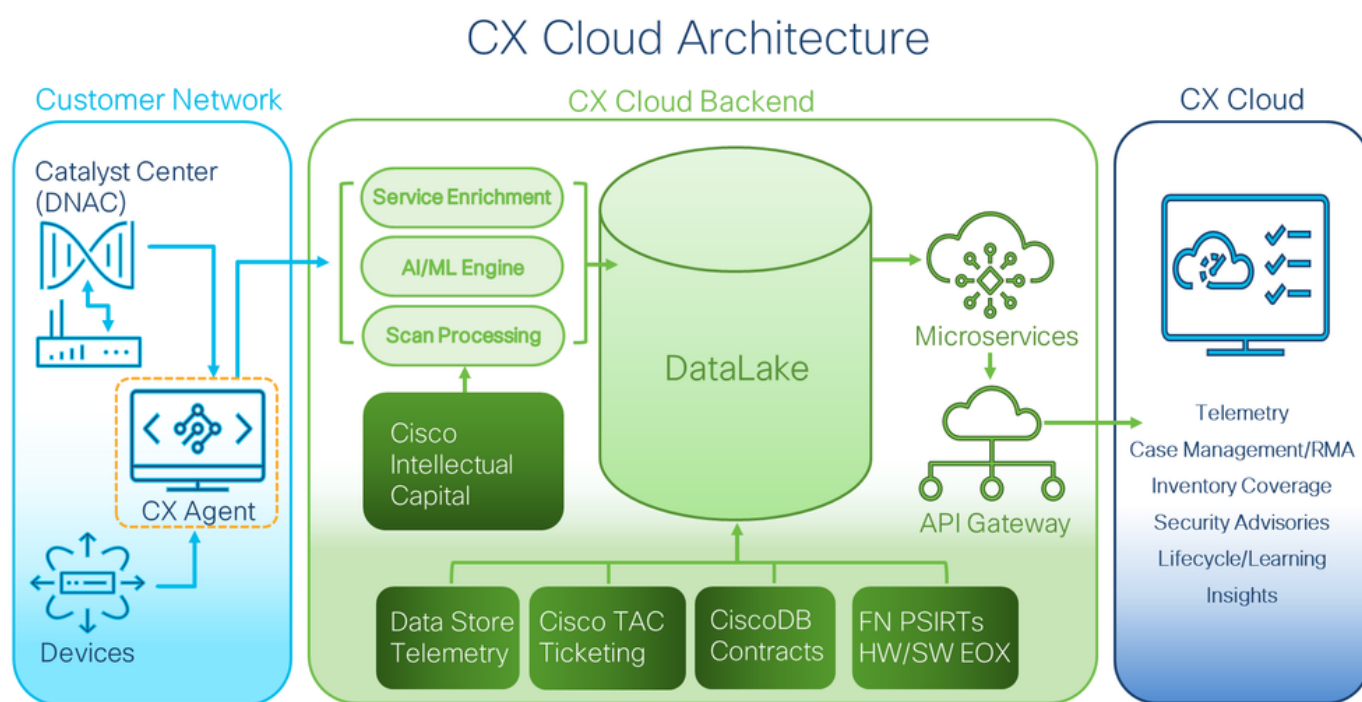
[Registros y supervisión](#)

[Comandos de telemetría de Cisco](#)

[Resumen de seguridad](#)

Introducción

Este documento describe el agente de experiencia del cliente (CX) de Cisco. Cisco CX Agent es una plataforma altamente escalable que recopila datos de telemetría de los dispositivos de red del cliente para ofrecer información práctica a los clientes. CX Agent permite la transformación de inteligencia artificial (IA)/aprendizaje automatizado (ML) de datos de configuración activos en ejecución en información proactiva y predictiva que se muestra en CX Cloud (incluidas las ofertas de Success Tracks, Smart Net Total Care (SNTC) y Business Critical Services (BCS) o Lifecycle Services (LCS)).



Arquitectura de nube CX

Esta guía está destinada únicamente a administradores de partners y de la nube de CX. Los usuarios con roles de administrador de superusuarios (SUA) y administrador tienen los permisos necesarios para realizar las acciones descritas en esta guía.

Esta guía es específica de CX Agent v3.1. Consulte la página [Cisco CX Agent](#) para acceder a las versiones anteriores.

 Nota: las imágenes de esta guía se utilizan únicamente como referencia. El contenido real puede variar.

Prerequisites

El agente CX se ejecuta como máquina virtual (VM) y está disponible para su descarga como dispositivo virtual abierto (OVA) o disco duro virtual (VHD).

Requisitos de implementación

- Se necesita uno de los siguientes hipervisores para una nueva instalación:
 - VMware ESXi v5.5 o posterior

- Oracle Virtual Box v5.2.30 o posterior
- Hipervisor de Windows versión 2012 a 2022 y versión 2025
- Las configuraciones de la siguiente tabla son necesarias para implementar VM:

Tipo de implementación de agente CX	Número de núcleos de CPU	RAM	Disco duro	*Número máximo de recursos directamente conectado al agente CX	Hipervisores admitidos
OVA pequeño	8 QUATER	16 GB	200 GB	10,000	VMware ESXi, Oracle VirtualBox y Windows Hyper-V
OVA medio	16 QUATER	32 GB	600 GB	20,000	VMware ESXi
OVA grande	32 QUATER	64 GB	1200 GB	50,000:	VMware ESXi

*Además de conectar 20 clústeres Cisco Catalyst Center (Catalyst Center) que no sean clústeres o 10 clústeres Catalyst Center para cada instancia de CX Cloud Agent.

 Nota: El servicio RADKit está disponible exclusivamente para implementaciones de agentes CX de tipos de OVA medianos y grandes.

- Para los clientes que utilizan Data Centers estadounidenses designados como la región de datos principal para almacenar datos en la nube de CX, el agente de CX debe poder conectarse a los servidores que se muestran aquí mediante el nombre de dominio completo (FQDN) y HTTPS en el puerto TCP 443:
 - FQDN: agent.us.cisco.cloud
 - FQDN: ng.acs.agent.us.cisco.cloud
 - FQDN: cloudsso.cisco.com
 - FQDN: api-cx.cisco.com
- Para los clientes que utilizan Data Centers europeos designados como la región de datos principal para almacenar datos de CX Cloud: el agente CX debe poder conectarse a ambos servidores que se muestran aquí, mediante el FQDN y mediante HTTPS en el puerto 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 utilizan Data Centers de Asia Pacífico designados como la región de datos principal para almacenar datos de CX Cloud: el agente CX debe poder conectarse a ambos

servidores que se muestran aquí, mediante el FQDN y mediante HTTPS en el puerto 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 utilizan Data Centers designados de Europa y Asia-Pacífico como su región de datos principal, conectividad a FQDN: agent.us.cisco.cloud solo es necesario para registrar el agente en la nube de CX con CX Cloud durante la configuración inicial. Una vez que CX Cloud Agent se haya registrado correctamente en CX Cloud, esta conexión ya no es necesaria.
- Para la gestión local del agente en la nube CX, debe estar accesible el puerto 22.
- Para clientes que utilizan RADKit con FQDN y HTTPS en el puerto TCP 443:
 - FQDN de US: radkit.us.cisco.cloud
 - FQDN de EMEA: radkit.emea.cisco.cloud
 - FQDN de APJC: radkit.apjc.cisco.cloud
- Para permitir que RADKit adjunte el resultado a una solicitud de servicio, el agente CX debe poder acceder al FQDN cxd.cisco.com.
- La siguiente tabla proporciona un resumen de los puertos y protocolos que deben abrirse y activarse para que CX Cloud Agent funcione correctamente:

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 radkit.emea.cisco.cloud Catalyst 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 Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- Una dirección IP se detecta automáticamente si el protocolo de configuración dinámica de host (DHCP) está habilitado en el entorno de VM; De lo contrario, debe haber disponible una dirección IPv4 libre, una máscara de subred, una dirección IP de puerta de enlace predeterminada y una dirección IP del servidor del Servicio de nombres de dominio (DNS).
- Sólo se admite IPv4.
- Las versiones certificadas de Catalyst Center de clúster de nodo único y alta disponibilidad (HA) son las 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x y Catalyst Center Virtual Appliance y Catalyst Center Virtual Appliance.

- Si la red tiene intercepción SSL, introduzca la dirección IP del agente CX de la lista de permisos.
- Para todos los activos conectados directamente, se requiere el nivel de privilegio SSH 15.
- Utilice sólo los nombres de host proporcionados; no se pueden utilizar direcciones IP estáticas.

Acceso a dominios críticos

Para iniciar la transición a la nube de CX, los usuarios necesitan acceder a los siguientes dominios. Utilice sólo los nombres de host proporcionados; no utilice direcciones IP estáticas.

Dominios específicos del portal de agentes CX

Dominios principales	Otros dominios
cisco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

Dominios específicos de OVA del agente CX

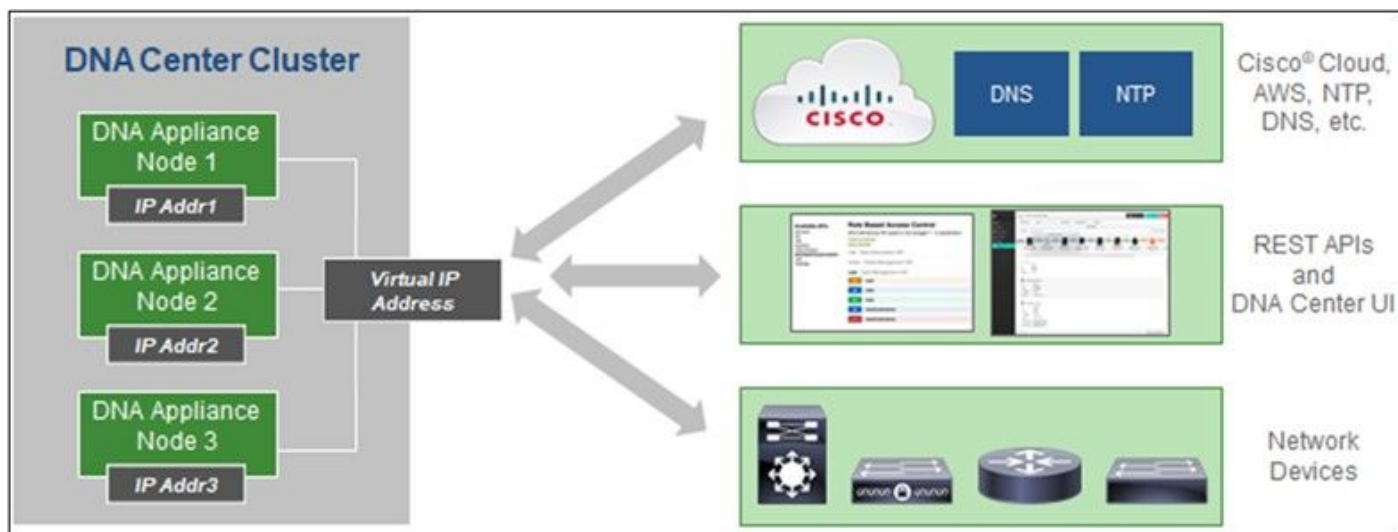
AMÉRICA	EMEA	Asia Pacífico, Japón y China
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.cisco.cloud	agent.us.cisco.cloud	agent.us.cisco.cloud
ng.acs.agent.us.cisco.cloud	agent.emea.cisco.cloud	agent.apjc.cisco.cloud

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

 Nota: Se debe permitir el acceso saliente con la redirección habilitada en el puerto 443 para los FQDN especificados.

Versiones compatibles con Catalyst Center

Las versiones compatibles de Catalyst Center de nodo único y clúster de HA son 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x y Catalyst Center Virtual Appliance y Catalyst Center Virtual Appliance.



Clúster HA de varios nodos Cisco DNA Center

Navegadores admitidos

Para disfrutar de la mejor experiencia en Cisco.com, se recomienda la última versión oficial de estos navegadores:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Lista de productos admitidos

Para ver la lista de productos admitidos por CX Agent, consulte la [Lista de productos admitidos](#).

Actualización/Instalación de CX Agent v3.1

- Los clientes existentes que actualicen a la nueva versión deben consultar [Actualización del agente CX v3.1](#).
- Los nuevos clientes que implementen una instalación de OVA v3.1 flexible y nueva deben consultar [Agregar agente CX](#).

Actualización de VM existentes a configuraciones grandes y medianas

Los clientes pueden actualizar su configuración de VM existente a mediana o grande mediante las opciones de OVA flexible en función del tamaño y la complejidad de la red.

Para actualizar la configuración de VM existente de pequeña a mediana o grande, consulte la sección [Actualización de VM de agente CX a configuración mediana y grande](#).

Actualización a CX Agent v3.1

Los clientes existentes pueden actualizar a la última versión habilitando las actualizaciones automáticas o decidiendo actualizar manualmente desde su versión existente.

Actualizaciones automáticas

Los clientes pueden activar la opción Automatic Software Upgrade para asegurarse de que su sistema se actualiza cuando se lanzan las nuevas versiones. Esta opción está activada de forma predeterminada para las nuevas instalaciones, pero se puede modificar en cualquier momento para alinearla con las políticas de la empresa o para programar actualizaciones durante los períodos de mantenimiento planificados.

Actualizaciones automáticas

 Nota: Las actualizaciones automáticas están desactivadas de forma predeterminada para las instancias existentes del agente CX, pero los usuarios pueden activarlas en cualquier

 momento.

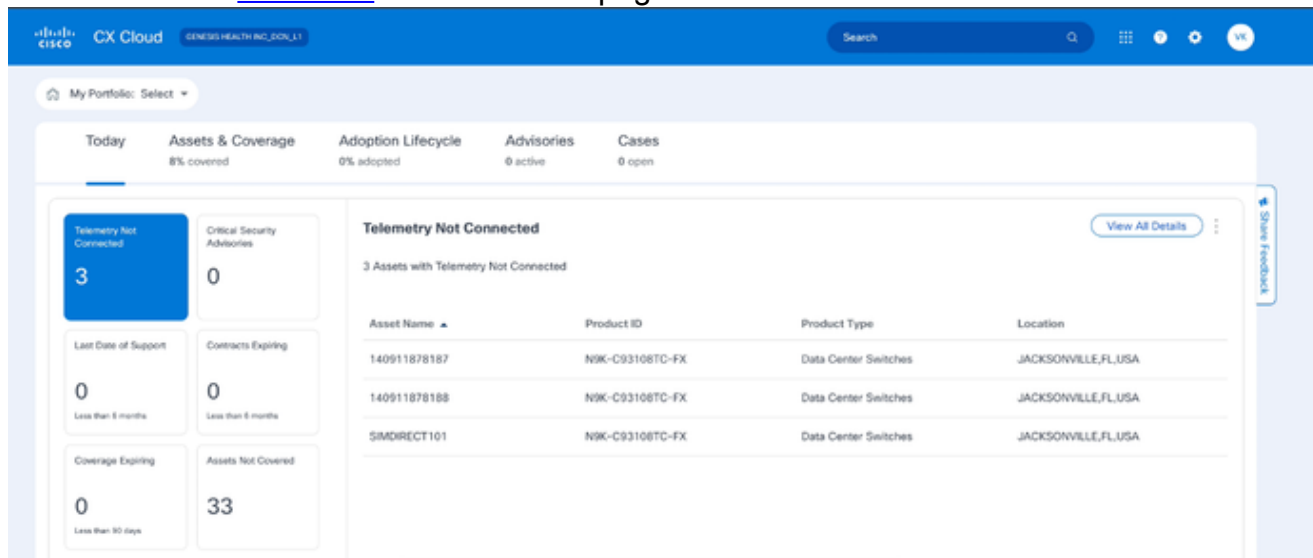
Actualizaciones manuales

Los clientes que prefieran no utilizar actualizaciones automáticas y no hayan activado Actualizaciones automáticas de software pueden optar por actualizar manualmente. CX Agent v2.4.x y versiones posteriores admiten una actualización directa a v3.1 siguiendo los pasos descritos en esta sección.

 **Nota:** Los clientes de CX Agent v2.3.x y versiones posteriores deben actualizar progresivamente a v2.4.x antes de actualizar a v3.1 o realizar una instalación de OVA nueva.

Para instalar la actualización CX Agent v3.1 desde CX Cloud:

1. Inicie sesión en [CX Cloud](#). Se muestra la página Inicio.



The screenshot shows the CX Cloud dashboard. The top navigation bar includes the Cisco logo, 'CX Cloud', and a search bar. Below the navigation bar, there's a 'My Portfolio: Select' dropdown. The main content area is divided into several sections. On the left, there are four summary cards: 'Telemetry Not Connected' (3), 'Critical Security Advisories' (0), 'Last Date of Support' (0), and 'Contracts Expiring' (0). Below these are two more cards: 'Coverage Expiring' (0) and 'Assets Not Covered' (33). The right section is titled 'Telemetry Not Connected' and shows a table with 3 assets. The table has columns for Asset Name, Product ID, Product Type, and Location. The assets listed are 140911878187, 140911878188, and SIMDIRECT101, all with Product ID N9K-C93108TC-FX and Location JACKSONVILLE,FL,USA.

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

Página de inicio de CX Cloud

2. Seleccione el icono Centro de administración. Se abre la ventana Orígenes de datos.

4. Seleccione la versión de software 3.1.0 en la lista desplegable Elegir una versión de

software para actualizar a.

5. Haga clic en Install Update para instalar CX Agent v3.1.

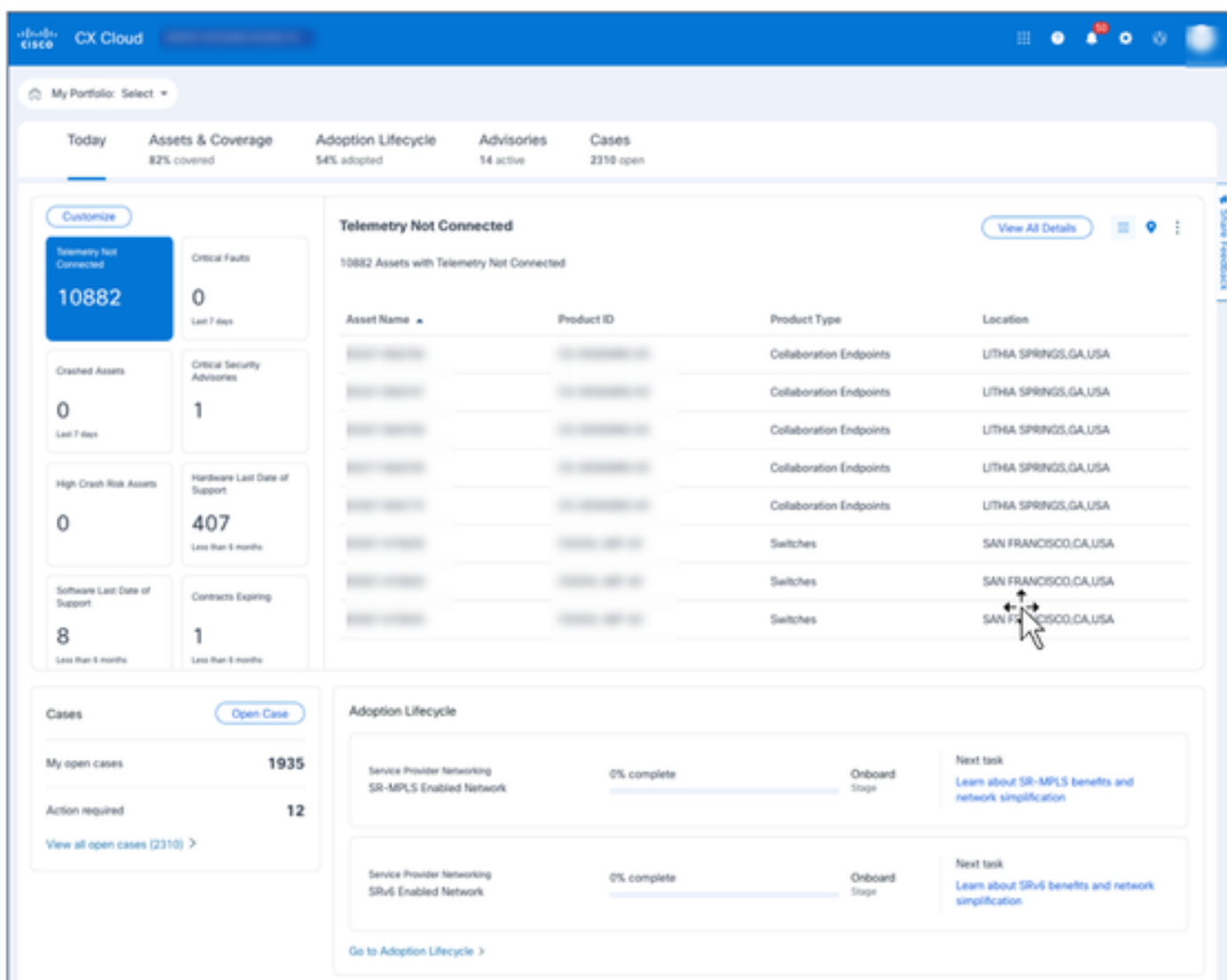
 Nota: Los clientes pueden programar la actualización para más adelante desactivando la casilla de verificación Instalar ahora, que muestra las opciones de programación.

Adición de un agente CX

Los clientes pueden añadir hasta 20 instancias de agente CX en la nube CX.

Para agregar un agente CX:

1. Inicie sesión en [CX Cloud](#). Se muestra la página Inicio.



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

- Today**: Overview of current status.
- Assets & Coverage**: 82% covered.
- Adoption Lifecycle**: 54% adopted.
- Advisories**: 14 active.
- Cases**: 2310 open.

On the left, there's a 'Customize' section with several cards:

- Telemetry Not Connected**: 10882.
- Critical Faults**: 0.
- Crashed Assets**: 0.
- Critical Security Advisories**: 1.
- High Crash Risk Assets**: 0.
- Hardware Last Date of Support**: 407.
- Software Last Date of Support**: 8.
- Contracts Expiring**: 1.

The central part of the dashboard features a table titled 'Telemetry Not Connected' with 10882 assets. The table has columns for Asset Name, Product ID, Product Type, and Location. A mouse cursor is pointing at the 'SAN FRANCISCO, CA, USA' location in the last row.

At the bottom, there's a 'Cases' section with 'My open cases' (1935) and 'Action required' (12). To the right, the 'Adoption Lifecycle' section shows progress bars for 'Service Provider Networking SR-MPLS Enabled Network' and 'Service Provider Networking SRvS Enabled Network', both at 0% complete.

Página de inicio de CX Cloud

2. Seleccione el icono Centro de administración. Se abre la ventana Orígenes de datos.

Cisco

CX Cloud

9999

Back

Asset Groups

Identity & Access

Partner Access

Data Collection

Data Sources

Insights

Data Sources

See Usage Report Details

Search data sources

Add Data Source

16 data sources

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

Orígenes de datos

- Haga clic en Agregar origen de datos. Se abre la página Agregar origen de datos. Las opciones mostradas varían en función de las suscripciones del cliente.

Add Data Source



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

Add Data Source



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

Add Data Source



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

Add Data Source



Contracts
Supports assets associated with a contract

Add Data Source



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

Add Data Source



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

Add Data Source



Meraki dashboard
Supports Meraki

Add Data Source



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

Add Data Source



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

Add Data Source

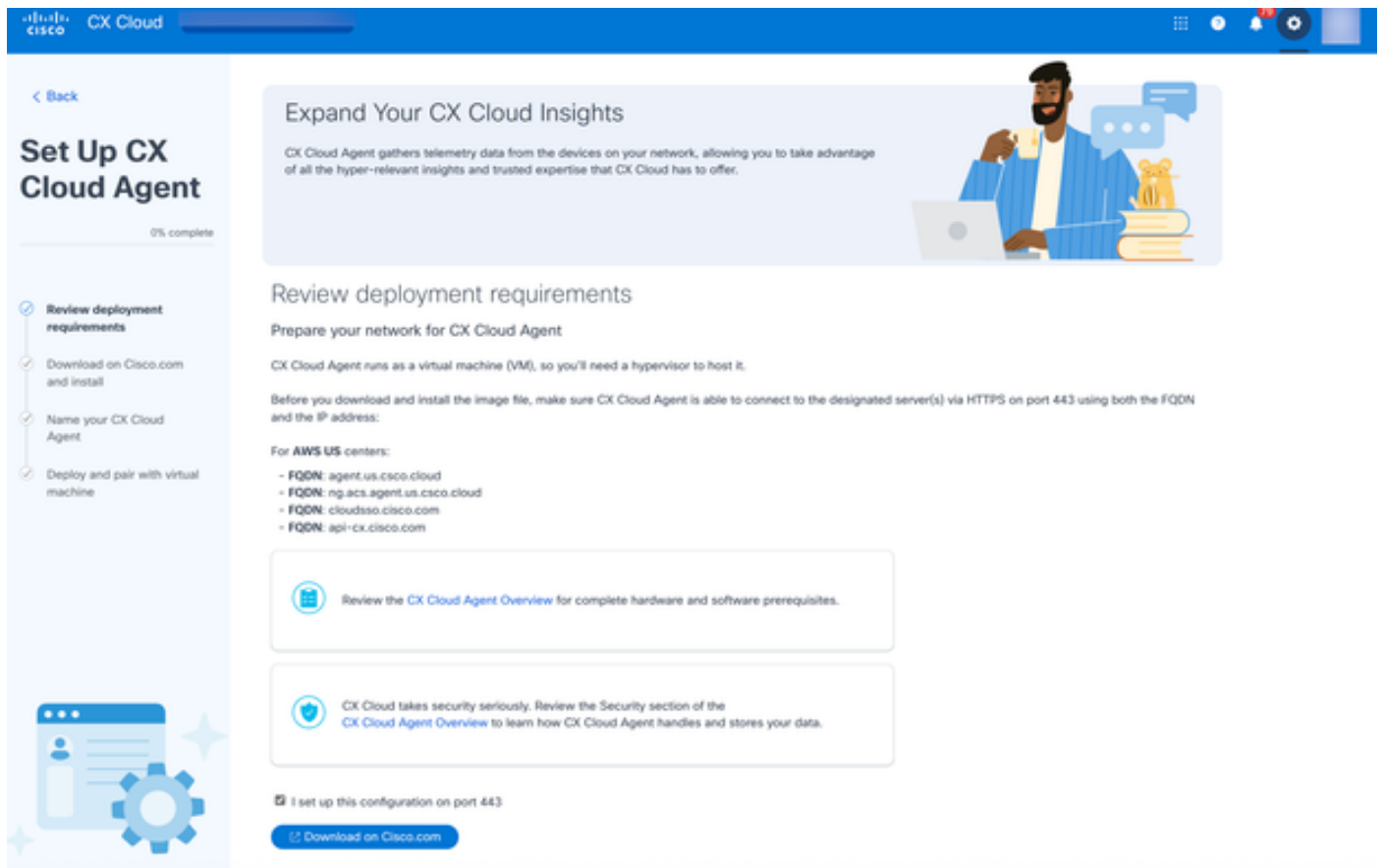


Webex
Supports the Success Track for Collaboration

Add Data Source

Agregar origen de datos

- Haga clic en Agregar origen de datos de la opción Agente CX. Se abre la ventana Set Up CX Agent.



Set Up CX Cloud Agent
0% complete

Review deployment requirements

Download on Cisco.com and install

Name your CX Cloud Agent

Deploy and pair with virtual machine

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](#)

Adición de un agente CX

5. Revise la sección Revisar requisitos de implementación y active la casilla de verificación I set up this configuration on port 443.
6. Haga clic en Descargar en Cisco.com. La ventana Descarga de Software se abre en otra pestaña.
7. Descargue el archivo "CX Agent v3.1.0 OVA".

 **Nota:** Se genera un código de emparejamiento necesario para completar la configuración del agente CX después de implementar el archivo "OVA".

8. Introduzca el nombre del agente CX en el campo Name Your CX Cloud Agent.

The screenshot shows the 'Name Your CX Cloud Agent' step in the Cisco CX Cloud Agent setup process. The page has a blue header with the Cisco logo and 'CX Cloud' text. On the left, a sidebar titled 'Set Up CX Cloud Agent' shows a progress bar at 50% complete and a list of steps: 'Review deployment requirements', 'Download on Cisco.com and install', 'Name your CX Cloud Agent' (current step), and 'Deploy and pair with virtual machine'. The main content area has the title 'Name Your CX Cloud Agent' and a subtext 'Make sure the name is unique, so you can find it later.' Below this is a text input field and a 'CONTINUE' button.

Nombre Agente CX

9. Haga clic en Continuar. Se abre la ventana Implementar y emparejar con la máquina virtual.

The screenshot shows the 'Deploy and pair with your virtual machine' step in the Cisco CX Cloud Agent setup process. The page has a blue header with the Cisco logo and 'CX Cloud' text. On the left, a sidebar titled 'Set Up CX Cloud Agent' shows a progress bar at 75% complete and a list of steps: 'Review deployment requirements', 'Download on Cisco.com and install', 'Name your CX Cloud Agent', and 'Deploy and pair with virtual machine' (current step). The main content area has the title 'Deploy and pair with your virtual machine' and a subtext 'Deploy the downloaded file on your virtual machine. After deployment, you'll receive a pairing code. Please enter the code below.' Below this is a 'Pairing Code' input field with a red asterisk and a 'CONTINUE' button. There is also a section for 'Automatic Software Upgrades' with a toggle switch and explanatory text.

Código de vinculación

10. Introduzca el código de emparejamiento recibido después del despliegue del archivo "OVA" descargado.

11. Haga clic en Continuar. Se muestra el progreso del registro, seguido de un mensaje de confirmación.

 Nota: Repita los pasos anteriores para agregar instancias adicionales del agente CX como origen de datos.

Configuración de CX Agent para BCS/LCS

La nueva función de recopilación convergente de Cisco optimiza la configuración de CX Agent

v3.1 para BCS/LCS, lo que simplifica la experiencia del cliente.



Nota: Esta configuración es específica para los ingenieros de soporte técnico de Cisco responsables de la configuración del recopilador para los clientes de BCS/LCS.

Los clientes de BCS/LCS pueden visitar la [CX Cloud Community](#) para obtener más información sobre la incorporación de usuarios y otra información relacionada.

Prerequisites

Los ingenieros de asistencia técnica con acceso de administrador superusuario (SUA) y administrador solo pueden realizar la configuración de agente CX para BCS/LCS.

Configuración del agente CX

Para configurar el agente CX para BCS/LCS, póngase en contacto con el servicio de asistencia de Cisco.

Configuración de funciones RADKit

CX Agent v3.1 proporciona una configuración de RADKit opcional diseñada para mejorar la gestión remota y la resolución de problemas de los dispositivos de Cisco en CX Cloud. Cuando está activada, los usuarios autorizados pueden realizar operaciones de forma segura, como la captura de datos, la configuración y las actualizaciones de software de forma remota. Estos parámetros se pueden activar o desactivar en cualquier momento en función de los requisitos operativos del cliente.

Para obtener información detallada sobre RADKit, consulte [Cisco RADKit](#).

Integración del cliente RADKit a través de CLI

Para integrar el servicio de cliente RADKit, cree una cuenta de administrador e inscriba el servicio siguiendo estos pasos:



Nota: Los siguientes pasos requieren acceso raíz a la máquina virtual del agente CX.

1. Abra el terminal y Secure Shell (SSH) en una VM utilizando las credenciales adecuadas, por ejemplo:

```
ssh your_username@your_vm_ip
```

2. Ejecute el siguiente comando para habilitar la conectividad de red:

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

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

3. En el equipo local, envíe una solicitud POST al extremo del administrador para crear una cuenta de administrador. El organismo de solicitud debe incluir:

- `admin_name` (obligatorio): El nombre de usuario de la cuenta de administrador
- `correo electrónico` (opcional): La dirección de correo electrónico de la cuenta de administrador
- `nombre_completo` (opcional): El nombre completo del administrador.
- `descripción` (opcional): Una descripción de la cuenta de administrador

El siguiente ejemplo muestra cómo enviar esta solicitud mediante cURL:

```
curl -X POST \
  http://<your_vm_ip>:30100/radkitmanager/v1/createAdmin \
  -H "Tipo de contenido: application/json" \
  -d '{
    "admin_name": "admin_user123",
    "correo electrónico": "admin@example.com",
    "nombre_completo": "Usuario administrador",
    "descripción": "Cuenta de administrador para administrar el
sistema"
  }'
```

Una vez creada correctamente una cuenta de administrador, el servidor responde con un mensaje de confirmación que indica que la cuenta de administrador se ha creado correctamente. Esta respuesta también incluye una contraseña temporal que se debe cambiar la primera vez que inicie sesión. Sin embargo, si la cuenta de administrador ya existe, el servidor devuelve un código de estado 400 con el mensaje "Admin already created".

4. Abra el navegador web y navegue hasta la interfaz de usuario web de RADKit:

`https://<your_vm_ip>:30101/`.

5. Inicie sesión con el nombre de usuario del administrador (`admin_name`) y la contraseña temporal proporcionada en la respuesta.



Nota: La primera vez que inicie sesión, se le pedirá a los usuarios que cambien la contraseña. Siga las instrucciones para establecer una nueva contraseña.

6. Ejecute el cliente RADKit en el equipo local para inscribir el servicio.

7. Después de la autenticación, genere una contraseña de un solo uso ejecutando el siguiente comando:

grant_service_top()

8. En el equipo local, envíe una solicitud POST al extremo del jefe para inscribir el servicio. El organismo de solicitud debe incluir:

- OTP (obligatorio): La cadena de contraseña de un solo uso

El siguiente ejemplo muestra cómo enviar esta solicitud mediante cURL:

```
curl -X POST \
  http://<your_vm_ip>:30100/radkitmanager/v1/enrollService \
  -H "Tipo de contenido: application/json" \
  -d '{
    "one_time_password": "PROD:1234-1234-1234"
  }'
```

Una vez realizada la inscripción correctamente, se muestra un mensaje de confirmación y los usuarios pueden administrar el servicio RADKit con una cuenta de administrador.

Para deshabilitar la conectividad de red, ejecute el siguiente comando:

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

Configuración de Vault para agentes CX existentes

La función de configuración opcional de la caja fuerte permite a CX Cloud conectarse de forma segura a un servicio de caja fuerte para acceder a datos confidenciales, como fichas y listas de inventario, mediante las credenciales más recientes. Cuando está activada, CX Cloud utiliza automáticamente la dirección y el token configurados. Esta configuración se puede habilitar o deshabilitar en cualquier momento. Actualmente, solo se soporta la configuración de bóveda de HashiCorp.

El depósito se puede configurar de dos maneras:

- Interfaz de usuario de nube CX
- A través de CLI

Configuración de HashiCorp Vault en la interfaz de usuario de la nube CX

Para configurar el depósito de HashiCorp para un agente CX existente:

1. Seleccione el icono Centro de administración. Se abre la ventana Orígenes de datos.
2. Haga clic en el origen de datos Agente CX. Se abrirá la ventana de detalles del agente CX.

Configuración

3. Haga clic en la pestaña Settings.
4. Active la opción de configuración del depósito.

Configuración del depósito

5. Introduzca los detalles en los campos Dirección y Token.

6. Haga clic en Enviar. Se muestra una confirmación y la dirección IP agregada.

Los clientes pueden quitar el depósito configurado haciendo clic en Quitar.

Integración de CX Agent con HashiCorp Vault a través de CLI

En esta sección se describe el procedimiento para configurar la conexión entre el agente de Cisco CX y una instancia de HashiCorp Vault. Esta integración permite el almacenamiento y la recuperación seguros de las credenciales del dispositivo, lo que mejora el estado de seguridad general.

Prerequisites

- cxcroot access to CX Agent VM
- Una instancia de depósito accesible y en ejecución

Integración con HashiCorp Vault

- Para habilitar la integración de depósito, ejecute el siguiente comando:

```
cxcli agent vault on
```

- Para desactivar la integración del depósito, ejecute el siguiente comando:

```
cxcli agent vault off
```

- Para comprobar el estado actual de la integración del depósito, ejecute el siguiente comando:

```
estado de cxcli agent vault
```

Integración de HashiCorp Vault

Para habilitar la integración de depósito:

1. Inicie sesión en el agente CX a través de SSH con la cuenta de usuario cxcroot para acceder al agente CX.
2. Cambie al usuario root para elevar los privilegios ejecutando el siguiente comando:

```
sudo su
```

3. Ejecute el siguiente comando para comprobar el estado de integración actual del almacén:

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

integración de depósito desactivada

4. Ejecute el siguiente comando para habilitar la integración de almacén:

```
cxcli agent vault on
```

5. Actualice los campos siguientes:

- Dirección de almacén
- Token raíz del almacén

6. Para verificar, verifique el estado de la integración con la bóveda. El mensaje de respuesta debe confirmar que la integración está habilitada:

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

Introduzca la dirección de HashiCorp Vault:

Introduzca el token de HashiCorp Vault:

```
integración de almacén habilitada root@cxcloudagent: /home/cxcroot#
```

Inhabilitación de la Integración de HashiCorp Vault

Para acceder al agente CX:

1. Inicie sesión en el agente CX a través de SSH con la cuenta de usuario cxcroot.
2. Cambie al usuario root para elevar los privilegios ejecutando el siguiente comando:

```
sudo su
```

3. Ejecute el siguiente comando para inhabilitar la integración de HashiCorp Vault:

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

```
integración de depósito desactivada
```

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

HashiCorp Esquema de credenciales del dispositivo Vault

Esquema de Credenciales del Almacén: Para obtener información detallada sobre las opciones disponibles y los campos compatibles para las credenciales de los dispositivos, descargue el archivo "Esquema de credenciales de almacén" ([vault-credentials-schema.json](#)).

Ejemplo: A continuación se muestra un ejemplo de una credencial JSON basada en el esquema:

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

```
"telnet": {
 "user": "cisco",
 "password": "*****",
 "enableUser": "cisco",
 "enablePassword": "*****"
}
}
}
```



Nota: Los usuarios pueden especificar varios protocolos en un único archivo JSON de credenciales. Sin embargo, evite incluir protocolos duplicados de la misma familia (por ejemplo, no incluya SNMPv2c y SNMPv3 en el mismo archivo de credenciales).

## Configuración de credenciales de dispositivos en HashiCorp Vault (primera vez)

1. Inicie sesión en una instancia de Vault.

### Secrets Engines

[Enable new engine +](#)

**cubbyhole/**

per-token private secret storage

...

**secret/**

key/value secret storage

...

Clave

2. Cree un nuevo secreto de valor de clave mediante la siguiente ruta: secret/seed/credentials.
3. Elija el motor de almacenamiento secreto de valor de clave (secret/).

Secrets / secret

**secret** version 2

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

[Create secret +](#)

### No secrets yet

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

Clave secreta de valor

4. Haga clic en Create secret. Se abre la ventana Create Secret.

Secrets / secret / Create

## Create Secret

☐ JSON

**Path for this secret**  
Names with forward slashes define hierarchical path structures.

seed/credentials

**Secret data**

credentialName1

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

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

key  

[Show secret metadata](#)

Secreto del cliente

5. Actualice los campos siguientes:

- Ruta para secreto: simiente/credenciales
- Datos secretos: colección de claves: secretos de valor
- clave: nombre de credencial único personalizado
- valor: credenciales JSON

6. Haga clic en Guardar. El secreto debe almacenarse ahora en el almacén de HashiCorp.

# seed/credentials

Overview Secret Metadata Paths Version History

JSON

DeleteDestroyCopyVersion 1Create new version

| Key             | Value                                                                                                                                                                                                                                                | Version 1 created Jun 04, 2025 03:39 PM |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| credentialName1 | <pre>{   "targetIp": "5.0.1.*",   "credentials": {     "snmpv3": {       "user": "cisco",       "authPassword": "cisco123",       "authAlgorithm": "MD5",       "privacyPassword": "cisco123",       "privacyAlgorithm": "AES-256"     }   } }</pre> |                                         |

Credenciales

## Adición de más credenciales a HashiCorp Vault

1. Inicie sesión en una instancia de almacén de HashiCorp.

# seed/credentials

Overview Secret Metadata Paths Version History

JSON

DeleteDestroyCopyVersion 1Create new version

| Key             | Value                                  | Version 1 created Jun 04, 2025 03:39 PM |
|-----------------|----------------------------------------|-----------------------------------------|
| credentialName1 | <div><div></div><div>*****</div></div> |                                         |

Agregar credenciales

2. Navegue hasta el Secreto "secret/seed/credentials" ya creado.

## Create New Version

☐ JSON

**Path for this secret**  
Names with forward slashes define hierarchical path structures.

seed/credentials

---

**Version data**

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

☐ **Show diff**  
No changes to show. Update secret to view diff

Crear versión

- Haga clic en Crear nueva versión.
- Agregue nuevos secretos proporcionando cualquier número de pares clave-valor según sea necesario.
- Haga clic en Guardar.

## Archivo inicial de nube CX con credenciales predeterminadas

- Simplifique el archivo simiente: Al utilizar credenciales configuradas mediante Hashicorp vault, simplifique el archivo de inicialización omitiendo la información confidencial
- Especifique sólo la dirección IP o el nombre de host: Los usuarios sólo pueden pasar la dirección IP o el nombre de host en el archivo simiente, dejando otros campos en blanco

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

IP o nombre de host

- Utilice las credenciales de HashiCorp vault y Seed File: Proporcione credenciales para algunos dispositivos en el archivo simiente mientras confía en el almacén para administrar las credenciales para otros dispositivos

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

IP o nombre de host

## Adición de Catalyst Center como origen de datos

Los usuarios con la función de usuario de superadministrador pueden agregar el origen de datos de Catalyst Center.

Para agregar Catalyst Center como origen de datos:

1. Seleccione el icono Centro de administración. Se abre la ventana Orígenes de datos.
2. Haga clic en Agregar origen de datos. Se muestra la página Agregar origen de datos.

## Add Data Source

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

Add Data Source

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

Add Data Source

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

Add Data Source

**Contracts**  
Supports assets associated with a contract

Add Data Source

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

Add Data Source

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

Add Data Source

**Meraki dashboard**  
Supports Meraki

Add Data Source

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

Add Data Source

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

Add Data Source

**Webex**  
Supports the Success Track for Collaboration

Add Data Source

Agregar origen de datos

3. Haga clic en Add Data Source en la opción Catalyst Center.

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

Select option



Cancel

Continue



Seleccionar agente CX

4. Seleccione el agente CX en la lista desplegable ¿Qué agente CX desea conectar a?
5. Haga clic en Continue (Continuar). Se abre la ventana Connect to CX Cloud.

## Connect to CX Cloud

### Connect a Catalyst Center

IP Address or FQDN \*

City \*

Select option



Username \*

Password \*

### Schedule inventory collection

Frequency

Select Time

Frequ... ▾

12:00 ▾

AM ▾

WEDT

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

Connect

Frecuencia

6. Introduzca los detalles siguientes:

- Dirección IP virtual o FQDN (es decir, dirección IP de Catalyst Center)
- Ciudad (es decir, la ubicación de Catalyst Center)
- Nombre de usuario
- Contraseña
- Frequency y Select Time para indicar la frecuencia con la que el agente CX debe realizar análisis de red en las secciones Schedule Inventory Collection

Nota: Active la casilla de verificación Ejecutar la primera colección ahora para ejecutar la colección ahora.

7. Haga clic en Connect (Conectar) Aparecerá una confirmación con la dirección IP de Catalyst Center.

## Agregar SolarWinds® como origen de datos

Nota: Si es necesario agregar la fuente de datos de SolarWinds®, póngase en contacto con el servicio de asistencia de Cisco para obtener ayuda.

Los clientes de BCS/LCS ahora pueden utilizar la función de agente CX para integrarse externamente con SolarWinds®, lo que proporciona una mayor transparencia, una capacidad de gestión mejorada y una experiencia de usuario mejorada a través de una mayor automatización. El agente CX recopila el inventario y otros datos necesarios para generar varios informes que son consistentes en términos de formato, integridad de los datos y precisión de los datos a los informes actuales generados por Operational Insights Collector CX Agent admite la integración con SolarWinds® al permitir que un cliente BCS/LCS reemplace OIC con CX Agent para recopilar datos de Solarwinds®. Esta función, incluida la fuente de datos Solarwinds®, está disponible exclusivamente para clientes de BCS/LCS.

El agente CX debe configurarse en BCS Forwarding antes de la primera recopilación; de lo contrario, los archivos permanecen sin procesar. Consulte la sección [Configuración del Agente CX para BCS o LCS](#) para obtener más información sobre la configuración del reenvío BCS.

Notas:

- Varias colecciones de la misma instancia de SolarWinds® sobrescriben archivos anteriores (las cargas posteriores tienen prioridad)
- Se admiten varias fuentes, pero cada instancia de SolarWinds® debe tener una IP y una ID de dispositivo únicas

## Adición de otros recursos como orígenes de datos

La recopilación de telemetría se ha ampliado a dispositivos no gestionados por Catalyst Center, lo que permite a los usuarios ver e interactuar con análisis e información derivada de la telemetría para una gama más amplia de dispositivos. Después de la configuración inicial del agente CX, los usuarios tienen la opción de configurar el agente CX para conectarse a 20 Catalyst Centers

adicionales dentro de la infraestructura supervisada por CX Cloud.

Los usuarios pueden identificar los dispositivos que se incorporarán a CX Cloud identificándolos de forma única mediante un archivo simiente o especificando un rango de IP, que debe ser analizado por el agente CX. Ambos enfoques se basan en el protocolo simple de administración de red (SNMP) para la detección y en Secure Shell (SSH) para la conectividad. Deben configurarse correctamente para habilitar la recopilación de telemetría correcta.

Para agregar otros activos como orígenes de datos, utilice cualquiera de las opciones siguientes:

- Cargar un archivo simiente mediante una plantilla de archivo simiente
- Proporcione un intervalo de direcciones IP

## Protocolos de detección

Tanto la detección directa de dispositivos basada en archivos simientes como la detección basada en rangos de IP se basan en SNMP como protocolo de detección. Existen diferentes versiones de SNMP, pero el agente CX es compatible con SNMPv2c y SNMPv3 y se pueden configurar una o ambas versiones. El usuario debe proporcionar la misma información, que se describe a continuación con todo detalle, para completar la configuración y habilitar la conectividad entre el dispositivo administrado por SNMP y el administrador de servicio SNMP.

SNMPv2c y SNMPv3 difieren en términos de seguridad y modelo de configuración remota. SNMPv3 utiliza un sistema de seguridad criptográfica mejorado que admite el cifrado SHA para autenticar los mensajes y garantizar su privacidad. Se recomienda utilizar SNMPv3 en todas las redes públicas y de Internet para protegerse de los riesgos y amenazas de seguridad. En CX Cloud, es preferible que SNMPv3 esté configurado y no SNMPv2c, excepto para los dispositivos antiguos que carecen de compatibilidad integrada con SNMPv3. Si el usuario configura ambas versiones de SNMP, el agente CX intenta, de forma predeterminada, comunicarse con cada dispositivo respectivo mediante SNMPv3 y vuelve a SNMPv2c si la comunicación no se puede negociar correctamente.

## Protocolos de conectividad

Como parte de la configuración de conectividad directa de dispositivos, los usuarios deben especificar detalles del protocolo de conectividad de dispositivos: SSH (o, alternativamente, Telnet). Se debe utilizar SSHv2, excepto en los casos de recursos heredados individuales que carecen de la compatibilidad integrada adecuada. Tenga en cuenta que el protocolo SSHv1 contiene vulnerabilidades fundamentales. A falta de seguridad adicional, los datos de telemetría y los activos subyacentes pueden verse comprometidos debido a estas vulnerabilidades cuando se confía en SSHv1. Telnet también es inseguro. La información de credenciales (p. ej., nombres de usuario y contraseñas) enviada a través de telnet no está cifrada y, por lo tanto, es vulnerable a peligros, sin seguridad adicional.

## Limitaciones del procesamiento de telemetría para dispositivos

Las siguientes son limitaciones al procesar datos de telemetría para dispositivos:

- Es posible que algunos dispositivos aparezcan como accesibles en el Resumen de la recopilación, pero no se ven en la página Activos en la nube de CX.
- Si un dispositivo del archivo simiente o de las colecciones de rangos de IP también es parte del inventario de Catalyst Center, el dispositivo se informa solamente una vez para la entrada de Catalyst Center. Los dispositivos respectivos dentro del archivo simiente o la entrada de rango de IP se omiten para evitar la duplicación.
- Los teléfonos IP de Cisco no son compatibles con CX Cloud para la recopilación de datos por parte del agente CX. Como resultado, los teléfonos IP de Cisco no se muestran en la lista de recursos.

## Adición de otros activos mediante un archivo simiente

Un archivo simiente es un archivo .csv donde cada línea representa un registro de datos del sistema. En un archivo simiente, cada registro de archivo simiente corresponde a un dispositivo único desde el cual el agente CX debe recopilar la telemetría. Todos los mensajes de error o de información para cada entrada de dispositivo del archivo simiente que se está importando se capturan como parte de los detalles del registro de trabajos. Todos los dispositivos de un archivo simiente se consideran dispositivos administrados, incluso si no se puede acceder a ellos en el momento de la configuración inicial. En caso de que se cargue un nuevo archivo simiente para sustituir al anterior, se mostrará la fecha de la última carga en CX Cloud.

El agente CX intentará conectarse a los dispositivos, pero es posible que no pueda procesar cada uno de ellos para mostrarlos en las páginas Assets en los casos en los que no pueda determinar las PID o los números de serie.

Se omitirá cualquier fila del archivo simiente que comience con un punto y coma. La fila de encabezado del archivo simiente comienza con un punto y coma y se puede mantener tal cual (opción recomendada) o eliminarse mientras se crea el archivo simiente del cliente.

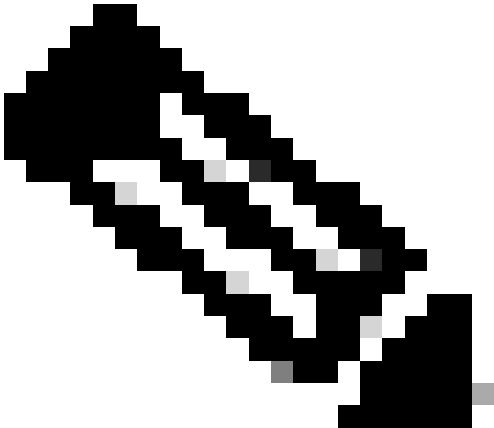
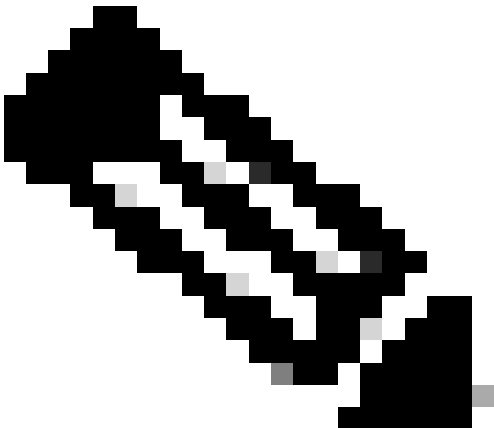
Los usuarios pueden cargar un archivo de inicialización de Common Services Platform Collector (CSPC) de la misma forma que un archivo de inicialización de nube CX estándar, y cualquier cambio de formato necesario se gestiona en la nube CX.

Para CX Agent v3.1 y versiones posteriores, los clientes pueden cargar archivos de inicialización en formato CSPC o CX; sólo el archivo de inicialización con formato CX es compatible con las versiones anteriores del agente CX.

Es importante que el formato del archivo simiente de ejemplo, incluidos los encabezados de columna, no se modifique en modo alguno.

En la tabla siguiente se identifican todas las columnas del archivo simiente necesarias y los datos que se deben incluir en cada columna.

| Columna de archivo<br>simiente | Encabezado/identificador de<br>columna                                         | Objetivo de la columna                                                                                                                                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R                              | Dirección IP o nombre de<br>host                                               | Proporcione una dirección IP o nombre de<br>host válidos y únicos para el dispositivo.                                                                                                                                                                          |
| B                              | versión del protocolo SNMP                                                     | El agente CX requiere el protocolo SNMP, que<br>se utiliza para la detección de dispositivos en<br>la red del cliente. Los valores pueden ser<br>snmpv2c o snmpv3, pero se recomienda<br>snmpv3 debido a consideraciones de<br>seguridad.                       |
| C                              | snmpRo : Obligatorio si<br>col#=3 se selecciona como<br>'snmpv2c'              | Si se selecciona la variante heredada de<br>SNMPv2 para un dispositivo específico, se<br>deben especificar las credenciales snmpRO<br>(de solo lectura) para la recopilación SNMP<br>del dispositivo. De lo contrario, la entrada<br>puede estar en blanco.     |
| D                              | snmpv3NombreDeUsuario:<br>Obligatorio si col#=3 se<br>selecciona como 'snmpv3' | Si se selecciona SNMPv3 para comunicarse<br>con un dispositivo específico, se debe<br>proporcionar el nombre de usuario de inicio de<br>sesión correspondiente.                                                                                                 |
| E                              | snmpv3AuthAlgorithm: Los<br>valores pueden ser MD5 o<br>SHA                    | El protocolo SNMPv3 permite la autenticación<br>mediante el resumen de mensajes (MD5) o el<br>algoritmo hash seguro (SHA). Si el dispositivo<br>está configurado con autenticación segura, se<br>debe proporcionar el algoritmo de<br>autenticación respectivo. |

| Columna de archivo<br>simiente | Encabezado/identificador de<br>columna                      | Objetivo de la columna                                                                                                                                                                                                                                               |
|--------------------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |                                                             |  <p>Nota: MD5 se considera inseguro y SHA se puede utilizar en todos los dispositivos que lo admitan.</p>                                                                          |
| F                              | snmpv3AuthPassword:<br>contraseña                           | Si se configura un algoritmo criptográfico MD5 o SHA en el dispositivo, se debe proporcionar la contraseña de autenticación relevante para el acceso del dispositivo.                                                                                                |
| G                              | snmpv3PrivAlgorithm: los<br>valores pueden ser DES,<br>3DES | <p>Si el dispositivo se configura con el algoritmo de privacidad SNMPv3 (este algoritmo se utiliza para cifrar la respuesta), se debe proporcionar el algoritmo respectivo.</p>  |

| Columna de archivo<br>simiente | Encabezado/identificador de<br>columna                                                                                                                         | Objetivo de la columna                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |                                                                                                                                                                | <p>Nota: Las claves de 56 bits que utiliza el estándar de cifrado de datos (DES) se consideran demasiado cortas para proporcionar seguridad criptográfica y dicho estándar se puede utilizar en todos los dispositivos que lo admitan.</p>                                                                                                                                                                                                                                                   |
| H                              | snmpv3PrivPassword:<br>contraseña                                                                                                                              | Si el algoritmo de privacidad SNMPv3 está configurado en el dispositivo, se debe proporcionar su contraseña de privacidad respectiva para la conexión del dispositivo.                                                                                                                                                                                                                                                                                                                       |
| I                              | snmpv3EngineID: engineID,<br>ID único que representa el<br>dispositivo, especifique el ID<br>del motor si está configurado<br>manualmente en el<br>dispositivo | El EngineID de SNMPv3 es un ID único que representa cada dispositivo. El agente CX envía este ID de motor como referencia mientras recopila los conjuntos de datos SNMP. Si el cliente configura el EngineID manualmente, se debe proporcionar el EngineID respectivo.                                                                                                                                                                                                                       |
| J                              | cliProtocol: los valores<br>pueden ser 'telnet', 'sshv1',<br>'sshv2'. Si está vacío, se<br>puede establecer como<br>'sshv2' de forma<br>predeterminada         | La interfaz de línea de comandos (CLI) está diseñada para interactuar directamente con el dispositivo. El agente CX utiliza este protocolo para la recopilación CLI de un dispositivo específico. Estos datos de recopilación de CLI se utilizan para los activos y otros informes de perspectivas en la nube de CX. Se recomienda SSHv2; a falta de otras medidas de seguridad de la red, los protocolos SSHv1 y Telnet no proporcionan por sí mismos una seguridad de transporte adecuada. |
| K                              | cliPort: Número de puerto<br>del protocolo CLI                                                                                                                 | Si se selecciona cualquier protocolo CLI, se debe proporcionar su número de puerto respectivo. Por ejemplo, 22 para SSH y 23 para telnet.                                                                                                                                                                                                                                                                                                                                                    |

| Columna de archivo<br>simiente | Encabezado/identificador de<br>columna                                                                                                                                           | Objetivo de la columna                                                                                                                                                                             |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L                              | cliUser: Nombre de usuario de CLI (se puede proporcionar el nombre de usuario/contraseña de CLI o BOTH, PERO ambas columnas (col#=12 y col#=13) no pueden estar vacías.)         | Se debe proporcionar el nombre de usuario de CLI correspondiente del dispositivo. El agente en la nube de CX lo utiliza en el momento de conectarse al dispositivo durante la recopilación de CLI. |
| M                              | cliPassword: Contraseña de usuario de CLI (se puede proporcionar el nombre de usuario/contraseña de CLI o BOTH, PERO ambas columnas (col#=12 y col#=13) no pueden estar vacías.) | Se debe proporcionar la contraseña CLI correspondiente del dispositivo. El agente CX lo utiliza en el momento de conectarse al dispositivo durante la recopilación de CLI.                         |
| N                              | cliEnableUser                                                                                                                                                                    | Si se configura enable en el dispositivo, se debe proporcionar el valor enableUsername del dispositivo.                                                                                            |
| O                              | cliEnablePassword                                                                                                                                                                | Si se configura enable en el dispositivo, se debe proporcionar el valor enablePassword del dispositivo.                                                                                            |
| P                              | Asistencia futura (no se necesitan entradas)                                                                                                                                     | Reservado para futuro uso                                                                                                                                                                          |
| A                              | Asistencia futura (no se necesitan entradas)                                                                                                                                     | Reservado para futuro uso                                                                                                                                                                          |
| R                              | Asistencia futura (no se necesitan entradas)                                                                                                                                     | Reservado para futuro uso                                                                                                                                                                          |
| S                              | Asistencia futura (no se necesitan entradas)                                                                                                                                     | Reservado para futuro uso                                                                                                                                                                          |

## Adición de otros activos mediante un nuevo archivo simiente

Para agregar otros recursos mediante un nuevo archivo simiente:

1. Haga clic en Agregar origen de datos en la ventana Centro de administración > Orígenes de datos.

### Add Data Source

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

Add Data Source

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

Add Data Source

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

Add Data Source

**Contracts**  
Supports assets associated with a contract

Add Data Source

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

Add Data Source

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

Add Data Source

**Meraki dashboard**  
Supports Meraki

Add Data Source

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

Add Data Source

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

Add Data Source

**Webex**  
Supports the Success Track for Collaboration

Add Data Source

Agregar origen de datos

2. Haga clic en Agregar origen de datos en la opción Otros activos por archivo simiente.

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

Select option ▼

---

Cancel Continue



Seleccionar agente CX

3. Seleccione el agente CX en la lista desplegable ¿Qué agente en la nube CX desea conectar a?

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

O/C\_Team\_test\_CXCAGent\_IP\_104 ▼

---

Cancel Continue

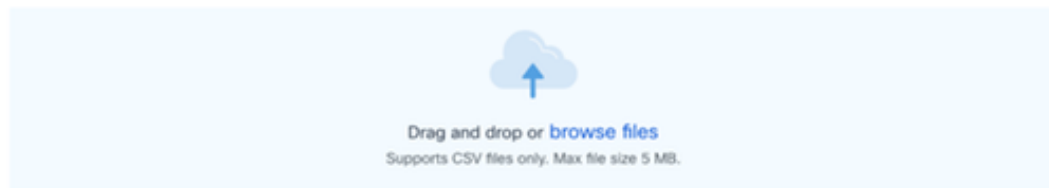


Continúe

4. Haga clic en Continue (Continuar). Se muestra la página Upload Your Seed File.

### Upload your seed file

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



### Schedule inventory collection

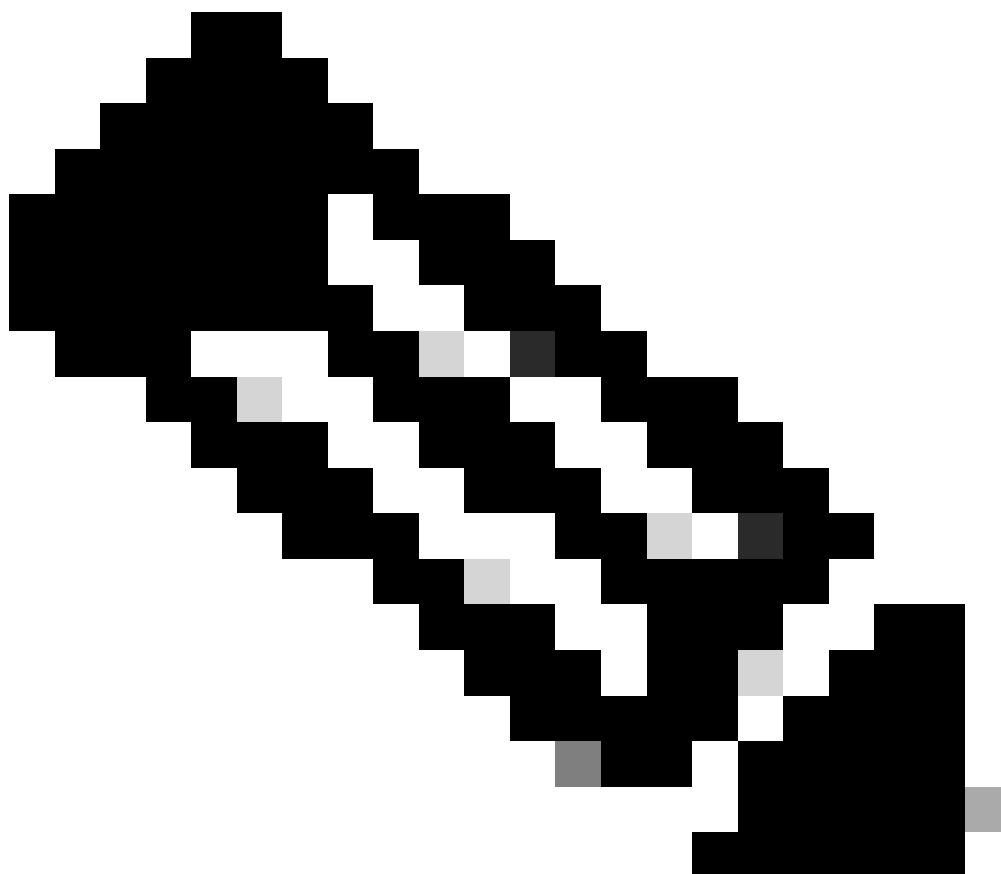
| Frequency   | Select time | Time Zone               |
|-------------|-------------|-------------------------|
| Frequency ▾ | 12:00 ▾     | AM ▾                    |
|             |             | Europe/Amsterdam (... ▾ |

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

Connect

Cargue el archivo simiente

5. Haga clic en la plantilla de archivo simiente con hipervínculo para descargar la plantilla.
6. Introduzca o importe manualmente los datos en el archivo. Una vez completada, guarde la plantilla como un archivo .csv para importar el archivo al agente CX.
7. Arrastre y suelte o haga clic en examinar archivos para cargar el archivo .csv.
8. Complete la sección Programar recopilación de inventario.



Nota: Antes de que se complete la configuración inicial de CX Cloud, CX Cloud Agent debe realizar la primera recopilación de telemetría procesando el archivo simiente y estableciendo la conexión con todos los dispositivos identificados. La recopilación se puede iniciar a demanda o ejecutarse según una programación definida aquí. Los usuarios pueden realizar la primera conexión de telemetría activando la casilla de verificación Ejecutar la primera recopilación ahora. Dependiendo del número de entradas especificadas en el archivo simiente y de otros factores, este proceso puede tardar bastante tiempo.

- 
9. Haga clic en Connect (Conectar) Se abre la ventana Orígenes de datos, que muestra un mensaje de confirmación.

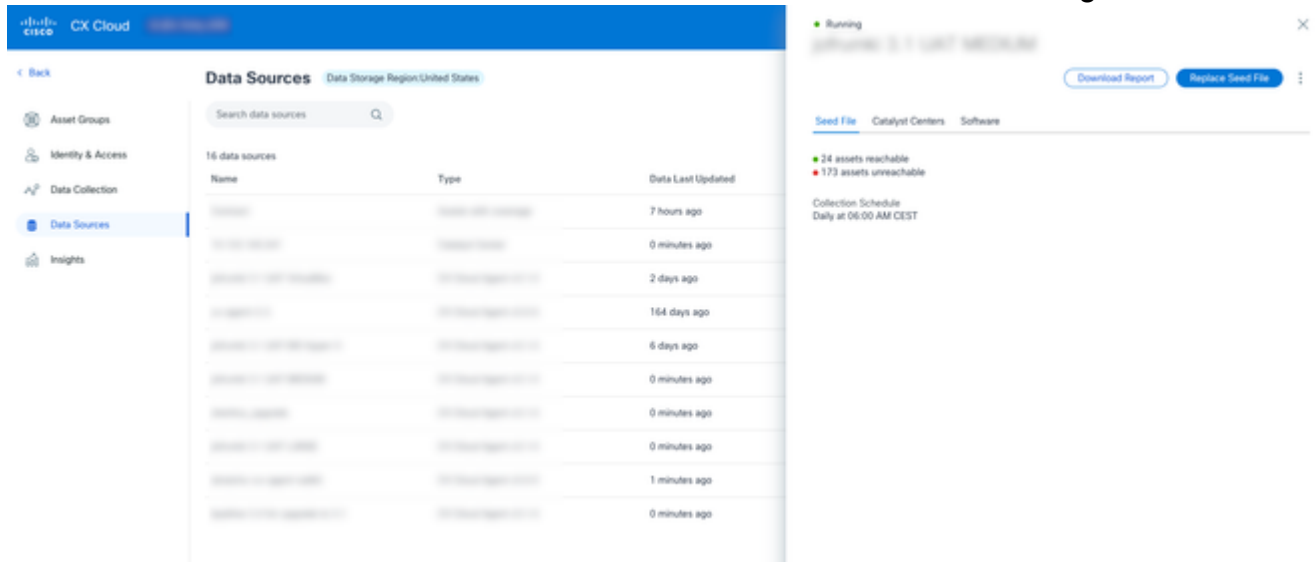
## Adición de otros activos mediante un archivo simiente modificado

Para agregar, modificar o eliminar dispositivos mediante el archivo simiente actual:

1. Abra el archivo simiente creado anteriormente, realice los cambios necesarios y guarde el archivo.

 **Nota:** Para agregar activos al archivo simiente, anexe esos activos al archivo simiente creado anteriormente y vuelva a cargar el archivo. Esto es necesario ya que cargar un nuevo archivo simiente reemplaza al actual. Para la detección y la recopilación, sólo se utiliza el último archivo simiente cargado.

2. En la página Orígenes de datos, haga clic en el origen de datos del agente CX que requiere un archivo simiente actualizado. Se abre la ventana de detalles CX Cloud Agent.

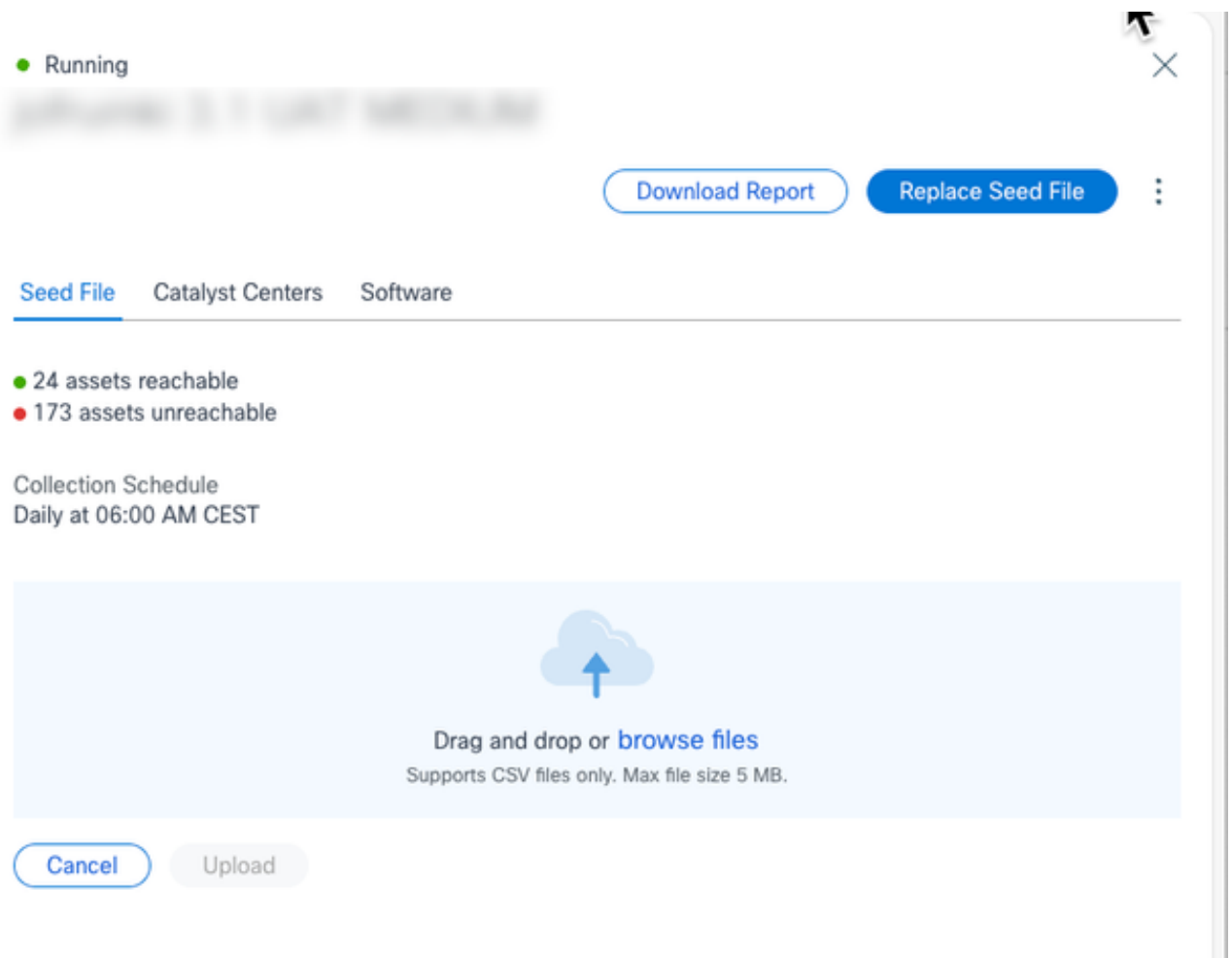


The screenshot displays the Cisco CX Cloud interface. The main section is titled 'Data Sources' and shows a list of 16 data sources. The table has columns for 'Name', 'Type', and 'Data Last Updated'. The 'Data Sources' tab is selected in the left sidebar. On the right, there is a 'Seed File' section with a 'Replace Seed File' button and a status indicator showing 24 assets reachable and 173 assets unreachable.

| Name | Type | Data Last Updated |
|------|------|-------------------|
| ...  | ...  | 7 hours ago       |
| ...  | ...  | 0 minutes ago     |
| ...  | ...  | 2 days ago        |
| ...  | ...  | 164 days ago      |
| ...  | ...  | 6 days ago        |
| ...  | ...  | 0 minutes ago     |
| ...  | ...  | 0 minutes ago     |
| ...  | ...  | 0 minutes ago     |
| ...  | ...  | 0 minutes ago     |
| ...  | ...  | 1 minutes ago     |
| ...  | ...  | 0 minutes ago     |

Archivo simiente

3. Haga clic en Replace Seed File.



Reemplazar archivo simiente

4. Arrastre y suelte o haga clic en examinar archivos para cargar el archivo simiente modificado.
5. Haga clic en Cargar.

## Credenciales por Defecto para el Archivo Inicial

El agente CX proporciona credenciales predeterminadas que los clientes pueden configurar localmente en el agente, lo que elimina la necesidad de incluir contraseñas confidenciales directamente en el archivo simiente. Esto mejora la seguridad al reducir la exposición de la información confidencial y dar respuesta a una preocupación clave del cliente.

## Adición de otros activos mediante rangos de IP

Los rangos de IP permiten a los usuarios identificar los activos de hardware y, posteriormente, recopilar la telemetría de esos dispositivos en función de las direcciones IP. Los dispositivos para la recopilación de telemetría se pueden identificar de forma exclusiva mediante la especificación de un único rango de IP de nivel de red, que el agente CX puede analizar mediante el protocolo SNMP. Si se elige el rango de IP para identificar un dispositivo conectado directamente, las direcciones IP a las que se hace referencia pueden ser lo más restrictivas posible, a la vez que se permite la cobertura para todos los recursos requeridos.

- Se pueden proporcionar direcciones IP específicas, o se pueden utilizar comodines para reemplazar octetos de una dirección IP para crear un rango.
- Si una dirección IP específica no se incluye en el intervalo IP identificado durante la configuración, el agente CX no intenta comunicarse con un dispositivo que tenga dicha dirección IP ni recopila telemetría de dicho dispositivo.
- Si introduce \*.\*.\*, el agente CX podrá utilizar las credenciales proporcionadas por el usuario con cualquier dirección IP. Por ejemplo: 172.16.\*.\* permite que las credenciales se utilicen para todos los dispositivos de la subred 172.16.0.0/16.
- Si se produce algún cambio en la red o en la base instalada (IB), se puede modificar el intervalo IP. Consulte la sección [Edición de Intervalos IP](#)

El agente CX intentará conectarse a los dispositivos, pero es posible que no pueda procesar cada uno para mostrarlo en la vista Assets en los casos en los que no pueda determinar los PID o los números de serie.



#### Notas:

Al hacer clic en Editar intervalo de direcciones IP se inicia la detección de dispositivos a petición. Cuando se agrega o elimina un nuevo dispositivo (dentro o fuera) a un rango de IP especificado, el cliente siempre debe hacer clic en Editar rango de direcciones IP (consulte la sección [Edición de rangos de IP](#)) y completar los pasos necesarios para iniciar la detección de dispositivos bajo demanda para incluir cualquier dispositivo recién agregado al inventario de recolección de agentes CX.

---

Para agregar dispositivos mediante un intervalo IP, los usuarios deben especificar todas las credenciales aplicables a través de la interfaz de usuario de configuración. Los campos visibles varían en función de los protocolos seleccionados en las ventanas anteriores. Si se realizan varias selecciones para el mismo protocolo, por ejemplo, al seleccionar SNMPv2c y SNMPv3 o al seleccionar SSHv2 y SSHv1, el agente CX negocia automáticamente la selección del protocolo en función de las capacidades de cada dispositivo.

Al conectar dispositivos mediante direcciones IP, el cliente debe asegurarse de que todos los protocolos relevantes en el rango de IP junto con las versiones SSH y las credenciales Telnet sean válidos o las conexiones fallarán.

## Adición de otros recursos por intervalos de IP

Para agregar dispositivos mediante el intervalo IP:

1. Seleccione el icono Centro de Administración. Se abre la ventana Orígenes de Datos.
2. Haga clic en Agregar origen de datos en la ventana Centro de administración > Orígenes de datos.

## Add Data Source

Search data sources



### Catalyst Center

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

Add Data Source



### Cisco Catalyst SD-WAN Manager

Supports the Success Track for WAN

Add Data Source



### Common Services Platform Collector (CSPC)

Supports assets managed by CSPC

Add Data Source



### Contracts

Supports assets associated with a contract

Add Data Source



### CX Cloud Agent

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

Add Data Source



### Intersight

Supports the Data Center Compute and Data Center Networking Success Tracks

Add Data Source



### Meraki dashboard

Supports Meraki

Add Data Source



### Other Assets by IP Ranges

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

Add Data Source



### Other Assets by Seed File

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

Add Data Source



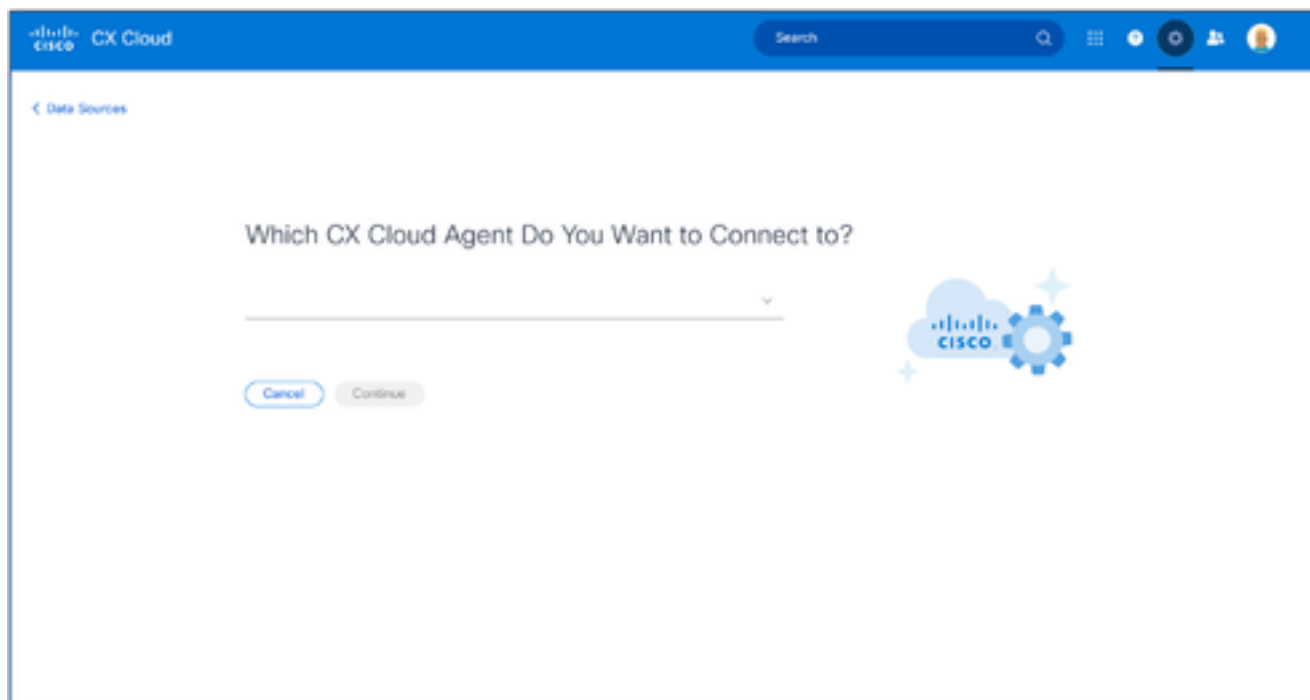
### Webex

Supports the Success Track for Collaboration

Add Data Source

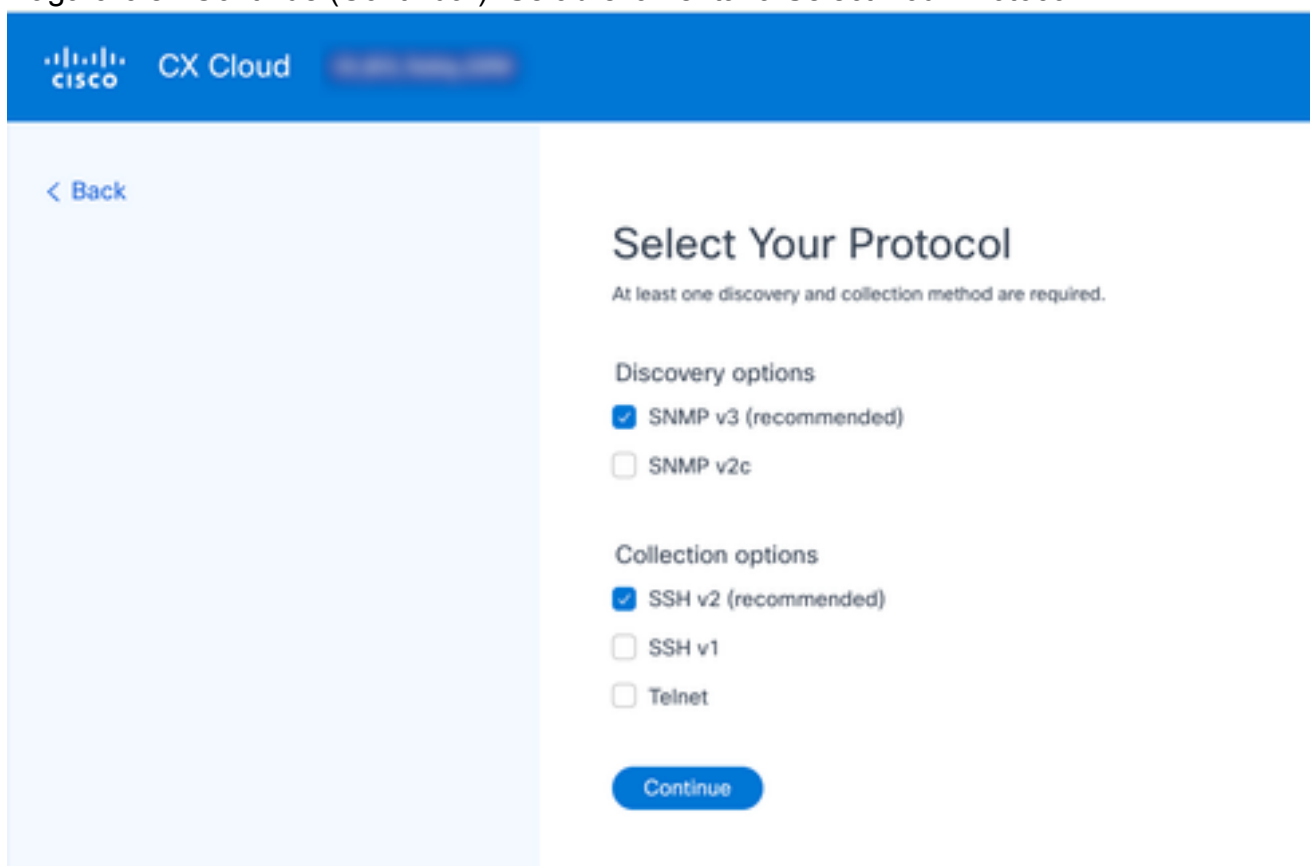
Agregar origen de datos

3. Haga clic en Add Data Source en la opción Other Assets by IP Ranges.



Seleccionar agente en la nube CX

4. Seleccione el agente CX en la lista desplegable ¿Qué agente en la nube CX desea conectar a?
5. Haga clic en Continue (Continuar). Se abre la ventana Select Your Protocol.



Seleccione su protocolo

6. Active las casillas de verificación correspondientes para las opciones de detección y las opciones de recopilación.

7. Haga clic en Continue (Continuar).

Provide Discovery Details

Edit the protocols

Starting IP Address

Ending IP Address

SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Select

Privacy Algorithm

Privacy Password

Select

SSHV2 credentials

Username

Password

Enable mode (optional)

Schedule Inventory Collection

Frequency

Select Time

Freq...

12:00

AM

WEDT

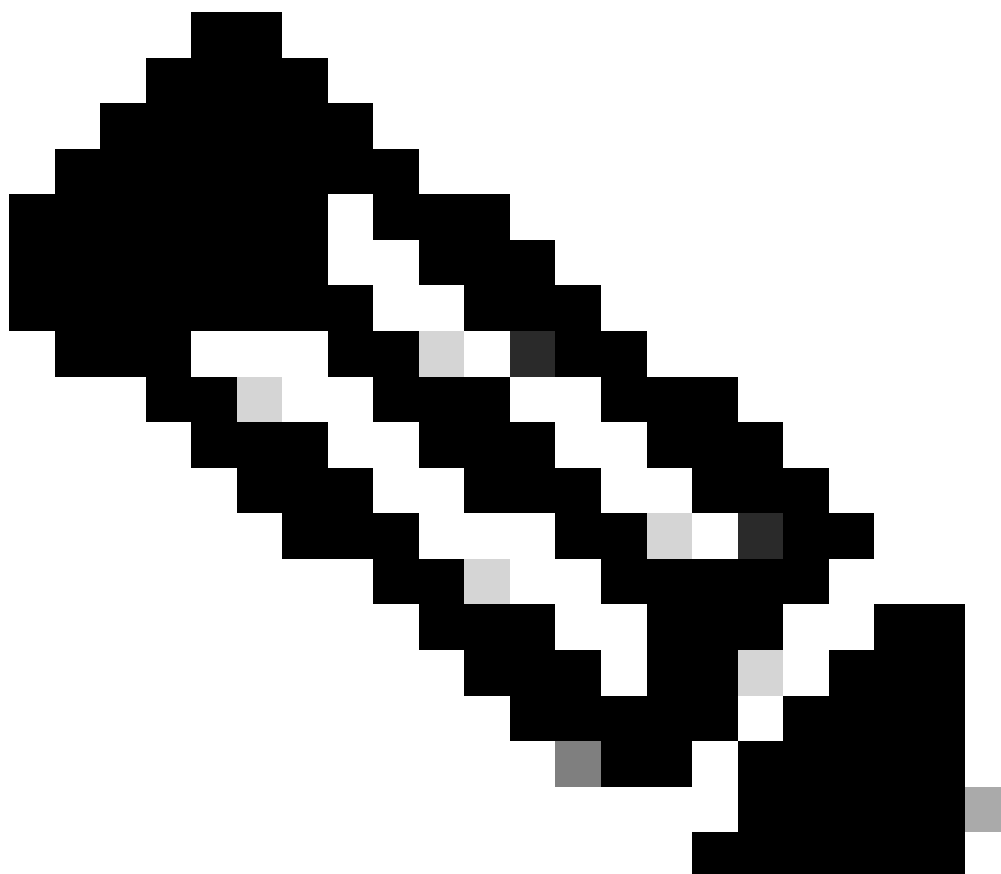
☒ Run the first collection now (this may take up to 75 minutes)

Add Another IP Range

Complete Setup

Detalles de descubrimiento

8. Introduzca los detalles necesarios en las secciones Proporcionar detalles de detección y Programar recopilación de inventario.



Nota: Para agregar otro rango de IP para el agente CX seleccionado, haga clic en Add Another IP Range para volver a la ventana Set Your Protocol y repita los pasos de esta sección.

- 
9. Haga clic en Complete Setup. Aparecerá una confirmación cuando la implementación se haya realizado correctamente.

**Data Sources** Region: United States

Search data sources

4 data sources

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

Mensaje de confirmación

## Edición de rangos IP

Para editar un intervalo IP:

1. Acceda a la ventana Orígenes de Datos.
2. Haga clic en el agente CX que requiera la edición del rango IP en Orígenes de datos. Se abrirá la ventana de detalles.

**Data Sources** Data Storage Region: United States

Search data sources

| Name                                | Type              |
|-------------------------------------|-------------------|
| Contract                            | Assets with cover |
| Cloud Network                       | Internight        |
| 10.126.77.82                        | Cisco DNA Cent    |
| CKCA-837-vishnu-agent-10.126.77.209 | CX Cloud Agent    |
| CX Cloud Agent1                     | CX Cloud Agent    |
| Agent 1_adhdhand_2.4-937_small_207  | CX Cloud Agent    |
| Agent 2_adhdhand_2.4-937_large_308  | CX Cloud Agent    |
| 10.126.77.85                        | Cisco DNA Cent    |
| OK_Team_Test_CXCAgent_IP_104        | CX Cloud Agent    |
| 10.126.77.82                        | Cisco DNA Cent    |

**Agent** Not running

Download Report Edit IP Ranges

IP Address Ranges Cisco DNA Centers Software

10010 assets reachable Show errors (1)

| IP Range      | Collection Schedule     | Last Discovered     |
|---------------|-------------------------|---------------------|
| 10.126.77.82  | Daily at 10:00 PM IST   | Rediscover IP range |
| 10.126.77.85  | Daily at 09:00 AM IST   | Rediscover IP range |
| 10.126.77.209 | Mondays at 08:00 AM IST | Rediscover IP range |
| 10.126.77.209 | Mondays at 04:00 AM IST | Rediscover IP range |

Orígenes de datos

3. Haga clic en Edit IP Address Range. Se abre la ventana Connect to CX Cloud.

**Provide Discovery Details** Edit the protocols

Starting IP Address Ending IP Address

SNMP V2c credentials

Read Community

SSHV2 credentials

Username Enable Username (Optional)

Password Enable Password (Optional)

Telnet credentials

Username Enable Username (Optional)

Password Enable Password (Optional)

Delete this IP range Add Another IP Range Complete Setup

4. Haga clic en Editar los protocolos. Se abre la ventana Select Your Protocol.

[< Back](#)

**Added IP Address Ranges (4)**

Edit

Edit

Edit

Edit

## Select Your Protocol

At least one discovery and collection method are required.

**Discovery options**

☐ SNMP v3 (recommended)

☒ SNMP v2c

**Collection options**

☒ SSH v2 (recommended)

☐ SSH v1

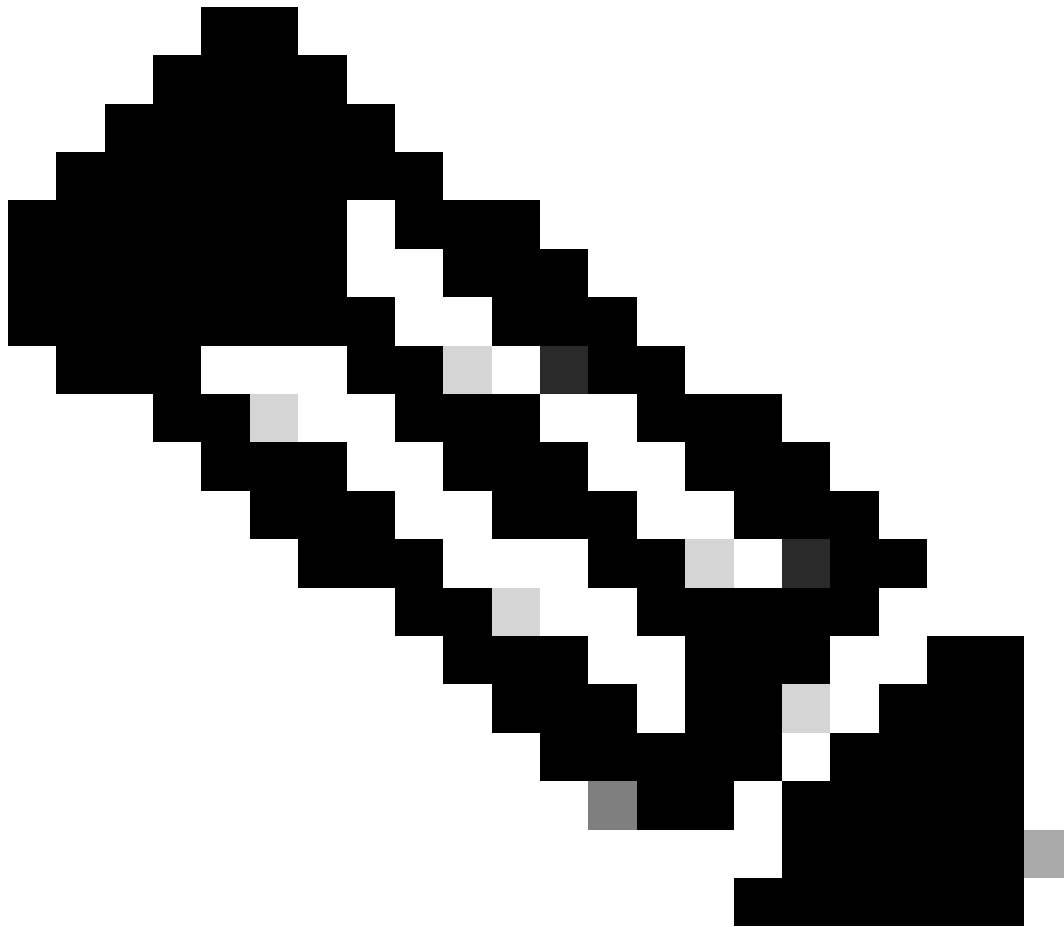
☒ Telnet

Continue

Selezionare il protocollo

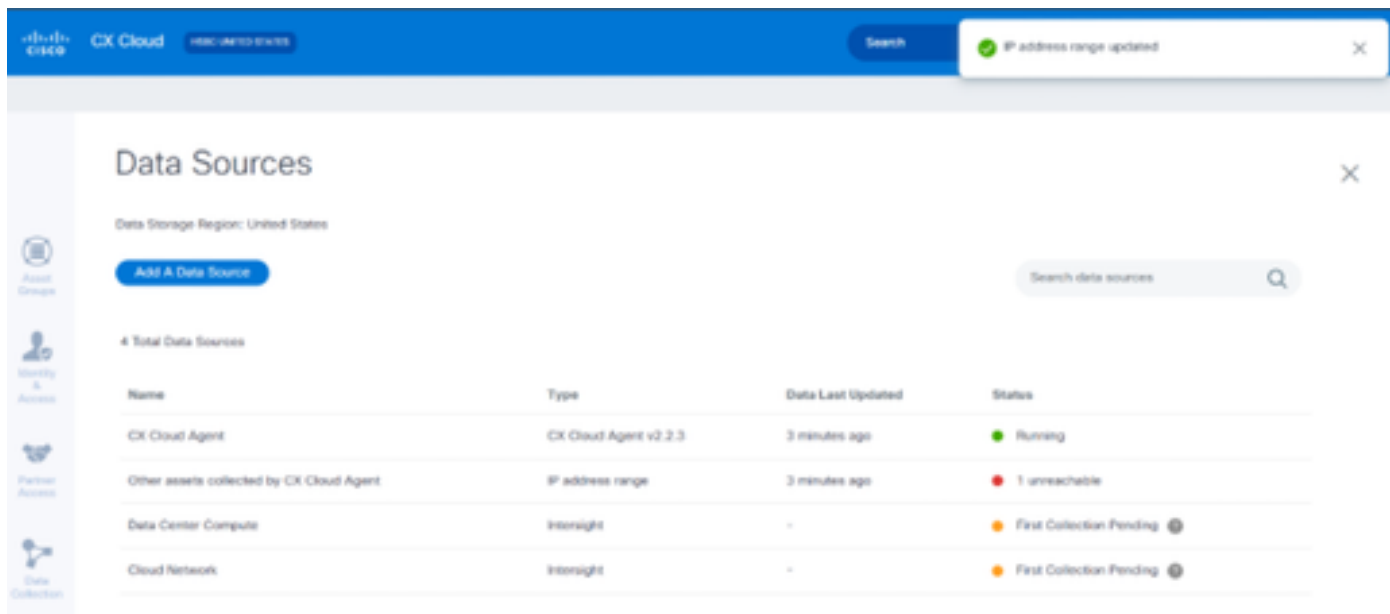
5. Selezionare le caselle di verifica corrispondenti per scegliere i protocolli applicabili e fare clic su Continuar per tornare alla finestra Fornire dettagli di rilevamento.





Nota: Este mensaje de confirmación no verifica si los dispositivos dentro del rango modificado son alcanzables o si sus credenciales son aceptadas. Esta confirmación se produce cuando el cliente inicia el proceso de detección.

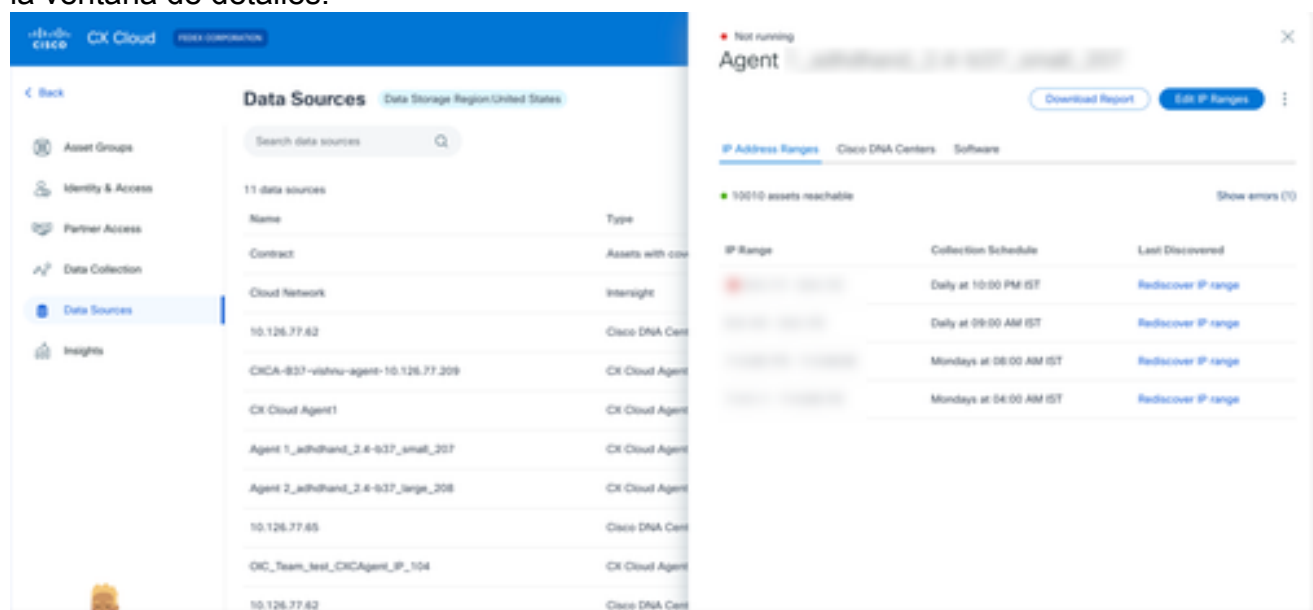
---



## Eliminando intervalo IP

Para eliminar un intervalo IP:

1. Acceda a la ventana Orígenes de Datos.
2. Seleccione el agente CX correspondiente con el intervalo IP que debe eliminarse. Se abrirá la ventana de detalles.



Orígenes de datos

3. Haga clic en Edit IP Ranges. Se abre la ventana Proporcionar detalles de detección.

 CX Cloud FEDEx CORPORATION

[< Back](#)

**Added IP Address Ranges (4)**

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

### Provide Discovery Details

[Edit the protocols](#)

Starting IP Address:  Ending IP Address:

**SNMP V2c credentials**

Read Community:

**SSHv2 credentials**

Username:  Enable Username (Optional):

Password:  Enable Password (Optional):

**Telnet credentials**

Username:  Enable Username (Optional):

Password:  Enable Password (Optional):

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

Proporcionar detalles de descubrimiento

4. Haga clic en el enlace Delete this IP range. Se muestra el mensaje de confirmación.



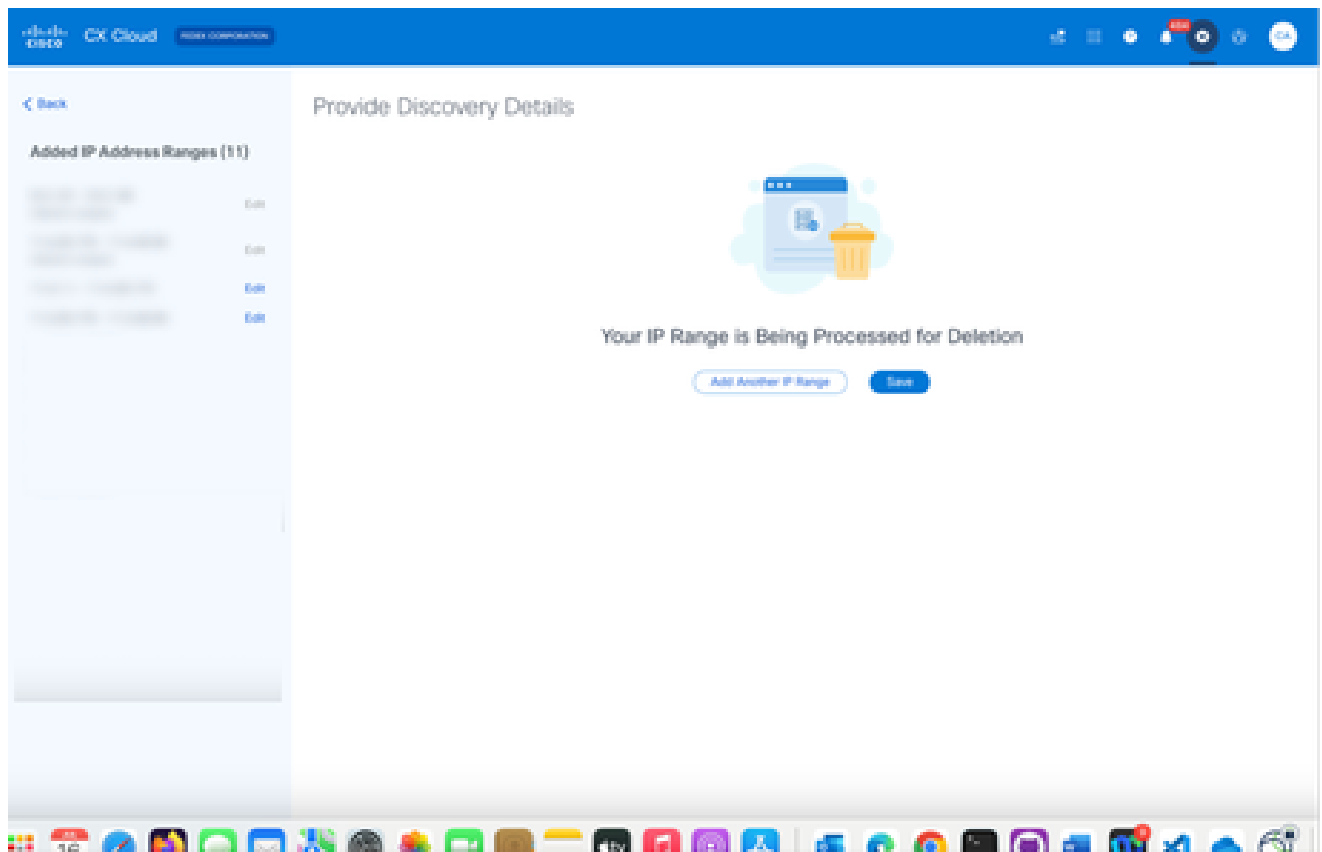
## Delete This IP Range

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

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

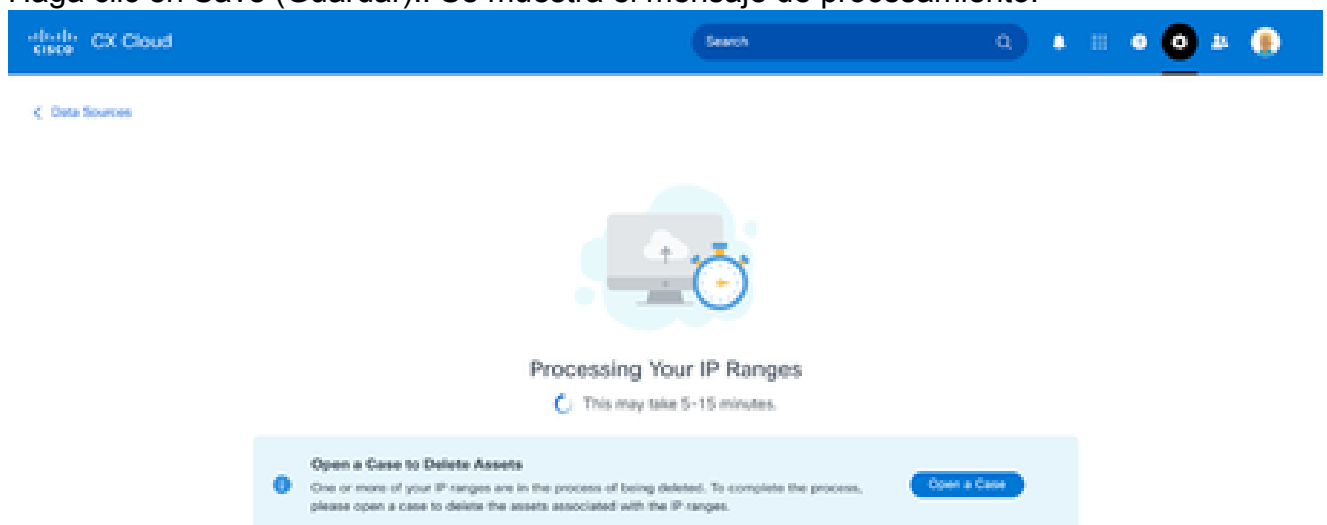
Confirmación Eliminar mensaje

5. Haga clic en Eliminar.



Eliminación de intervalo IP

6. Haga clic en Save (Guardar).. Se muestra el mensaje de procesamiento.



7. Haga clic en Abrir un caso para crear un caso y eliminar los recursos asociados con el rango de IP. Se abre la ventana Orígenes de datos, que muestra un mensaje de confirmación.

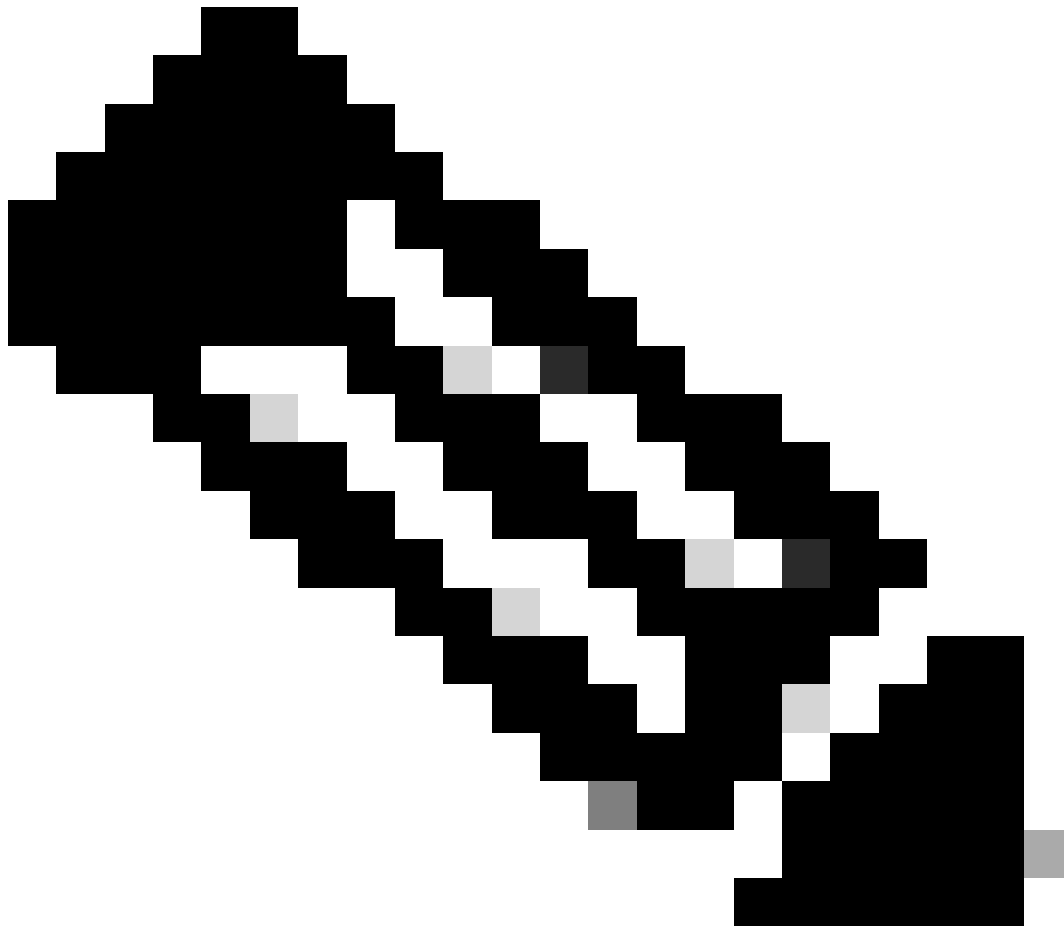
## Acerca de los dispositivos detectados desde varios controladores

Si el Catalyst Center y otros activos recopilados por el agente CX (conexión directa de dispositivos) están en el mismo agente CX, es posible que algunos dispositivos puedan ser descubiertos por el Cisco Catalyst Center y la conexión directa de dispositivos al agente CX, lo que provoca la recopilación de datos duplicados de esos dispositivos. Para evitar la recopilación de datos duplicados y que un solo controlador administre los dispositivos, se debe determinar una prioridad para la cual el agente CX administra los dispositivos.

- Si Cisco Catalyst Center descubre un dispositivo por primera vez y, a continuación, lo vuelve a descubrir mediante una conexión directa con el dispositivo (mediante un archivo simiente o un intervalo IP), Cisco Catalyst Center tiene prioridad a la hora de controlar el dispositivo.
- Si un dispositivo se descubre por primera vez mediante una conexión directa del dispositivo al agente CX y, a continuación, se redescubre mediante Cisco Catalyst Center, Cisco Catalyst Center tiene prioridad a la hora de controlar el dispositivo.

## Programación de análisis de diagnóstico

Los clientes pueden programar análisis de diagnóstico a demanda en la nube de CX para las pistas de éxito elegibles y sus dispositivos cubiertos para cumplimentar los errores prioritarios en Recomendaciones.



Nota: Cisco recomienda programar análisis de diagnóstico o iniciar análisis bajo demanda con un intervalo de al menos 6-7 horas entre las programaciones de recopilación de inventario para que no se superpongan. La ejecución simultánea de varias exploraciones de diagnóstico puede ralentizar el proceso de exploración y, potencialmente, provocar errores de exploración.

---

Para programar análisis de diagnóstico:

1. En la página Inicio, haga clic en el icono Configuración (engranaje).
2. En la página Orígenes de datos, seleccione Recopilación de datos en el panel izquierdo.
3. Haga clic en Schedule Scan.

## Data Collection

Diagnostic Scans ⓘ

Schedule Scan

< October 2022 >

Sun Mon Tue Wed Thu Fri Sat

1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

23 24 25 26 27 28 29

30 31

No Diagnostic Scans Found

Inventory Collection ⓘ

3 Collections

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

Programación de análisis

4. Configure una planificación para este análisis.

### 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 programación de análisis

5. En la lista de dispositivos, seleccione todos los dispositivos para la exploración y haga clic en Agregar.

## New Scheduled Scan

Data Sources

Other assets collected by CX Cloud Agent X

Schedule

Frequency at Time IST Save Changes

Description (Optional)

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

Add >

< Remove

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

1 2 Next

Programar análisis

6. Haga clic en Save Changes cuando la programación se complete.

Las exploraciones de diagnóstico y las programaciones de recopilación de inventario se pueden editar y eliminar desde la página Recopilación de datos.

Asset Groups

Identity & Access

Partner Access

**Data Collection**

Data Sources

Insights

Automation

## Data Collection

Diagnostic Scans

2 Scans

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

Inventory Collection

8 Collections

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

Schedule Scan

October 2022

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
|     |     |     |     |     |     | 1   |
| 3   | 4   | 5   | 6   | 7   | 8   |     |
| 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

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

[View detailed instructions](#)

Recopilación de datos con las opciones Editar y Eliminar programación

## Actualización de VM de agente CX a configuraciones medianas y

## grandes

Una vez que se actualizan las VM, no es posible:

- Reducir de una configuración grande o mediana a una pequeña
- Reducir de una configuración grande a mediana
- Actualizar de una configuración mediana a una grande

Antes de actualizar la VM, Cisco recomienda tomar una instantánea con el fin de recuperarla en caso de fallo. Consulte [Copia de seguridad y restauración de la VM en la nube de CX](#) para obtener más información.

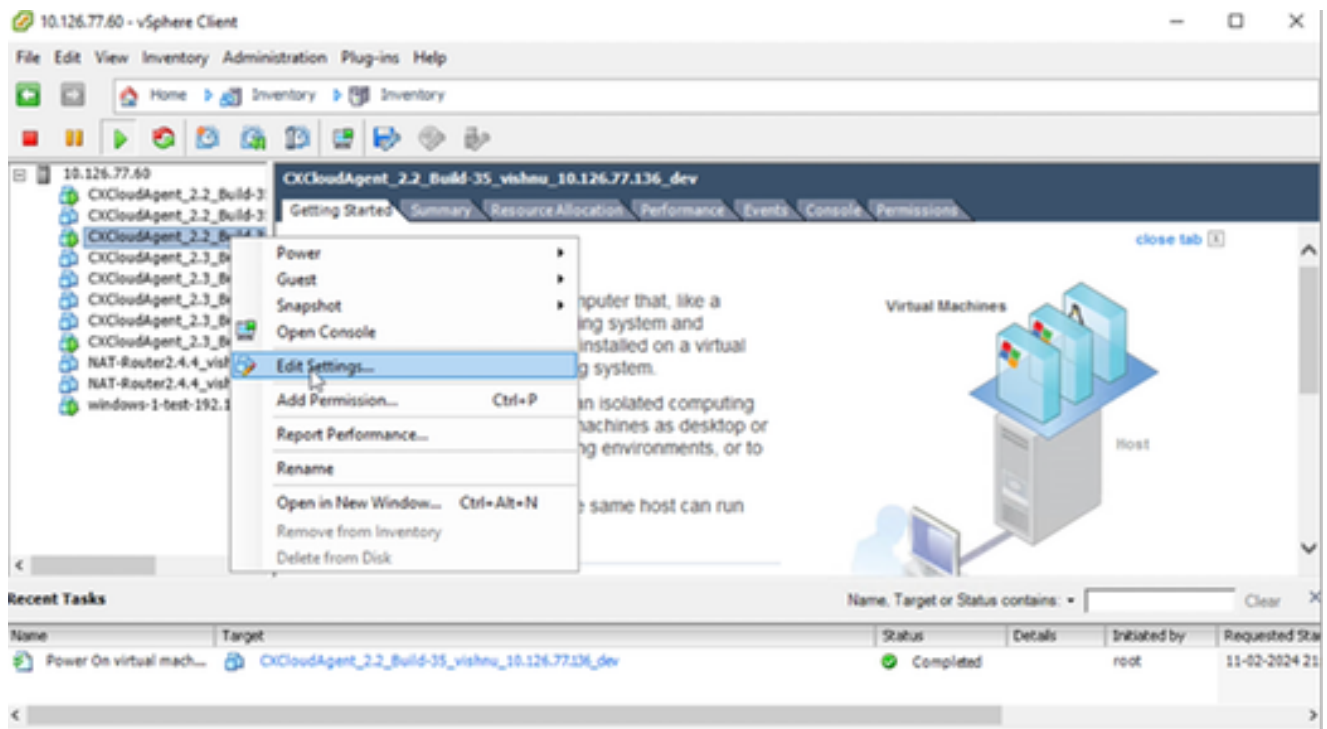
## Reconfiguración mediante VMware vSphere Thick Client

Para actualizar la configuración de VM con el cliente VMware vSphere Thick existente:



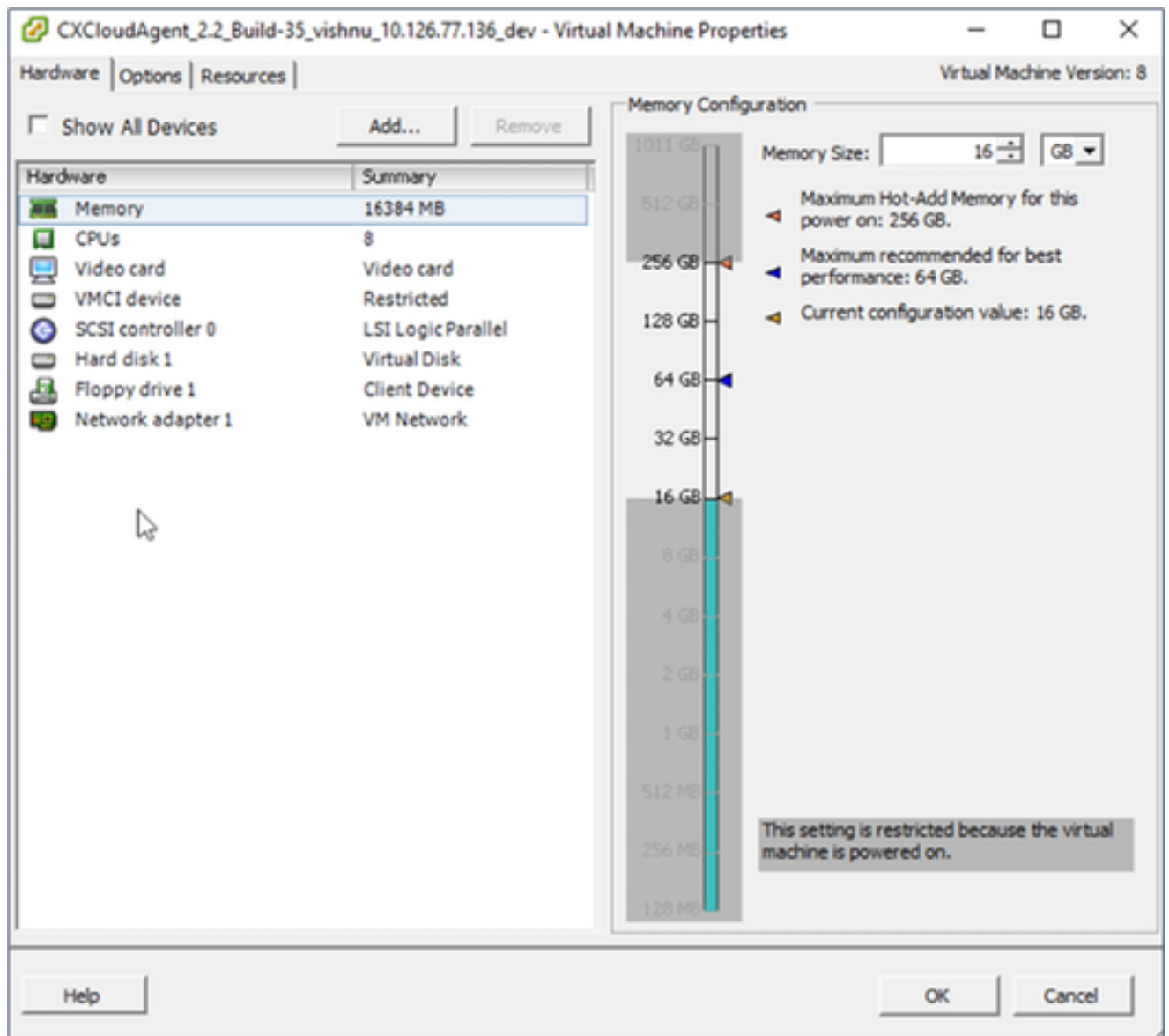
Cliente vSphere

1. Inicie sesión en VMware vSphere Client. La página Inicio muestra una lista de VM.



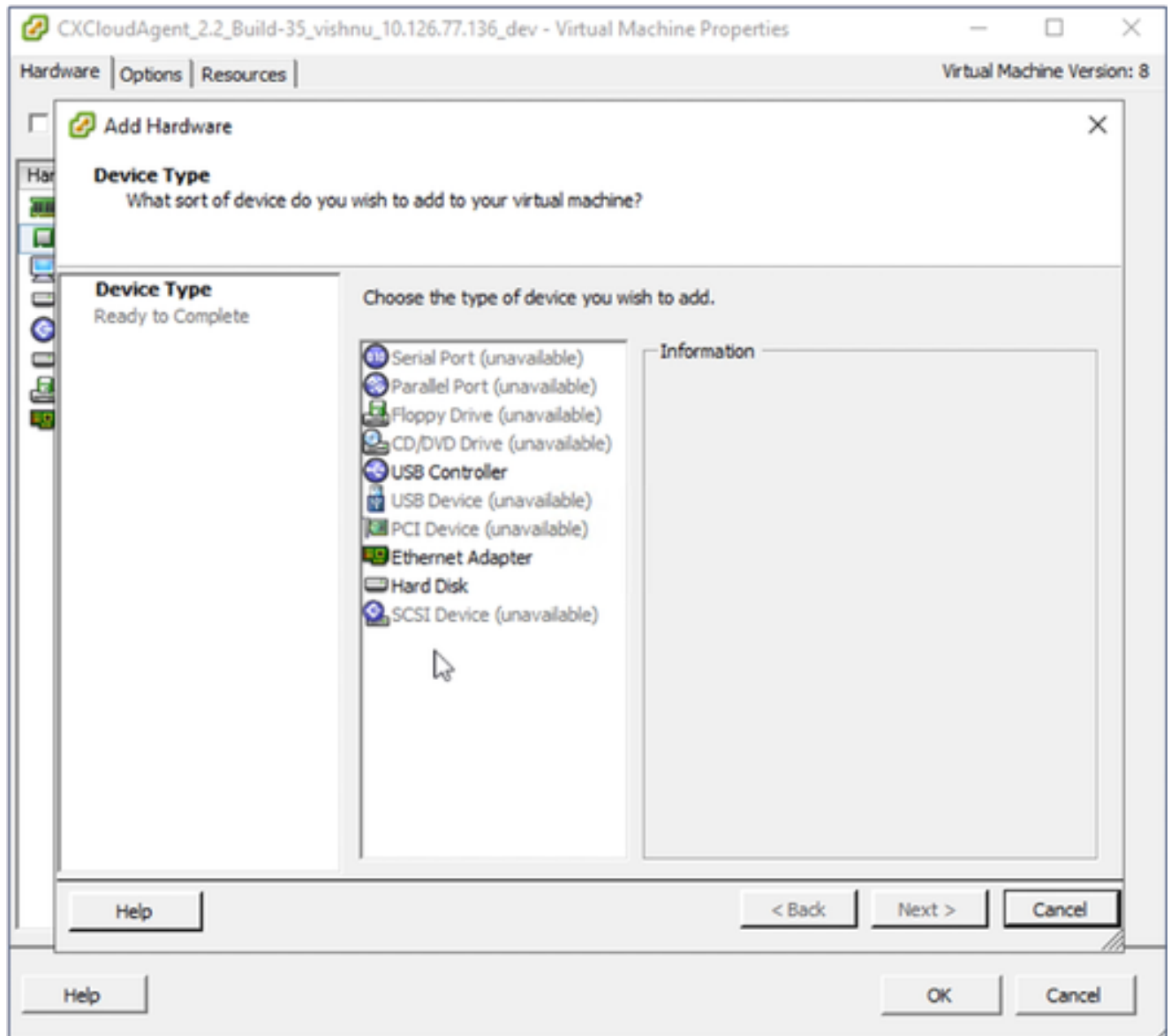
Editar configuración

2. Haga clic con el botón derecho del ratón en la VM de destino y seleccione Editar configuración en el menú. Se abre la ventana VM Properties.



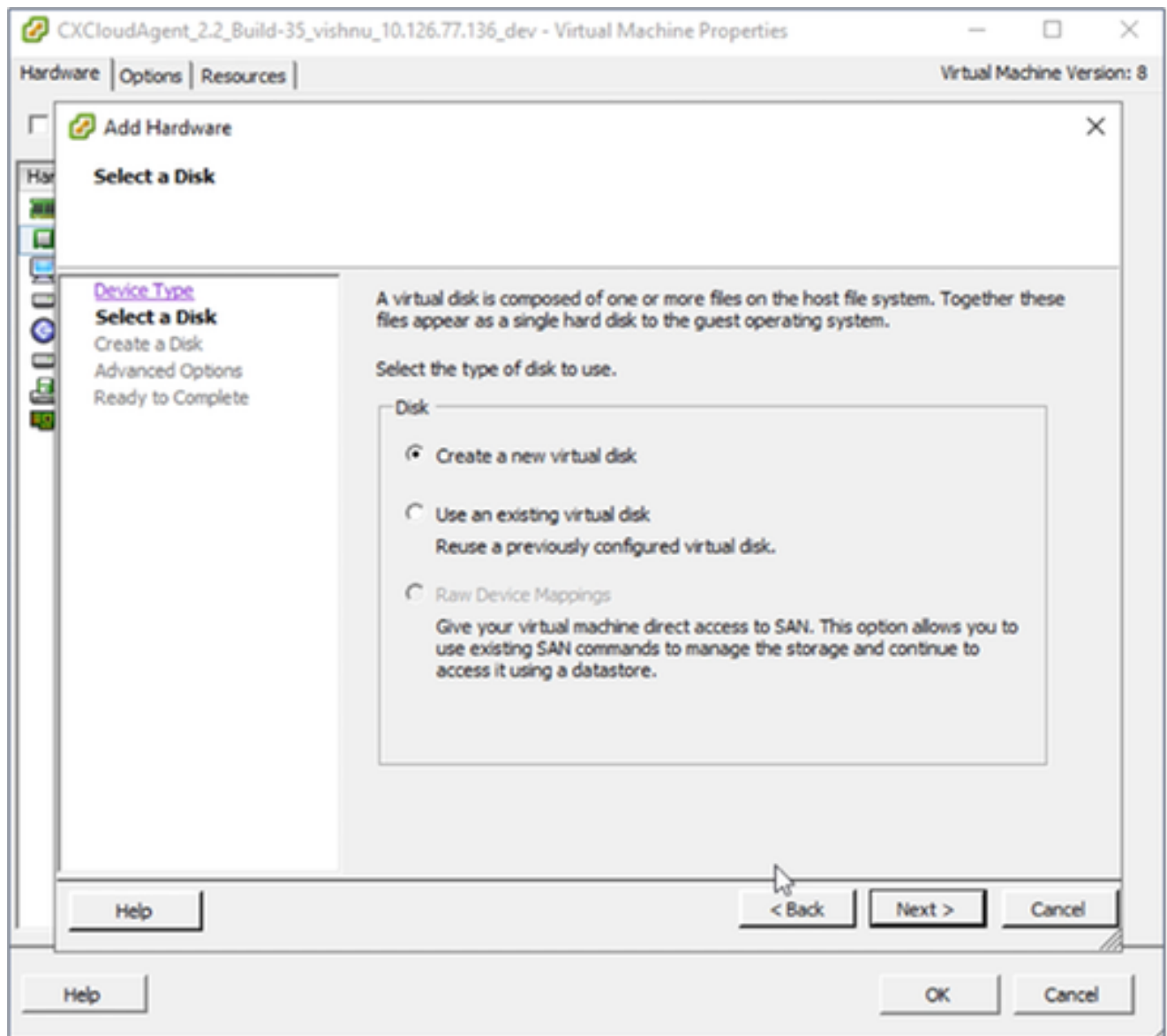
Propiedades de VM

3. Actualice los valores de Memory Size según lo especificado:  
 Media: 32 GB (32768 MB)  
 Grande: 64 GB (65536 MB)
4. Seleccione CPUs y actualice los valores según lo especificado:  
 Medio: 16 núcleos (8 sockets, \*2 núcleos/socket)  
 Grande: 32 núcleos (16 zócalos \*2 núcleos/zócalo)
5. Haga clic en Add (Agregar). Se abrirá la ventana Add Hardware.



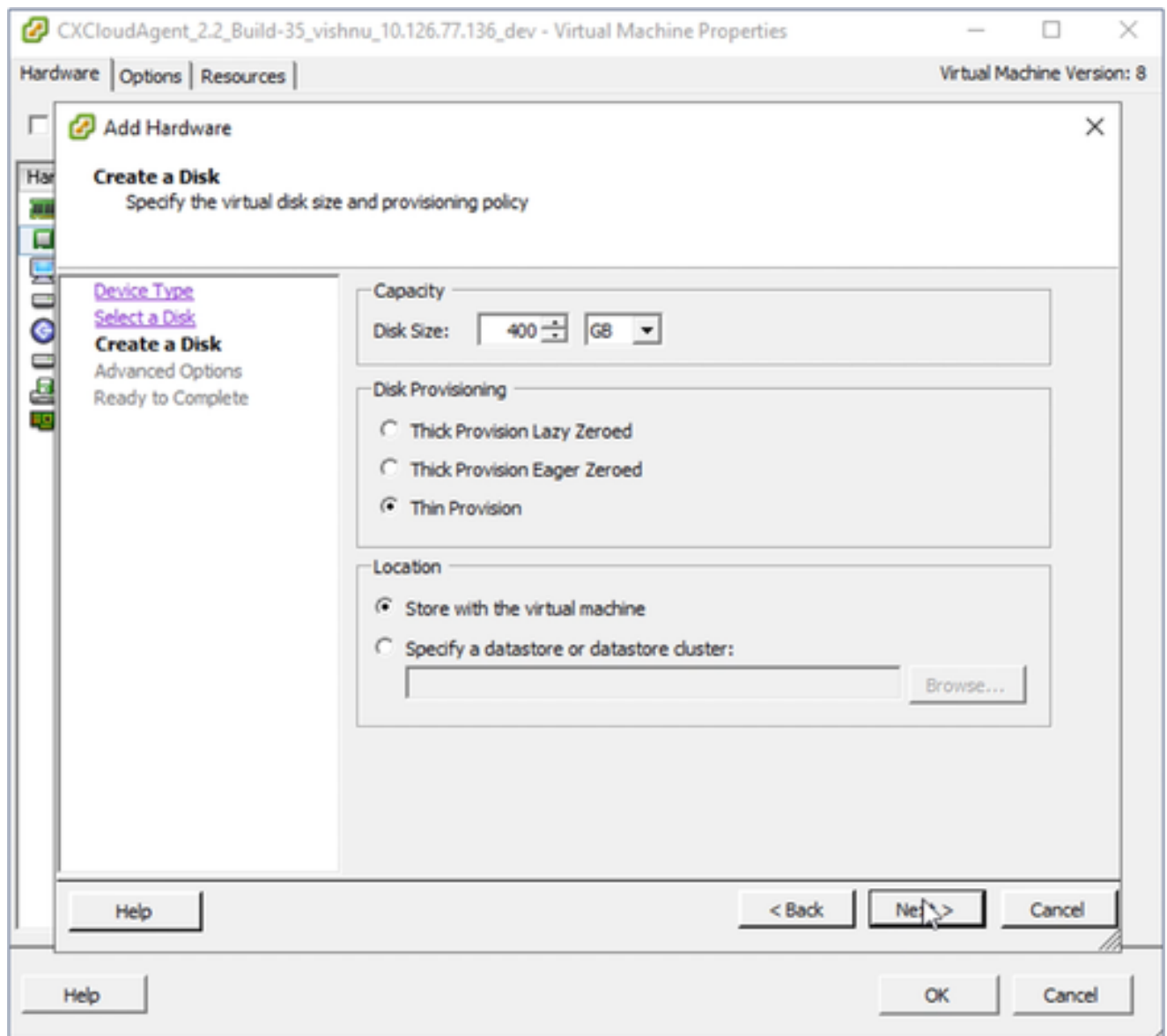
tipo de dispositivo

6. Seleccione Disco duro como el tipo de dispositivo.
7. Haga clic en Next (Siguiente).



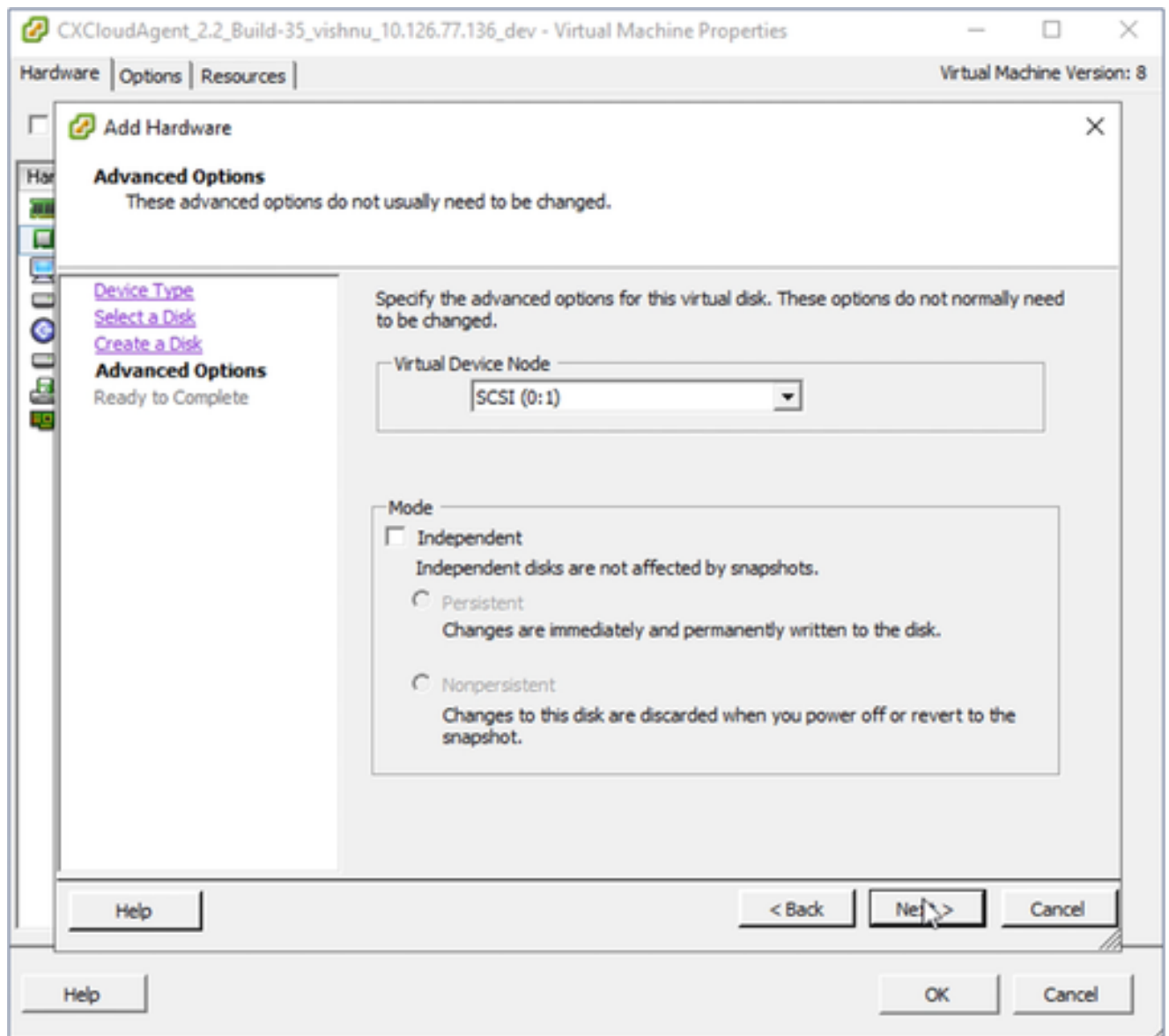
Seleccionar disco

8. Seleccione el botón de opción Create a new virtual disk y haga clic en Next.



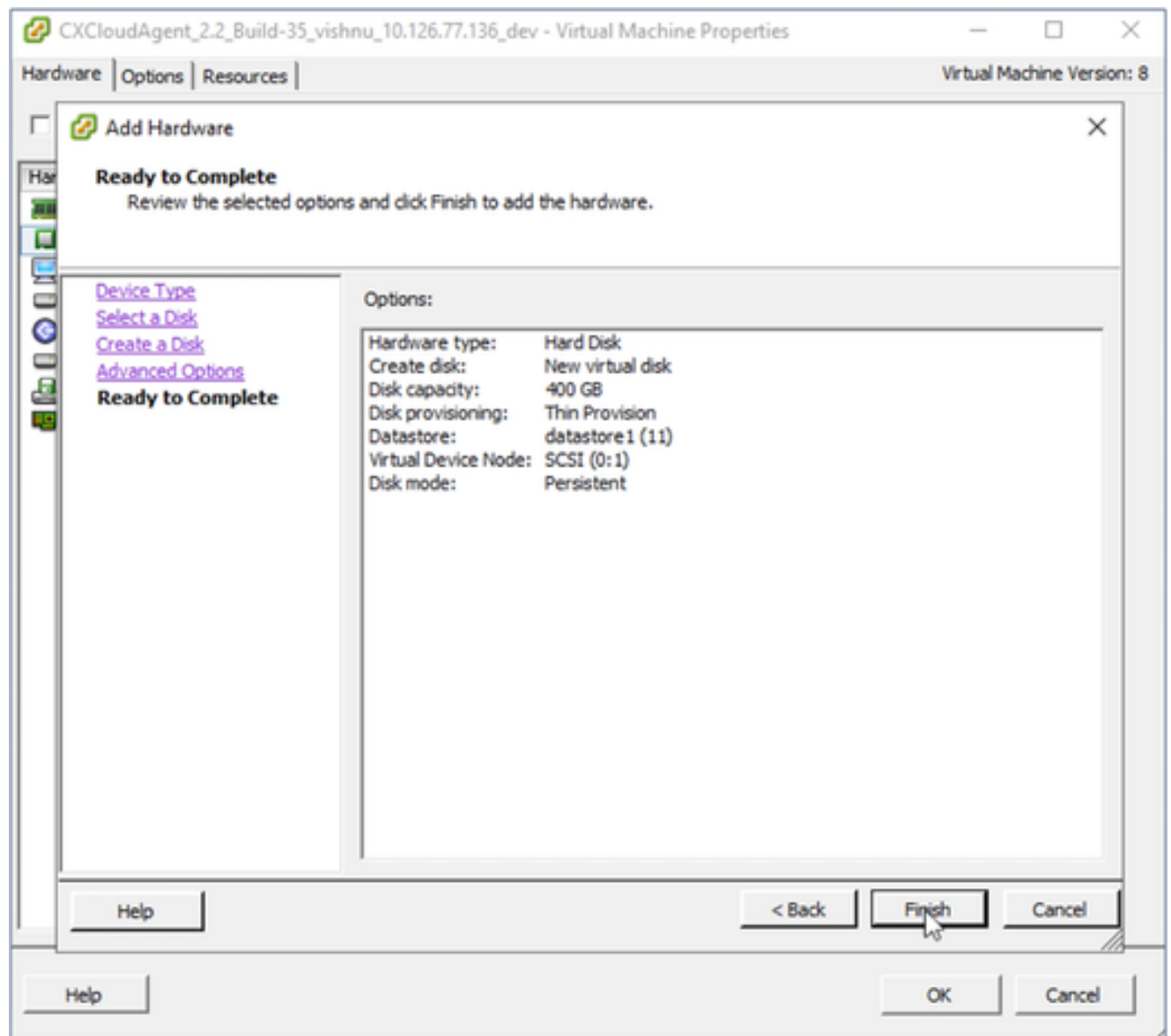
Crear disco

9. Actualice Capacity > Disk Size según lo especificado:  
Pequeñas y medianas empresas: 400 GB (tamaño inicial de 200 GB, aumento del espacio total a 600 GB)  
Pequeño a grande: 1000 GB (tamaño inicial: 200 GB, aumento del espacio total a 1200 GB)
10. Seleccione el botón de opción Thin Provisioning para Disk Provisioning.
11. Haga clic en Next (Siguiente). Se muestra la ventana Opciones avanzadas.



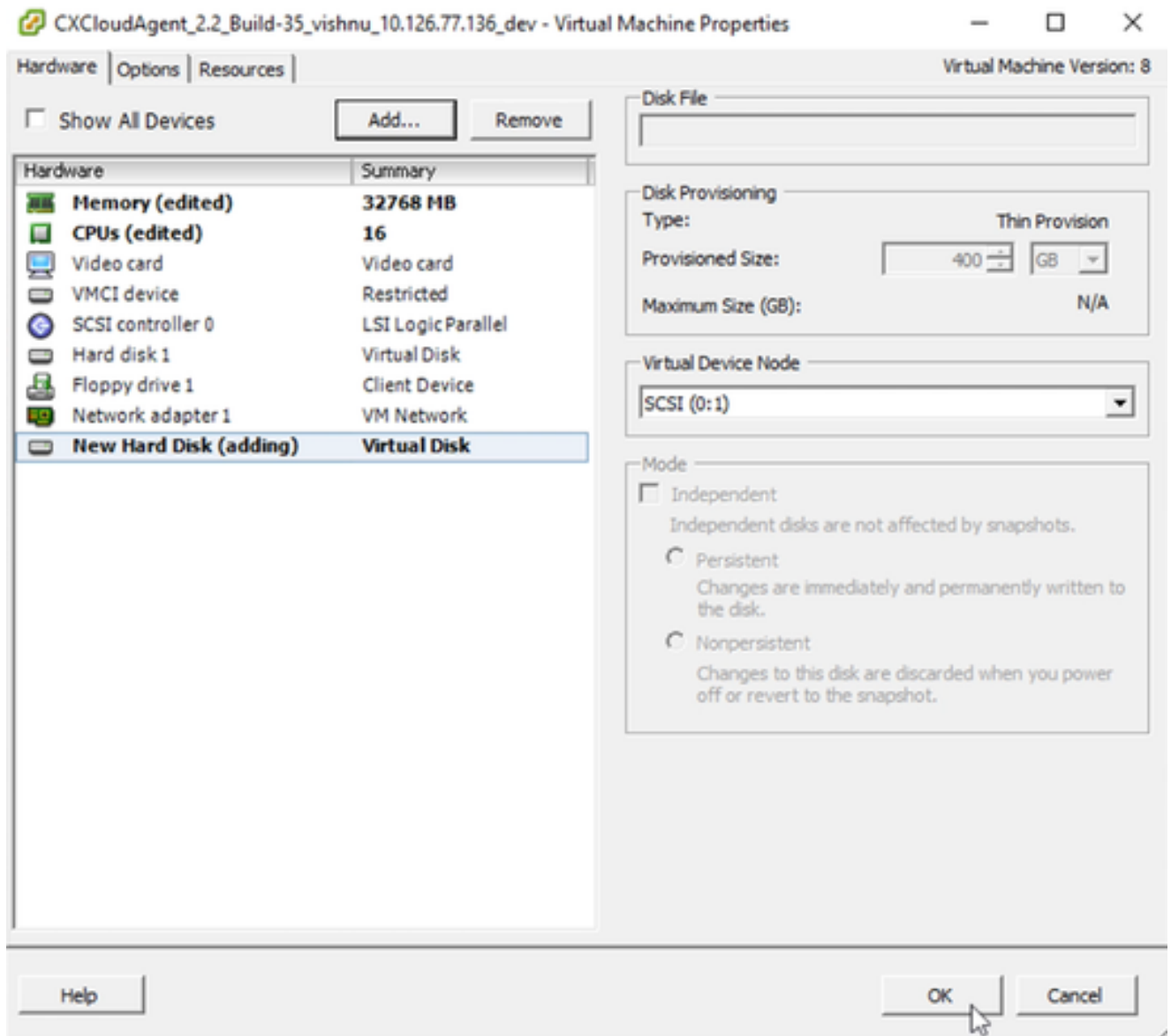
Opciones avanzadas

12. No realice cambios. Para continuar, haga clic en Next (Siguiente).



Listo para completar

13. Haga clic en Finish (Finalizar).



Hardware

14. Haga clic en Aceptar para completar la reconfiguración. La reconfiguración finalizada se muestra en el panel Tareas recientes.

10.126.77.60 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Inventory Inventory

10.126.77.60

- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.3\_Build-7\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.3\_Build-7\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.3\_Build-7\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.3\_Build-7\_vishnu\_10.126.77.136\_dev
- CxCloudAgent\_2.3\_Build-7\_vishnu\_10.126.77.136\_dev
- NAT-Router2.4.4\_vishnu\_10.126.77.136\_dev
- NAT-Router2.4.4\_vishnu\_10.126.77.136\_dev
- windows-1-test-192.168.77

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

Getting Started Summary Resource Allocation Performance Events Console Permissions

close tab

### What is a Virtual Machine?

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

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

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



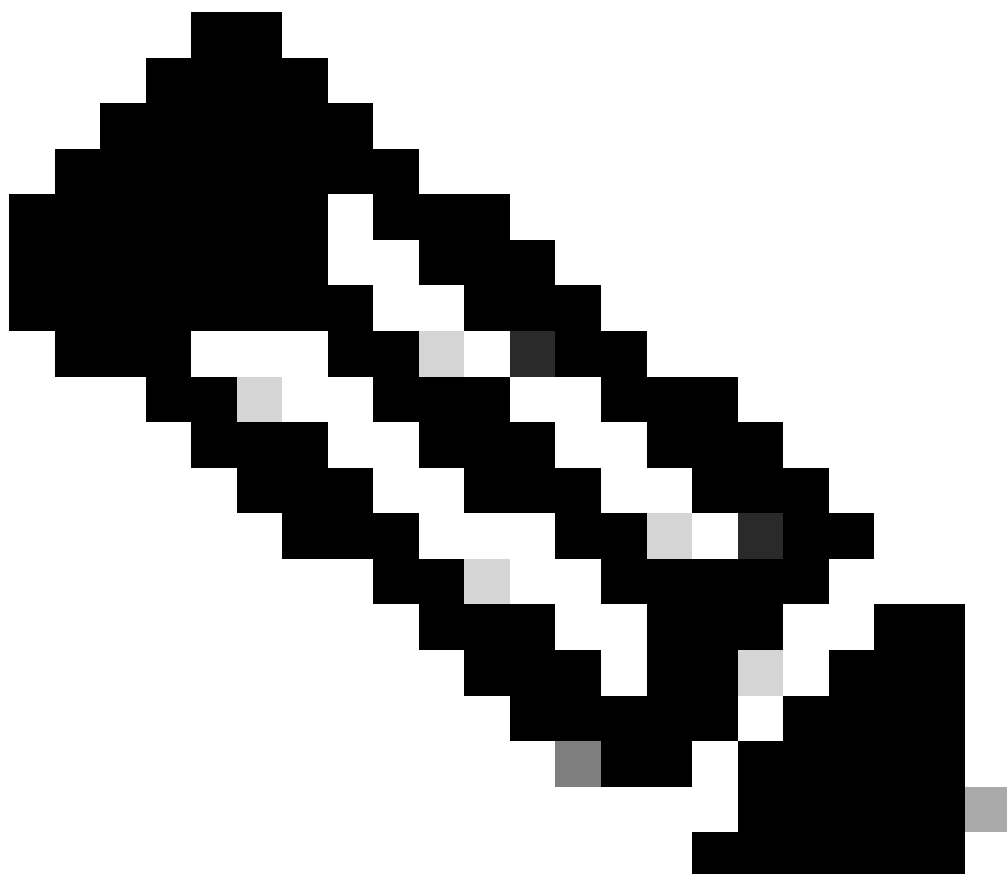
Recent Tasks

Name, Target or Status contains: Clear

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

Tasks root

Tareas recientes



Nota: Los cambios de configuración tardan aproximadamente cinco minutos en completarse.

---

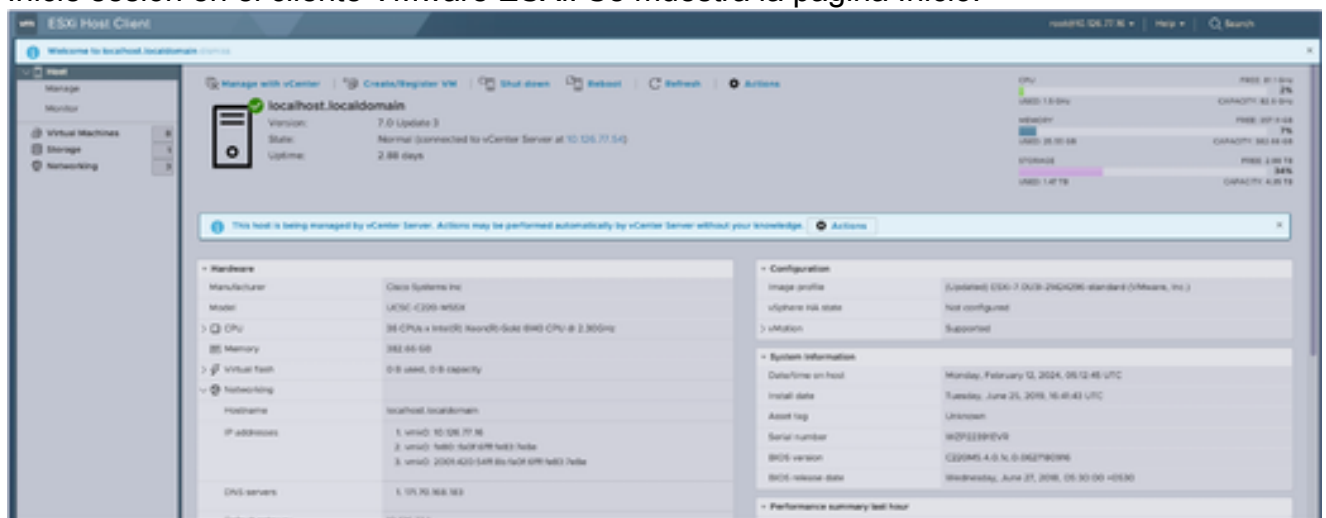
## Reconfiguración mediante el cliente web ESXi v6.0

Para actualizar las configuraciones de VM mediante Web Client ESXi v6.0:



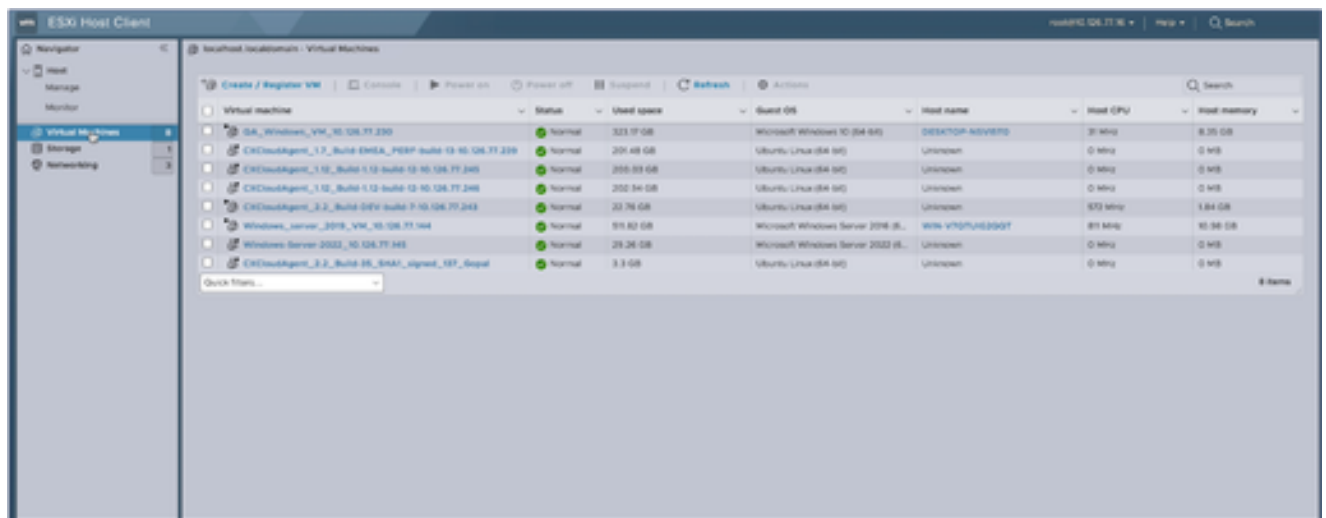
Cliente ESXi

1. Inicie sesión en el cliente VMware ESXi. Se muestra la página Inicio.



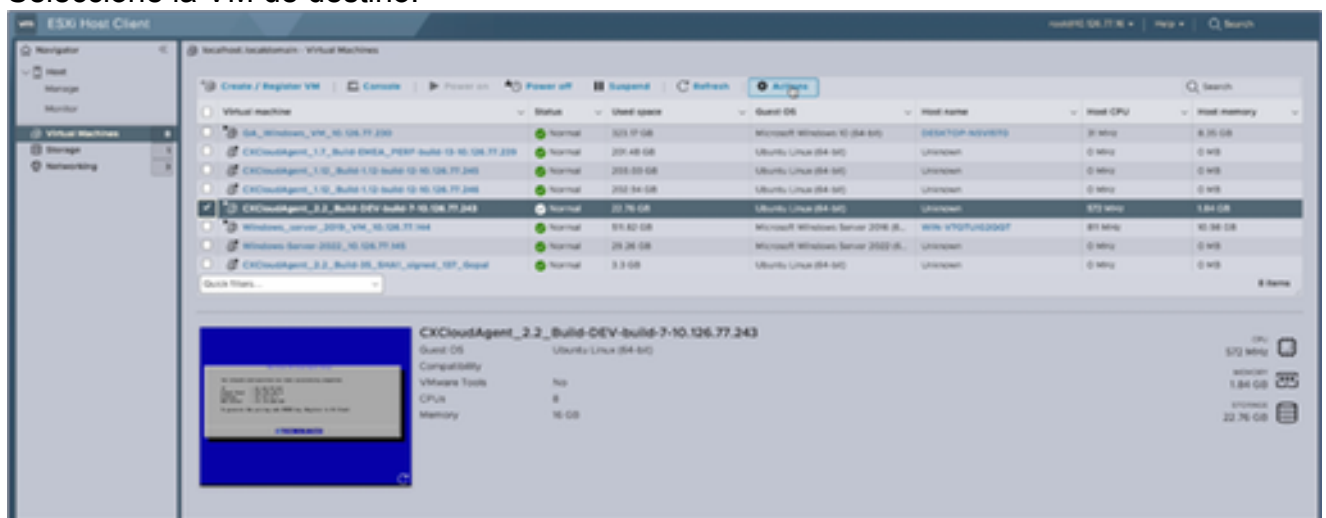
Página de inicio de ESXi

2. Haga clic en Máquina virtual para mostrar una lista de VM.



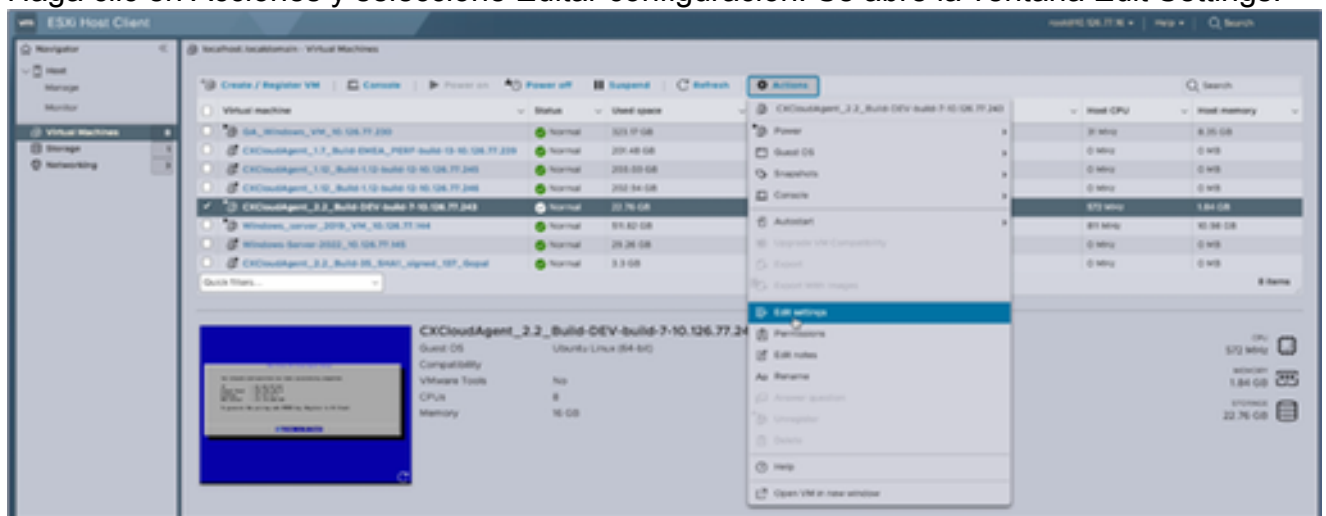
Lista de VM

### 3. Seleccione la VM de destino.

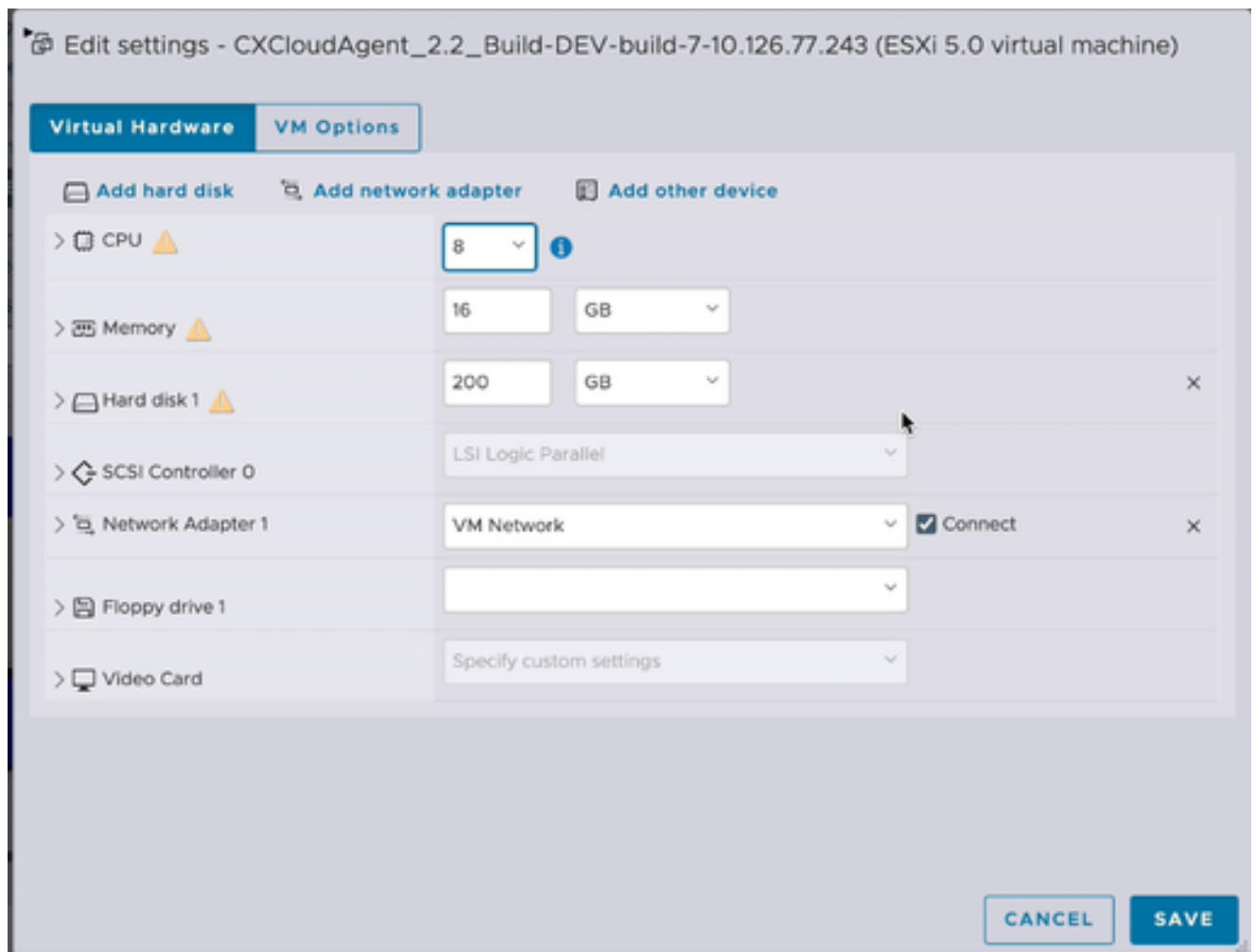


VM objetivo

### 4. Haga clic en Acciones y seleccione Editar configuración. Se abre la ventana Edit Settings.

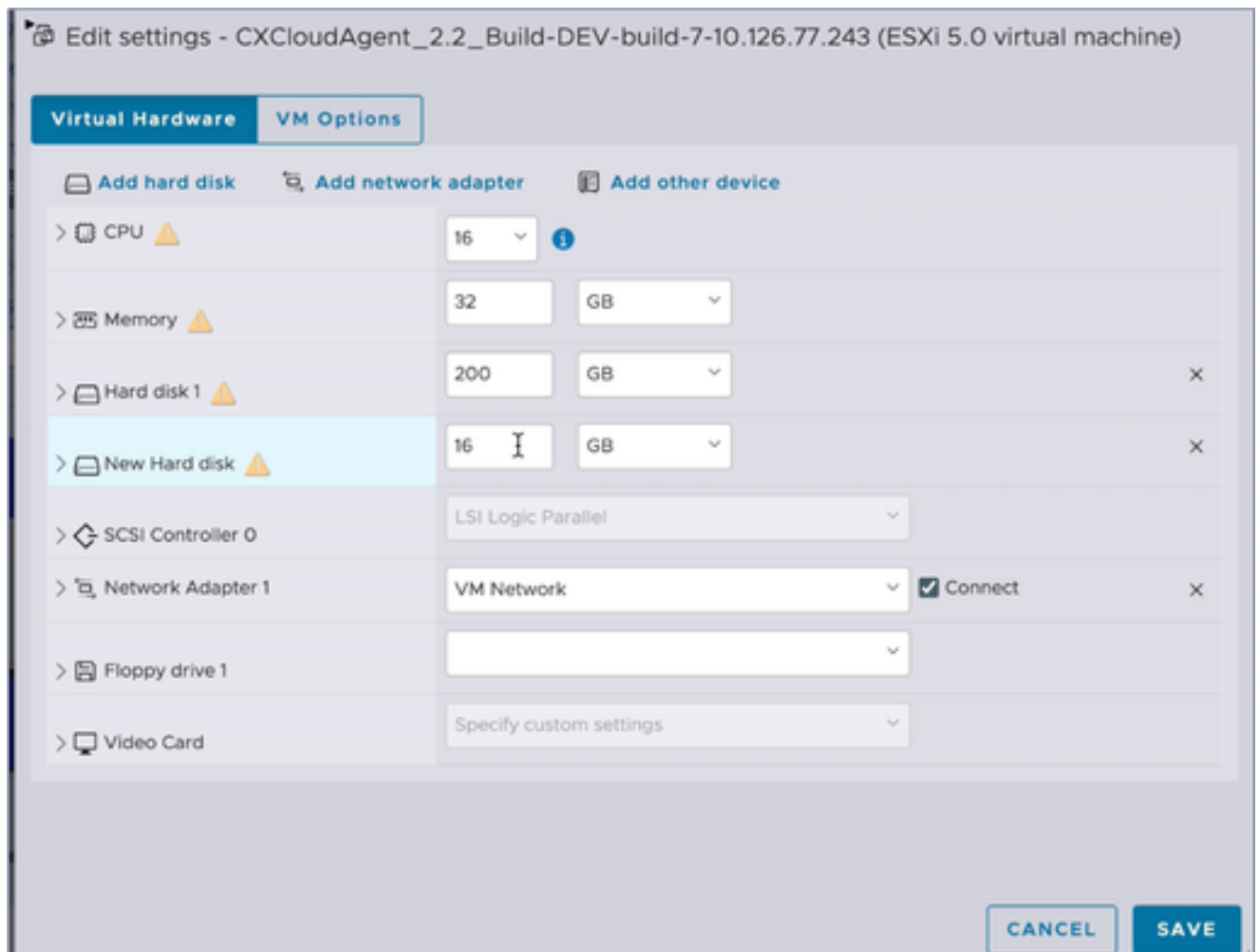


Acciones



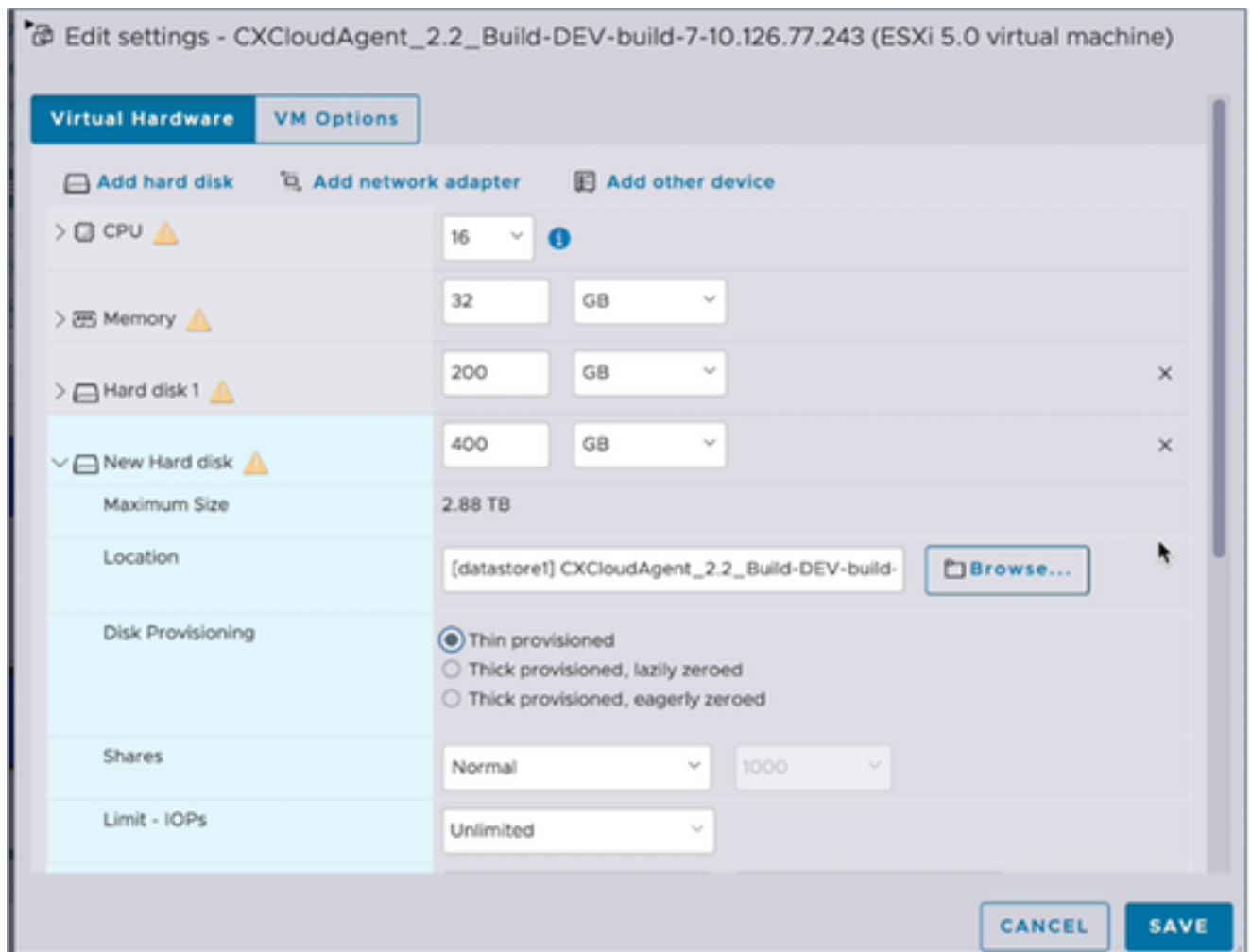
Editar configuración

5. Actualice el valor de CPU según lo especificado:  
Medio: 16 núcleos (8 sockets, \*2 núcleos/socket)  
Grande: 32 núcleos (16 zócalos \*2 núcleos/zócalo)
6. Actualice el valor Memory según lo especificado:  
Medio: 32 GB  
Grande: 64 GB
7. Haga clic en Agregar disco duro > Nuevo disco duro estándar. La nueva entrada del disco duro se muestra en la ventana Editar configuración.



Editar configuración

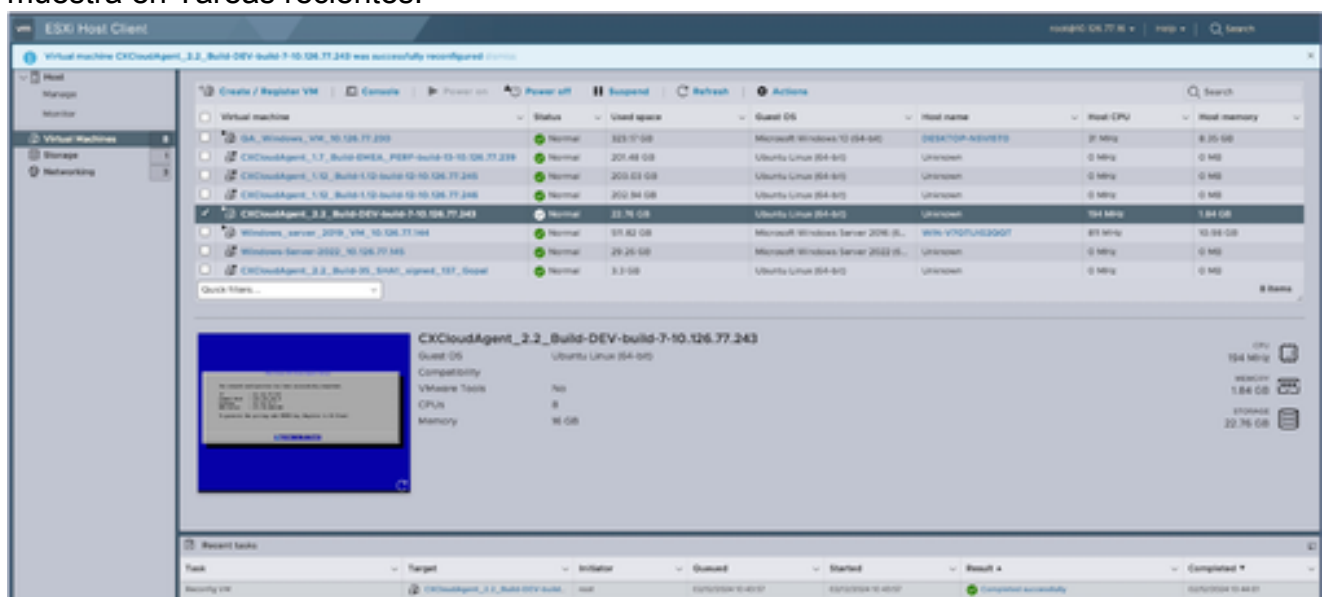
8. Actualice los valores del nuevo disco duro según lo especificado:  
Pequeñas y medianas empresas: 400 GB (tamaño inicial de 200 GB, aumento del espacio total a 600 GB)  
Pequeño a grande: 1000 GB (tamaño inicial: 200 GB, aumento del espacio total a 1200 GB)
9. Haga clic en la flecha para expandir Nuevo disco duro. Se muestran las propiedades.



Editar configuración

10. Seleccione el botón de opción Thin provisioned.

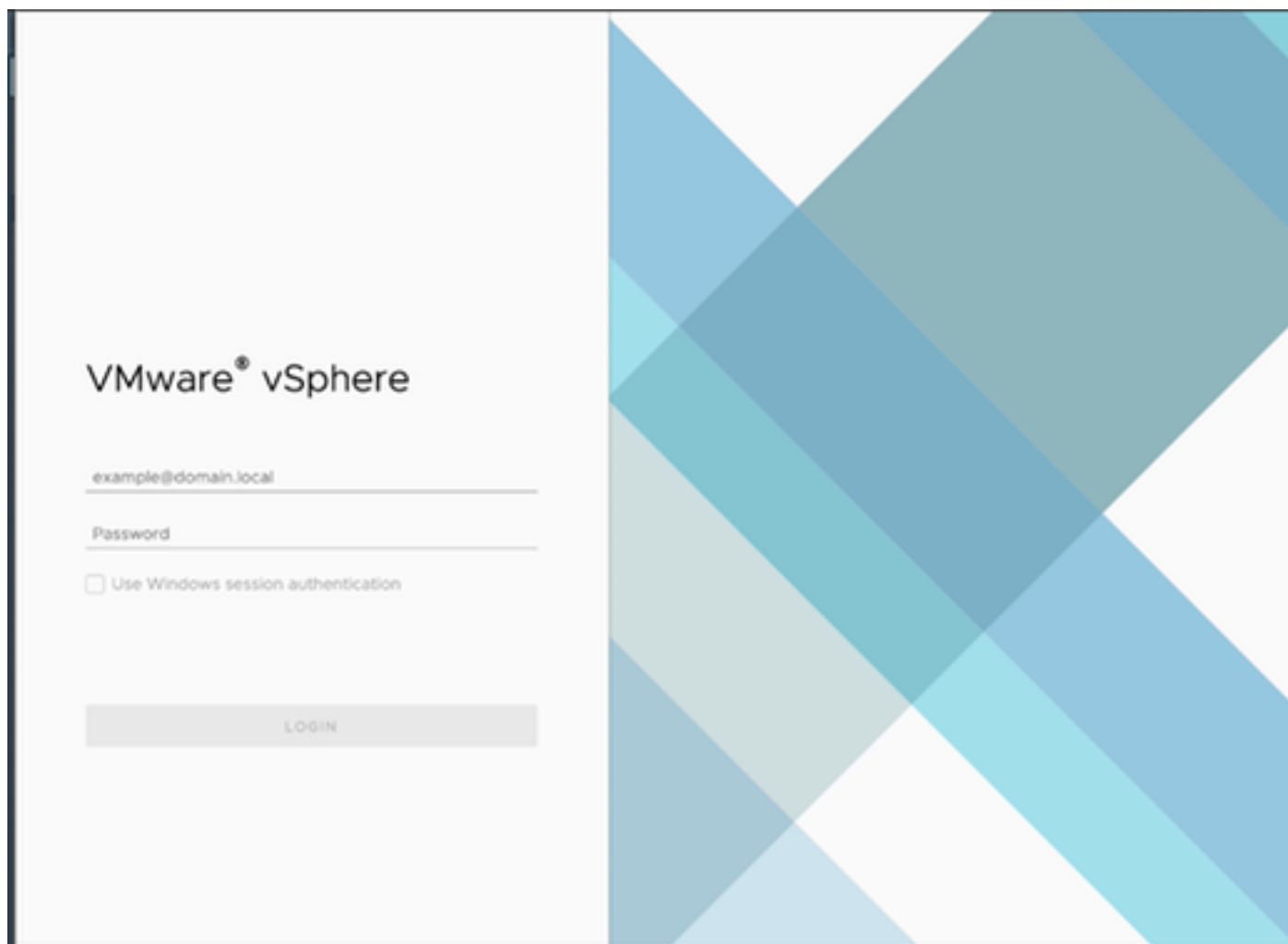
11. Haga clic en Save para completar la configuración. La actualización de la configuración se muestra en Tareas recientes.



Tareas recientes

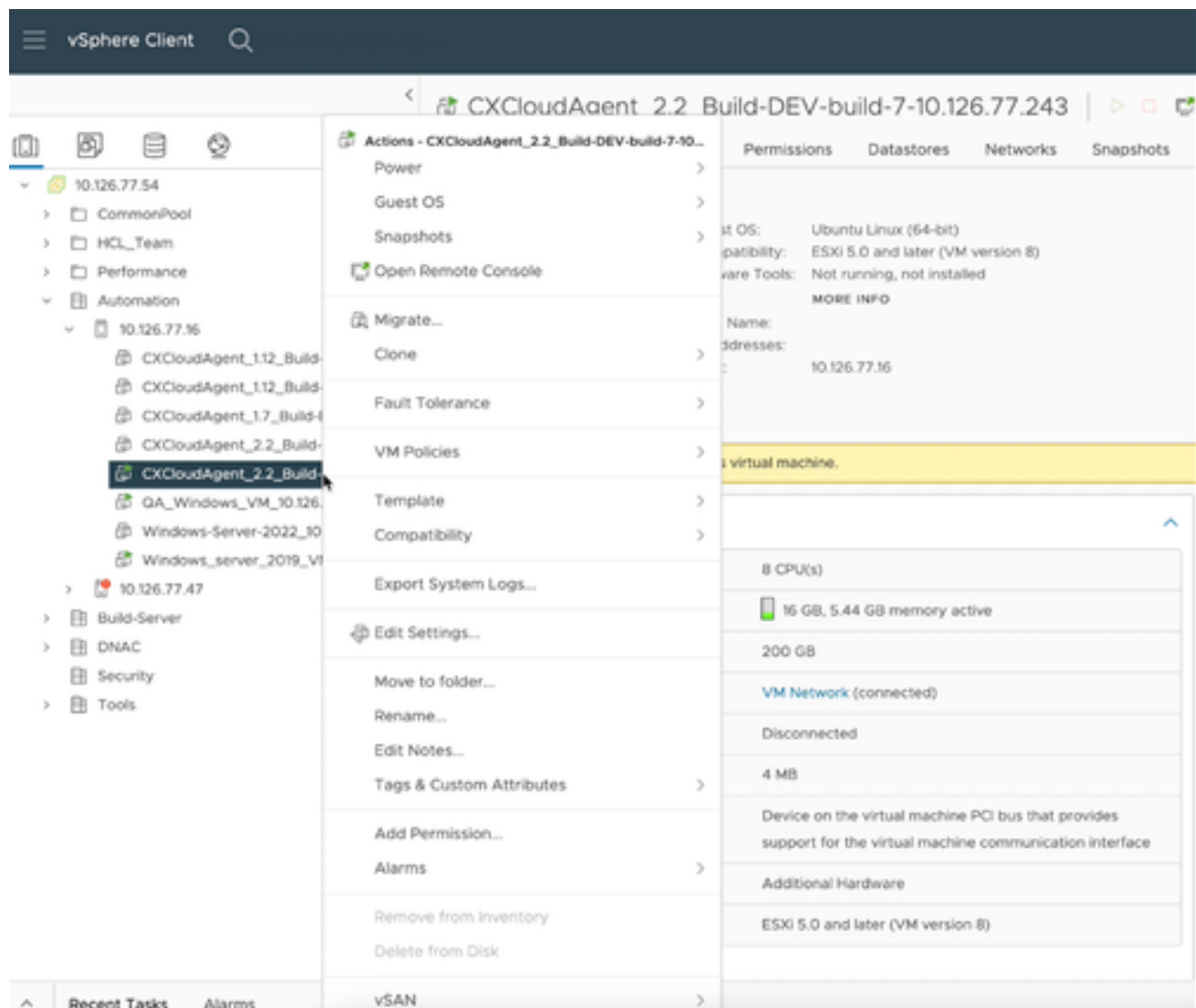
## Reconfiguración mediante Web Client vCenter

Para actualizar las configuraciones de VM mediante Web Client vCenter:



vCenter

1. Inicie sesión en vCenter. Se muestra la página Inicio.



Lista de VM

2. Haga clic con el botón derecho del ratón en la VM de destino y seleccione Editar configuración en el menú. Se abre la ventana Edit Settings.

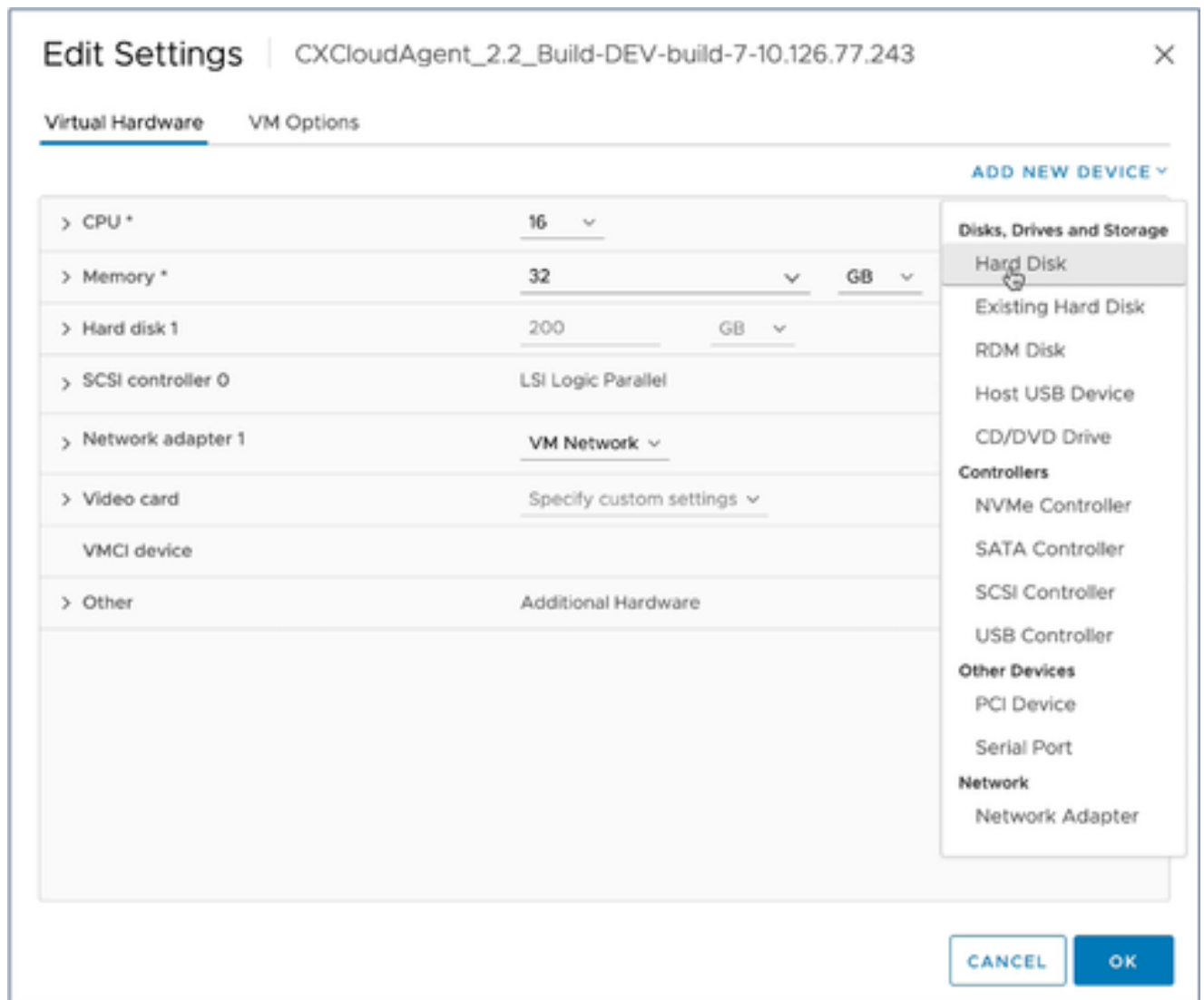
|                                                                                                 |                           |                                                                                               |
|-------------------------------------------------------------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------|
| > CPU                                                                                           | 8 ▾                       |            |
| > Memory                                                                                        | 16 ▾                      | GB ▾                                                                                          |
| > Hard disk 1  | 200                       | GB ▾                                                                                          |
| > SCSI controller 0                                                                             | LSI Logic Parallel        |                                                                                               |
| > Network adapter 1                                                                             | VM Network ▾              |  Connected |
| > Video card                                                                                    | Specify custom settings ▾ |                                                                                               |
| VMCI device                                                                                     |                           |                                                                                               |
| > Other                                                                                         | Additional Hardware       |                                                                                               |

CANCEL

OK

Editar configuración

3. Actualice los valores de CPU según lo especificado:  
Medio: 16 núcleos (8 sockets, \*2 núcleos/socket)  
Grande: 32 núcleos (16 zócalos \*2 núcleos/zócalo)
4. Actualice los valores de Memoria según lo especificado:  
Medio: 32 GB  
Grande: 64 GB



Editar configuración

5. Haga clic en Add New Device y seleccione Hard Disk. Se agrega la entrada New Hard disk.

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

Virtual Hardware
VM Options

ADD NEW DEVICE

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

CANCEL
OK

Editar configuración

6. Actualizar la memoria del nuevo disco duro según lo especificado:

Pequeñas y medianas empresas: 400 GB (tamaño inicial de 200 GB, aumento del espacio total a 600 GB)

Pequeño a grande: 1000 GB (tamaño inicial: 200 GB, aumento del espacio total a 1200 GB)

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

Virtual Hardware
VM Options

ADD NEW DEVICE

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

CANCEL
OK

Editar configuración

7. Seleccione Aprovisionamiento ligero en la lista desplegable Aprovisionamiento de disco.
8. Haga clic en Aceptar para completar la actualización.

## Implementación y configuración de red

Seleccione cualquiera de estas opciones para implementar el agente CX:

- [VMware vSphere/vCenter Thick Client ESXi 5.5/6.0](#)
- [Instalación de VMware vSphere/vCenter Web Client ESXi 6.0](#) o [Web Client vCenter](#)
- [Caja Virtual de Oracle 7.0.12](#)
- [Instalación de Microsoft Hyper-V](#)

## Implementación de OVA

Instalación de Thick Client ESXi 5.5/6.0

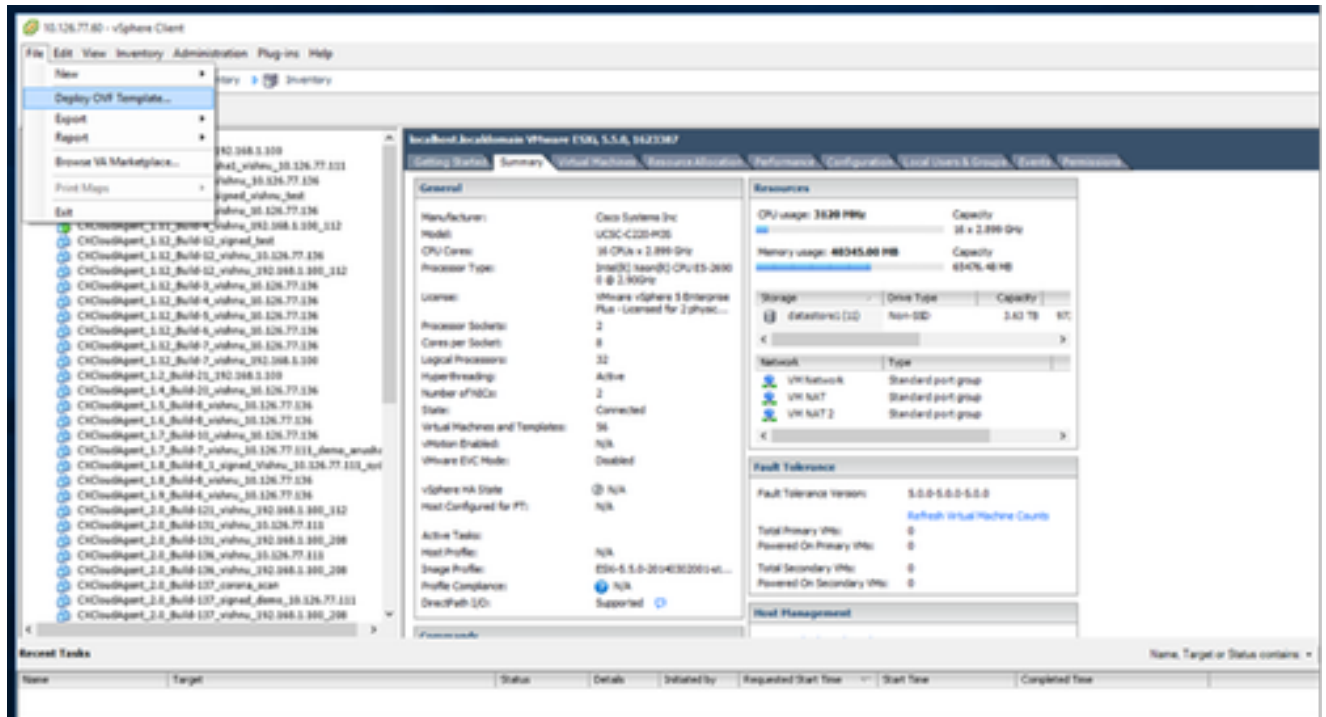
Este cliente permite la implementación de OVA del agente CX mediante el cliente de espesor vSphere.

1. Después de descargar la imagen, inicie el cliente VMware vSphere e inicie sesión.



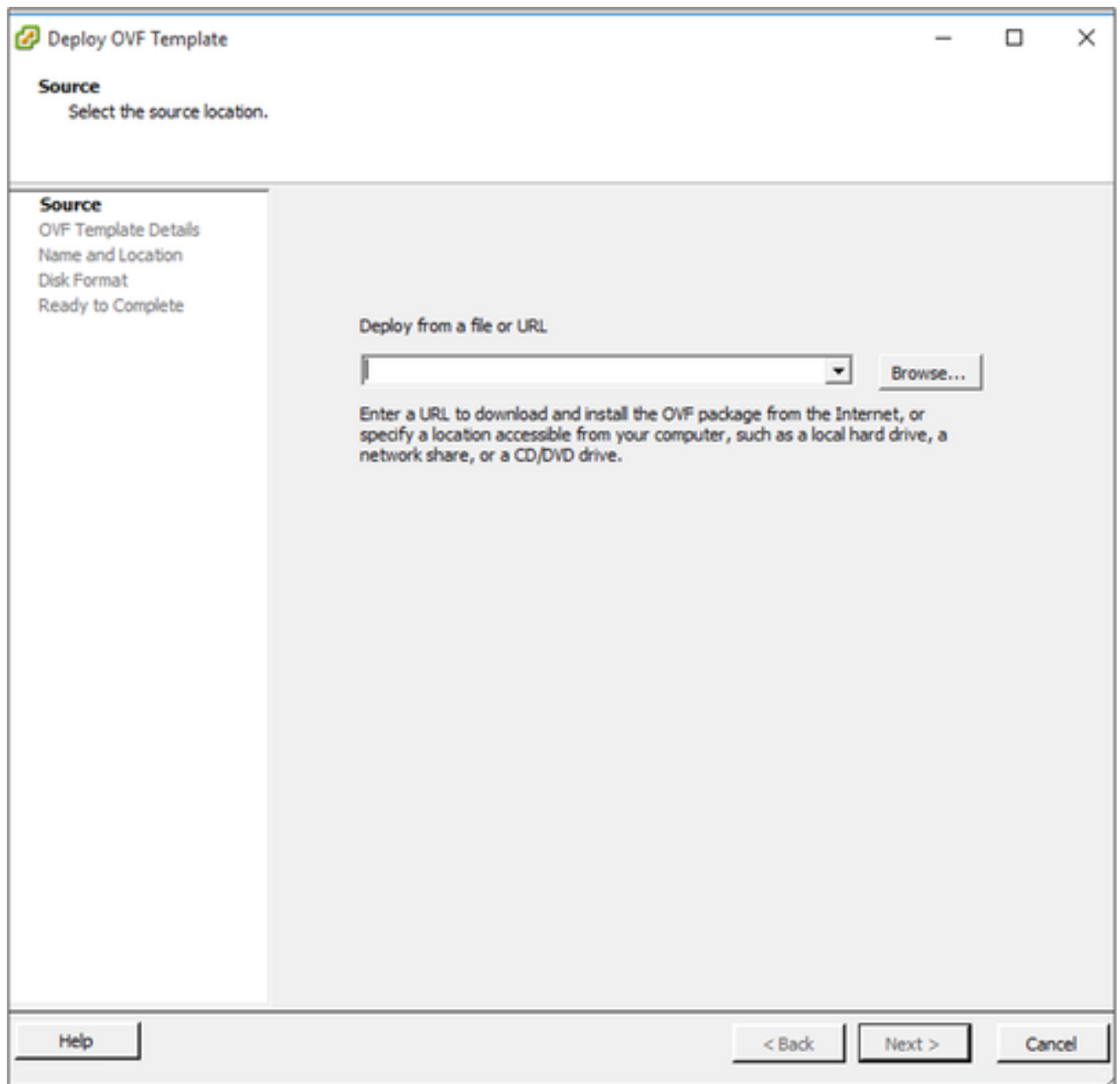
Inicio de sesión

2. En el menú, seleccione File > Deploy OVF Template.



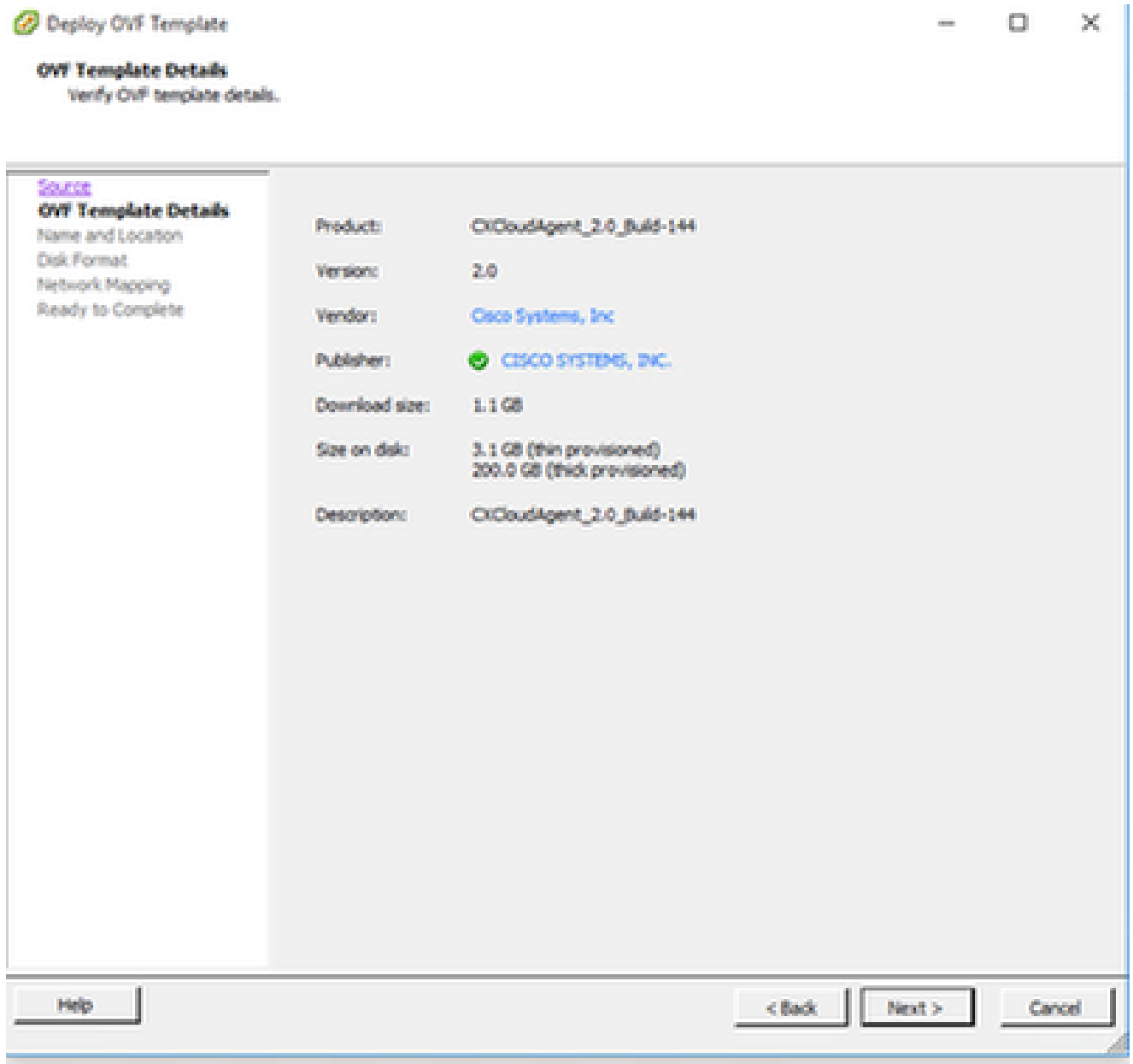
Cliente vSphere

3. Busque el archivo OVA y haga clic en Next.



Ruta OVA

4. Verifique los detalles de OVF y haga clic en Next.



Detalles de plantilla

5. Introduzca un nombre único y haga clic en Next.

 Deploy OVF Template — □ ×

**Name and Location**  
Specify a name and location for the deployed template

---

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

Name:

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

Help

< Back

Next >

Cancel

Nombre y ubicación

6. Seleccione un Formato de disco y haga clic en Siguiente (se recomienda una provisión ligera).

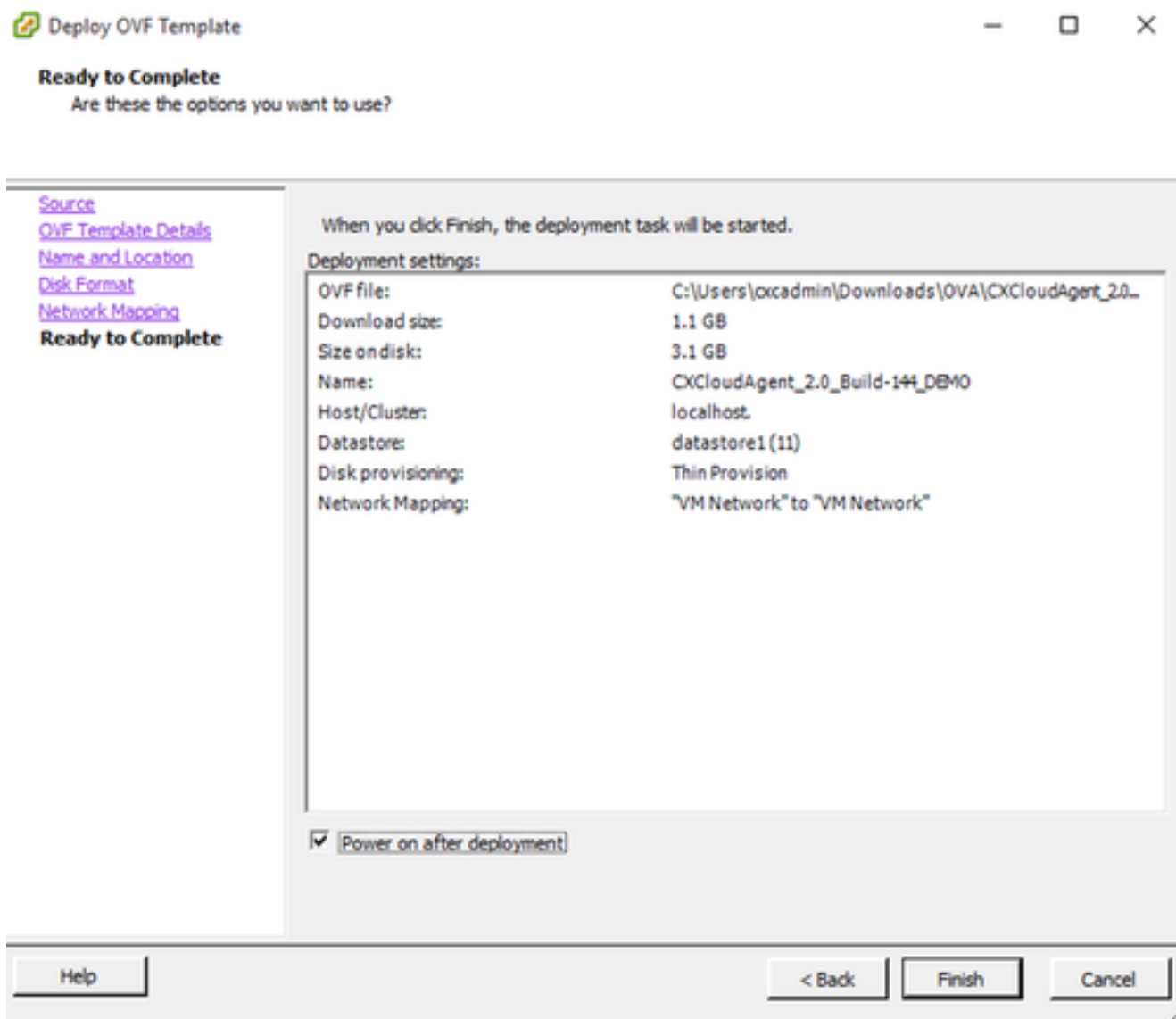
The screenshot shows a window titled "Deploy OVF Template" with standard Windows window controls (minimize, maximize, close) in the top right corner. The main heading is "Disk Format" with the instruction "In which format do you want to store the virtual disks?". On the left, a sidebar contains a list of steps: "Source", "OVF Template Details", "Name and Location", "Disk Format" (which is highlighted), "Network Mapping", and "Ready to Complete". The main area contains the following fields and options:

- Datastore:** A text box containing "datastore1 (11)".
- Available space (GB):** A text box containing "973.1".
- Provisioning Options:** Three radio buttons are listed:
  - ☐ Thick Provision Lazy Zeroed
  - ☐ Thick Provision Eager Zeroed
  - ☒ Thin Provision

At the bottom of the window, there are three buttons: "Help" on the left, "< Back" in the center, and "Next >" and "Cancel" on the right.

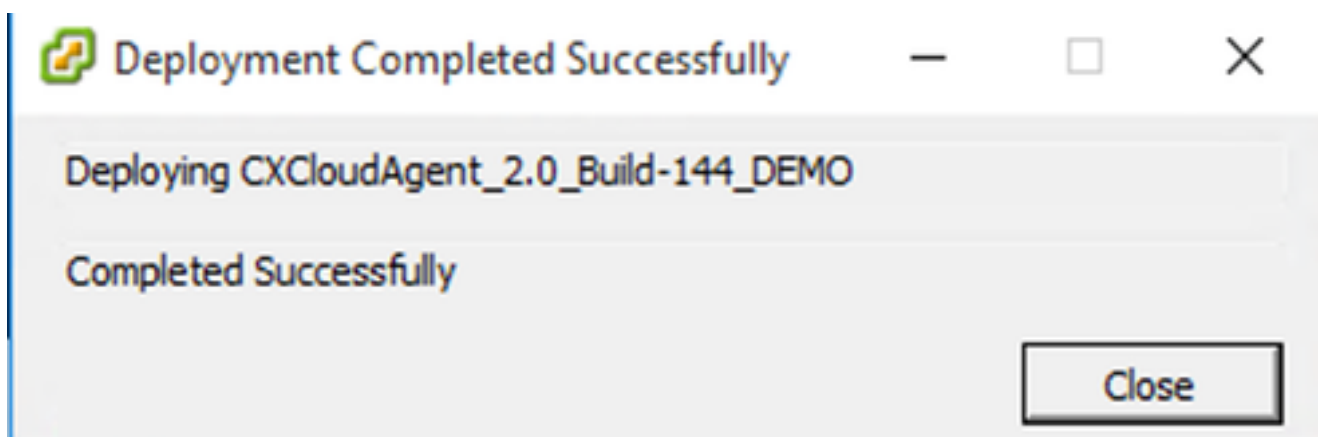
Formato de disco

7. Active la casilla de verificación Encender después de la implementación y haga clic en Cerrar.



Listo para completar

La implementación puede tardar varios minutos. La confirmación se muestra tras la correcta implementación.



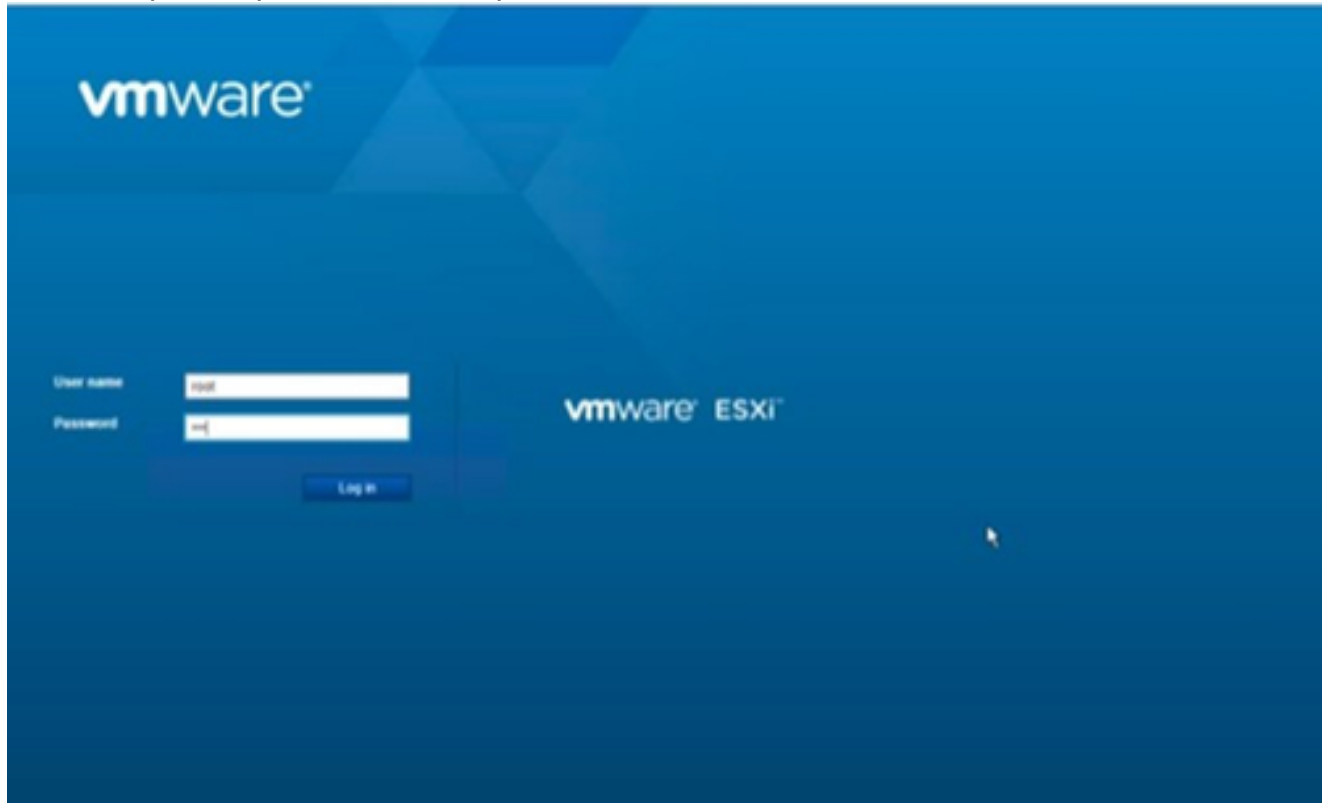
Implementación completa

8. Seleccione la VM implementada, abra la consola y vaya a [Configuración de red](#) para continuar con los siguientes pasos.

## Instalación del cliente web ESXi 6.0

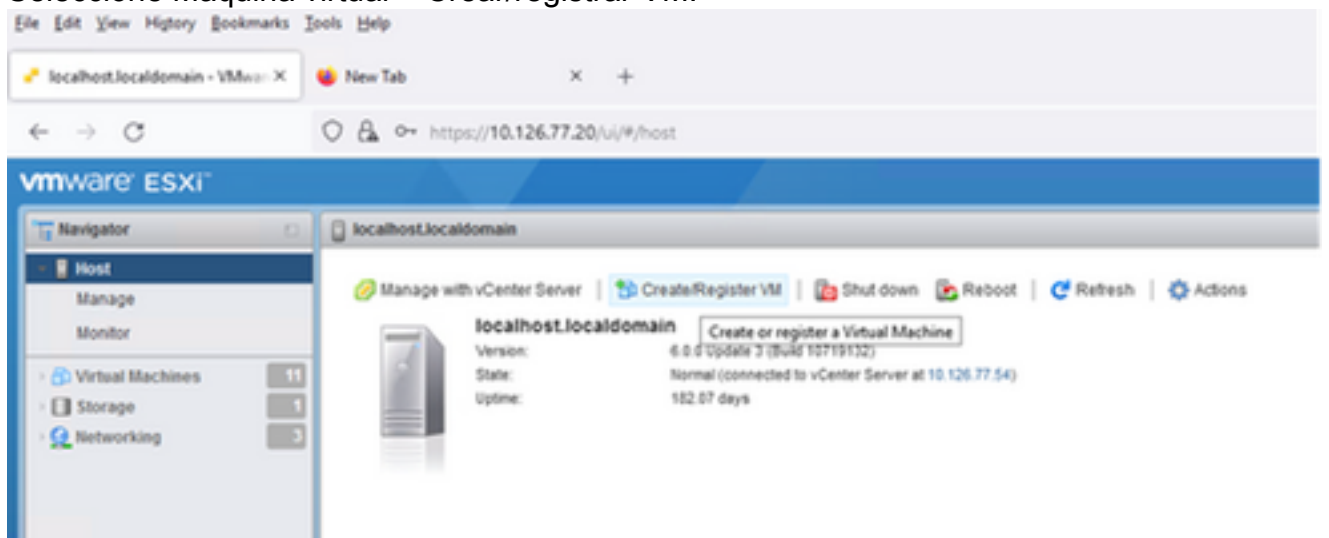
Este cliente implementa CX Cloud OVA mediante la Web de vSphere.

1. Inicie sesión en la interfaz de usuario de VMWare con las credenciales de ESXi/hipervisor utilizadas para implementar la máquina virtual.



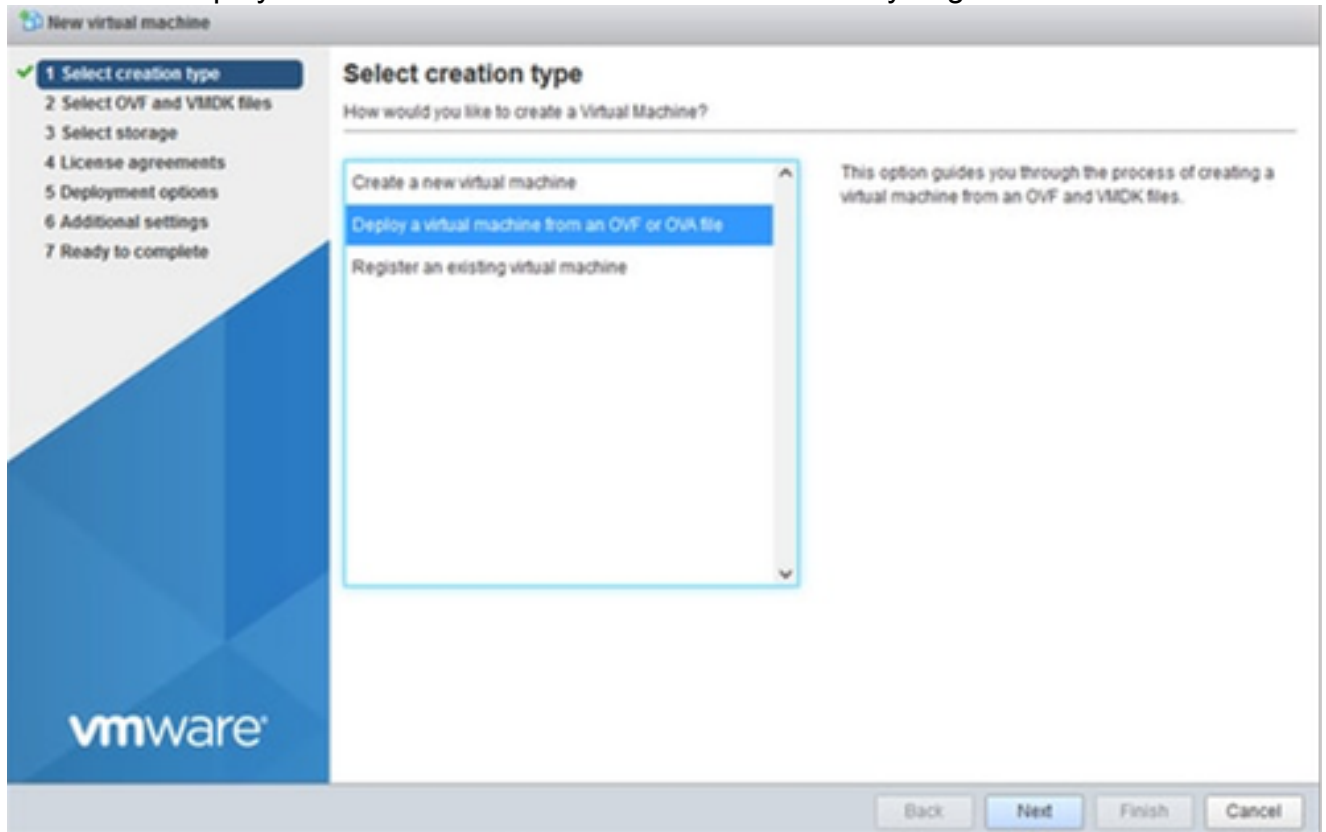
Conexión a VMWare ESXi

2. Seleccione Máquina virtual > Crear/registrar VM.



Crear VM

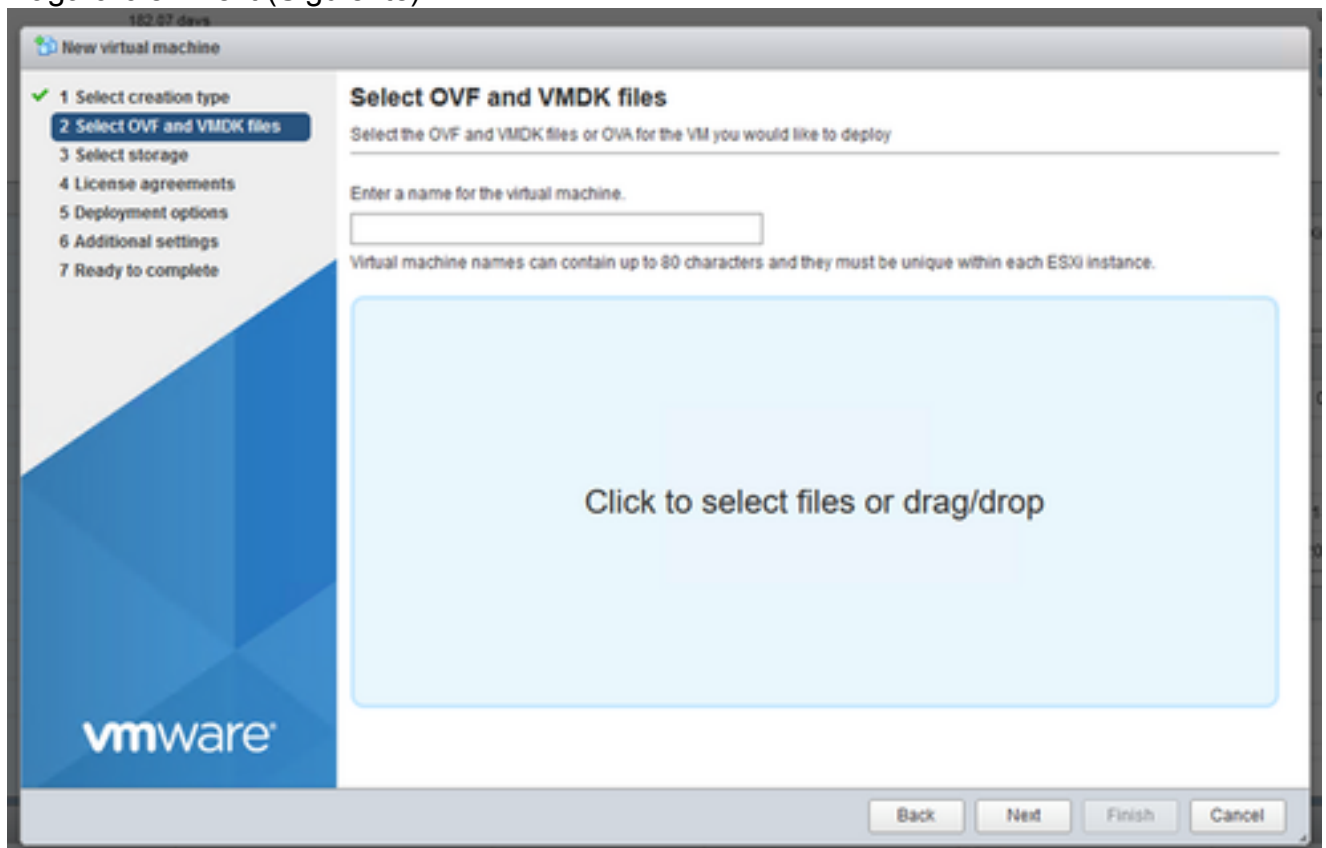
3. Seleccione Deploy a virtual machine from an OVF or OVA file y haga clic en Next.



Seleccionar tipo de creación

4. Introduzca el nombre de la máquina virtual, navegue para seleccionar el archivo o arrastre y suelte el archivo OVA descargado.

5. Haga clic en Next (Siguiente).



Selección de OVA

6. Seleccione Standard storage y haga clic en Next.

New virtual machine - CX Cloud Agrnt 2.0 DEMO

- 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

### Select storage

Select the storage type and datastore

☒ Standard ☐ Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

| Name       | Capacity | Free    | Type  | Thin pro... | Access |
|------------|----------|---------|-------|-------------|--------|
| datastore1 | 4.35 TB  | 3.57 TB | VMFS5 | Supported   | Single |

1 items

Back Next Finish Cancel

Seleccionar almacenamiento

7. Seleccione las opciones de implementación adecuadas y haga clic en Siguiente.

New virtual machine - CX Cloud Agrnt 2.0 DEMO

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

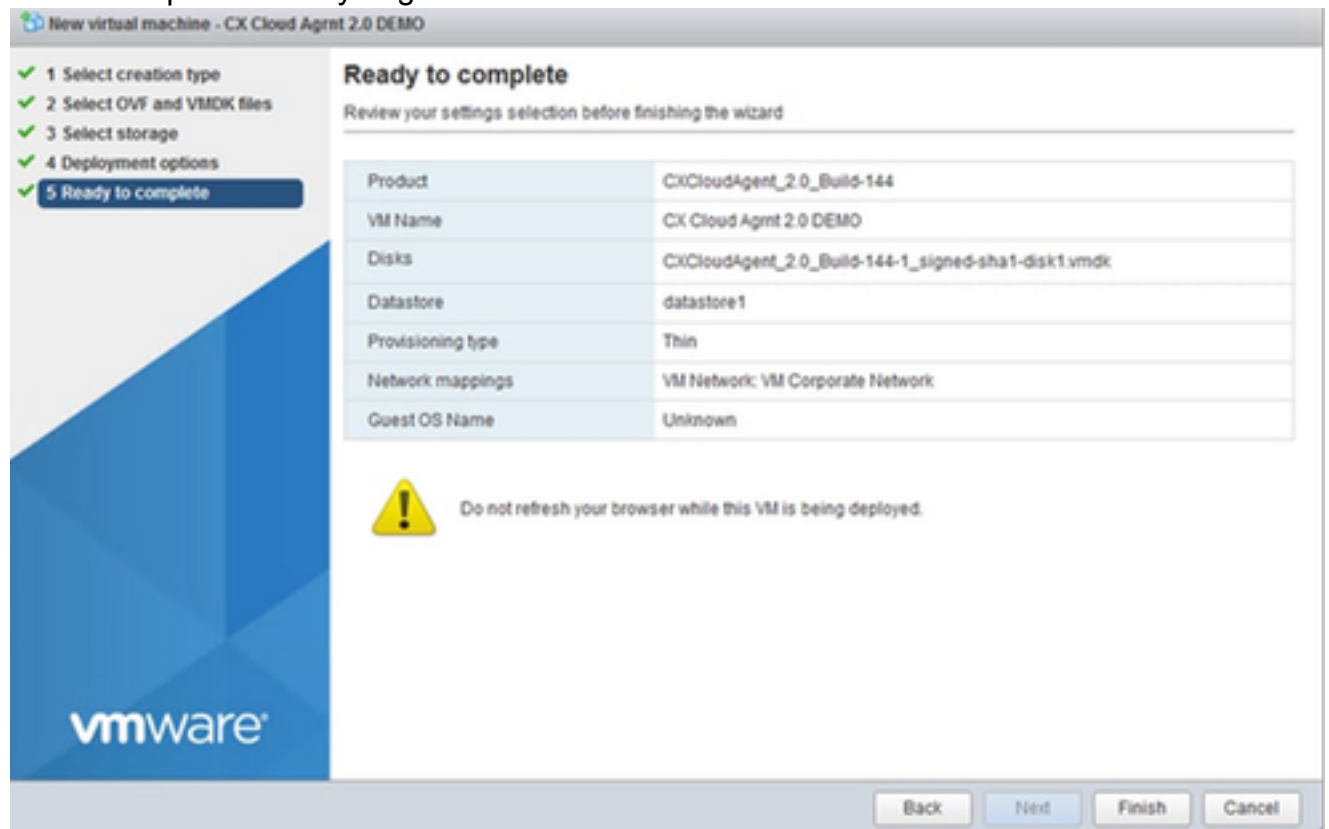
### Deployment options

Select deployment options

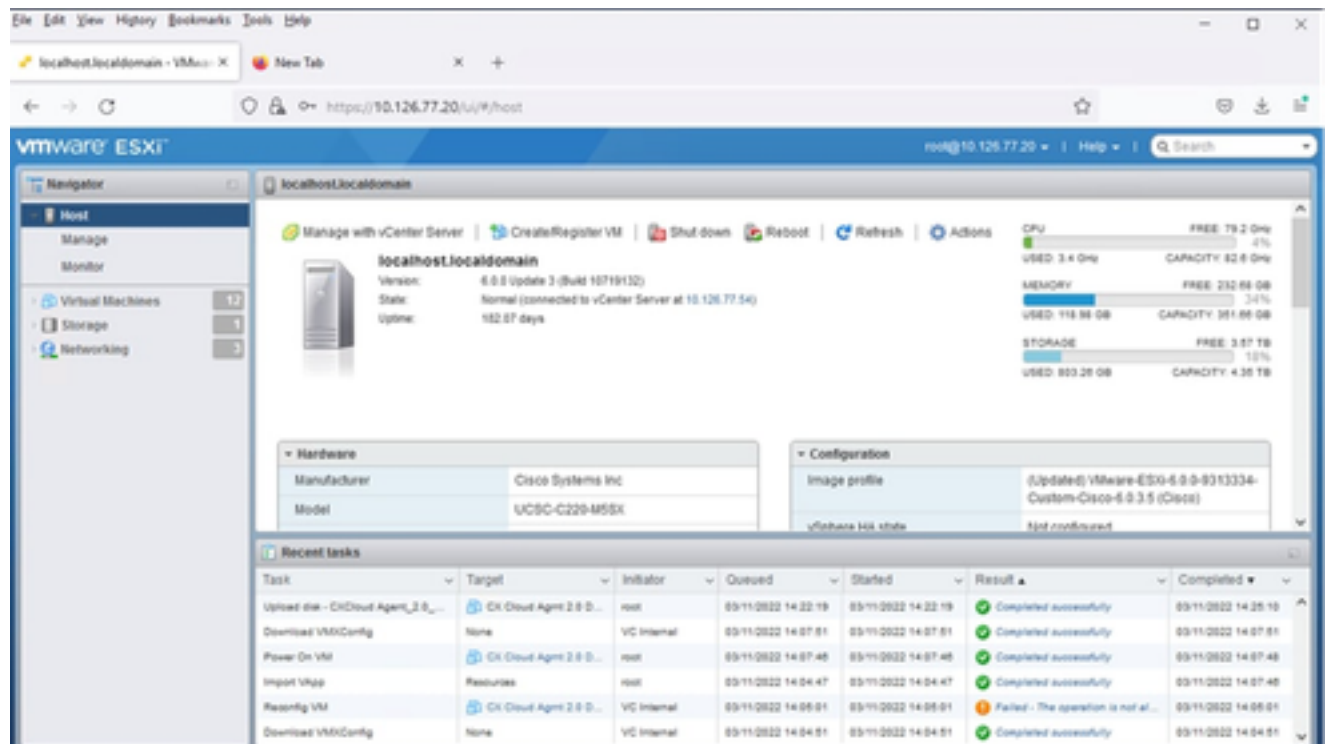
|                        |                                                                   |
|------------------------|-------------------------------------------------------------------|
| Network mappings       | VM Network: VM Corporate Network                                  |
| Disk provisioning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

Back Next Finish Cancel

## 8. Revise los parámetros y haga clic en Finish.

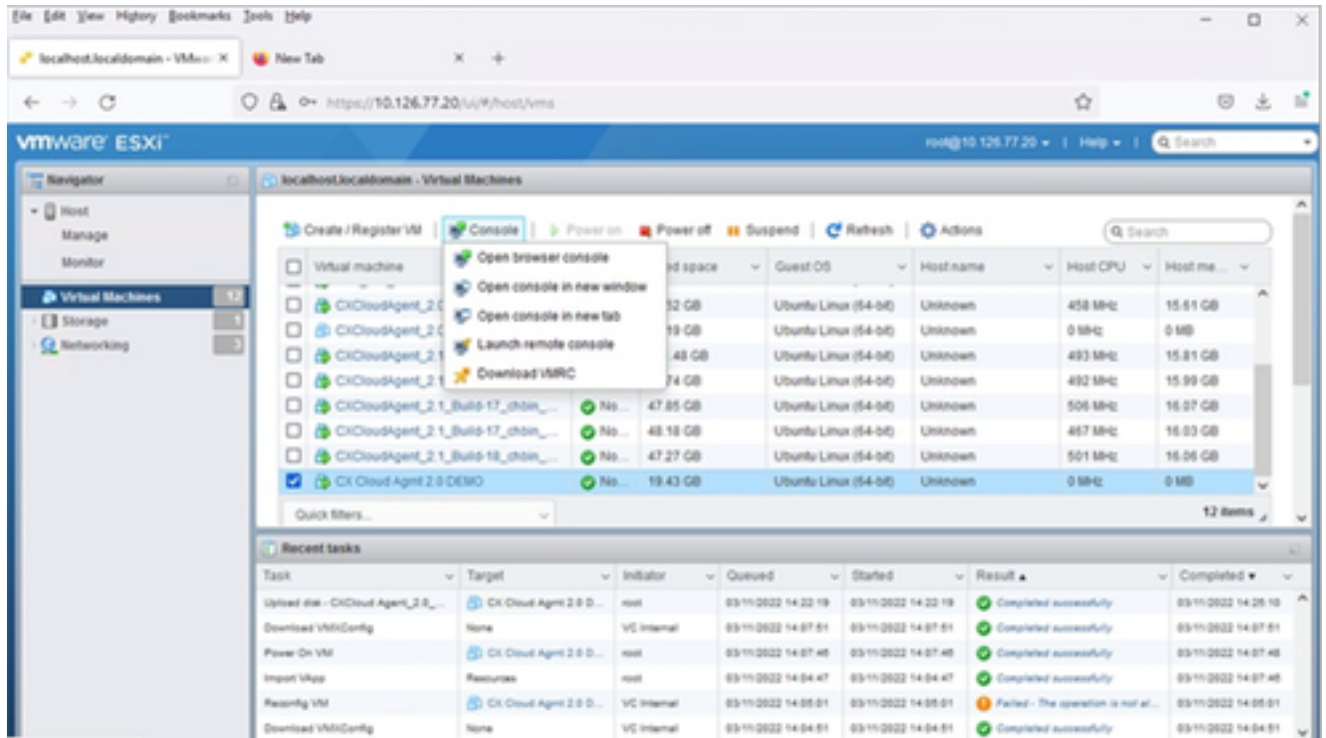


Listo para completar



Finalización correcta

9. Seleccione la máquina virtual que acaba de implementar y seleccione Console > Open browser console.



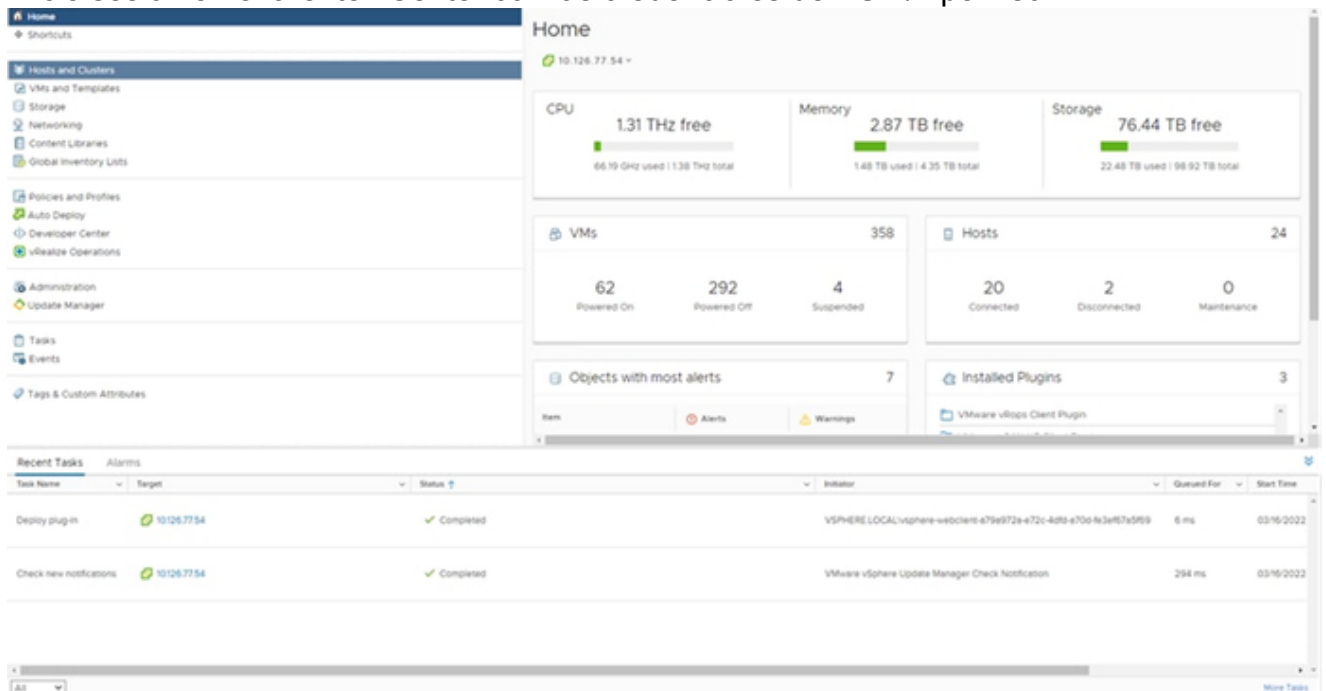
Consola

10. Vaya a [Network Configuration](#) para continuar con los siguientes pasos.

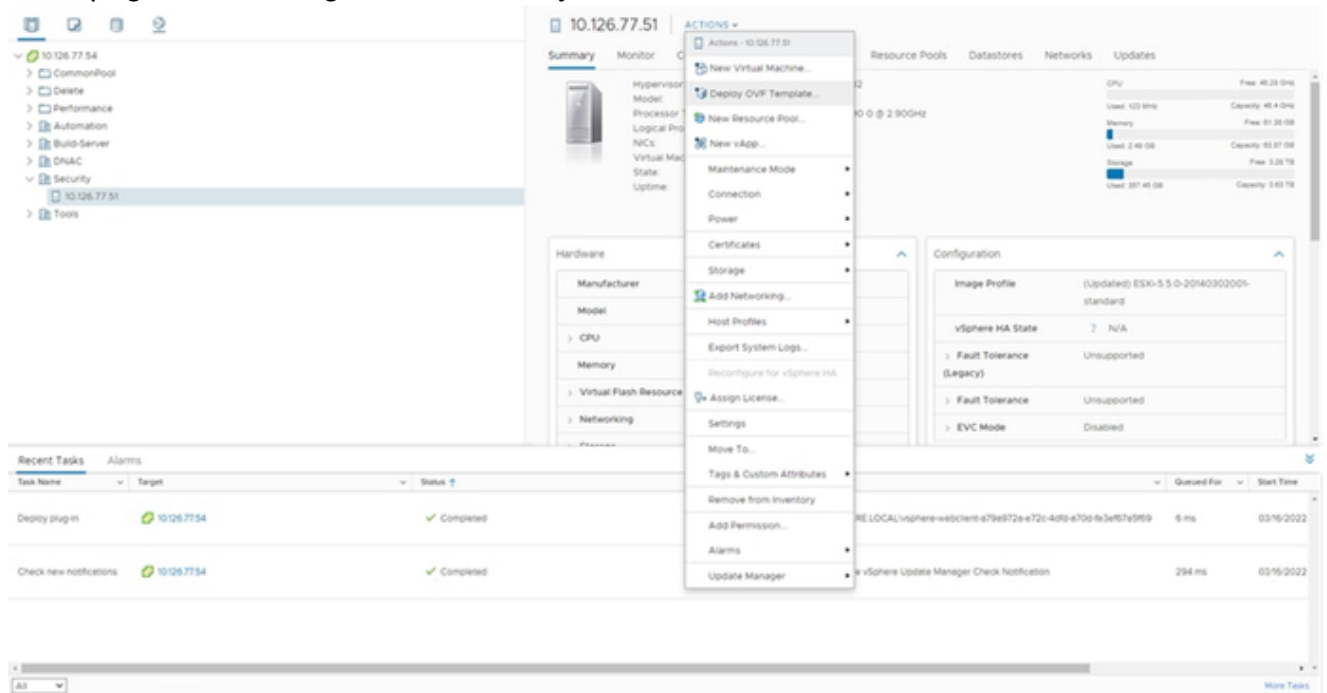
## Instalación de Web Client vCenter

Este cliente permite la implementación de OVA de agente CX mediante el uso de Web Client vCenter.

1. Inicie sesión en el cliente vCenter con las credenciales de ESXi/hipervisor.



2. En la página Inicio, haga clic en Hosts y clústeres.



3. Seleccione la VM y haga clic en Acción > Implementar plantilla de OVF.

## Deploy OVF Template

### 1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

### Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

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

☒ Local file

Choose Files

No file chosen



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



CANCEL

BACK

NEXT

Implementación de OVF

- 4. Agregue la URL directamente o busque y seleccione el archivo OVA.
- 5. Haga clic en Next (Siguiente).

### Deploy OVF Template

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

### Select a name and folder

Specify a unique name and target location

Virtual machine name: CXCloudAgent\_2.3\_Build-Demo

Select a location for the virtual machine.

10.126.77.54

- CommonPool
  - M3 - Simulator
  - M4
  - M5**
- HCL\_Team
- Performance
- Automation
- Build-Server
- DNAC
- Security
- Tools

CANCEL
BACK
NEXT

Nombre y carpeta

- Introduzca un nombre único y navegue hasta la ubicación, si fuera necesario.
- Haga clic en Next (Siguiente).

### Deploy OVF Template

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

### Select a compute resource

Select the destination compute resource for this operation

Build-Server

- Build-Server
- Build-Server**

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

Seleccionar recurso informático

- Seleccione un recurso informático y haga clic en Siguiente.

### Deploy OVF Template

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

### Review details

Verify the template details.

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

CANCEL
BACK
NEXT

Revisar detalles

9. Revise los detalles y haga clic en Next.

### Deploy OVF Template

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

### Configuration

Select a deployment configuration

☒ Small
 ☐ Medium
 ☐ Large

3 Items

**Description**

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

CANCEL
BACK
NEXT

Configuración

10. Seleccione la configuración de implementación y haga clic en Siguiente.

### Deploy OVF Template

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

### Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Thick Provision Lazy Zeroed Default

☐ Disable Storage DRS for this

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

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Configuración

11. Seleccione Storage > Select virtual disk format en la lista desplegable y haga clic en Next.

### Deploy OVF Template

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

### Select networks

Select a destination network for each source network.

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

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Seleccionar redes

12. Seleccione las opciones apropiadas en Select networks y haga clic en Next.

### Deploy OVF Template

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

### Ready to complete

Review your selections before finishing the wizard

✓ Select a name and folder

Name: CXCloudAgent\_2.3\_Build-Demo  
Template name: CXCloudAgent\_2.3\_Build-69-1\_SHA1  
Folder: Build-Server

✓ Select a compute resource

Resource: 10.126.77.52

✓ Review details

Download size: 1.4 GB

✓ Select storage

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

✓ Select networks

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

CANCEL

BACK

FINISH

Listo para completar

13. Revise las selecciones y haga clic en Finalizar. Se muestra la página Inicio.

vSphere Client

10.126.77.54

CommonHost

HCL\_Team

Performance

Automation

Build-Server

10.126.77.69

10.126.77.52

**CXCloudAgent\_2.3\_Build-Demo**

DNAC

Security

Tools

CXCloudAgent\_2.3\_Build-Demo

Powered Off

Guest OS: Ubuntu Linux (54-bit)

Compatibility: ESXi 5.0 and later (VM version 8)

VMware Tools: Not running, not installed

DNS Name: MORE INFO

IP Addresses: 10.126.77.52

LAUNCH WEB CONSOLE

LAUNCH REMOTE CONSOLE

VM Hardware

CPU: 8 CPU(s)

Memory: 16 GB, 0 GB memory active

Notes

CXCloudAgent\_2.3\_Build-69

EDIT NOTES

Summary

Monitor

Configure

Permissions

Datastores

Networks

Snapshots

Updates

SWITCH TO NEW VIEW

CPU USAGE: 0 Hz

MEMORY USAGE: 0 B

STORAGE USAGE: 1.45 KB

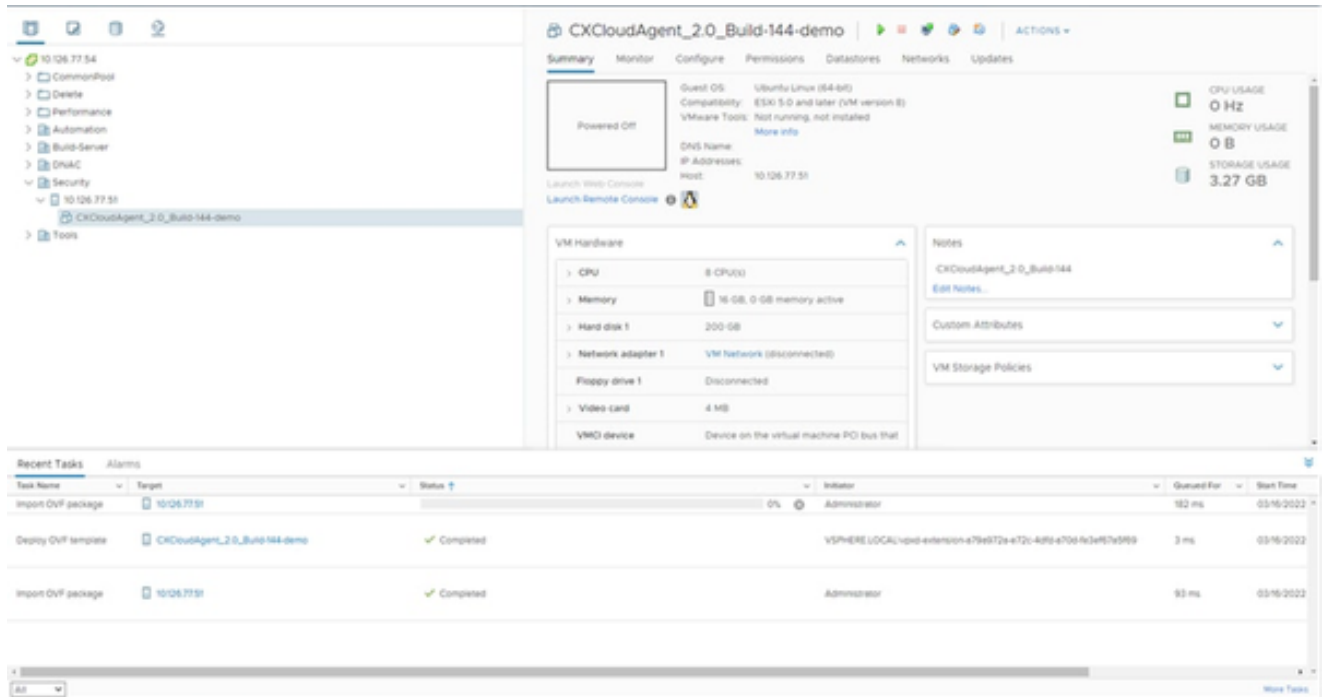
Recent Tasks

Alarms

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

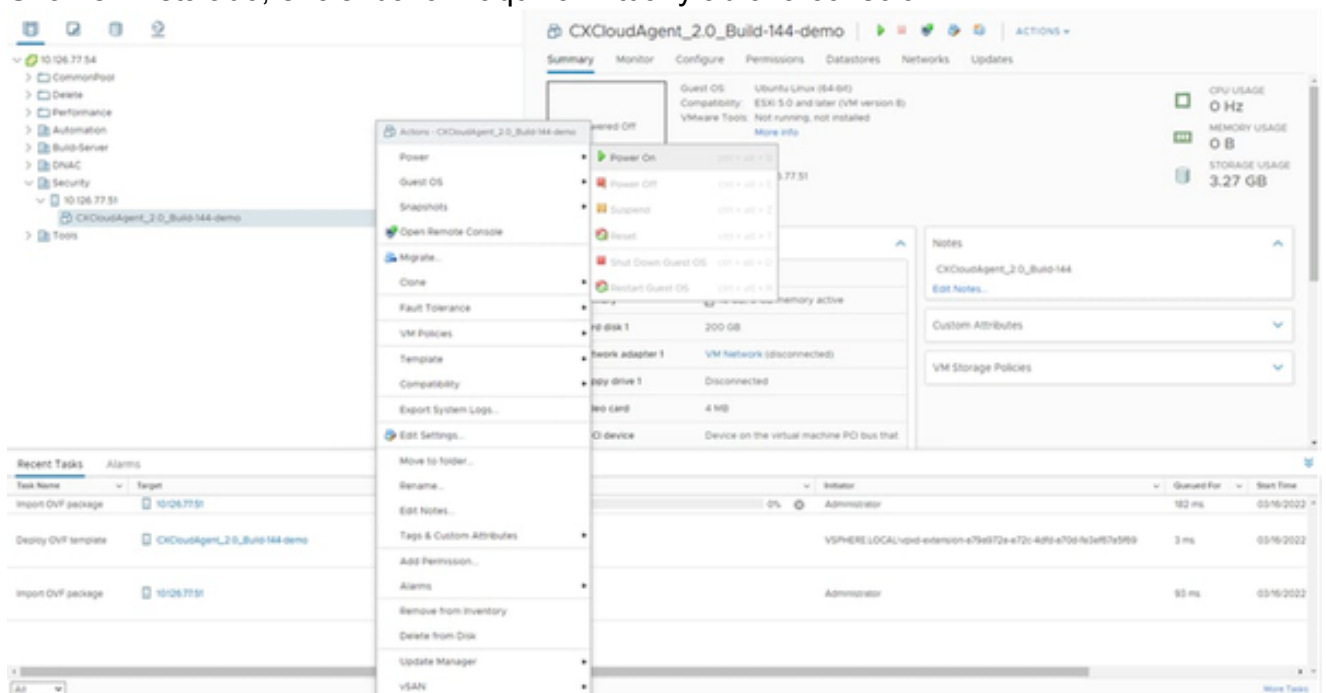
VM agregada

14. Haga clic en la máquina virtual recién agregada para ver el estado.



VM agregada

15. Una vez instalado, encienda la máquina virtual y abra la consola.



Abrir consola

16. Vaya a [Network Configuration](#) para continuar con los siguientes pasos.

Instalación de Oracle Virtual Box 7.0.12

Este cliente implementa OVA de agente CX a través de la caja virtual de Oracle.

1. Descargue el OVA CXCloudAgent\_3.1 en el cuadro de ventanas de cualquier carpeta.
2. Vaya a la carpeta mediante la interfaz de línea de comandos.

3. Descomprima el archivo OVA mediante el comando tar -xvf D:\CXCloudAgent\_3.1\_Build-xx.oVA.

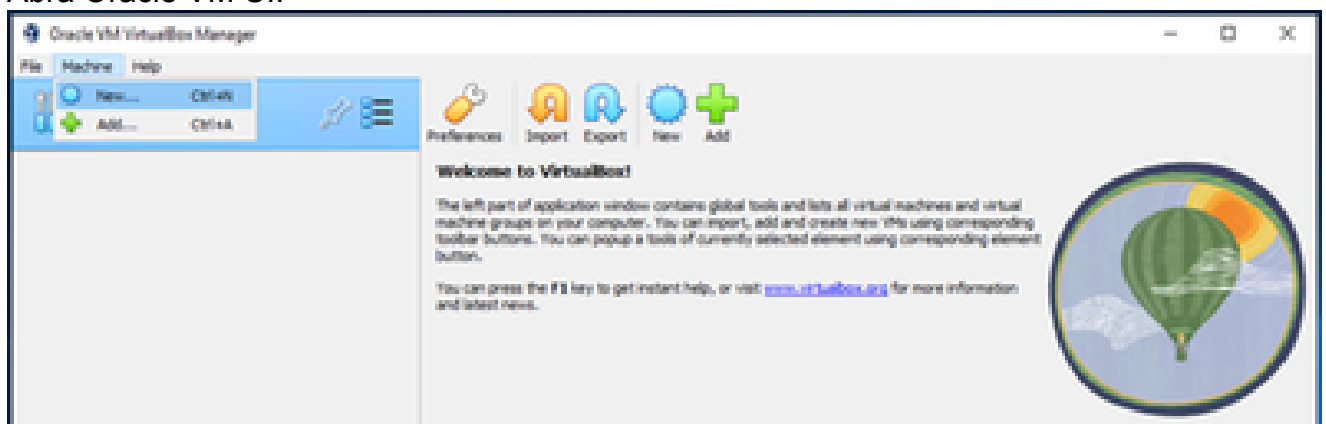
```
D:\>cd CXCAGENT

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

D:\CXCAGENT>
```

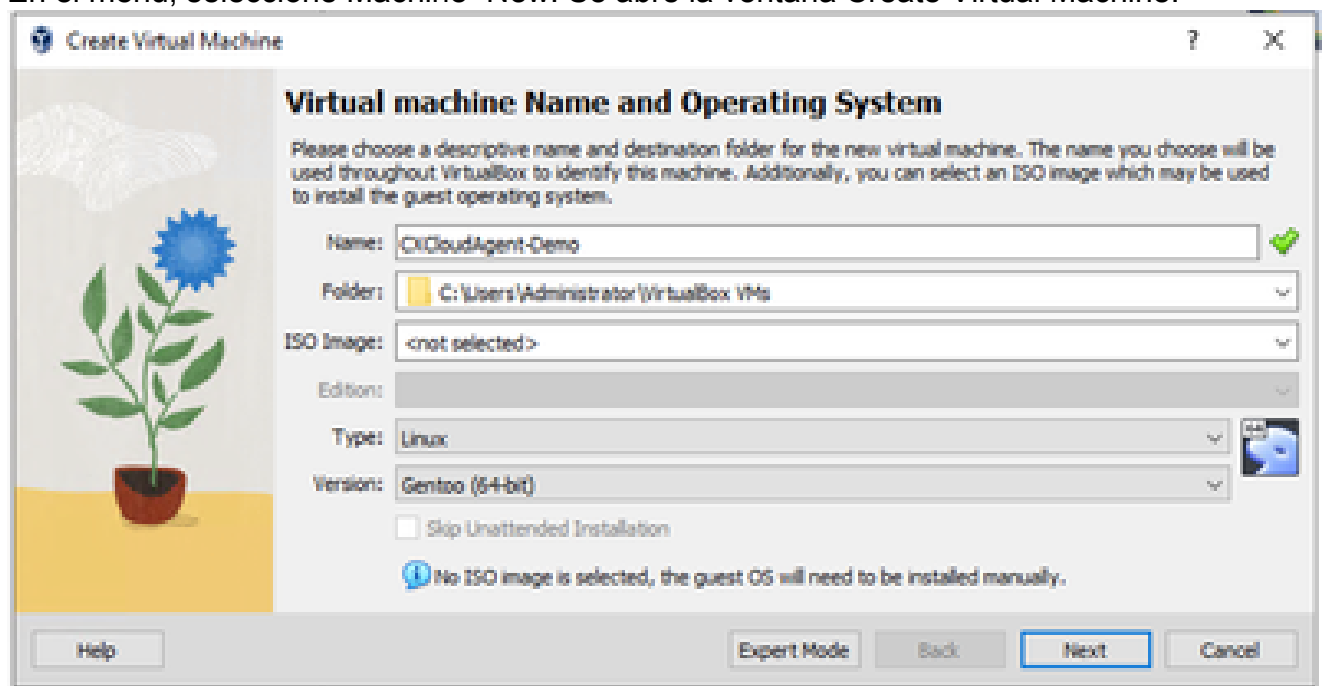
Descomprimir archivo OVA

4. Abra Oracle VM UI.



Oracle VM

5. En el menú, seleccione Machine>New. Se abre la ventana Create Virtual Machine.



Crear máquina virtual

6. Ingrese los siguientes detalles en la ventana Nombre de la máquina virtual y sistema operativo.

Nombre: Nombre de VM

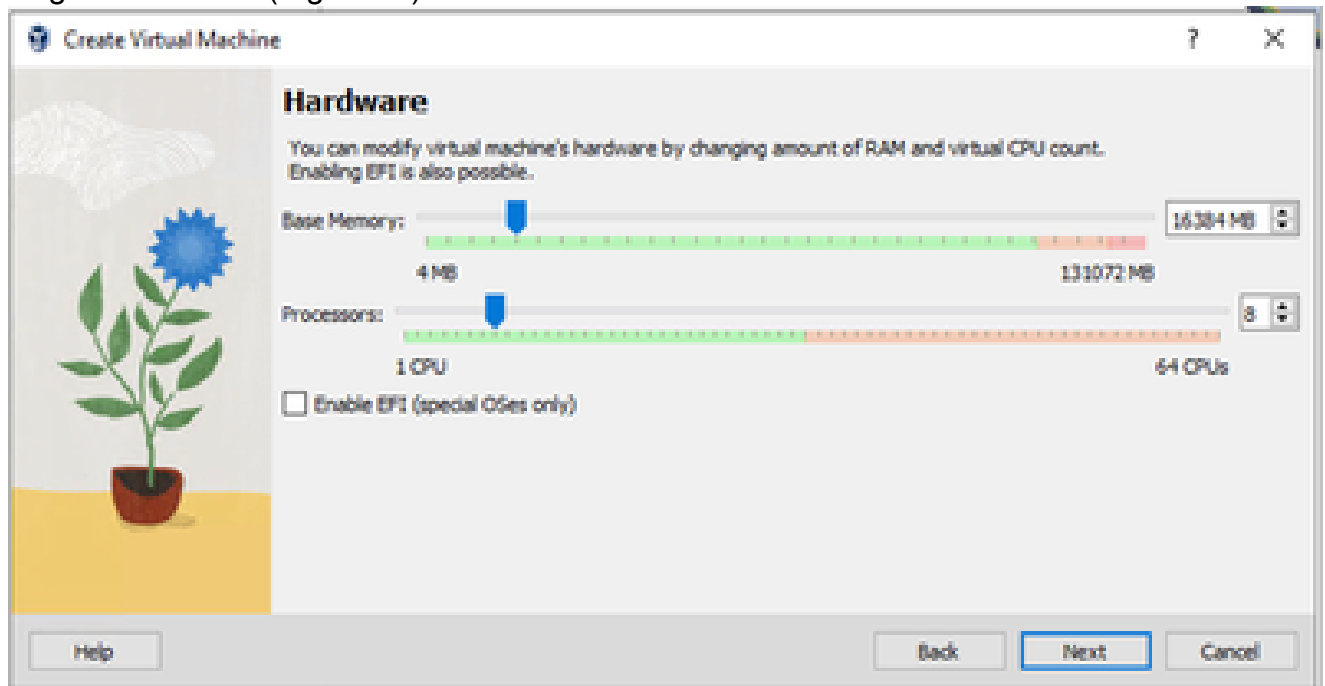
Carpeta: Ubicación en la que se almacenarán los datos de VM

Imagen ISO: ninguno

Tipo: Linux

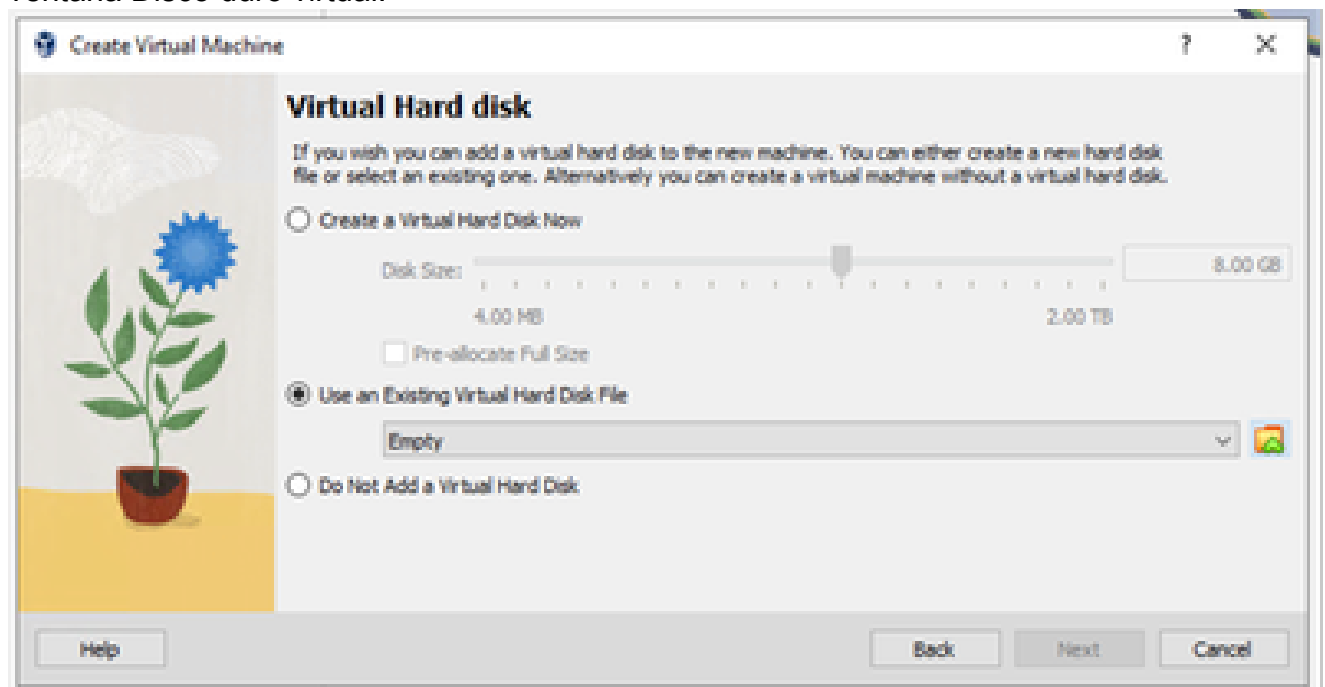
Versión: Gentoo (64 bits)

7. Haga clic en Next (Siguiente). Se abre la ventana Hardware.



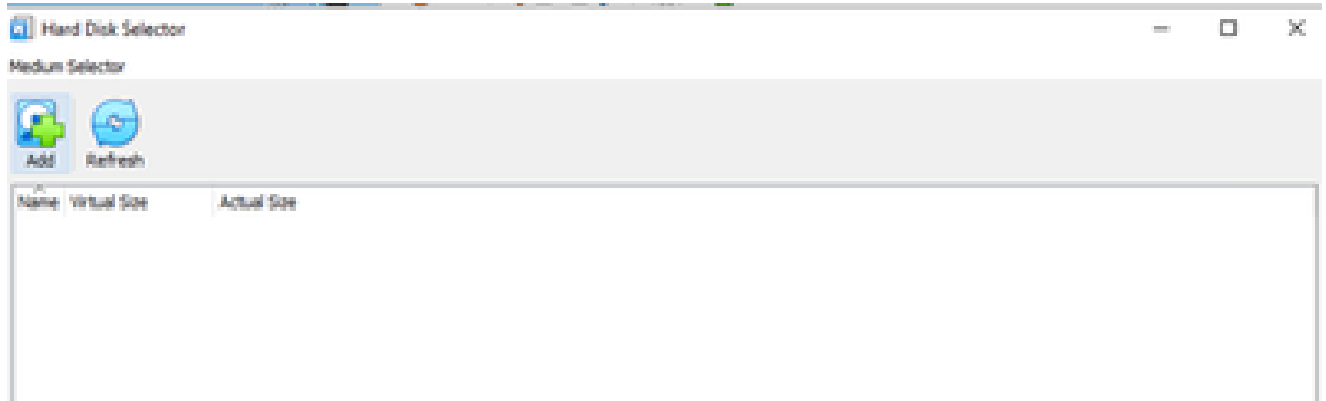
Hardware

8. Ingrese Base Memory (16384 MB) y Processors (8 CPU) y haga clic en Next. Se abre la ventana Disco duro virtual.



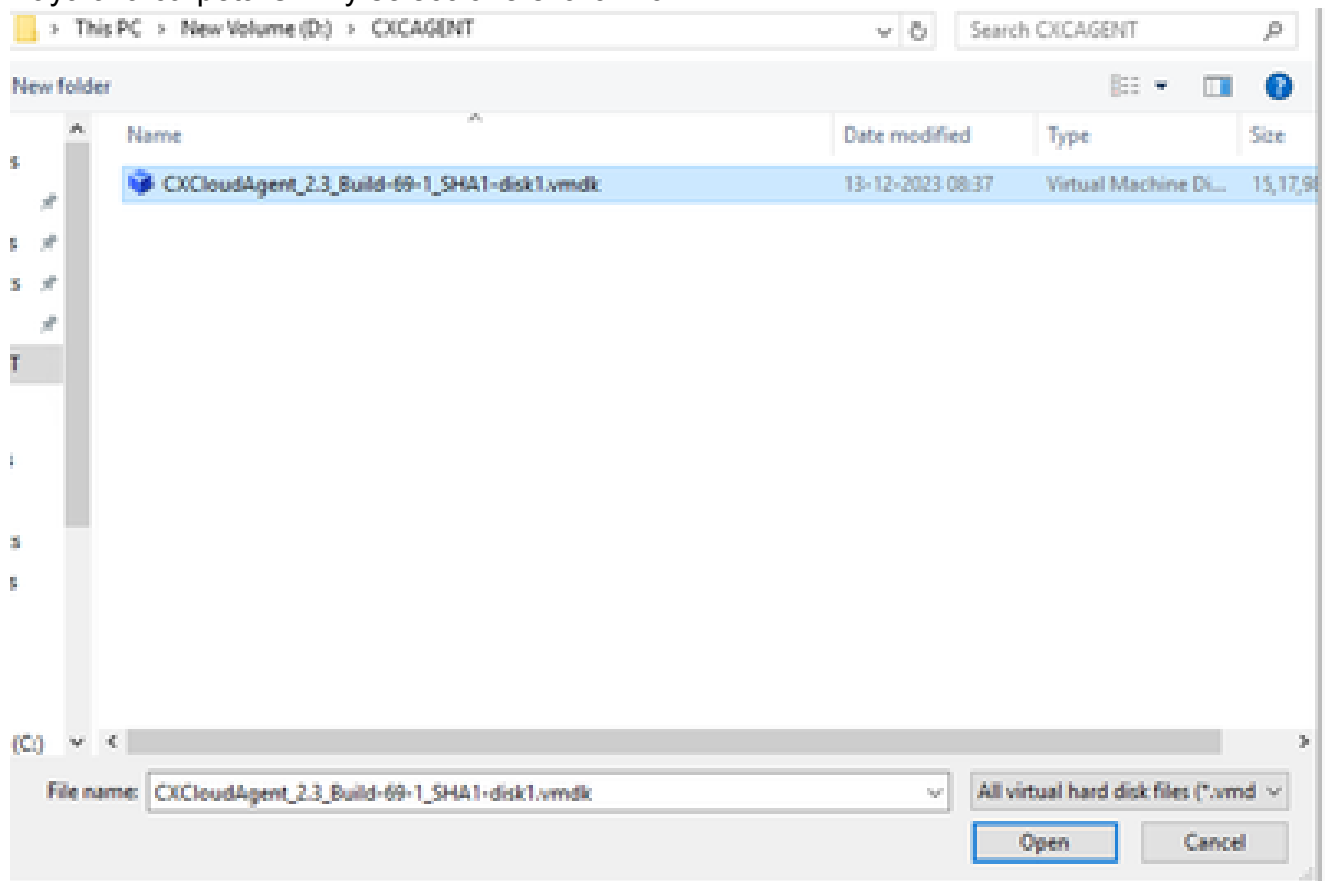
Disco duro virtual

9. Seleccione el botón de opción Use an Existing Virtual Hard Disk File y seleccione el icono Browse. Se abrirá la ventana Selector de disco duro.



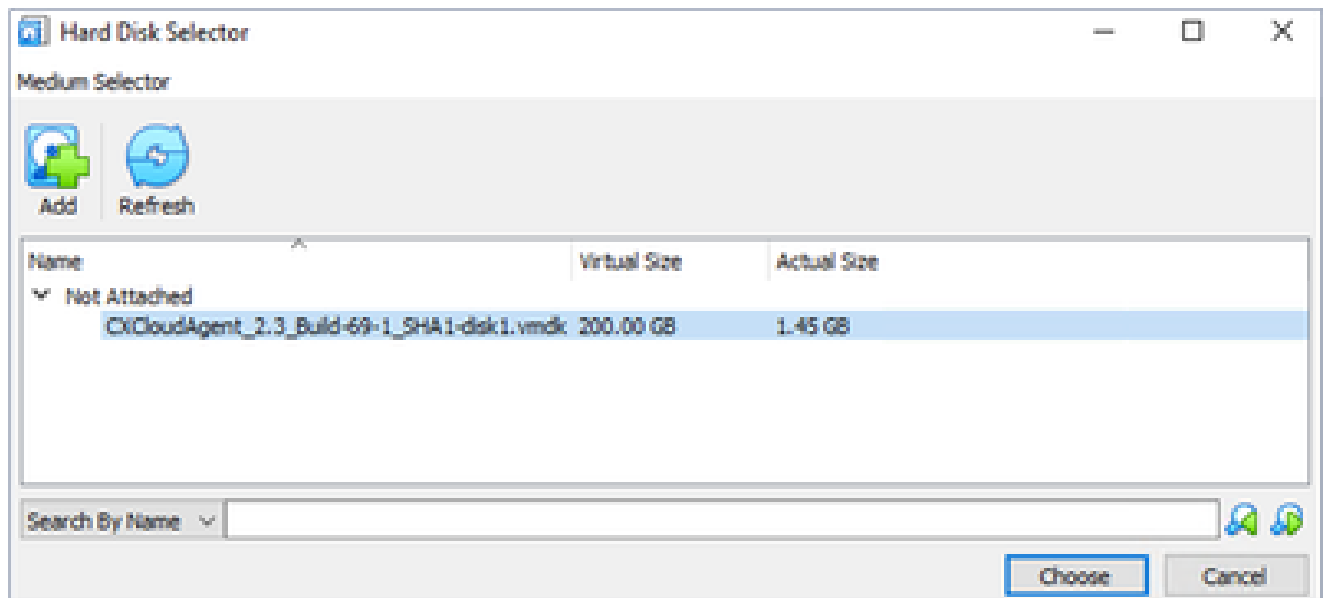
Selector de disco duro

10. Vaya a la carpeta OVA y seleccione el archivo VMDK.



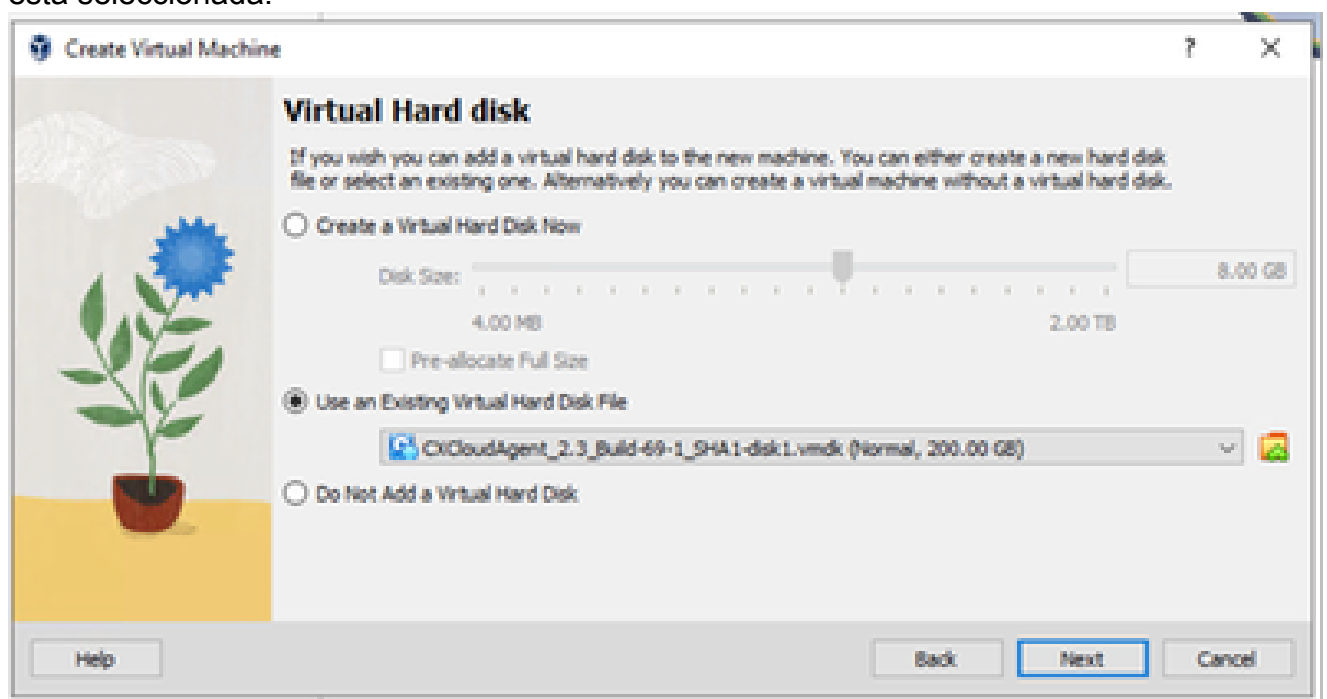
Carpeta OVA

11. Haga clic en Abrir. El archivo se muestra en la ventana Hardware Disk Selector.



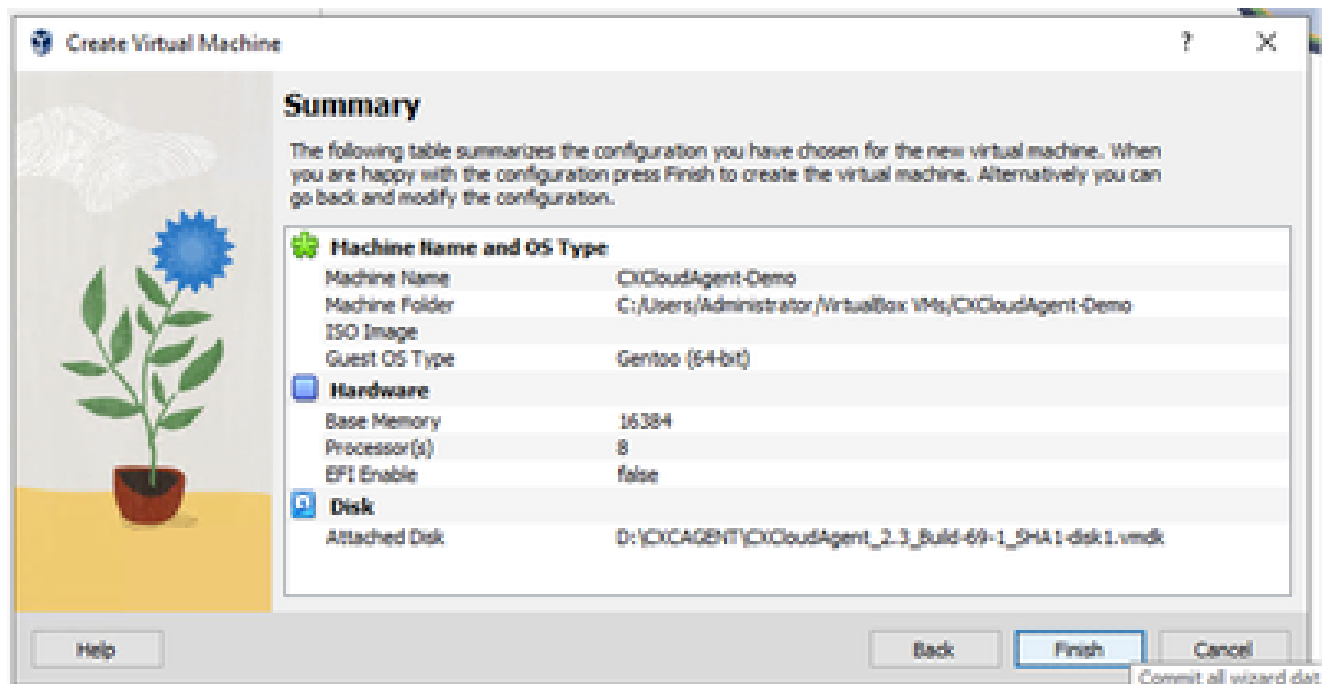
Selector de disco duro

- Haga clic en Elegir. Se abre la ventana Disco duro virtual. Confirme que la opción mostrada está seleccionada.



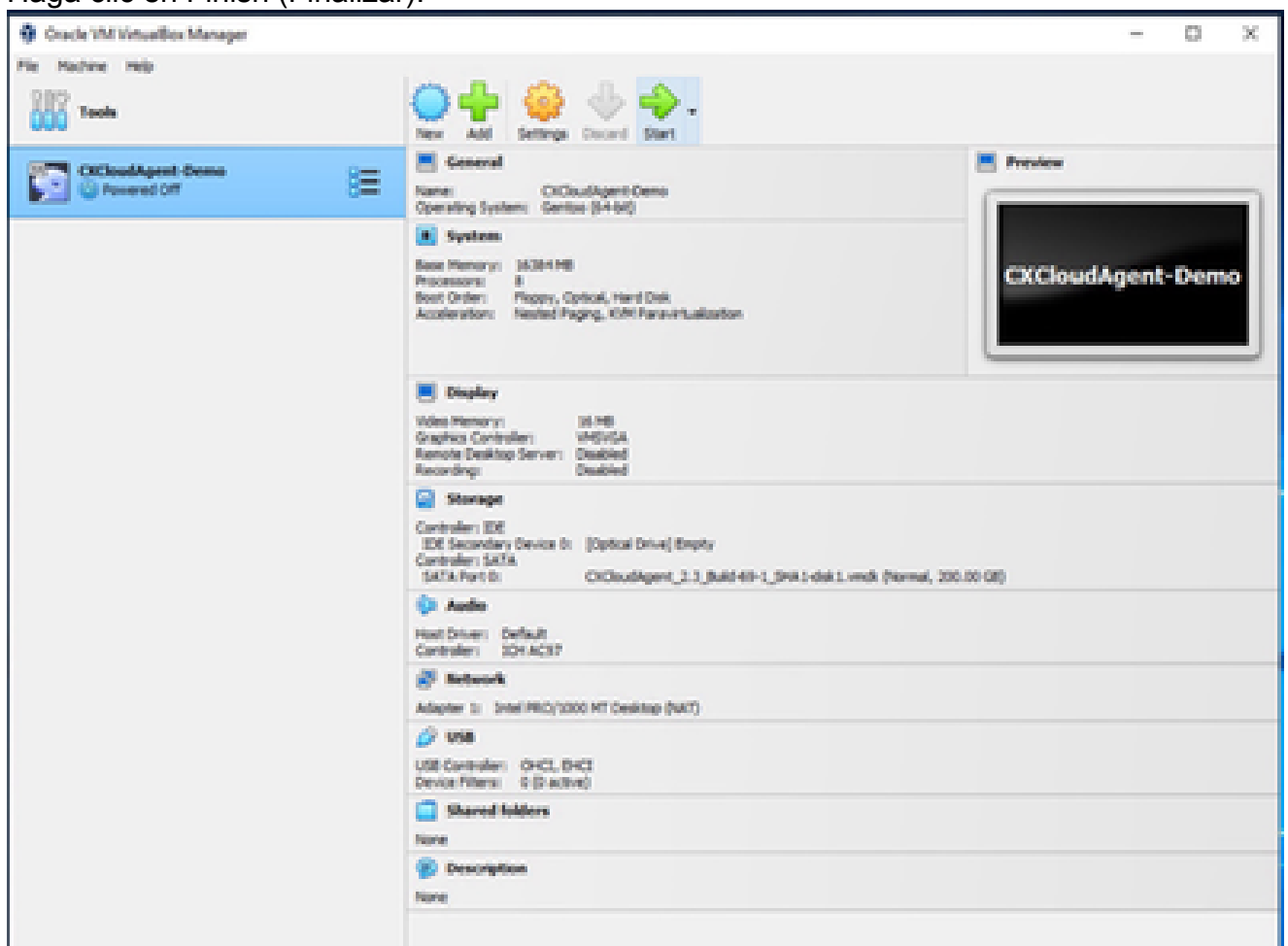
Seleccionar archivo

- Haga clic en Next (Siguiente). Se abre la ventana Summary.



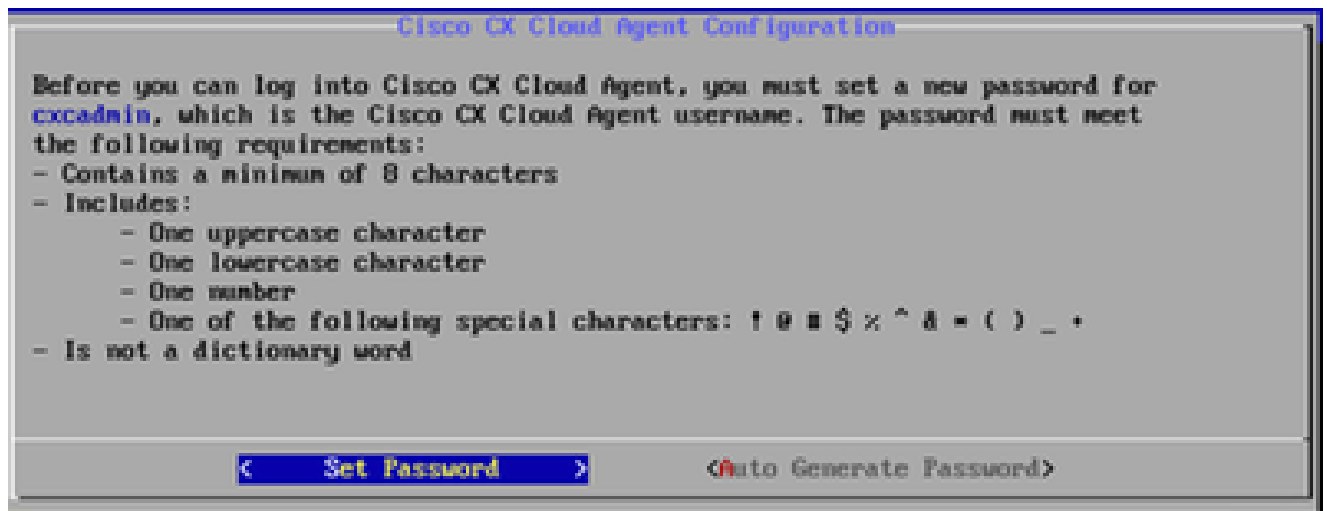
Summary

14. Haga clic en Finish (Finalizar).



Inicio de la consola VM

15. Seleccione la VM implementada y haga clic en Start. La máquina virtual se enciende y la pantalla de la consola se muestra para la configuración.



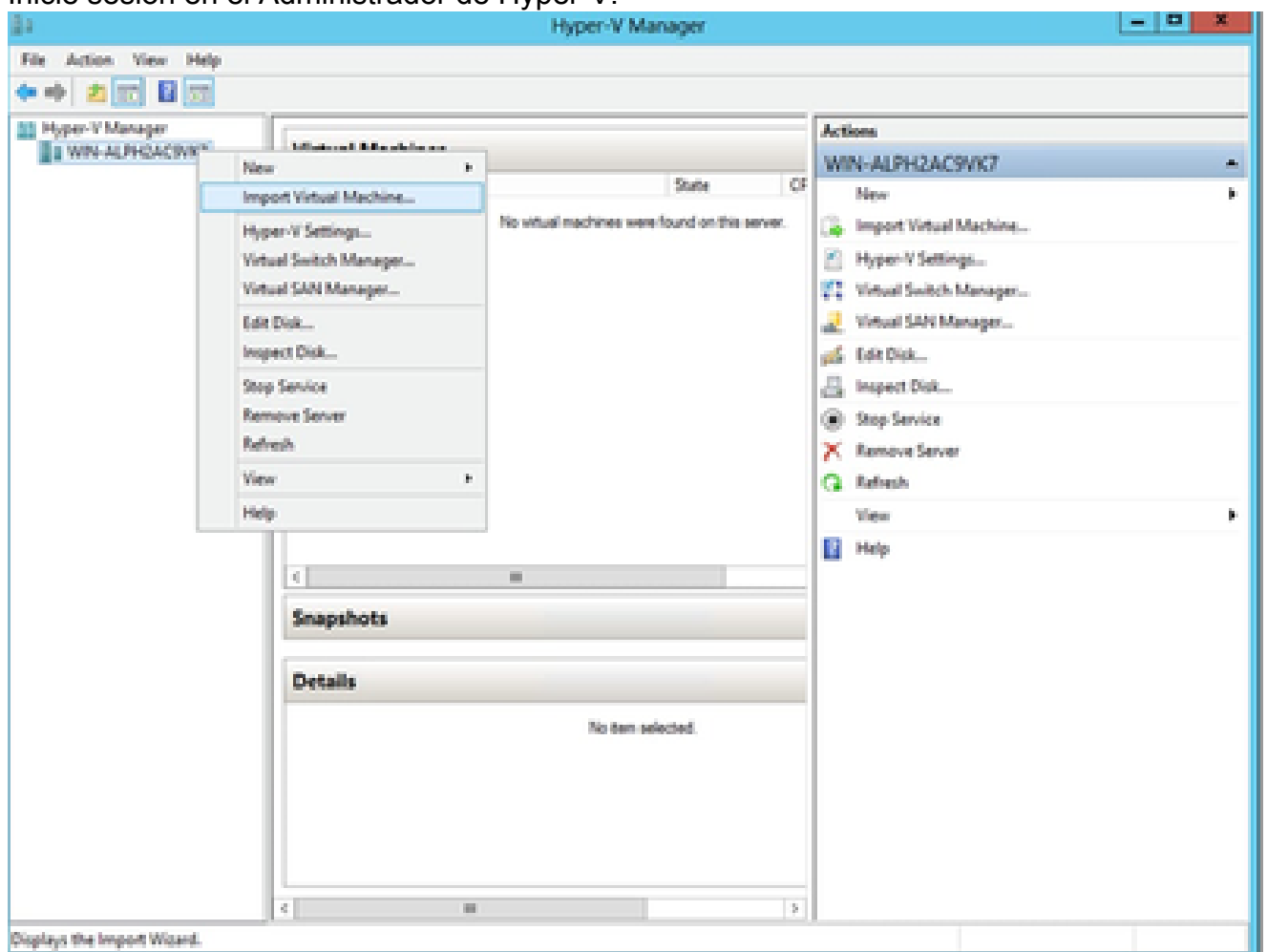
Abrir la consola

16. Vaya a [Network Configuration](#) para continuar con los siguientes pasos.

## Instalación de Microsoft Hyper-V

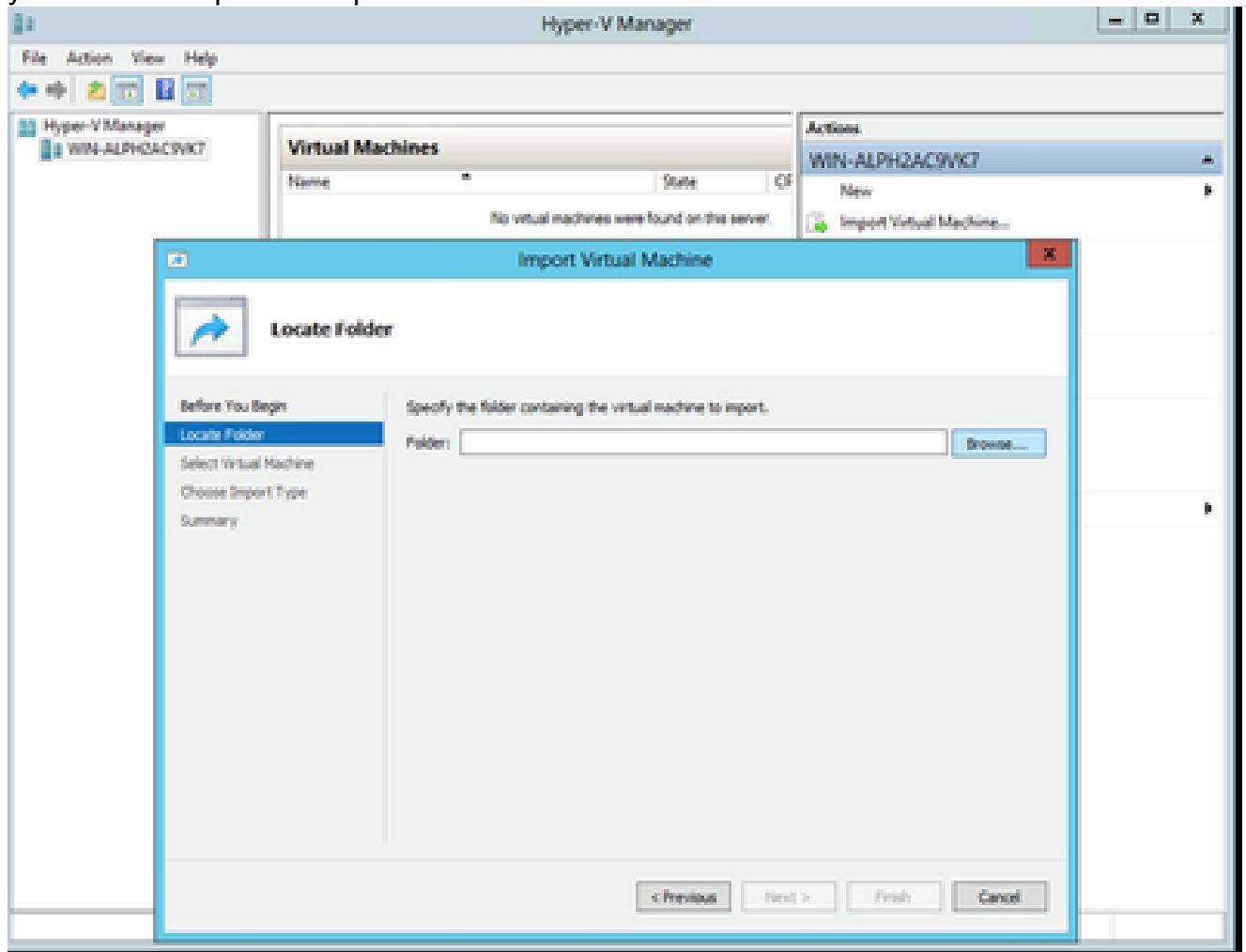
Este cliente implementa el agente CX OVA a través de la instalación de Microsoft Hyper-V.

1. Inicie sesión en el Administrador de Hyper-V.



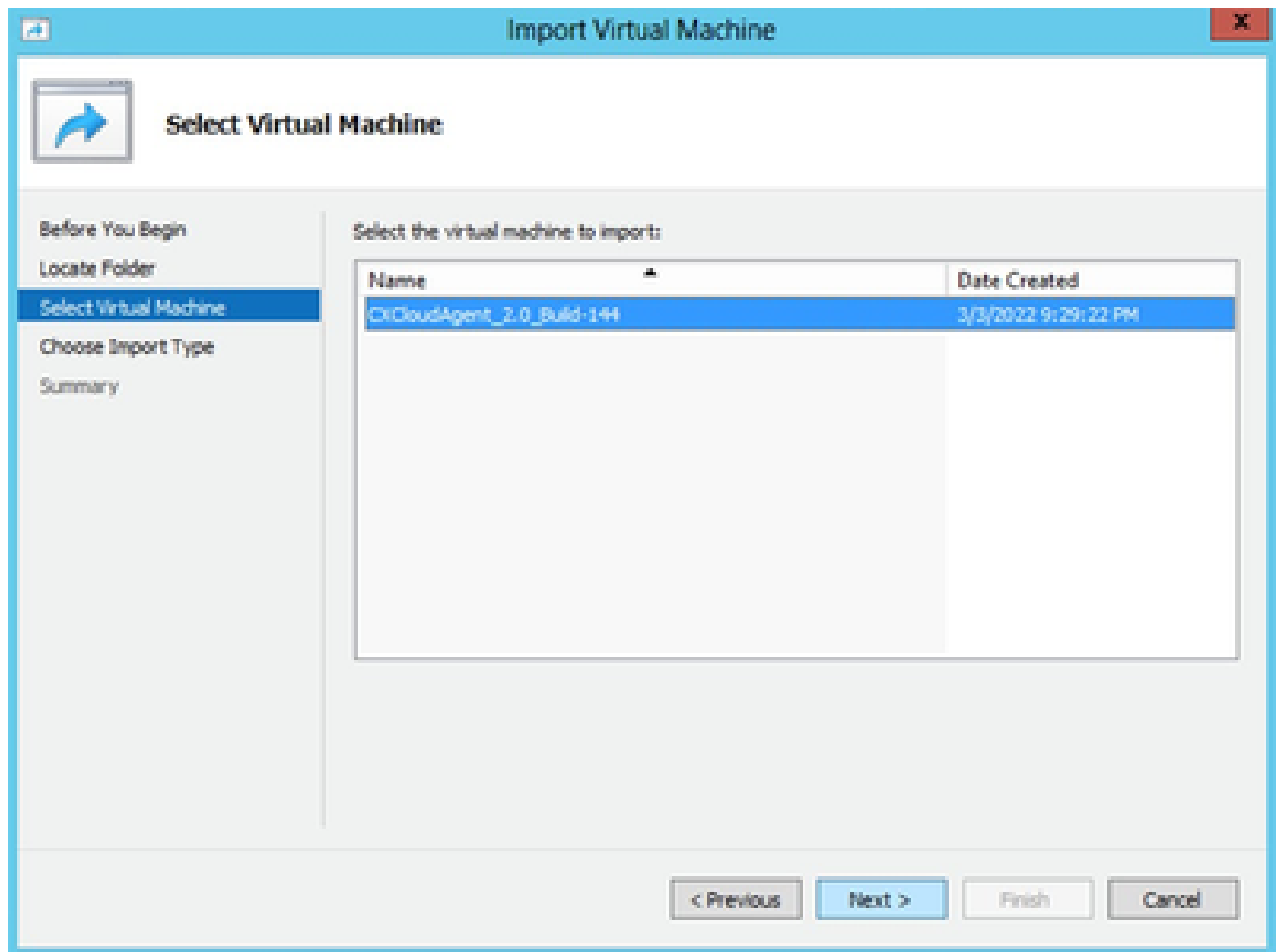
Administrador de Hyper-V

2. Seleccione la máquina virtual de destino, haga clic con el botón derecho para abrir el menú y seleccione Importar máquina virtual.



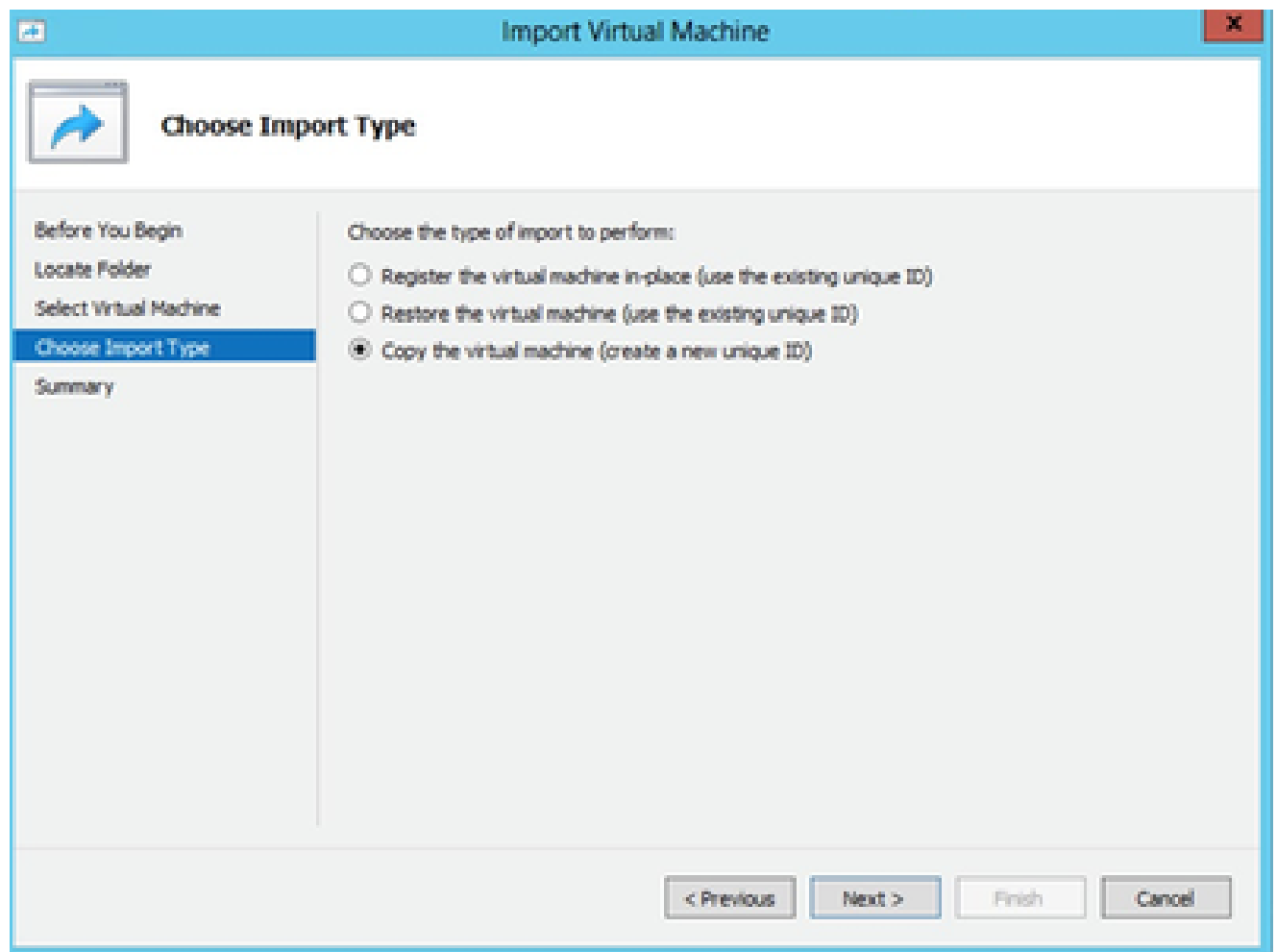
Carpeta para importar

3. Busque y seleccione la carpeta de descarga y haga clic en Next.



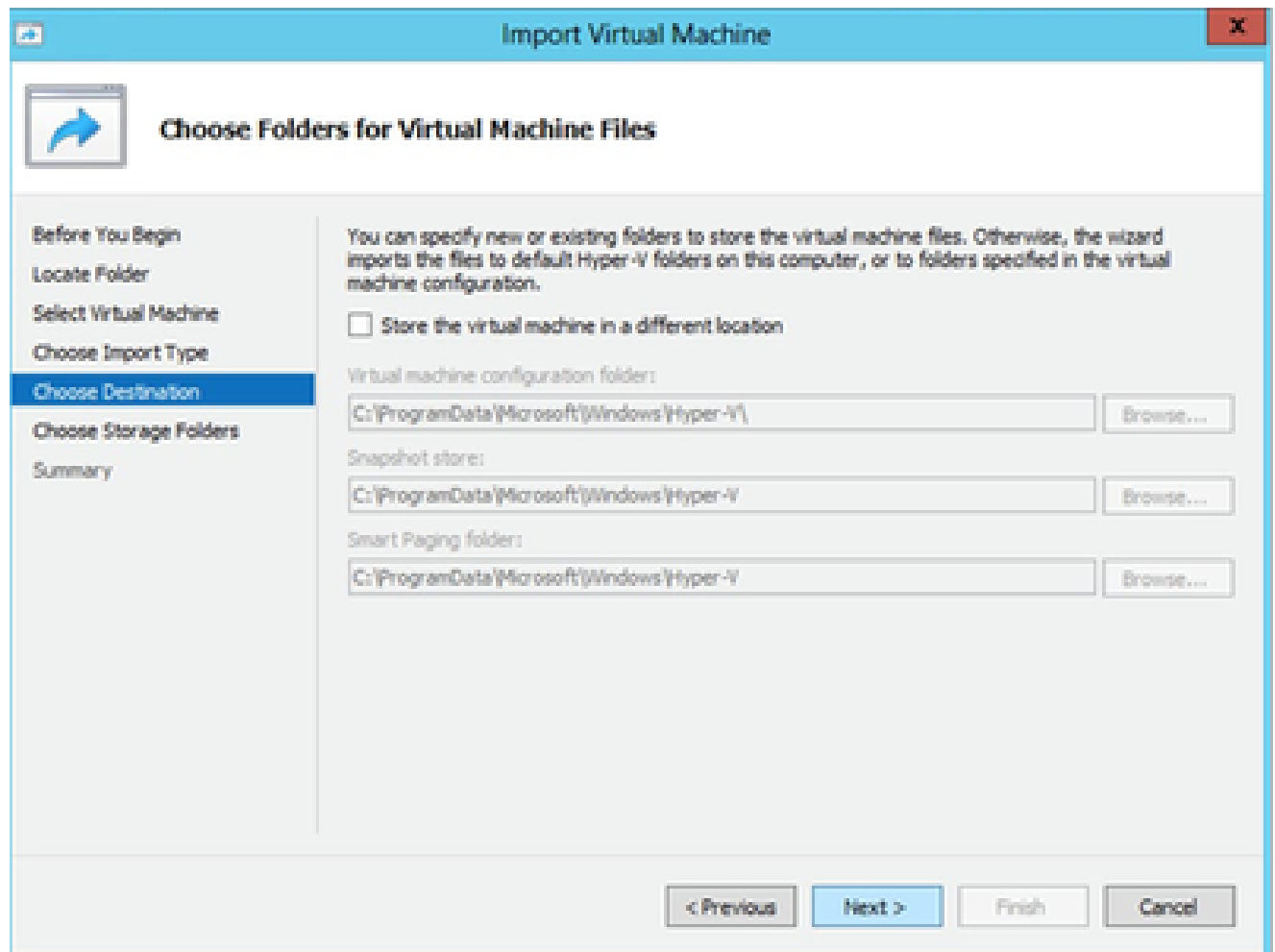
Seleccionar VM

4. Seleccione la VM y haga clic en Next.



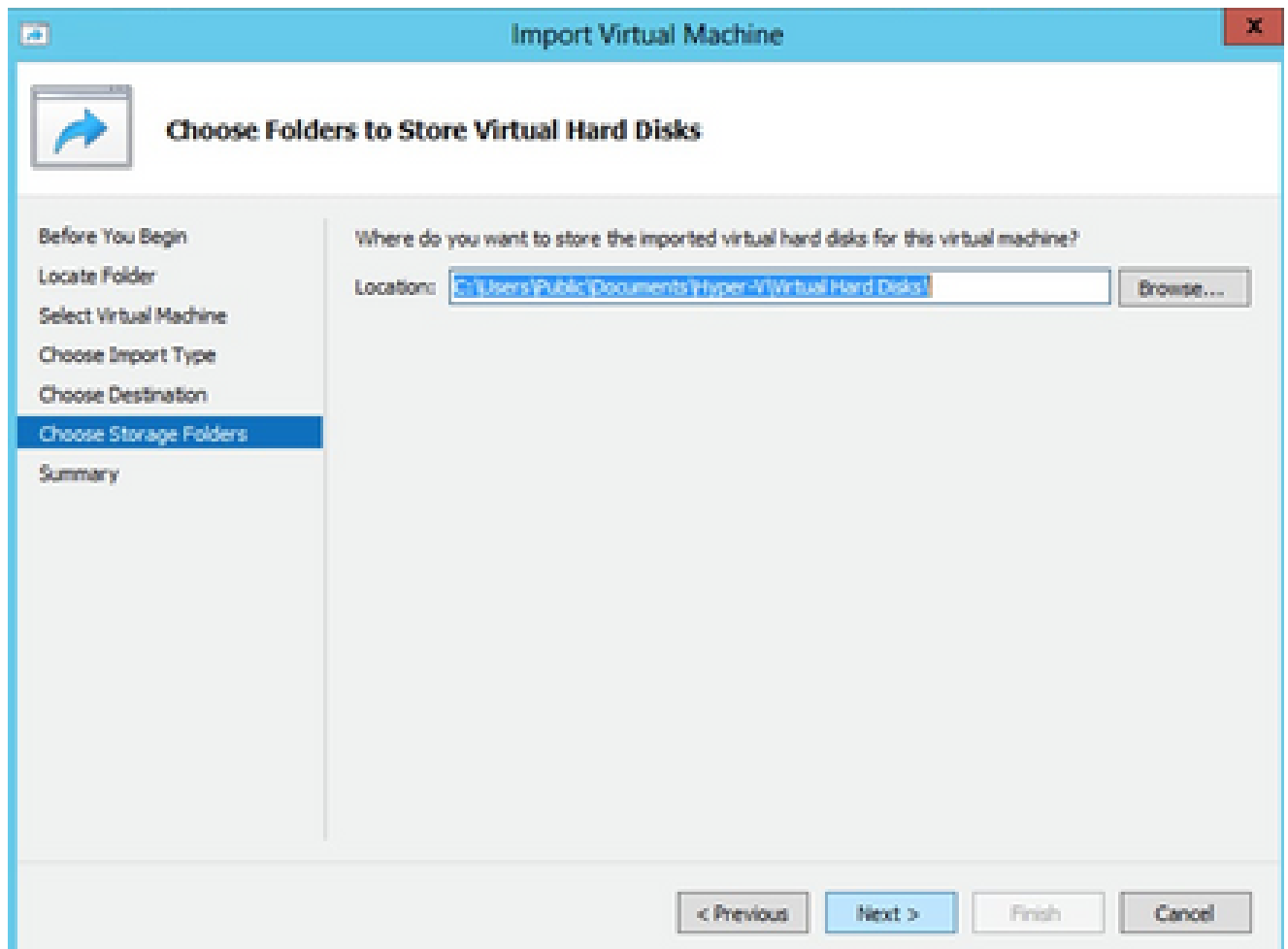
Tipo de importación

5. Seleccione el botón de opción Copy the virtual machine (create a new unique ID) y haga clic en Next.



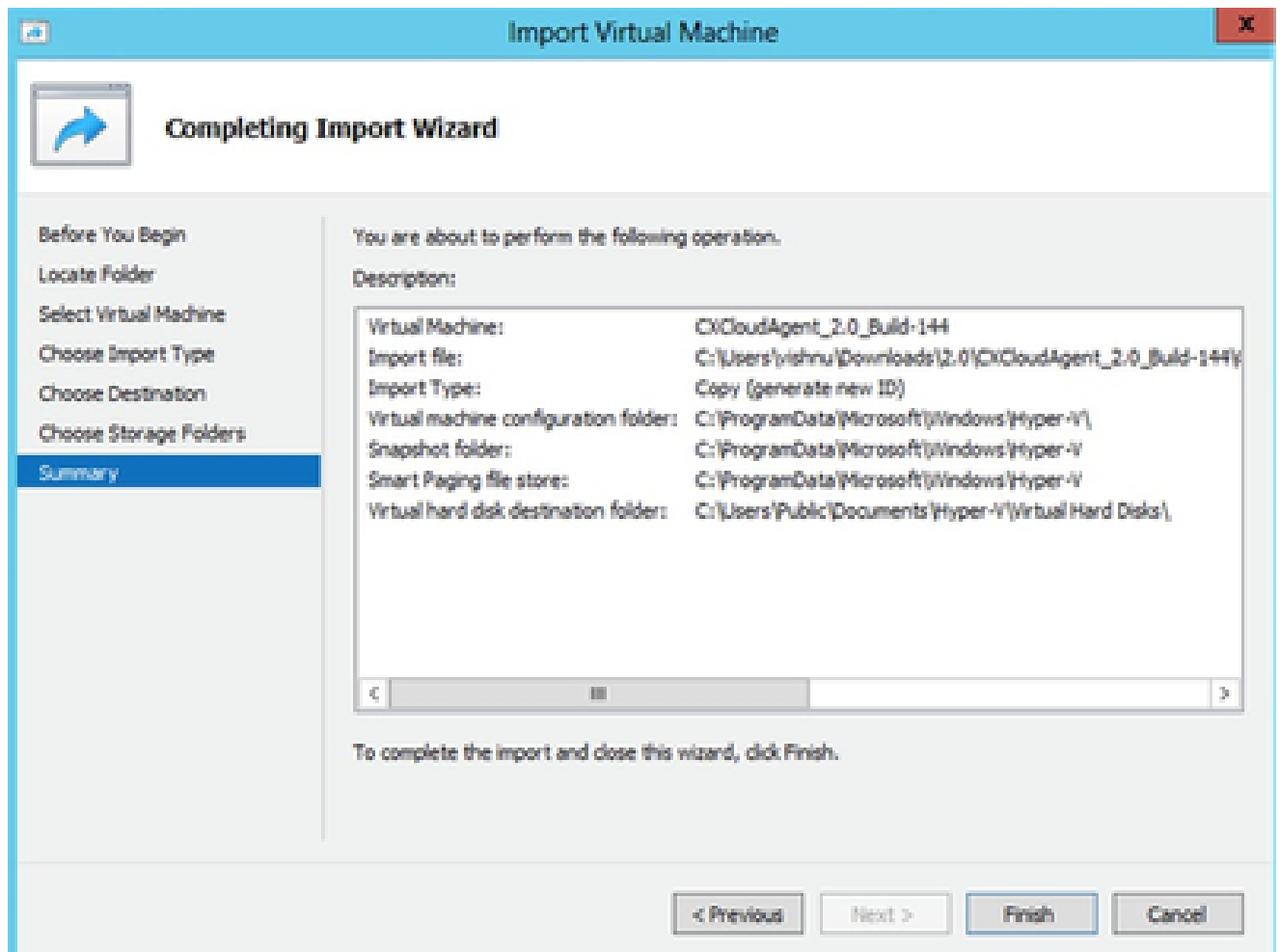
Elegir carpetas para archivos de máquina virtual

6. Busque la carpeta para los archivos de VM. Cisco recomienda utilizar las rutas predeterminadas.
7. Haga clic en Next (Siguiente).



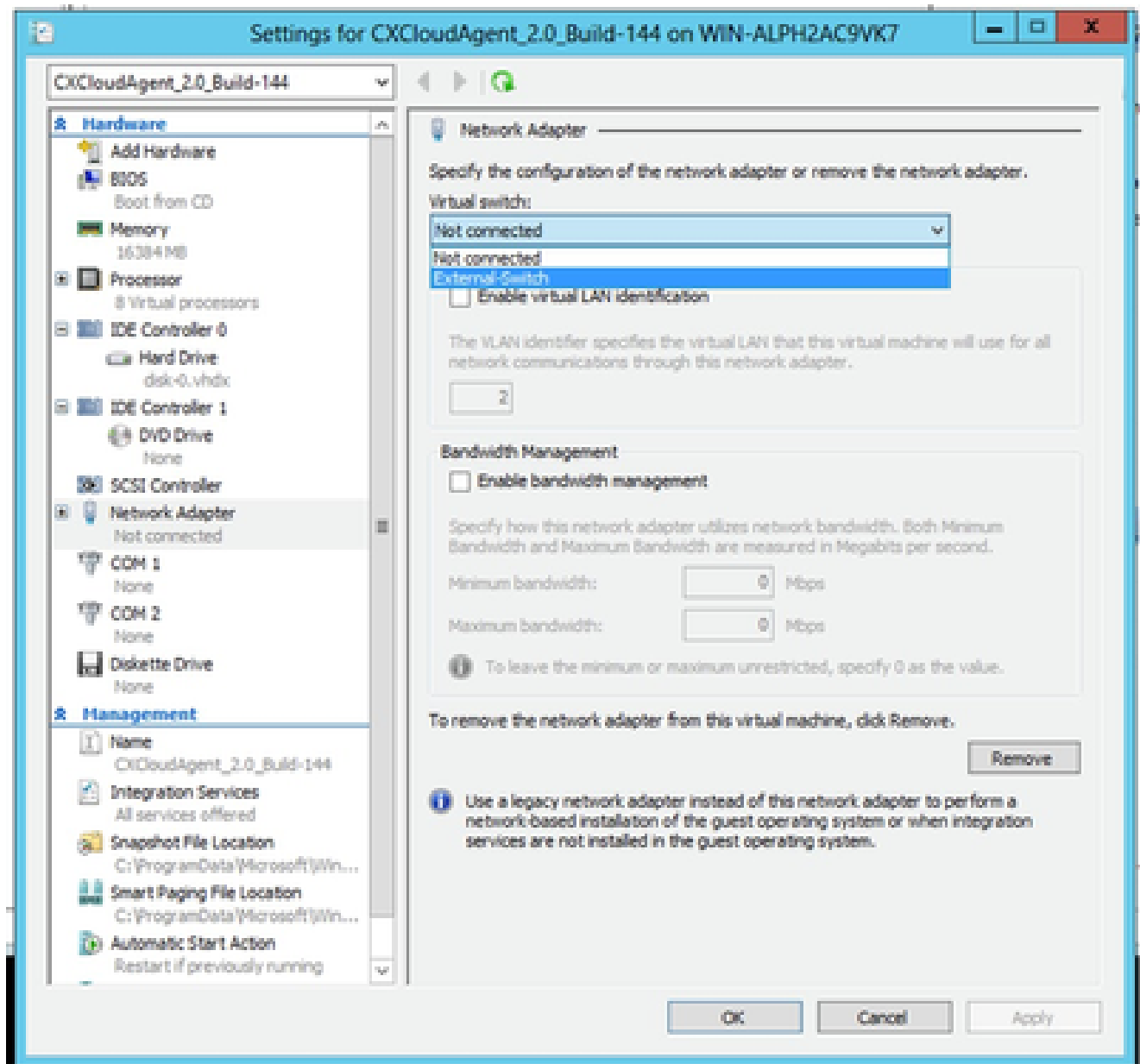
Carpeta para almacenar los discos duros virtuales

8. Busque y seleccione la carpeta en la que desea almacenar los discos duros de VM. Cisco recomienda utilizar las rutas predeterminadas.
9. Haga clic en Next (Siguiente). Se muestra el resumen de VM.



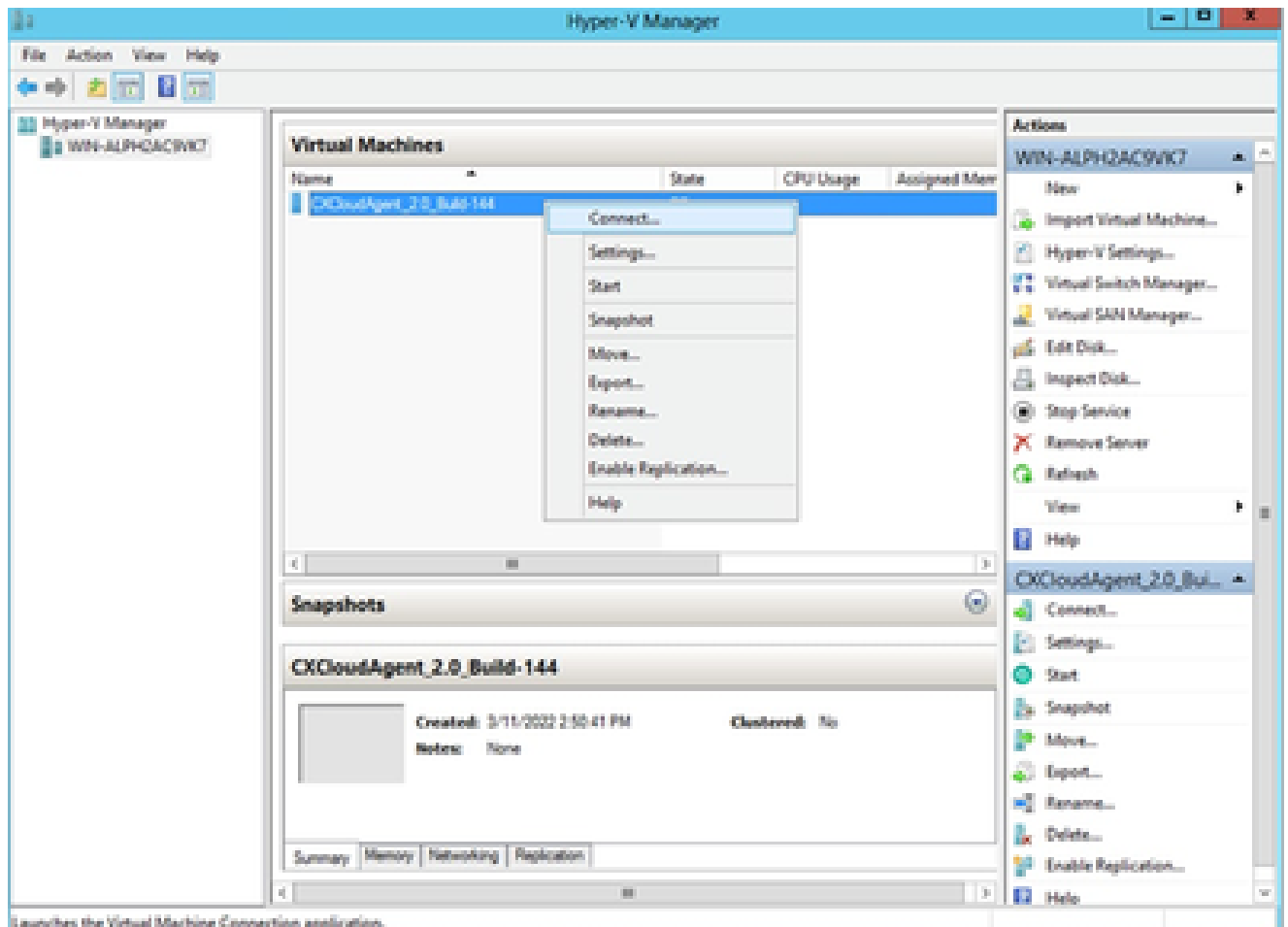
Summary

10. Verifique todas las entradas y haga clic en Finish.
11. Una vez completada correctamente la importación, se crea una nueva VM en Hyper-V. Abra la configuración de VM.



Switch virtual

12. Seleccione el adaptador de red en el panel izquierdo y seleccione el switch virtual disponible en la lista desplegable.

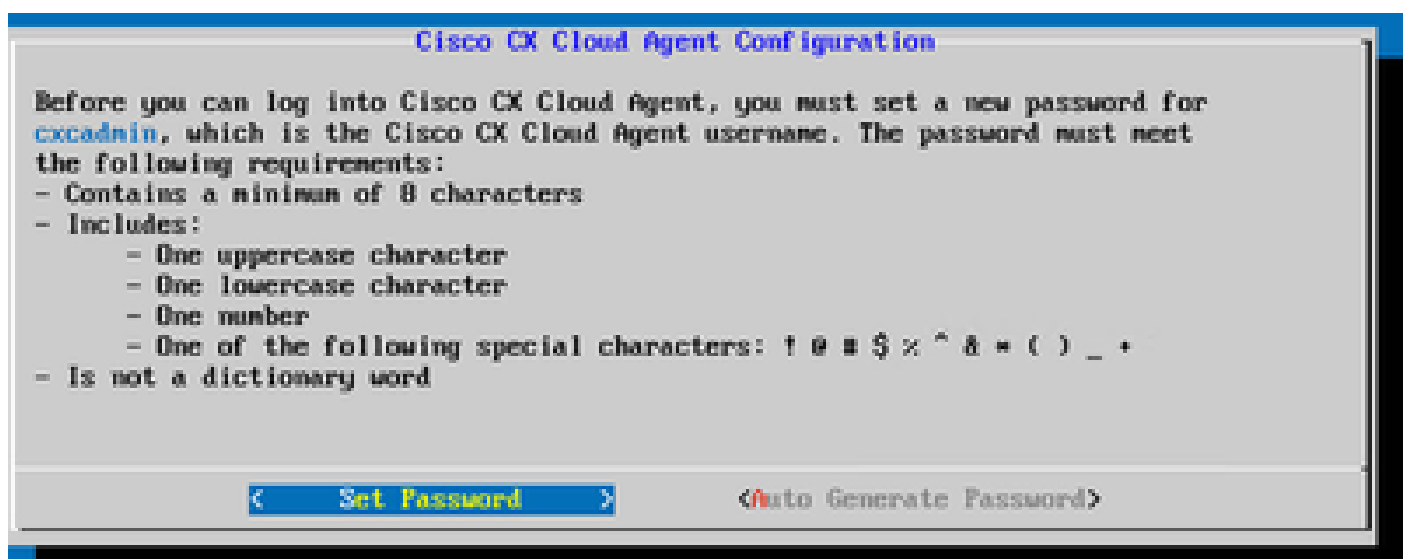


VM inicial

13. Seleccione Connect para iniciar la máquina virtual.
14. Vaya a [Network Configuration](#) para continuar con los siguientes pasos.

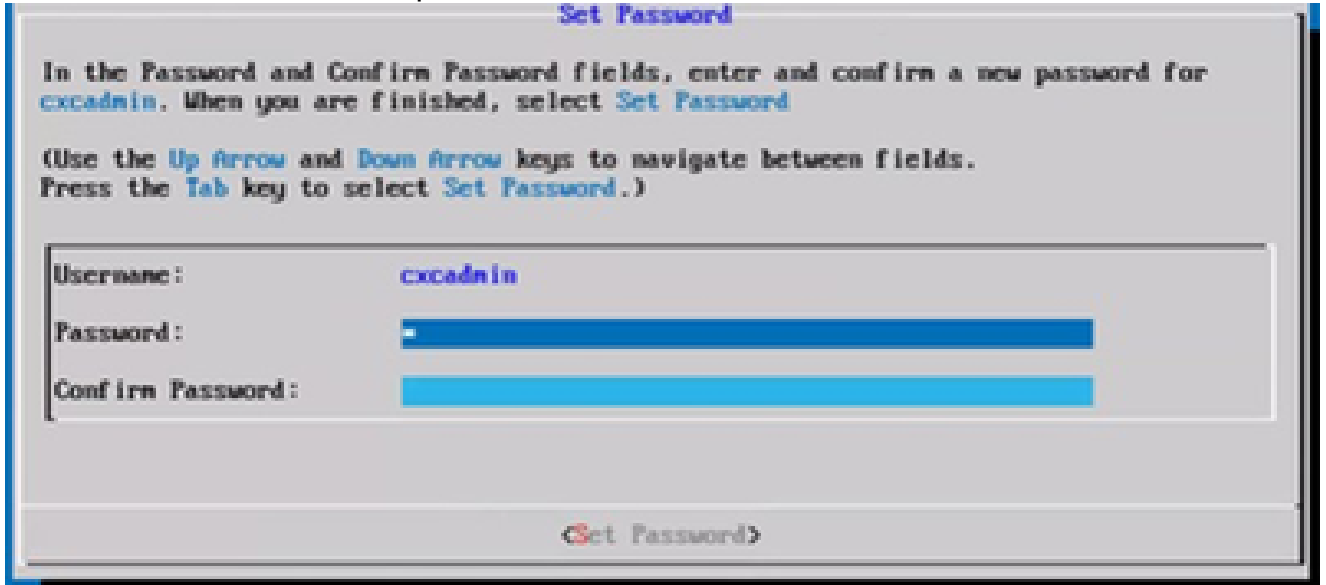
## Configuración de red

Para establecer la contraseña del agente en la nube CX para el nombre de usuario cxcadmin:



Establecer contraseña

1. Haga clic en Set Password para agregar una nueva contraseña para cxcadmin O haga clic en Auto Generate Password para obtener una nueva contraseña.



Nueva contraseña

2. Si se selecciona Set Password, ingrese la contraseña para cxcadmin y confírmela. Haga clic en Set Password y vaya al paso 3.

O

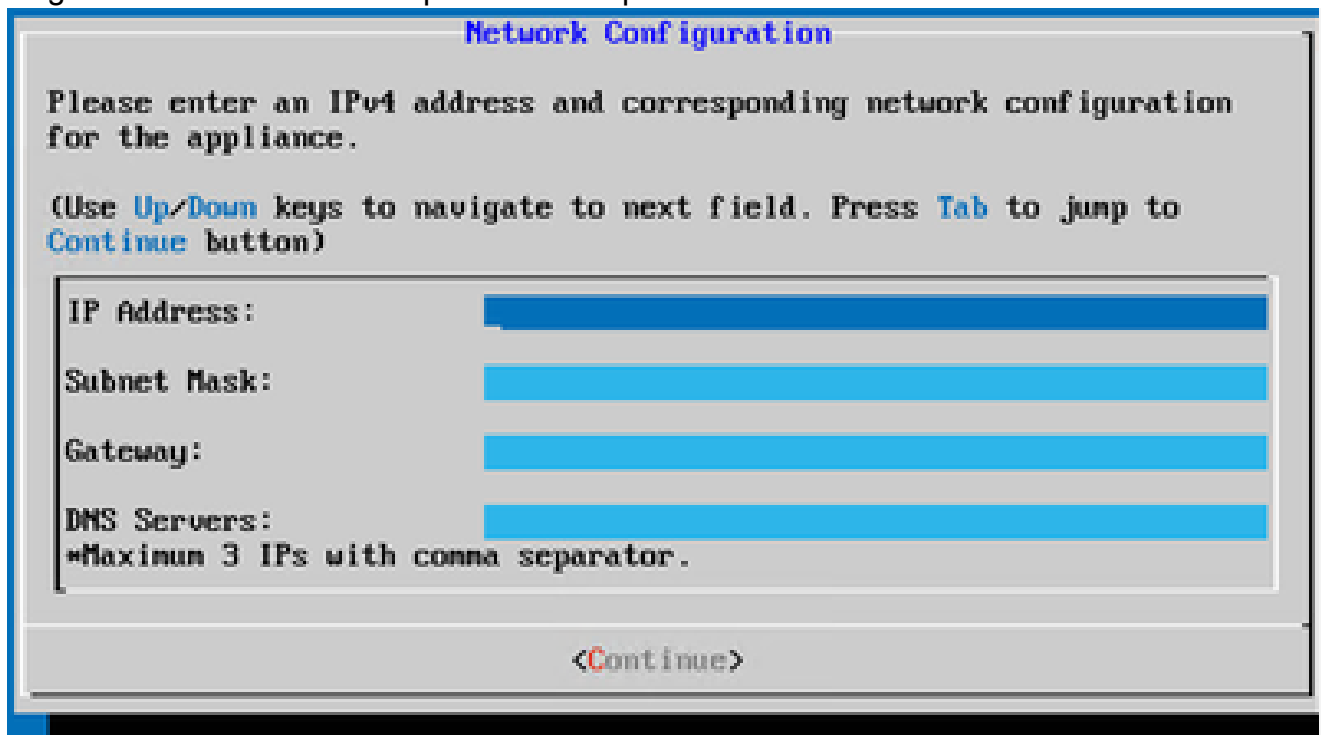
Si se selecciona Auto Generate Password, copie la contraseña generada y guárdela para su uso futuro. Haga clic en Save Password y vaya al paso 4.



Contraseña generada automáticamente



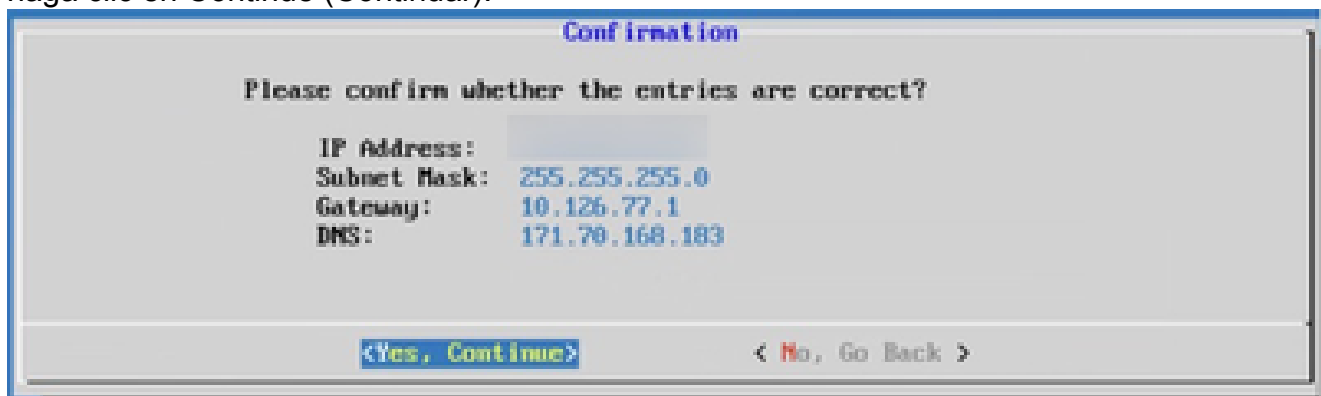
3. Haga clic en Save Password para utilizarlo para la autenticación.



The image shows a 'Network Configuration' window with a title bar. Inside, it says 'Please enter an IPv4 address and corresponding network configuration for the appliance.' followed by '(Use Up/Down keys to navigate to next field. Press Tab to jump to Continue button)'. There are four input fields: 'IP Address:', 'Subnet Mask:', 'Gateway:', and 'DNS Servers:'. Below the 'DNS Servers:' field is a note: '\*Maximum 3 IPs with comma separator.'. At the bottom right is a '<Continue>' button.

Configuración de red

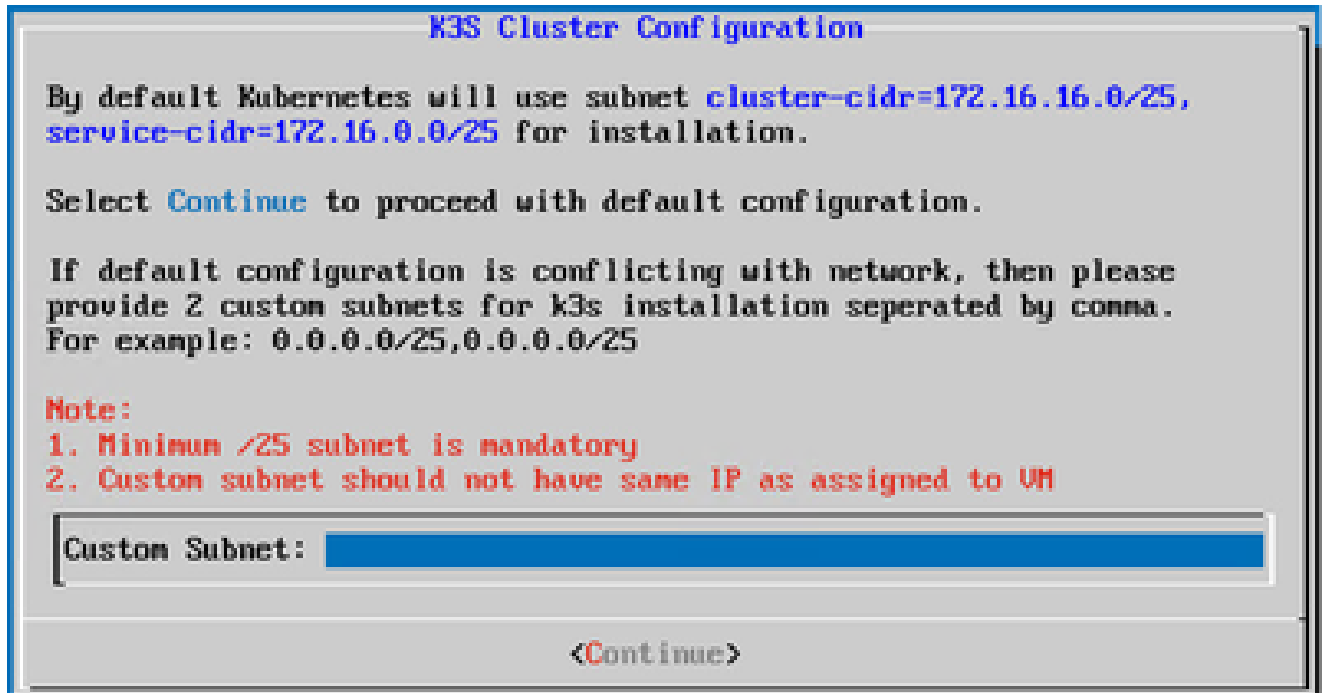
4. Introduzca la dirección IP, la máscara de subred, la puerta de enlace y el servidor DNS y haga clic en Continue (Continuar).



The image shows a 'Confirmation' window with a title bar. It asks 'Please confirm whether the entries are correct?'. Below this, it lists the entered values: 'IP Address:', 'Subnet Mask: 255.255.255.0', 'Gateway: 10.126.77.1', and 'DNS: 171.70.168.183'. At the bottom, there are two buttons: '<Yes, Continue>' and '<No, Go Back>'. The 'Yes, Continue' button is highlighted.

Confirmación

5. Confirme las entradas y haga clic en Yes, Continue.

A terminal window titled "K3S Cluster Configuration" with a blue header bar. The text inside is as follows:

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

Select `Continue` to proceed with default configuration.

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

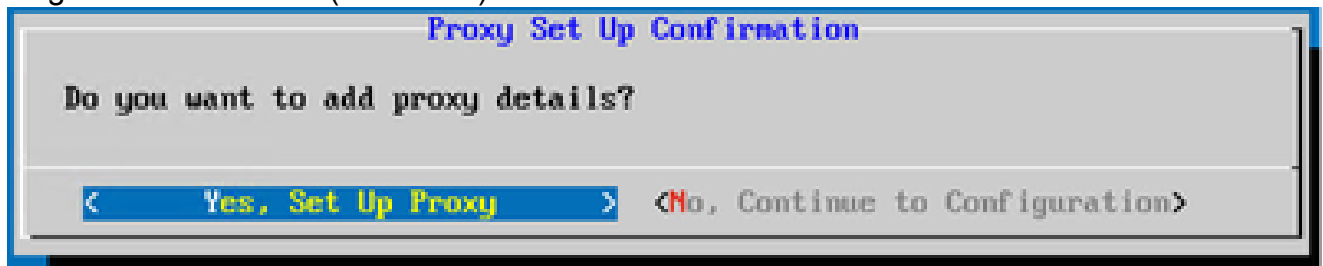
**Note:**  
1. Minimum `/25` subnet is mandatory  
2. Custom subnet should not have same IP as assigned to VM

Custom Subnet:

`<Continue>`

Subred personalizada

6. Ingrese la dirección IP de subred personalizada para la configuración del clúster K3S (si la subred predeterminada de un cliente entra en conflicto con la red de sus dispositivos, seleccione otra subred personalizada).
7. Haga clic en Continue (Continuar).

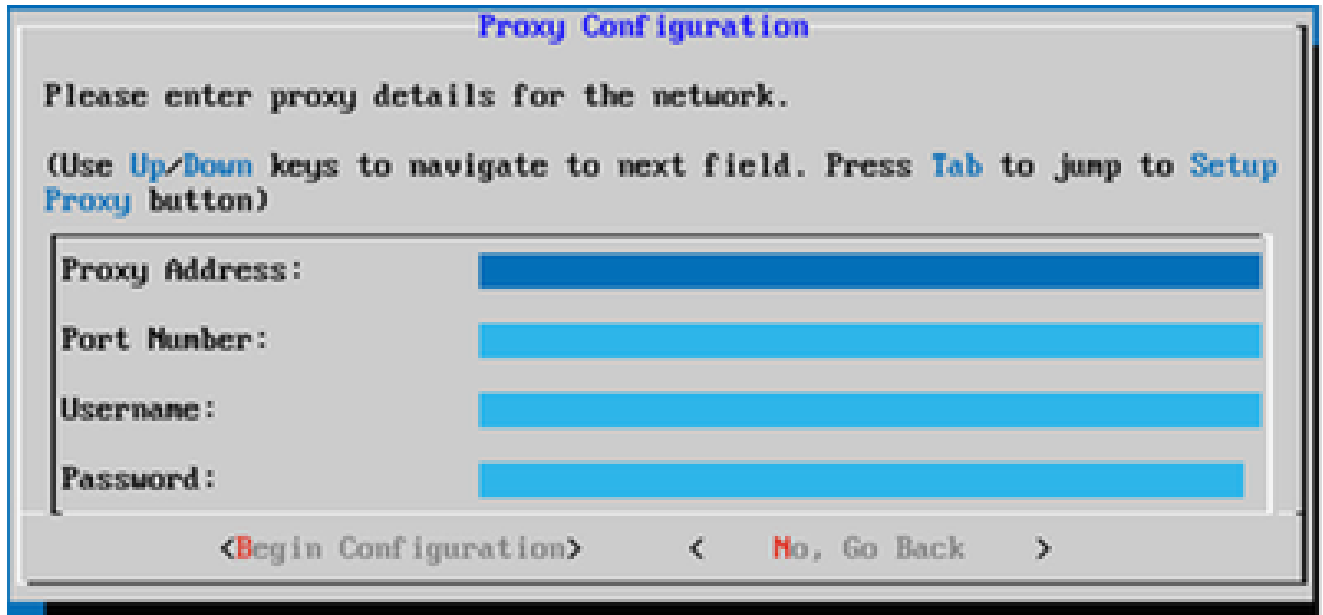
A terminal window titled "Proxy Set Up Confirmation" with a blue header bar. The text inside is as follows:

Do you want to add proxy details?

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

Configuración de proxy

8. Haga clic en Yes, Set Up Proxy para establecer los detalles del proxy o haga clic en No, Continue to Configuration para continuar directamente con el paso 11.

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

**Proxy Configuration**

Please enter proxy details for the network.

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

Proxy Address:

Port Number:

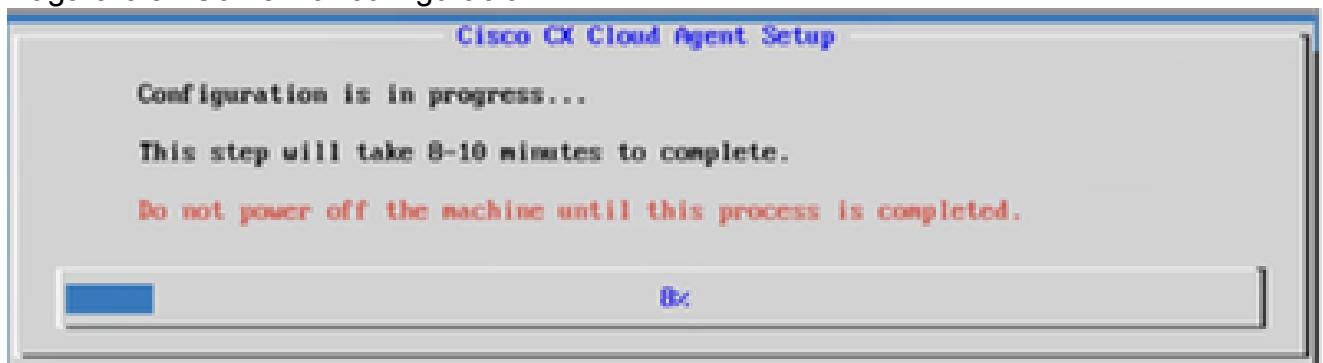
Username:

Password:

<Begin Configuration>      < No, Go Back >

Configuración de proxy

9. Ingrese la Dirección de Proxy, el Número de Puerto, el Nombre de Usuario y la Contraseña.
10. Haga clic en Comenzar configuración.

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

**Cisco CX Cloud Agent Setup**

Configuration is in progress...

This step will take 8-10 minutes to complete.

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

<Back>

Configuración del agente en la nube CX

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

**Cisco CX Cloud Agent Configuration**

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

<Continue>

Configuración del agente en la nube CX

11. Haga clic en Continue (Continuar).

## Cisco CX Cloud Agent Configuration

Following is the summary of CX Cloud Connectivity verification results.

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

### US:

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

### APJC:

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

### EMEA:

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

<Check Again>

< Continue >

La configuración continúa

12. Haga clic en Continue para continuar con la configuración para alcanzar el dominio exitosamente. La configuración puede tardar varios minutos en completarse.

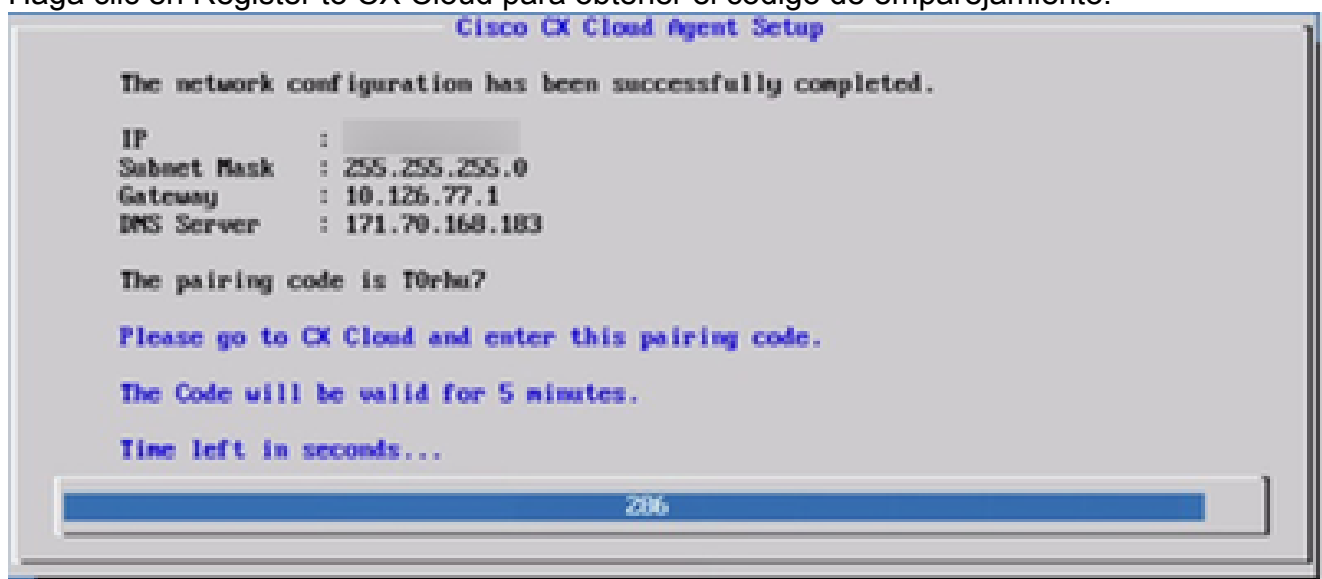


Nota: Si no se puede llegar a los dominios correctamente, el cliente debe solucionar el problema de disponibilidad de los dominios realizando cambios en su firewall para asegurarse de que se puede acceder a los dominios. Haga clic en Check Again una vez que se resuelva el problema de disponibilidad de dominios.



Inscríbase en CX Cloud

13. Haga clic en Register to CX Cloud para obtener el código de emparejamiento.



Código de vinculación

14. Copie el código de emparejamiento y vuelva a CX Cloud para continuar con la configuración.



Registro correcto



Nota: Si el código de emparejamiento caduca, haga clic en Register to CX Cloud para generar un nuevo código de emparejamiento (paso 13).

15. Haga clic en Aceptar.

## Enfoque alternativo para generar código de emparejamiento mediante CLI

Los usuarios también pueden generar un código de emparejamiento mediante las opciones de CLI.

Para generar un código de emparejamiento mediante CLI:

1. Inicie sesión en Cloud Agent mediante SSH con la credencial de usuario cxcadmin.
2. Genere el código de emparejamiento mediante el comando `cxcli agent generatePairingCode`.

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

Pairing Code : x3710P
Expires in: 5 minutes
Please use the Pairing Code in the CX Cloud to proceed with CX Cloud Agent registration.

cxcadmin@cxcloudagent:~$
```

Generar CLI de código de vinculación

3. Copie el código de emparejamiento y vuelva a CX Cloud para continuar con la configuración.

## Configuración de dispositivos para reenviar Syslog a CX Cloud Agent

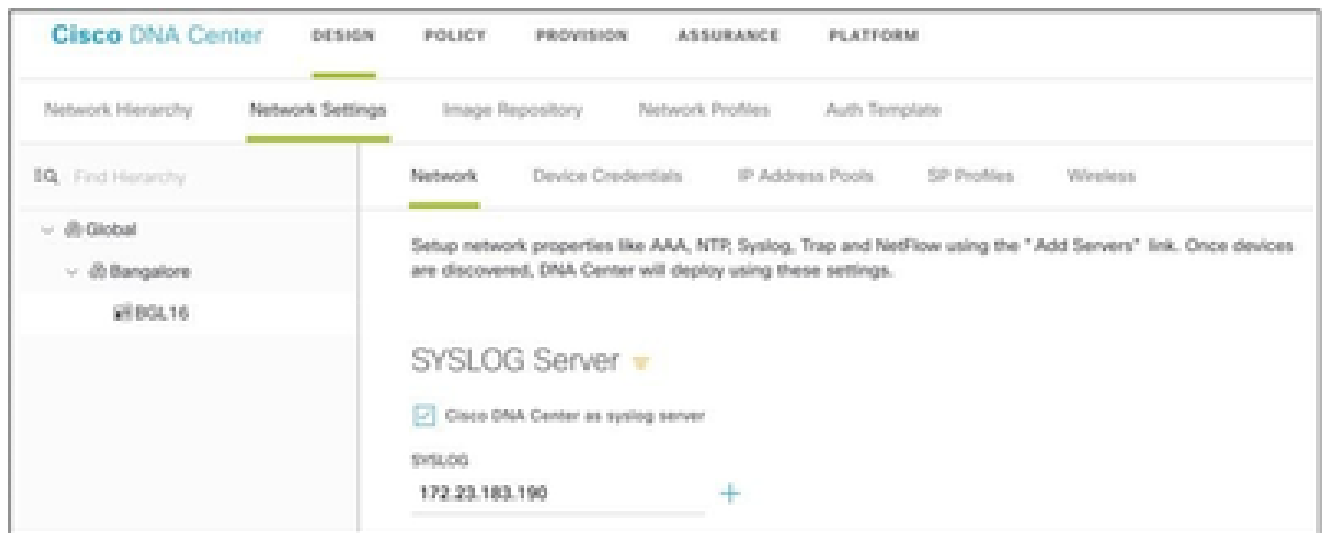
### Prerequisites

Las versiones compatibles de Cisco Catalyst Center son 2.1.2.0 a 2.2.3.5, 2.3.3.4 a 2.3.3.6, 2.3.5.0 y Cisco Catalyst Center Virtual Appliance

### Configurar la configuración de Syslog Forward

Para configurar el reenvío de Syslog al agente CX en Cisco Catalyst Center, siga estos pasos:

1. Inicie Cisco Catalyst Center.
2. Vaya a Diseño > Configuración de red > Red.
3. Para cada sitio, agregue la IP del agente CX como el servidor Syslog.



Servidor Syslog

 Nota: Una vez configurados, todos los dispositivos asociados con ese sitio se configuran para enviar syslog con nivel crítico al agente CX. Los dispositivos deben estar asociados a un sitio para habilitar el reenvío de syslog desde el dispositivo a CX Cloud Agent. Cuando se actualiza una configuración del servidor syslog, todos los dispositivos asociados a ese sitio se establecen automáticamente en el nivel crítico predeterminado.

## Configuración de otros recursos (recopilación directa de dispositivos) para reenviar el registro del sistema al agente CX

Los dispositivos deben configurarse para enviar mensajes de Syslog al agente CX para utilizar la función de gestión de fallos de CX Cloud.

 Nota: El agente CX solo informa de la información de registro del sistema de los recursos de Campus Success Track Level 2 a CX Cloud. Se impide que otros recursos tengan su registro del sistema configurado en el agente CX y no se informa de sus datos de registro del sistema en la nube CX.

### Servidores Syslog existentes con capacidad de reenvío

Realice las instrucciones de configuración para el software del servidor syslog y agregue la dirección IP del agente CX como nuevo destino.

 Nota: Cuando reenvíe registros del sistema, asegúrese de que se conserva la dirección IP de origen del mensaje original de registro del sistema.

### Servidores Syslog existentes sin capacidad de reenvío O sin servidor Syslog

Configure cada dispositivo para enviar registros del sistema directamente a la dirección IP del agente CX. Consulte esta documentación para conocer los pasos de configuración específicos.

[Guía de configuración de Cisco IOS® XE](#)

[Guía de configuración del controlador inalámbrico AireOS](#)

## Habilitación de la Configuración de Syslog de Nivel de Información para Cisco Catalyst Center

Para hacer visible el nivel de información de Syslog, siga estos pasos:

1. Vaya a Herramientas>Telemetría.



## TOOLS

Discovery

Inventory

Topology

Image Repository

Command Runner

License Manager

Template Editor

Telemetry

Data and Reports

2. Seleccione y expanda la Vista de sitio y seleccione un sitio de la jerarquía de sitios.



Vista del sitio

3. Seleccione el sitio necesario y seleccione todos los dispositivos mediante la casilla de verificación Device name.
4. Seleccione Visibilidad óptima en el menú desplegable Acciones.



Acciones

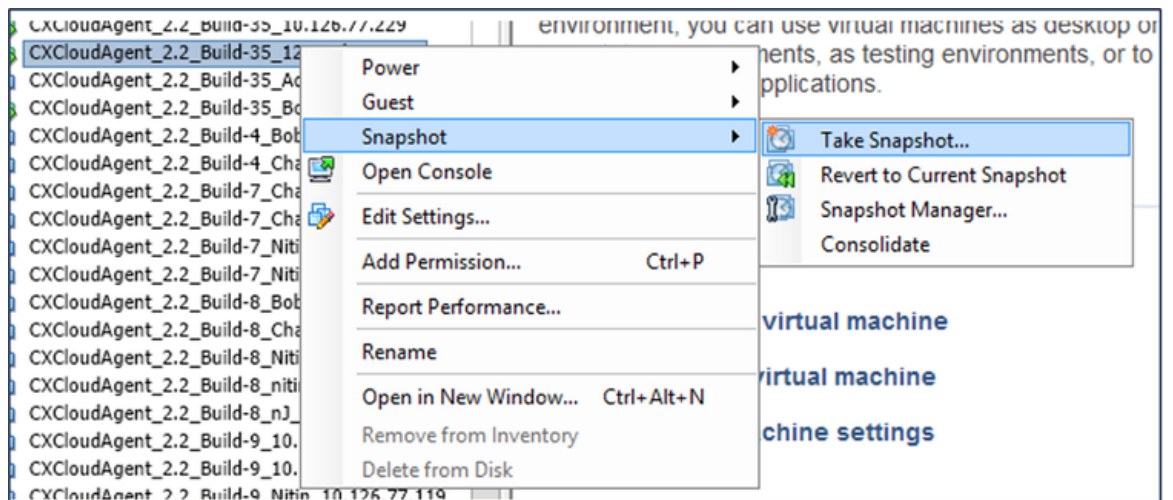
## Copia de seguridad y restauración de la VM en la nube CX

Se recomienda conservar el estado y los datos de una VM del agente CX en un momento específico mediante la función de instantánea. Esta función facilita la restauración de la VM en la nube de CX en el momento específico en que se realiza la instantánea.

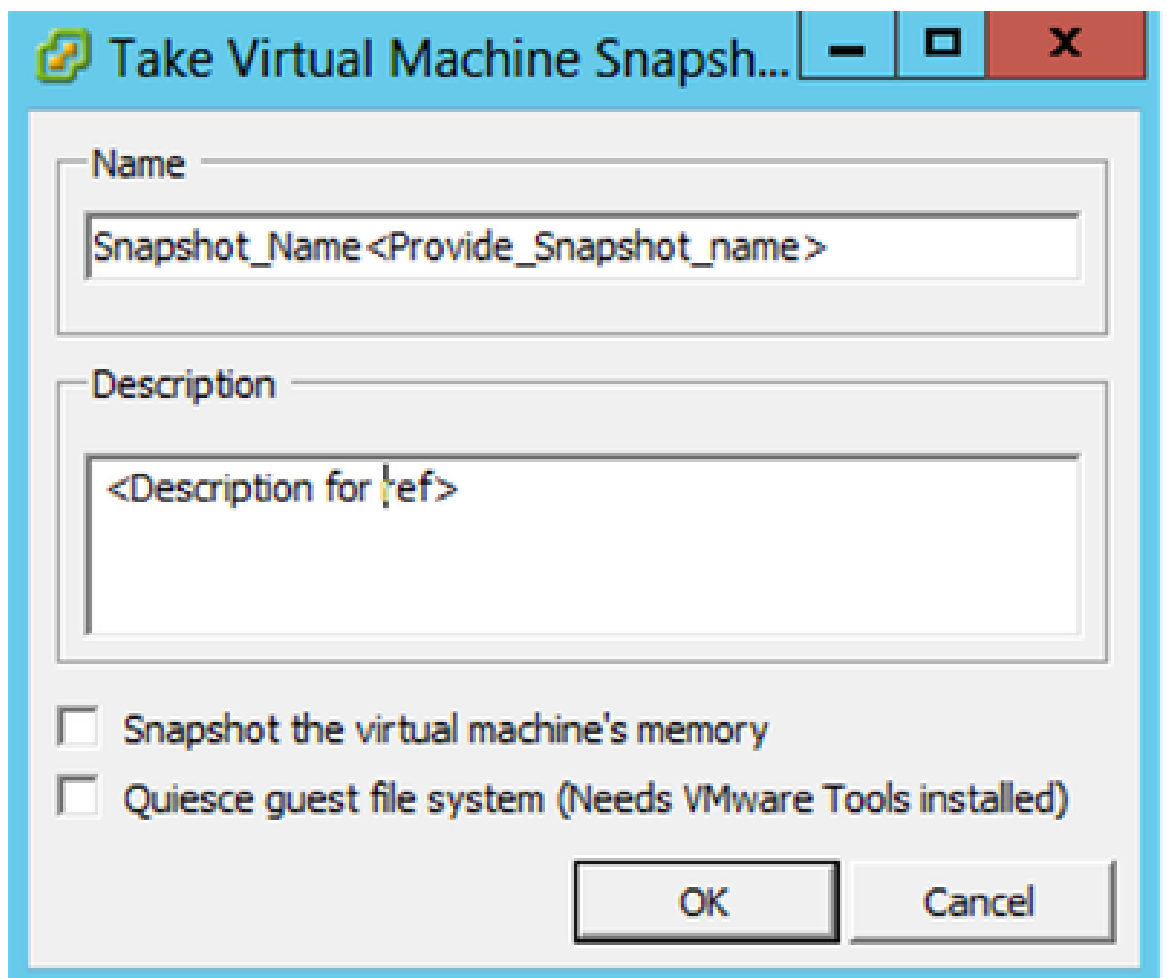
### Copia de seguridad de la VM en nube CX

Para realizar una copia de seguridad de la VM en la nube CX:

1. Haga clic con el botón derecho en la VM y seleccione Snapshot > Take Snapshot. Se abre la ventana Take Virtual Machine Snapshot.



Seleccionar VM

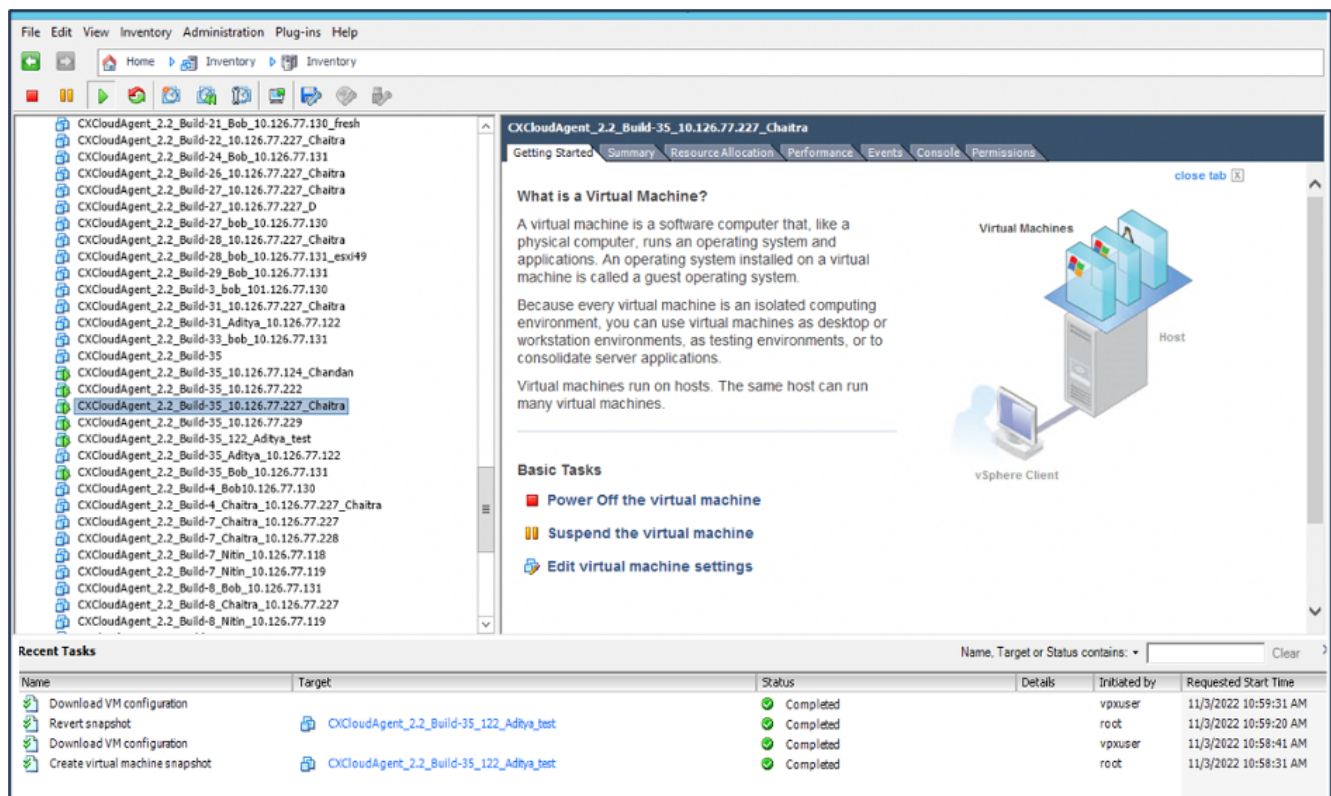


Tomar instantánea de máquina virtual

2. Ingrese Name y Description.

 Nota: Compruebe que la casilla de verificación Instantánea de la memoria de la máquina virtual está desactivada.

3. Haga clic en Aceptar. El estado Crear instantánea de máquina virtual se muestra como Completado en la lista Tareas recientes.

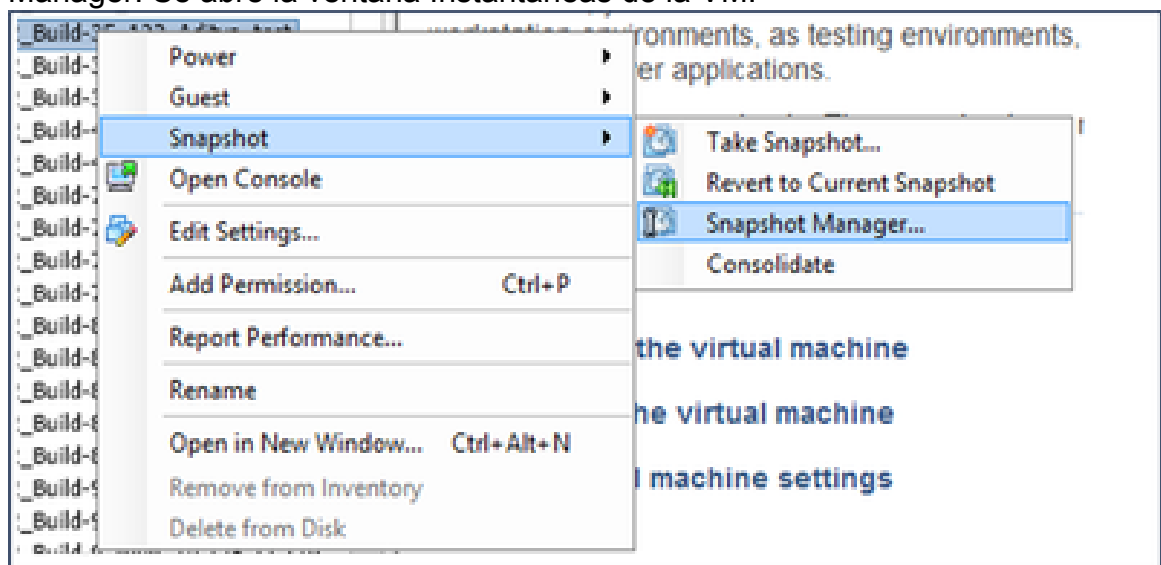


Tareas recientes

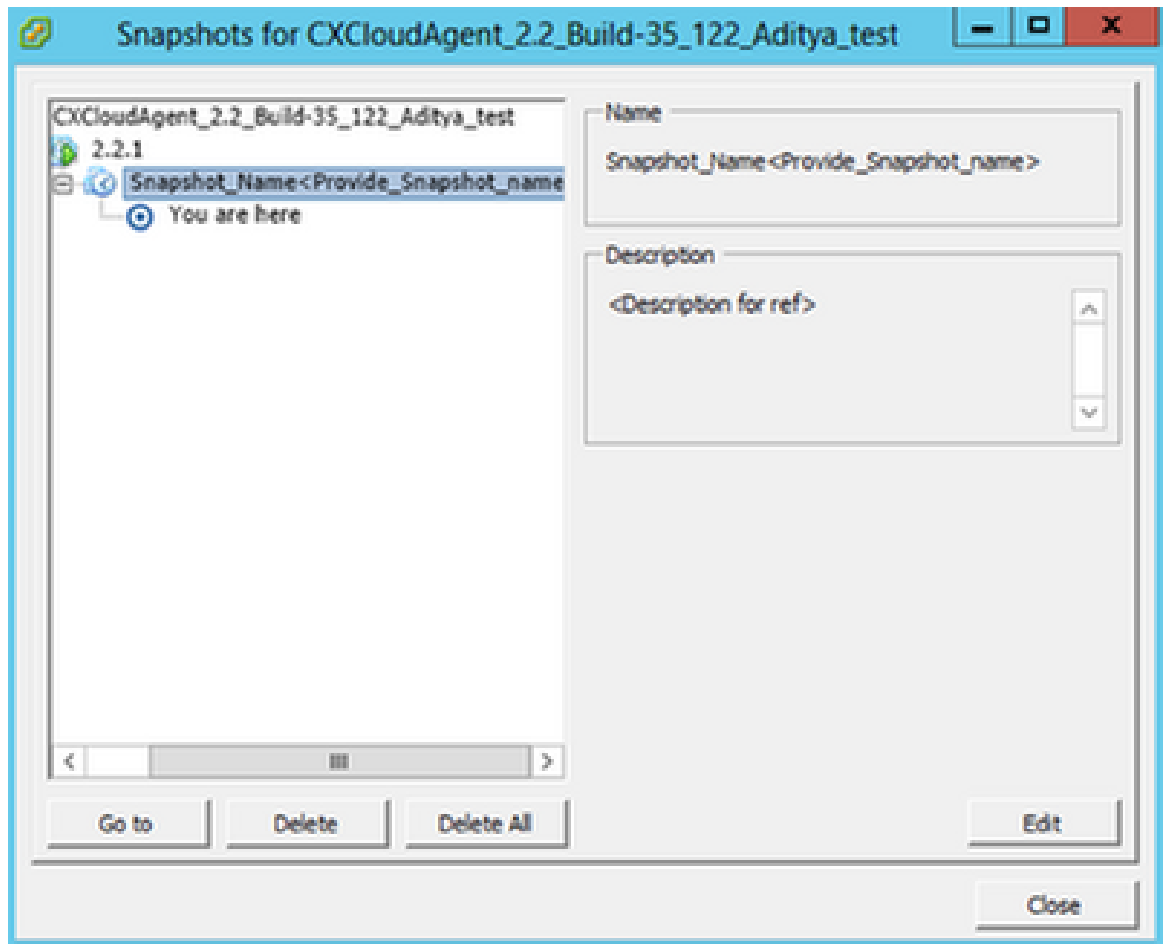
## Restauración de la VM en la nube CX

Para restaurar la VM en la nube de CX:

1. Haga clic con el botón derecho en la VM y seleccione Snapshot > Snapshot Manager. Se abre la ventana Instantáneas de la VM.

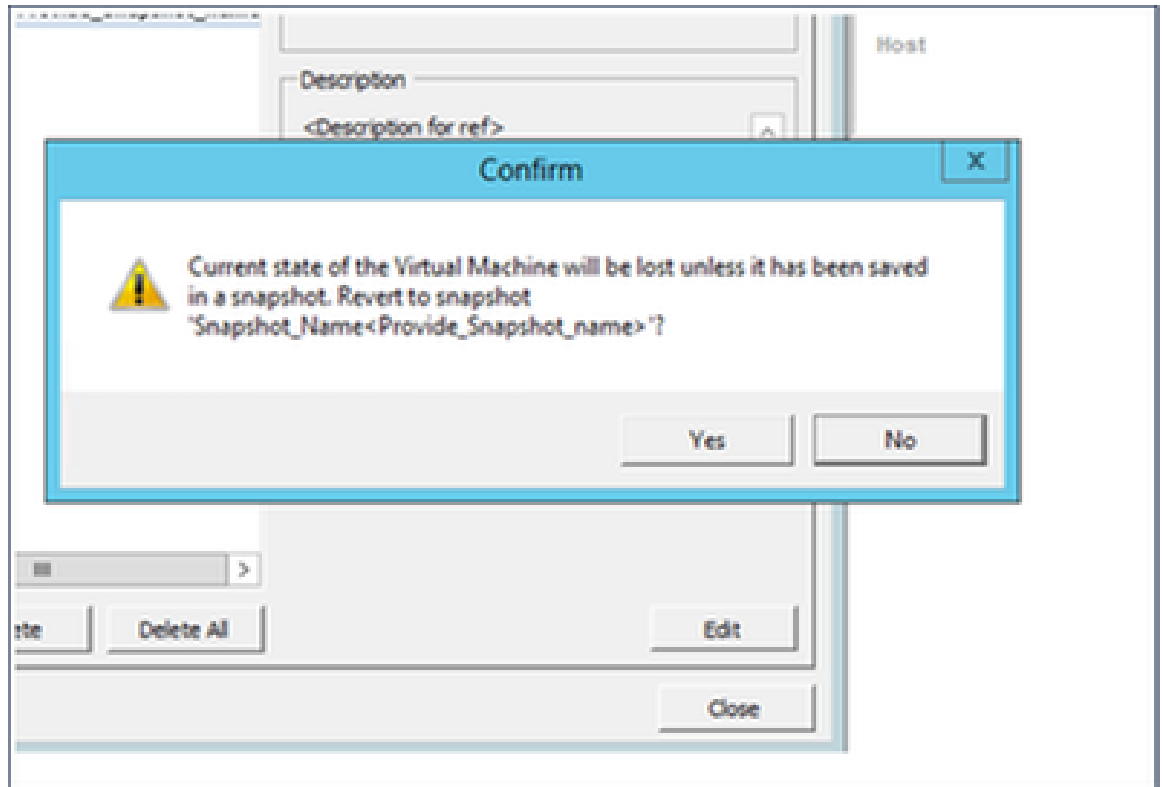


Ventana Seleccionar VM



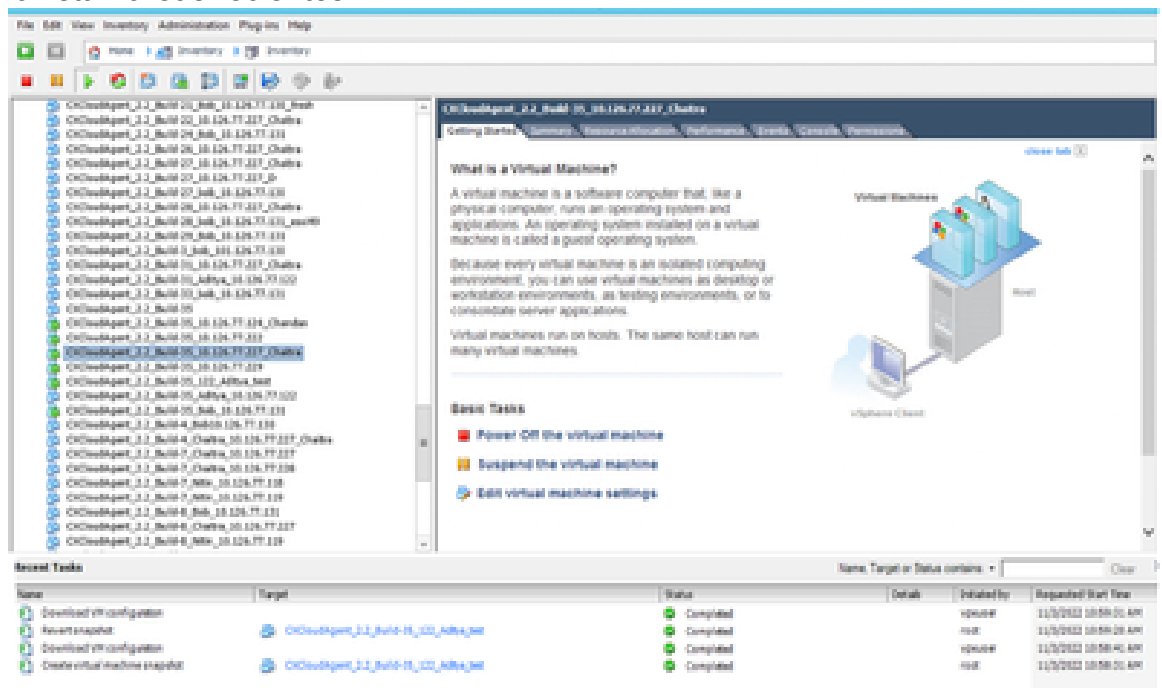
Ventana Instantáneas

2. Haga clic en Ir a. Se abrirá la ventana Confirm.



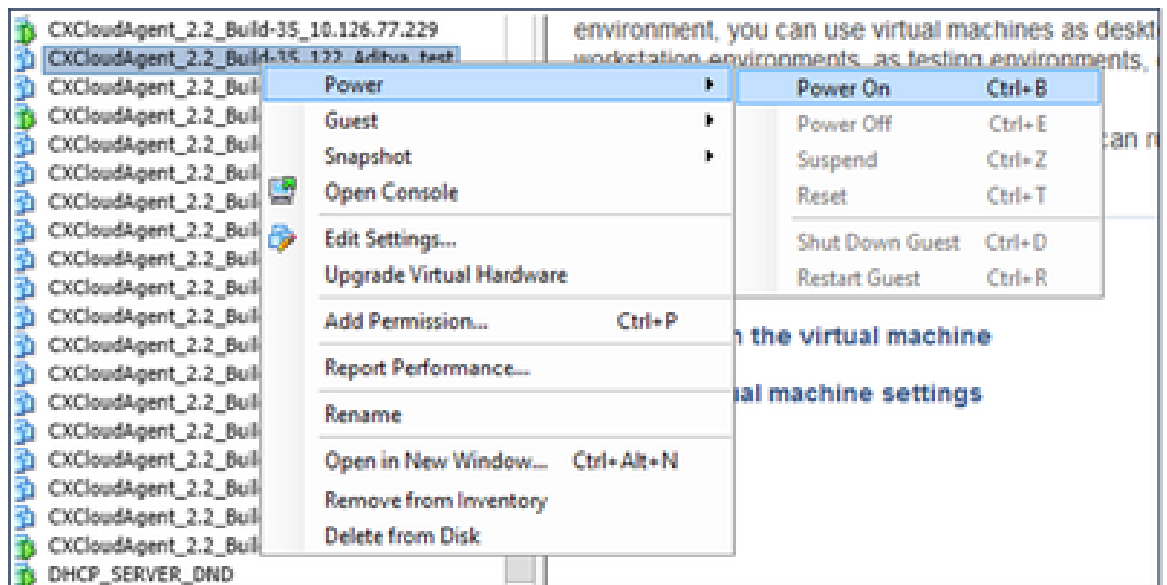
Confirmar ventana

- Haga clic en Sí El estado Revertir instantánea se muestra como Completado en la lista Tareas recientes.



Tareas recientes

- Haga clic con el botón derecho del ratón en la VM y seleccione Power > Power On para encender la VM.



## Security

El agente CX garantiza al cliente una seguridad integral. La conexión entre la nube CX y el agente CX está protegida mediante TLS. El usuario SSH predeterminado del Cloud Agent está limitado a realizar solo operaciones básicas.

### Seguridad Física

Implemente la imagen OVA del agente CX en una empresa de servidor VMware segura. El OVA se comparte de forma segura a través del centro de descargas de software de Cisco. La contraseña del cargador de arranque (modo de usuario único) se establece con una contraseña aleatoria única. Los usuarios deben consultar esta [FAQ](#) para configurar esta contraseña del cargador de arranque (modo de usuario único).

### Seguridad de cuentas

Durante la implementación, se crea la cuenta de usuario cxcadmin. Los usuarios se ven obligados a establecer una contraseña durante la configuración inicial. cxcadmin user/credentials se utilizan para acceder a las API del agente CX y para conectarse al dispositivo a través de SSH.

los usuarios de cxcadmin tienen acceso restringido con los menos privilegios. La contraseña cxcadmin sigue la política de seguridad y se trocea unidireccionalmente con un período de caducidad de 90 días. los usuarios de cxcadmin pueden crear un usuario de cxcroot mediante la utilidad denominada remoteaccount. los usuarios de cxcroot pueden obtener privilegios de root.

### Seguridad de redes:

Se puede acceder a la máquina virtual del agente CX mediante SSH con credenciales de usuario cxcadmin. Los puertos entrantes están restringidos a 22 (SSH), 514 (Syslog).

### Autenticación

Autenticación basada en contraseña: El dispositivo mantiene un único usuario (cxcadmin) que le permite autenticarse y comunicarse con el agente CX.

- Acciones privilegiadas de raíz en el dispositivo mediante SSH.

los usuarios de cxcadmin pueden crear un usuario de cxcroot mediante una utilidad denominada remoteaccount. Esta utilidad muestra una contraseña cifrada RSA/ECB/PKCS1v1\_5 que sólo se puede descifrar desde el portal SWIM ([Formulario de solicitud de descifrado](#)). Solo el personal autorizado tiene acceso a este portal. los usuarios de cxcroot pueden obtener privilegios de root con esta contraseña descifrada. La frase de paso sólo es válida durante dos días. Los usuarios de cxcadmin deben volver a crear la cuenta y obtener la contraseña del portal SWIM después de que caduque la contraseña.

## Endurecimiento

El dispositivo Agente CX sigue los estándares de endurecimiento del Centro de seguridad de Internet.

## Seguridad de datos

El dispositivo Agente CX no almacena ninguna información personal del cliente. La aplicación de credenciales del dispositivo (que se ejecuta como uno de los grupos de dispositivos) almacena las credenciales cifradas del servidor dentro de una base de datos segura. Los datos recopilados no se almacenan de ninguna forma dentro del dispositivo, excepto temporalmente cuando se procesan. Los datos de telemetría se cargan en CX Cloud tan pronto como sea posible después de que se haya completado la recopilación y se eliminan rápidamente del almacenamiento local después de que se confirme que la carga se ha realizado correctamente.

## Transmisión de datos

El paquete de registro contiene el certificado de dispositivo [X.509](#) y las claves únicas necesarias para establecer una conexión segura con IoT Core. El uso de ese agente establece una conexión segura mediante Message Queue Server Telemetry Transport (MQTT) sobre Transport Layer Security (TLS) v1.2

## Registros y supervisión

Los registros no contienen ningún tipo de información personal identificable (PII). Los registros de auditoría capturan todas las acciones sensibles a la seguridad realizadas en el dispositivo CX Cloud Agent.

## Comandos de telemetría de Cisco

CX Cloud recupera la telemetría de recursos mediante las API y los comandos enumerados en los [comandos de telemetría de Cisco](#). Este documento clasifica los comandos en función de su aplicabilidad al inventario de Cisco Catalyst Center, Diagnostic Bridge, Intersight, Compliance Insights, Faults y todas las demás fuentes de telemetría recopiladas por el agente CX.

La información confidencial de la telemetría de activos se oculta antes de transmitirse a la nube. El agente CX enmascara los datos confidenciales de todos los recursos recopilados que envían telemetría directamente al agente CX. Esto incluye contraseñas, claves, cadenas de comunidad, nombres de usuario, etc. Los controladores proporcionan enmascaramiento de datos para todos los recursos gestionados por el controlador antes de transferir esta información al agente CX. En algunos casos, la telemetría de los recursos gestionados por el controlador puede seguir anonimizándose. Consulte la [documentación de soporte del producto](#) correspondiente para obtener más información sobre el anonimato de la telemetría (por ejemplo, la sección [Anonimizar datos](#) de la Guía del administrador de Cisco Catalyst Center).

Aunque la lista de comandos de telemetría no se puede personalizar y las reglas de enmascaramiento de datos no se pueden modificar, los clientes pueden controlar los accesos a la nube de CX de telemetría de los activos especificando los orígenes de datos como se describe en la [documentación de soporte del producto](#) para dispositivos gestionados por el controlador o en la sección Conexión de orígenes de datos de este documento (para Otros recursos recopilados por el agente CX).

## Resumen de seguridad

| Funciones de seguridad              | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Contraseña del cargador de arranque | La contraseña del cargador de arranque (modo de usuario único) se establece con una contraseña aleatoria única. Los usuarios deben consultar <a href="#">FAQ</a> para establecer su contraseña de cargador de arranque (modo de usuario único).                                                                                                                                                                                                           |
| Acceso de usuario                   | SSH: <ul style="list-style-type: none"><li>· El acceso al dispositivo mediante el usuario cxcadmin requiere la creación de credenciales durante la instalación.</li><li>· El acceso al dispositivo mediante el usuario cxcroot requiere que el personal autorizado descifre las credenciales mediante el portal SWIM.</li></ul>                                                                                                                           |
| Cuentas de usuario                  | cxcadmin: cuenta de usuario predeterminada creada; El usuario puede ejecutar los comandos de la aplicación Agente CX utilizando cxcli y tiene menos privilegios en el dispositivo; cxcroot user y su contraseña cifrada se generan mediante cxcadmin user. <ul style="list-style-type: none"><li>· cxcroot: cxcadmin puede crear este usuario mediante la utilidad remoteaccount; El usuario puede obtener privilegios de root con esta cuenta.</li></ul> |
| cxcadmin                            | <ul style="list-style-type: none"><li>· La contraseña es unidireccional con SHA-256 y se almacena de forma</li></ul>                                                                                                                                                                                                                                                                                                                                      |

|                           |                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| password policy           | <p>segura.</p> <ul style="list-style-type: none"> <li>· Un mínimo de ocho (8) caracteres, que contengan tres de estas categorías: mayúsculas, minúsculas, números y caracteres especiales.</li> </ul>                                                                                                             |
| cxcroot password policy   | <ul style="list-style-type: none"> <li>· la contraseña cxcroot está encriptada RSA/ECB/PKCS1v1_5</li> <li>· La frase de contraseña generada debe descifrarse en el portal SWIM.</li> <li>· El usuario cxcroot y la contraseña son válidos durante dos días y se pueden regenerar usando cxcadmin user.</li> </ul> |
| ssh login password policy | <ul style="list-style-type: none"> <li>· Un mínimo de ocho caracteres que contenga tres de estas categorías: mayúsculas, minúsculas, números y caracteres especiales.</li> <li>· Cinco intentos fallidos de inicio de sesión bloquean la caja durante 30 minutos; La contraseña caduca en 90 días.</li> </ul>     |
| Puertos                   | Puertos entrantes abiertos: 514 (Syslog) y 22 (SSH)                                                                                                                                                                                                                                                               |
| Seguridad de datos        | <ul style="list-style-type: none"> <li>· No se almacena información del cliente.</li> <li>· No se almacenan datos del Equipo.</li> <li>· Credenciales de servidor de Cisco Catalyst Center cifradas y almacenadas en la base de datos.</li> </ul>                                                                 |

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).