Descripción general de CX Cloud Agent v2.2

Contenido

Introducción

Este documento describe Cisco Customer Experience (CX) Cloud Agent.

Prerequisites

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

Requirements

Requisitos para la implementación:

- Cualquiera de estos hipervisores:
  - VMware ESXi versión 5.5 o posterior
  - Oracle Virtual Box 5.2.30 o posterior
  - Hipervisor de Windows versión 2012 a 2022
- El hipervisor puede alojar una VM que requiere:
  - CPU de 8 núcleos
  - 16 GB de memoria/RAM
  - 200 GB de espacio en disco
- 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 en la nube 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.csco.cloud
  - FQDN: ng.acs.agent.us.csco.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 en la nube de CX: el agente en la nube de CX debe poder

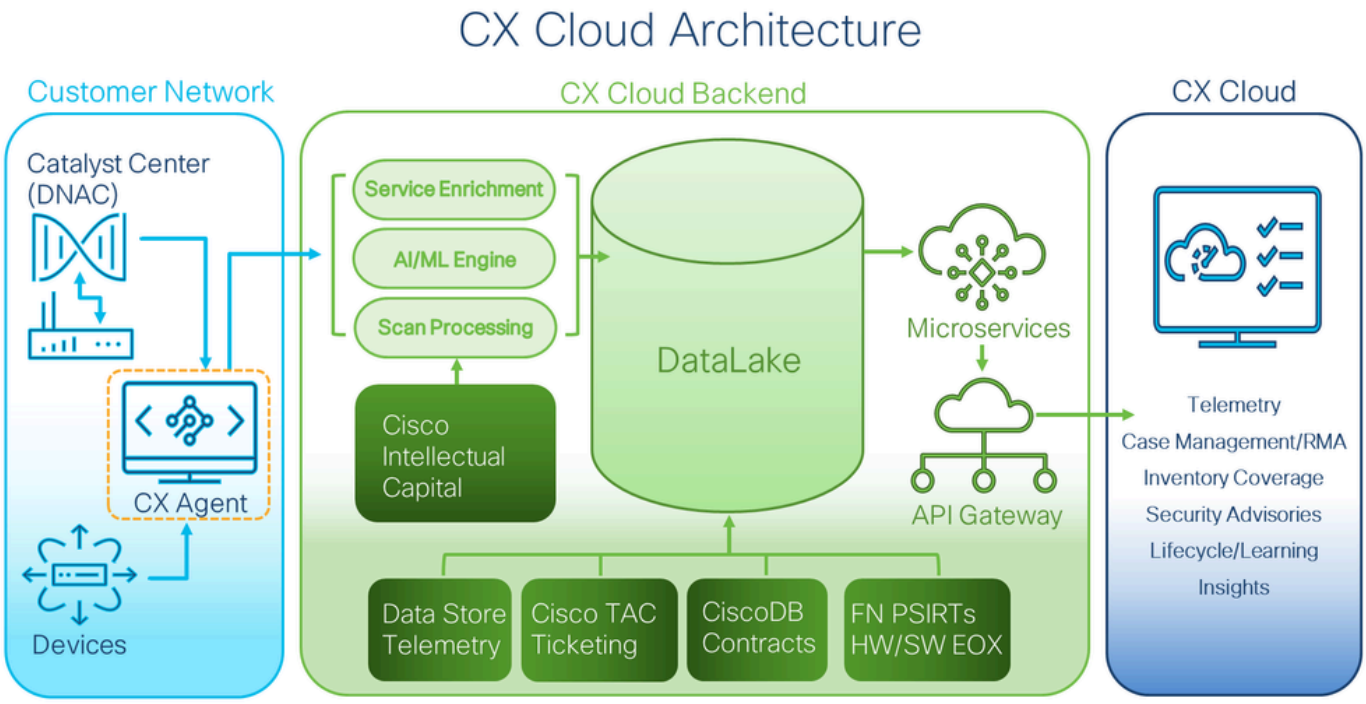
conectarse a los dos servidores que se muestran aquí, mediante el FQDN y el uso de HTTPS en el puerto TCP 443:
    - FQDN: agent.us.csco.cloud
    - FQDN: agente.emea.cisco.cloud
    - FQDN: ng.acs.agent.emea.cisco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Para los clientes que utilizan Data Centers de Asia Pacífico designados como la región de datos principal para almacenar datos de la nube CX: el agente de nube CX debe poder conectarse a ambos servidores que se muestran aquí, mediante el FQDN y el uso de HTTPS en el puerto TCP 443:
    - FQDN: agent.us.csco.cloud
    - FQDN: agent.apjc.cisco.cloud
    - FQDN: ng.acs.agent.apjc.cisco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Para los clientes que utilizan Data Centers designados de Europa y Asia-Pacífico como su región de datos principal, la conectividad a FQDN: agent.us.csco.cloud solo es necesaria para registrar el agente de nube 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.
- Esta tabla proporciona un resumen de los puertos y protocolos que deben abrirse y activarse para que CX Cloud Agent funcione correctamente:

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

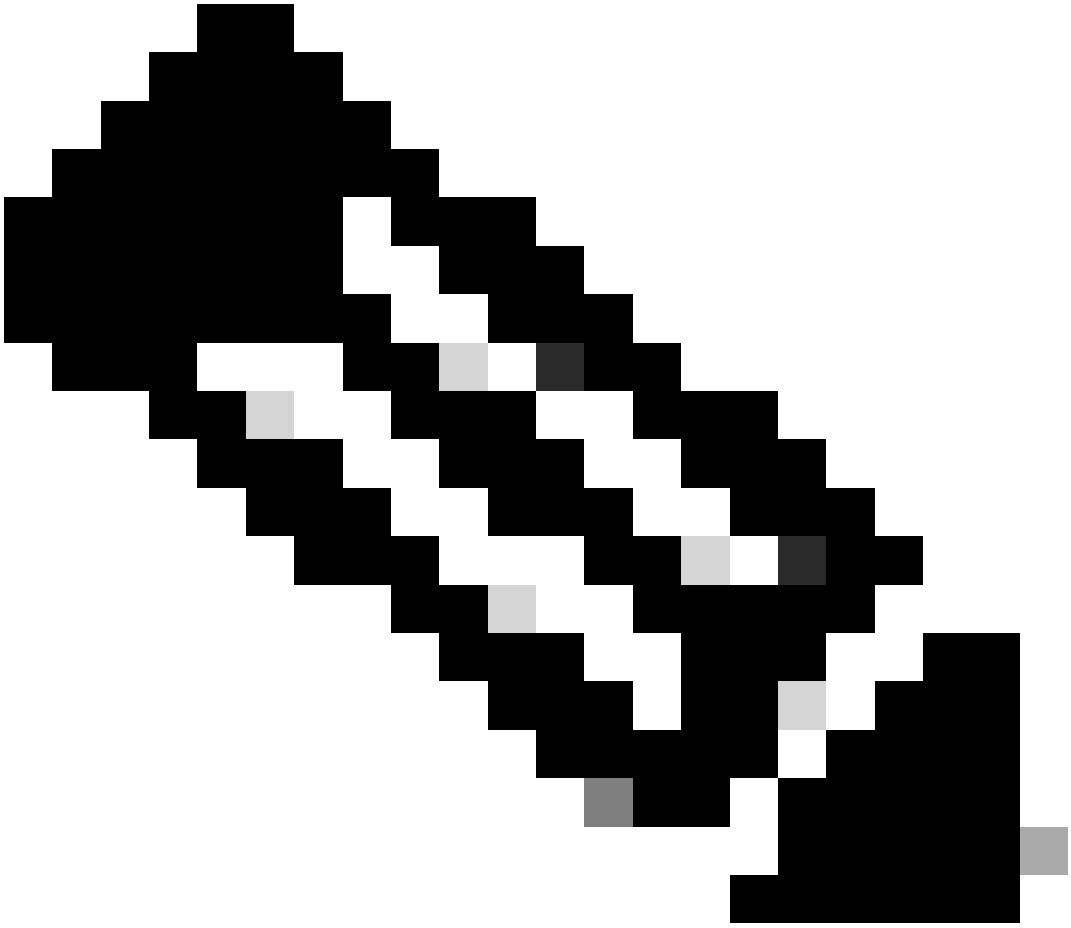
Antecedentes

El agente en la nube de Cisco (CX) es una plataforma muy escalable que recopila datos de telemetría de los dispositivos de red del cliente para ofrecer información práctica a los clientes. CX Cloud 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.

Esta guía es específica para CX Cloud Agent v2.2 y versiones posteriores. Consulte la página Cisco CX Cloud Agent para acceder a las versiones anteriores.



Arquitectura de nube CX



Nota: las imágenes (y el contenido de la misma) de esta guía se ofrecen únicamente a modo de referencia. El contenido real puede variar.

- Una dirección IP se detecta automáticamente si el protocolo de configuración dinámica de host (DHCP) está activado en el entorno de máquina virtual; 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 nodo único y clúster de alta disponibilidad (HA) de Cisco DNA Center son las 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x y el dispositivo virtual Cisco Catalyst Center Virtual Appliance y el dispositivo virtual Cisco DNA Center.
- Si la red cuenta con interceptación SSL, introduzca en la lista de permisos la dirección IP del agente en la nube CX.
- 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 estos dominios. Utilice sólo los nombres de host proporcionados; no utilice direcciones IP estáticas.

Dominios específicos del portal CX Cloud Agent

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

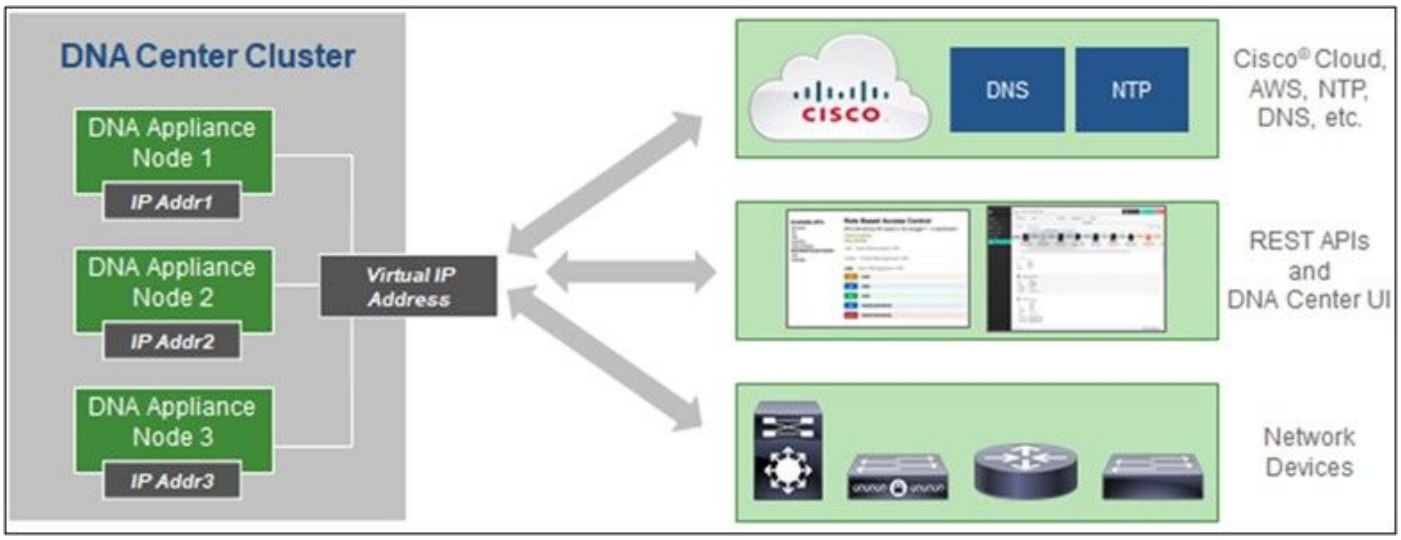
Dominios específicos de OVA de CX Cloud Agent

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.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.cisco.cloud	agent.apjc.cisco.cloud
	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

Nota: El acceso saliente debe estar permitido con la redirección habilitada en el puerto 443 para el FQDN especificado.

Versión admitida de Cisco DNA Center

Las versiones de Cisco DNA Center de un solo nodo y clúster HA compatibles son 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x y Cisco Catalyst Center Virtual Appliance y Cisco DNA 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

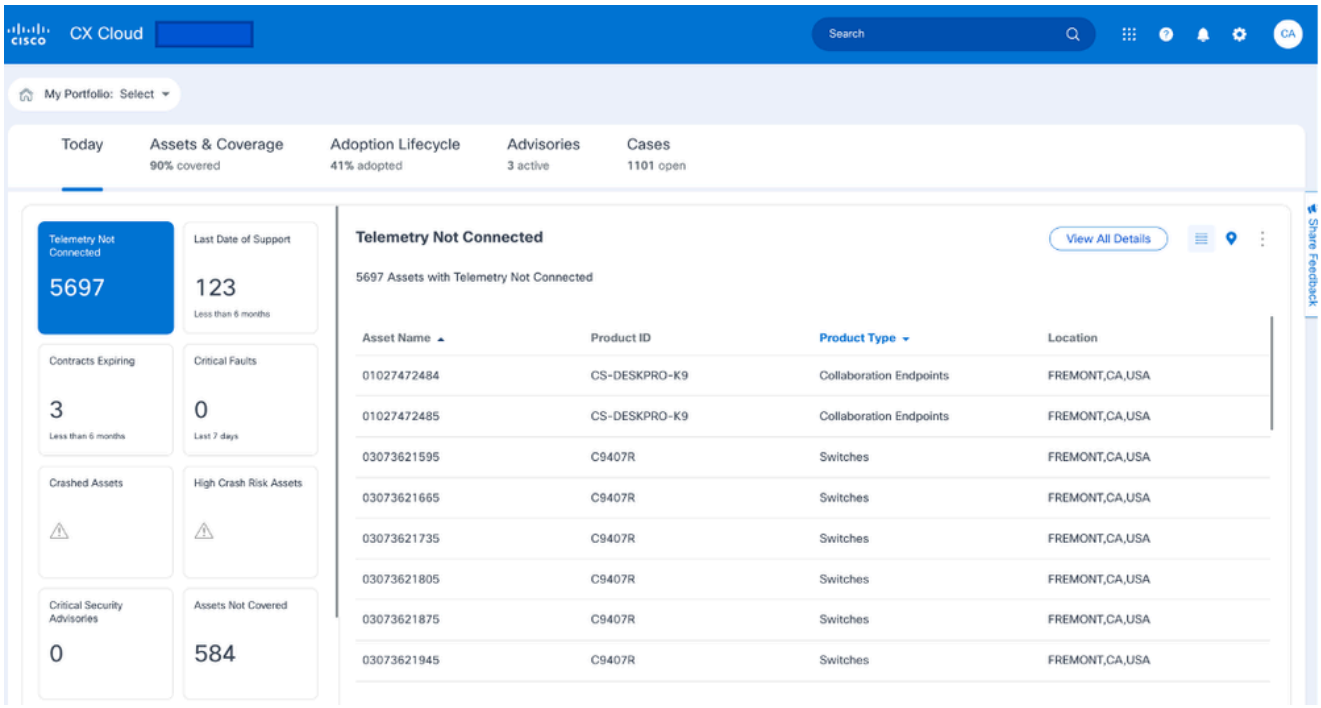
Lista de productos admitidos

Para ver la lista de productos admitidos por CX Cloud Agent, consulte la Lista de productos admitidos.

Conexión de orígenes de datos

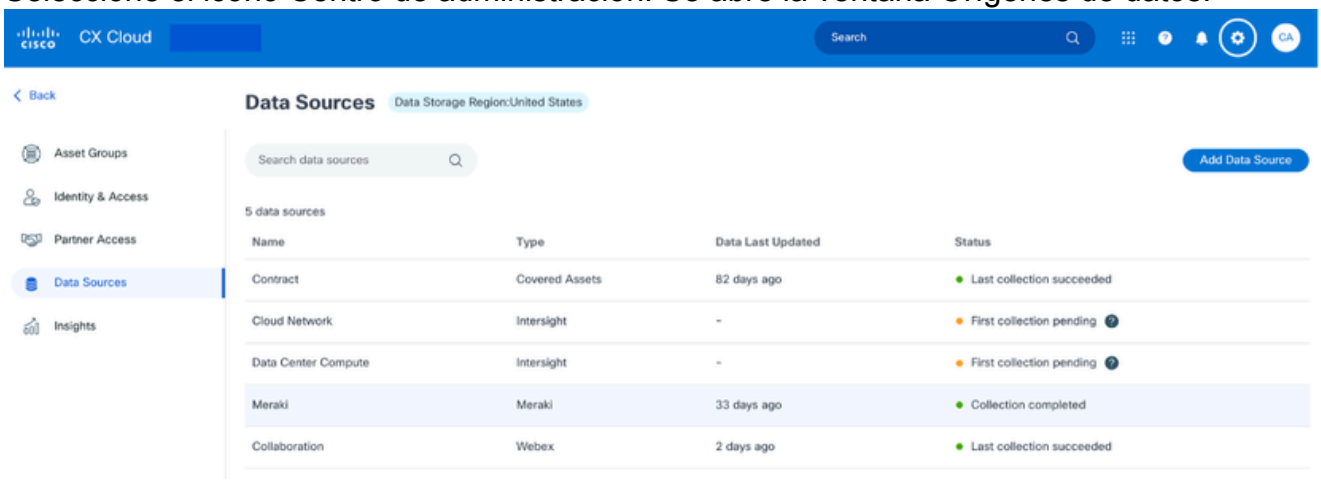
Para conectar orígenes de datos:

1. Haga clic en cx.cisco.com para iniciar sesión en CX Cloud.



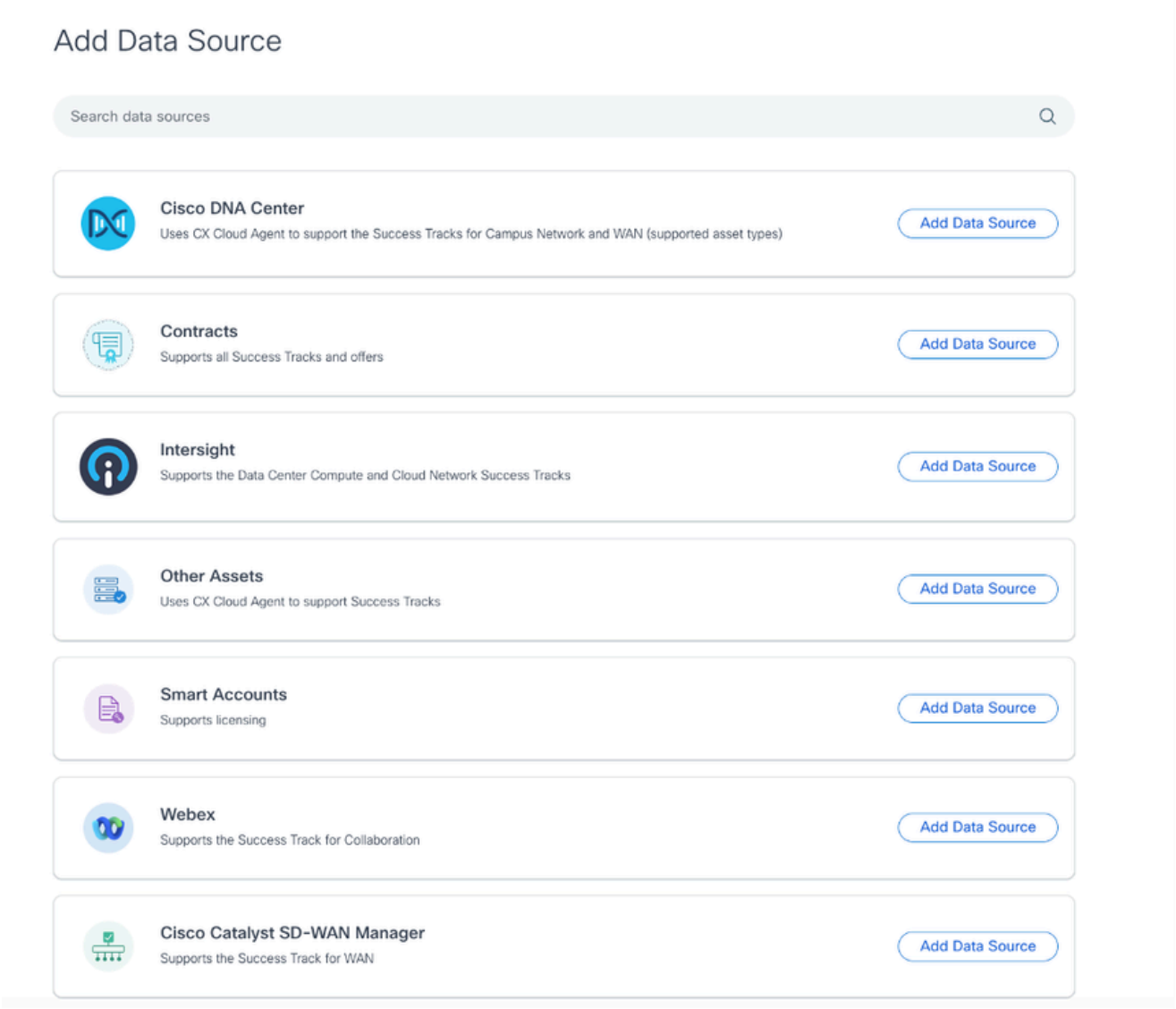
Página de inicio de CX Cloud

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



Orígenes de datos

3. Haga clic en Agregar origen de datos. Se abre la ventana Agregar origen de datos. Las opciones mostradas pueden variar en función de las suscripciones del cliente.



Agregar origen de datos

4. Haga clic en Agregar origen de datos para seleccionar el origen de datos aplicable. Si el agente en la nube de CX no se ha configurado previamente, se abrirá la ventana Configuración del agente en la nube de CX, donde debe completarse la configuración. Si la configuración ha finalizado, la conexión continúa. Consulte una de estas secciones para continuar:

Configuración de CX Cloud Agent

Adición de Cisco DNA Center como origen de datos

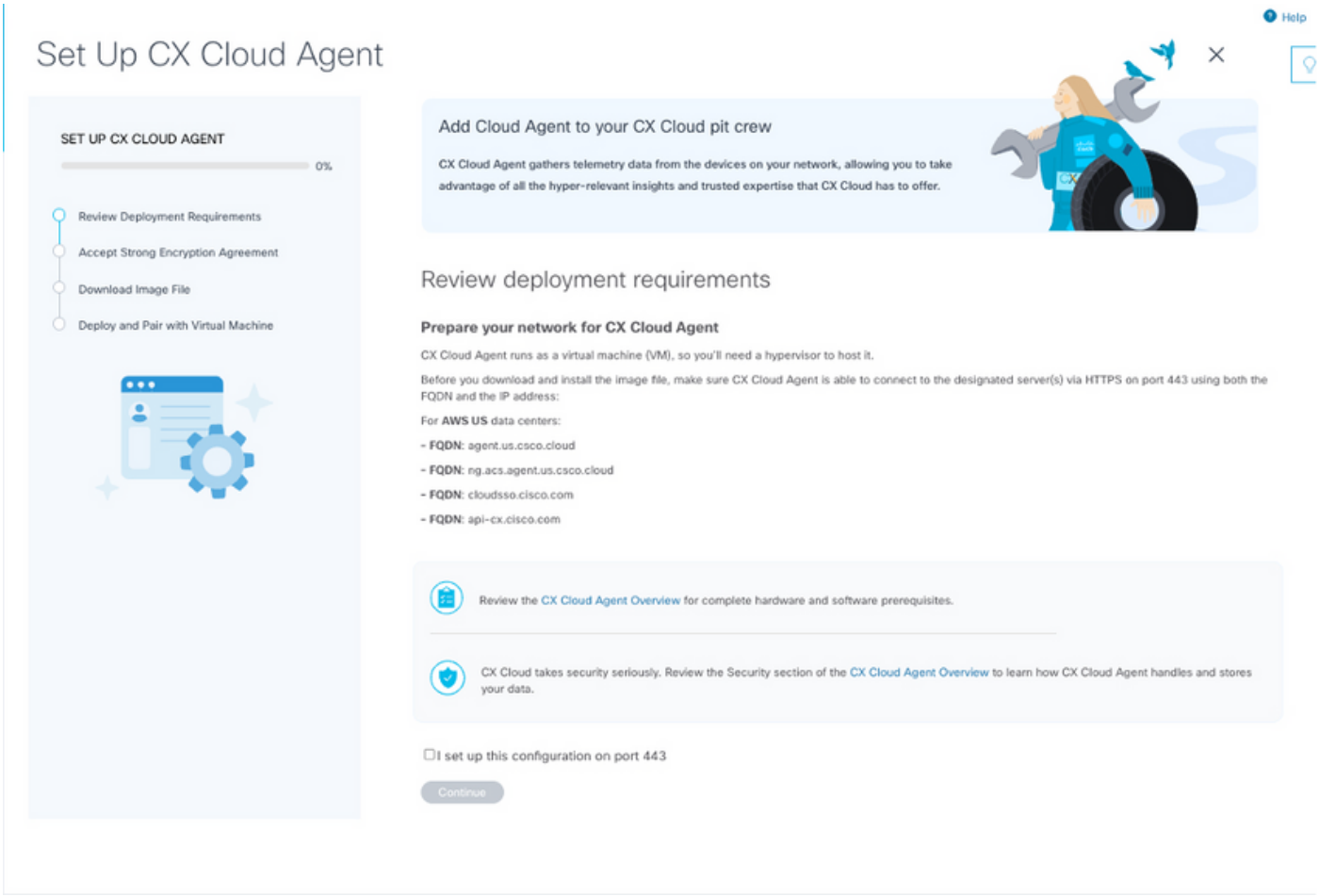
Adición de otros recursos como orígenes de datos

Nota: La opción Otros activos sólo está disponible si la conectividad de dispositivo directo no se ha configurado previamente.

Configuración de CX Cloud Agent

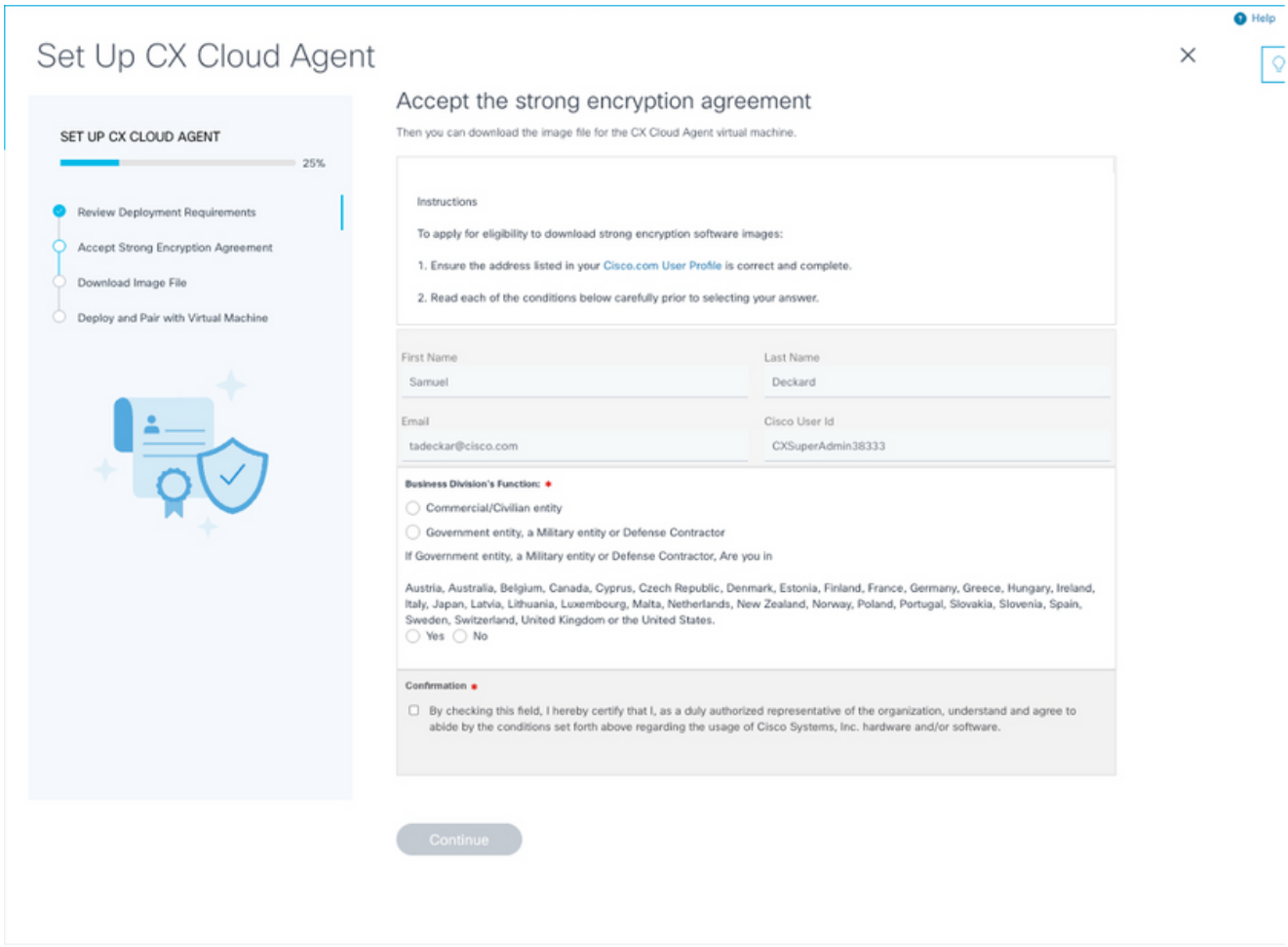
La configuración del agente en la nube de CX se solicita al conectar orígenes de datos si no se ha completado previamente.

Para configurar CX Cloud Agent:



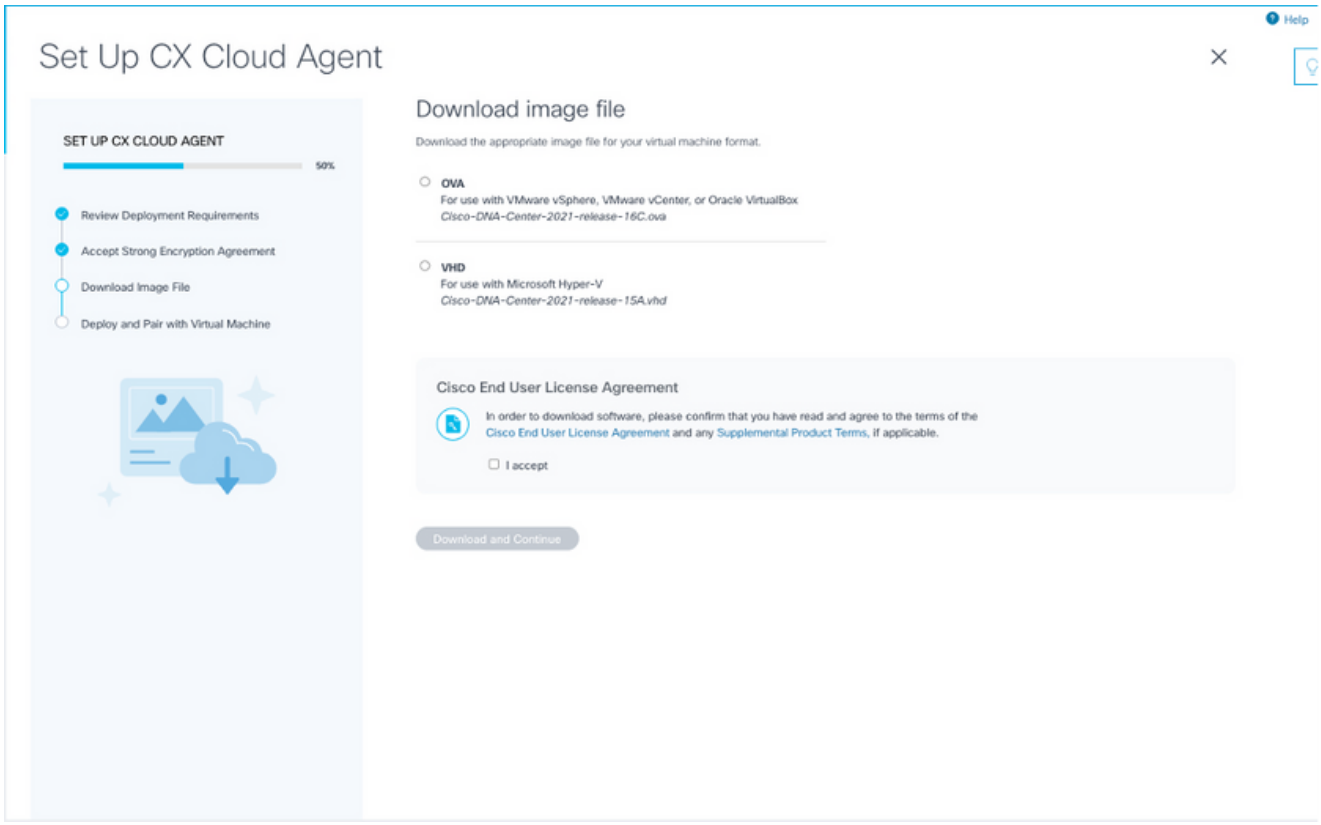
Revisar requisitos de implementación

1. Revise los requisitos de implementación de revisión y active la casilla de verificación I set up this configuration on port 443.
2. Haga clic en Continue (Continuar). Se abre la ventana Set Up CX Cloud Agent - Accept (Configuración del agente en la nube de CX).



Acuerdo de cifrado

3. Verifique la información que se ha introducido previamente en los campos First Name, Last Name, E-mail y Cisco User Id.
4. Seleccione la función de la división empresarial adecuada.
5. Seleccione la casilla de verificación Confirmación para aceptar las condiciones de uso.
6. Haga clic en Continue (Continuar). Se abre la ventana Set Up CX Cloud Agent - Download image file.



Descargar imagen

7. Seleccione el formato de archivo adecuado para descargar el archivo de imagen necesario para la instalación.
8. Seleccione la casilla de verificación I accept para aceptar el Acuerdo de licencia del usuario final de Cisco.
9. Haga clic en Descargar y continuar. Se abre la ventana Set Up CX Cloud Agent - Deploy and pair with your virtual machine .
10. Consulte Configuración de red para obtener el código de emparejamiento requerido en la siguiente sección.

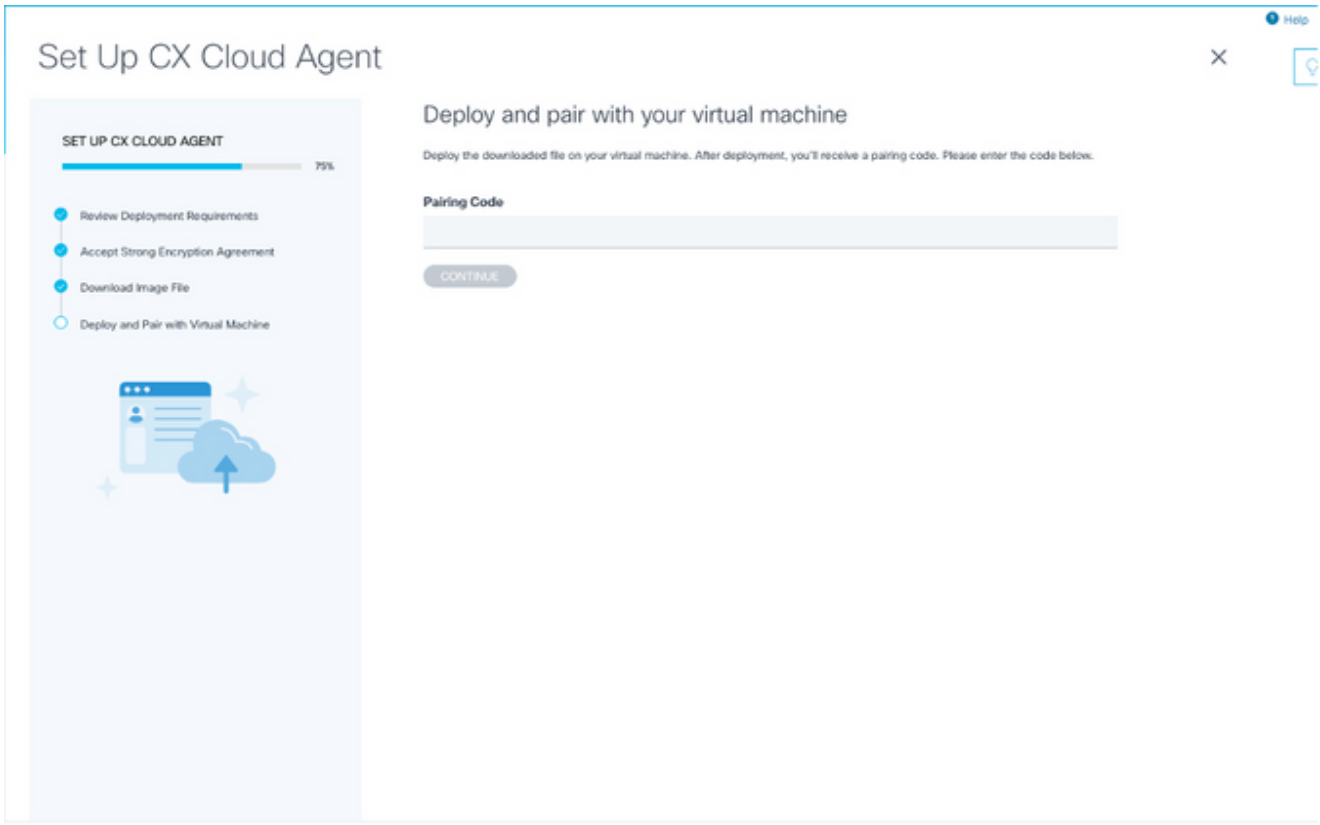
Conexión de CX Cloud Agent a CX Cloud

Es necesario conectar CX Cloud Agent a CX Cloud para que comience la recopilación de telemetría, de modo que la información de la interfaz de usuario se pueda actualizar para mostrar los recursos y la información actuales. En esta sección se proporcionan detalles para completar las directrices de conexión y solución de problemas.

Para conectar CX Cloud Agent a CX Cloud:

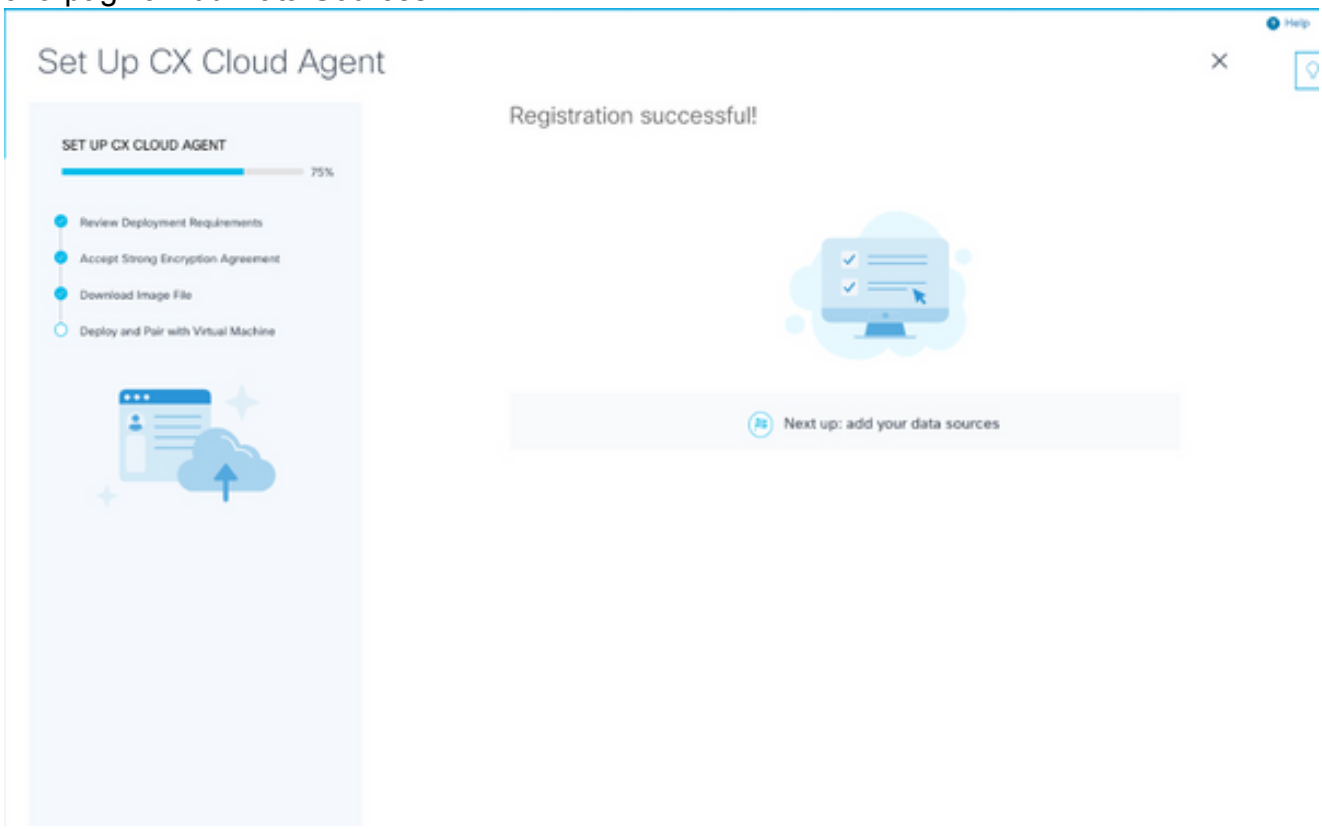
1. Ingrese el Código de emparejamiento proporcionado en el cuadro de diálogo de la consola o en la Interfaz de línea de comandos (CLI) de la máquina virtual conectada a través del agente.

Nota: El código de vinculación se recibe después de la implementación del archivo OVA descargado.



Código de vinculación

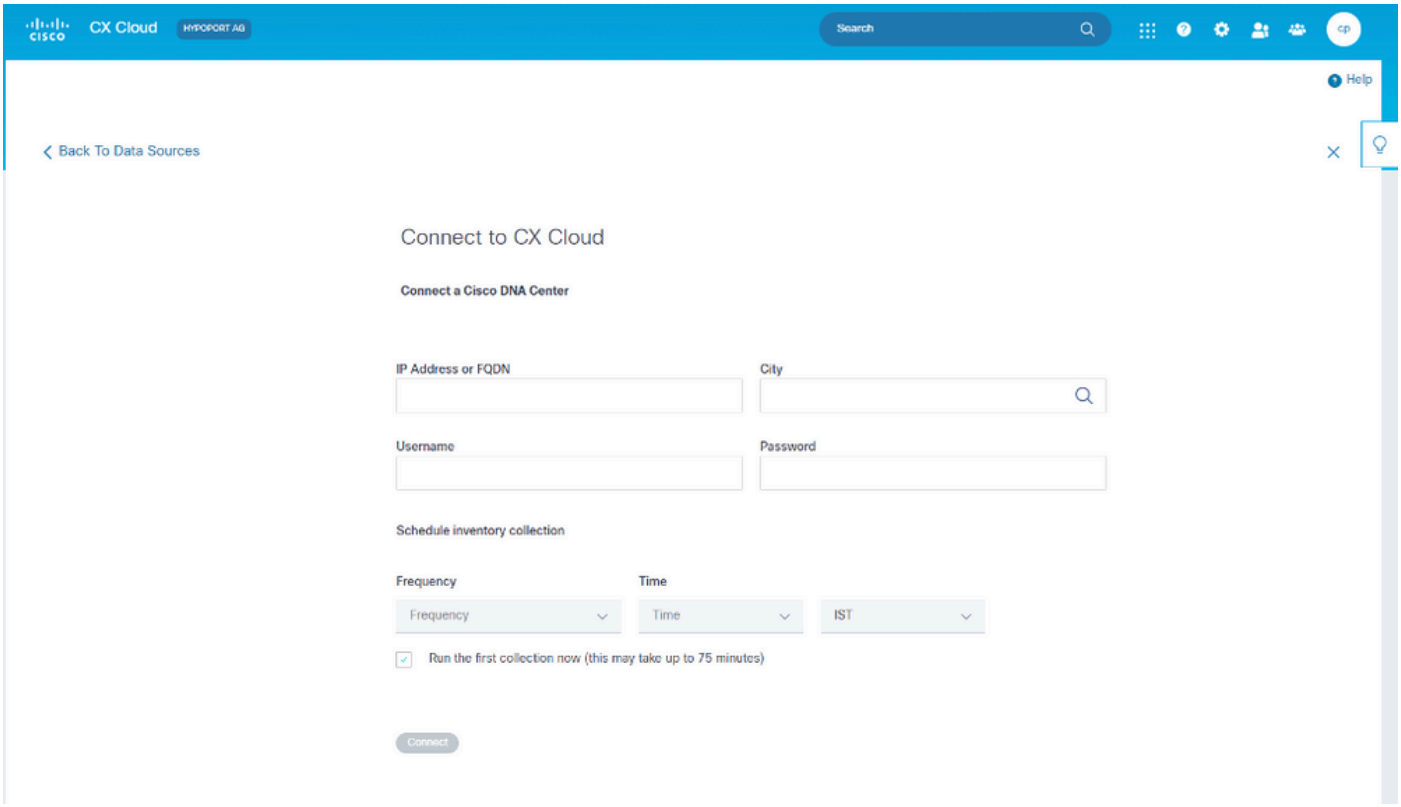
2. Haga clic en Continue para registrar el agente en la nube de CX. La ventana Set Up CX Cloud Agent - Registration success se abre brevemente antes de navegar automáticamente a la página Add Data Sources.



Registro correcto

Adición de Cisco DNA Center como origen de datos

Cuando se selecciona Cisco DNA Center en la ventana de conexión de orígenes de datos (consulte Conexión de la imagen de orígenes de datos en la sección Conexión de orígenes de datos), se abre esta ventana:



Conexión a la nube CX

Para agregar Cisco DNA Center como origen de datos:

1. Introduzca la dirección IP o la dirección IP virtual del Cisco DNA Center o FQDN, ciudad (ubicación del Cisco DNA Center), nombre de usuario y contraseña.

   Nota: No utilice una IP de nodo de cluster individual.

2. Programe una recopilación de inventario introduciendo una frecuencia y una hora para indicar la frecuencia con que el agente en la nube de CX puede realizar análisis de red y actualizar la información de los dispositivos conectados.

   Nota: La primera recopilación de inventario puede tardar hasta 75 minutos.

3. Haga clic en Connect (Conectar) Aparecerá una confirmación con la dirección IP del centro de DNA de Cisco.

Conectado correctamente

4. Haga clic en Add Another Cisco DNA Center, Done o Back to Data Sources para navegar de nuevo a la ventana Data Sources.

Adición de otros recursos como orígenes de datos

Overview

La recopilación de telemetría se ha ampliado a dispositivos no gestionados por el Cisco DNA Center, lo que permite a los clientes 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 en la nube de CX, los usuarios tienen la opción de configurar el agente en la nube de CX para conectarse a 20 Cisco DNA Centers adicionales dentro de la infraestructura supervisada por CX Cloud. Los usuarios también pueden conectar CX Cloud Agent directamente a otros recursos de hardware de su entorno, hasta 10 000 dispositivos conectados directamente.

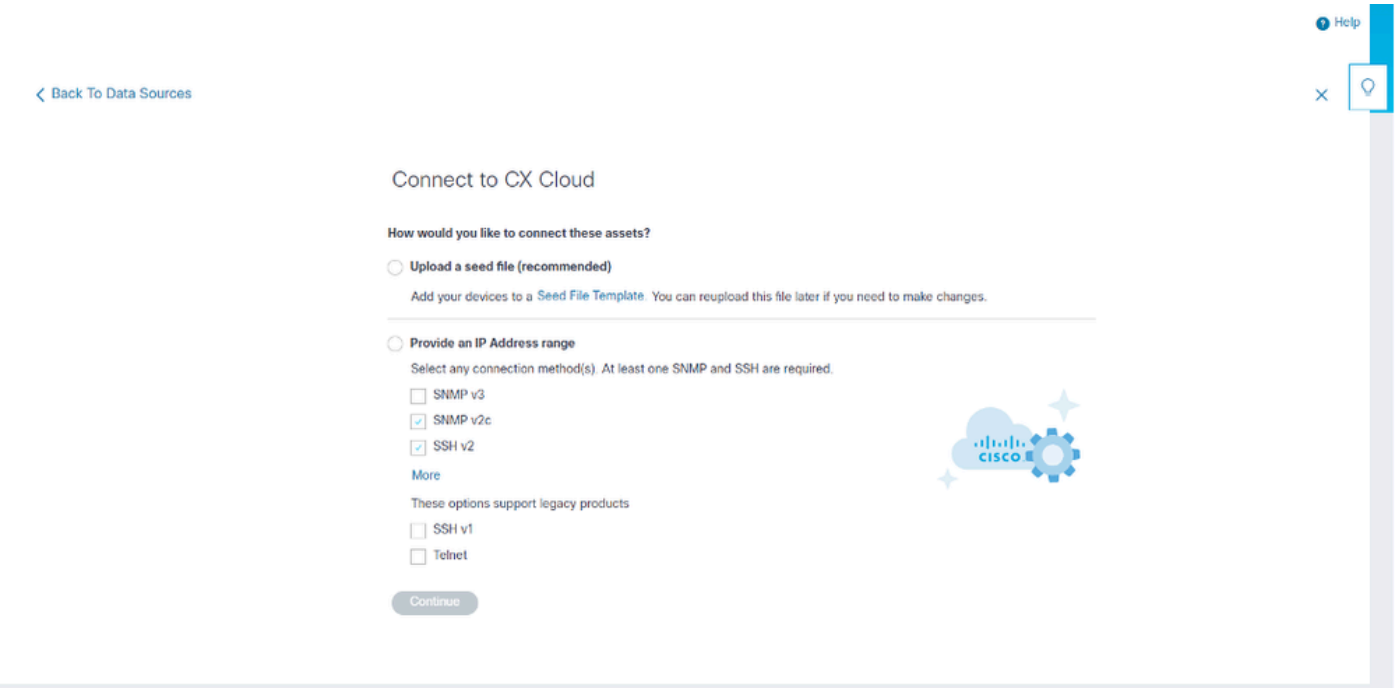
Los usuarios pueden identificar los dispositivos que se incorporarán a CX Cloud identificándolos de forma única mediante un archivo simiente o especificando un rango de IP, que CX Cloud Agent puede analizar. Ambos enfoques se basan en el protocolo simple de administración de red (SNMP) para la detección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

Nota:
Se puede utilizar el archivo simiente o el rango de IP. No es posible cambiar esta selección después de la configuración inicial.

Nota:
Un archivo simiente inicial se puede reemplazar por otro mientras que un rango de IP inicial

se puede editar a un nuevo rango de IP.

Cuando se selecciona Otros Activos en la ventana de conexión de orígenes de datos, se abre esta ventana:



Configuración de la conexión a la nube CX

Para agregar otros activos como orígenes de datos:

- Cargue 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 CX Cloud Agent es compatible con SNMPV2c y SNMP V3 y se pueden configurar una o ambas versiones. El usuario debe proporcionar la misma información, descrita 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 que SNMPv3 se utilice 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 dispositivos antiguos que no son compatibles con SNMPv3. Si el usuario configura ambas versiones de SNMP, CX Cloud Agent puede, de forma predeterminada, intentar comunicarse con cada dispositivo respectivo mediante SNMPv3 y volver a SNMPv2c si la comunicación no se puede negociar correctamente.

Protocolos de conectividad

Como parte de la configuración de la conectividad directa del dispositivo, los usuarios deben especificar los detalles del protocolo de conectividad del dispositivo: SSH (o, alternativamente, telnet). Se puede 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 (nombres de usuario y contraseñas) que se envía a través de telnet no está cifrada y, por lo tanto, es vulnerable a peligros, sin seguridad adicional.

Agregar dispositivos mediante un archivo simiente

Acerca del archivo simiente

Un archivo simiente es un archivo de valores separados por comas (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 CX Cloud Agent puede 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 en la nube de CX puede intentar conectarse a los dispositivos, pero no puede procesar cada uno de ellos para mostrarlos en las páginas de recursos en los casos en los que no puede determinar los PID o los números de serie. Se ignora 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.

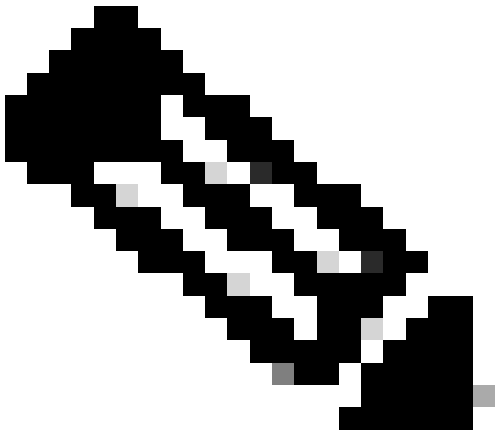
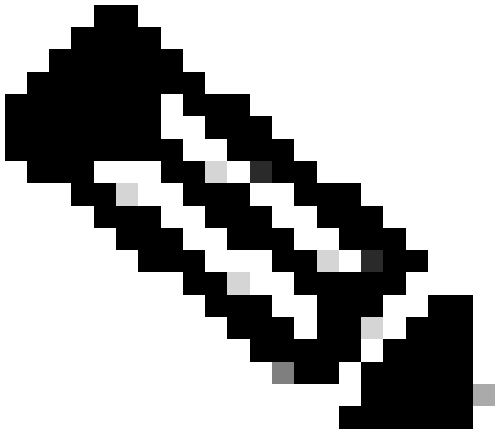
Es importante que el formato del archivo simiente de ejemplo, incluidos los encabezados de columna, no se modifique en modo alguno. Haga clic en el enlace proporcionado para ver un archivo simiente en formato PDF. Este PDF es sólo de referencia y se puede utilizar para crear un archivo simiente que debe guardarse en formato .csv.

Haga clic en este enlace para ver un archivo simiente que se puede utilizar para crear un archivo simiente en formato .csv.

Nota: Este PDF es sólo de referencia y se puede utilizar para crear un archivo simiente que debe guardarse en formato .csv.

Esta tabla identifica todas las columnas de archivos simientes necesarias y los datos que deben incluirse en cada columna.

Columna de archivo simiente	Encabezado/identificador de columna	Objetivo de la columna
R	Dirección IP o nombre de host	Proporcione una dirección IP o nombre de host válidos y únicos para el dispositivo.
B	versión del protocolo SNMP	El agente en la nube CX requiere el protocolo SNMP, que se utiliza para la detección de dispositivos en la red del cliente. Los valores pueden ser snmpv2c o snmpv3, pero se recomienda snmpv3 debido a consideraciones de seguridad.
C	snmpRo: Obligatorio si col#=3 se selecciona como 'snmpv2c'	Si se selecciona la variante heredada de SNMPv2 para un dispositivo específico, se deben especificar las credenciales snmpRO (de solo lectura) para la recopilación SNMP del dispositivo. De lo contrario, la entrada puede estar en blanco.
D	snmpv3UserName: Obligatorio si col#=3 se selecciona como 'snmpv3'	Si se selecciona SNMPv3 para comunicarse con un dispositivo específico, se debe proporcionar el nombre de usuario de inicio de sesión correspondiente.
E	snmpv3AuthAlgorithm: los valores pueden ser MD5 o SHA	El protocolo SNMPv3 permite la autenticación a través del algoritmo MD5 o SHA. Si el dispositivo está configurado con autenticación segura, se debe proporcionar el algoritmo de autenticación respectivo.

Columna de archivo simiente	Encabezado/identificador de columna	Objetivo de la columna
		 Nota: MD5 se considera inseguro y SHA se puede utilizar en todos los dispositivos que lo admitan.
F	snmpv3AuthPassword: password	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 valores pueden ser DES , 3DES	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. 

Columna de archivo simiente	Encabezado/identificador de columna	Objetivo de la columna
		Nota: las claves de 56 bits utilizadas por DES se consideran demasiado cortas para proporcionar seguridad criptográfica y 3DES se puede utilizar en todos los dispositivos que la admitan.
H	snmpv3PrivPassword: password	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, ID único que representa el dispositivo, especifique el ID del motor si está configurado manualmente en el dispositivo	El EngineID de SNMPv3 es un ID único que representa cada dispositivo. Este ID de motor se envía como referencia mientras CX Cloud Agent recopila los conjuntos de datos SNMP. Si el cliente configura el EngineID manualmente, se debe proporcionar el EngineID respectivo.
J	cliProtocol: los valores pueden ser 'telnet', 'sshv1', 'sshv2'. Si está vacío, se puede establecer como 'sshv2' de forma predeterminada	La CLI está diseñada para interactuar directamente con el dispositivo. El agente en la nube de CX utiliza este protocolo para la recopilación de 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 una seguridad de transporte adecuada.
K	cliPort: número de puerto 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 simiente	Encabezado/identificador de columna	Objetivo de la columna
L	cliUser: Nombre de usuario de CLI (se puede proporcionar 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 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 en la nube de 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

Limitaciones del procesamiento de telemetría para dispositivos

Estas son las limitaciones al procesar datos de telemetría para dispositivos:

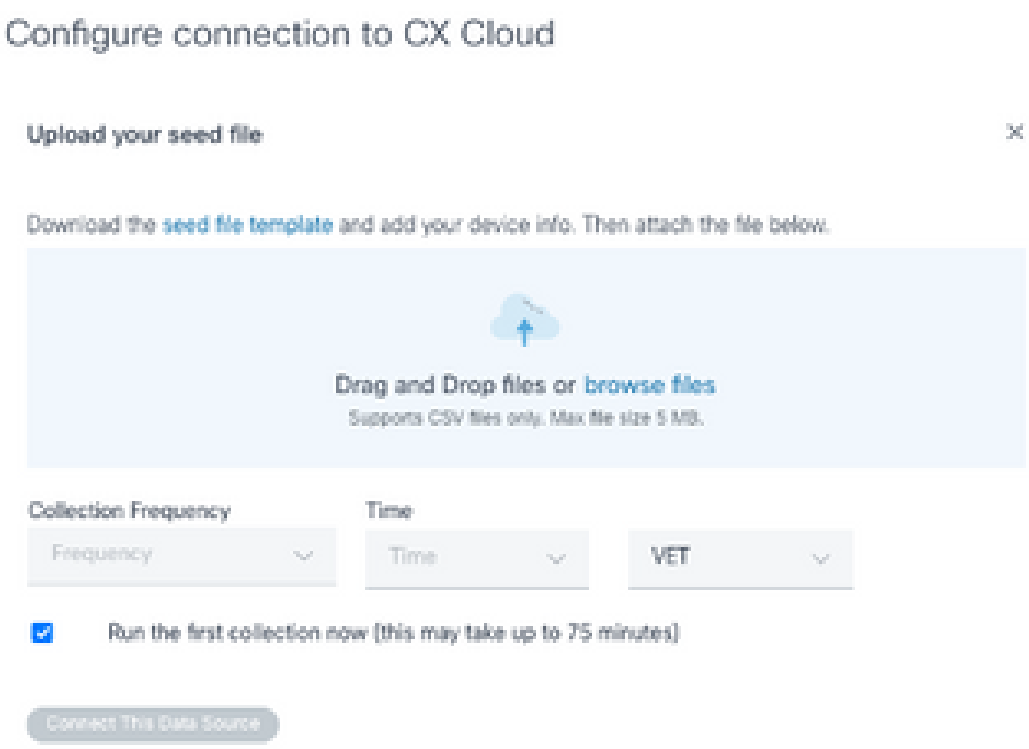
- Algunos dispositivos pueden aparecer como accesibles en el resumen de la recopilación, pero no están visibles en la página de activos de la nube de CX. Las limitaciones de instrumentación de dispositivos impiden el procesamiento de dicha telemetría de dispositivos.
- Los atributos de telemetría pueden ser inexactos o faltar en la página de activos de la nube de CX para los dispositivos que no forman parte de la opción de seguimiento del éxito en el campus.
- Si un dispositivo del archivo simiente o de las colecciones de rangos de IP también es parte del inventario de Cisco DNA Center, el dispositivo se informa solamente una vez para la entrada de Cisco DNA Center. La entrada del archivo simiente/rango de IP no se recopila ni procesa para evitar la duplicación.

Agregar dispositivos mediante un nuevo archivo simiente

Para agregar dispositivos mediante un nuevo archivo simiente:

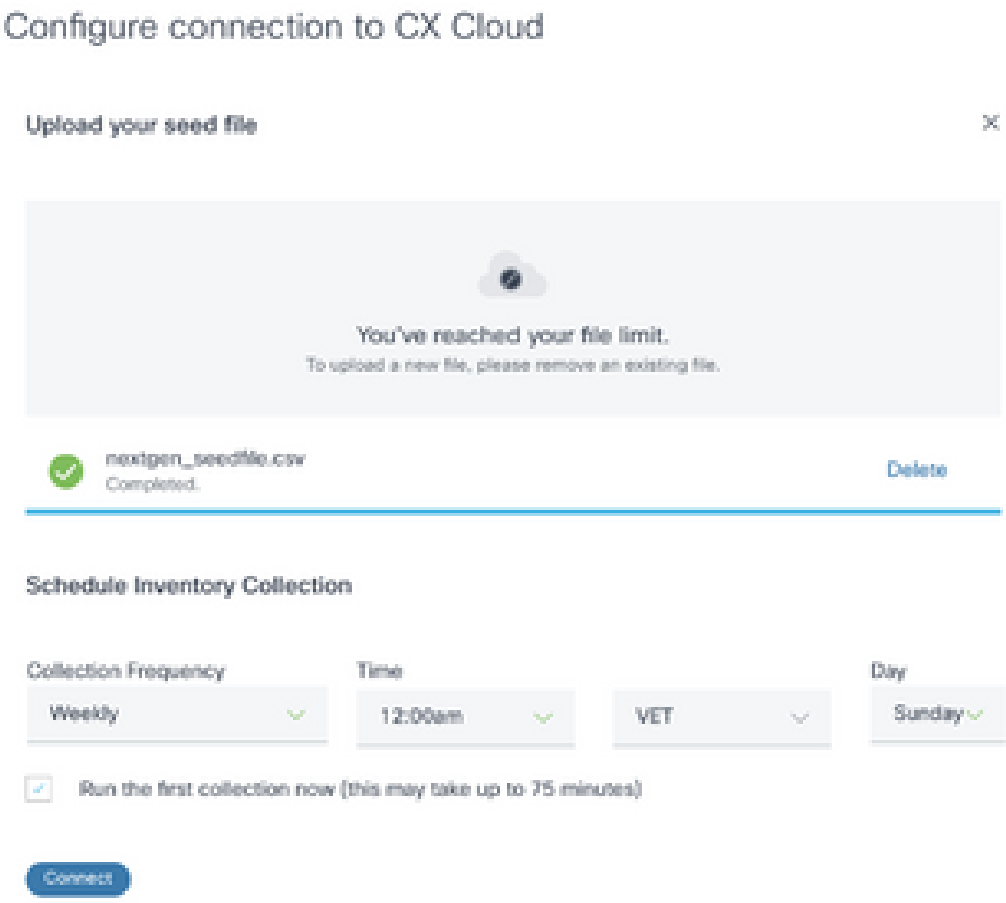
1. Descargue la plantilla de archivo simiente (PDF) utilizando el enlace incrustado en este documento (consulte Acerca del archivo simiente) o a través de un enlace en la ventana Configurar conexión a la nube de CX.

   Nota: El enlace de la ventana Configurar conexión a la nube de CX ya no está disponible una vez que se ha descargado el archivo simiente inicial.



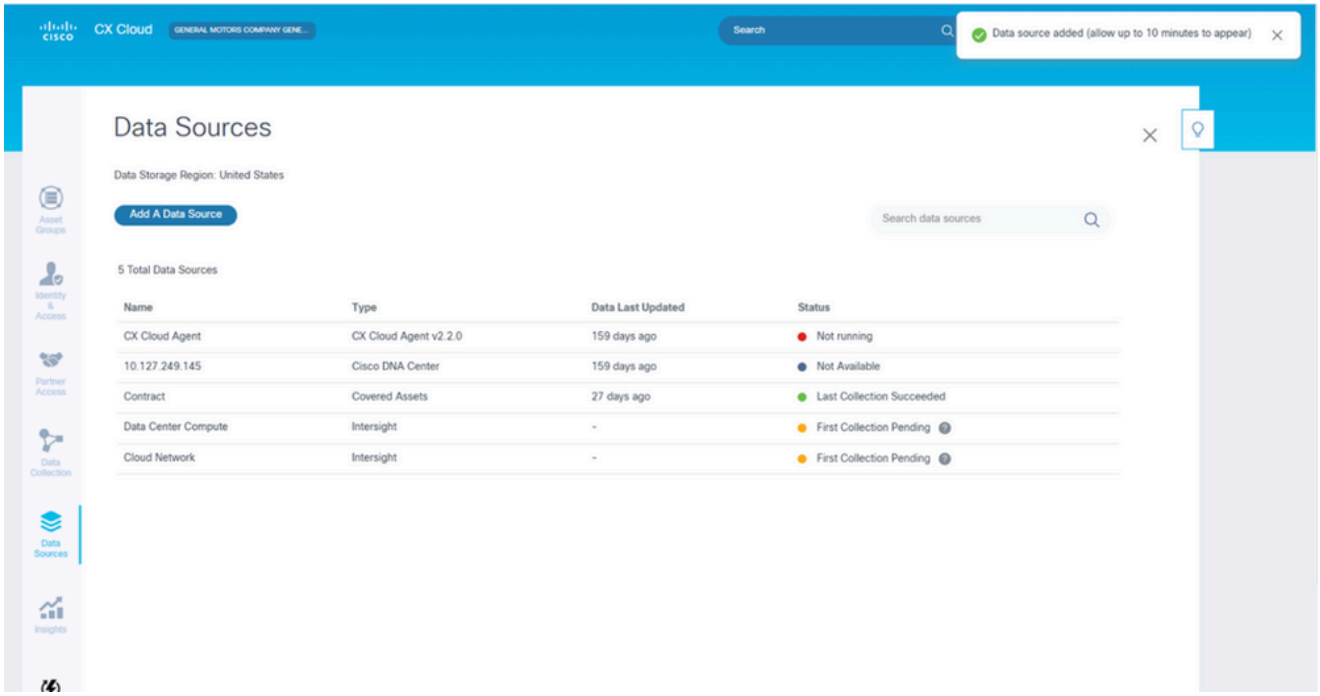
Configurar la ventana Conexión a la nube CX

2. Abra una hoja de cálculo de Excel (o cualquier hoja de cálculo preferida) e introduzca los encabezados tal y como se muestra en la plantilla.
3. Introduzca los datos manualmente o impórtelos al archivo.
4. Una vez completada, guarde la plantilla como archivo .csv para importar el archivo en CX Cloud Agent.



Ventana Cargar Archivo Inicial

5. En la ventana Upload your seed file, arrastre y suelte el archivo .csv recién creado o haga clic en browse files y navegue hasta el archivo .csv.
6. Complete la sección Recopilación de Inventario de Programación y haga clic en Conectar. Se abre la ventana Orígenes de datos y se muestra un mensaje de confirmación.
7. 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 colección ahora. Dependiendo del número de entradas especificadas en el archivo simiente y de otros factores, este proceso puede tardar bastante tiempo.



Mensaje de confirmación

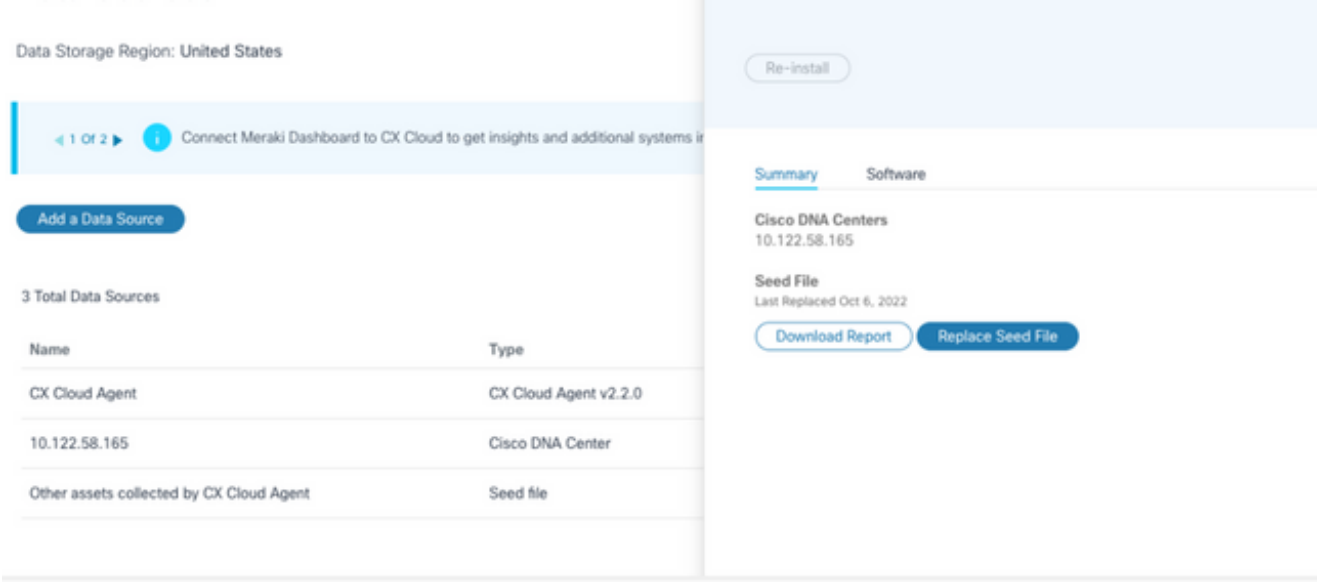
Agregar dispositivos mediante un archivo simiente modificado

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.

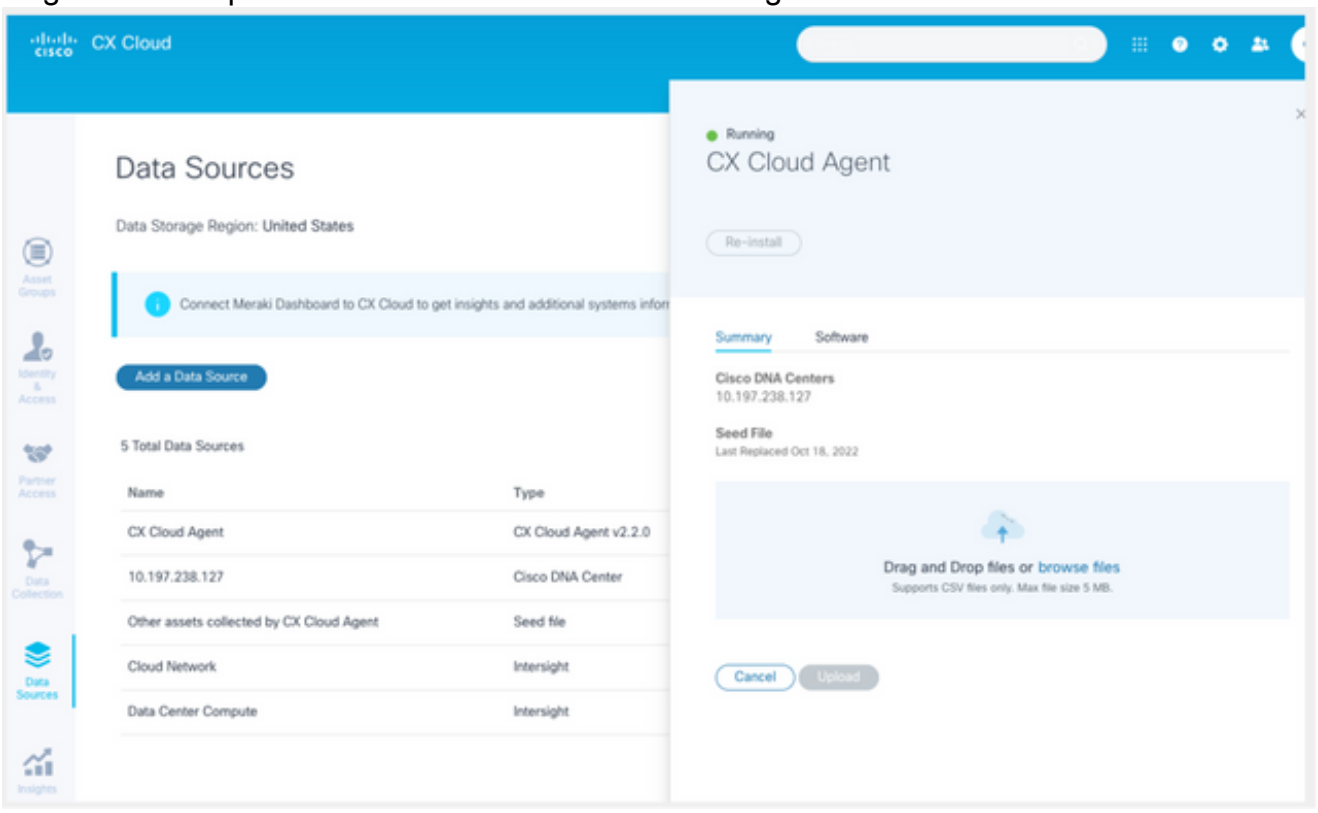
> Nota: Para añadir activos al archivo simiente, añada dichos activos al archivo simiente creado anteriormente y vuelva a cargar el archivo. Esto es necesario ya que cargar un nuevo archivo simiente reemplaza al actual. Para la detección y la recopilación, sólo se utiliza el último archivo simiente cargado.

2. En la página Orígenes de datos, seleccione un origen de datos que tenga un tipo de agente de nube CX. Se abre una ventana de detalles con las pestañas Summary y Software.



Ventana Detalles

3. Haga clic en Descargar informe para generar un informe de todos los activos del origen de datos seleccionado. El informe proporciona información sobre la dirección IP del dispositivo, el número de serie, la disponibilidad, el tipo de comando, el estado del comando y el error del comando, si corresponde.
4. Haga clic en Replace Seed File. Se abre la ventana Agente en la nube CX.



Ventana Agente en la nube CX

5. Arrastre y suelte el archivo simiente modificado en la ventana o busque el archivo y agréguelo en la ventana.
6. Haga clic en Cargar.

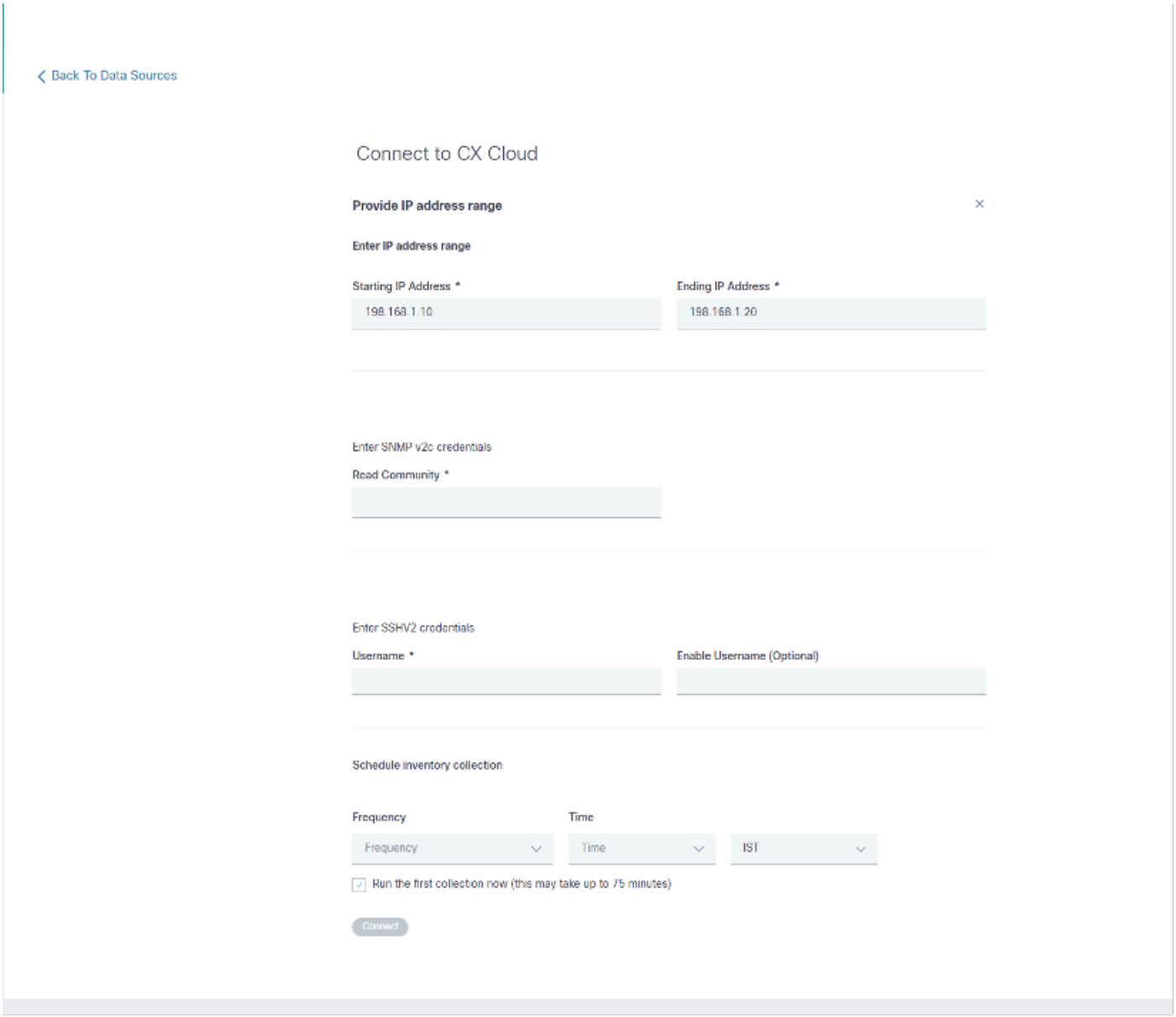
Agregar dispositivos mediante rangos de IP

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 solo rango de IP de nivel de red, que CX Cloud Agent 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 en la nube de CX no intenta comunicarse con un dispositivo que tenga dicha dirección IP ni recopila telemetría de dicho dispositivo.
- Si introduce *.*.*.*, CX Cloud Agent podrá utilizar las credenciales proporcionadas por el usuario con cualquier 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 en la nube de CX puede intentar conectarse a los dispositivos, pero no puede procesar cada uno para mostrarlo en la vista de recursos en los casos en los que no puede determinar las 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 a demanda para incluir cualquier dispositivo recién agregado al inventario de recolección de agentes en la nube de CX.



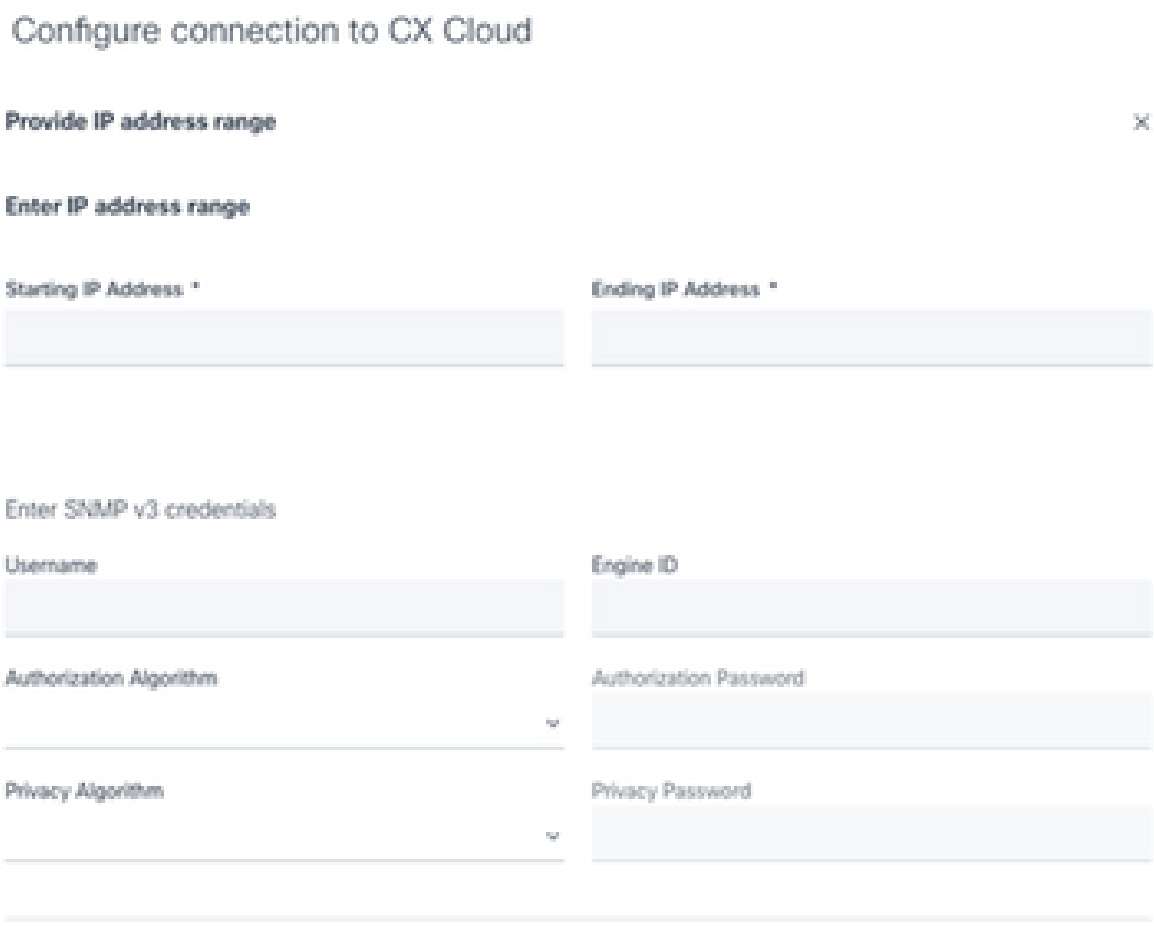
Ventana Intervalo de direcciones IP inicial

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, si se selecciona SNMPv2c y SNMPv3 o SSHv2 y SSHv1, CX Cloud Agent negocia automáticamente la selección del protocolo en función de las capacidades de cada dispositivo.

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

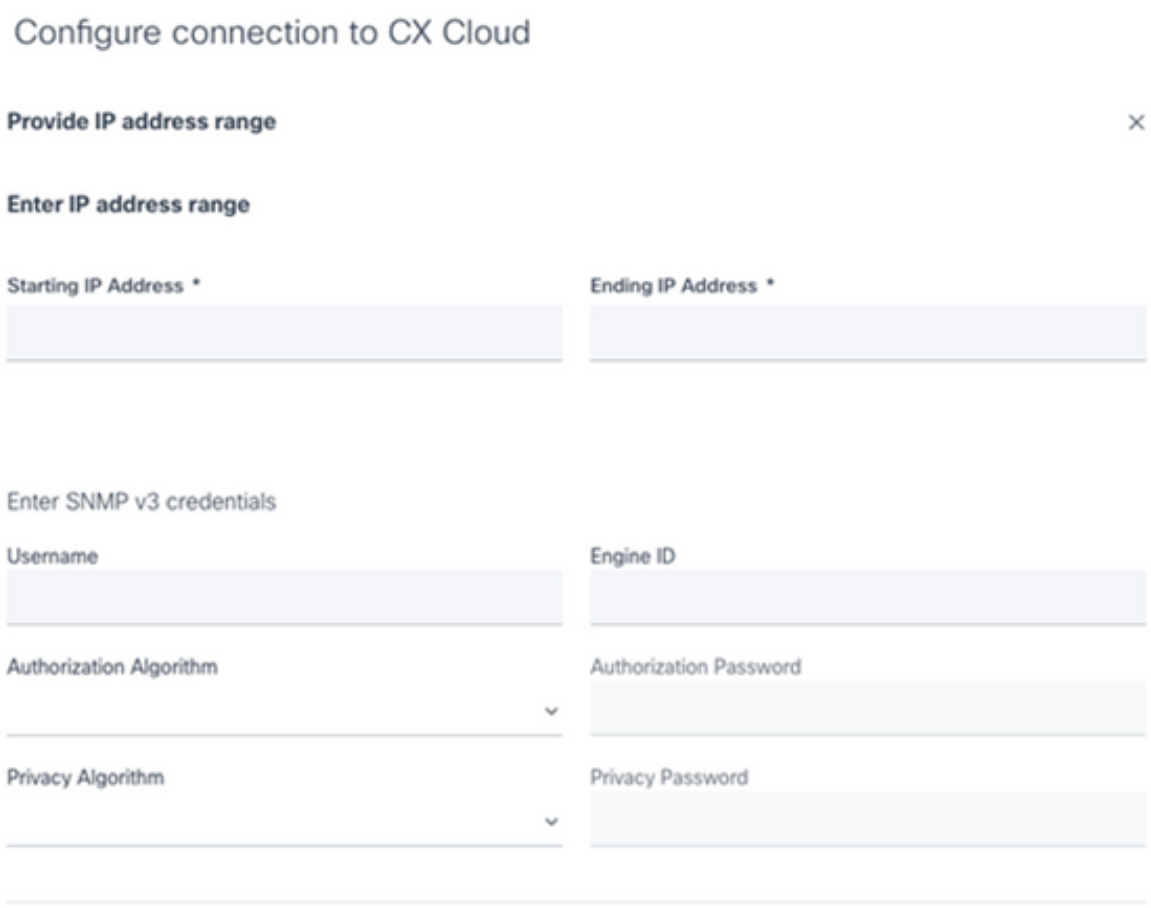
Para agregar dispositivos mediante el intervalo IP:

1. En la ventana Configure connection to CX Cloud, seleccione la opción Proporcionar un rango de direcciones IP.

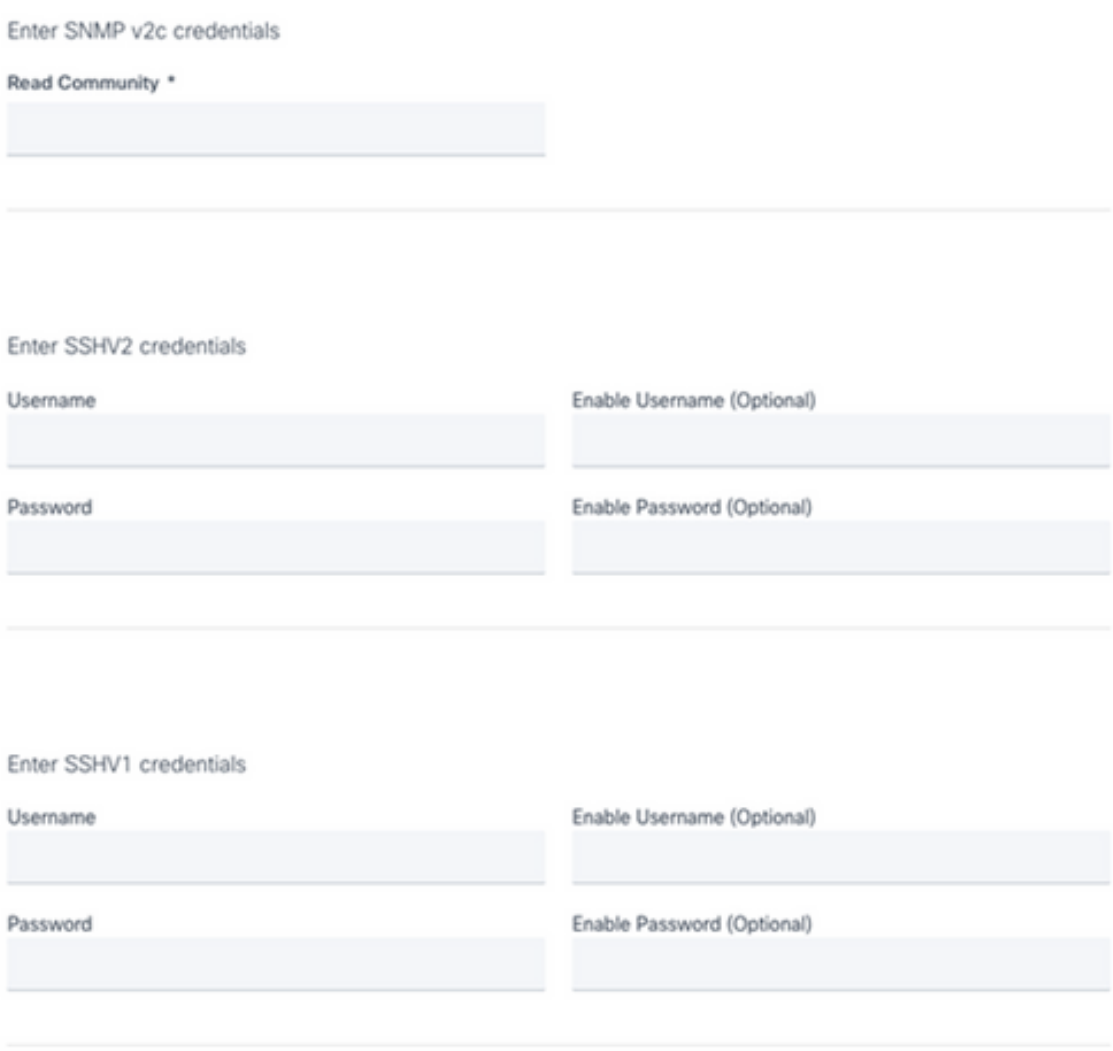


Formulario de agregar dispositivos mediante direcciones IP

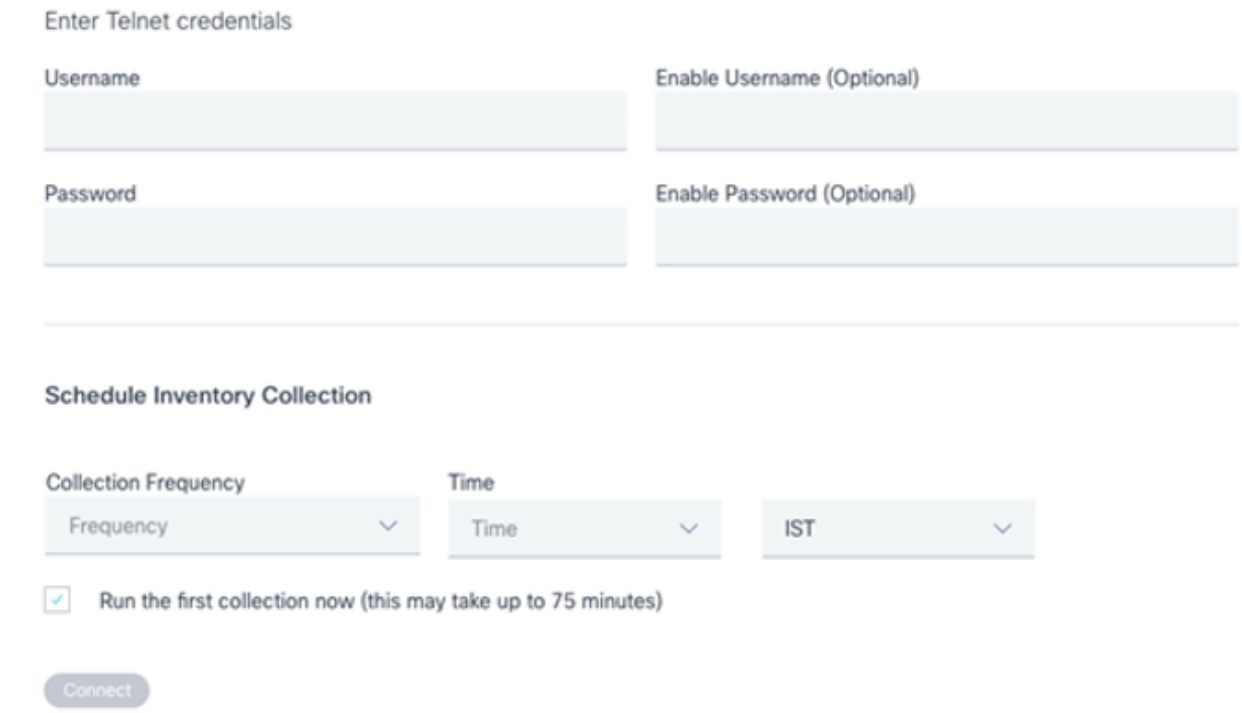
2. Complete el formulario con la información pertinente.
3. Se pueden seleccionar varias opciones de conexión. Estas pantallas muestran las credenciales de configuración de las opciones. Consulte Acerca del Archivo Inicial para obtener una descripción de los campos de credenciales para cada opción de conexión.



Credenciales de SNMP v3

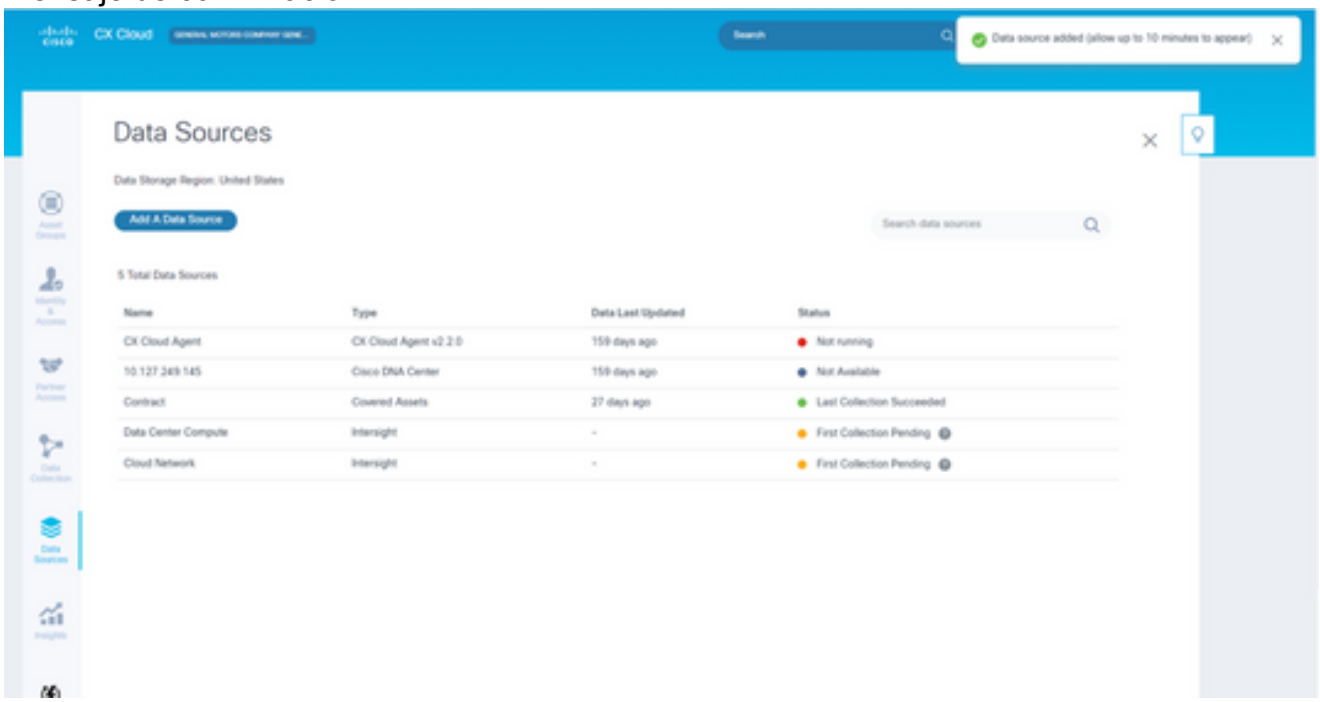


Credenciales de SNMP v2, SSHV2 y SSHV1



Credenciales de Telnet y Programación de Network Scan

4. Haga clic en Connect (Conectar) Se abre la ventana Orígenes de datos y se muestra un mensaje de confirmación.

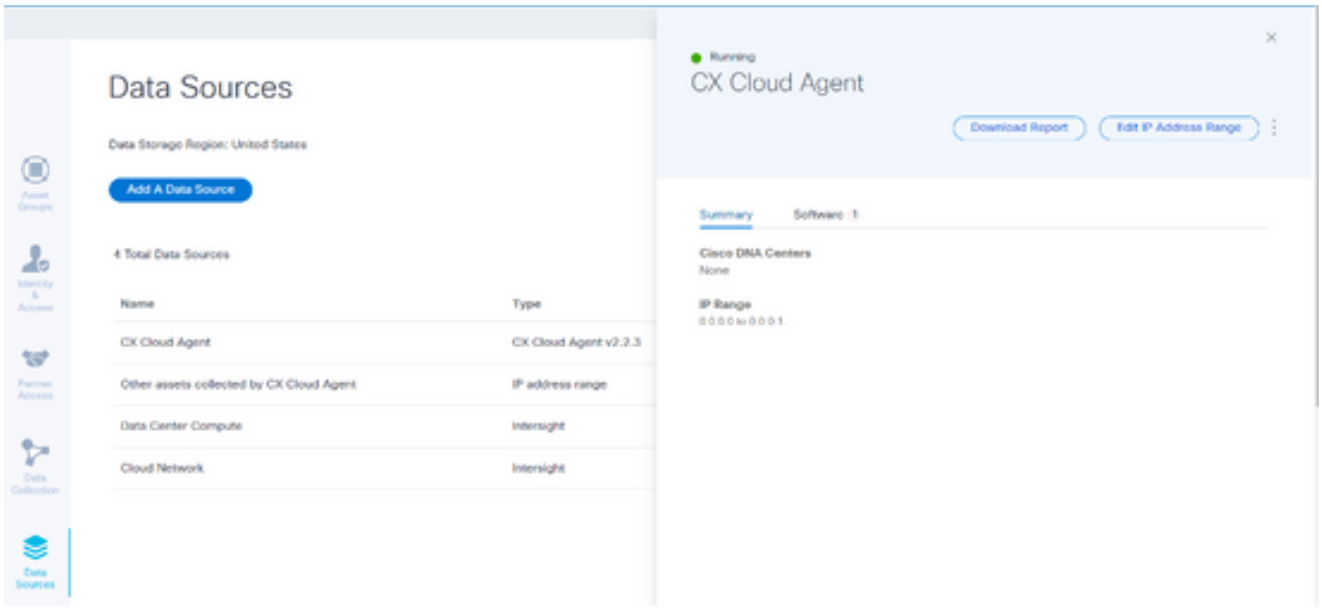


Confirmación

Edición de rangos IP

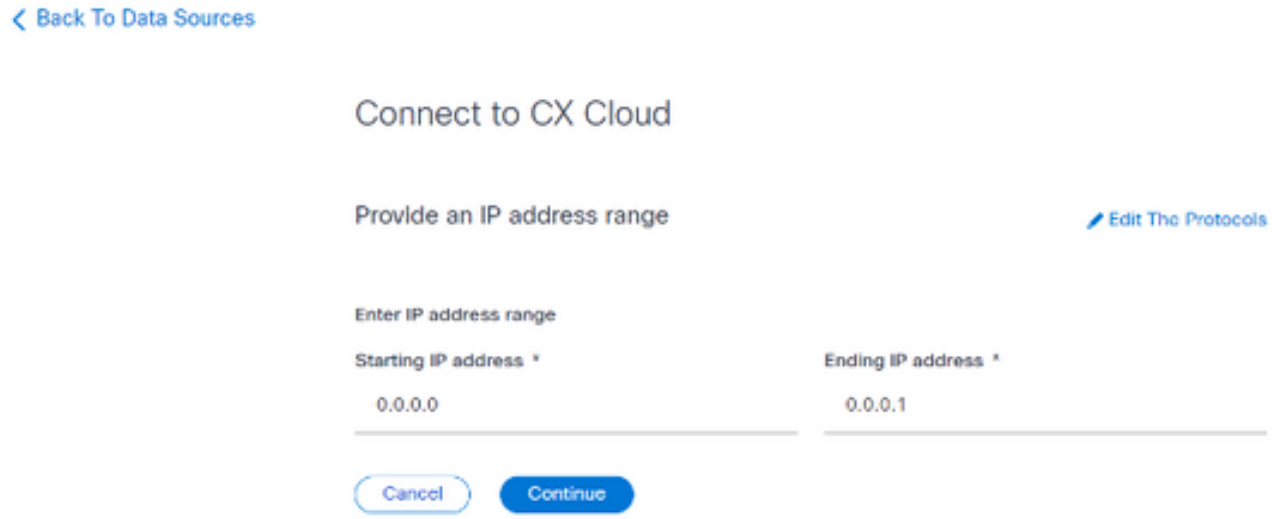
Para editar un rango de IP;

1. Acceda a la ventana Orígenes de Datos.



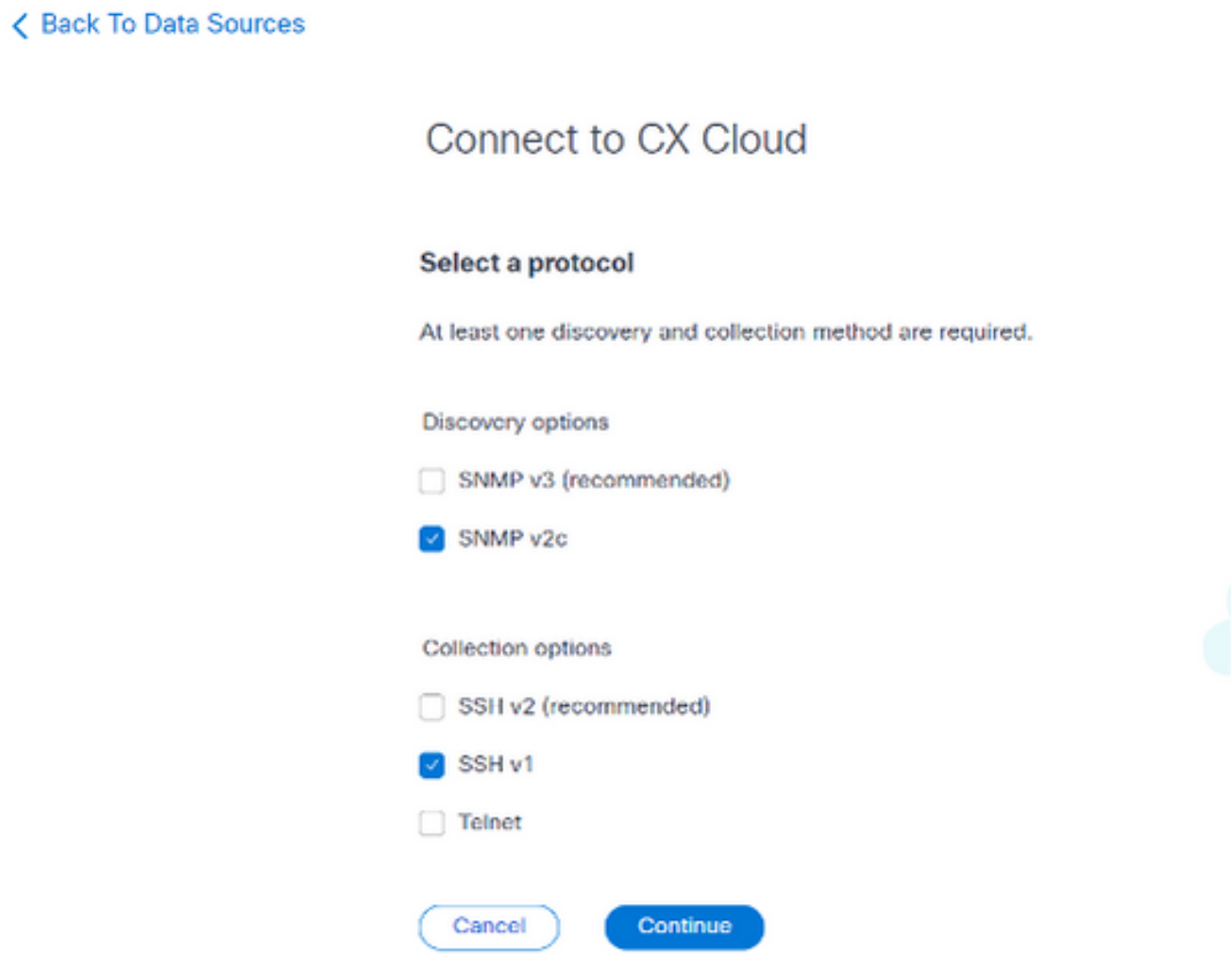
Orígenes de datos

2. Haga clic en el agente en la nube CX que requiere la edición del rango de IP en Orígenes de datos. Se abrirá la ventana de detalles.
3. Haga clic en Edit IP Address Range. Se abre la ventana Connect to CX Cloud.



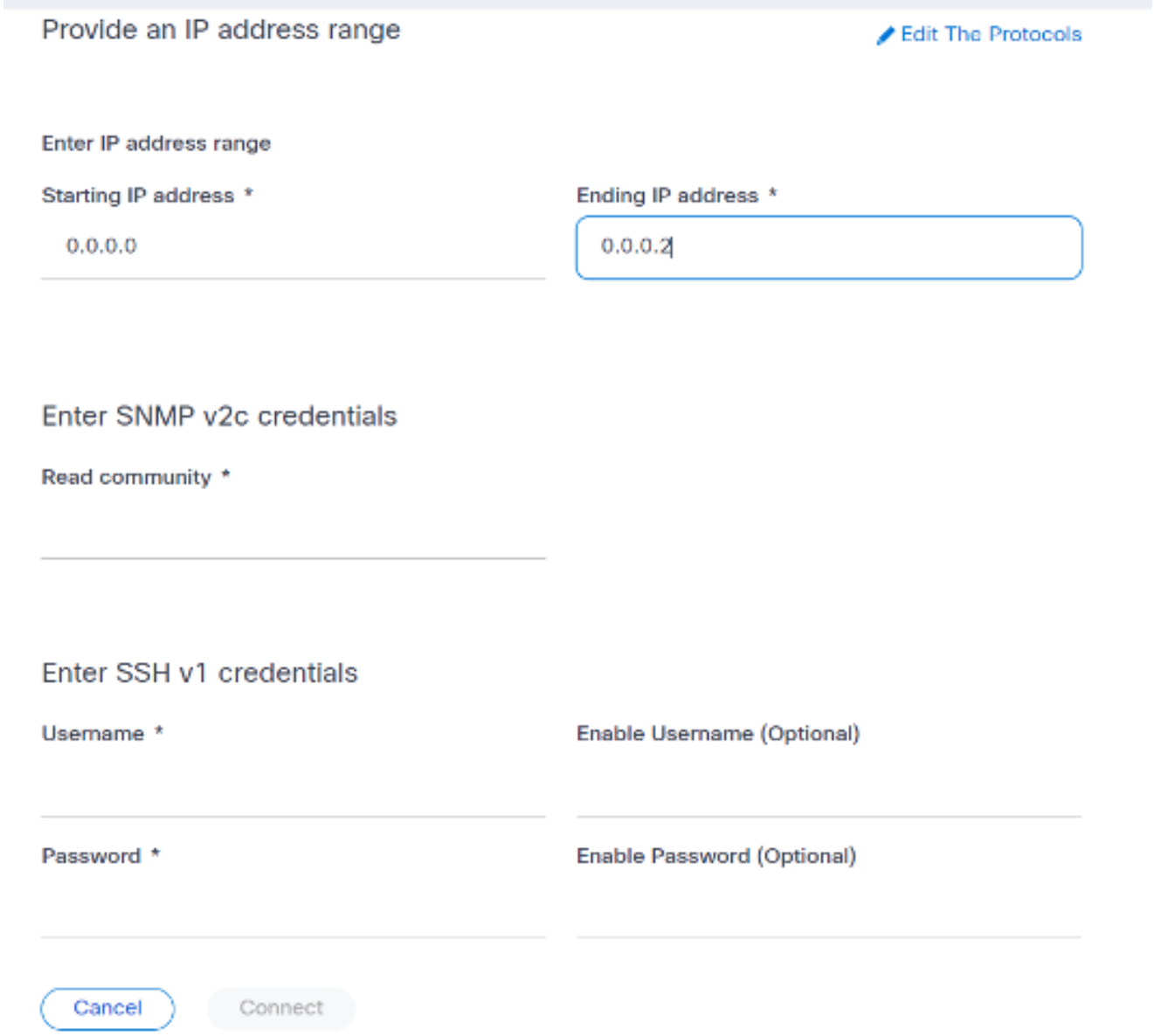
Proporcionar un intervalo IP

4. Actualice las nuevas direcciones IP en los campos Starting IP address y Ending IP address.
5. Haga clic en el enlace Edit the Protocols. Se abre la ventana Connect to CX Cloud - Select a protocol (Conectar a la nube CX - Seleccionar un protocolo).



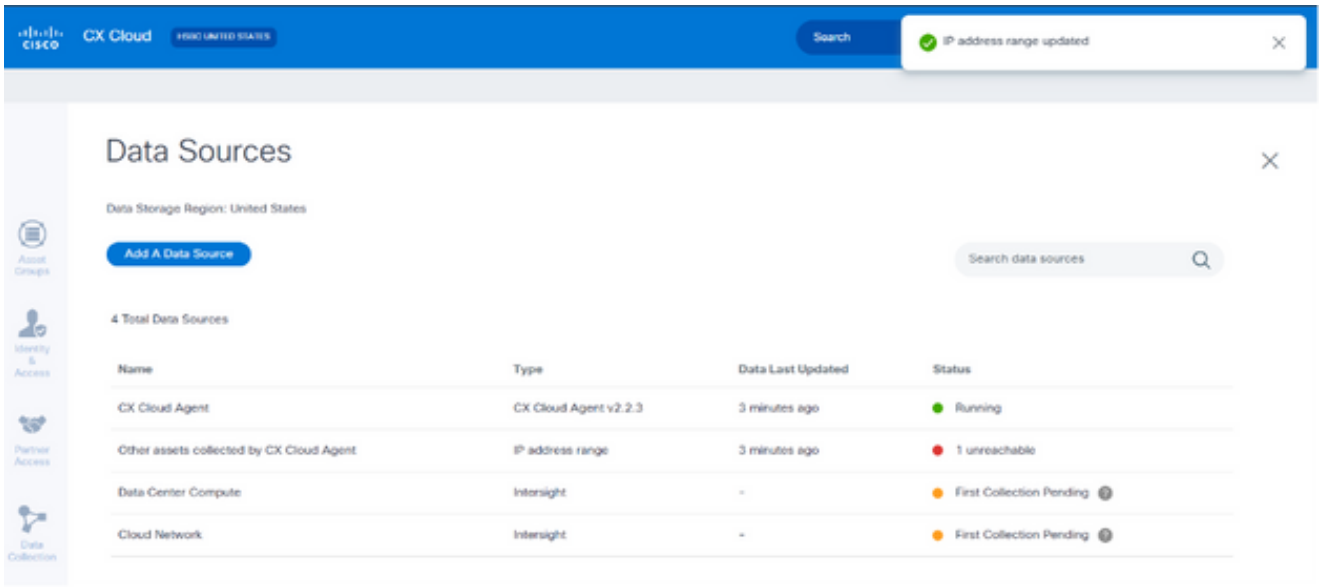
Seleccione un protocolo

6. Seleccione los protocolos aplicables haciendo clic en las casillas de verificación correspondientes.
7. Haga clic en Continue (Continuar). Se abrirá la ventana Proporcionar un intervalo de direcciones IP.



Introducir credenciales

8. Introduzca las credenciales de configuración.
9. Haga clic en Connect (Conectar) Se abre la ventana Orígenes de datos y se muestra un mensaje de confirmación.



Confirmación

Nota: El mensaje de confirmación no garantiza que se pueda acceder a los dispositivos del intervalo editado y que se hayan aceptado las credenciales.

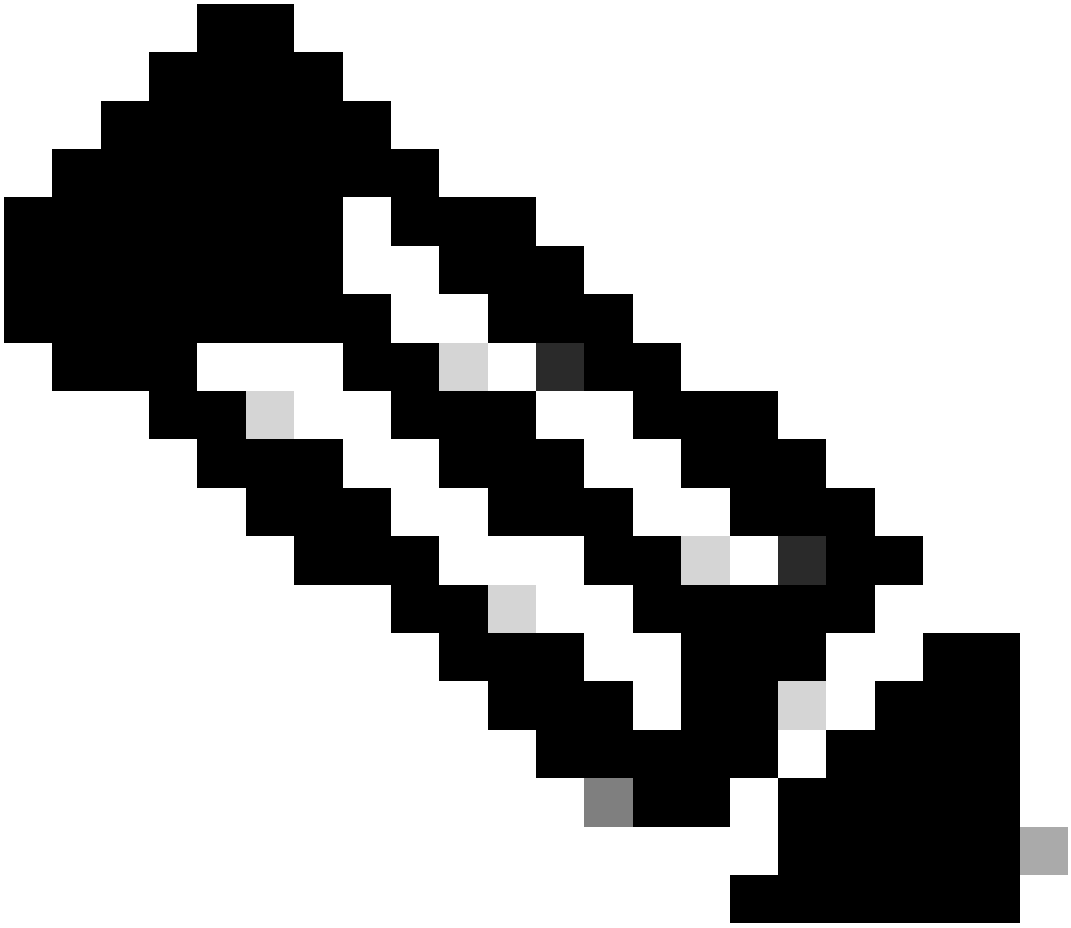
Acerca de los dispositivos detectados desde varios controladores

Es posible que tanto el Cisco DNA Center como la conexión directa del dispositivo al agente en la nube de CX descubran algunos dispositivos, lo que provoca la recopilación de datos duplicados de dichos dispositivos. Para evitar la recopilación de datos duplicados y que un solo controlador gestione los dispositivos, es necesario determinar la prioridad para la que CX Cloud Agent gestiona los dispositivos.

- Si Cisco DNA 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 DNA 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 en la nube CX y, a continuación, se vuelve a descubrir mediante Cisco DNA Center, este tendrá prioridad a la hora de controlar el dispositivo.

Programación de análisis de diagnóstico

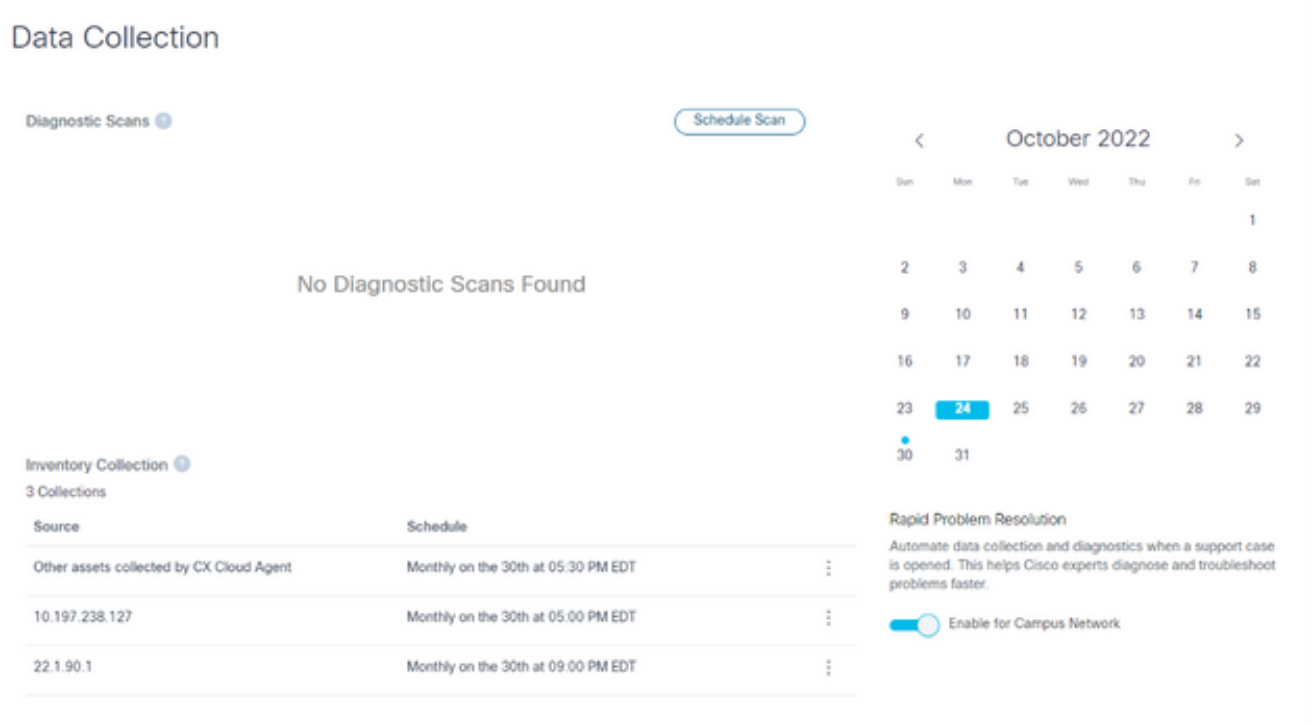
Los clientes pueden programar análisis de diagnóstico a demanda en CX Cloud.



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 solapen. La ejecución simultánea de varias exploraciones de diagnóstico puede ralentizar el proceso de exploración y, potencialmente, provocar errores de exploración.

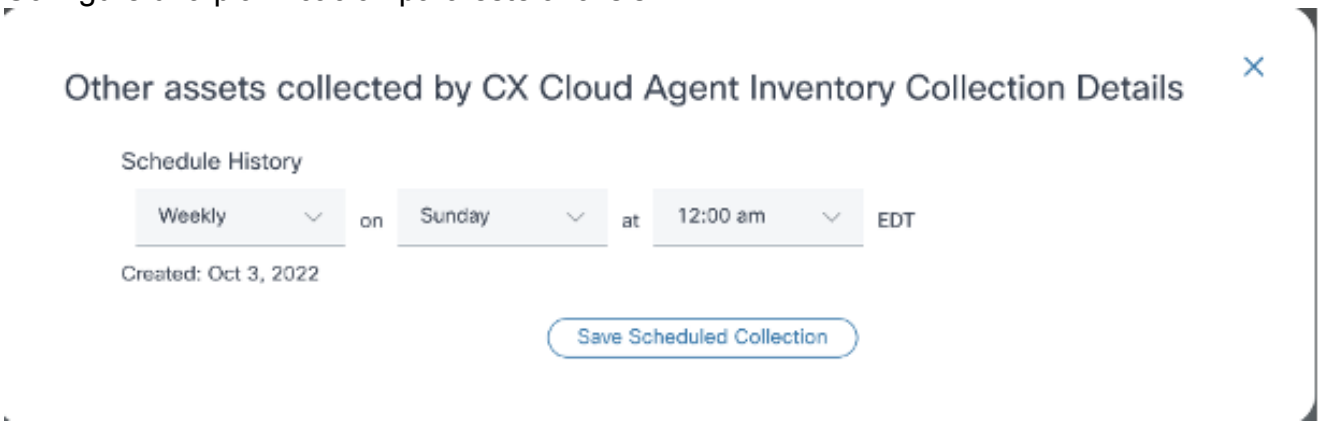
Para programar análisis de diagnóstico:

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.



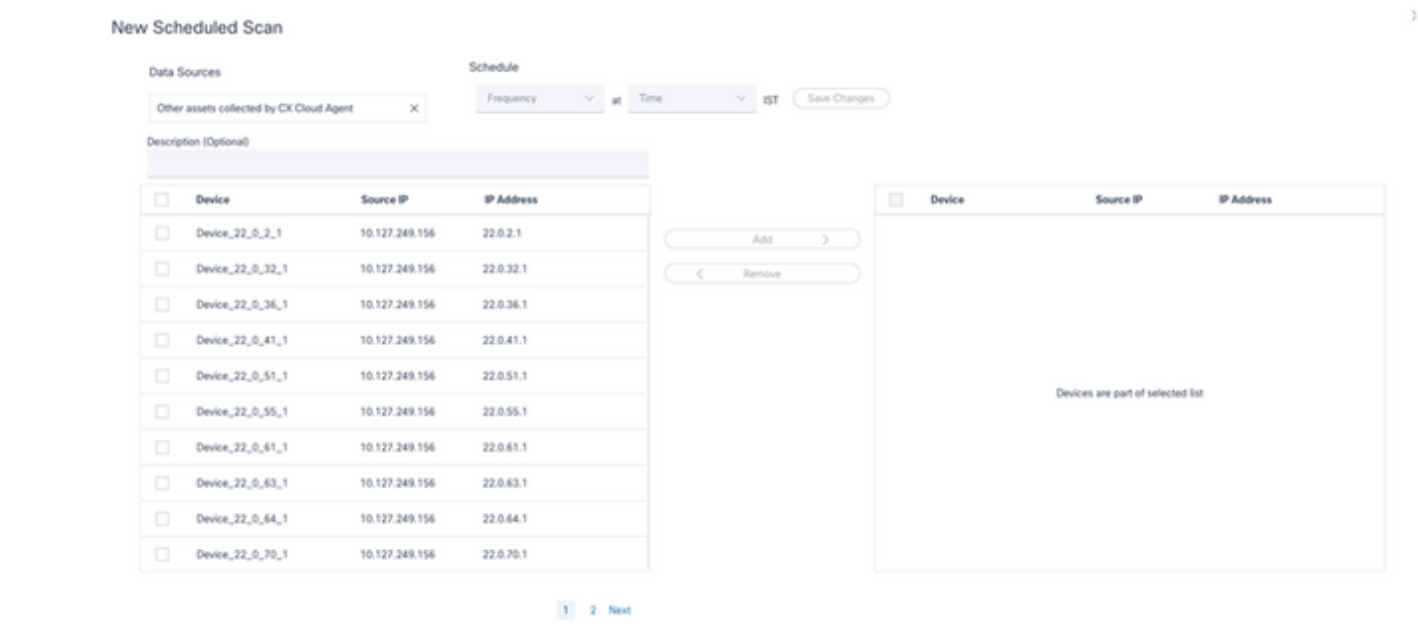
Recolección de datos

4. Configure una planificación para este análisis.



Configurar programación de análisis

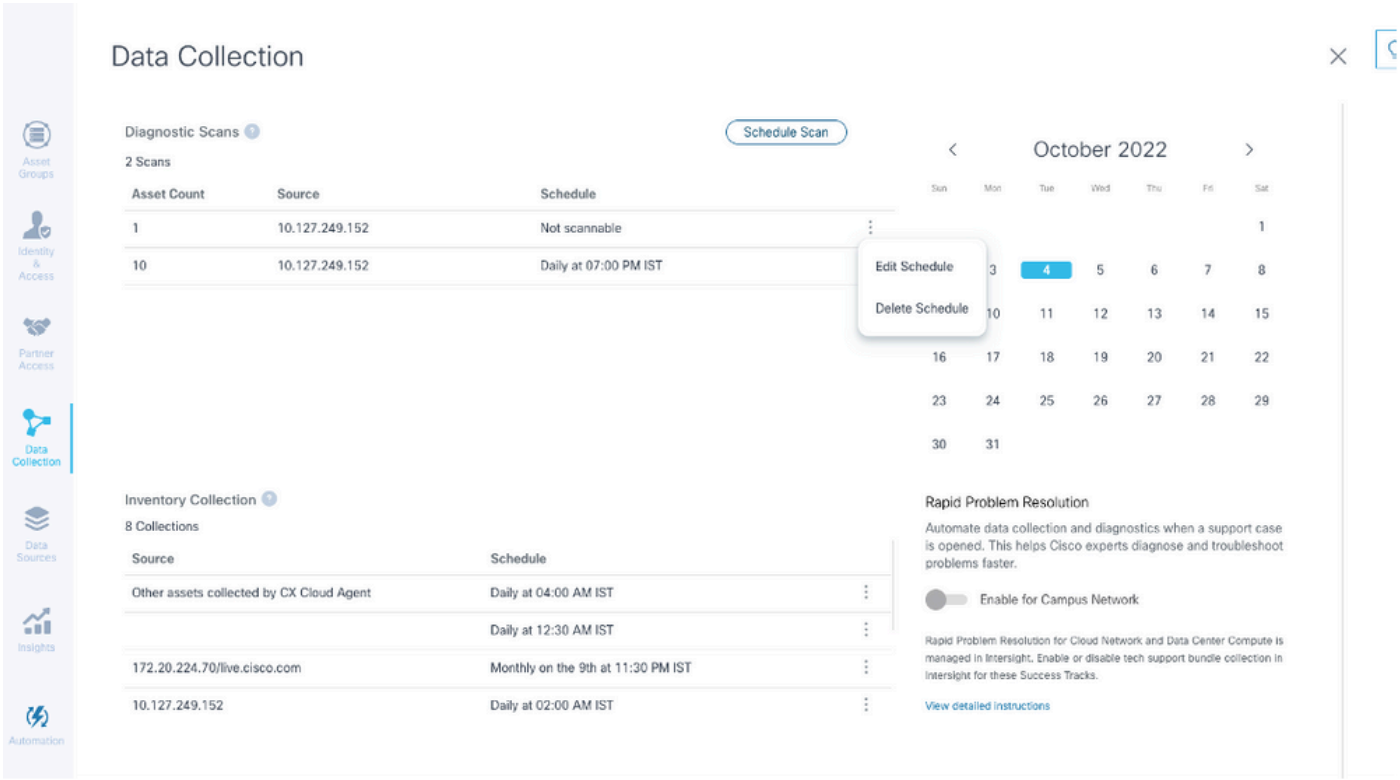
5. En la lista de dispositivos, seleccione todos los dispositivos para la exploración y haga clic en Agregar.



Programar un 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.



Recopilación de datos con las opciones Editar y Eliminar programación

Implementación y configuración de red

Seleccione cualquiera de estas opciones para implementar el agente en la nube CX:

- Para seleccionar VMware vSphere/vCenter Thick Client ESXi 5.5/6.0, vaya a Thick Client
- Para seleccionar VMware vSphere/vCenter Web Client ESXi 6.0, vaya a Web Client o vSphere Center
- Para seleccionar Oracle Virtual Box 5.2.30, vaya a Oracle VM
- Para seleccionar Microsoft Hyper-V, vaya a Hyper-V

Implementación de OVA

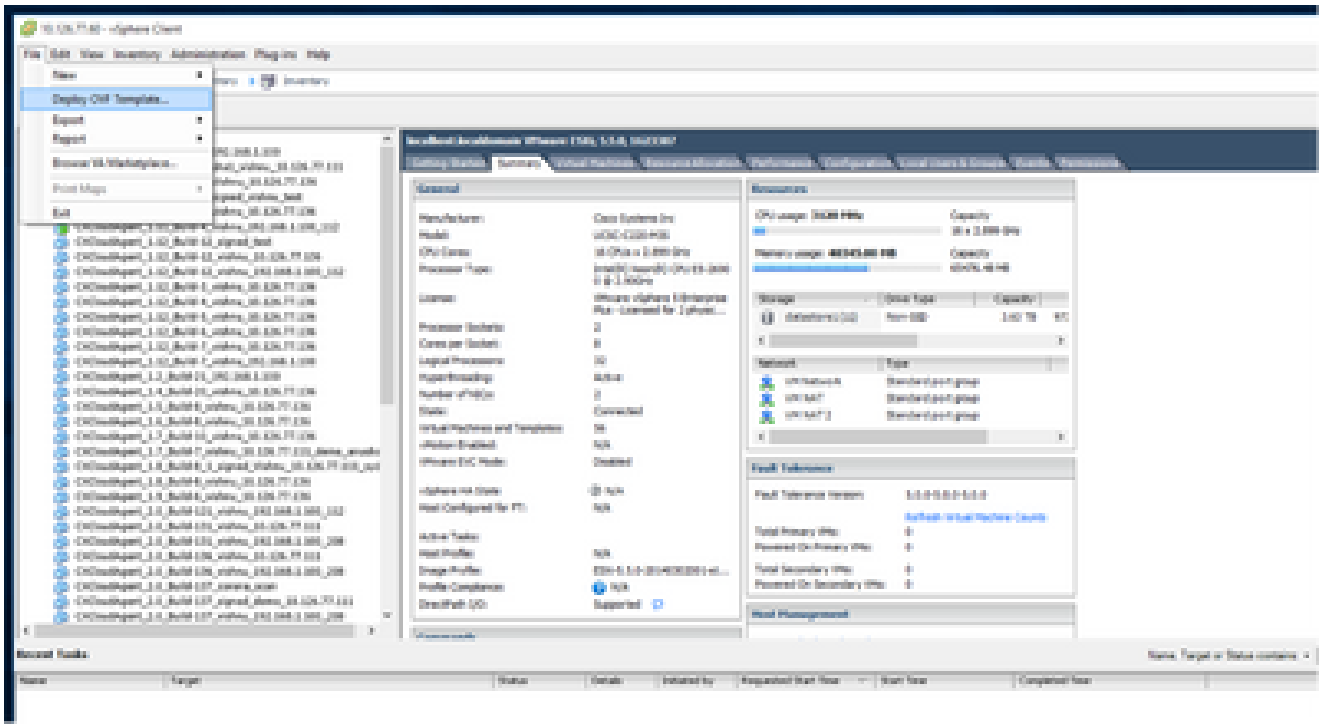
Instalación de Thick Client ESXi 5.5/6.0

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

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

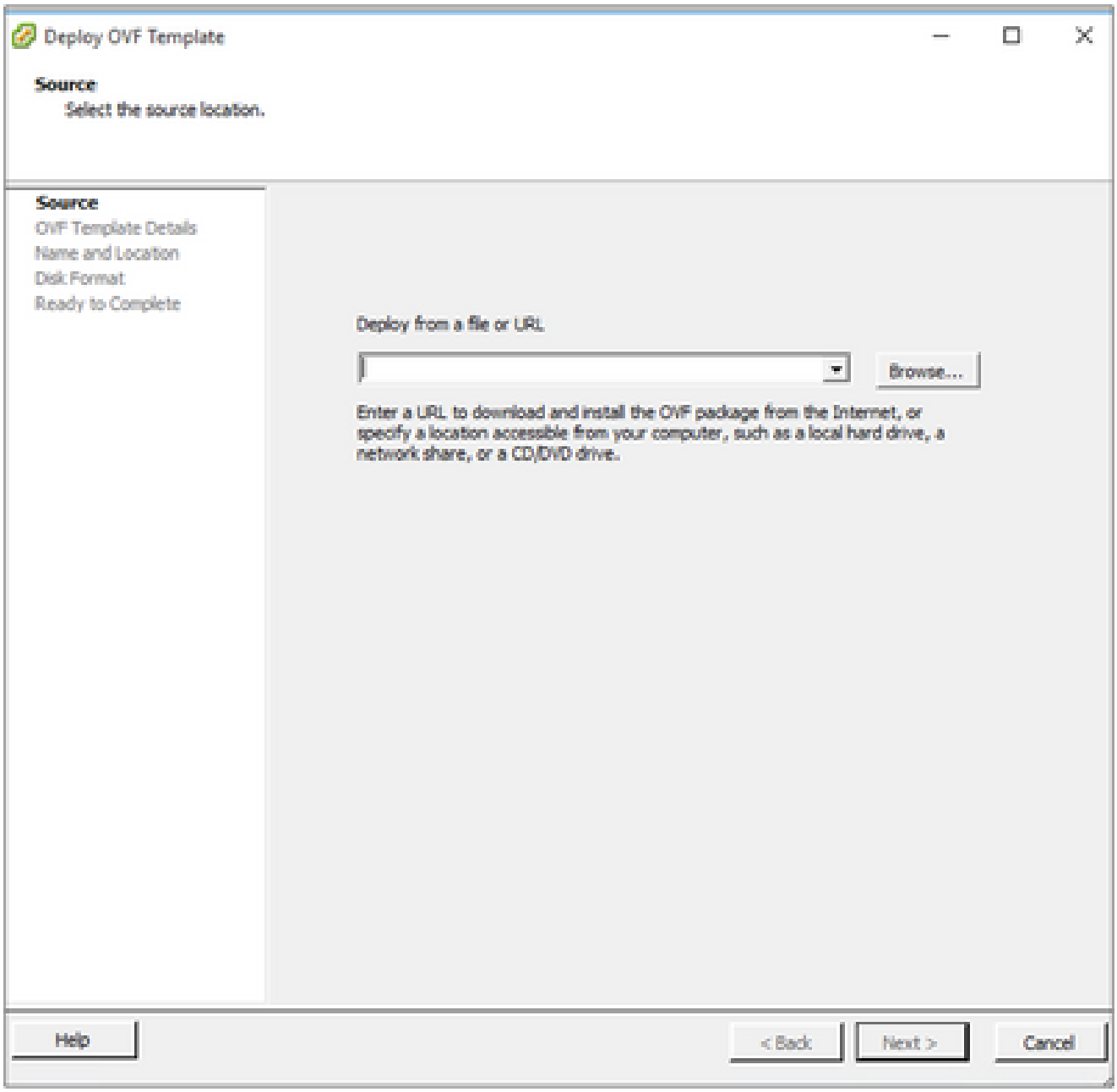
Inicio de sesión

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



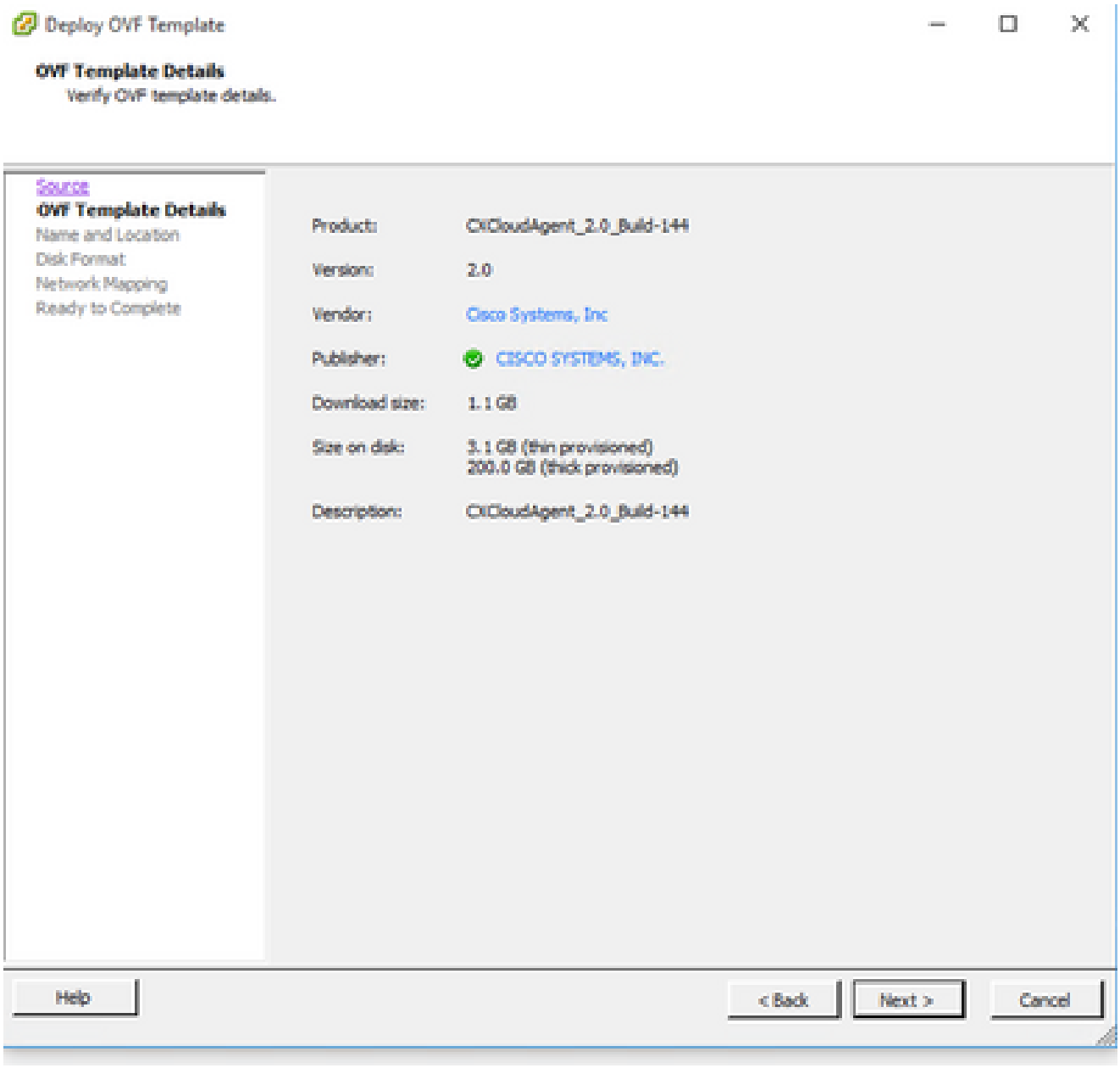
Cliente vSphere

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



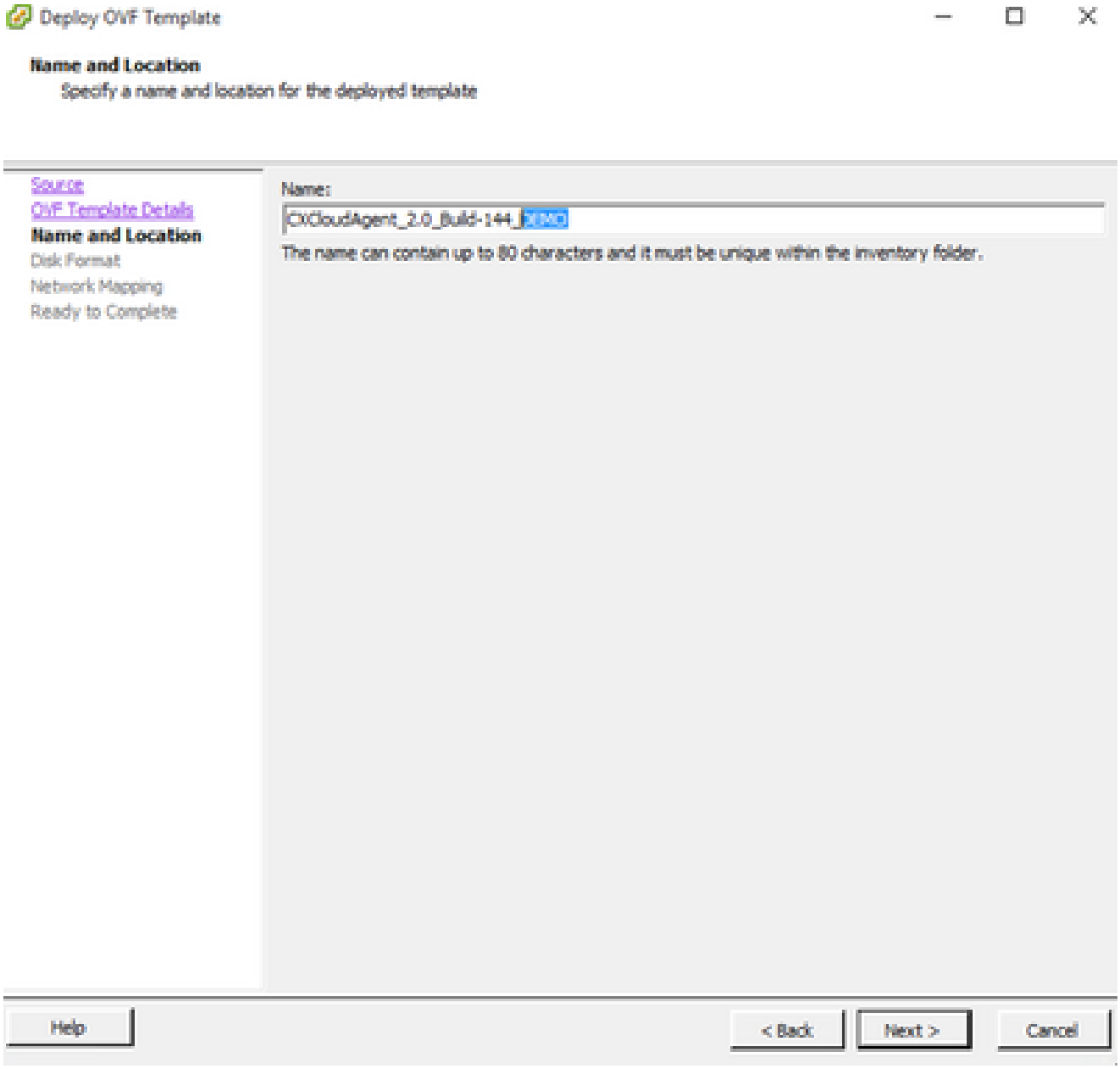
Ruta OVA

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



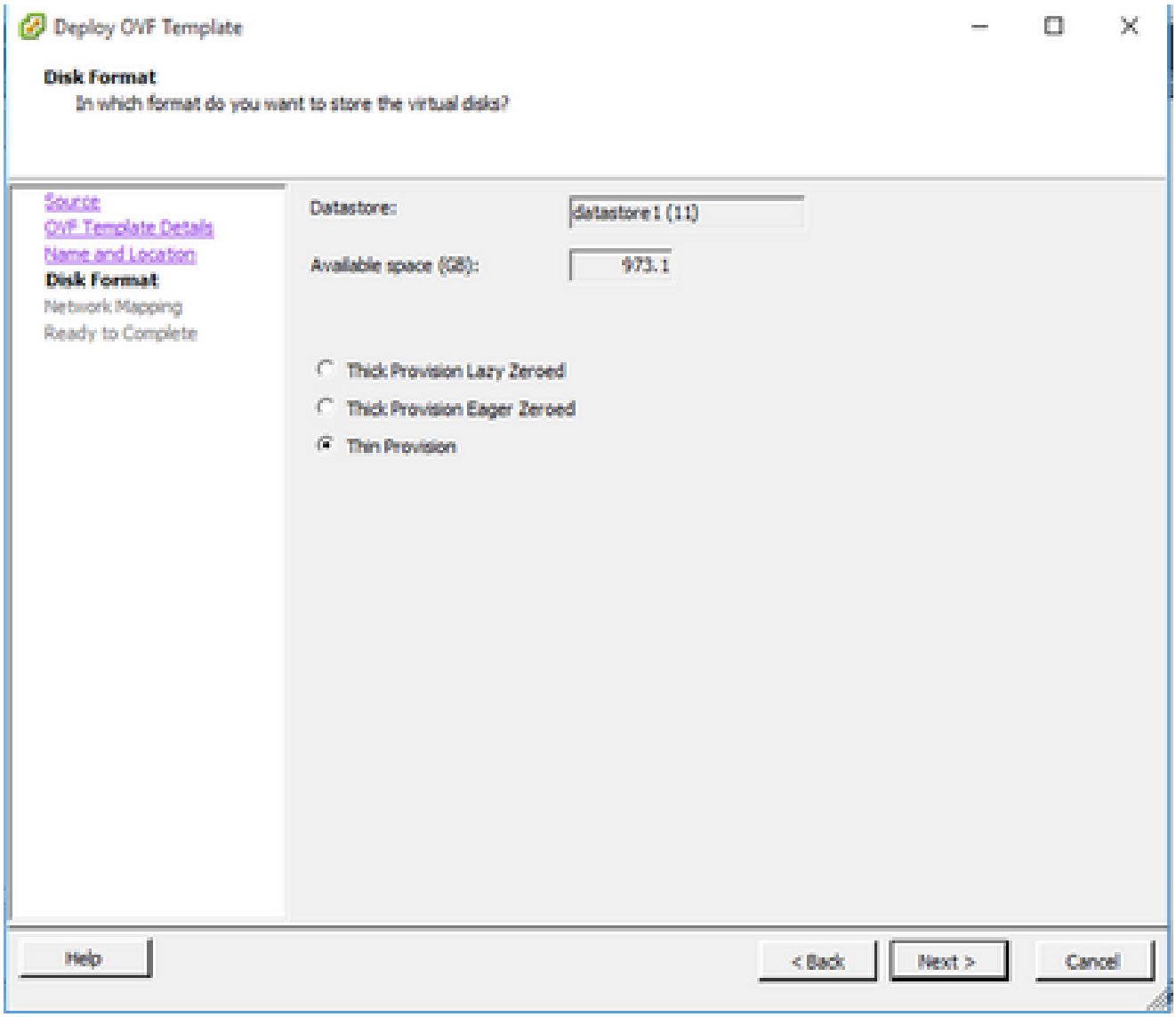
Detalles de plantilla

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



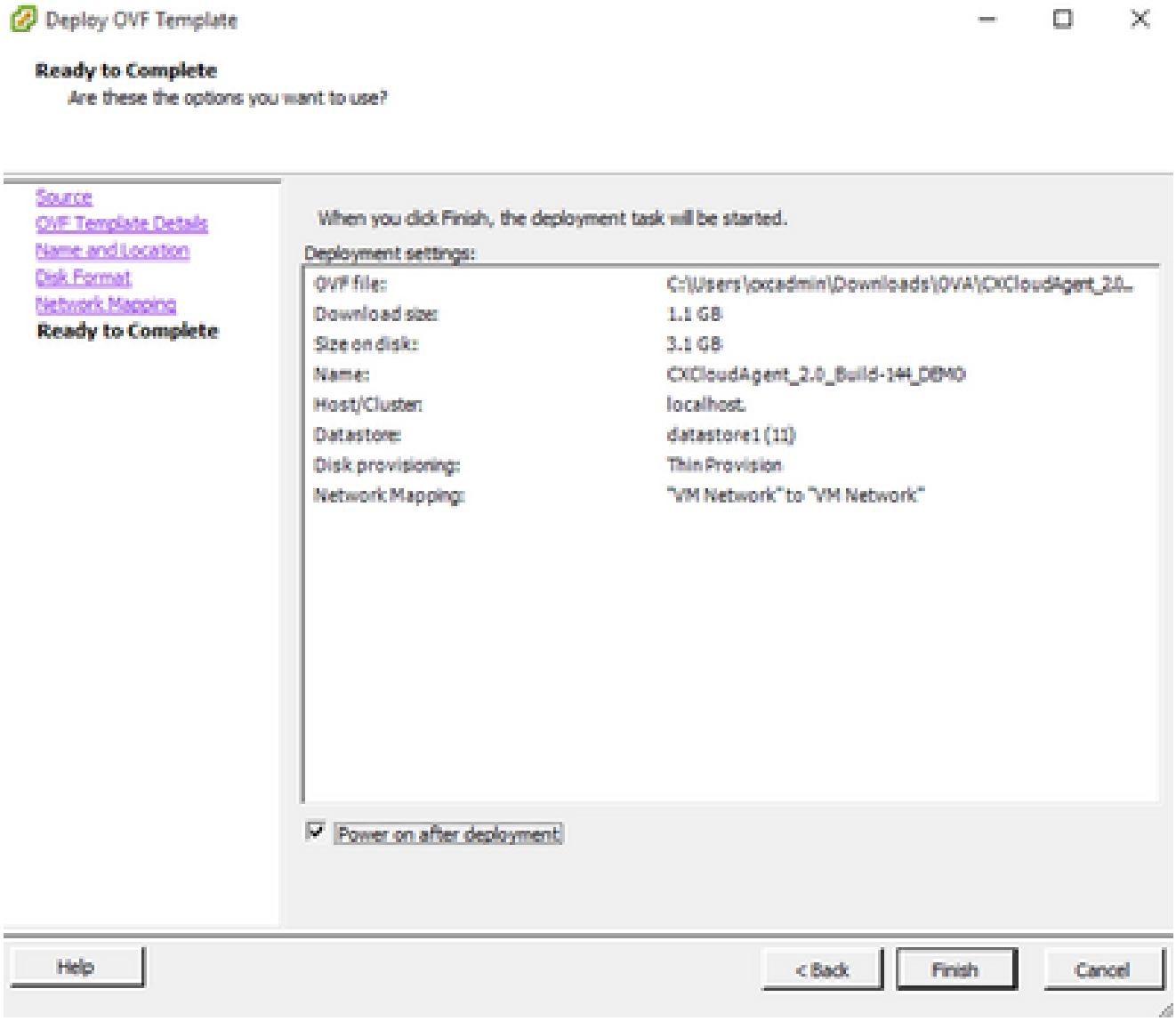
Nombre y ubicación

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



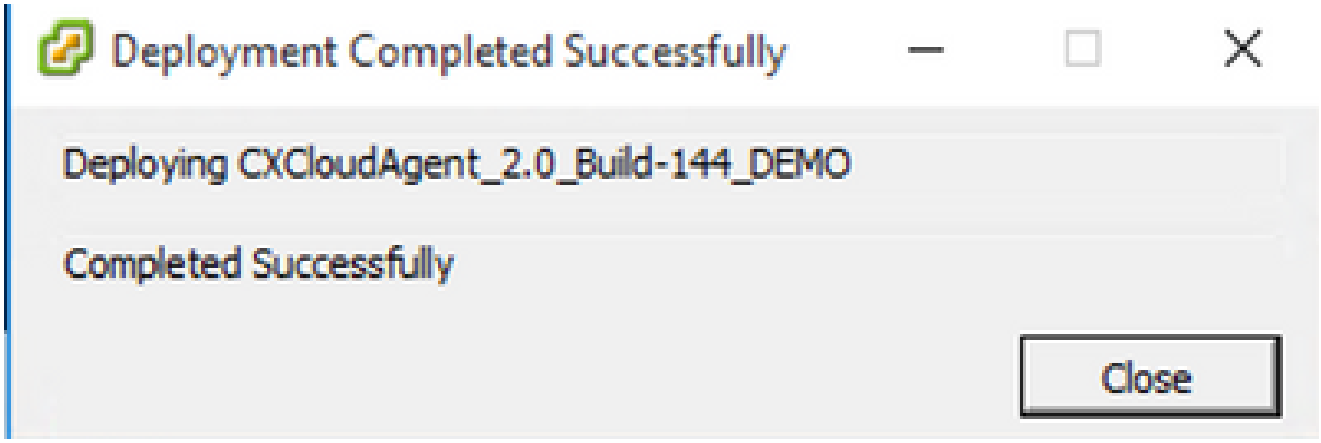
Formato de disco

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

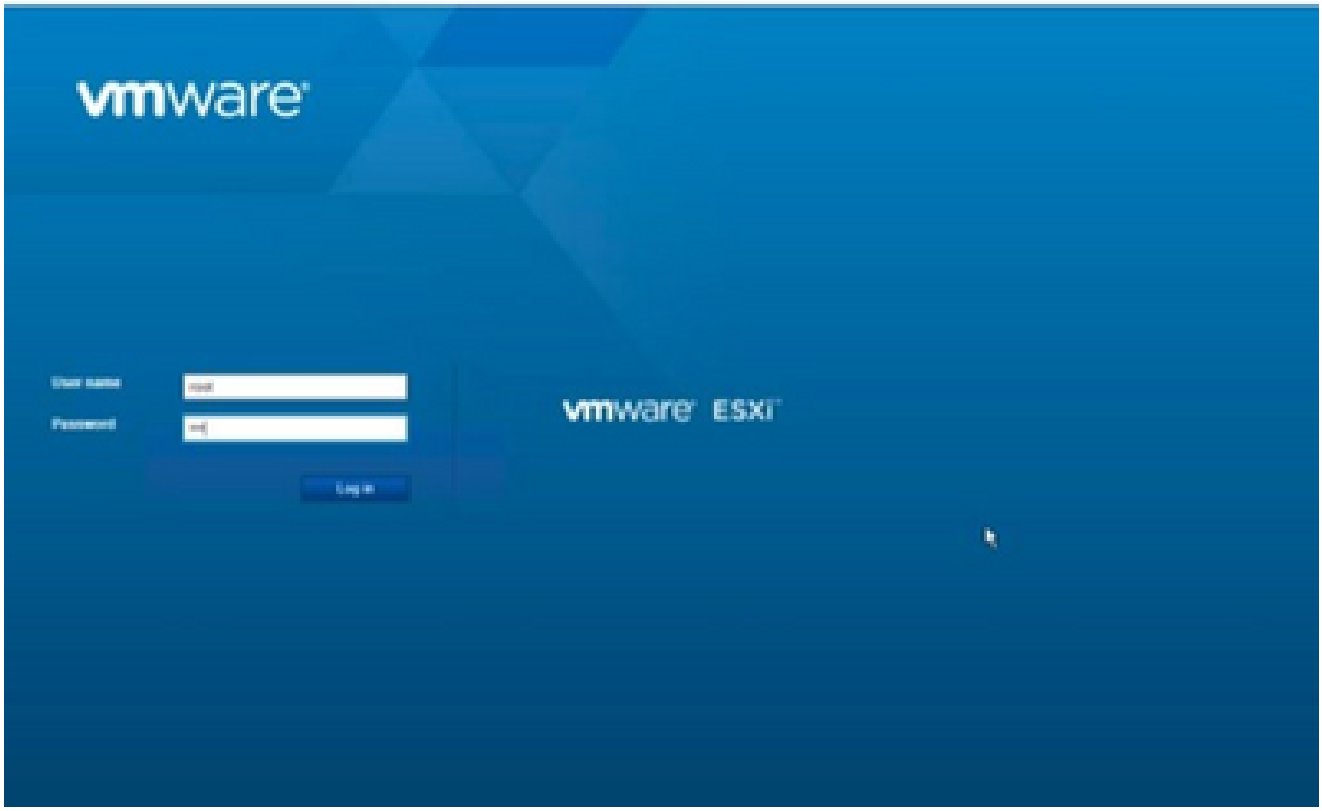
8. Seleccione la VM implementada, abra la consola y vaya a Configuración de red para

continuar con los siguientes pasos.

Instalación del cliente web ESXi 6.0

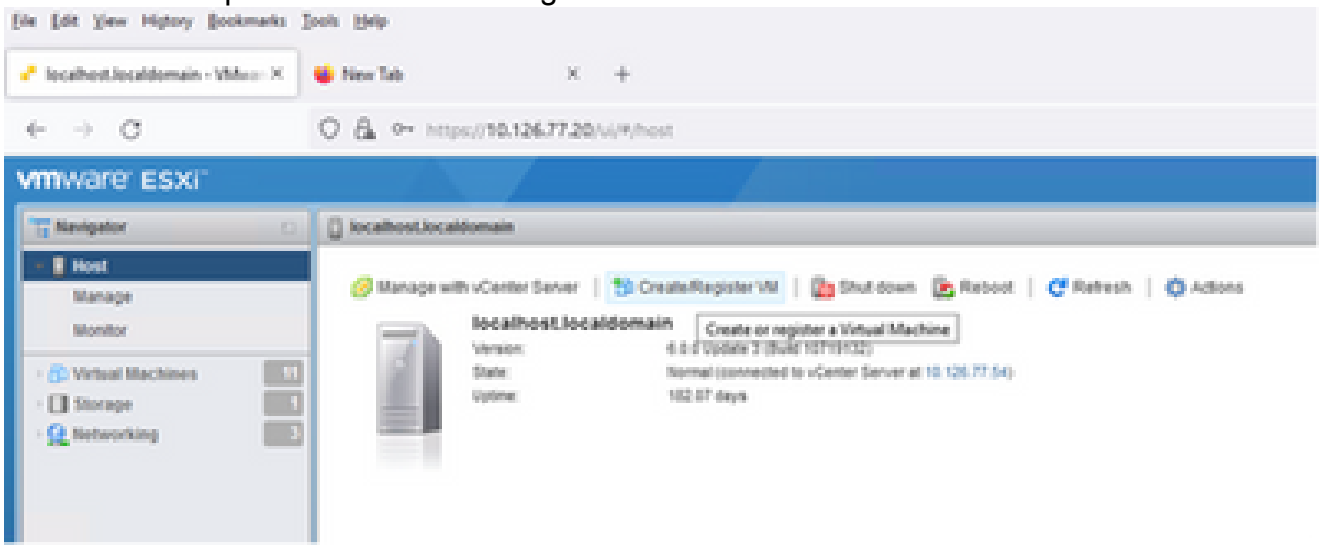
Este cliente implementa OVA de CX Cloud Agent mediante la Web de vSphere.

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



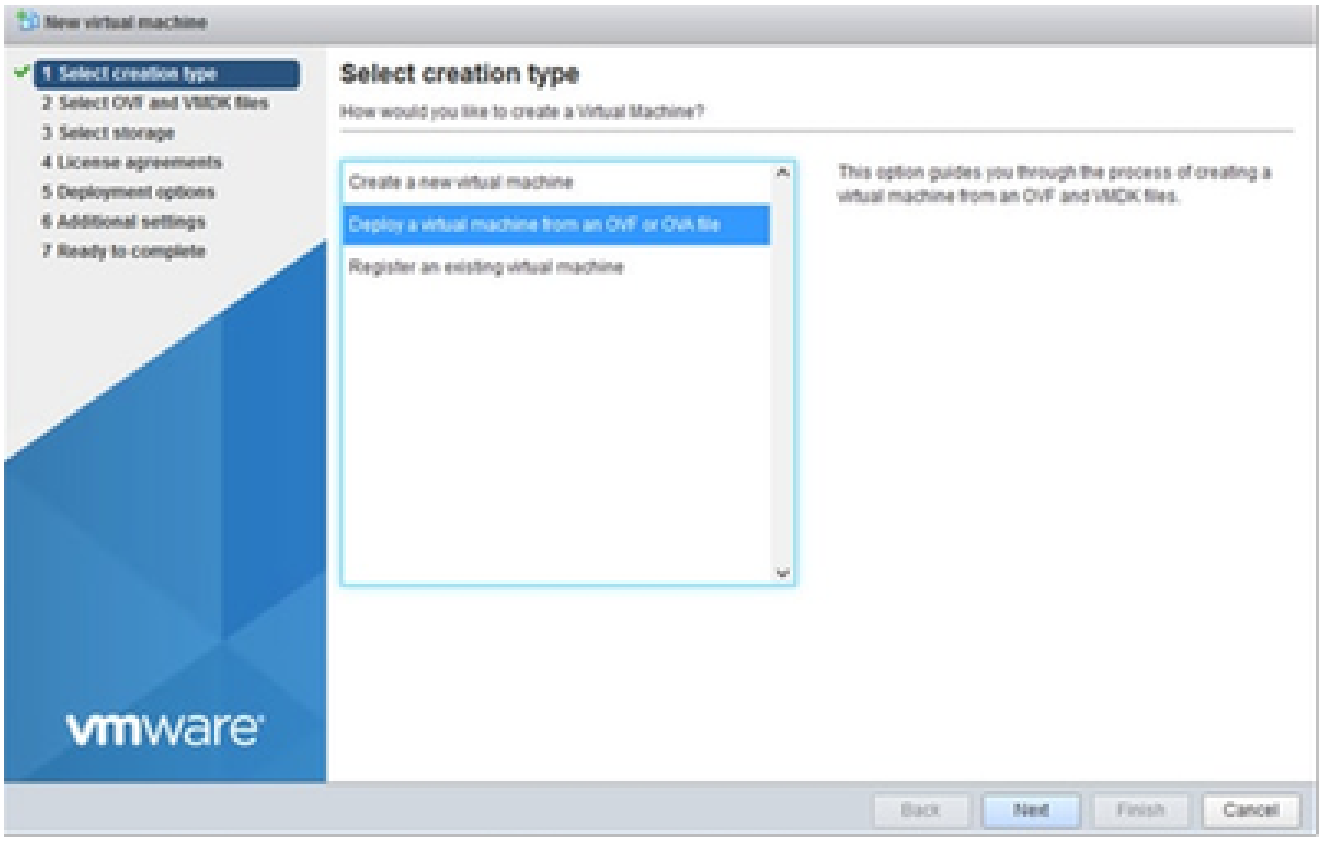
Conexión a VMWare ESXi

2. Seleccione Máquina virtual > Crear/registrar VM.



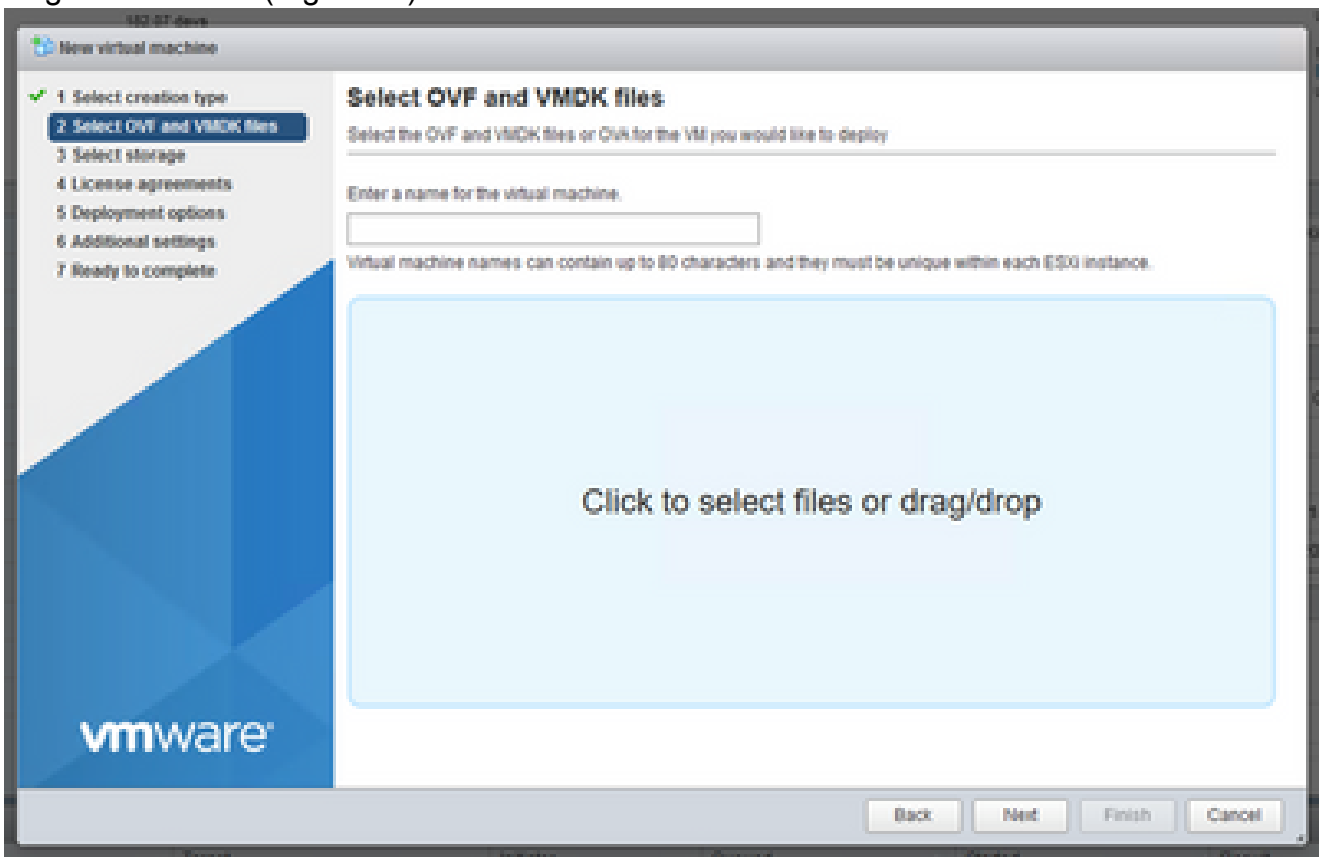
Crear VM

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



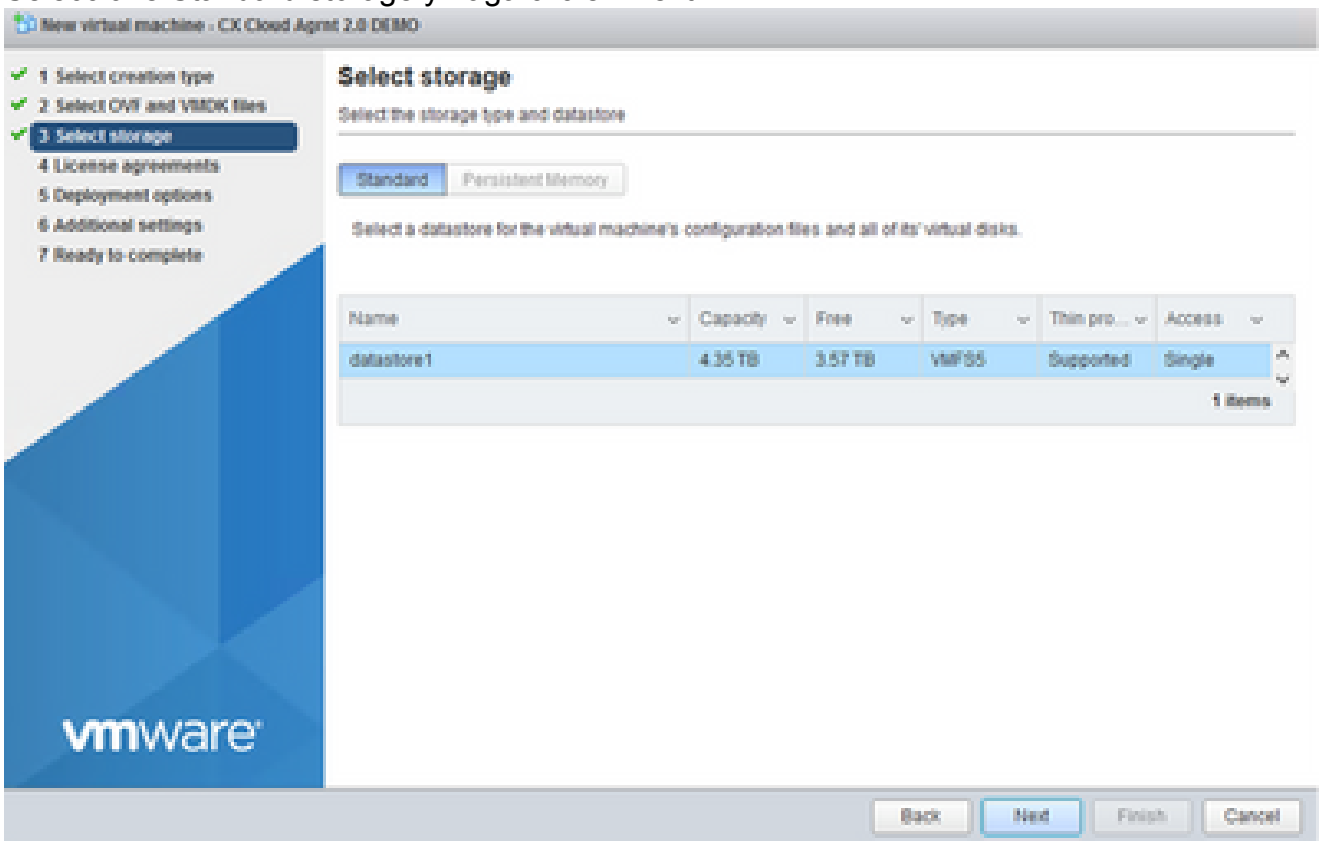
Seleccionar tipo de creación

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).



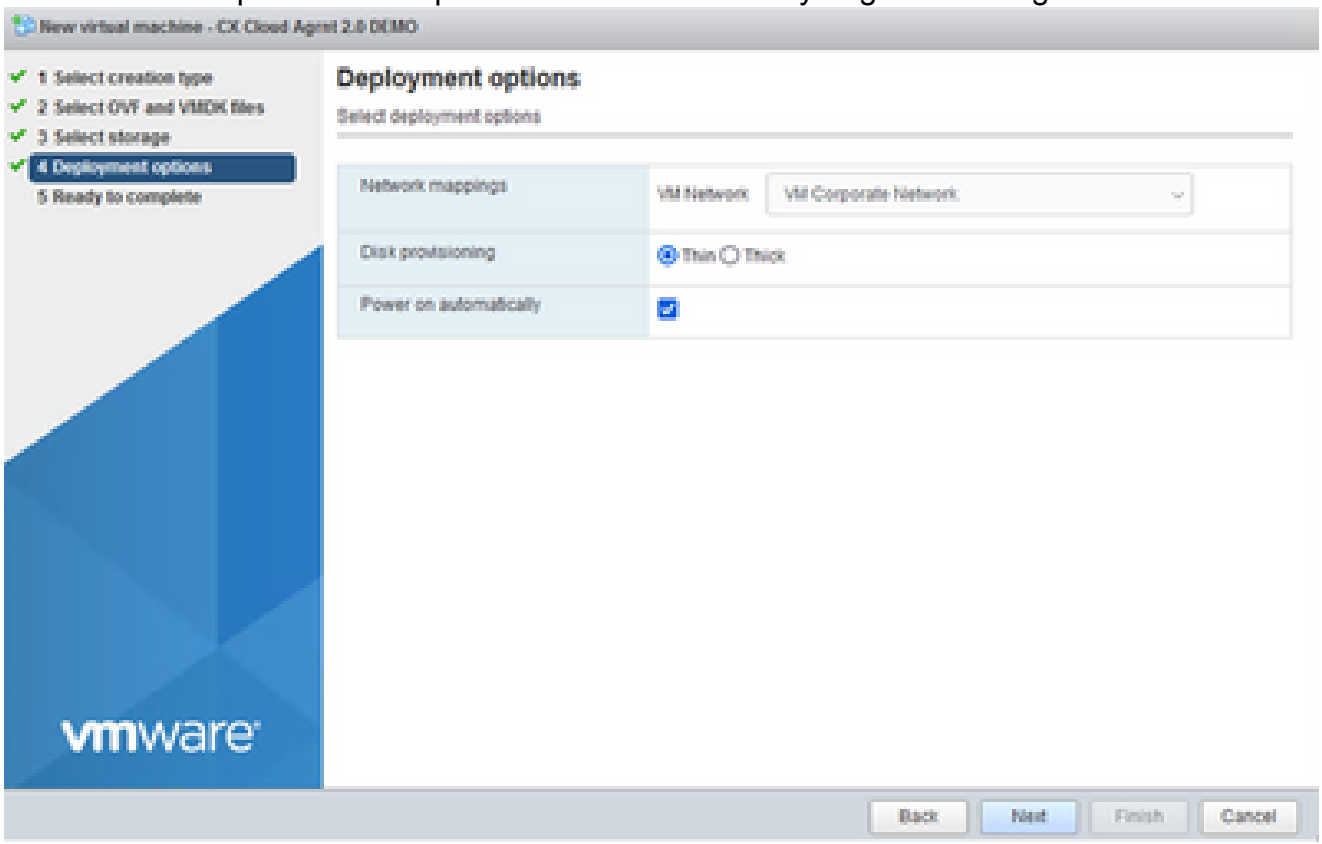
Selección de OVA

6. Seleccione Standard storage y haga clic en Next.



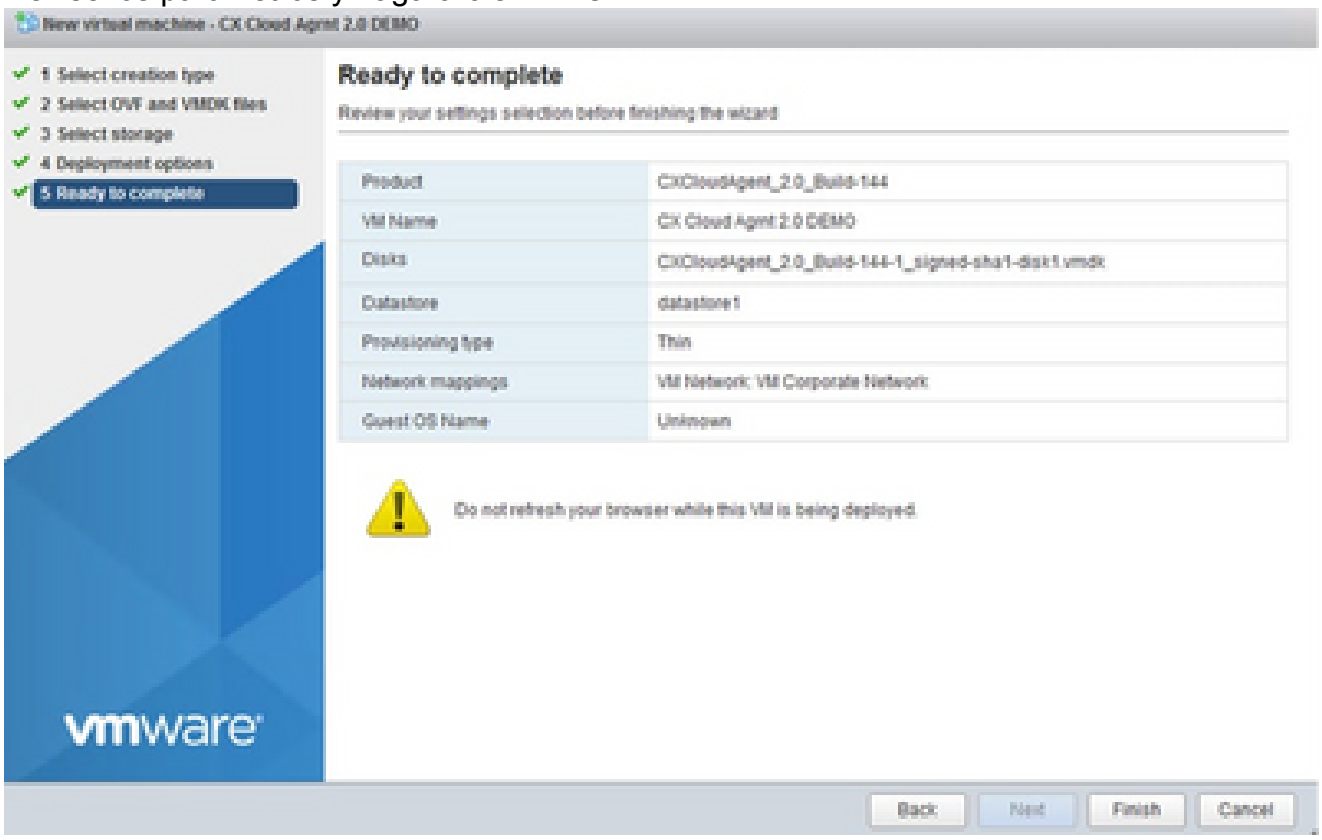
Seleccionar almacenamiento

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

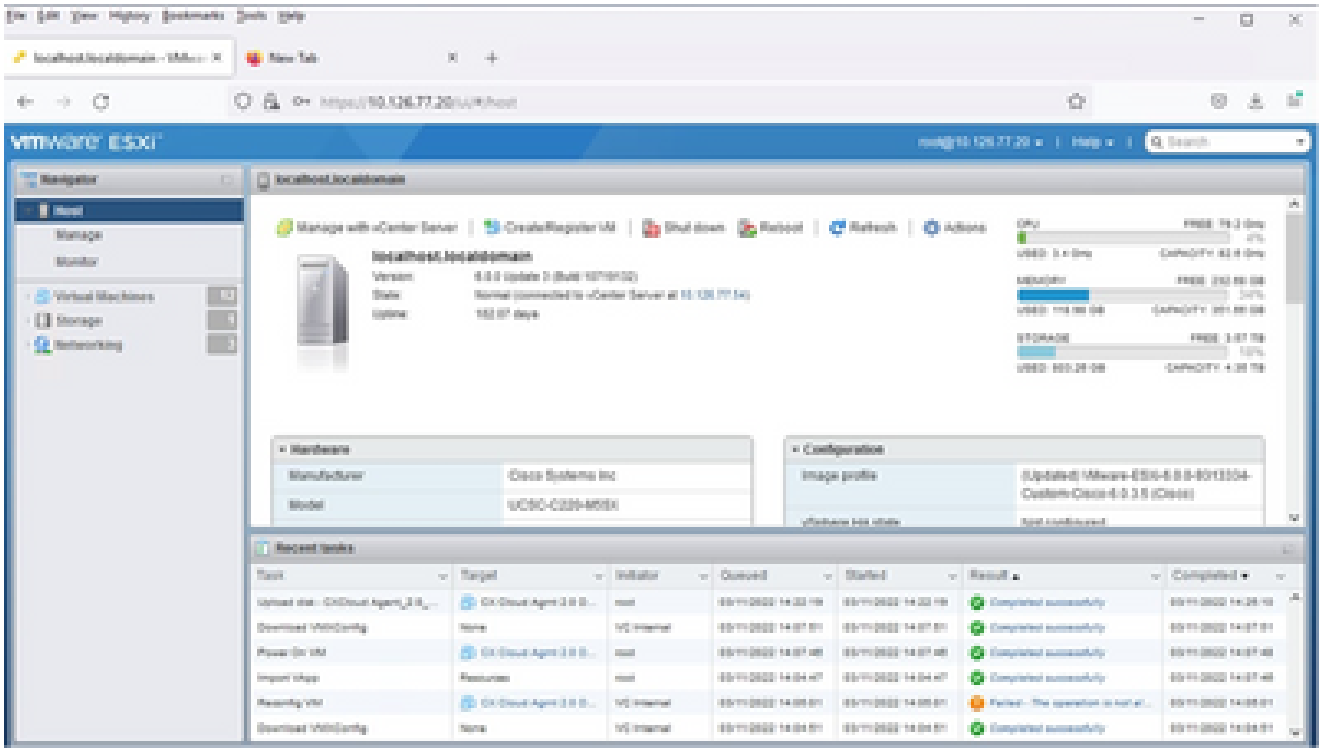


Opciones de implementación

8. Revise los parámetros y haga clic en Finish.

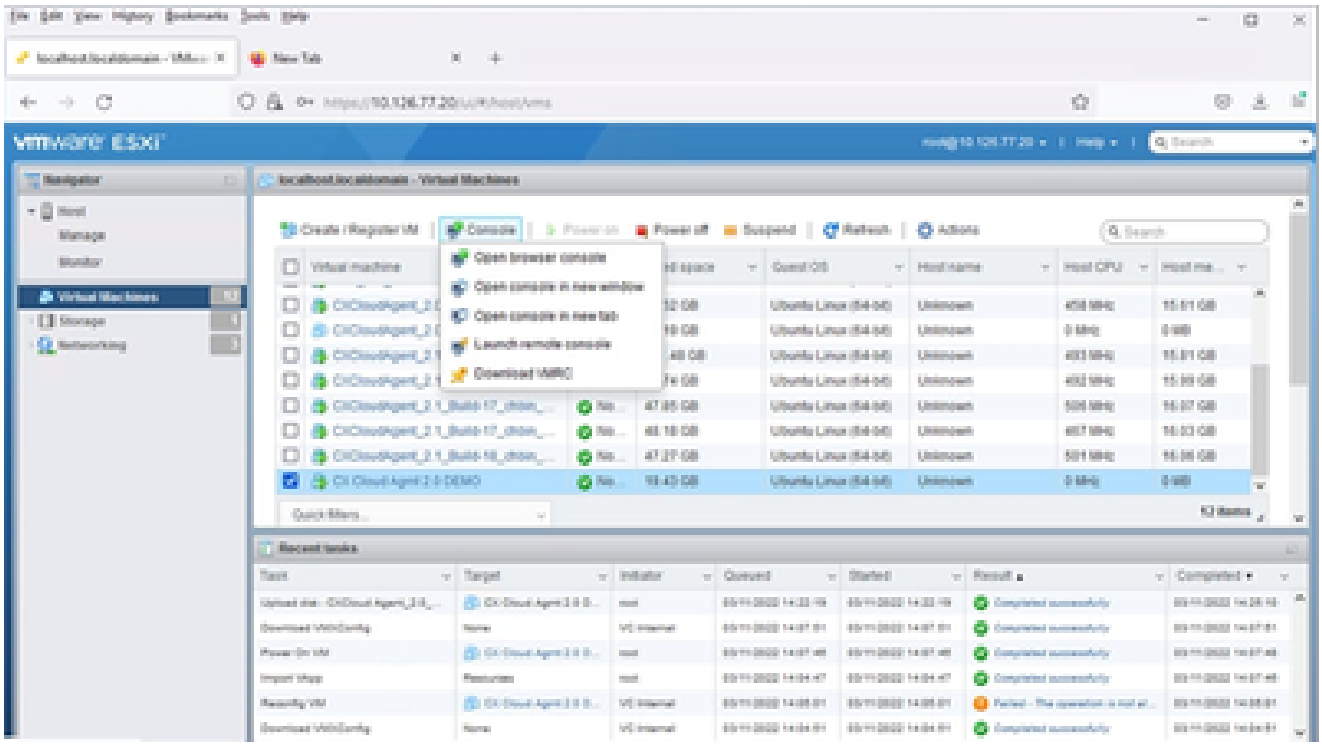


Listo para completar



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.

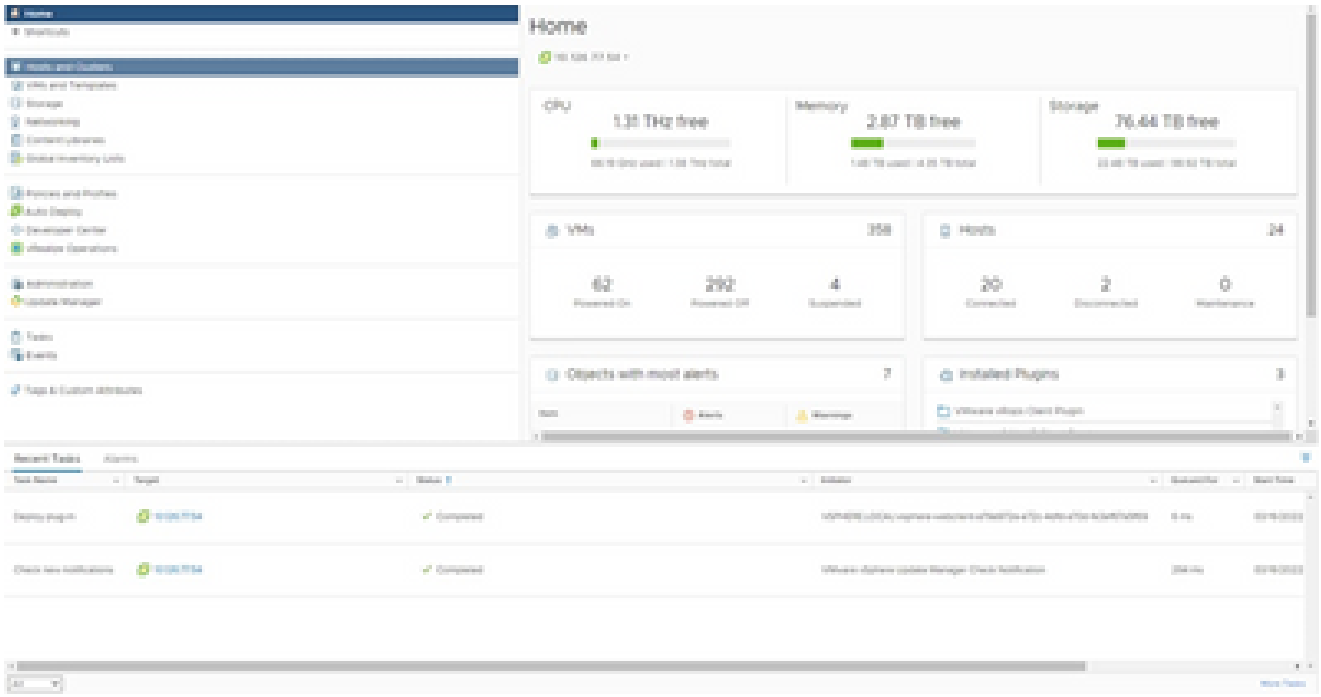
Instalación de Web Client vCenter

Siga estos pasos:

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

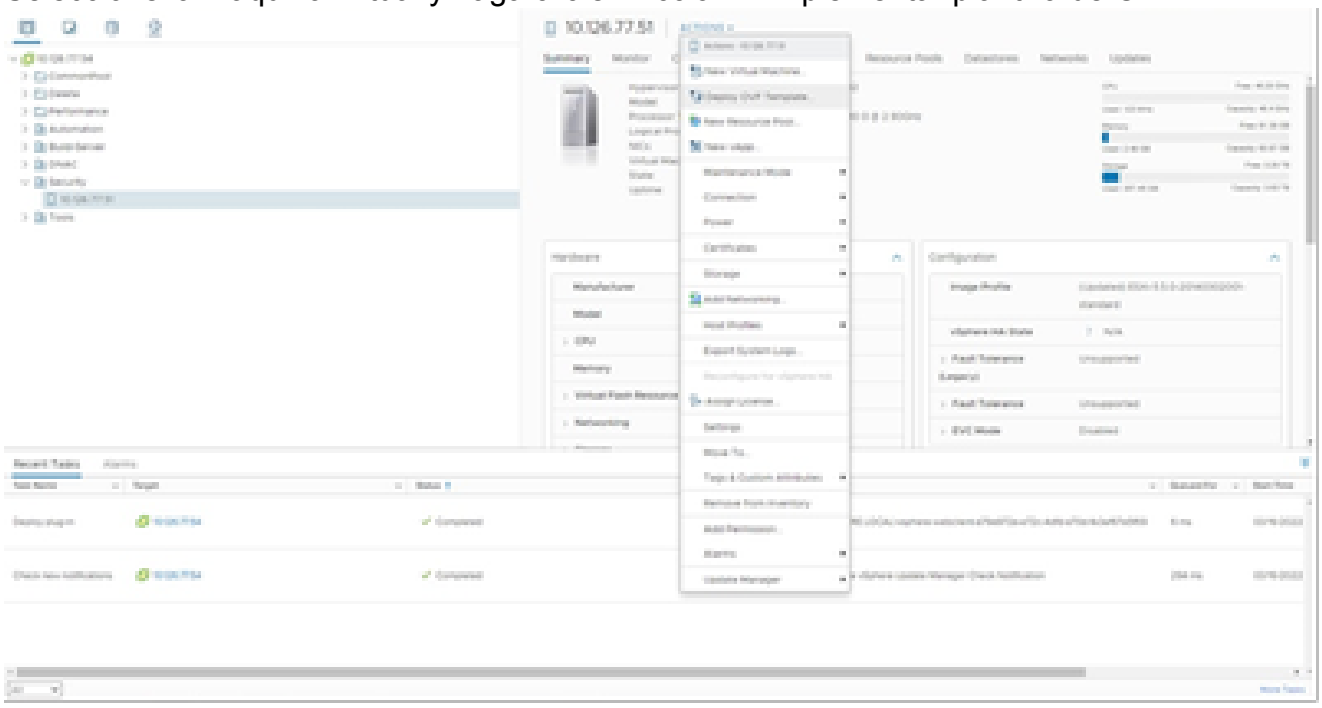
Inicie sesión

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

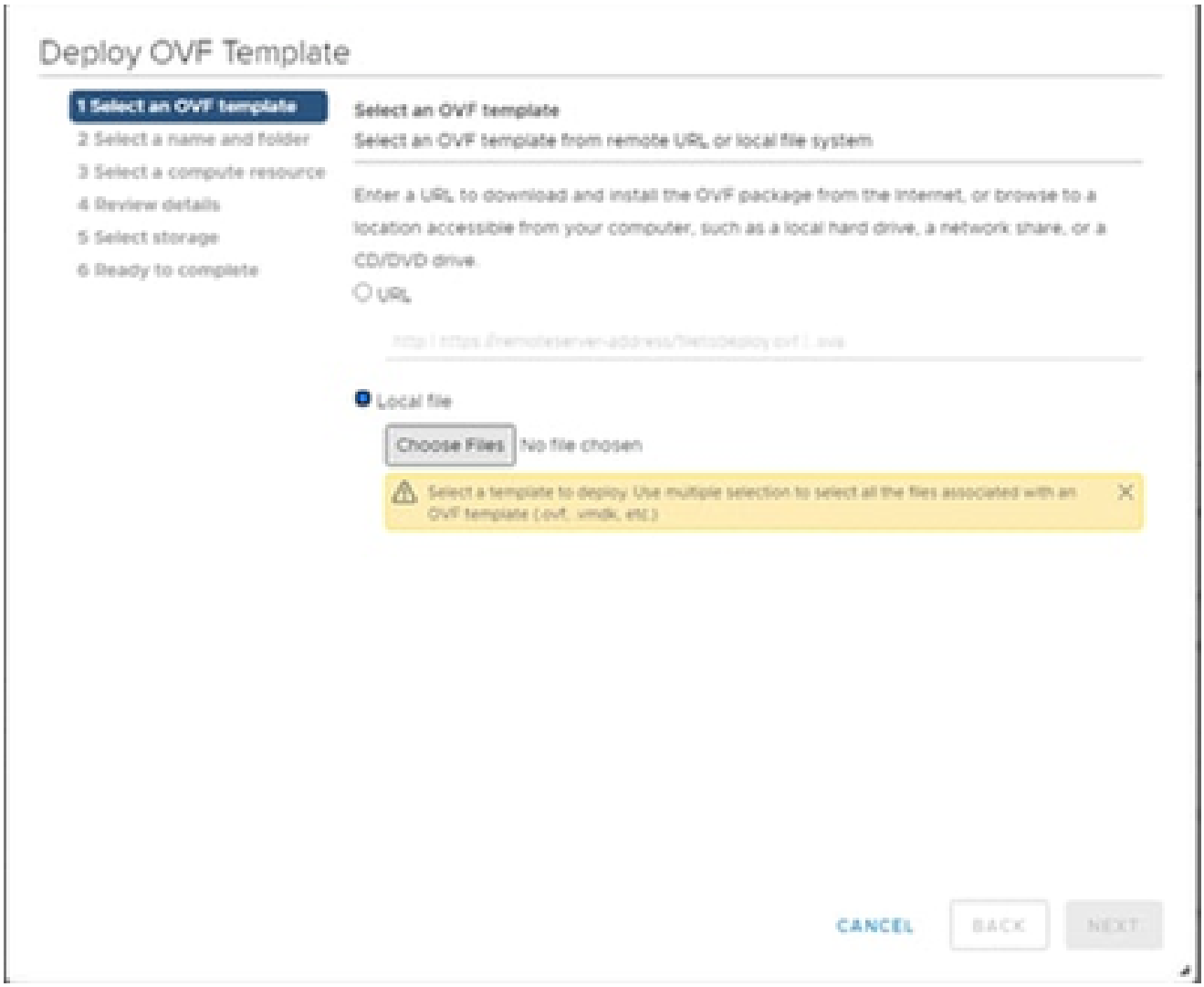


Página de inicio

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

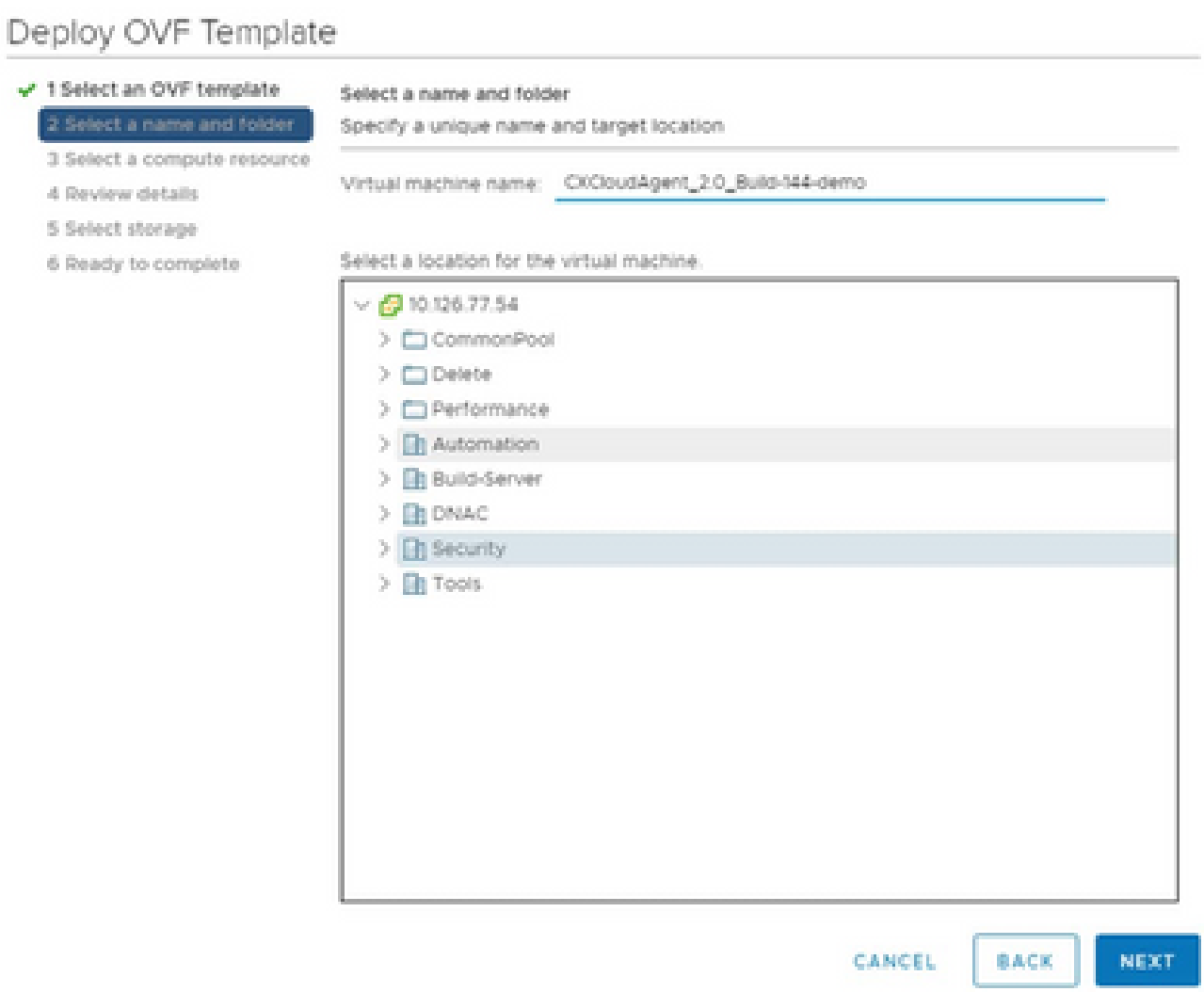


Acciones



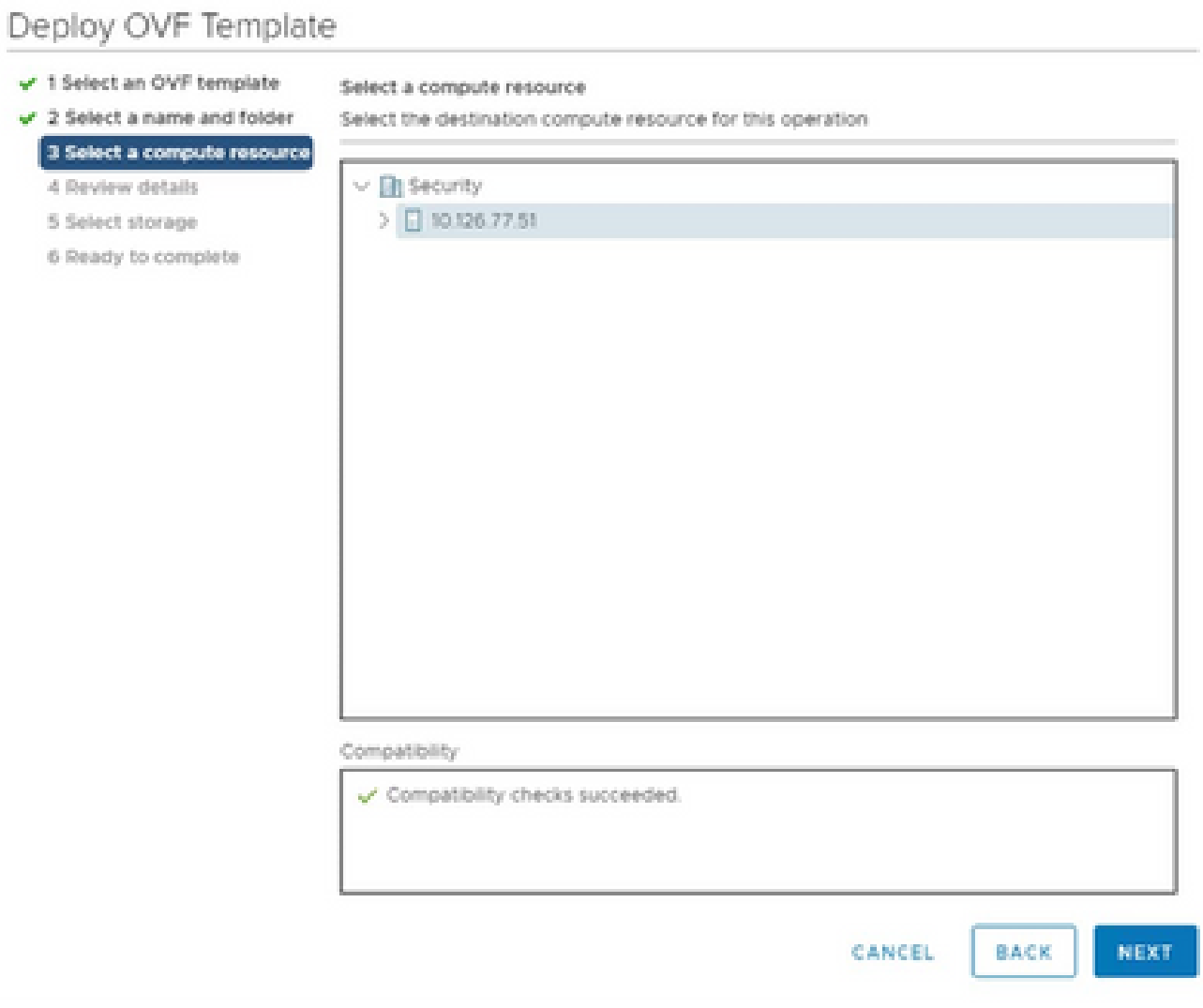
Seleccionar plantilla

4. Agregue la URL directamente o busque el archivo OVA y haga clic en Next.
5. Introduzca un nombre único y navegue hasta la ubicación, si fuera necesario.
6. Haga clic en Next (Siguiente).



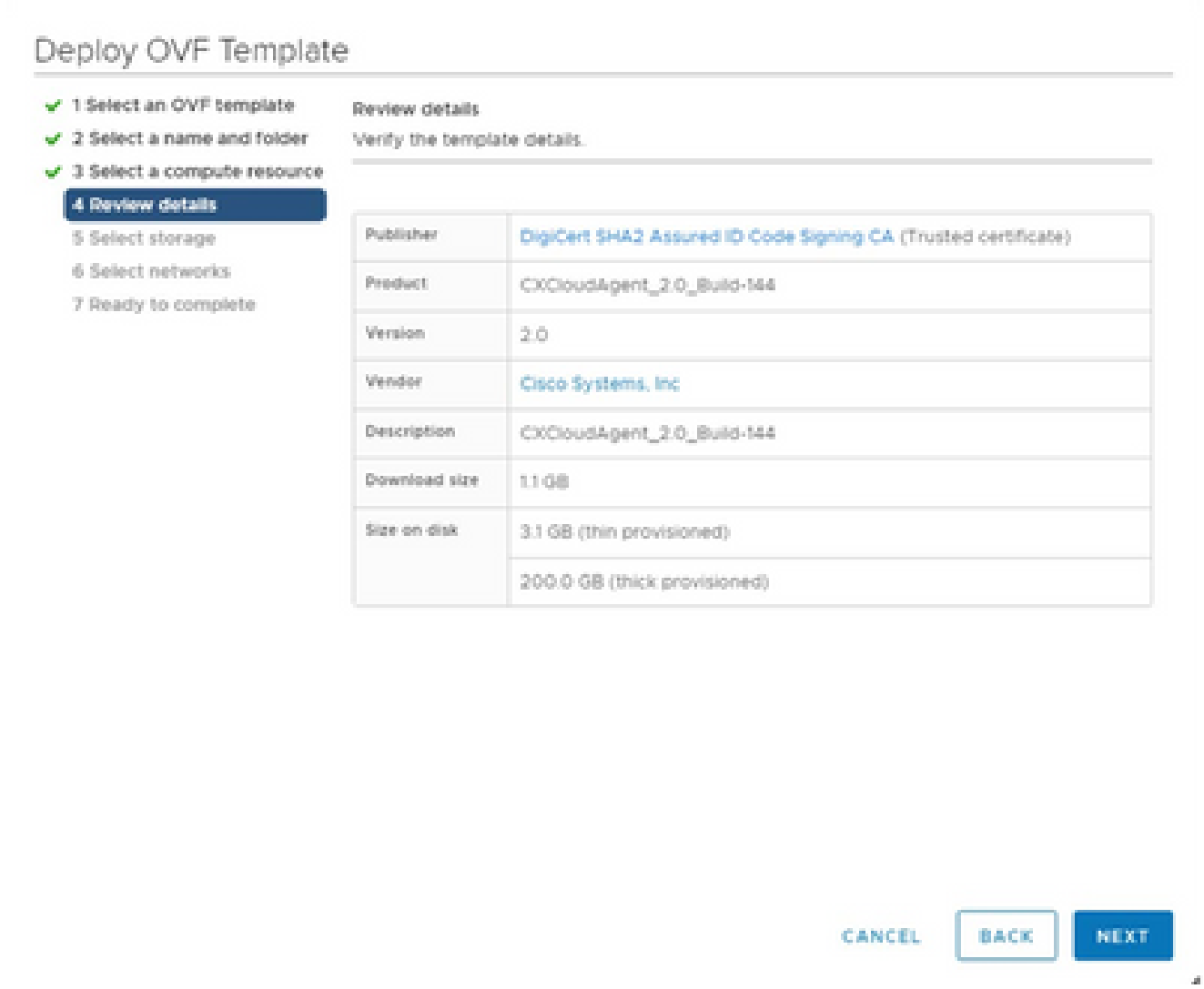
Nombre y carpeta

7. Seleccione un recurso informático y haga clic en Siguiente.



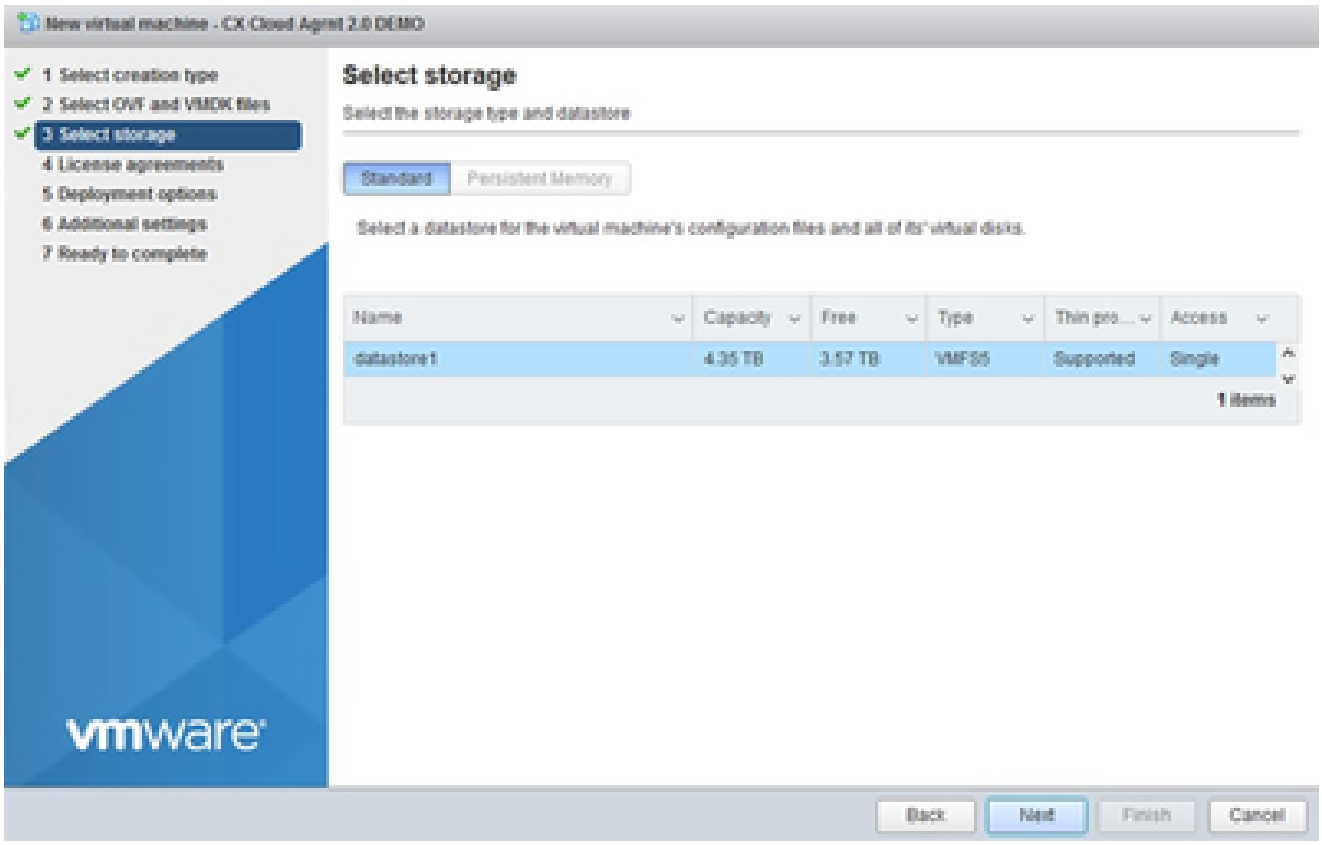
Seleccionar recurso de equipo

8. Revise los detalles y haga clic en Next.



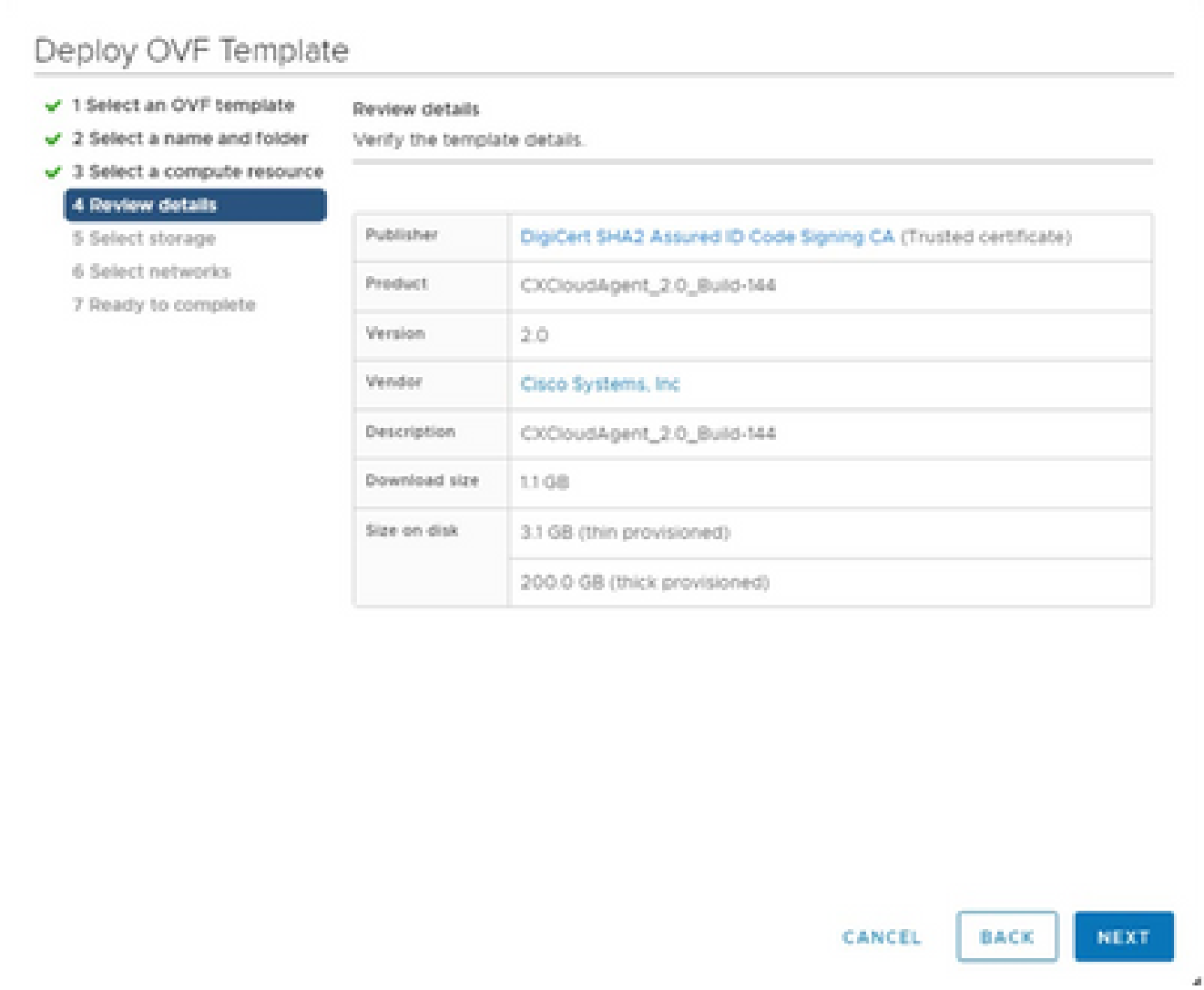
Revisar detalles

9. Seleccione el formato de disco virtual y haga clic en Next.



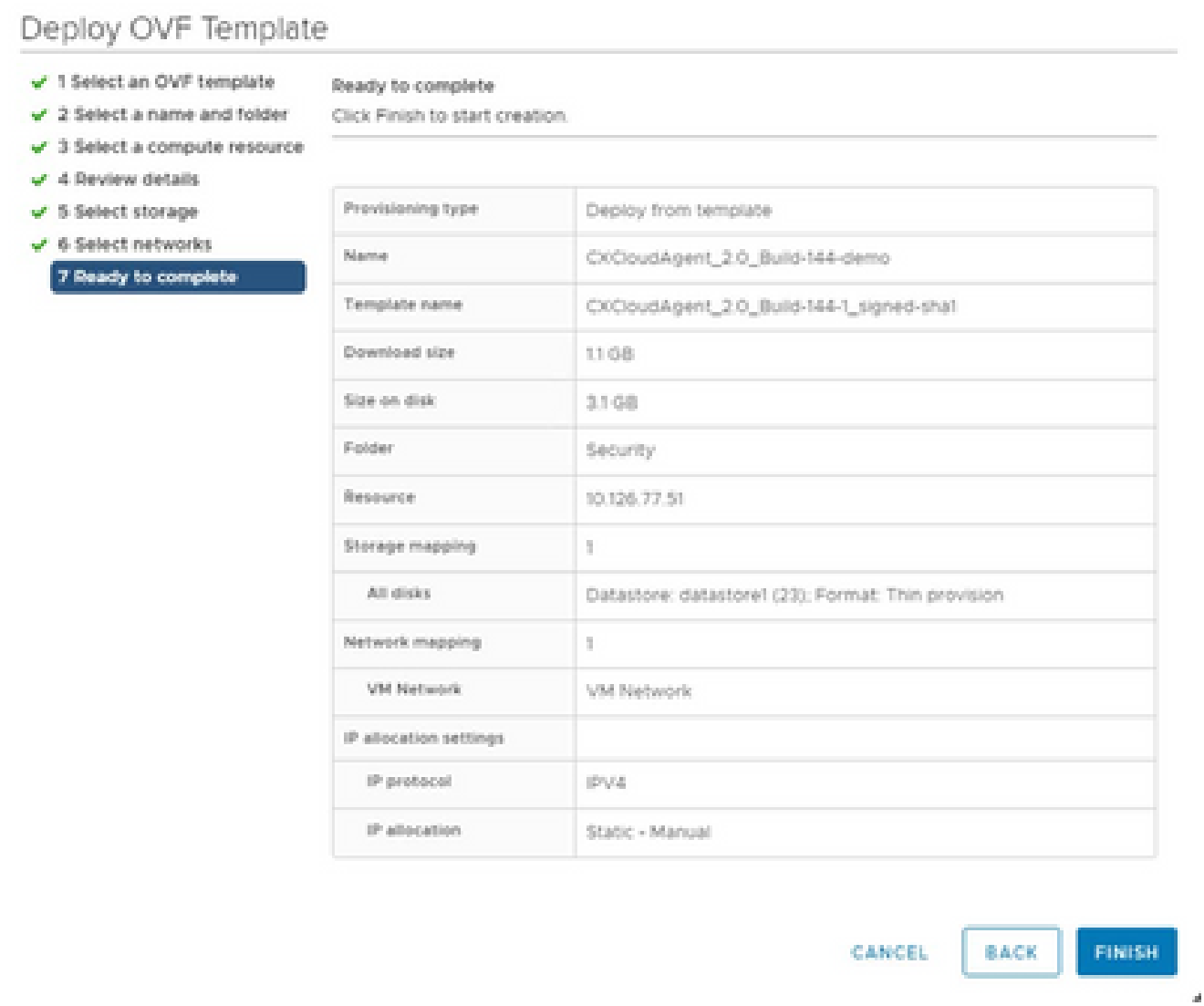
Seleccionar almacenamiento

10. Haga clic en Next (Siguiente).



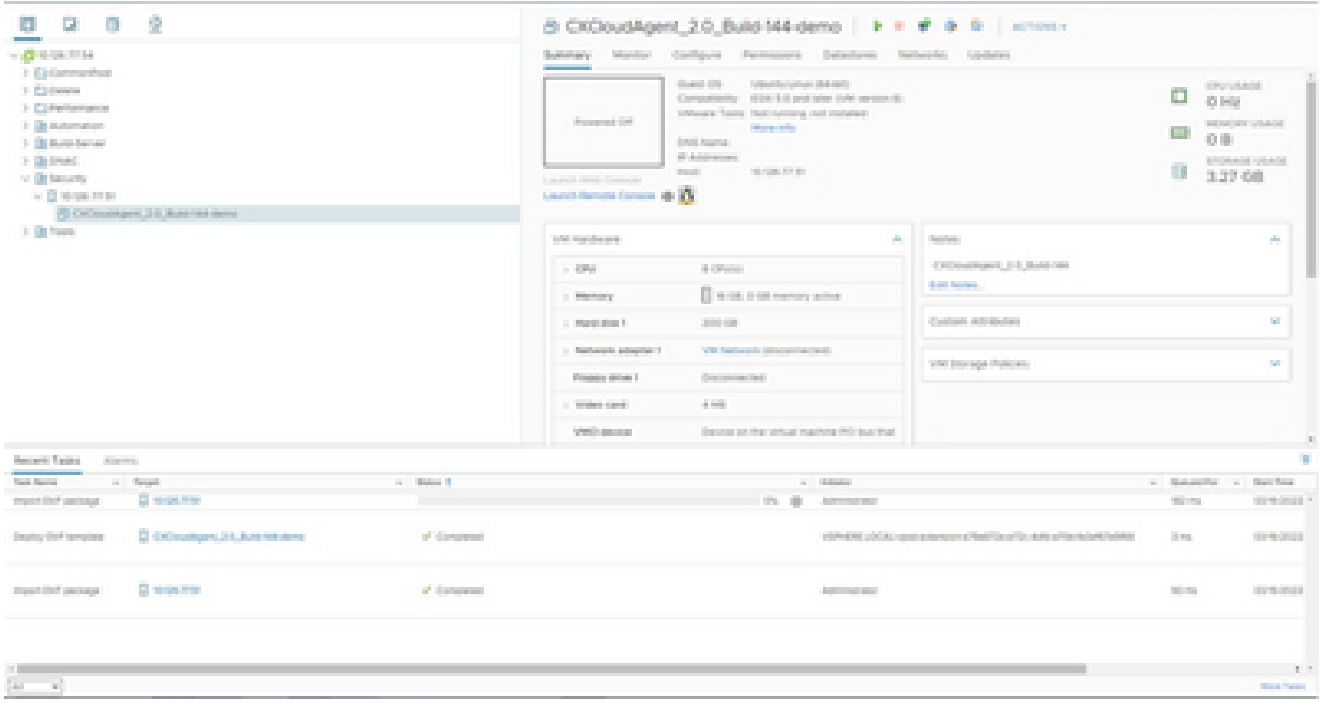
Seleccionar red

11. Haga clic en Finish (Finalizar).



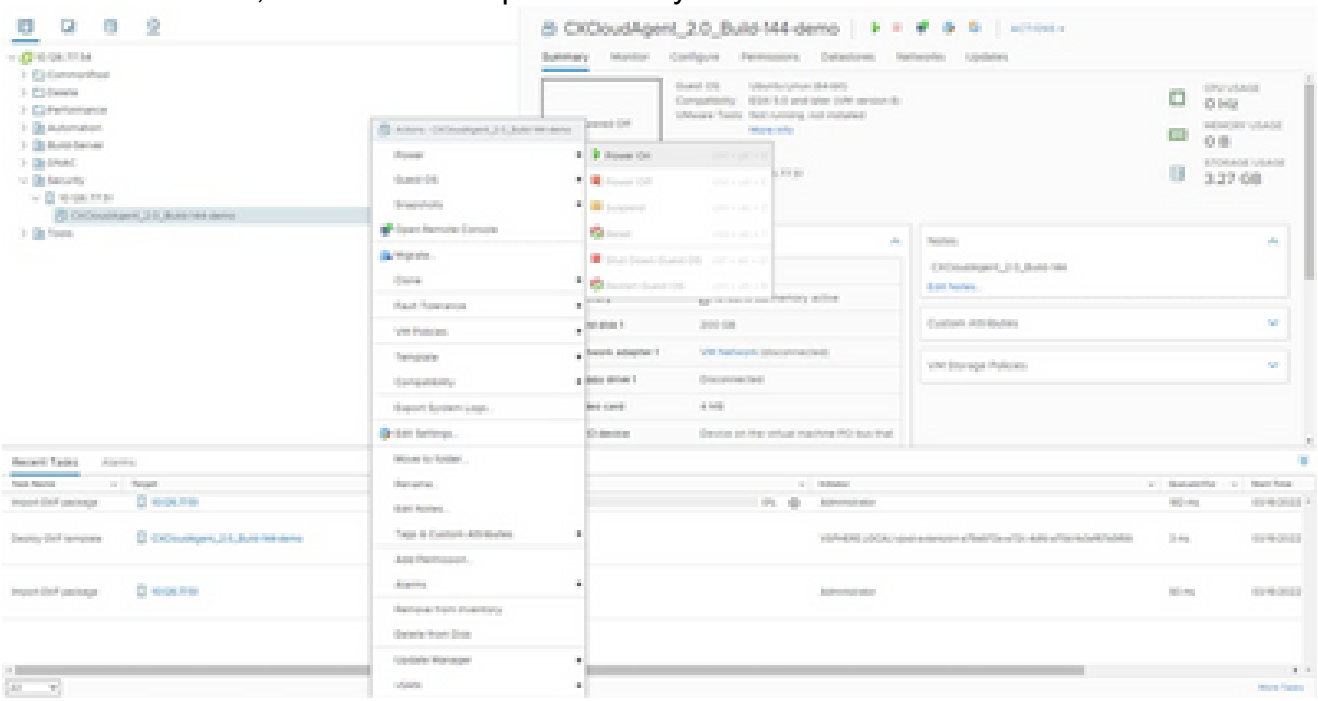
Listo para completar

12. Haga clic en el nombre de la máquina virtual recién agregada para ver el estado.



VM agregada

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



Abrir consola

14. Vaya a Network Configuration para continuar con los siguientes pasos.

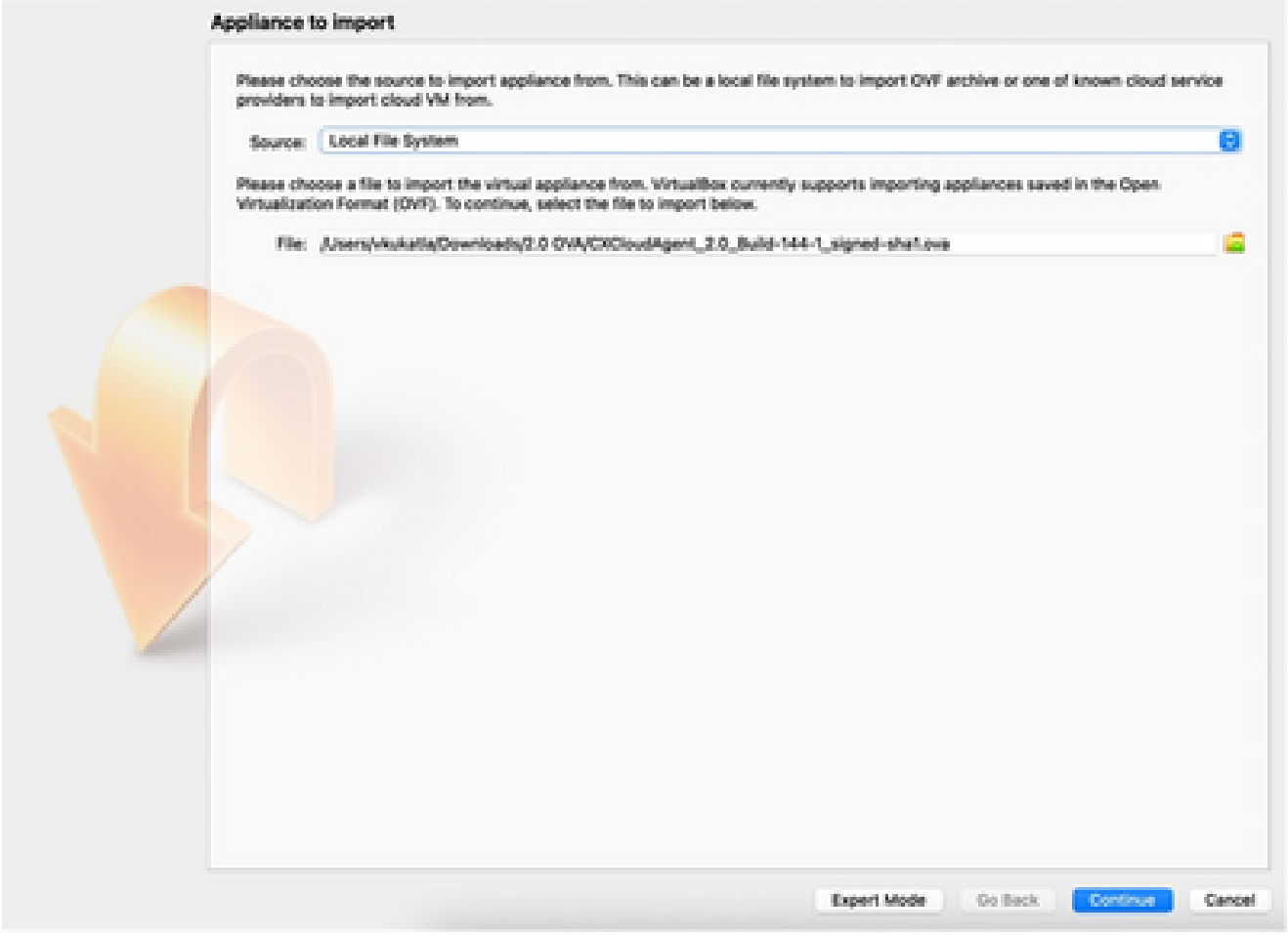
Instalación de Oracle Virtual Box 5.2.30

Este cliente implementa OVA de agente de nube CX a través de Oracle Virtual Box.

1. Abra la interfaz de usuario de Oracle VM y seleccione File> Import Appliance.

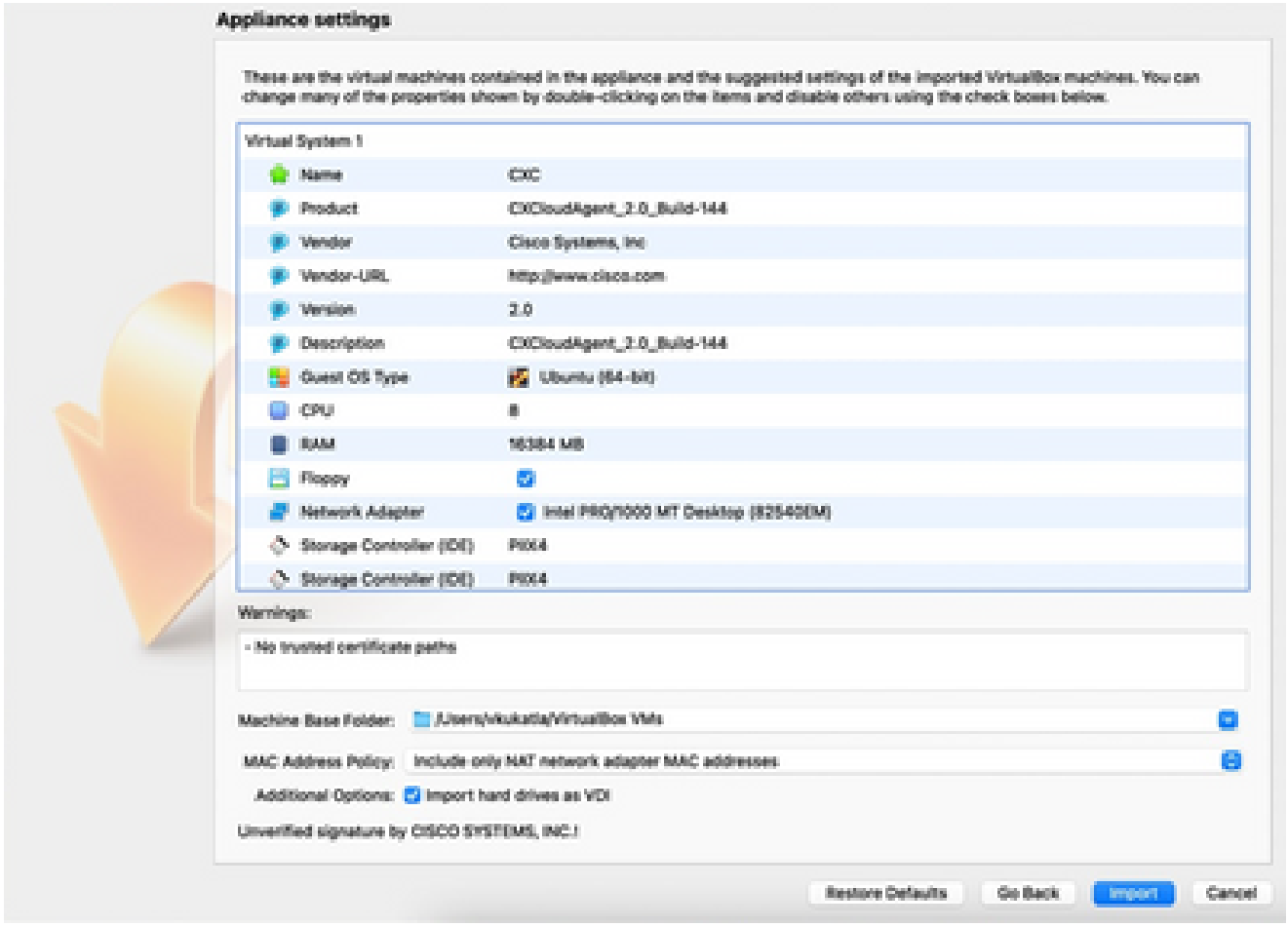
Oracle VM

2. Vaya a para importar el archivo OVA.



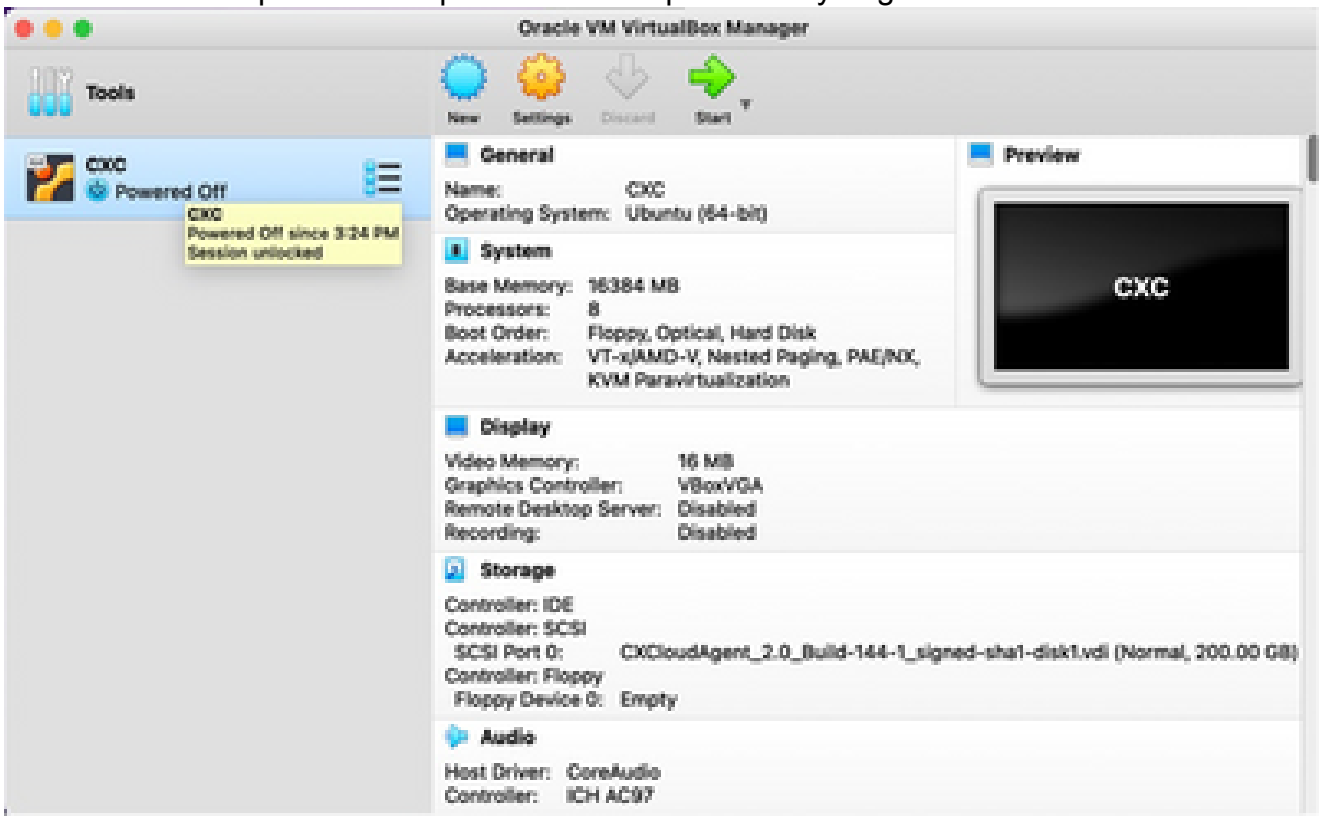
Seleccionar archivo

3. Haga clic en Importar.

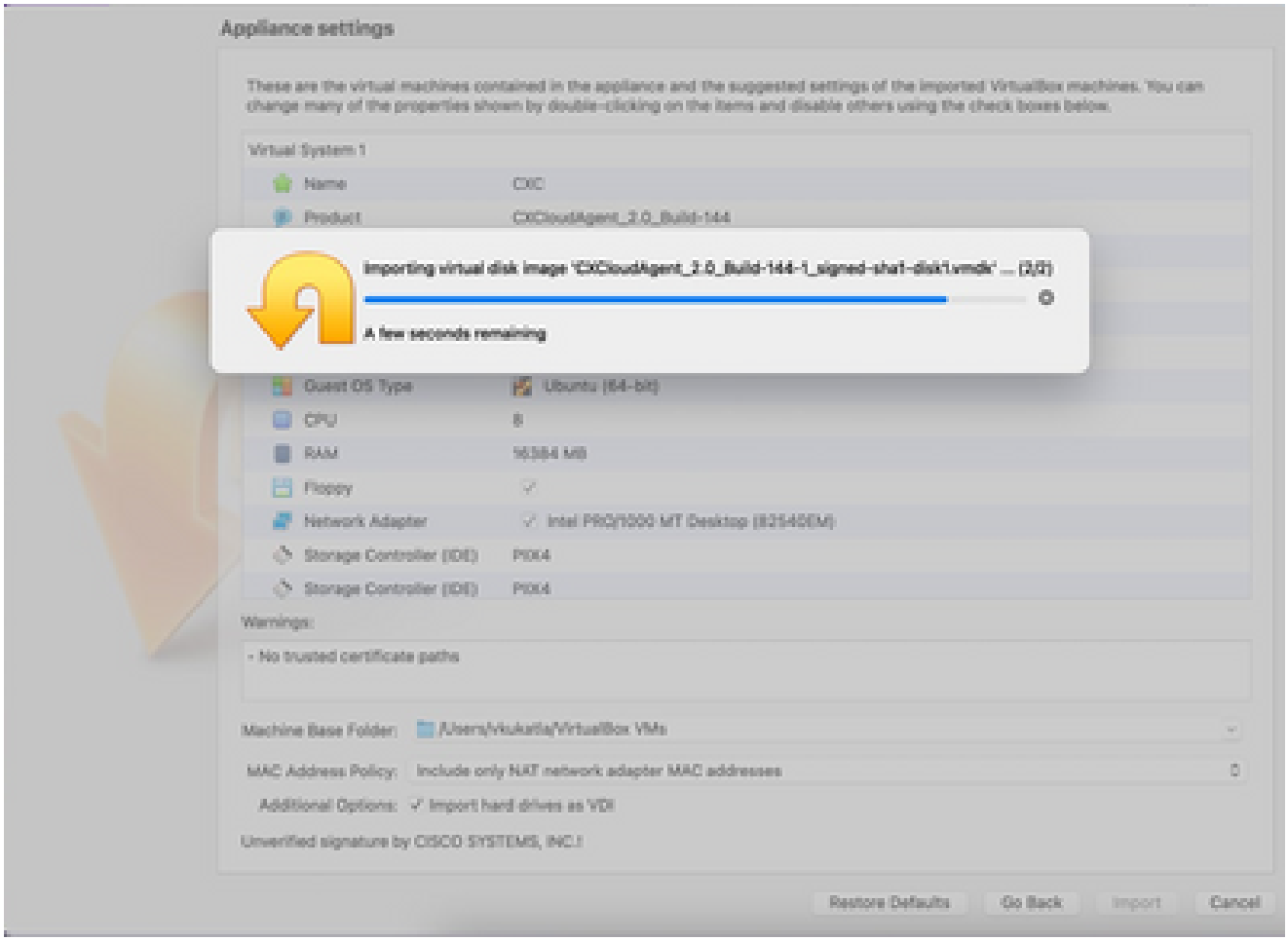


Importar archivo

4. Seleccione la máquina virtual que acaba de implementar y haga clic en Start.

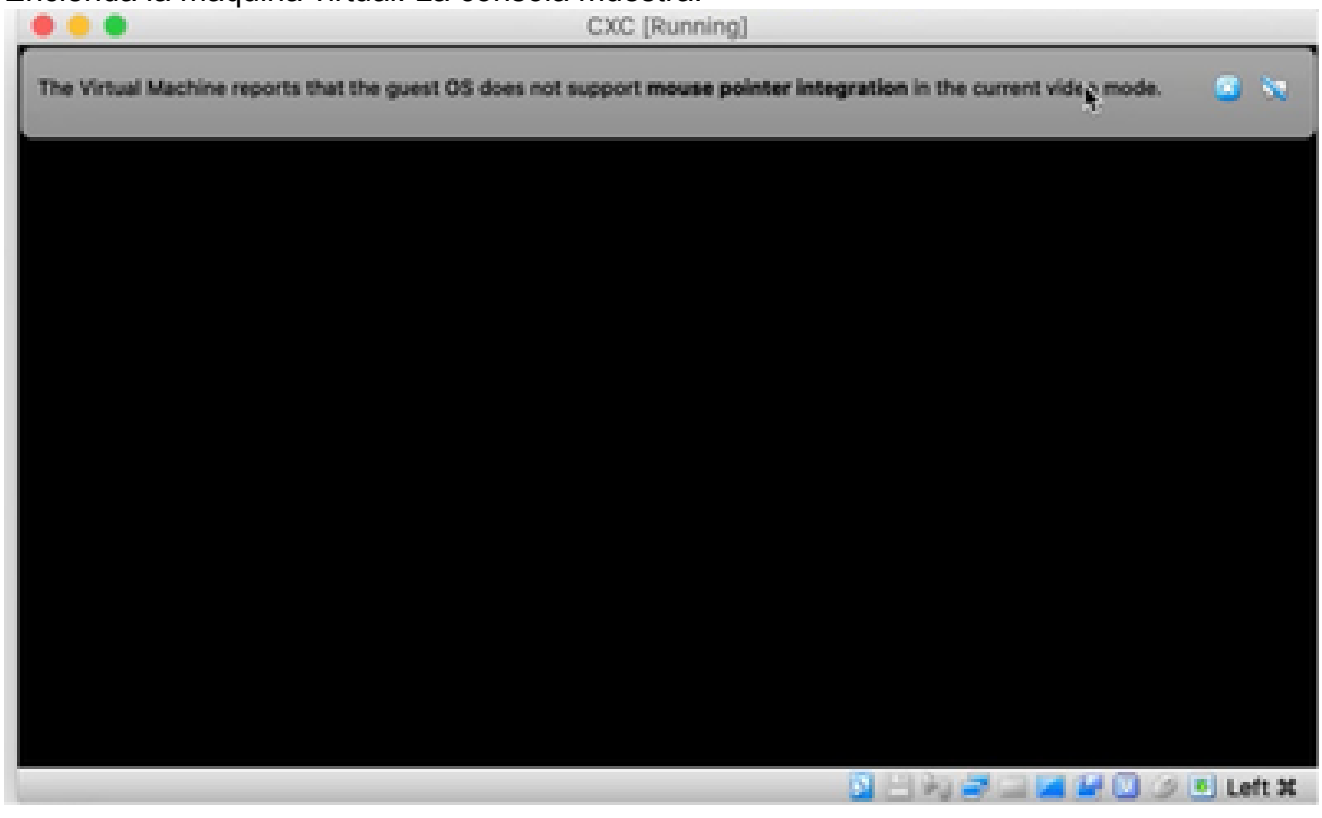


Inicio de la consola VM



Importación en curso

5. Encienda la máquina virtual. La consola muestra.



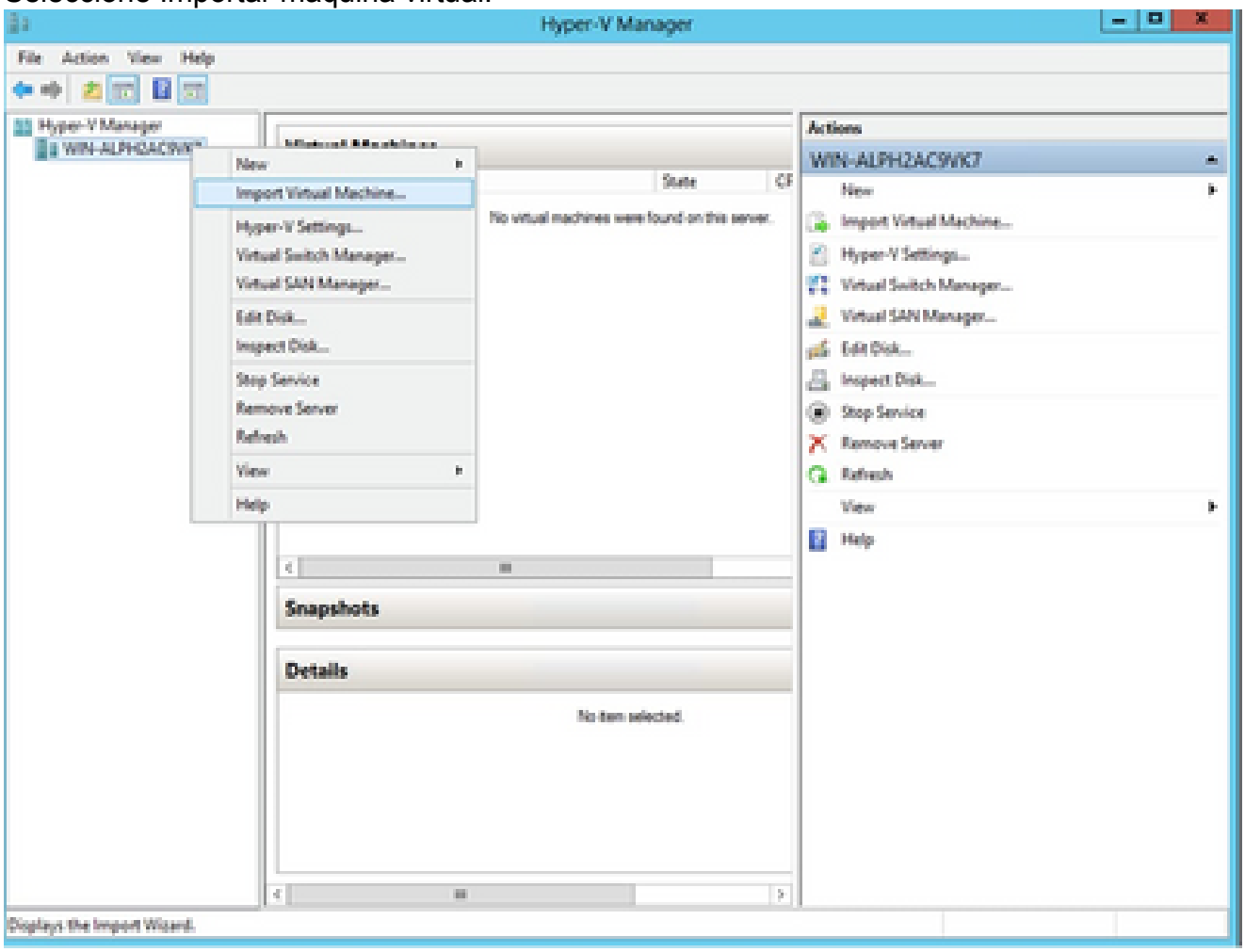
Abrir consola

6. Vaya a Network Configuration para continuar con los siguientes pasos.

Instalación de Microsoft Hyper-V

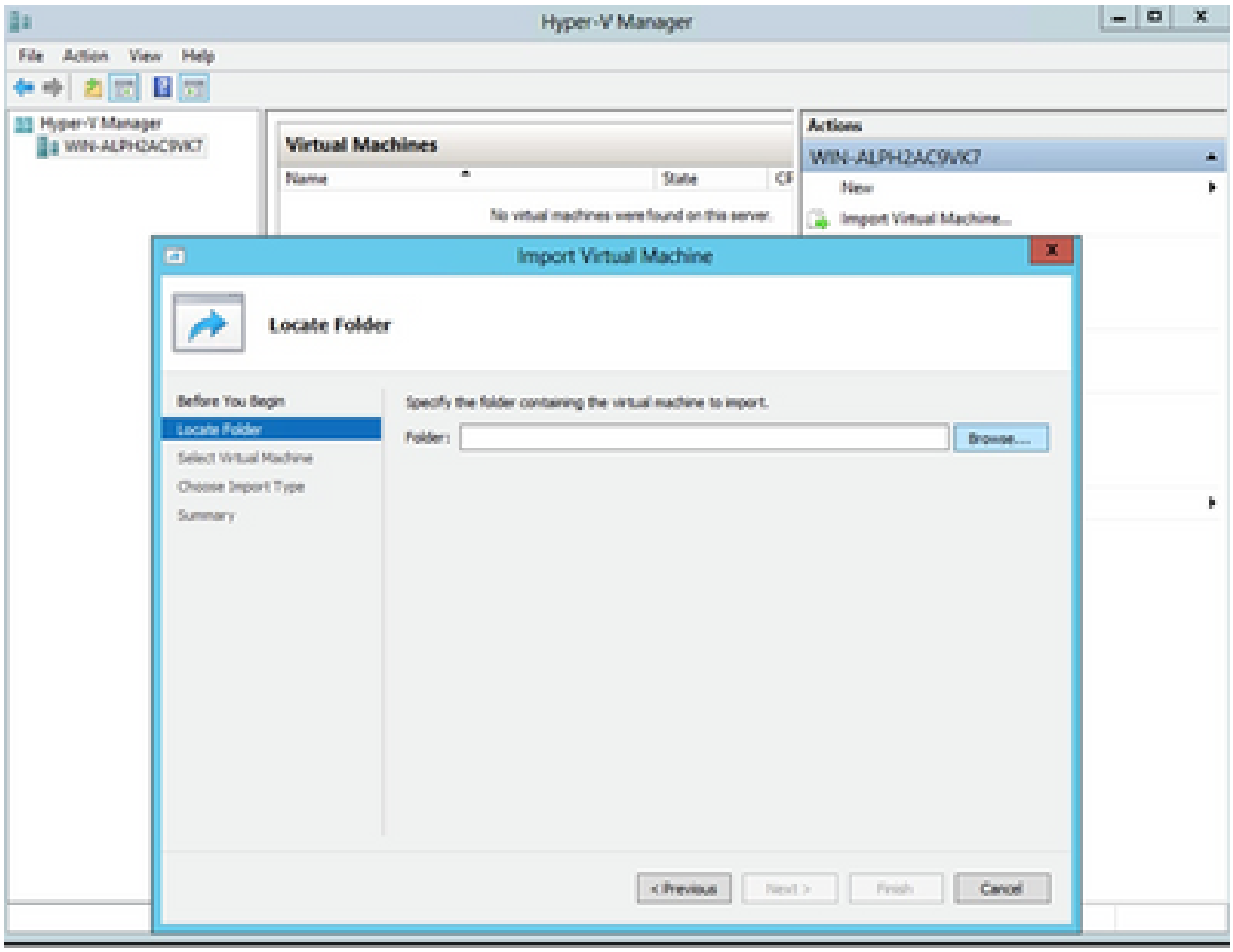
Siga estos pasos:

1. Seleccione Importar máquina virtual.



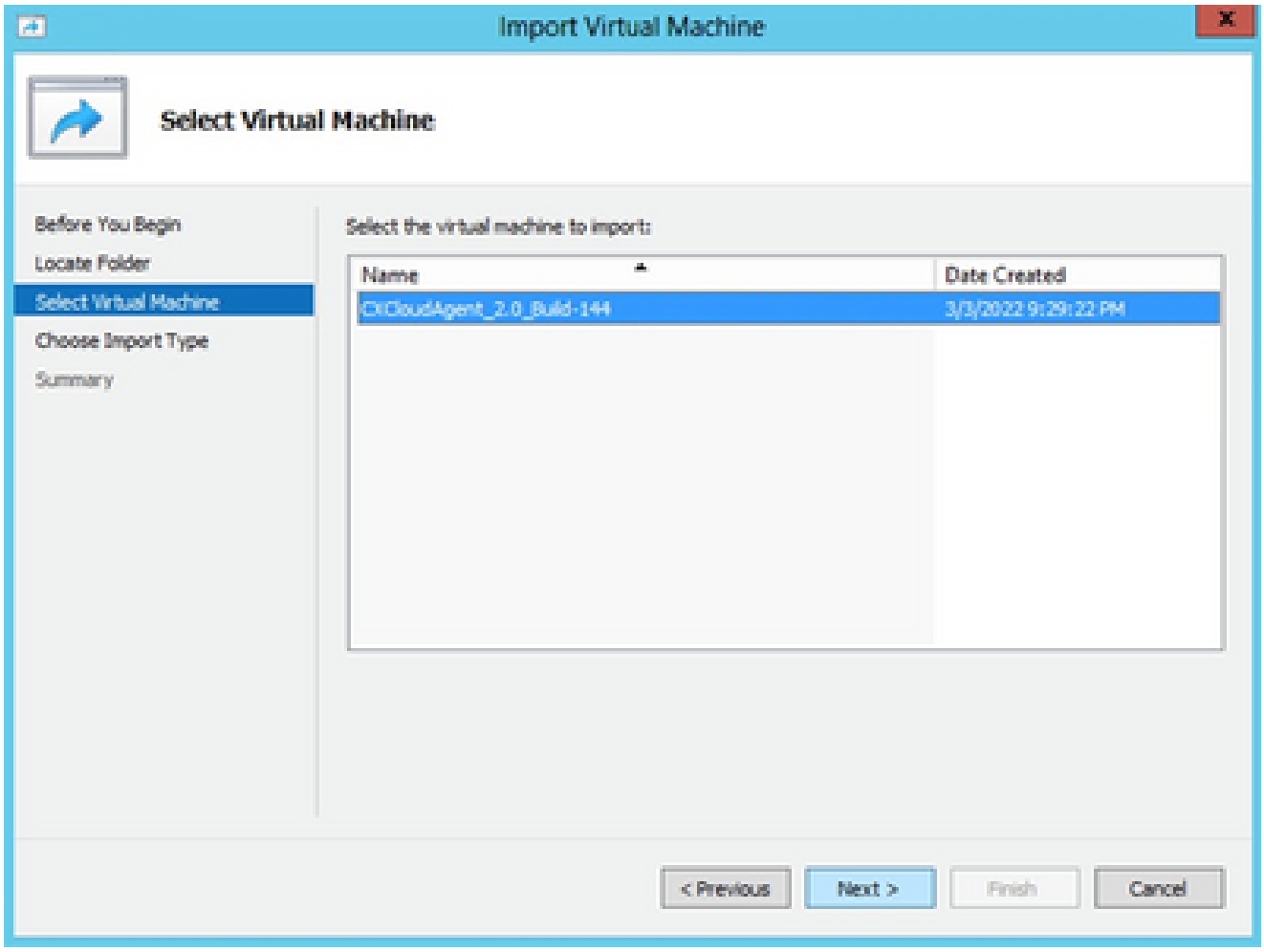
Administrador de Hyper-V

2. Busque y seleccione la carpeta de descarga.
3. Haga clic en Next (Siguiente).



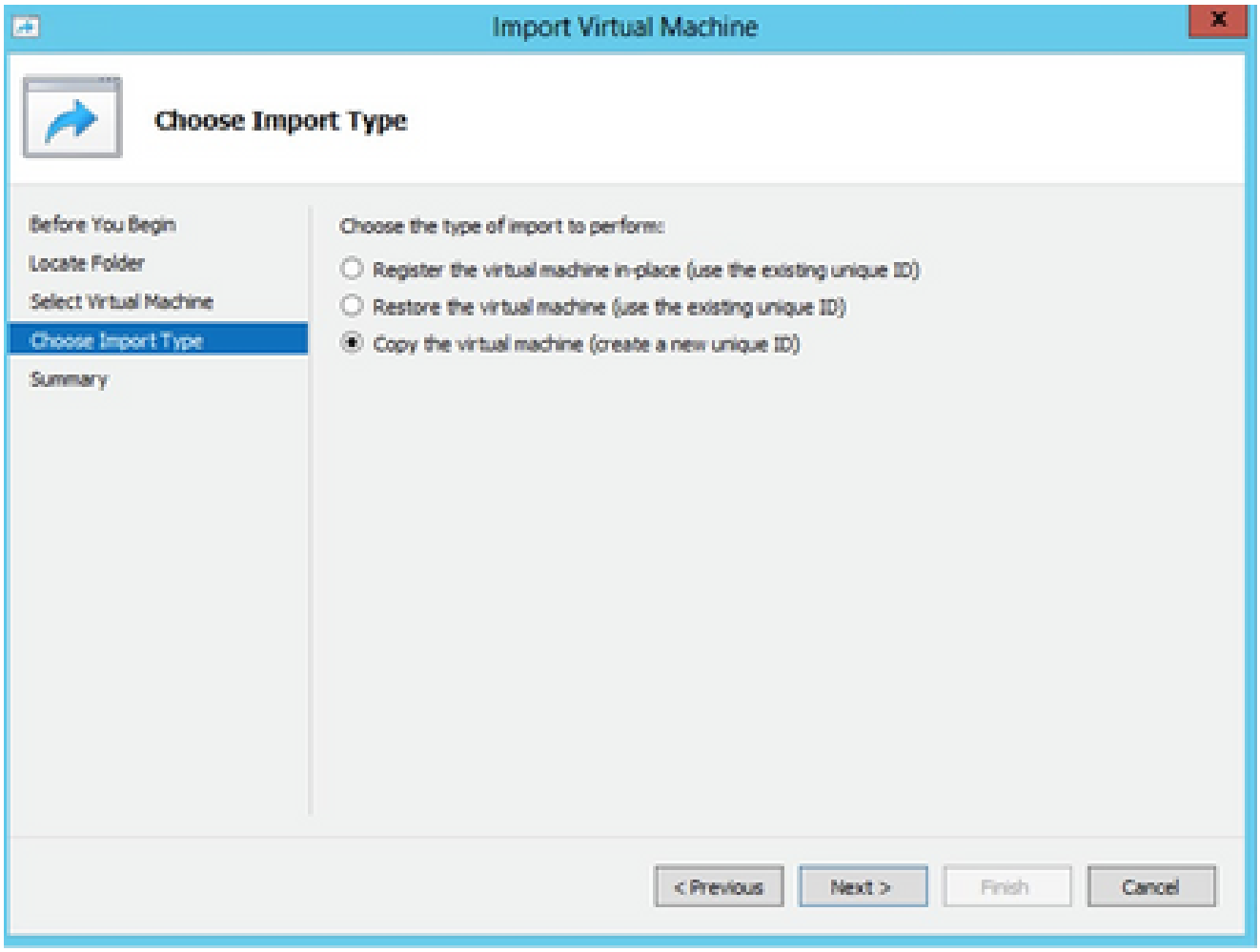
Carpeta para importar

4. Seleccione la VM y haga clic en Next.



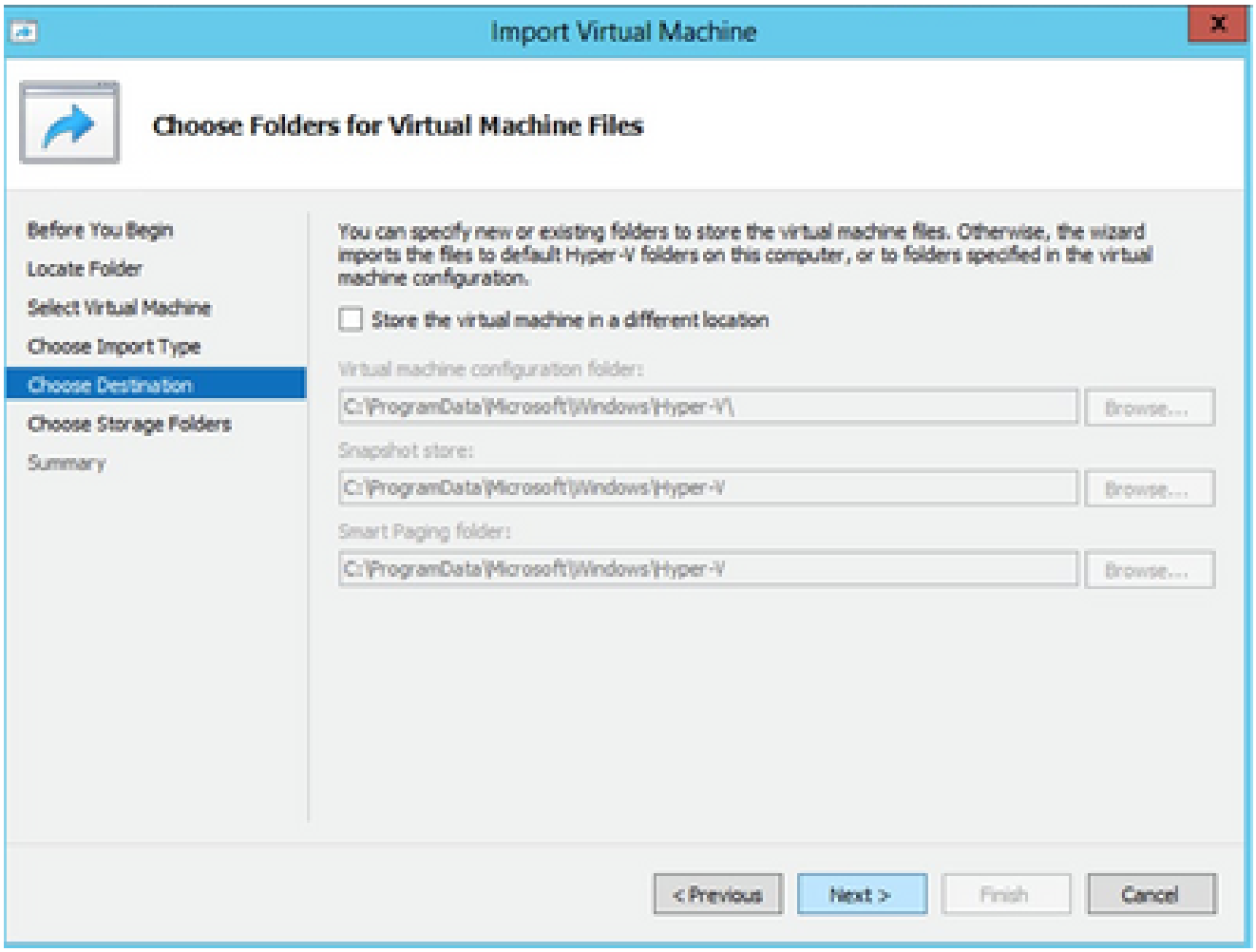
Seleccionar VM

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



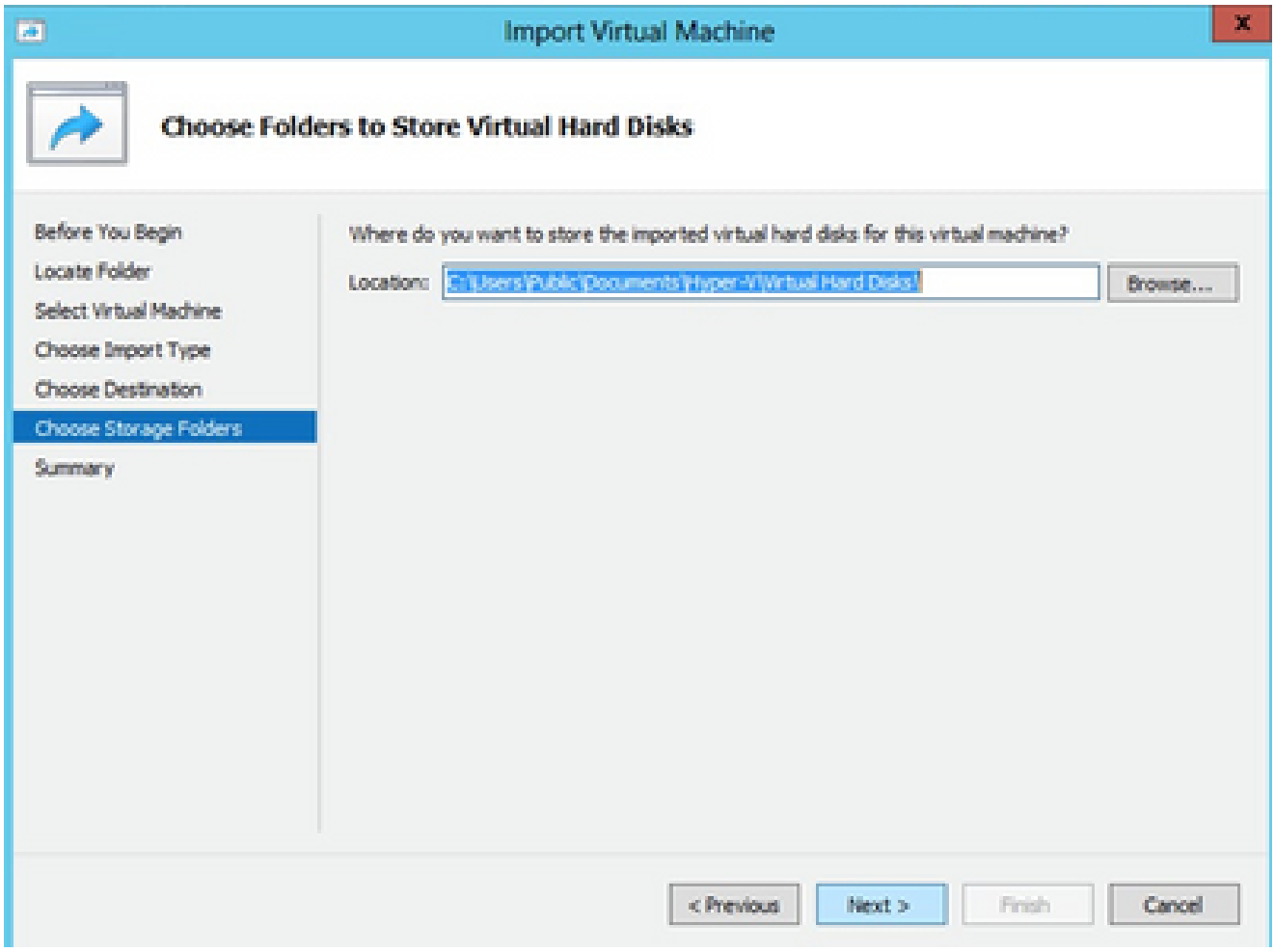
Tipo de importación

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



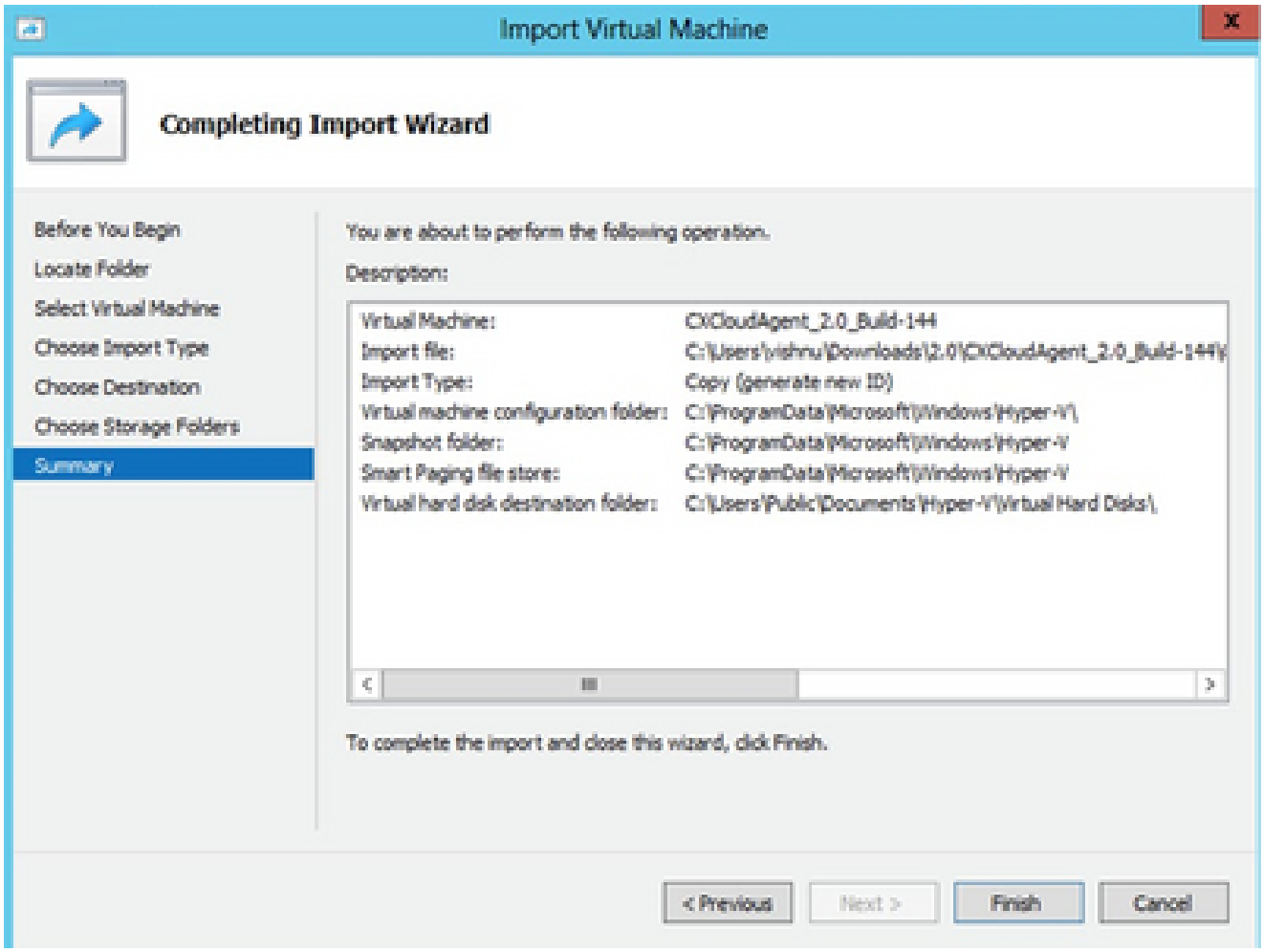
Elegir carpetas para archivos de máquina virtual

8. Busque y seleccione la carpeta en la que desea almacenar el disco duro de la máquina virtual. Se recomienda utilizar rutas predeterminadas.
9. Haga clic en Next (Siguiente).



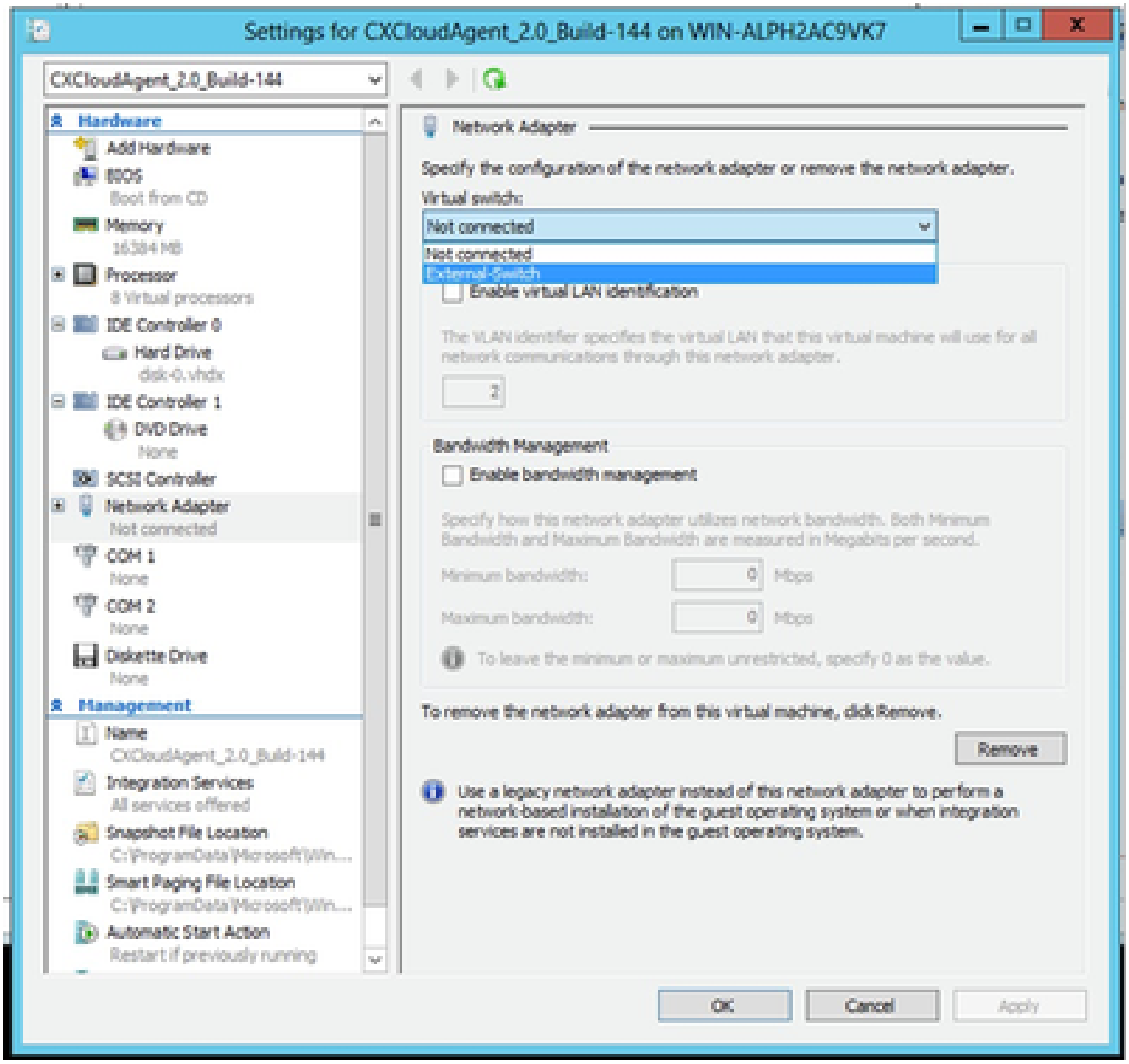
Carpeta para almacenar los discos duros virtuales

10. Se muestra el resumen de VM. Verifique todas las entradas y haga clic en Finish.



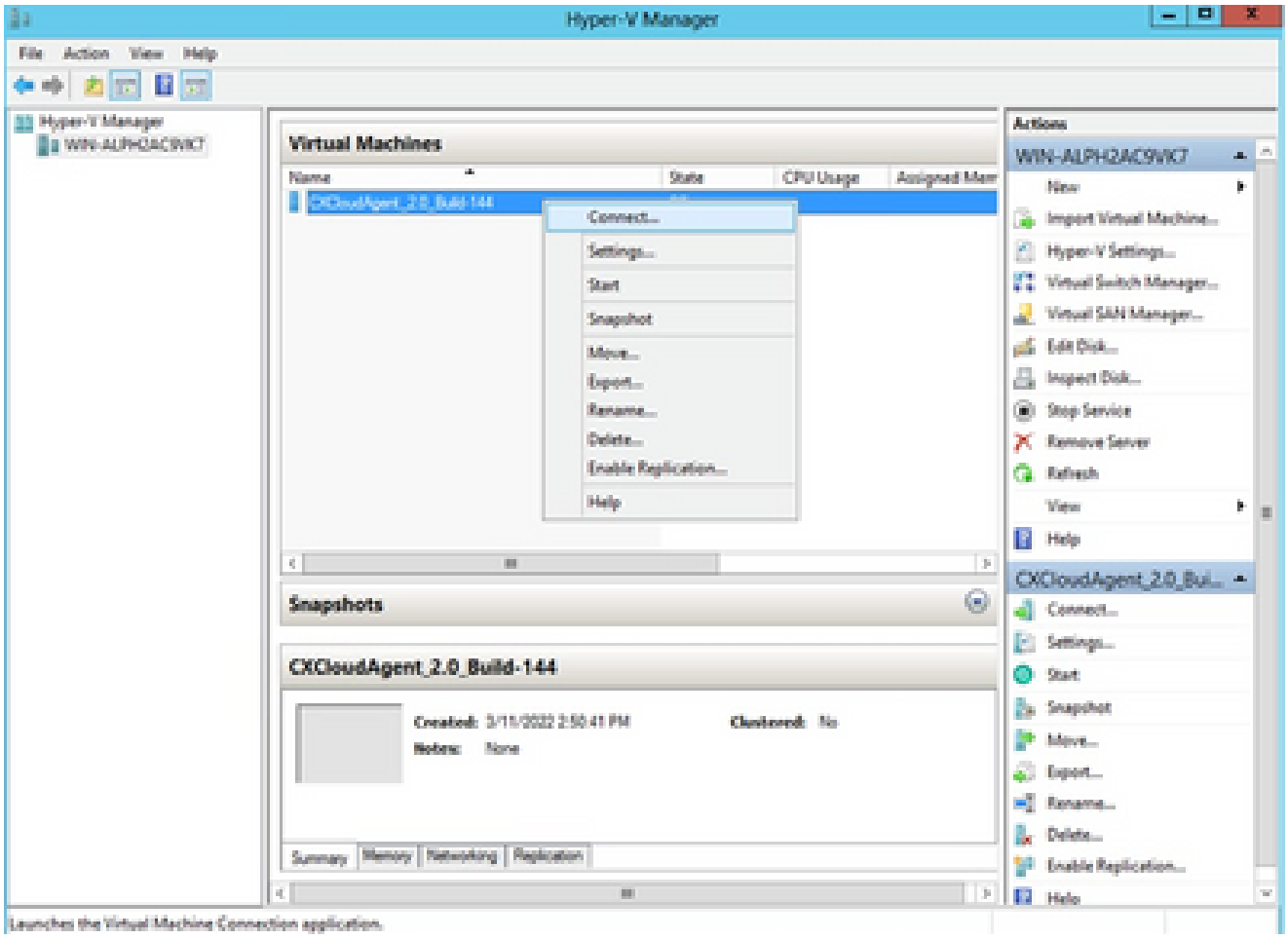
Summary

11. Una vez completada correctamente la importación, se crea una nueva VM en Hyper-V. Abra la configuración de VM.
12. Seleccione el adaptador de red en el panel izquierdo y elija el switch virtual disponible en el menú desplegable.



Switch virtual

13. Seleccione Connect para iniciar la máquina virtual.

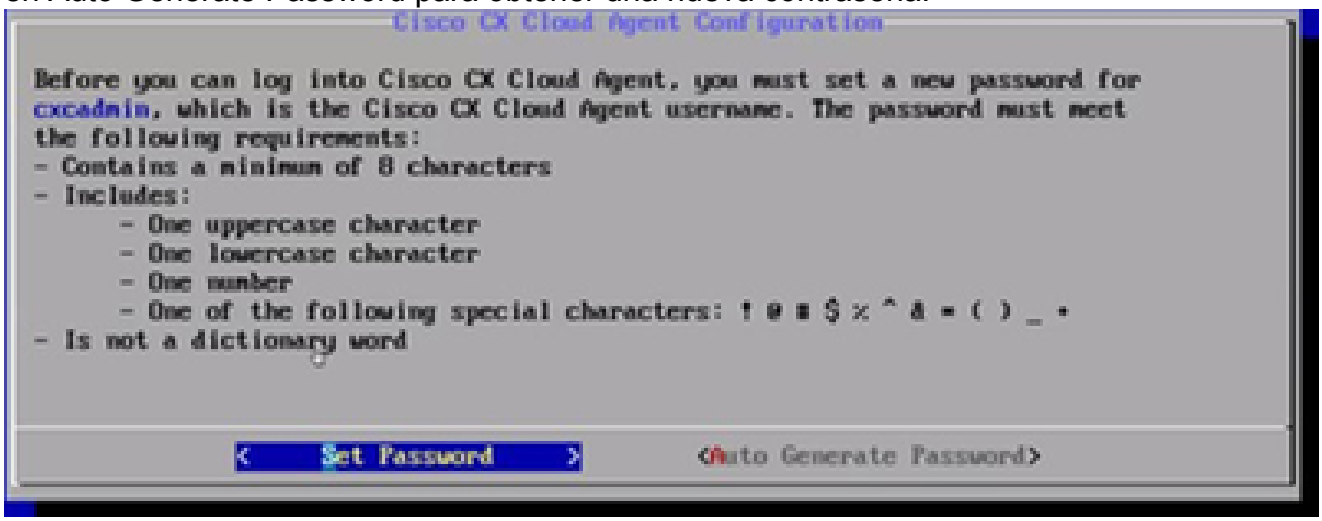


VM inicial

14. Vaya a Network Configuration para continuar con los siguientes pasos.

Configuración de red

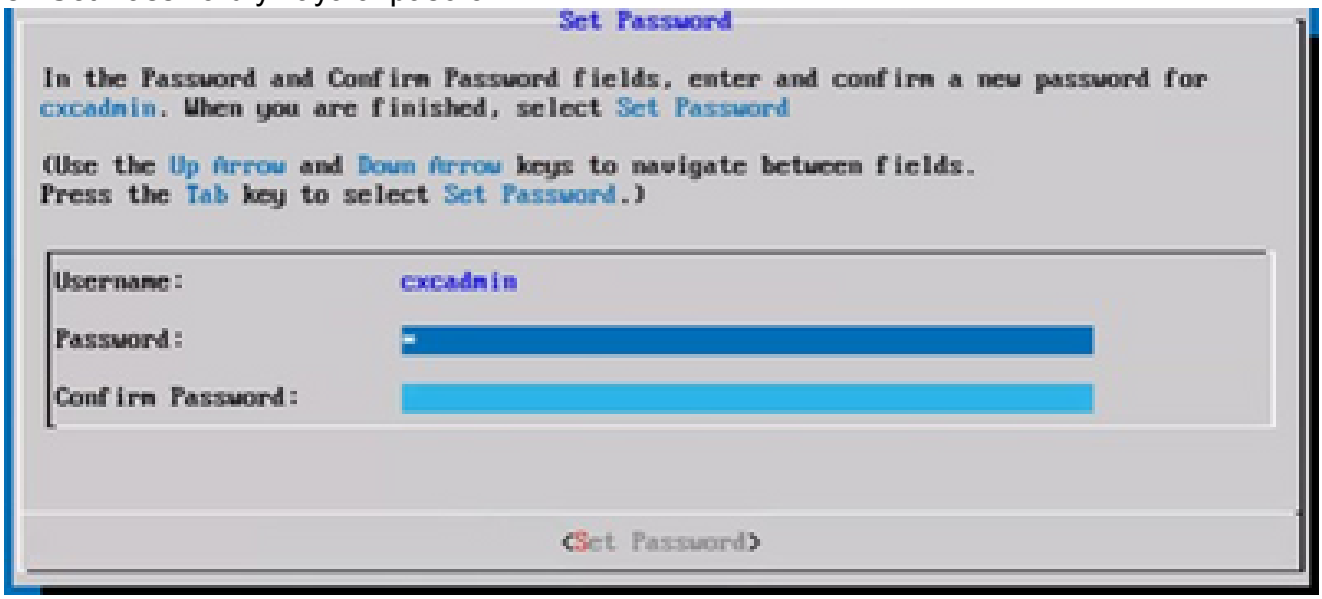
1. Haga clic en Set Password para agregar una nueva contraseña para cxcadmin O haga clic en Auto Generate Password para obtener una nueva contraseña.



Establecer contraseña

2. Si se selecciona Set Password, ingrese la contraseña para cxcadmin y confírmela. Haga clic

en Set Password y vaya al paso 3.



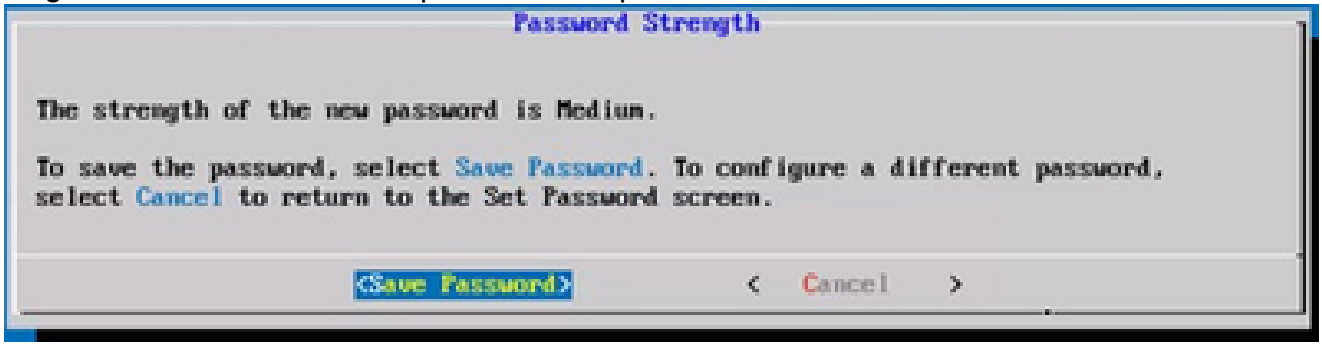
Nueva contraseña

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

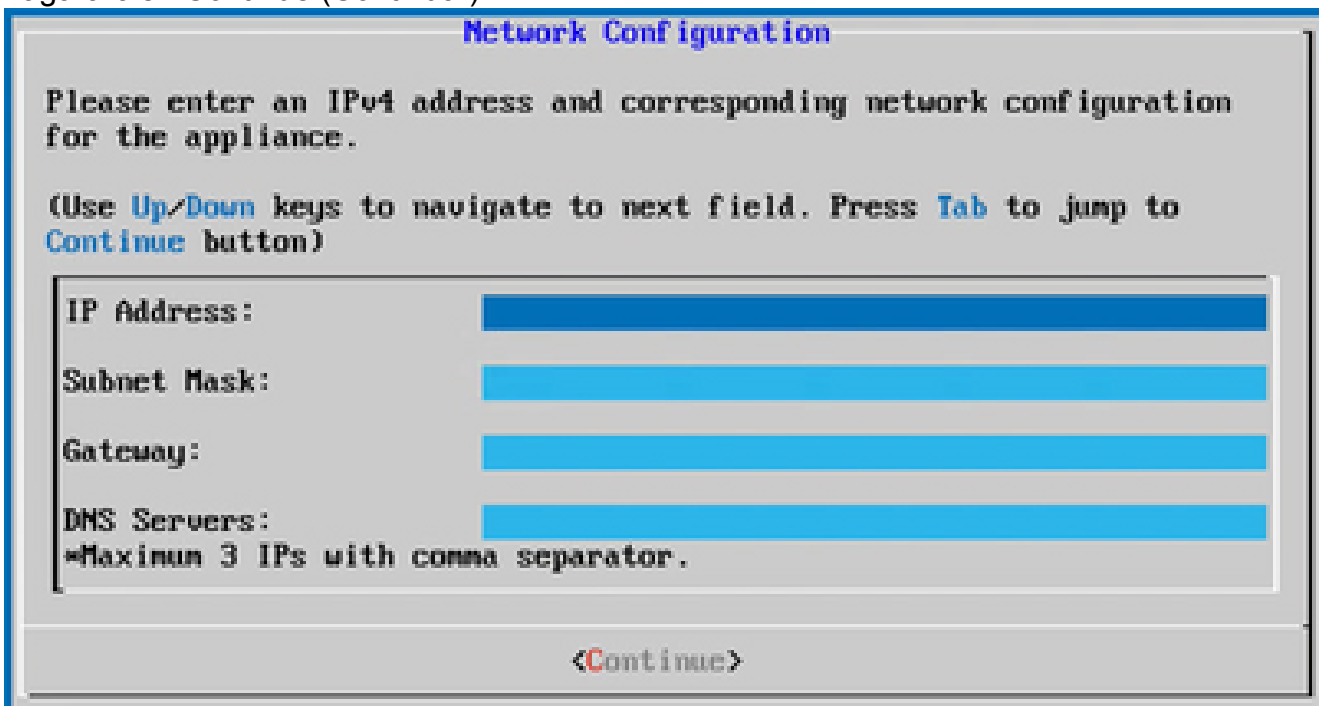
3. Haga clic en Save Password para utilizarlo para la autenticación.



Guardar contraseña

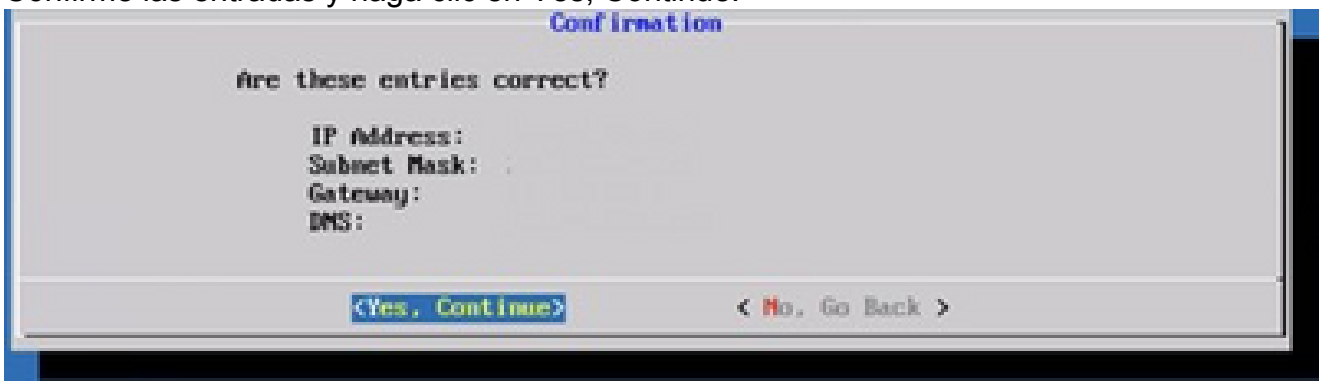
4. Introduzca la dirección IP, la máscara de subred, la puerta de enlace y el servidor DNS y

haga clic en Continue (Continuar).



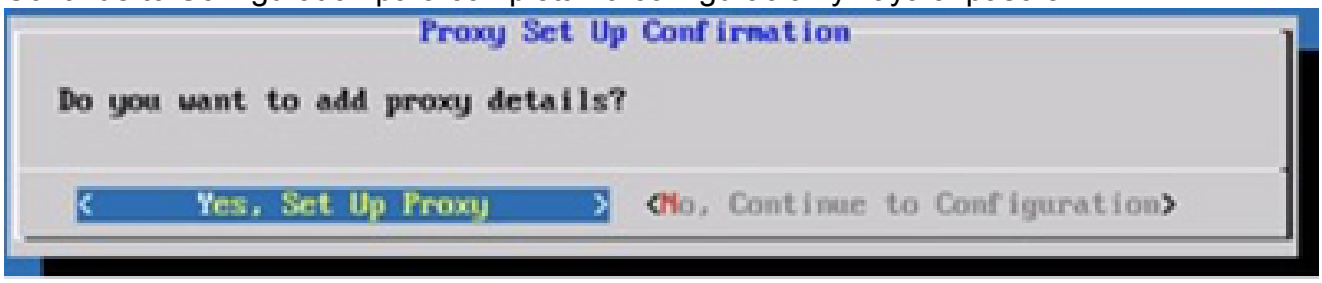
Configuración de red

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



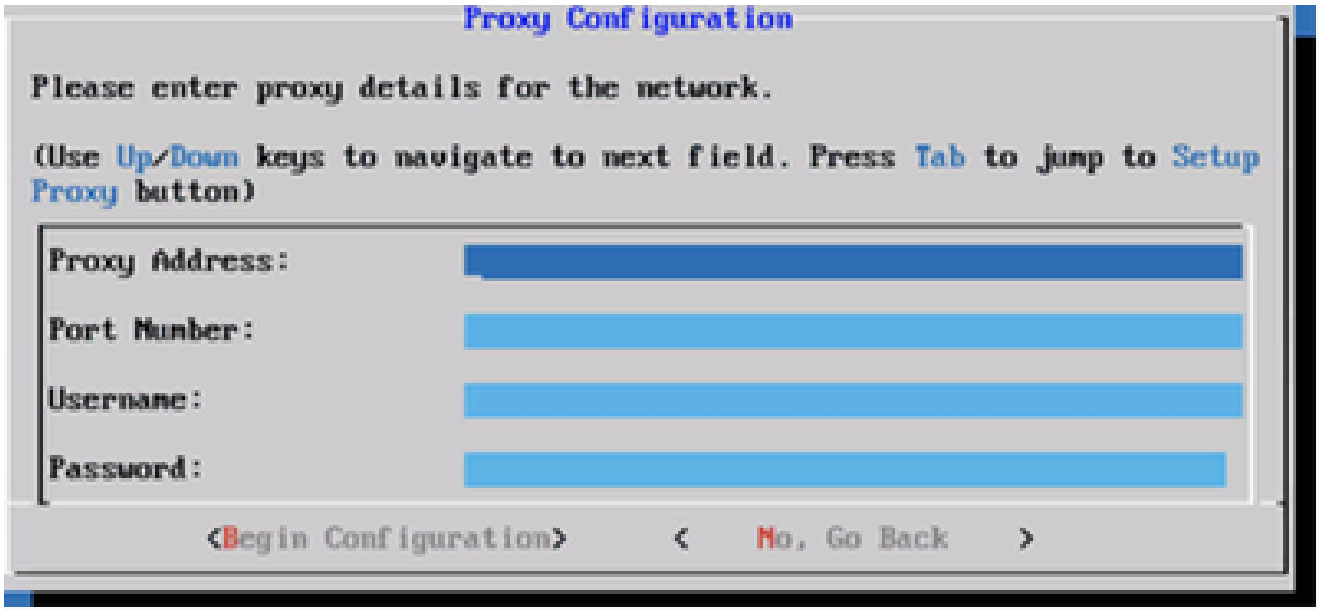
Configuración

6. Para establecer los detalles del proxy, haga clic en Yes, Set Up Proxy o haga clic en No, Continue to Configuration para completar la configuración y vaya al paso 8.



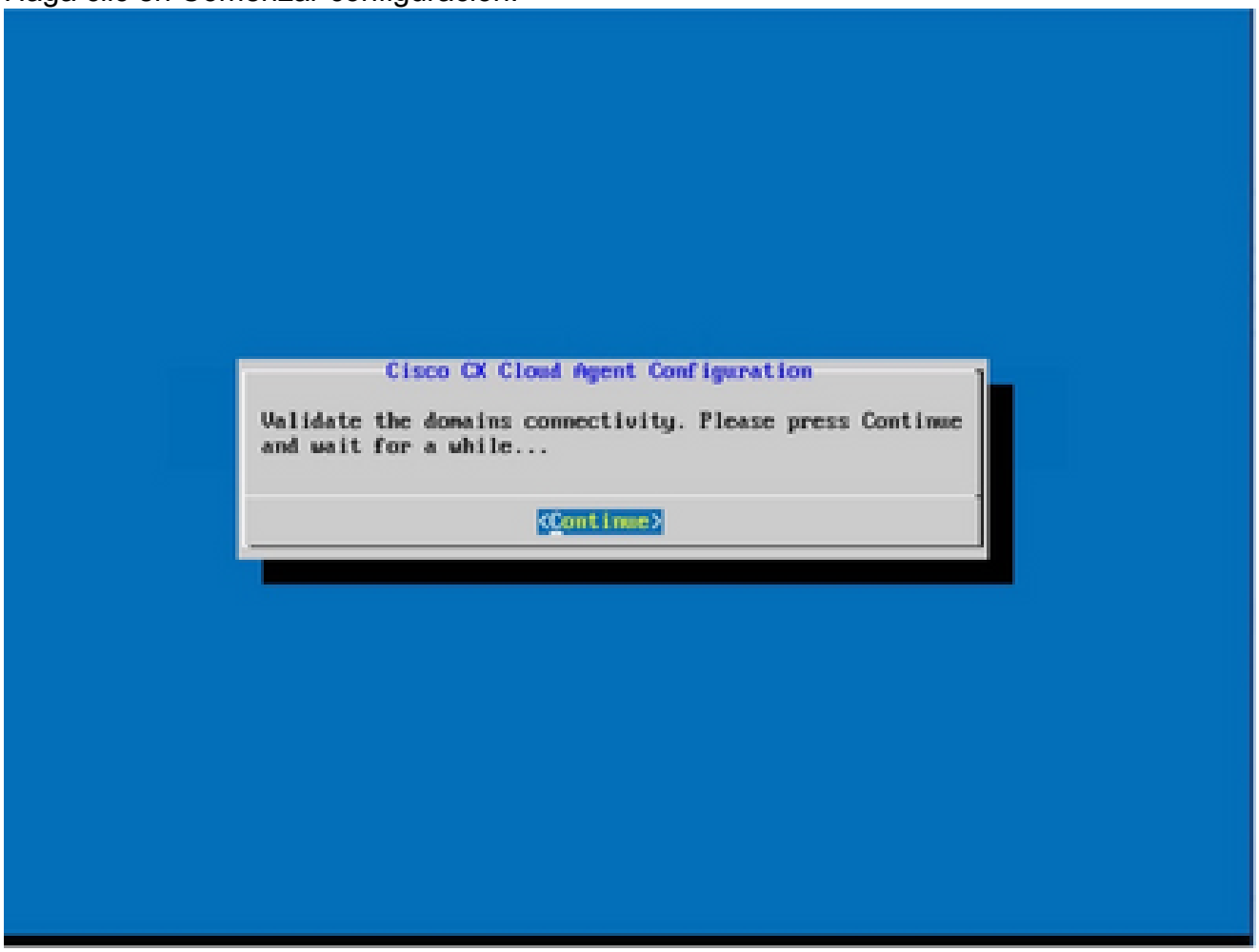
Configuración de proxy

7. Ingrese la Dirección de Proxy, el Número de Puerto, el Nombre de Usuario y la Contraseña.



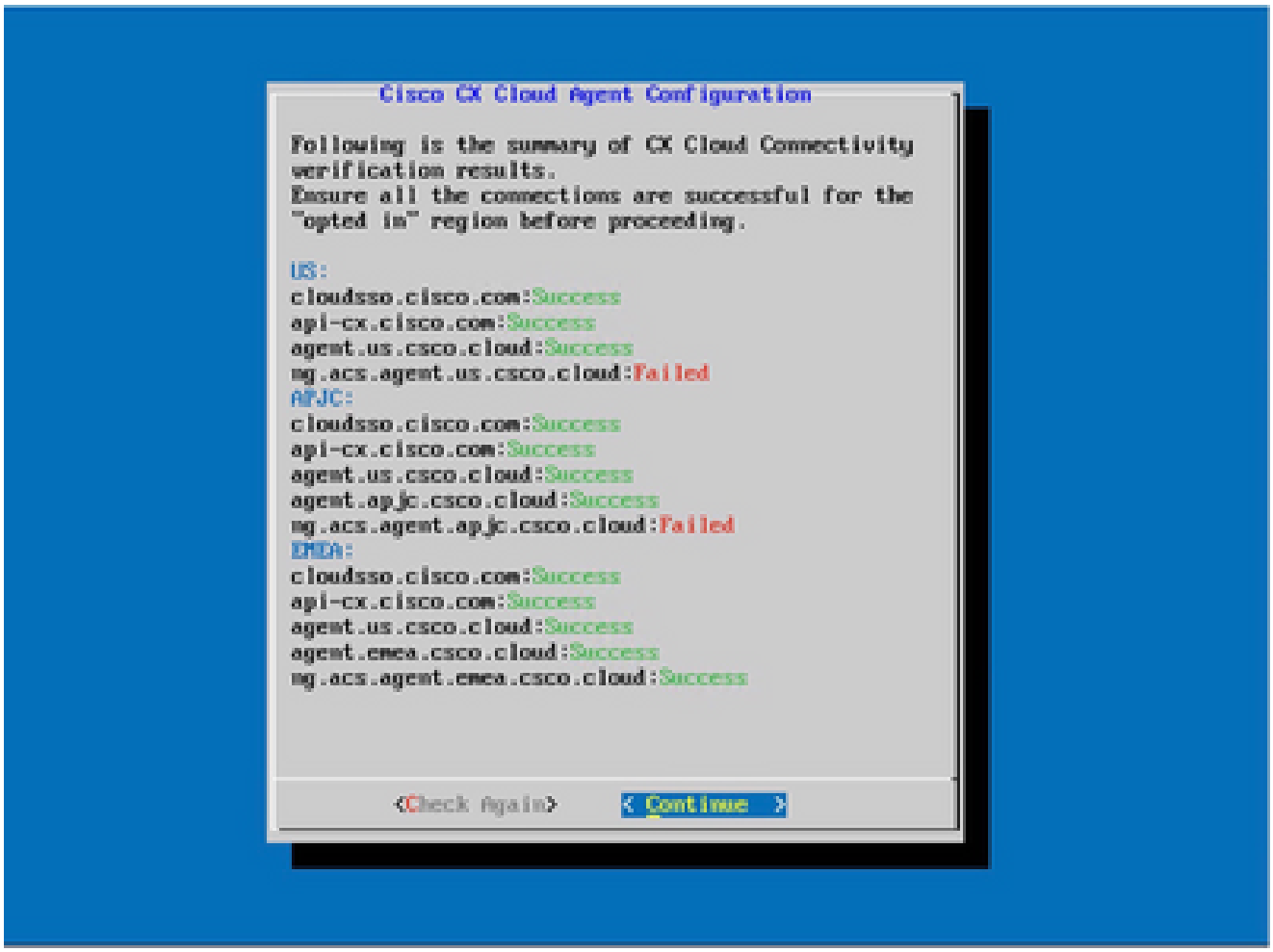
Configuración de proxy

8. Haga clic en Comenzar configuración.



Comienzo de la configuración

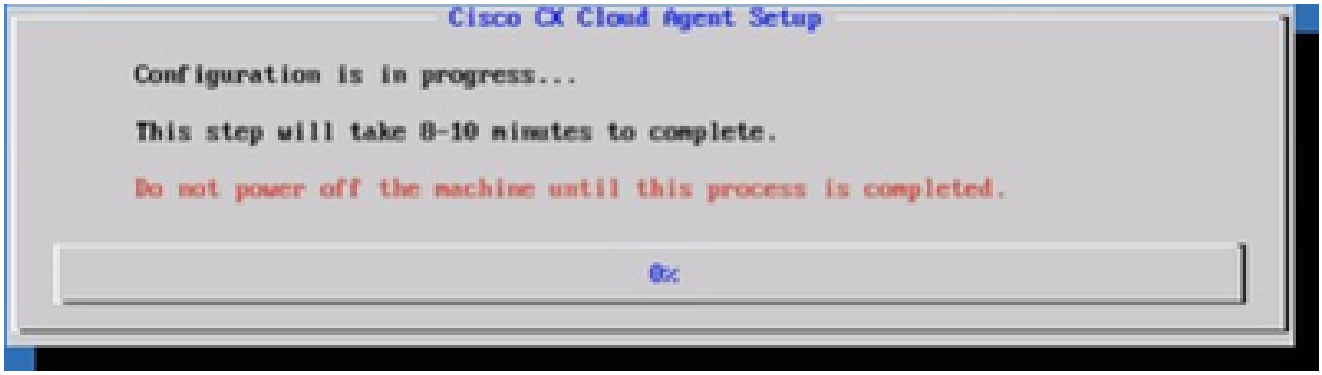
9. Haga clic en Continue (Continuar).



La configuración continúa

10. 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 corregir la 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.

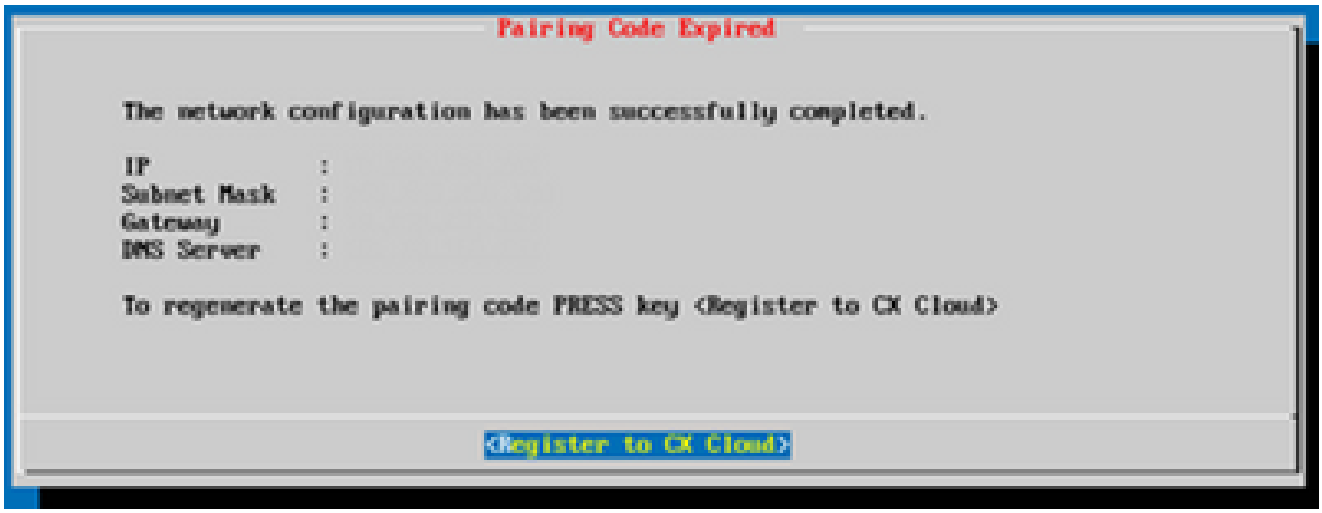


Configuración en curso

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

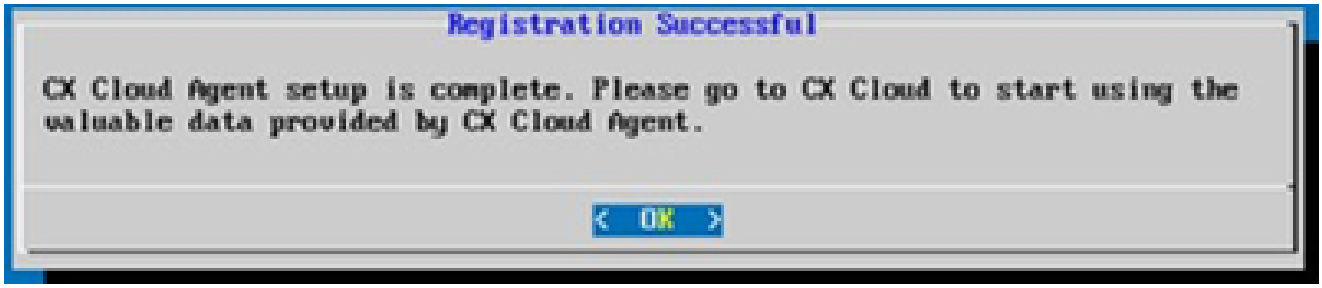
Código de vinculación

12. Si el código de vinculación caduca, haga clic en Register to CX Cloud para obtener el código de nuevo.



Código caducado

13. Click OK.



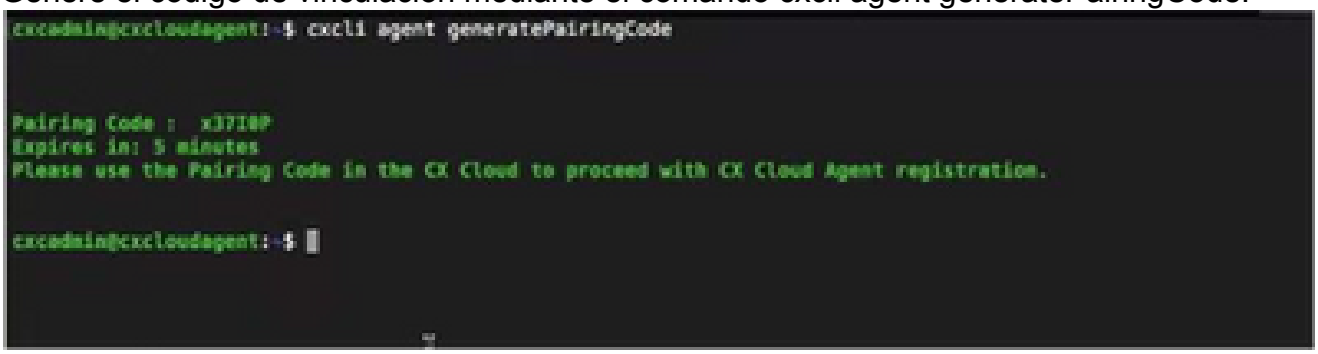
Registro correcto

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 vinculación mediante el comando cxcli agent generatePairingCode.



Generar CLI de código de vinculación

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

Configuración de Cisco DNA Center para reenviar Syslog a CX Cloud Agent

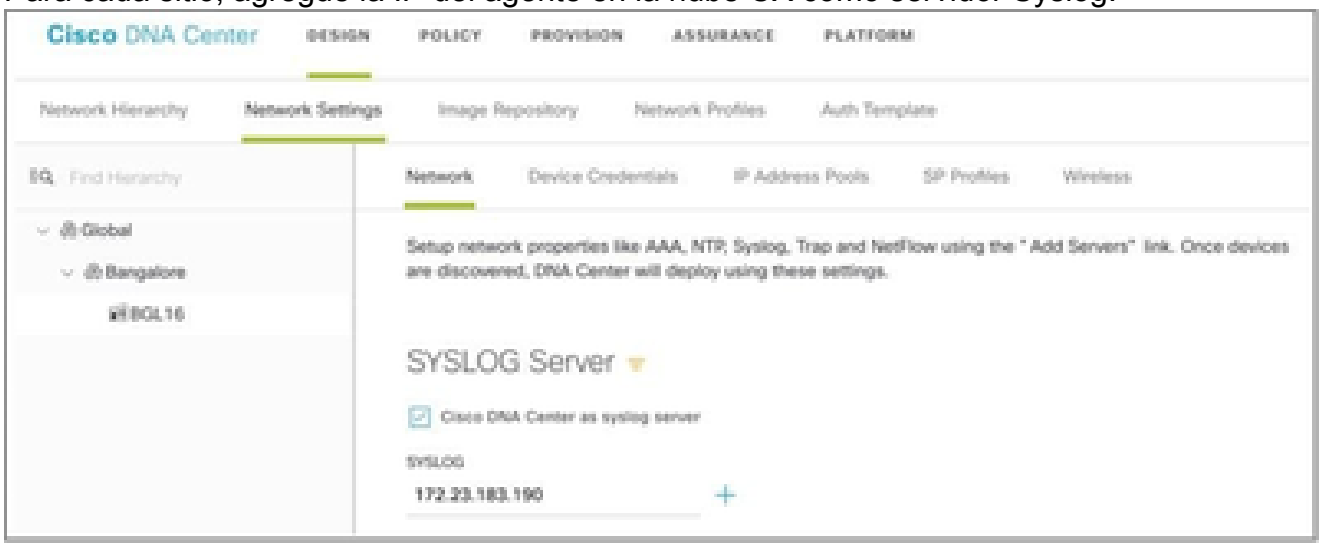
Prerequisites

Las versiones compatibles de Cisco DNA 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 DNA Center Virtual Appliance

Configurar la configuración de Syslog Forward

Para configurar el reenvío de Syslog a CX Cloud Agent en el Cisco DNA Center, siga estos pasos:

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



Notas:
Una vez configurados, todos los dispositivos asociados con ese sitio se configuran para enviar syslog con nivel crítico a CX Cloud Agent. 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 con ese sitio se establecen automáticamente en el nivel crítico predeterminado.

Configuración de otros recursos para reenviar Syslog a CX Cloud Agent

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

Nota: solo los dispositivos Campus Success Track Level 2 pueden configurar otros recursos para reenviar el registro del sistema.

Servidores Syslog existentes con capacidad de reenvío

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

Nota: Al reenviar registros del sistema, asegúrese de que se conserve 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 en la nube CX. Consulte esta documentación para conocer los pasos de configuración específicos.

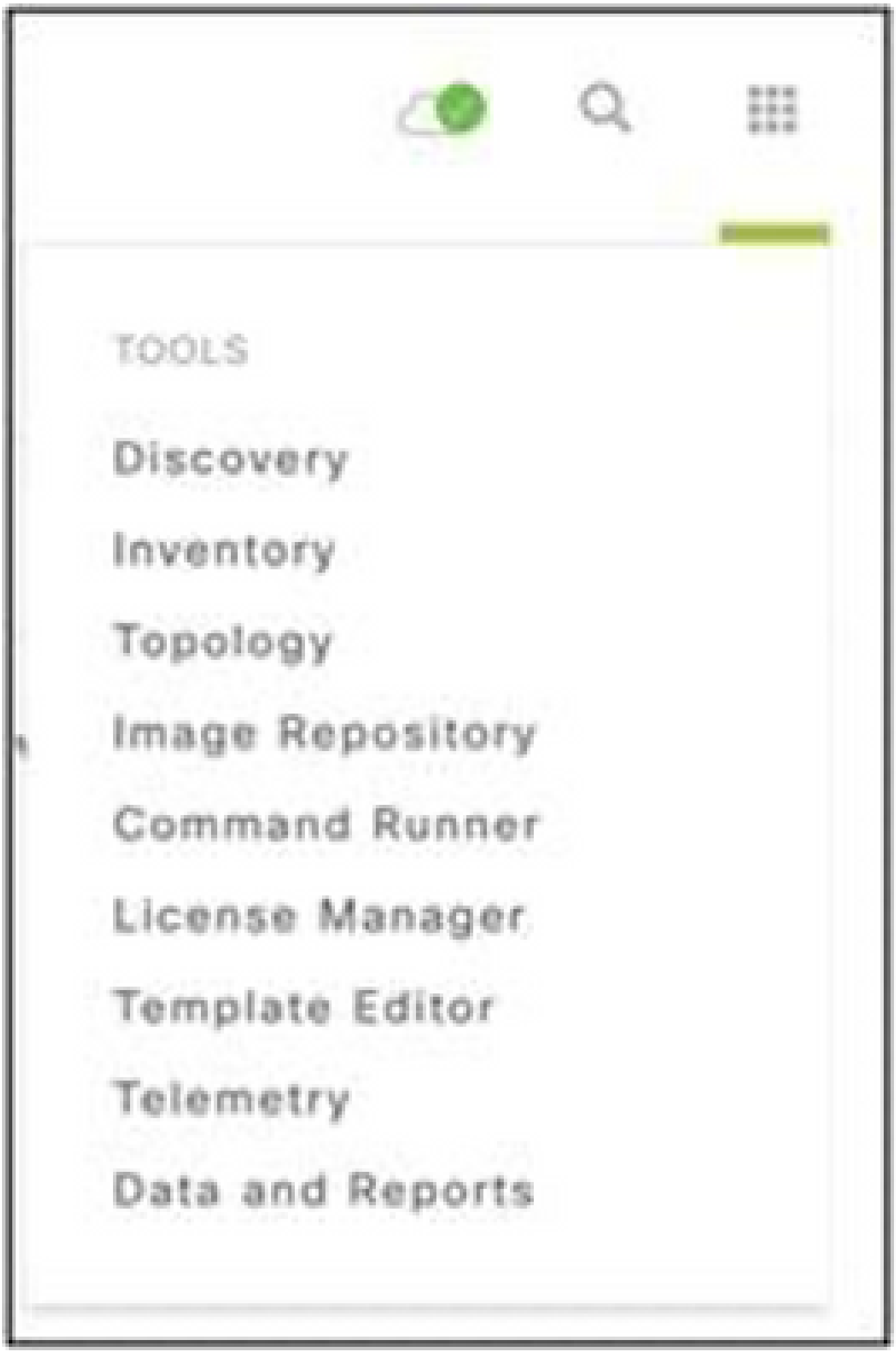
Guía de configuración de Cisco IOS® XE

Guía de configuración del controlador inalámbrico AireOS

Habilitar configuración de Syslog de nivel de información

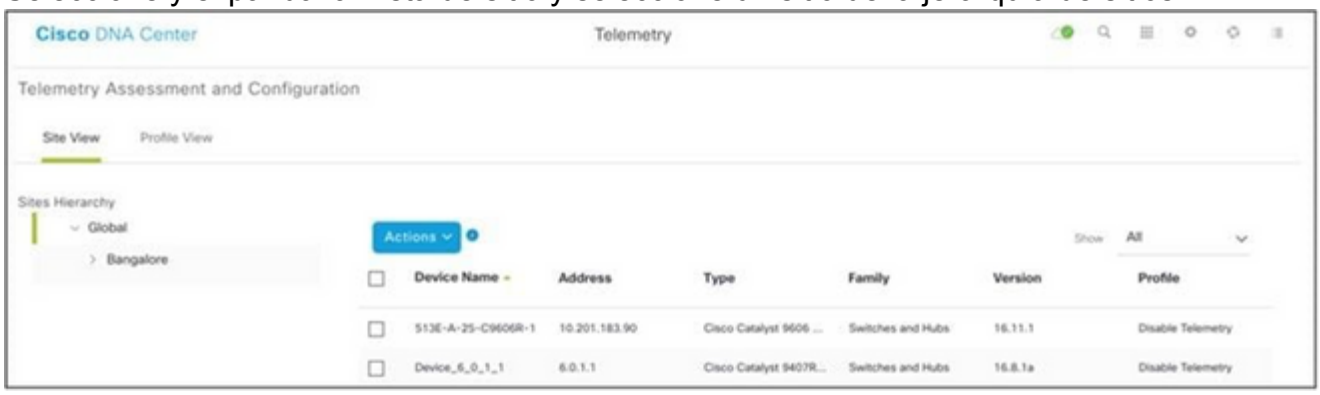
Para hacer visible el nivel de información de Syslog, siga estos pasos:

1. Vaya a Herramientas>Telemetría.


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

Menú Herramientas

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

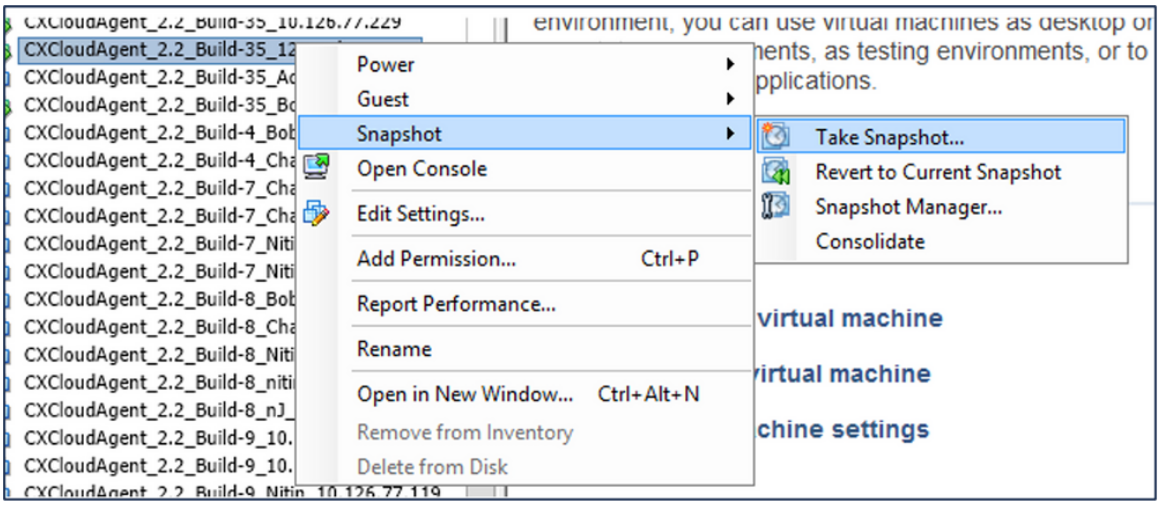
Copia de seguridad y restauración de la VM en la nube CX

Se recomienda conservar el estado y los datos de una VM del agente en la nube 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.

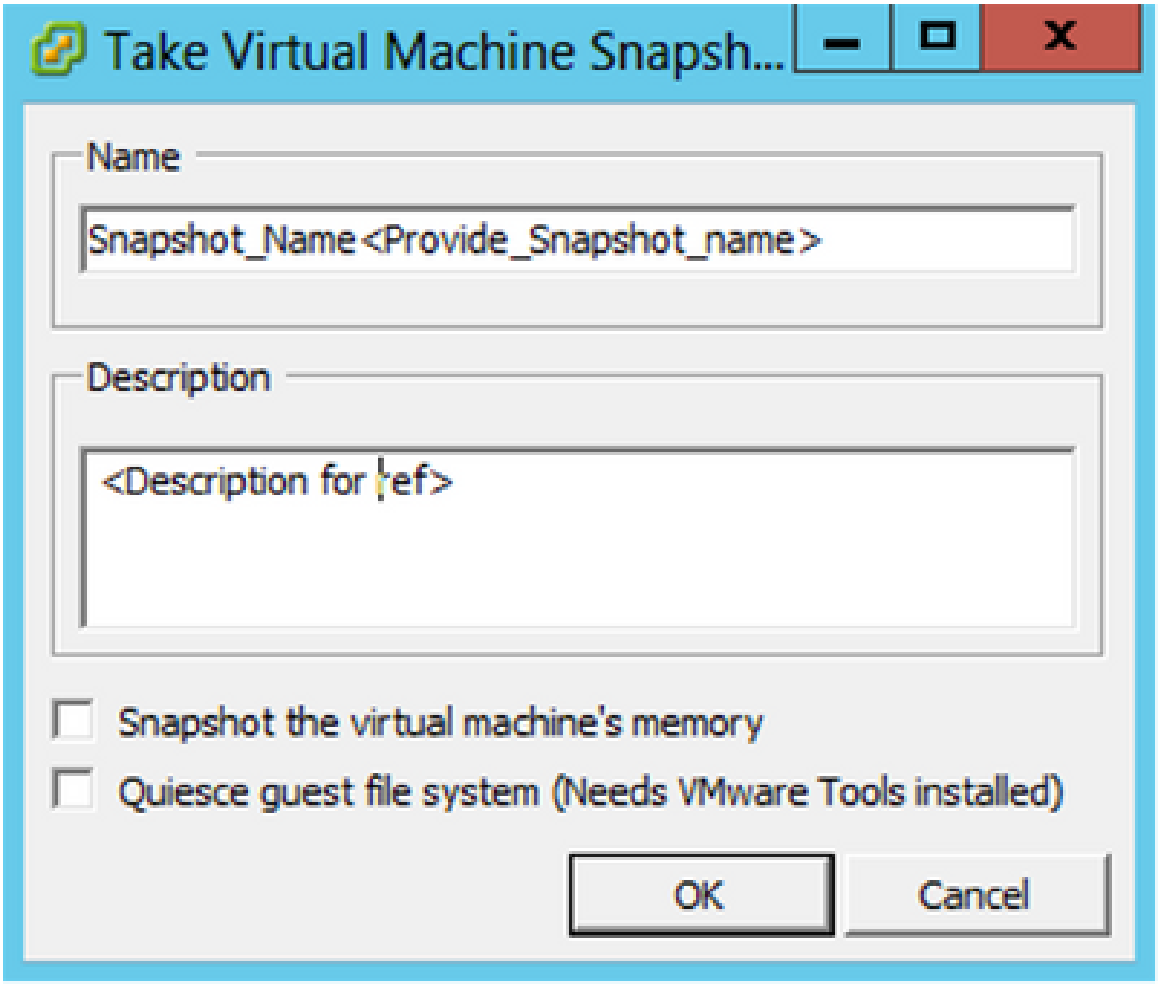
Copia de seguridad

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

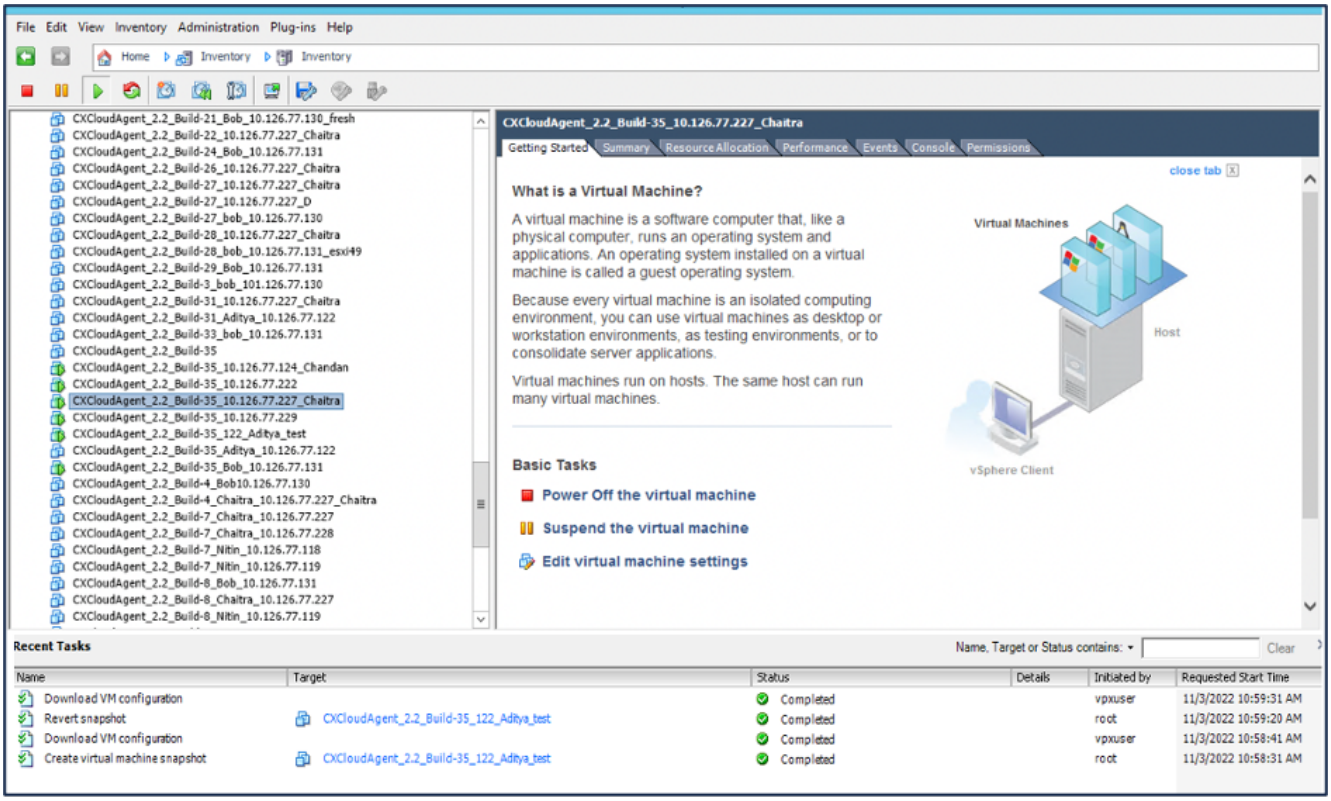


Tomar instantánea de máquina virtual

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.

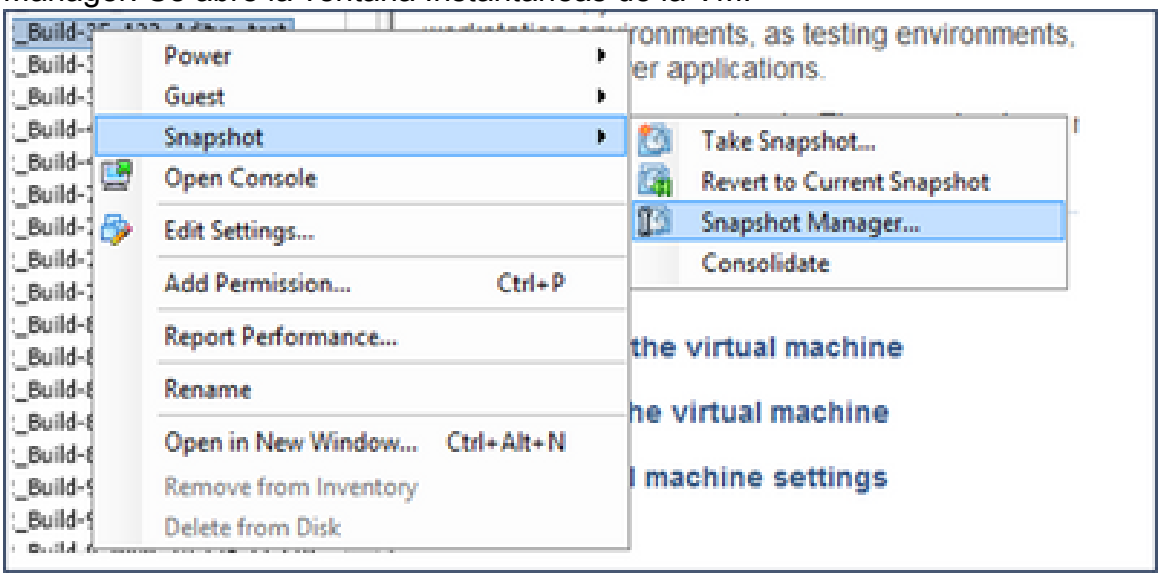


Tareas recientes

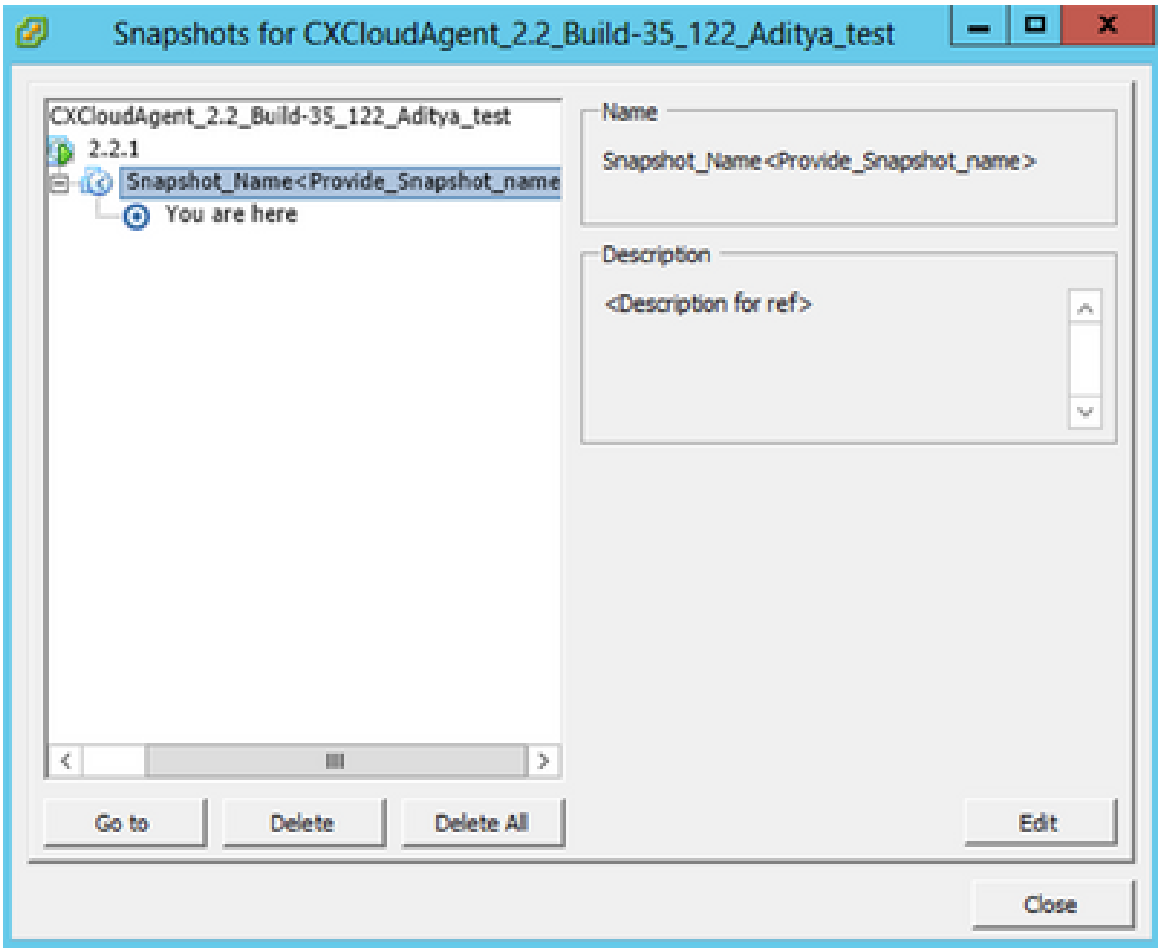
Restaurar

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.

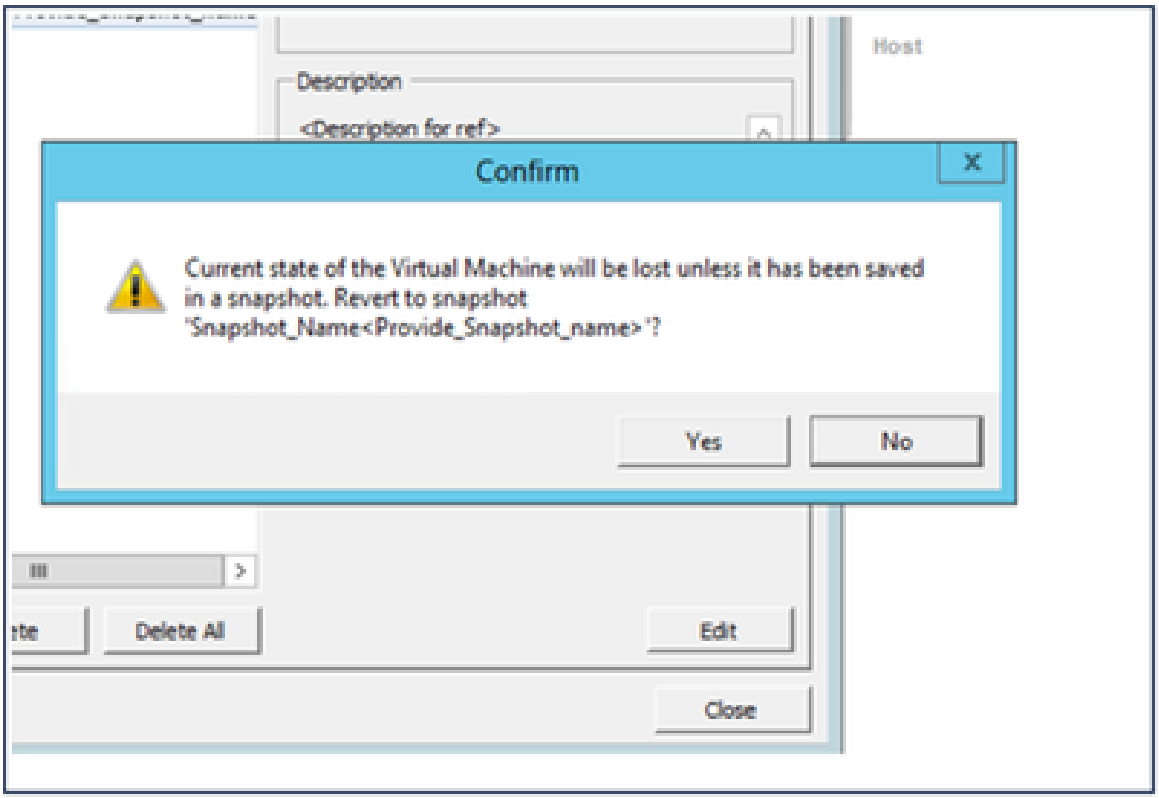


Ventana Seleccionar VM



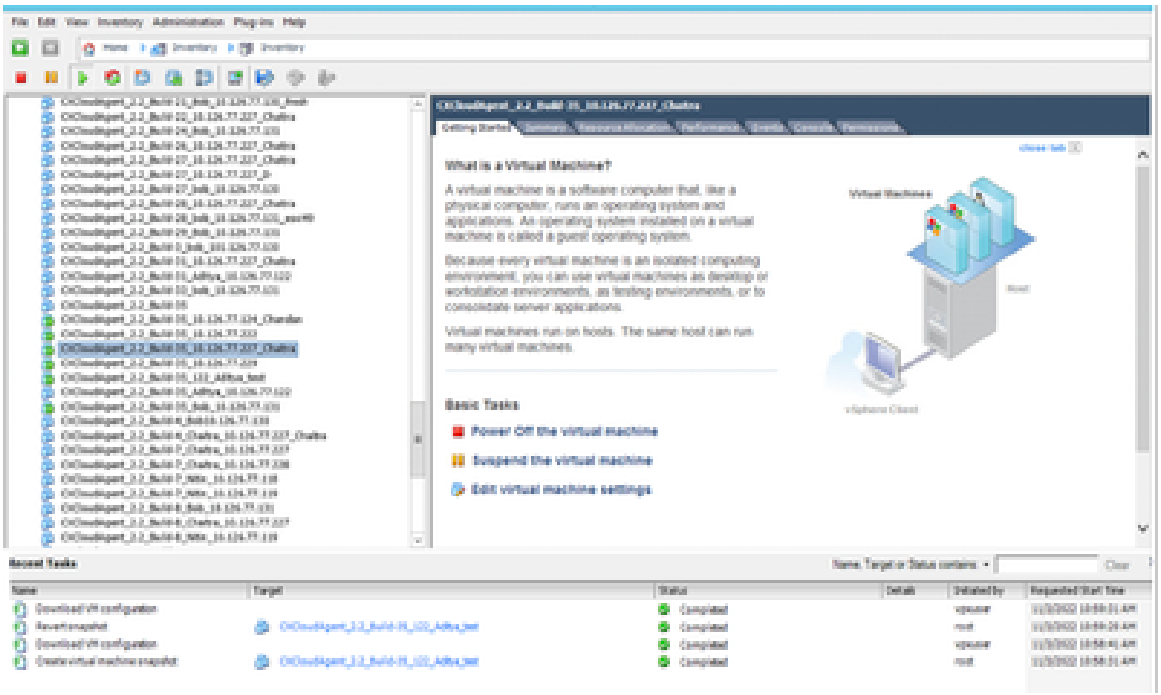
Ventana Instantáneas

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



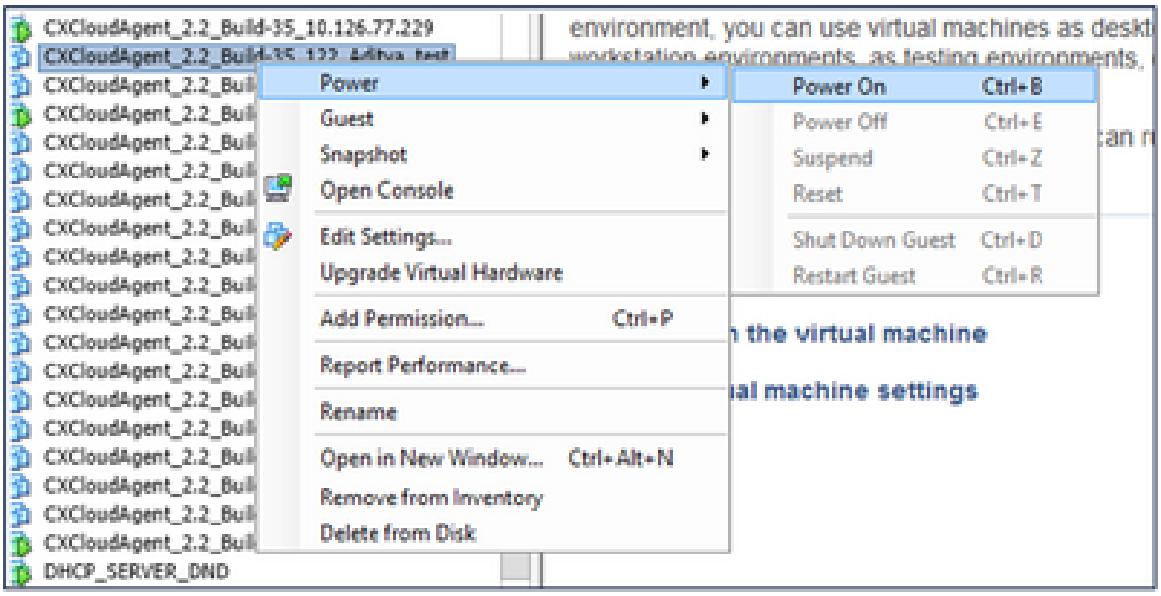
Confirmar ventana

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



Tareas recientes

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



Security

CX Cloud Agent garantiza al cliente una seguridad de extremo a extremo. La conexión entre CX Cloud y CX Cloud Agent está protegida con TLS. El usuario SSH predeterminado del Cloud Agent está limitado a realizar solo operaciones básicas.

Seguridad Física

Implemente la imagen OVA del agente de nube CX en una empresa de servidores VMware seguros. 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. Las credenciales/usuario cxcadmin se utilizan para acceder a las API del agente en la nube CX y para conectarse al dispositivo a través de SSH.

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

Seguridad de redes:

Se puede acceder a la máquina virtual del agente en la nube 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 permite al usuario autenticarse y comunicarse con el agente en la nube de 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 usando esta contraseña descifrada. La frase de paso es válida sólo 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 CX Cloud Agent cumple los estándares de consolidación del Center of Internet Security.

Seguridad de datos

El dispositivo CX Cloud Agent no almacena información personal de los clientes. La aplicación de credenciales del dispositivo (que se ejecuta como uno de los dispositivos) almacena las credenciales cifradas del servidor en 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 del centro de DNA de Cisco, al puente de diagnóstico, a la intersección, a las perspectivas de cumplimiento, a los fallos y a todas las demás fuentes de telemetría recopiladas por el agente en la nube de CX.

La información confidencial de la telemetría de activos se oculta antes de transmitirse a la nube. El agente en la nube de CX oculta los datos confidenciales de todos los recursos recopilados que envían telemetría directamente al agente en la nube de 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 en la nube de 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 DNA 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 recursos especificando las fuentes de datos como se describe en la documentación de soporte del producto para dispositivos gestionados por el controlador o en la sección Conexión de fuentes de datos de este documento (para Otros recursos recopilados por CX Cloud Agent).

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 FAQ para establecer su contraseña de cargador de arranque (modo de usuario único).
Acceso de usuario	SSH: · El acceso al dispositivo mediante el usuario cxcadmin requiere la creación de credenciales durante la instalación. · El acceso al dispositivo mediante el usuario cxcroot requiere que el personal autorizado descifre las credenciales mediante el portal SWIM.
Cuentas de usuario	· cxcadmin: cuenta de usuario predeterminada creada; el usuario puede ejecutar comandos de la aplicación Agente de nube CX usando cxcli y tiene menos privilegios en el dispositivo; el usuario cxcroot y su contraseña cifrada se generan usando cxcadmin user.

	cxcroot: cxcadmin puede crear este usuario mediante la utilidad remoteaccount; el usuario puede obtener privilegios de root con esta cuenta.
cxcadmin password policy	· La contraseña es unidireccional con SHA-256 y se almacena de forma segura. · Un mínimo de ocho (8) caracteres, que contengan tres de estas categorías: mayúsculas, minúsculas, números y caracteres especiales.
cxcroot password policy	· la contraseña cxcroot está encriptada RSA/ECB/PKCS1v1_5 · La frase de contraseña generada debe descifrarse en el portal SWIM. · El usuario cxcroot y la contraseña son válidos durante dos días y se pueden regenerar usando cxcadmin user.
ssh login password policy	· Un mínimo de ocho caracteres que contenga tres de estas categorías: mayúsculas, minúsculas, números y caracteres especiales. · Cinco intentos de inicio de sesión fallidos bloquean el equipo durante 30 minutos; la contraseña caduca en 90 días.
Puertos	Puertos entrantes abiertos: 514 (Syslog) y 22 (SSH)
Seguridad de datos	· No se almacena información del cliente. · No se almacenan datos del Equipo. · Credenciales de servidor de Cisco DNA Center cifradas y almacenadas en la base de datos.

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).