

# Descripción general de CX Cloud Agent v2.0

## Contenido

[Introducción](#)

[Prerequisites](#)

[Acceso a dominios críticos](#)

[Prerrequisitos para Actualizar a CX Cloud Agent v2.0](#)

[Versiones certificadas de Cisco DNA Center](#)

[Exploradores compatibles](#)

[Implementación de CX Cloud Agent](#)

[Conexión del agente de nube CX a la nube CX](#)

[Implementación y configuración de red](#)

[Implementación de OVA](#)

[Instalación de Thick Client ESXi 5.5/6.0](#)

[Instalación del cliente web ESXi 6.0](#)

[Instalación de Web Client vCenter](#)

[Instalación de Oracle Virtual Box 5.2.30](#)

[Instalación de Microsoft Hyper-V](#)

[Configuración de red](#)

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

[Configuración de Cisco DNA Center para reenviar Syslog a CX Cloud Agent](#)

[Requisito previo](#)

[Configuración de Syslog Forwarding](#)

[Habilitar configuración de Syslog de nivel de información](#)

[Security](#)

[Seguridad Física](#)

[Acceso de usuario](#)

[Seguridad de cuentas](#)

[Seguridad de redes:](#)

[Autenticación](#)

[Endurecimiento](#)

[Seguridad de datos](#)

[Transmisión de datos](#)

[Registros y supervisión](#)

[Resumen de seguridad](#)

[Preguntas Frecuentes](#)

[Agente de nube CX](#)

[Implementación](#)

[Versiones y parches](#)

[Autenticación y configuración de proxy](#)

[SSH de Secure Shell](#)

[Puertos y servicios](#)

[Conexión del agente en la nube CX con Cisco DNA Center](#)

[Análisis de diagnóstico de CX Cloud Agent utilizado](#)

[Registros del sistema de agentes en la nube CX](#)

[Resolución de problemas](#)

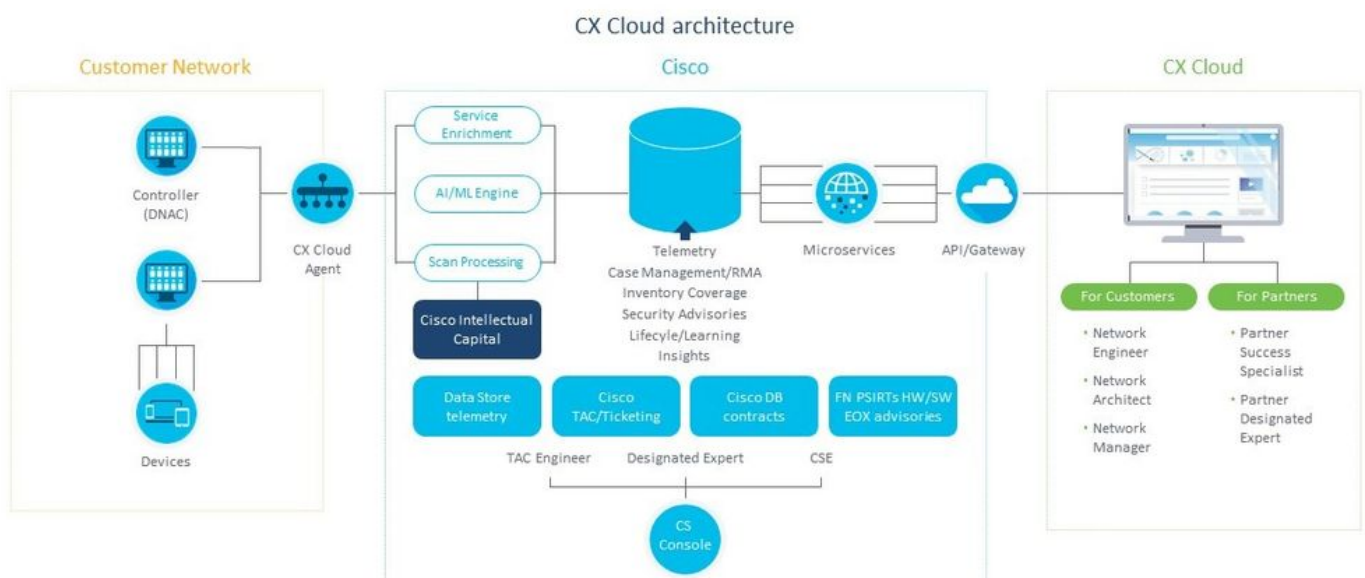
[Respuestas de fallos de recopilación](#)

[Respuestas de error de análisis de diagnóstico](#)

## Introducción

Este documento describe Cisco Customer Experience (CX) Cloud Agent. El agente en la nube de Cisco (CX) es una plataforma de software modular en las instalaciones modernizada que aloja funciones de microservicios en contenedores ligeros. Estas capacidades se pueden instalar, configurar y gestionar en las instalaciones del cliente desde la nube. CX Cloud Agent acelera la rentabilización de nuevas ofertas, amplía las capacidades y ayuda a desarrollar servicios de última generación impulsados por el Big Data, los análisis, la automatización, el aprendizaje automatizado/inteligencia artificial (ML/AI) y la transmisión.

**Nota:** Esta guía está pensada para usuarios de CX Cloud Agent v2.0. Consulte [Agente de la nube de Cisco CX](#) para obtener más información.



Arquitectura de agente de nube CX

**Nota:** Las imágenes (y el contenido de la misma) de esta guía son sólo de referencia. El contenido real puede variar.

## 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).

Requisitos para implementar:

- Cualquiera de estos hipervisores: VMWare ESXi versión 5.5 o posterior Oracle Virtual Box 5.2.30 Hipervisor de Windows versión 2012 a 2016

- 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 designados de Cisco UCS como la región de datos principal para almacenar datos de CX Cloud:  
El agente en la nube de CX debe poder conectarse a los servidores que se muestran aquí mediante el FQDN y HTTPS en el puerto TCP 443:  
FQDN: agent.us.cisco.cloud  
FQDN: ng.acs.agent.us.cisco.cloud  
FQDN: cloudssso.cisco.com  
FQDN: api-cx.cisco.com
- Para los clientes que utilizan Data Centers designados de Cisco Europe como la región de datos principal para almacenar datos de CX Cloud:  
El agente en la nube de CX debe poder conectarse a los dos 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: cloudssso.cisco.com  
FQDN: api-cx.cisco.com
- Para los clientes que utilizan Data Centers designados de Cisco para Asia-Pacífico como la región de datos principal para almacenar datos de CX Cloud:  
El agente en la nube de CX debe poder conectarse a los dos 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: cloudssso.cisco.com  
FQDN: api-cx.cisco.com
- Para los clientes que utilizan los Data Centers designados de Cisco para Europa y Cisco para Asia-Pacífico como su región de datos principal, la 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.

Otras notas sobre CX Cloud Agent:

- Una dirección IP se detectará automáticamente si se ha activado el protocolo de configuración dinámica de host (DHCP) 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 DNS.
- Sólo se admite IPv4, no IPv6.
- Se requieren las versiones 1.2.8 a 1.3.3.9 y 2.1.2.0 a 2.2.3.5 del clúster de alta disponibilidad (HA) y nodo único certificado de Cisco Digital Network Architecture (DNA) Center.
- Si la red cuenta con interceptación SSL, introduzca en la lista de permisos la dirección IP del agente en la nube CX.

## Acceso a dominios críticos

Para iniciar la transición a la nube de CX, los usuarios necesitan acceder a estos dominios.

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 la región:

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. <a href="#">cisco.cloud</a>	agent.apjc. <a href="#">cisco.cloud</a>
	ng.acs.agent.emea. <a href="#">cisco.cloud</a>	ng.acs.agent.apjc.cisco.cloud

#### Prerrequisitos para Actualizar a CX Cloud Agent v2.0

Los requisitos previos descritos en esta sección deben cumplirse antes de actualizar a CX Cloud Agent v2.0.

1. Asegúrese de que CX Cloud Agent v1.12.x y posteriores deben estar instalados antes del inicio de la actualización.
2. Siga estos pasos para configurar el servidor de nombres de dominio si aún no está configurado:  
Inicie sesión en la consola de la interfaz de línea de comandos (CLI) de la máquina virtual del agente en la nube CX. Ejecute el comando `cxcli agent configureDNS`. Introduzca la dirección IP de DNS. Haga clic `Exit`.
3. Asegúrese de que la red del cliente permite que los nombres de dominio en [Critical Domain Access](#) completen el nuevo registro del Cloud Agent durante la migración. El agente en la nube de CX debe ser capaz de alcanzar estos dominios y también los dominios deben poder resolverse desde el servidor DNS. Póngase en contacto con el equipo de red si no puede acceder a algún dominio.
4. Realice una instantánea de la VM del agente de nube antes de iniciar la actualización a la versión 2.0 (se requiere el acceso adecuado).

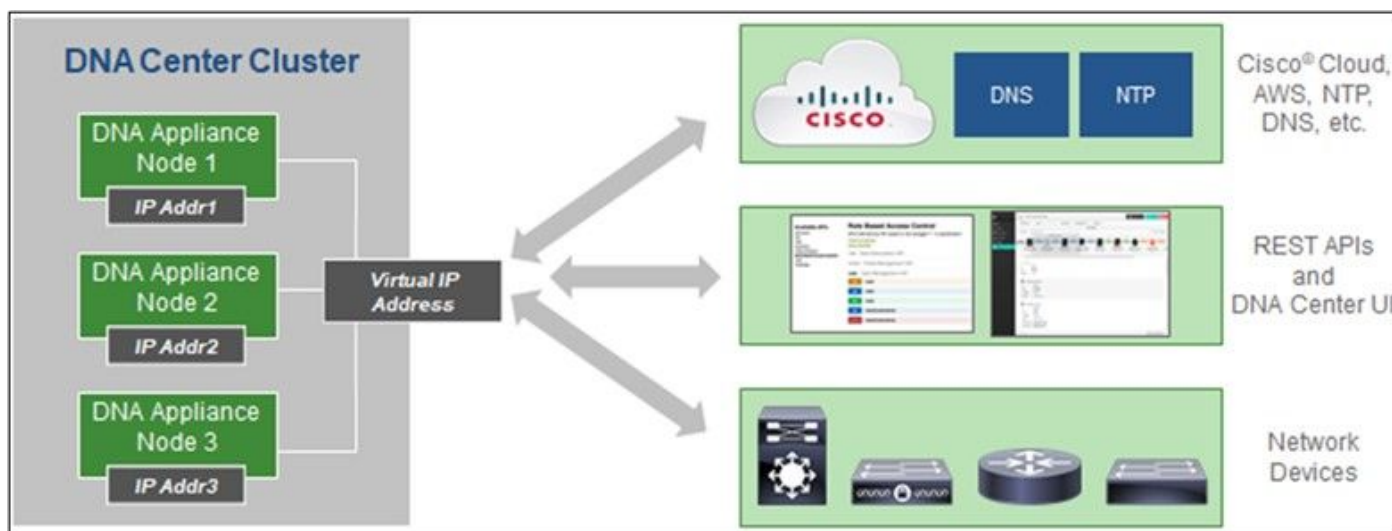
**Nota:** Las versiones anteriores a la 1.10 deben actualizarse primero a la v1.10, seguidas de actualizaciones incrementales a la v1.12.x y, a continuación, a la v2.0. Los usuarios pueden actualizar desde Admin Settings > Data Sources in CX Cloud portal. Haga clic `View Update` para completar la actualización.

Se deben cumplir las siguientes condiciones para una configuración correcta:

1. Lista de DNAC y sus credenciales
2. Usuario de DNAC con acceso al rol **Admin** o **Observer**
3. Dirección IP virtual o dirección IP física/independiente para clúster DNAC
4. Alcance satisfactorio entre Cloud Agent y DNAC
5. DNAC debe tener al menos 1 (un) dispositivo administrado

## Versiones certificadas de Cisco DNA Center

Las versiones certificadas de nodo único y clúster HA de Cisco DNA Center están comprendidas entre las versiones 1.2.8 y 1.3.3.9, y entre las versiones 2.1.2.0 y 2.2.3.5.



Clúster HA de varios nodos Cisco DNA Center

## Exploradores compatibles

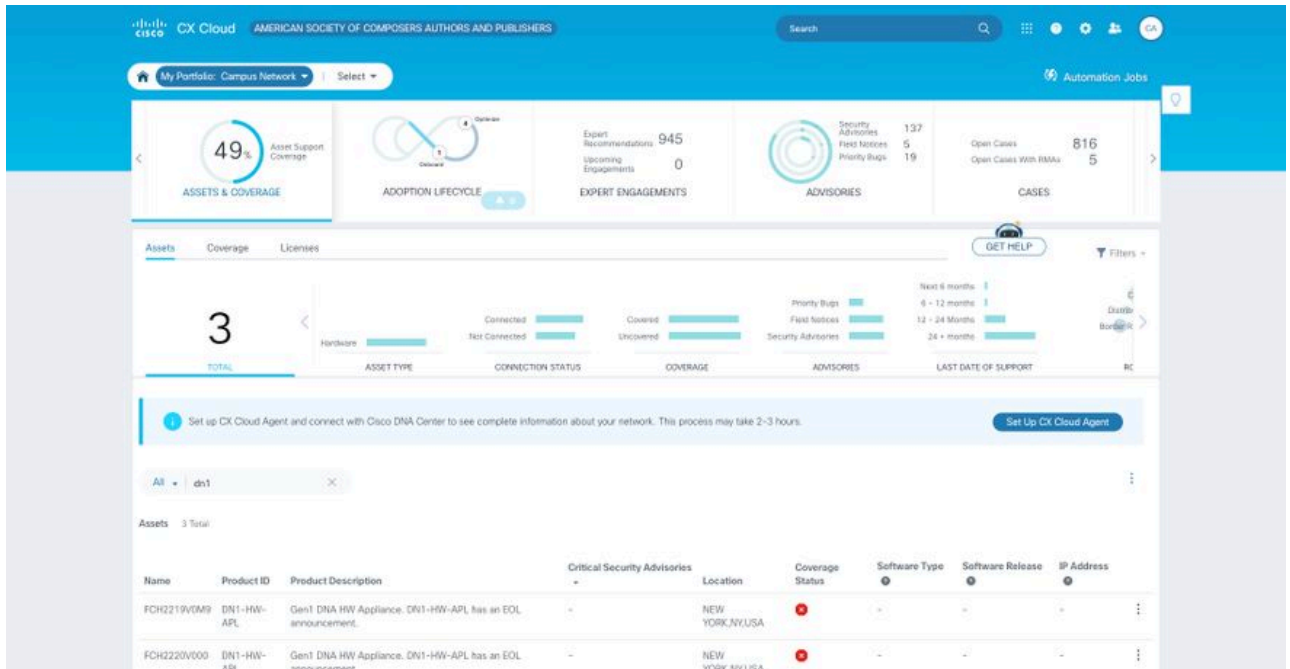
Para una mejor experiencia en Cisco.com, recomendamos la última versión oficial de estos navegadores:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

## Implementación de CX Cloud Agent

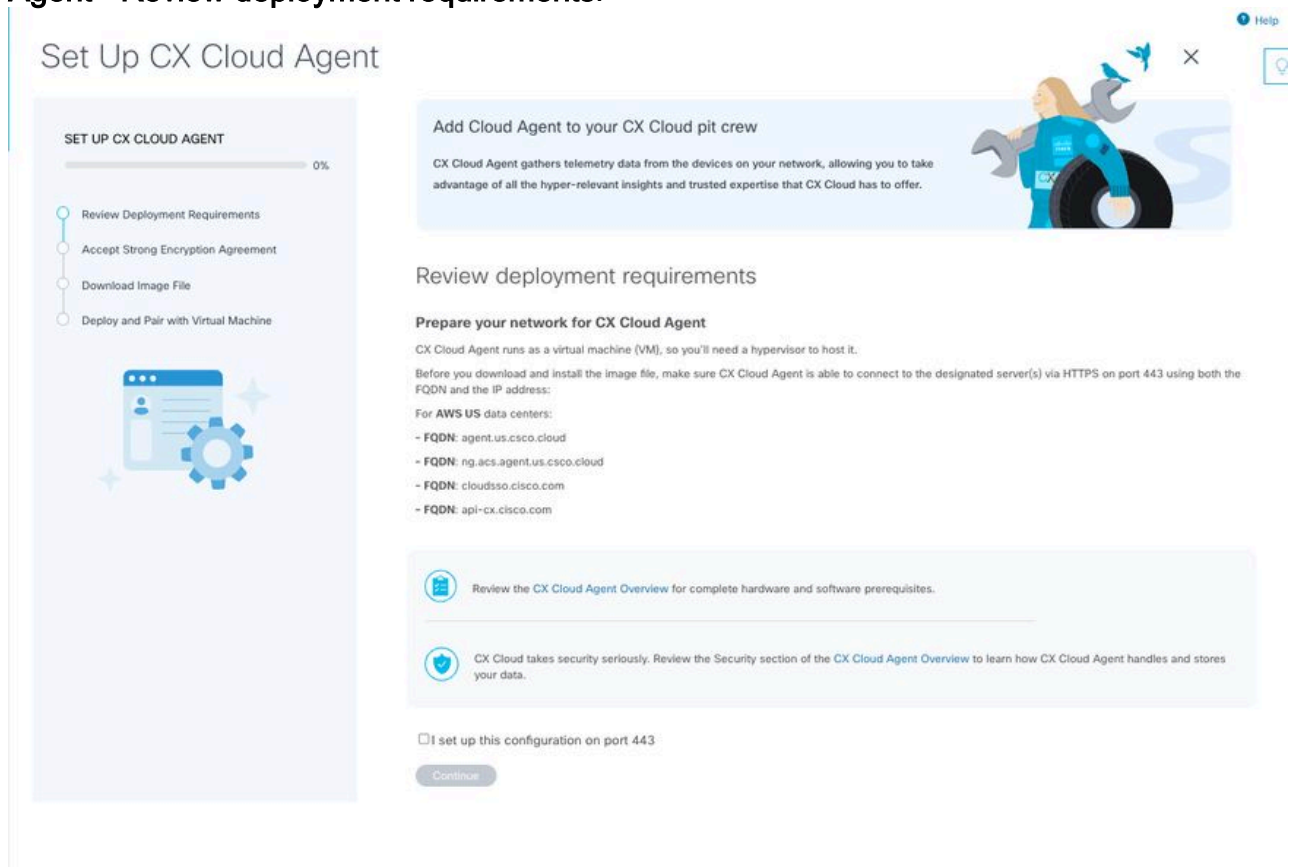
Para implementar CX Cloud Agent:

1. Haga clic en [cx.cisco.com](https://cx.cisco.com) para iniciar sesión en CX Cloud.
2. Seleccionar Campus Network y navegue hasta ASSETS & COVERAGE mosaico.



*Página de inicio*

- Haga clic en **Set Up CX Cloud Agent** en el banner. Se abre la ventana **Set Up CX Cloud Agent - Review deployment requirements**.



*Revisar los requisitos de implementación*

- Lea los requisitos previos en **Revisar requisitos de implementación** y seleccione la casilla de verificación **Yo configuré esta configuración en el puerto 443**.

**Nota:** Las imágenes (y el contenido de la misma) de esta guía son sólo de referencia. El contenido real puede variar.

- Haga clic en **Continuar**. Se abre la ventana **Set Up CX Cloud Agent - Accept the strong encryption agreement**.

**Set Up CX Cloud Agent**

25%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine

**Accept the strong encryption agreement**

Then you can download the image file for the CX Cloud Agent virtual machine.

**Instructions**

To apply for eligibility to download strong encryption software images:

1. Ensure the address listed in your [Cisco.com User Profile](#) is correct and complete.
2. Read each of the conditions below carefully prior to selecting your answer.

First Name	Last Name
Samuel	Deckard
Email	Cisco User Id
tadeckar@cisco.com	CXSuperAdmin38333

**Business Division's Function:**

- Commercial/Civilian entity
- Government entity, a Military entity or Defense Contractor

If Government entity, a Military entity or Defense Contractor, Are you in

Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom or the United States.

Yes  No

**Confirmation**

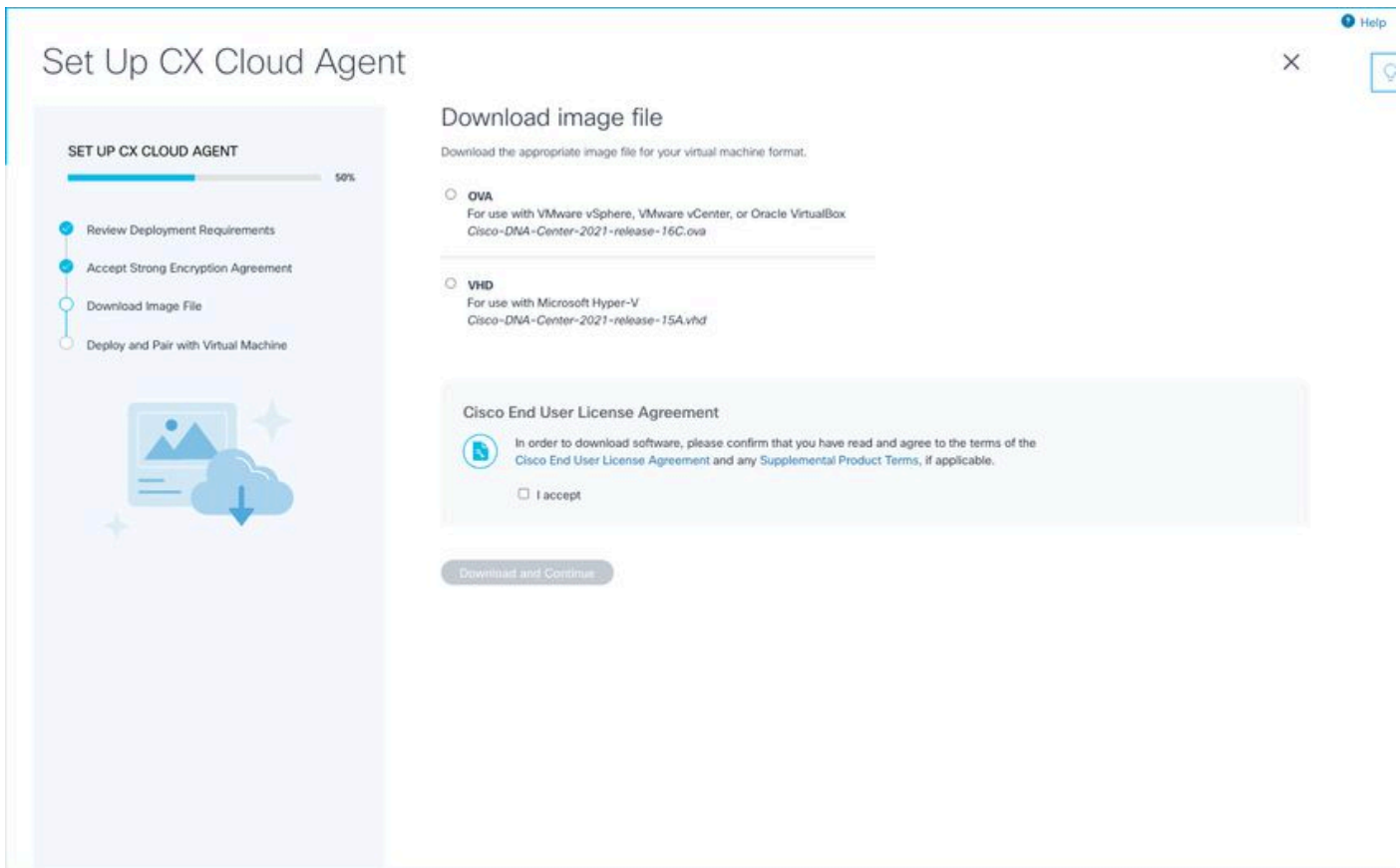
By checking this field, I hereby certify that I, as a duly authorized representative of the organization, understand and agree to abide by the conditions set forth above regarding the usage of Cisco Systems, Inc. hardware and/or software.

**Continue**

Acuerdo de cifrado

6. Verifique la información que se ha rellenado previamente en los campos **Nombre, Apellido, Correo electrónico e ID de usuario de CCO**.
7. Seleccione el **Business division's function**.
8. Seleccione el **Confirmation** para aceptar las condiciones de uso.
9. Haga clic en **Continuar**. Se abre la ventana **Set Up CX Cloud Agent - Download image file**.





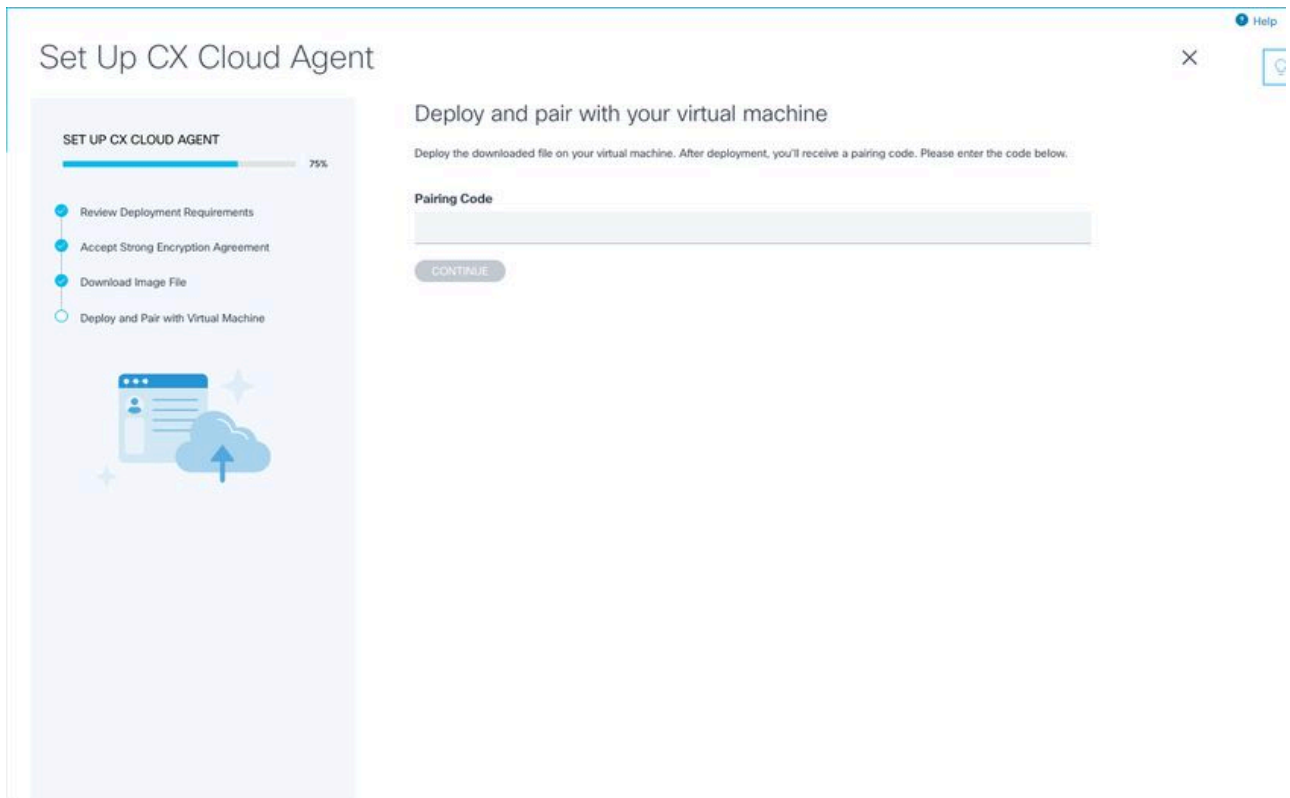
#### Descargar imagen

10. Seleccione el formato de archivo adecuado para descargar el archivo de imagen necesario para la instalación.
11. Active la casilla de verificación **I accept** para aceptar el Acuerdo de licencia del usuario final de Cisco.
12. Haga clic en **Descargar y continuar**. Se abre la ventana **Set Up CX Cloud Agent - Deploy and pair with your virtual machine**.
13. Consulte [Configuración de red](#) para la instalación de OVA y continúe con la siguiente sección para instalar CX Cloud Agent.

## Conexión del agente de nube CX a la nube CX

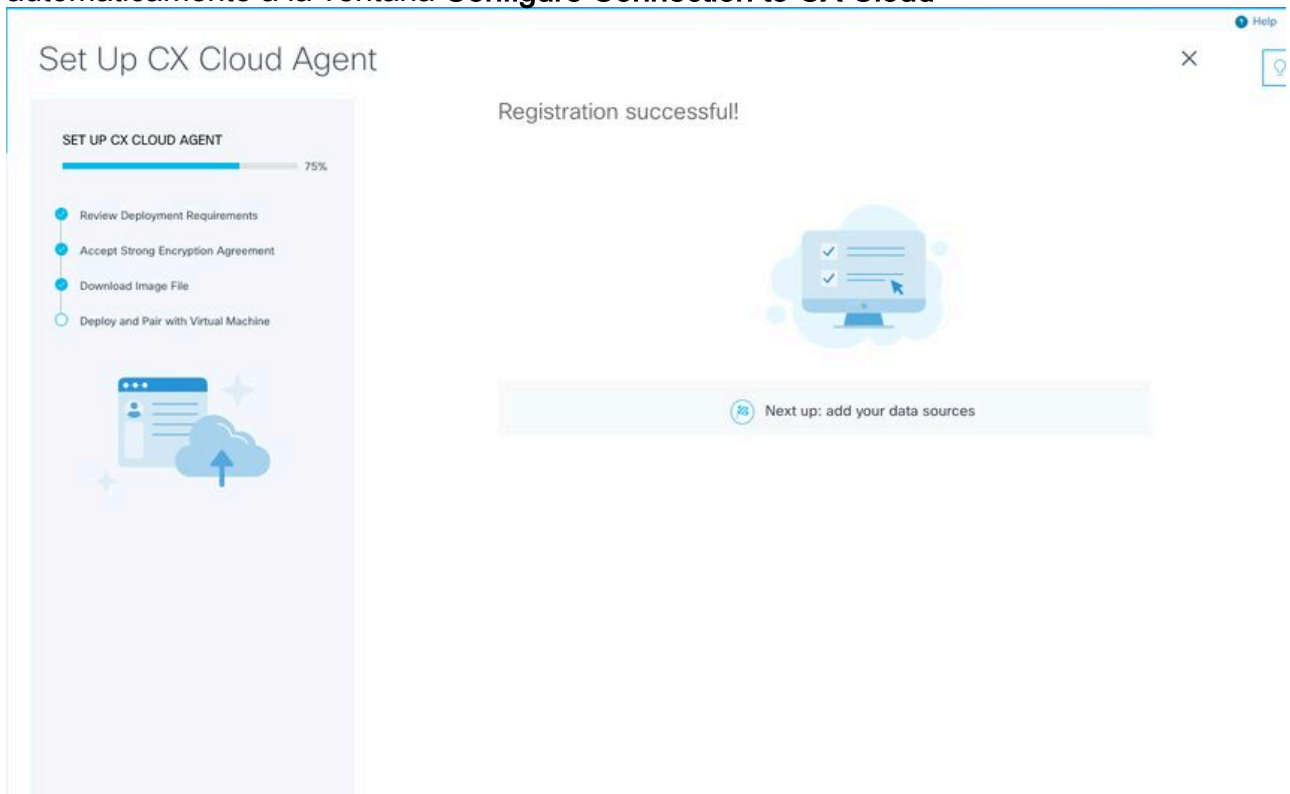
1. Ingrese el **Código de emparejamiento** proporcionado en el cuadro de diálogo de la consola o en la Interfaz de línea de comandos (CLI).





*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 muestra durante unos segundos antes de navegar automáticamente a la ventana **Configure Connection to CX Cloud**



*Registro correcto*

Help

< Back to Data Sources

Configure connection to CX Cloud

Connect a Cisco DNA Center

IP Address or FQDN Location (City, State, Country)

Username Password

Collection Frequency Time

Frequency Time IST

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

The first data source you add must be a Cisco DNA Center. After that you can add additional Cisco DNA Centers and devices not connected to a controller.


Connect This Data Source

Configurar conexión

3. Introduzca los datos y haga clic en **Conectar este origen de datos**. Se muestra el mensaje de confirmación "Conectado correctamente".

## Configure connection to CX Cloud

### Successfully Connected

 **Cisco DNA Center live.com**  
Inventory collection runs every day At 02:00 AM IST  
First inventory collection will run immediately when you finish adding your data sources

### Connect another data source to CX Cloud Agent?

+ Add Another Cisco DNA Center


Done Connecting Data Sources

DNAC agregado correctamente


**Nota:** Haga clic **Add Another Cisco DNA Center** para agregar varios DNAC.

## Configure connection to CX Cloud


### Successfully Connected



**Cisco DNA Center live.com**  
Inventory collection runs every day At 02:00 AM IST  
First inventory collection will run immediately when you finish adding your data sources



**Cisco DNA Center live.com**  
Inventory collection runs every day At 01:00 AM IST  
First inventory collection will run immediately when you finish adding your data sources



**Cisco DNA Center demo.com**  
Inventory collection runs every day At 01:00 AM IST  
First inventory collection will run immediately when you finish adding your data sources

### Connect another data source to CX Cloud Agent?



Add Another Cisco DNA Center

**Done Connecting Data Sources**

*Se han agregado varios DNAC*

4. Haga clic en **Finalizado la conexión de orígenes de datos**. Se abre la ventana **Orígenes de datos**.

Data Sources

Data Storage Region: United States

Connect Meraki Dashboard to CX Cloud to get insights and additional systems information about your Meraki assets. Get set up in about 10 minutes. [Add Meraki Dashboard](#)

[Add a Data Source](#) Search data sources

3 Total Data Sources

Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.0.3	1 minutes ago	Running
10.197.238.126	Cisco DNA Center	1 minutes ago	Reachable
22.1.90.1	Cisco DNA Center	1 minutes ago	Reachable

Orígenes de datos

## Implementación y configuración de red

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

- Si selecciona VMware vSphere/vCenter Thick Client ESXi 5.5/6.0, vaya a [Thick Client](#)
- Si selecciona VMware vSphere/vCenter Web Client ESXi 6.0, vaya a [Web Client](#) vSphere o [Center](#)
- Si selecciona Oracle Virtual Box 5.2.30, vaya a [Oracle VM](#)
- Si selecciona Microsoft Hyper-V, vaya a [Hyper-V](#)

## Implementación de OVA

### Instalación de Thick Client ESXi 5.5/6.0

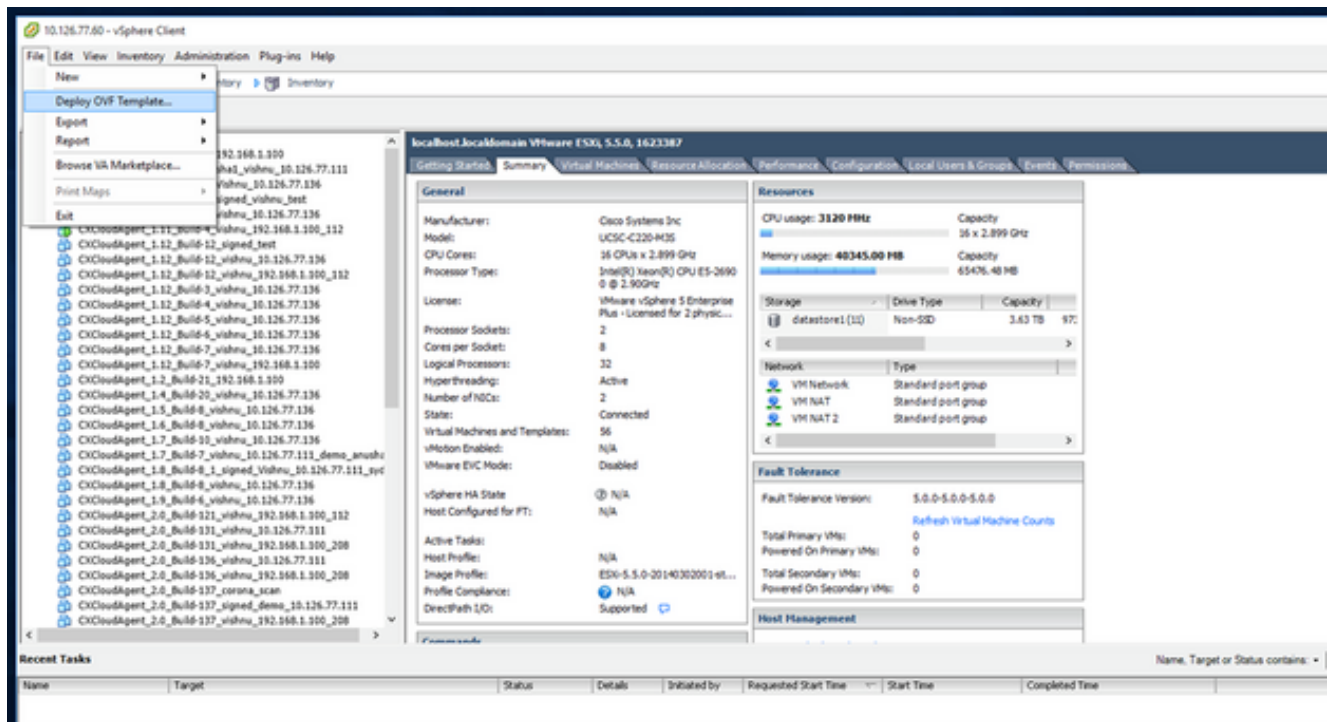
Este cliente permite la implementación de OVA de agente de nube CX mediante el uso del cliente pesado vSphere.

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



Inicio de sesión

2. Vaya a File > Deploy OVF Template.



Cliente vSphere

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

**Source**

Select the source location.

**Source**

- OVF Template Details
- Name and Location
- Disk Format
- Ready to Complete

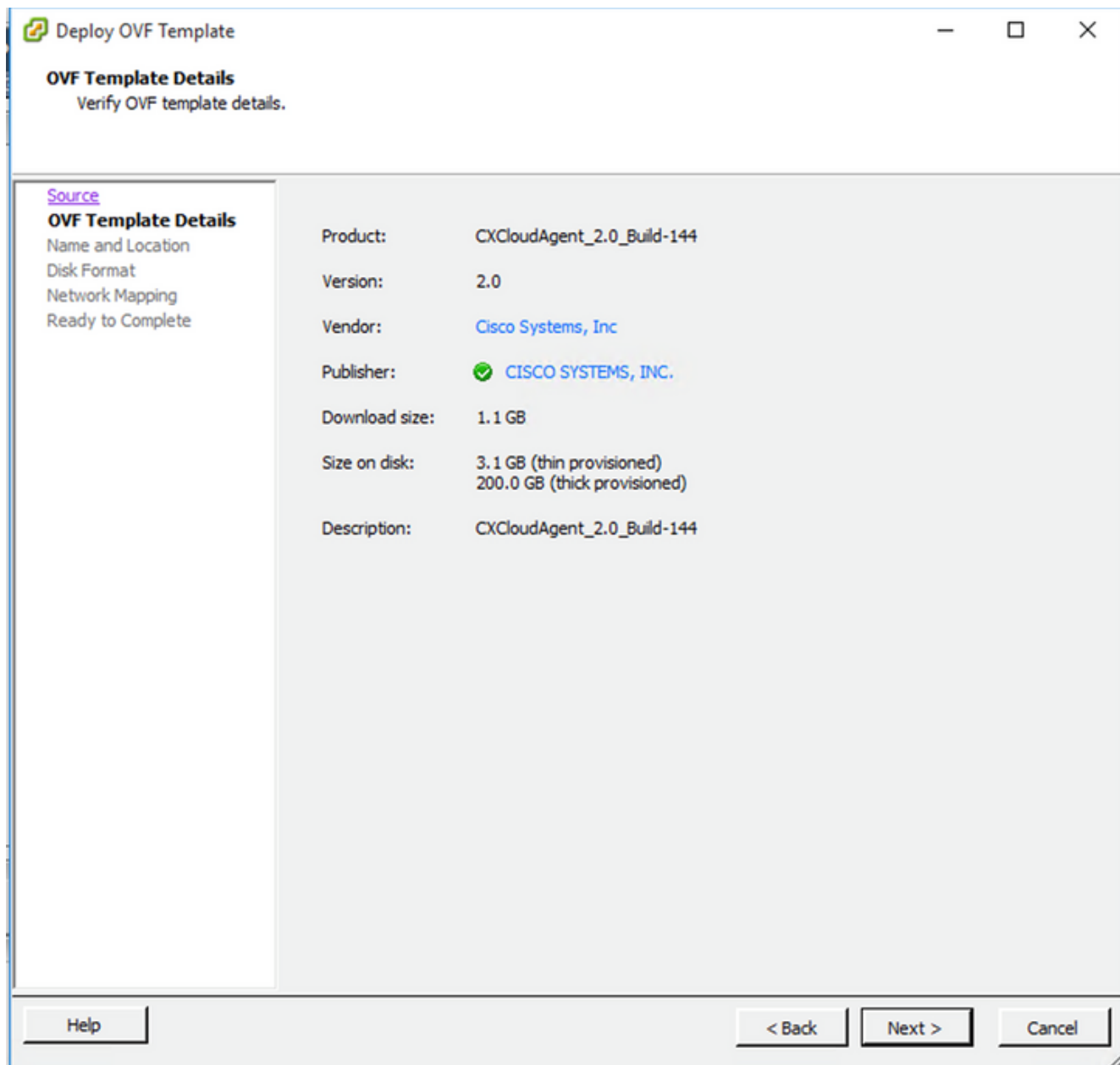
Deploy from a file or URL

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

Ruta OVA

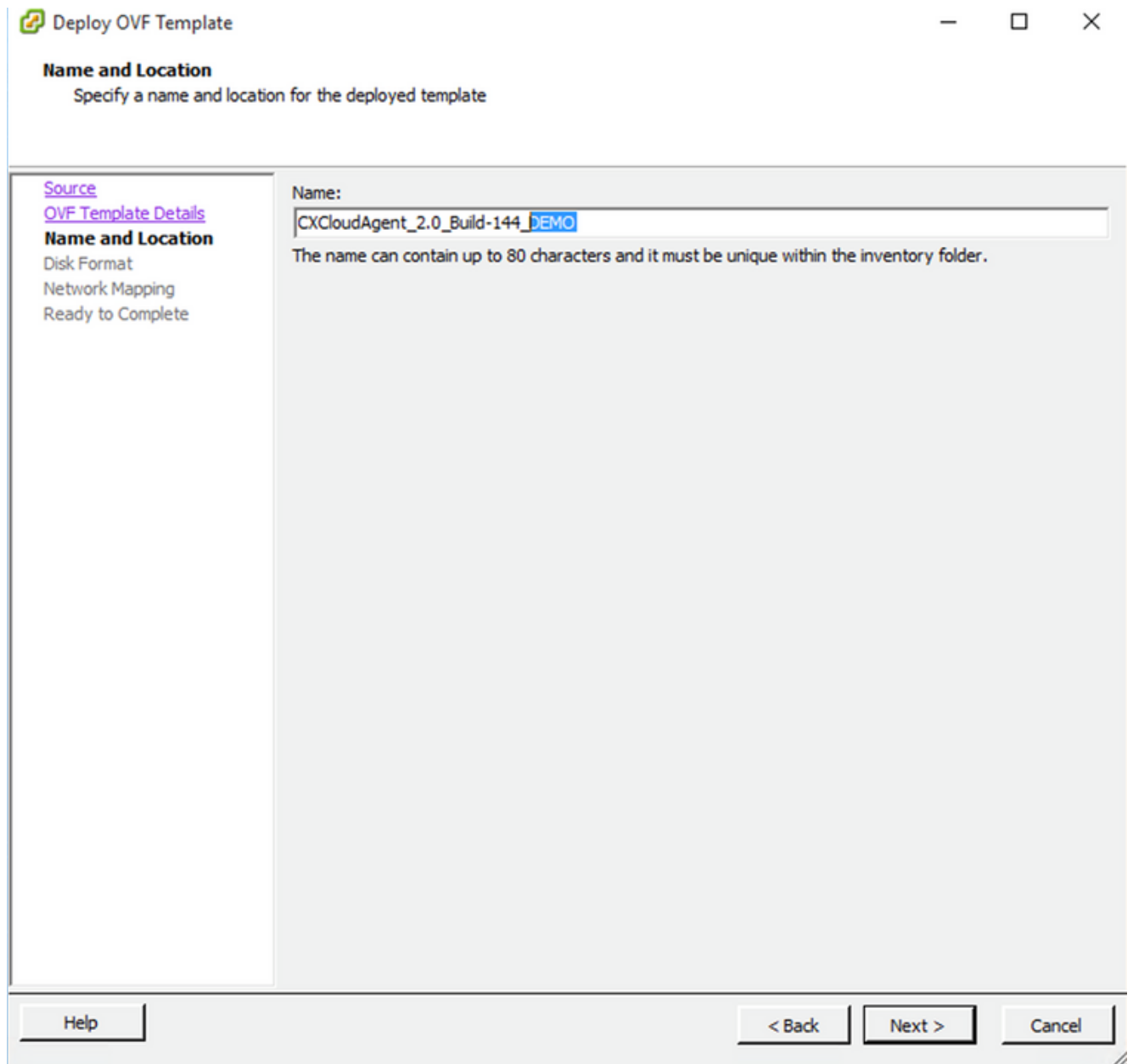
4. Verifique el OVF Details y haga clic en Next.





Detalles de plantilla

5. Introduzca un Unique Name y haga clic en Next.



Nombre y ubicación

6. Seleccione una Disk Format y haga clic en Next (Se recomienda una provisión ligera).

**Disk Format**

In which format do you want to store the virtual disks?

<a href="#">Source</a> <a href="#">OVF Template Details</a> <a href="#">Name and Location</a> <b>Disk Format</b> Network Mapping Ready to Complete	<p>Datastore: <input type="text" value="datastore1 (11)"/></p> <p>Available space (GB): <input type="text" value="973.1"/></p> <p><input type="radio"/> Thick Provision Lazy Zeroed <input type="radio"/> Thick Provision Eager Zeroed <input checked="" type="radio"/> Thin Provision</p>
---	--

Formato de disco

7. Seleccione el Power on after deployment y haga clic en Finish.

**Ready to Complete**

Are these the options you want to use?

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

When you click Finish, the deployment task will be started.

Deployment settings:

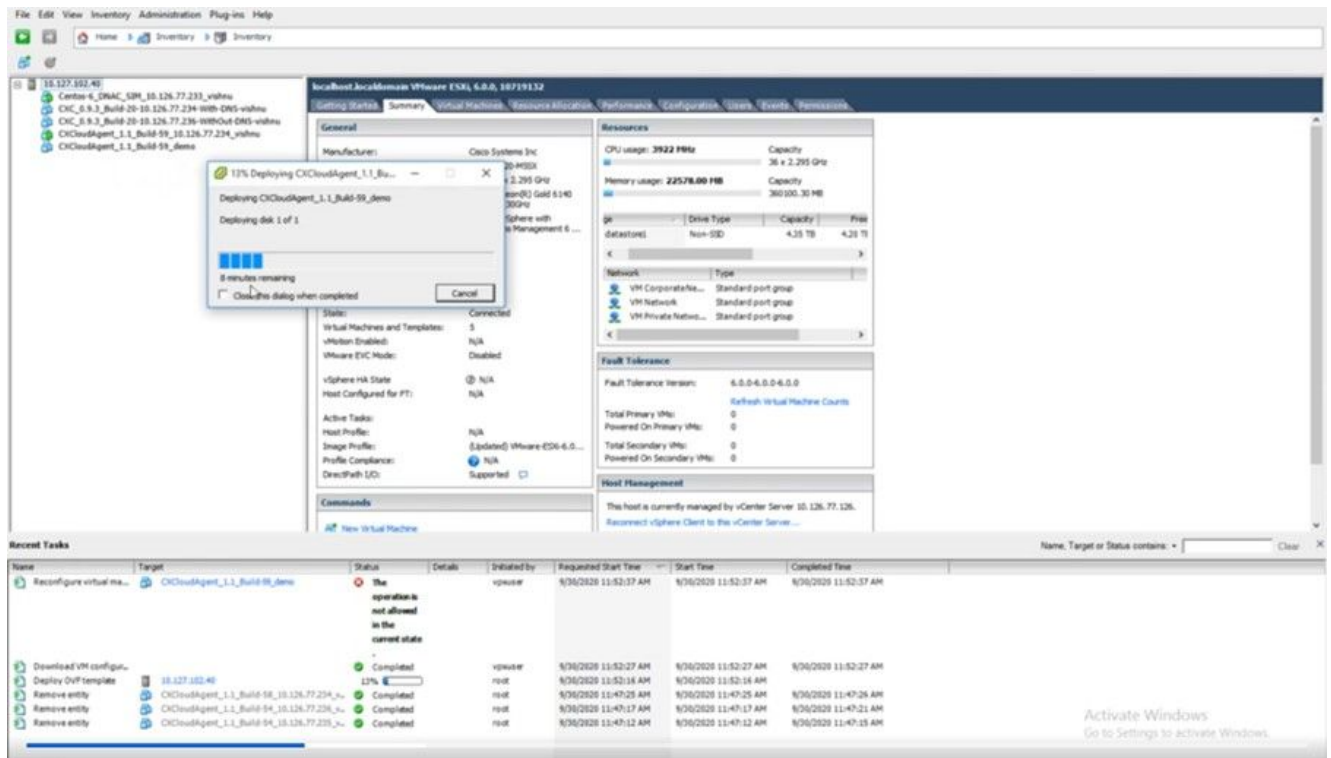
OVF file:	C:\Users\oxcadmin\Downloads\OVA\CXCloudAgent_2.0...
Download size:	1.1 GB
Size on disk:	3.1 GB
Name:	CXCloudAgent_2.0_Build-144_DEMO
Host/Cluster:	localhost
Datastore:	datastore1 (11)
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"

Power on after deployment

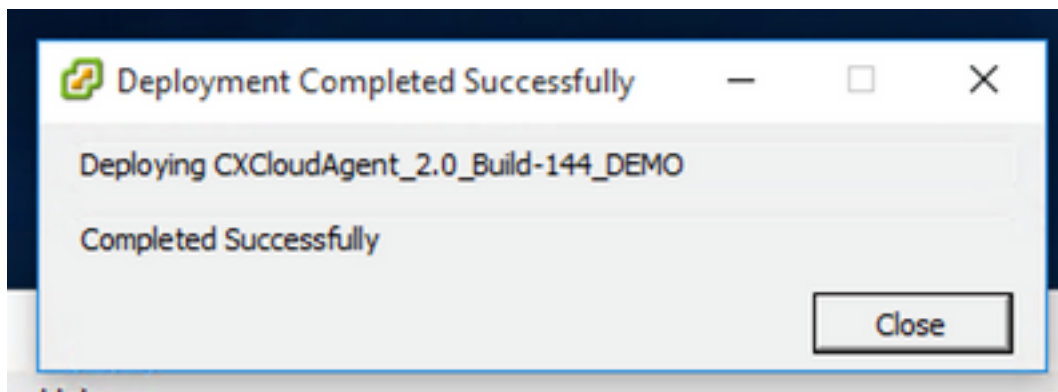
Help < Back Finish Cancel

Listo para completar

La implementación puede tardar varios minutos. Espere hasta que aparezca un mensaje de confirmación.



Implementación en curso



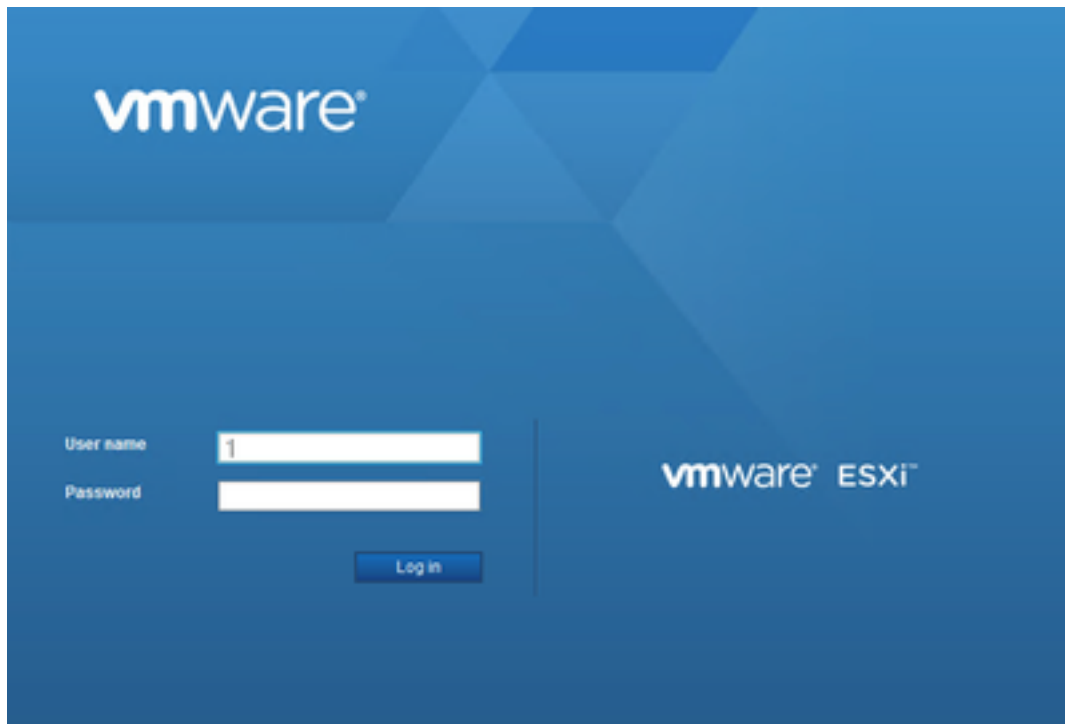
Implementación completada

8. Seleccione la máquina virtual que acaba de implementar, abra la consola y vaya a [Configuración de red](#).

## Instalación del cliente web ESXi 6.0

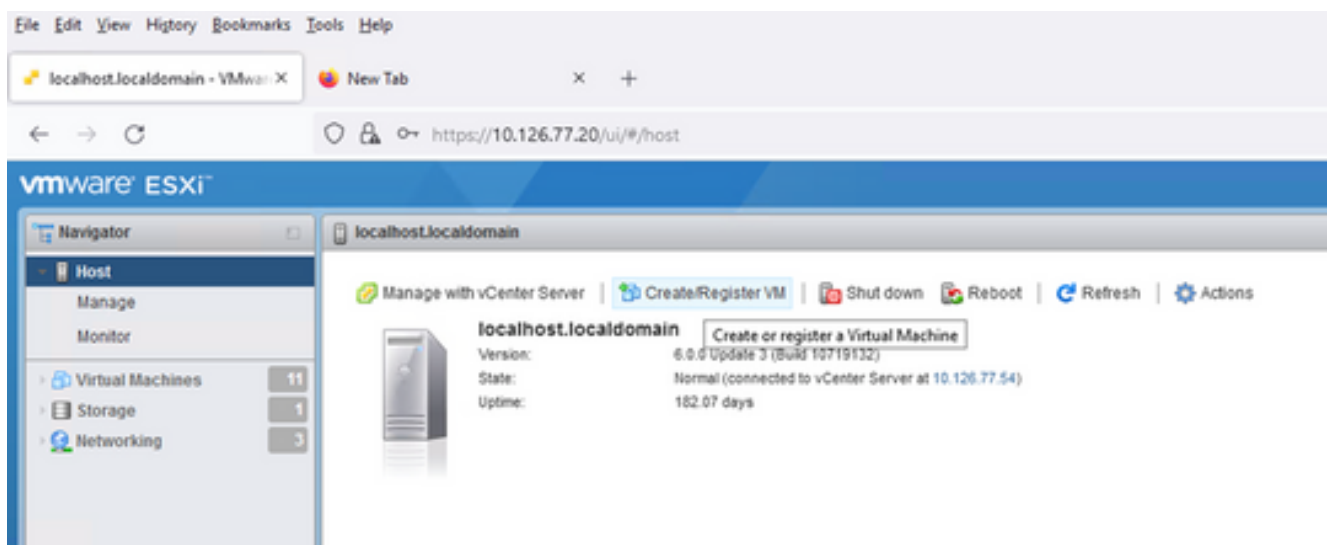
Este cliente implementa OVA de CX Cloud Agent mediante la Web de vSphere.

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

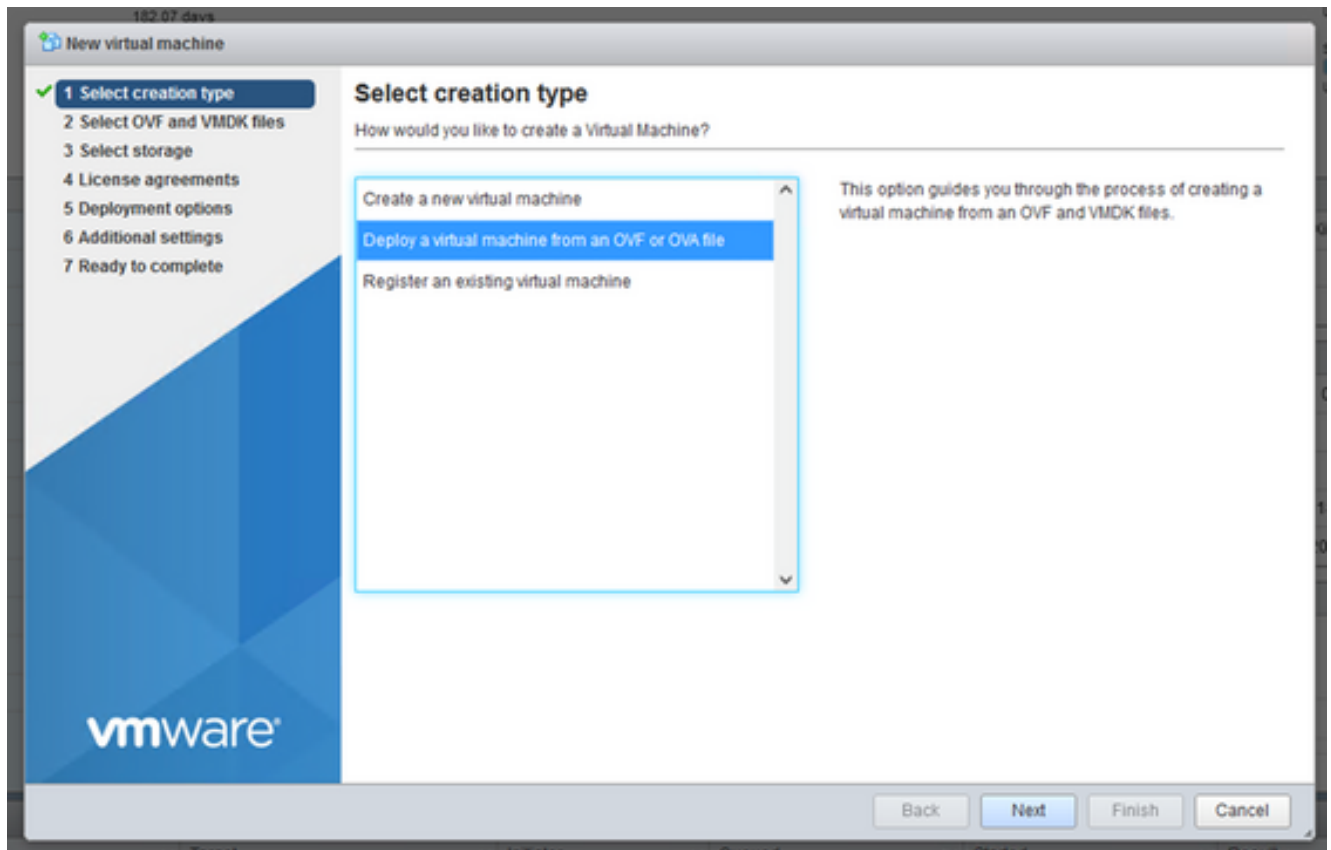


Inicio de sesión de VMware ESXi

2. Seleccionar Virtual Machine > Create / Register VM.

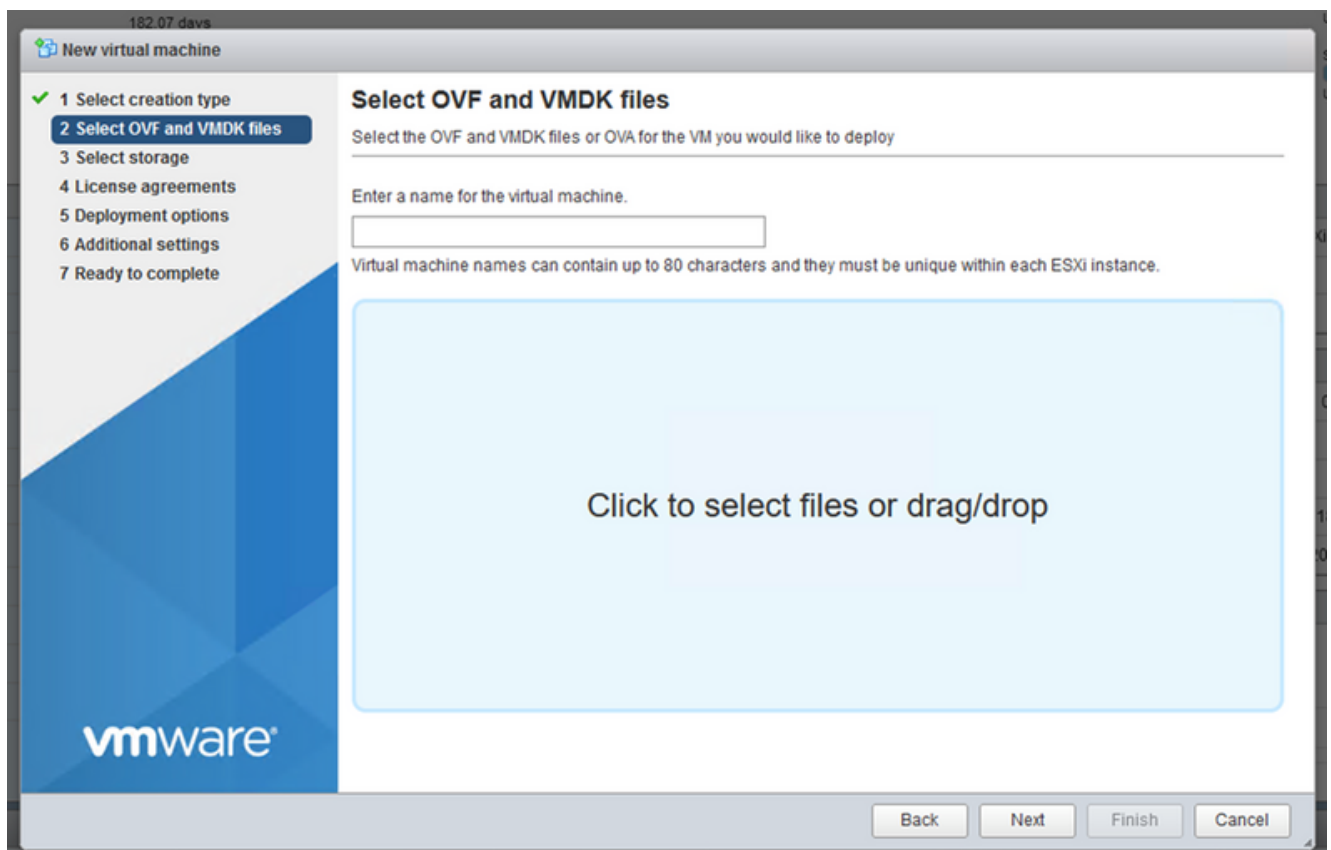


Crear VM



Implementación de OVA

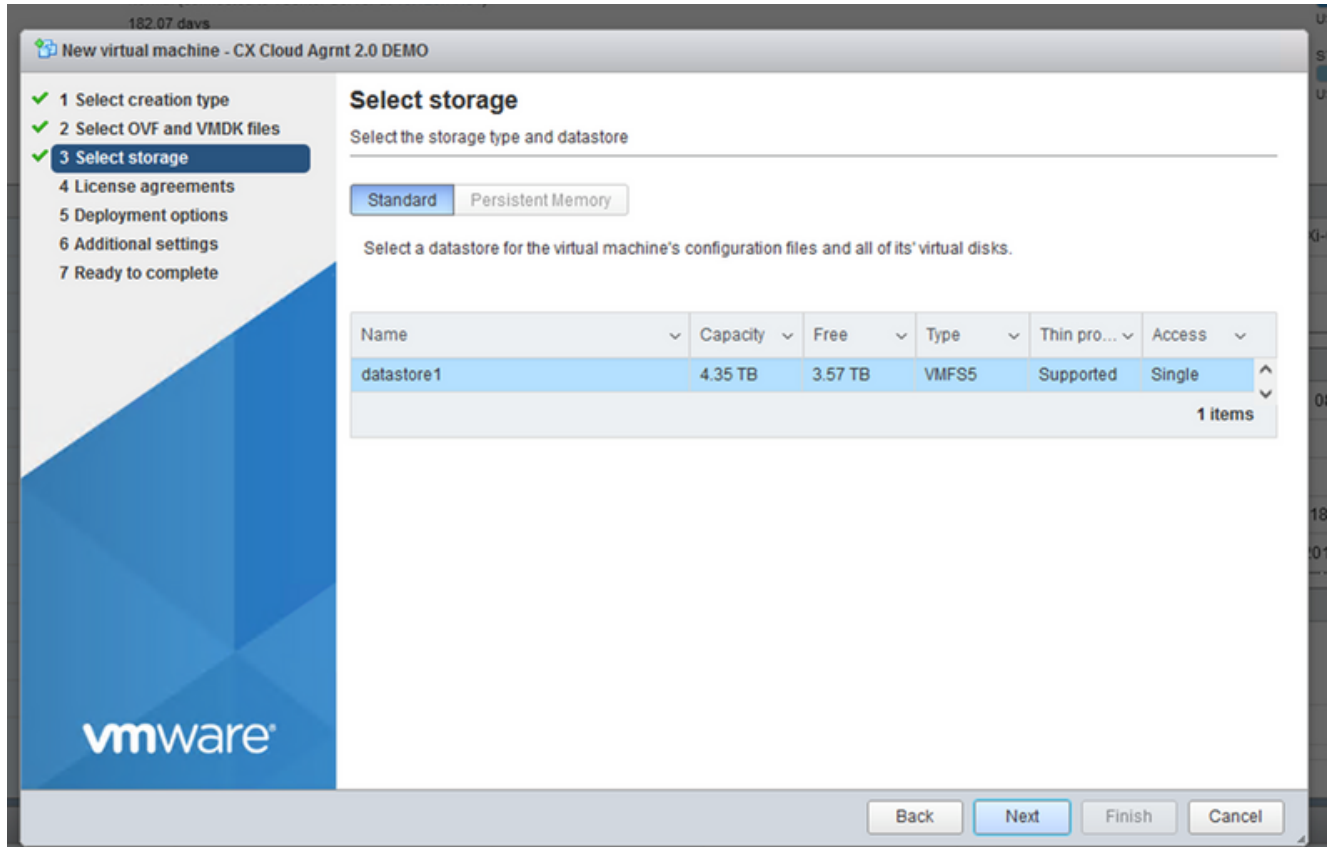
3. Seleccionar Deploy a virtual machine from an OVF or OVA file y haga clic en Next.
4. Introduzca el nombre de la máquina virtual, navegue para seleccionar el archivo o arrastre y suelte el archivo OVA descargado.
5. Haga clic Next.



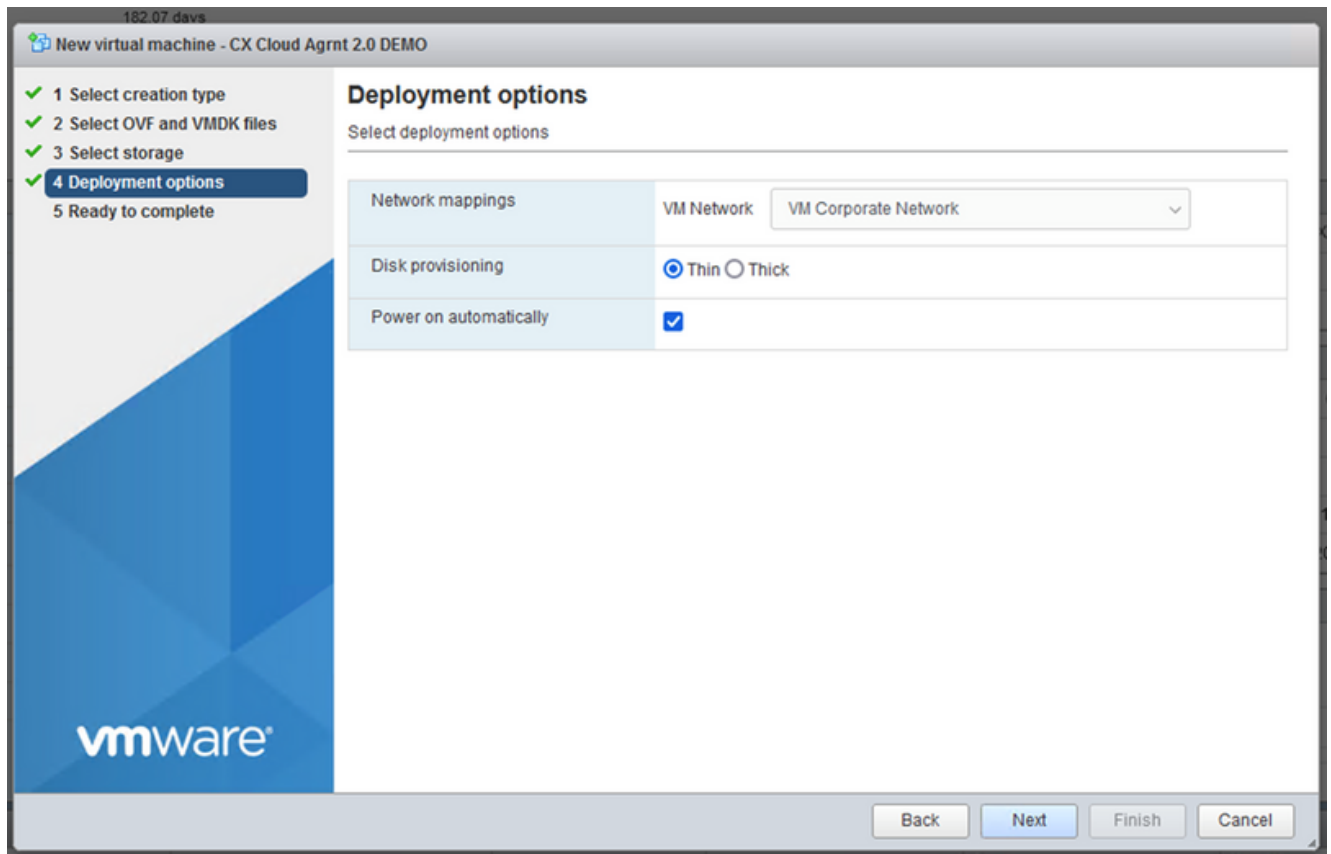
Selección de OVA



6. Seleccionar Standard Storage y haga clic en Next.

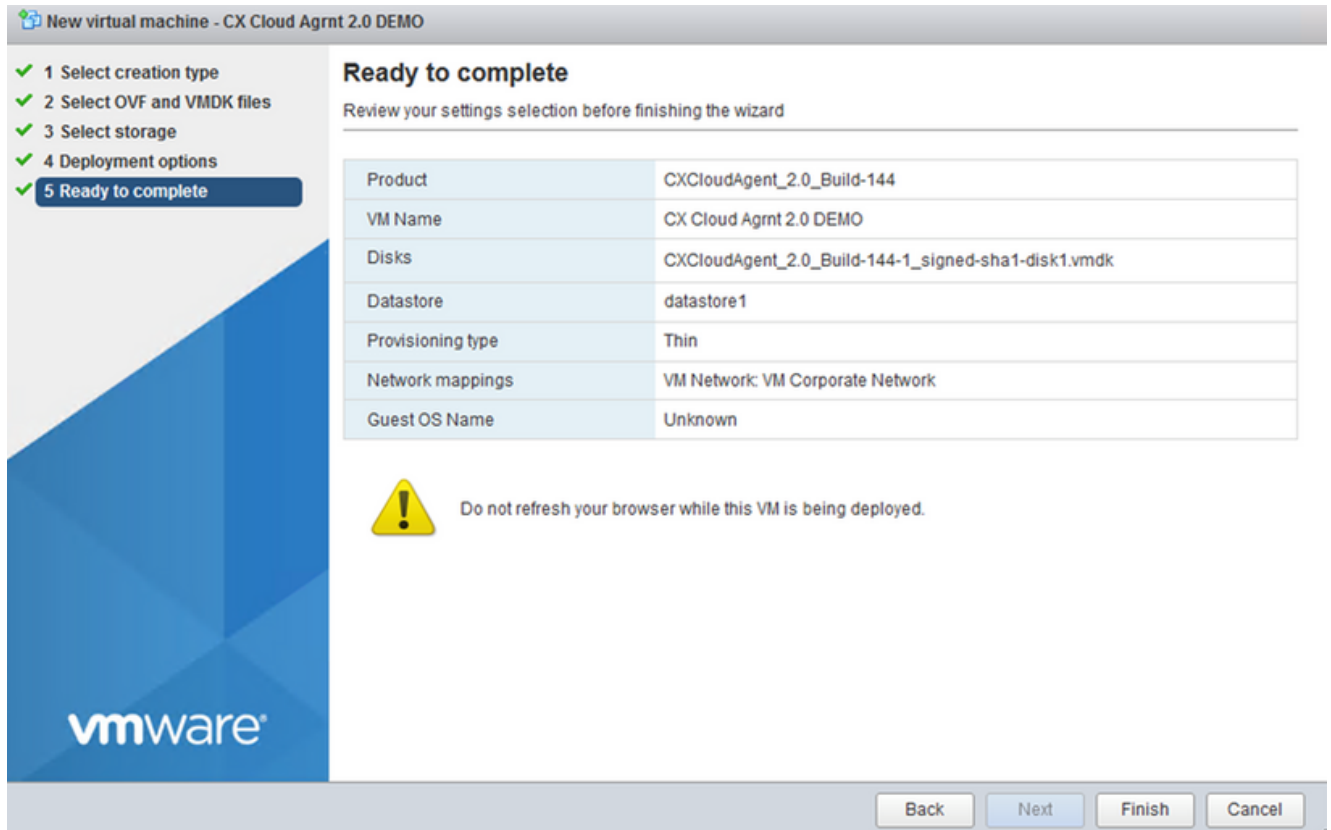


Seleccionar almacenamiento

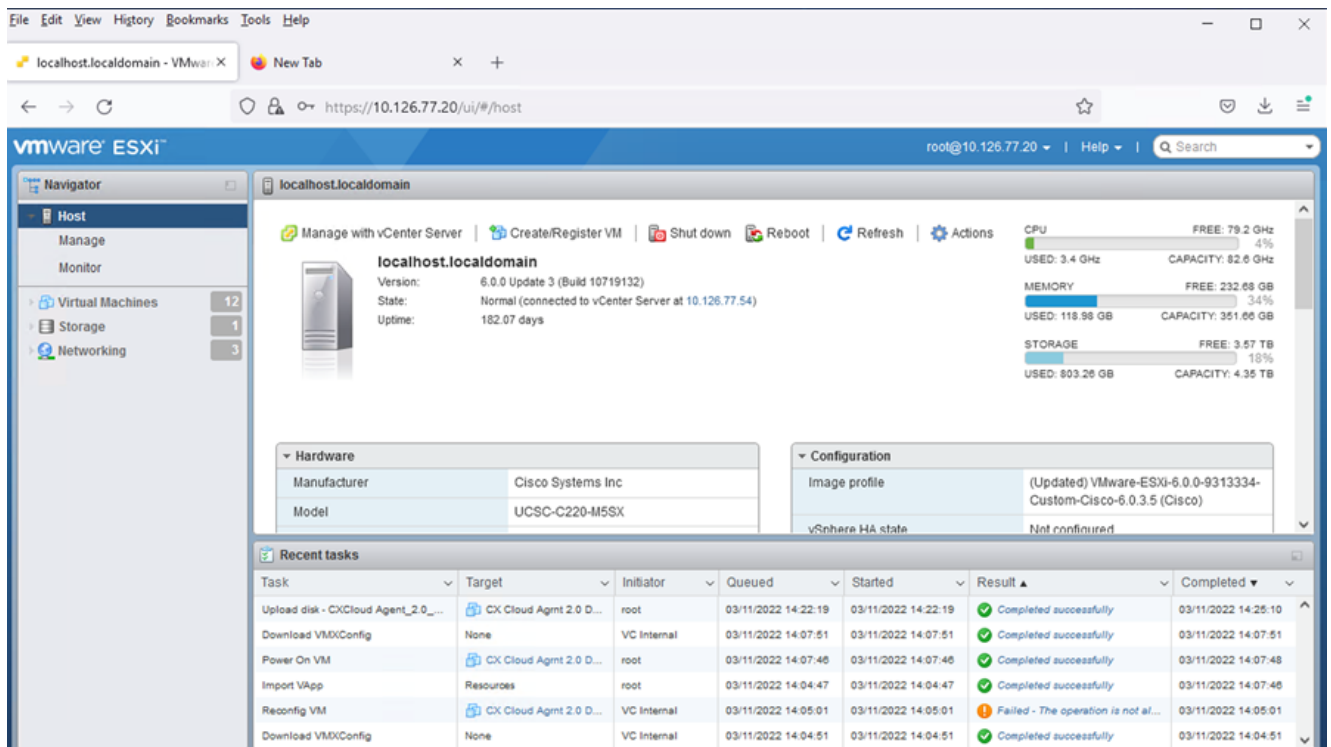


Opciones de implementación

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



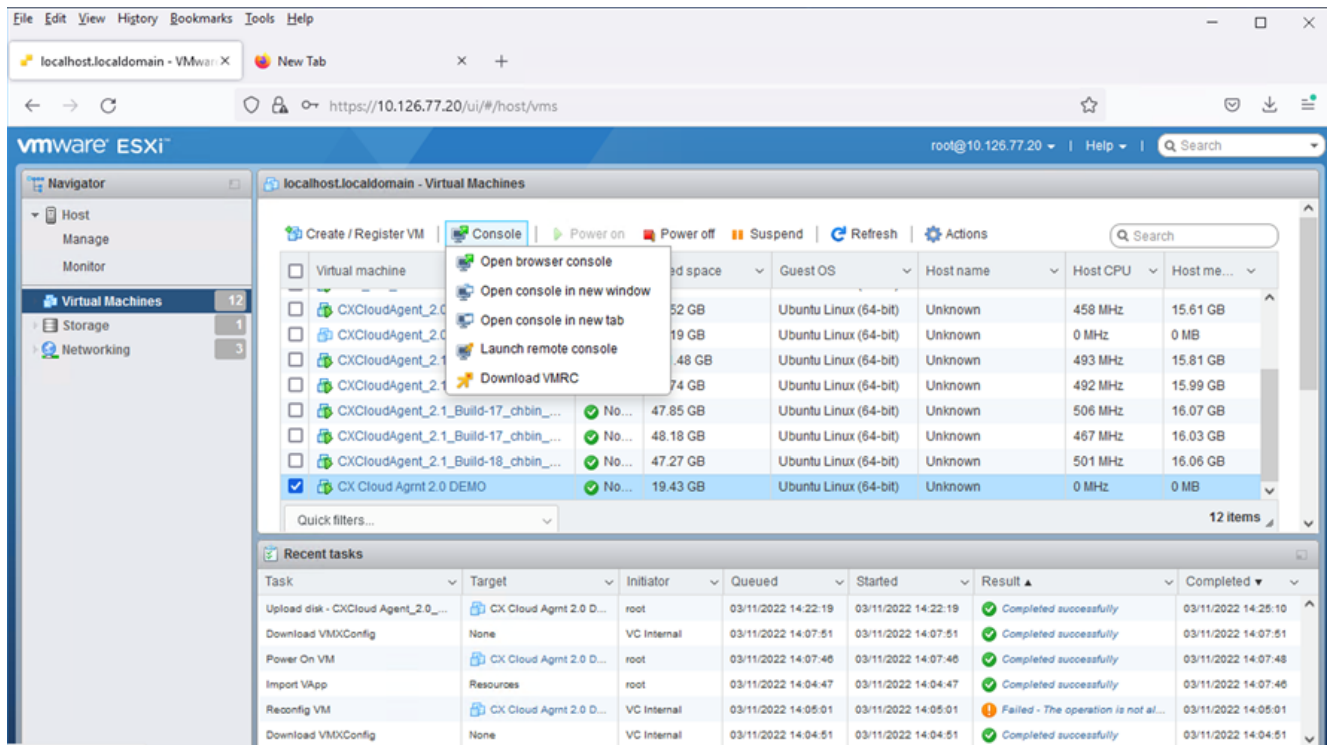
Listo para completar



Finalización correcta

8. Revise los parámetros y haga clic en Finish.

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



Abrir consola

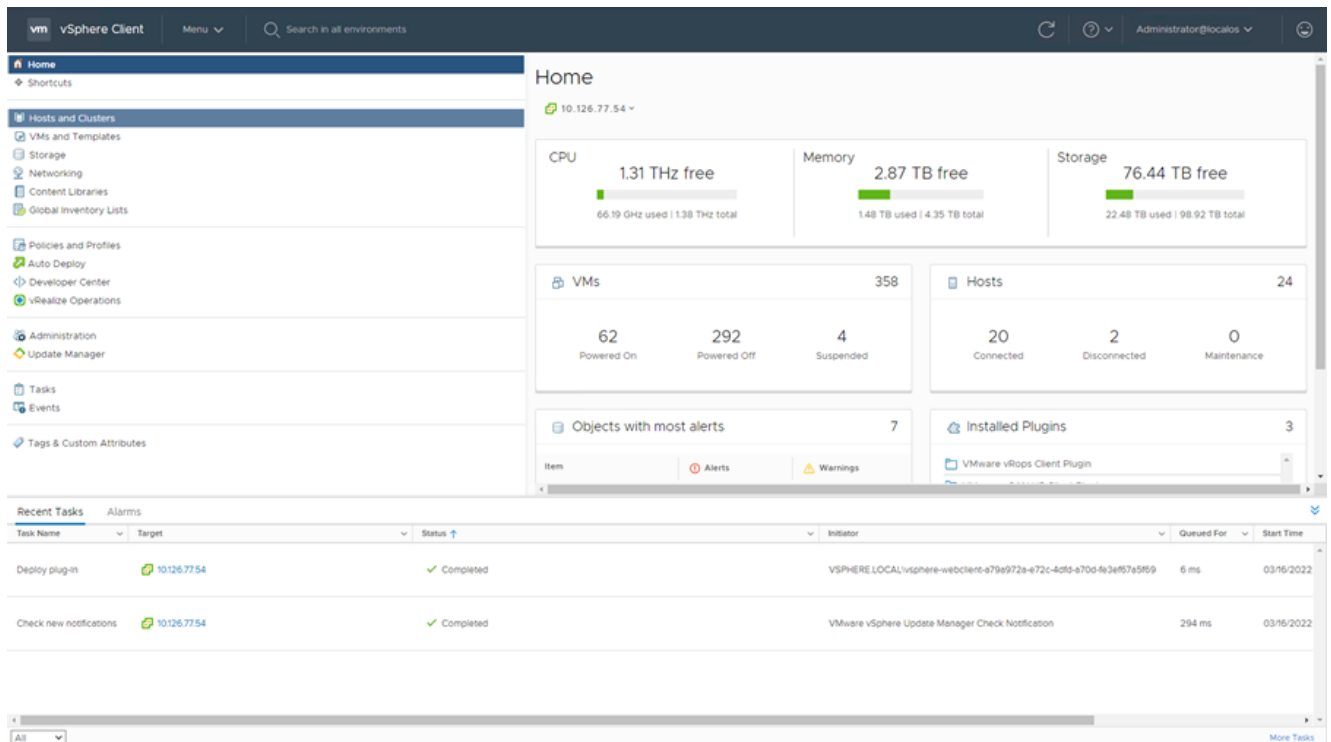
10. Vaya a [Network Configuration](#).

## Instalación de Web Client vCenter

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

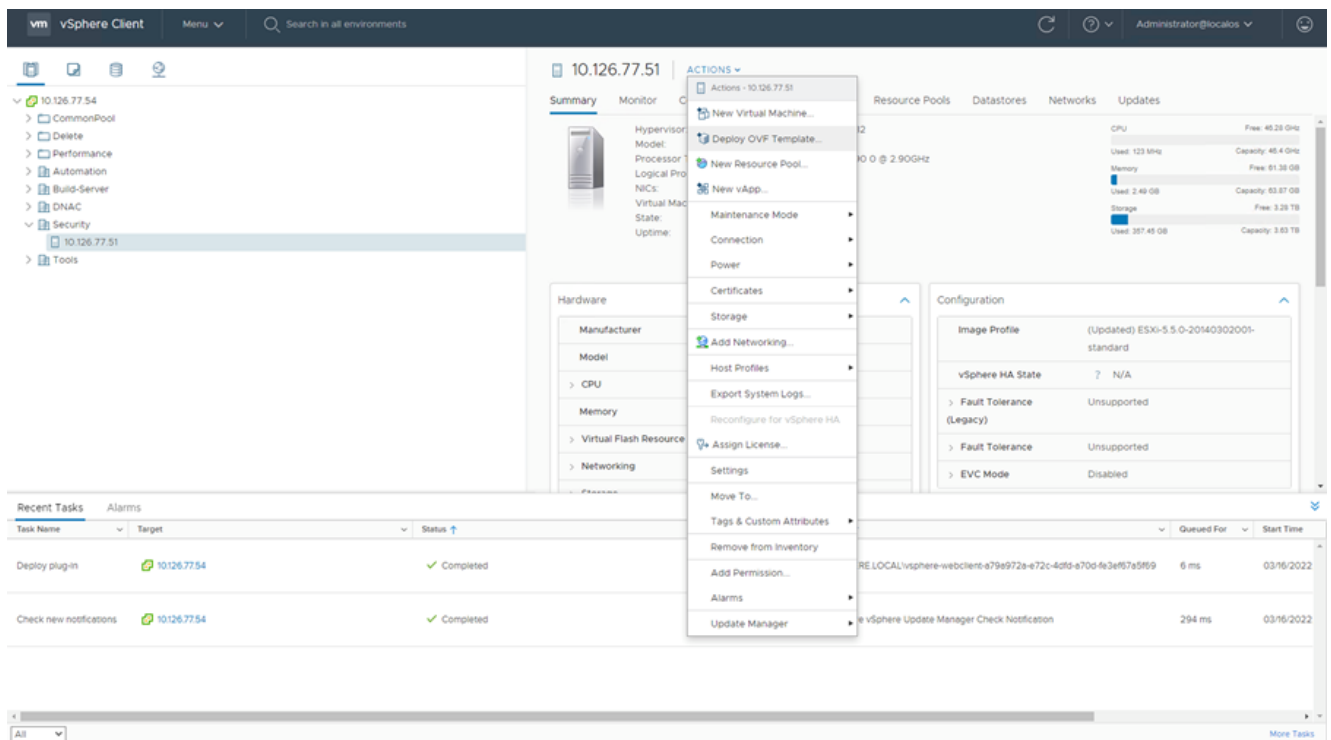


Inicio de sesión

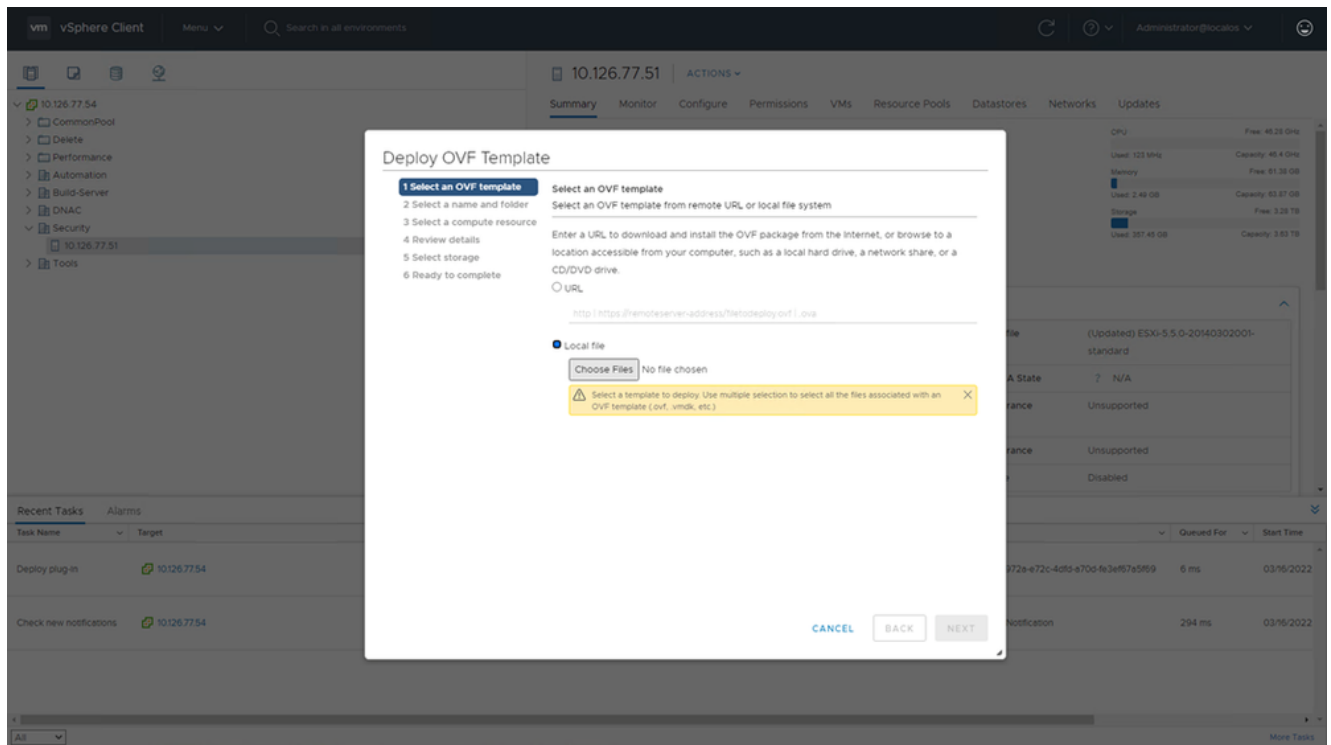


## Pantalla de inicio

2. En la página de inicio, haga clic en Hosts and Clusters.
3. Seleccione la máquina virtual y haga clic en Action > Deploy OVF Template.



## 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 es necesario.
6. Haga clic Next.

## Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: CXCloudAgent\_2.0\_Build-144-demo

Select a location for the virtual machine.

10.126.77.54

> CommonPool

> Delete

> Performance

> Automation

> Build-Server

> DNAC

> Security

> Tools

CANCEL

BACK

NEXT

Nombre y carpeta

7. Seleccione el recurso informático y haga clic en Next.

## Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

**3 Select a compute resource**

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

▼ Security

> 10.126.77.51

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

Seleccionar recurso de cálculo

8. Revise los detalles y haga clic en Next.



## Deploy OVF Template

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

### Review details

Verify the template details.

Publisher	DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate)
Product	CXCloudAgent_2.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CXCloudAgent_2.0_Build-144
Download size	1.1 GB
Size on disk	3.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

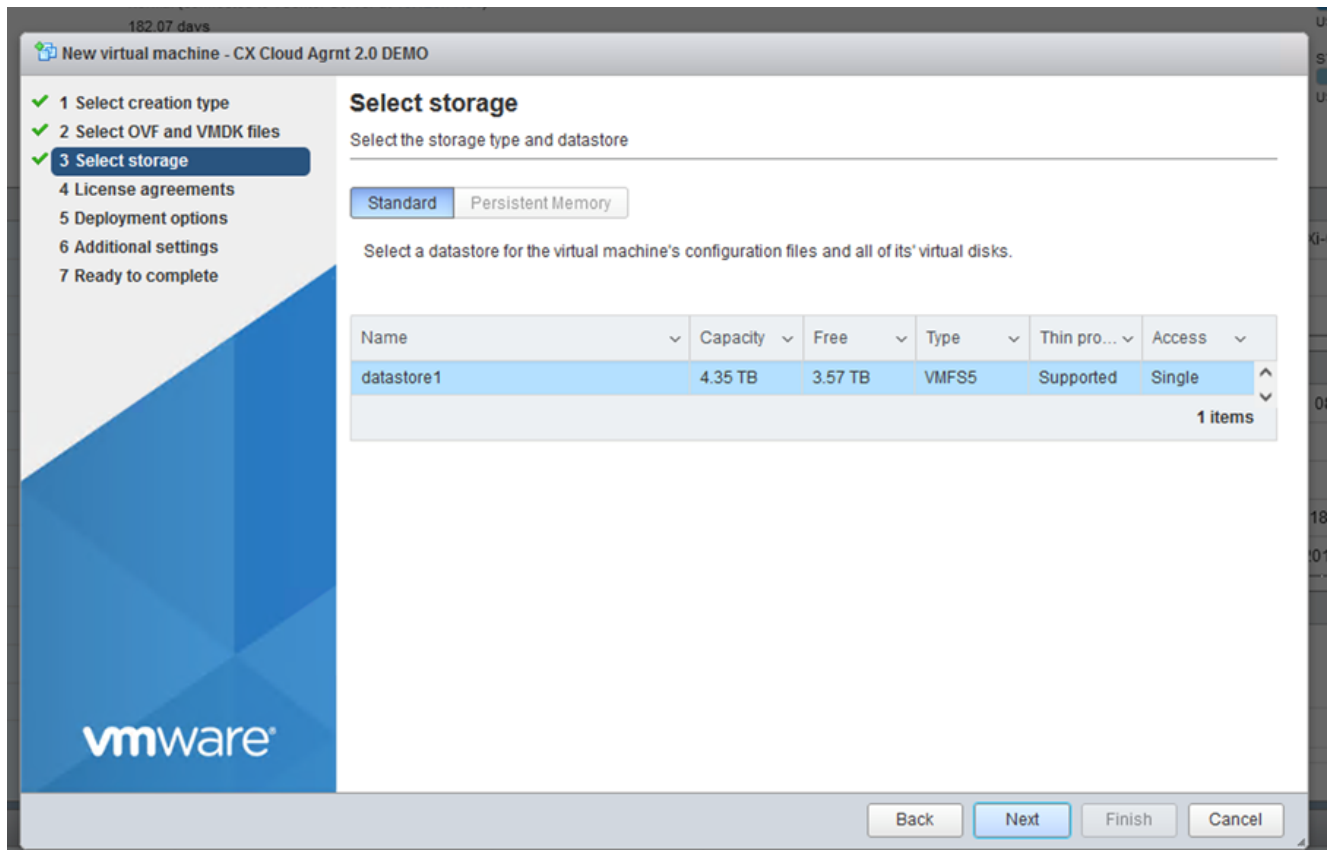
CANCEL

BACK

NEXT

Revisar detalles

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



Seleccionar almacenamiento

10. Haga clic Next.

## Deploy OVF Template

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

### Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 items

### IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

Seleccionar redes

11. Haga clic Finish.

## Deploy OVF Template

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

Ready to complete

Click Finish to start creation.

Provisioning type	Deploy from template
Name	CXCloudAgent_2.0_Build-144-demo
Template name	CXCloudAgent_2.0_Build-144-1_signed-sha1
Download size	1.1 GB
Size on disk	3.1 GB
Folder	Security
Resource	10.126.77.51
Storage mapping	1
All disks	Datastore: datastore1 (23); Format: Thin provision
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

CANCEL

BACK

FINISH

Listo para completar

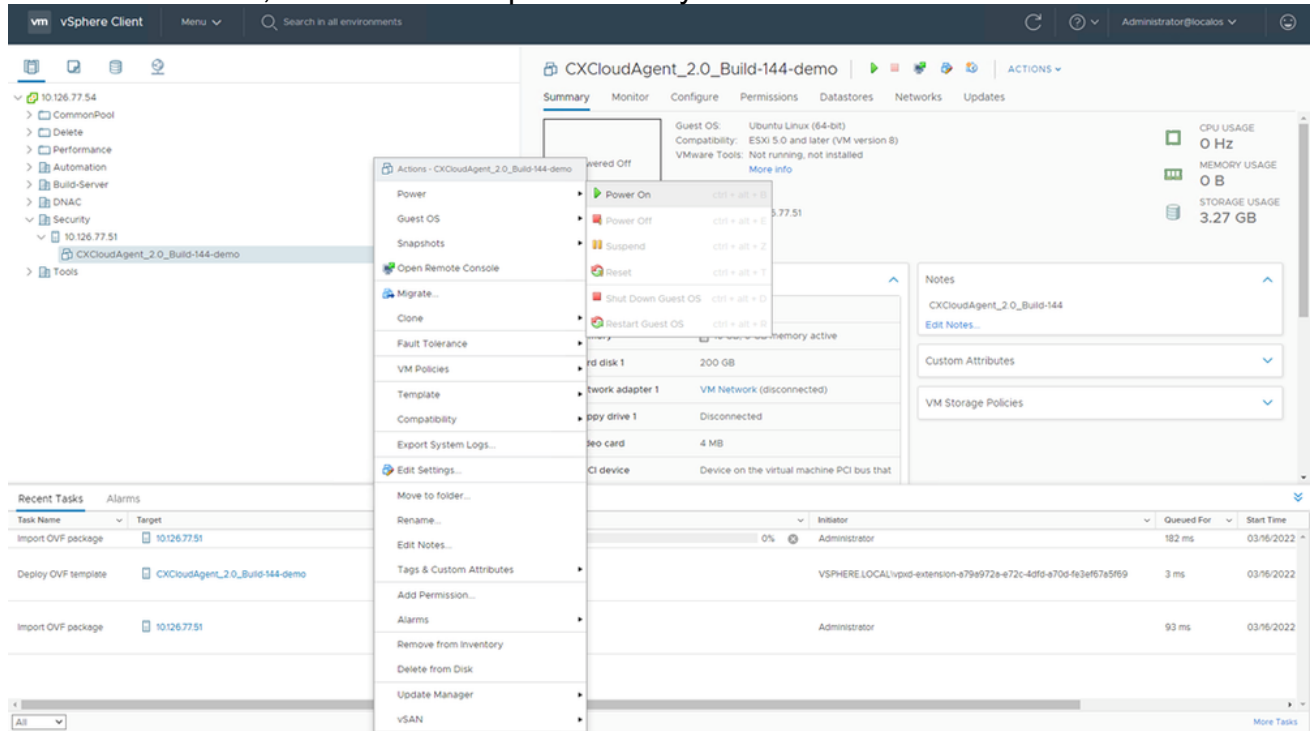
12. Se agrega una nueva VM. Haga clic en su nombre para ver el estado.

The screenshot shows the vSphere Client interface. The left sidebar displays a folder structure with 'Security' expanded to show the VM 'CXCloudAgent\_2.0\_Build-144-demo'. The main panel shows the VM's status as 'Powered Off'. Key details include: Guest OS: Ubuntu Linux (64-bit), Compatibility: ESXi 5.0 and later (VM version 8), VM Tools: Not running, not installed. DNS Name: IP Addresses: Host: 10.126.77.51. VM Hardware includes 8 CPU(s), 16 GB memory active, 200 GB Hard disk 1, VM Network (disconnected) Network adapter 1, Disconnected Floppy drive 1, 4 MB Video card, and VMCI device. A 'Recent Tasks' table at the bottom shows the deployment of this VM template as completed.

Task Name	Target	Status	Initiator	Queued For	Start Time
Import OVF package	10.126.77.51	0%	Administrator	182 ms	03/16/2022
Deploy OVF template	CXCloudAgent_2.0_Build-144-demo	✓ Completed	VSPHERE LOCAL/vpxd-extension-e79e972e-e72c-4dfd-e70d-f63ef67a5f69	3 ms	03/16/2022
Import OVF package	10.126.77.51	✓ Completed	Administrator	93 ms	03/16/2022

VM agregada

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



Abrir consola

14. Vaya a [Network Configuration](#).

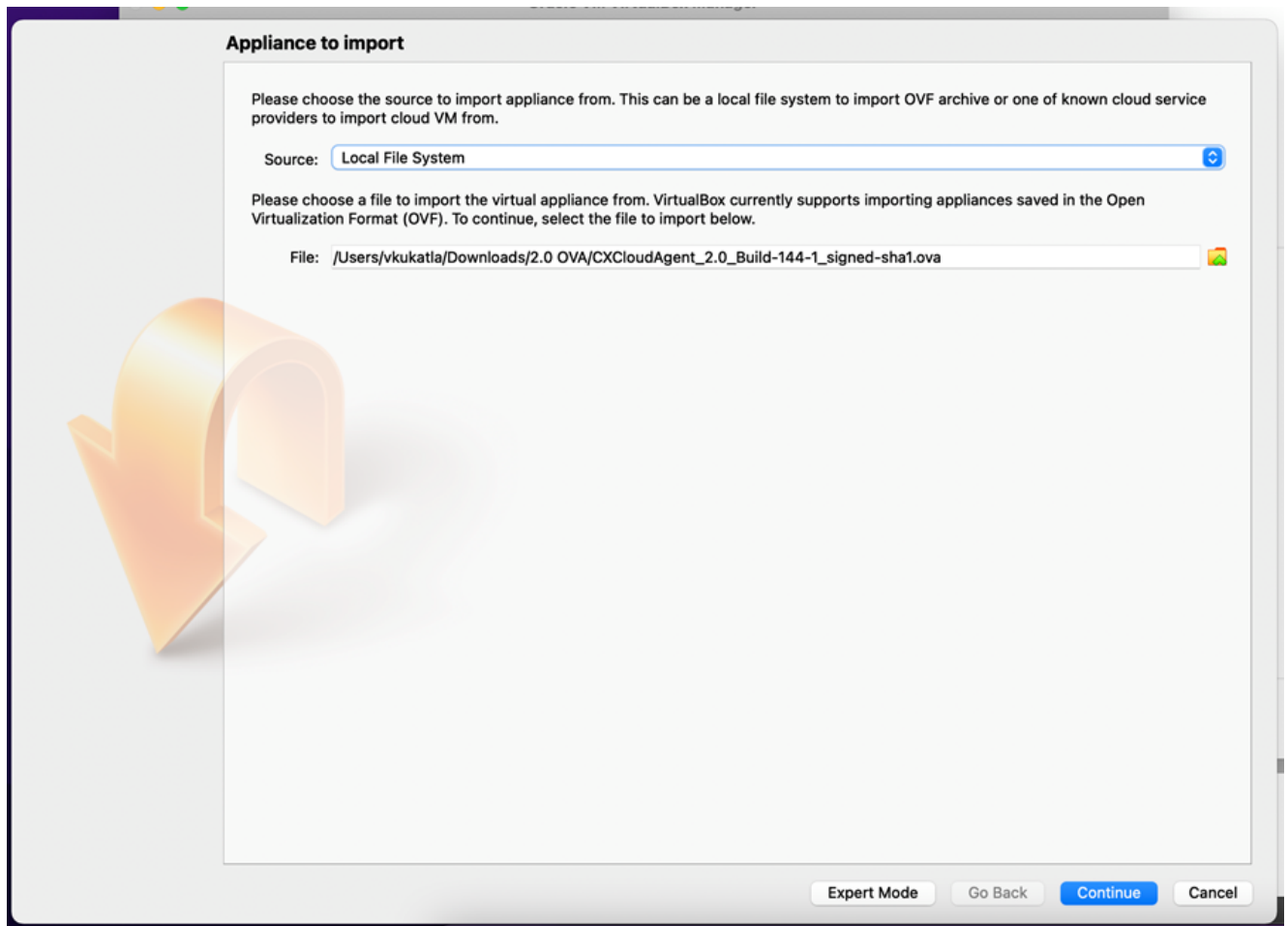
## Instalación de Oracle Virtual Box 5.2.30

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



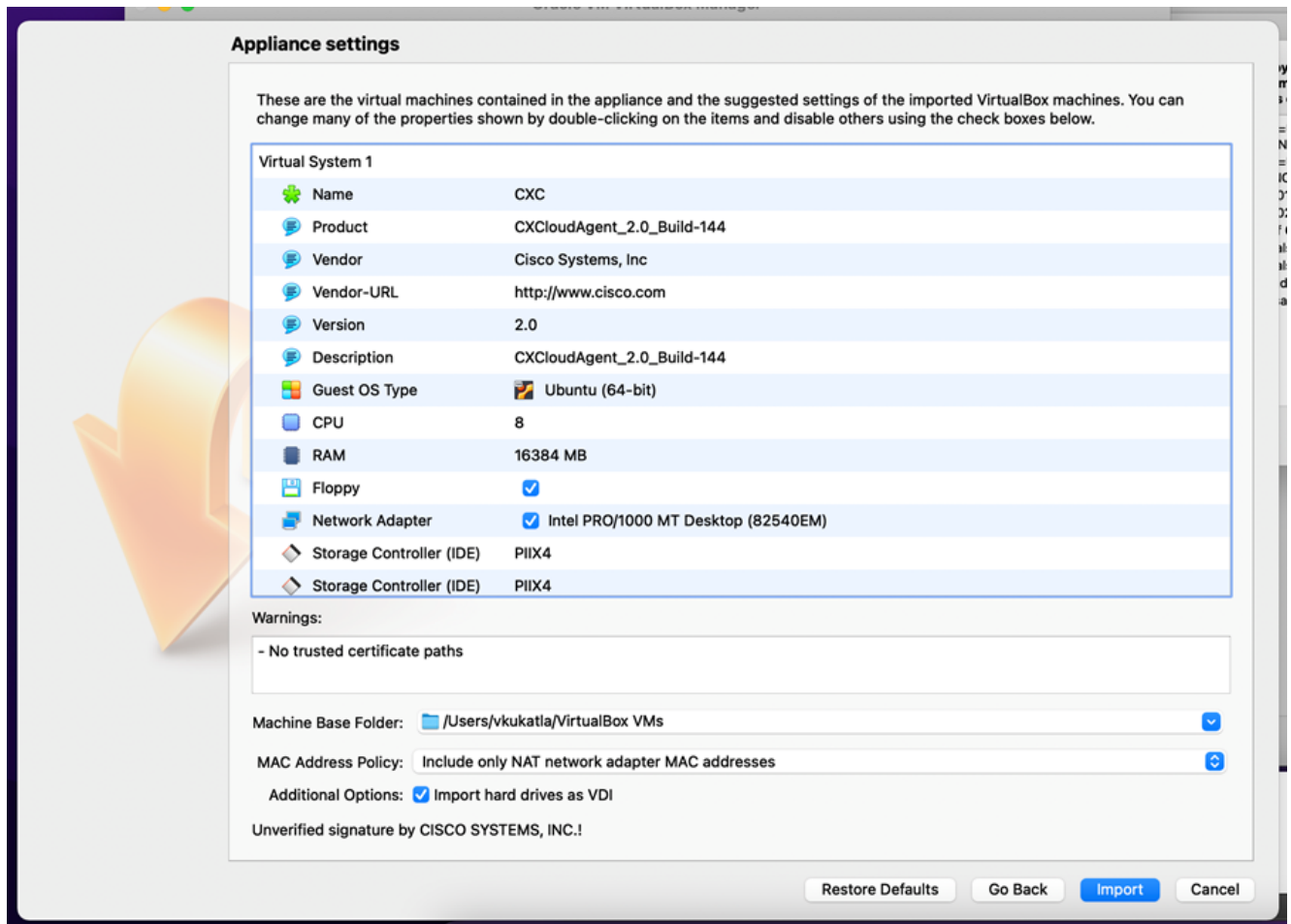
## Oracle VM

1. Abra Oracle VM UI y seleccione File > Import Appliance.
2. Vaya a para importar el archivo OVA.



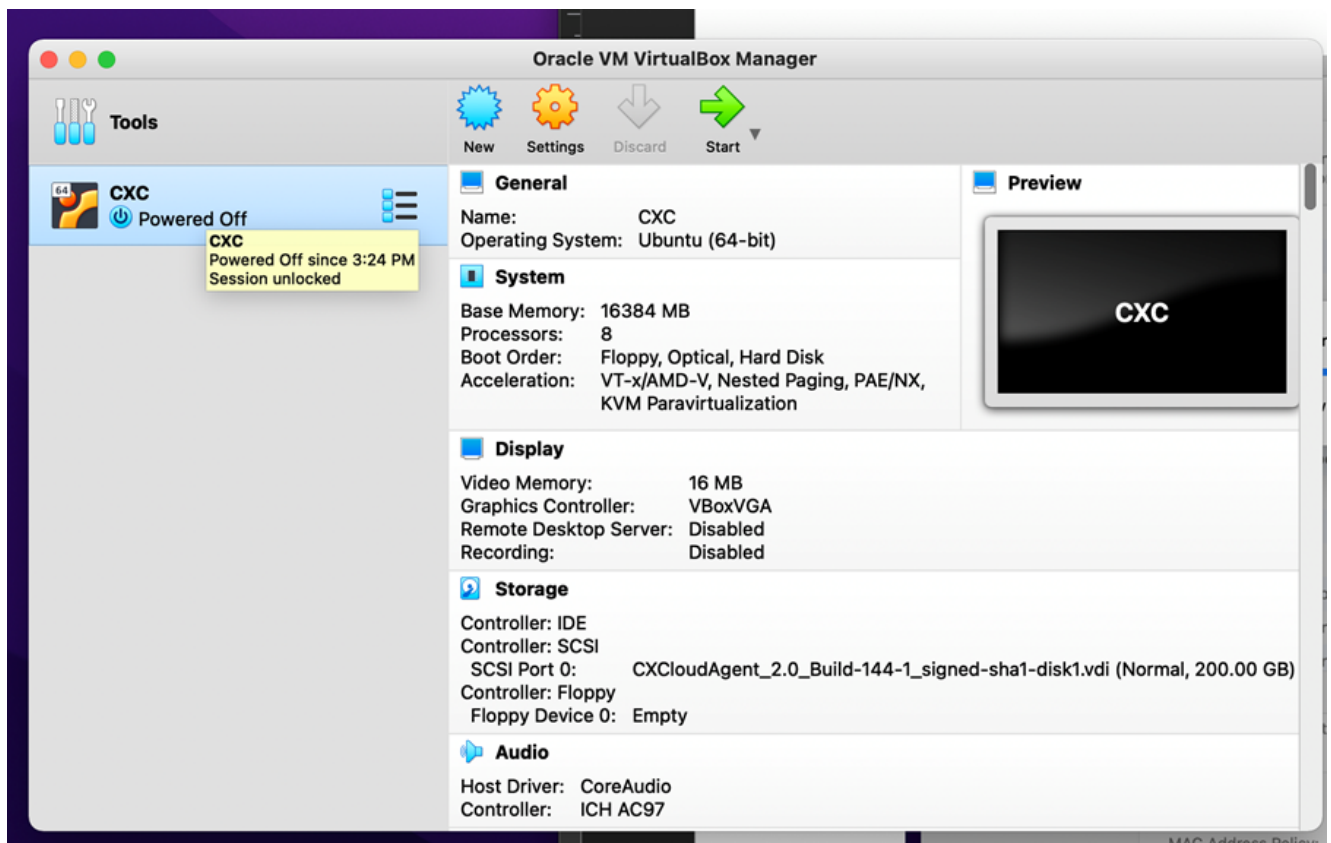
Seleccionar archivo

3. Haga clic Import.



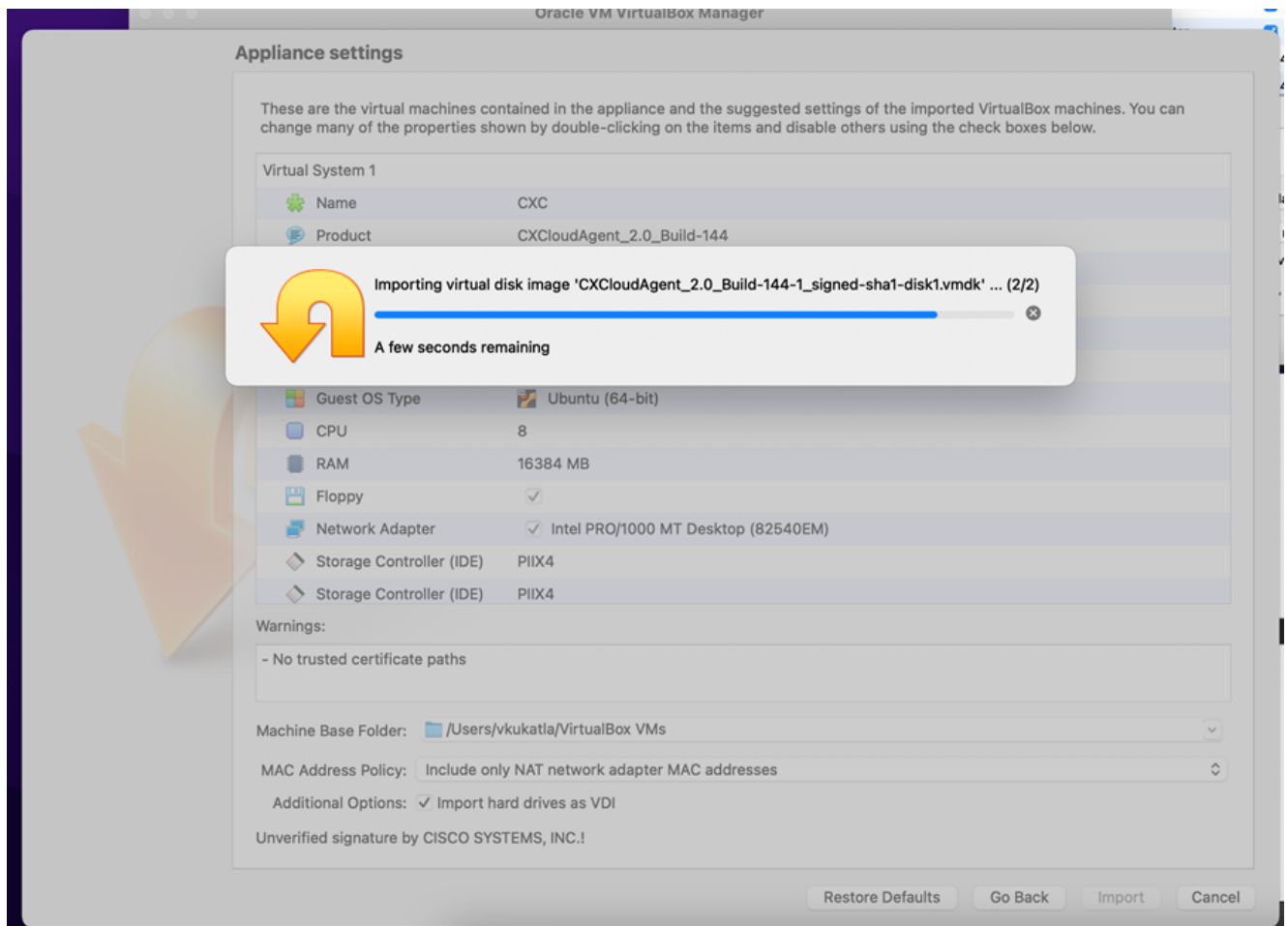
Importar archivo

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



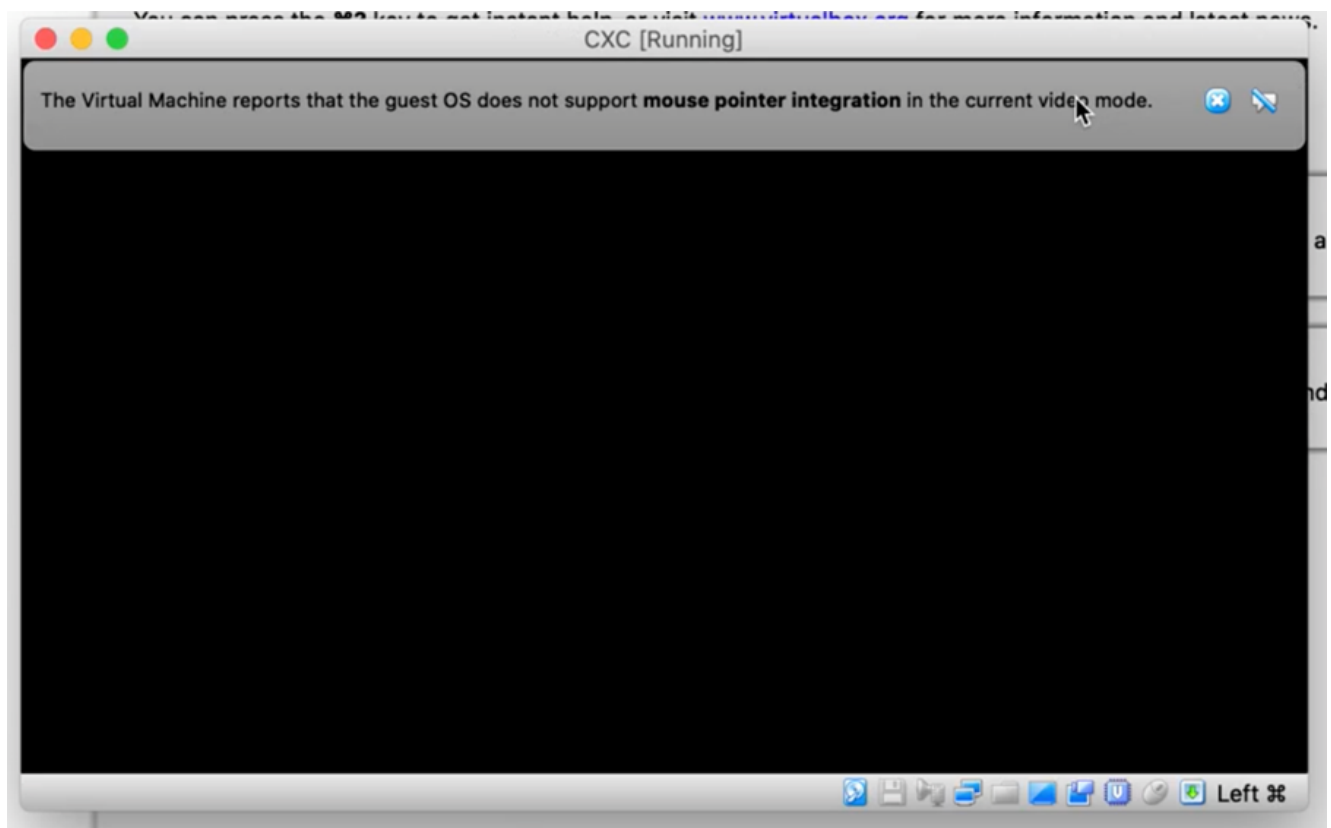
Inicio de consola VM





Importación en curso

5. Encienda la máquina virtual. La consola muestra.

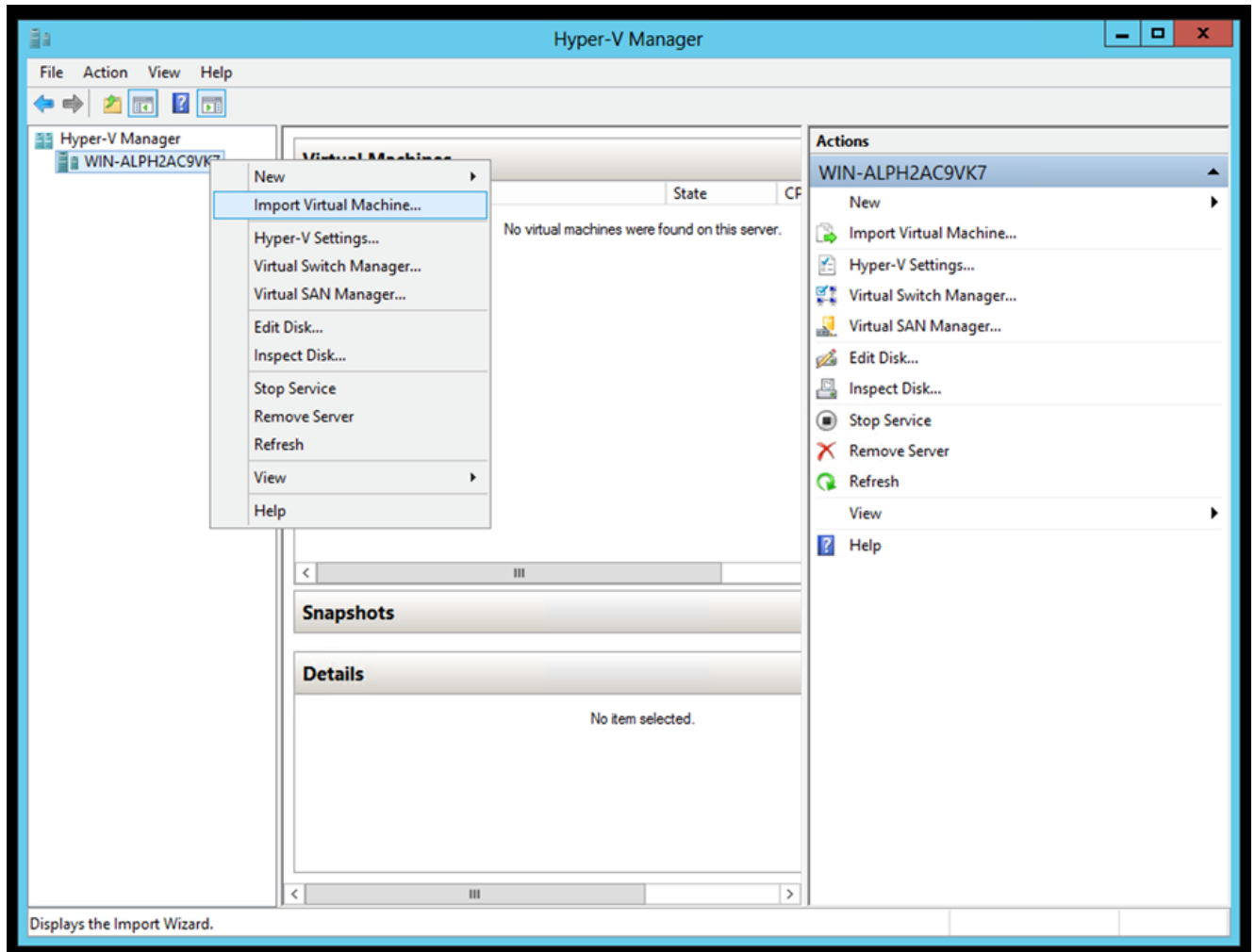


Abrir la consola

6. Vaya a [Network Configuration](#).

## Instalación de Microsoft Hyper-V

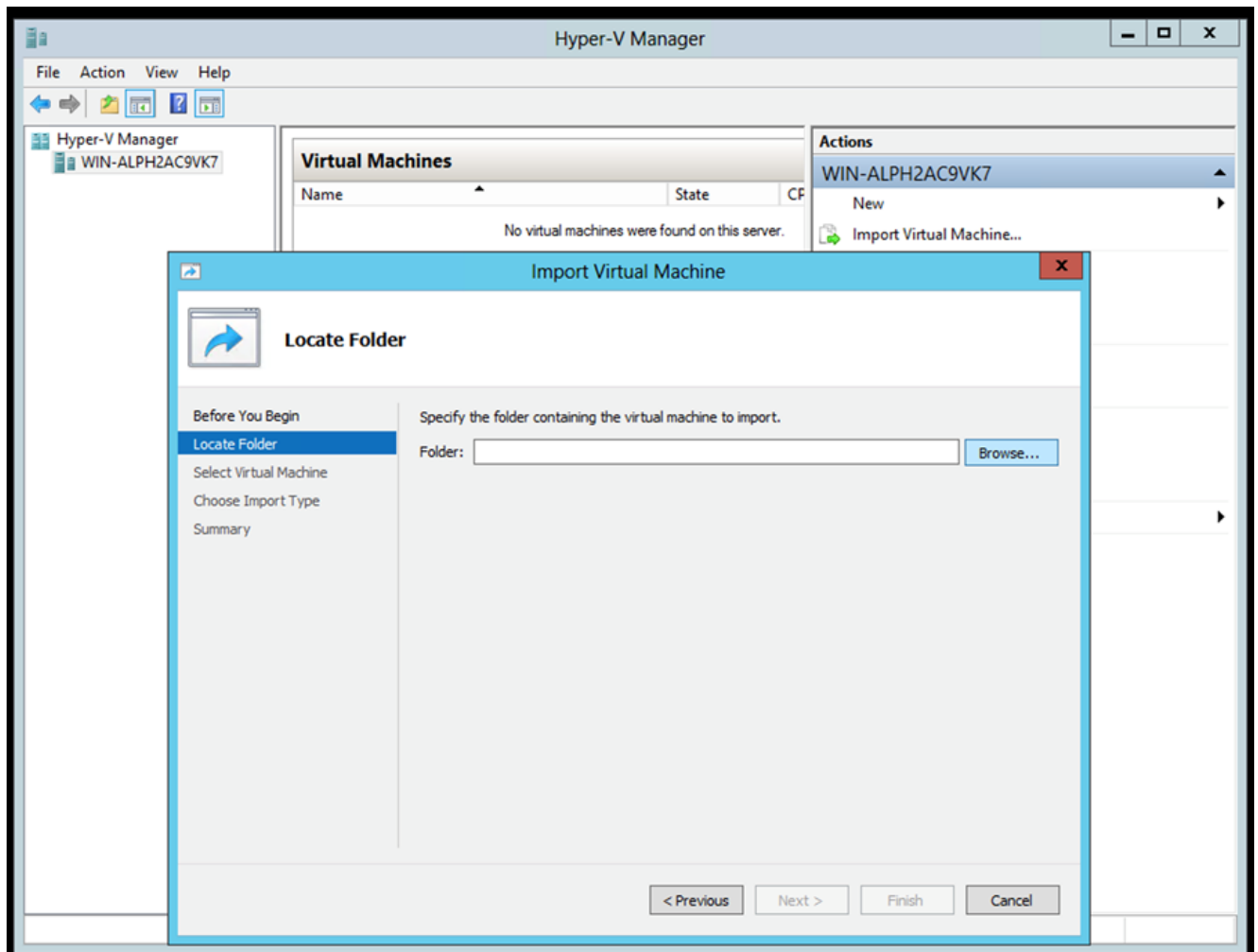
1. Seleccionar Import Virtual Machine.



Administrador de Hyper-V

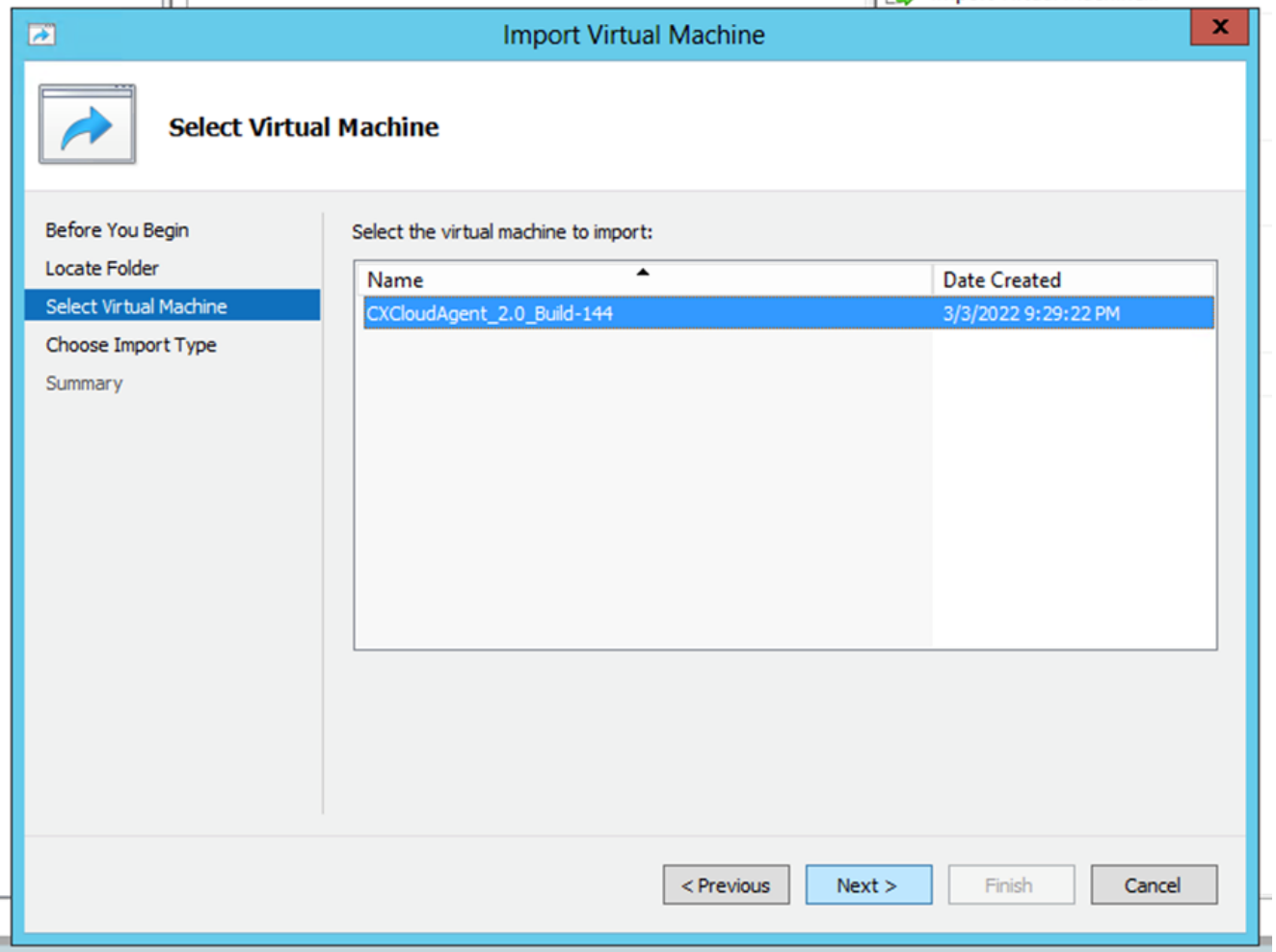
2. Busque y seleccione la carpeta de descarga.

3. Haga clic Next.



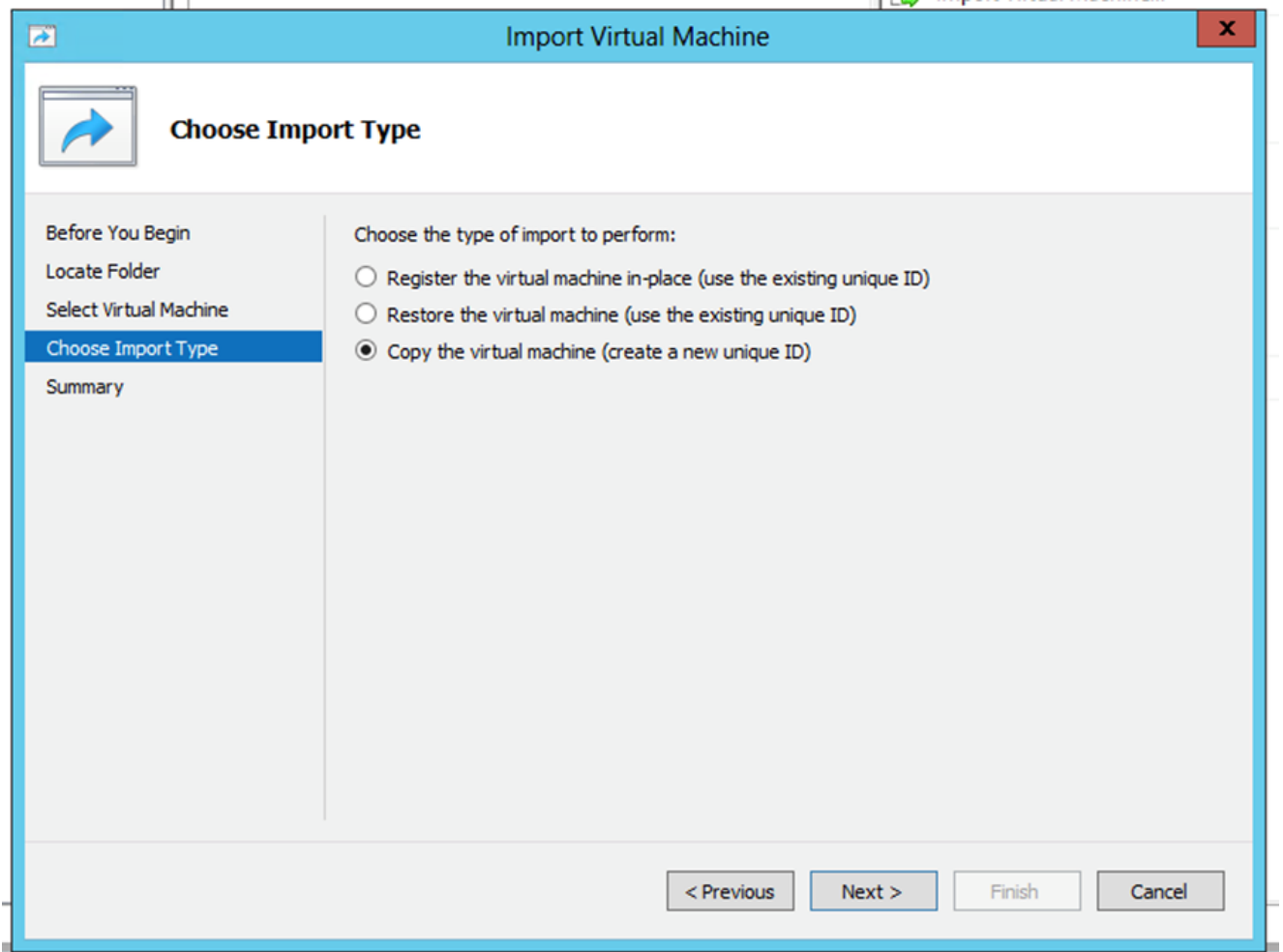
Carpeta para importar

4. Seleccione la máquina virtual y haga clic en Next.



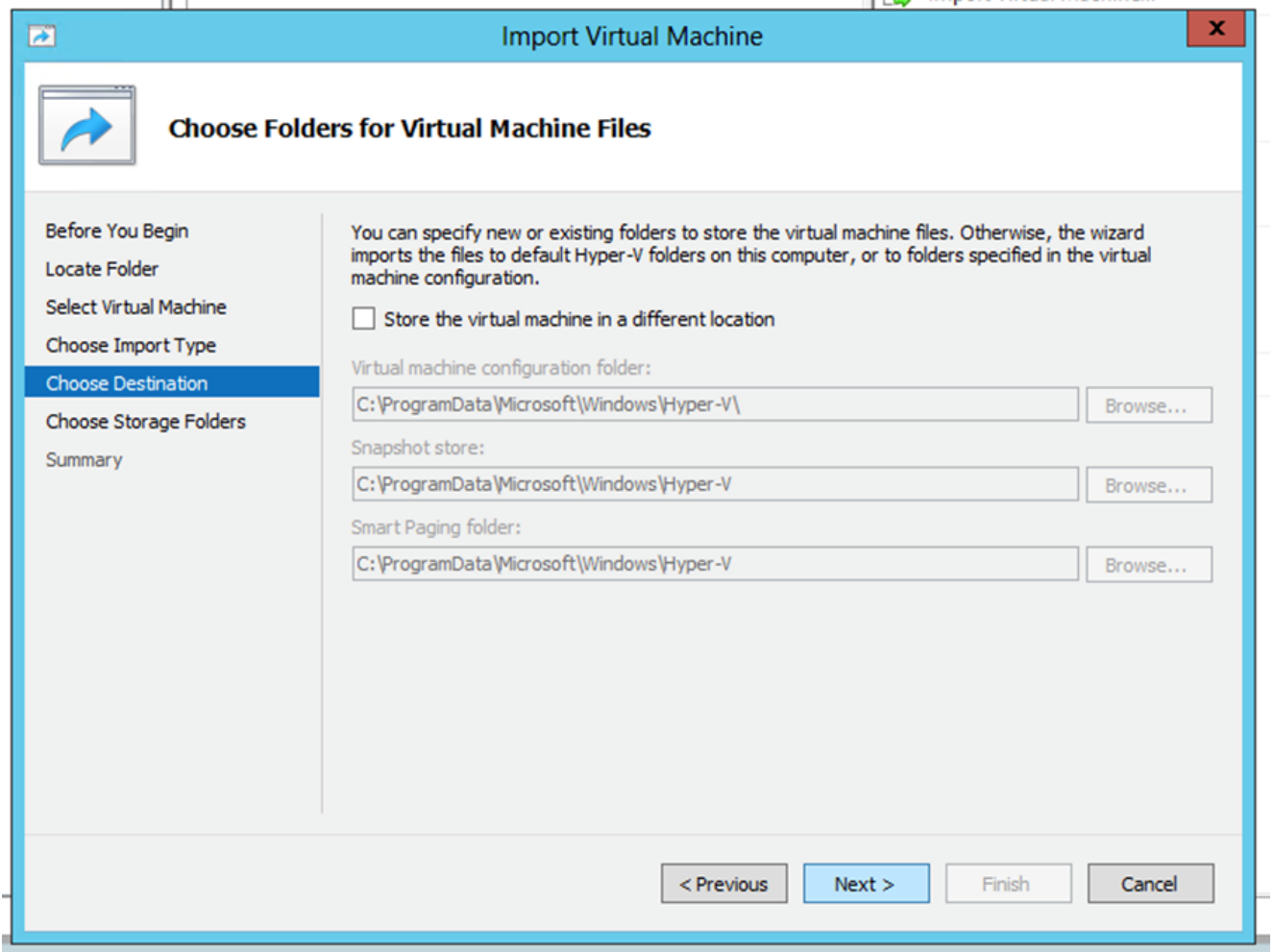
Seleccionar VM

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



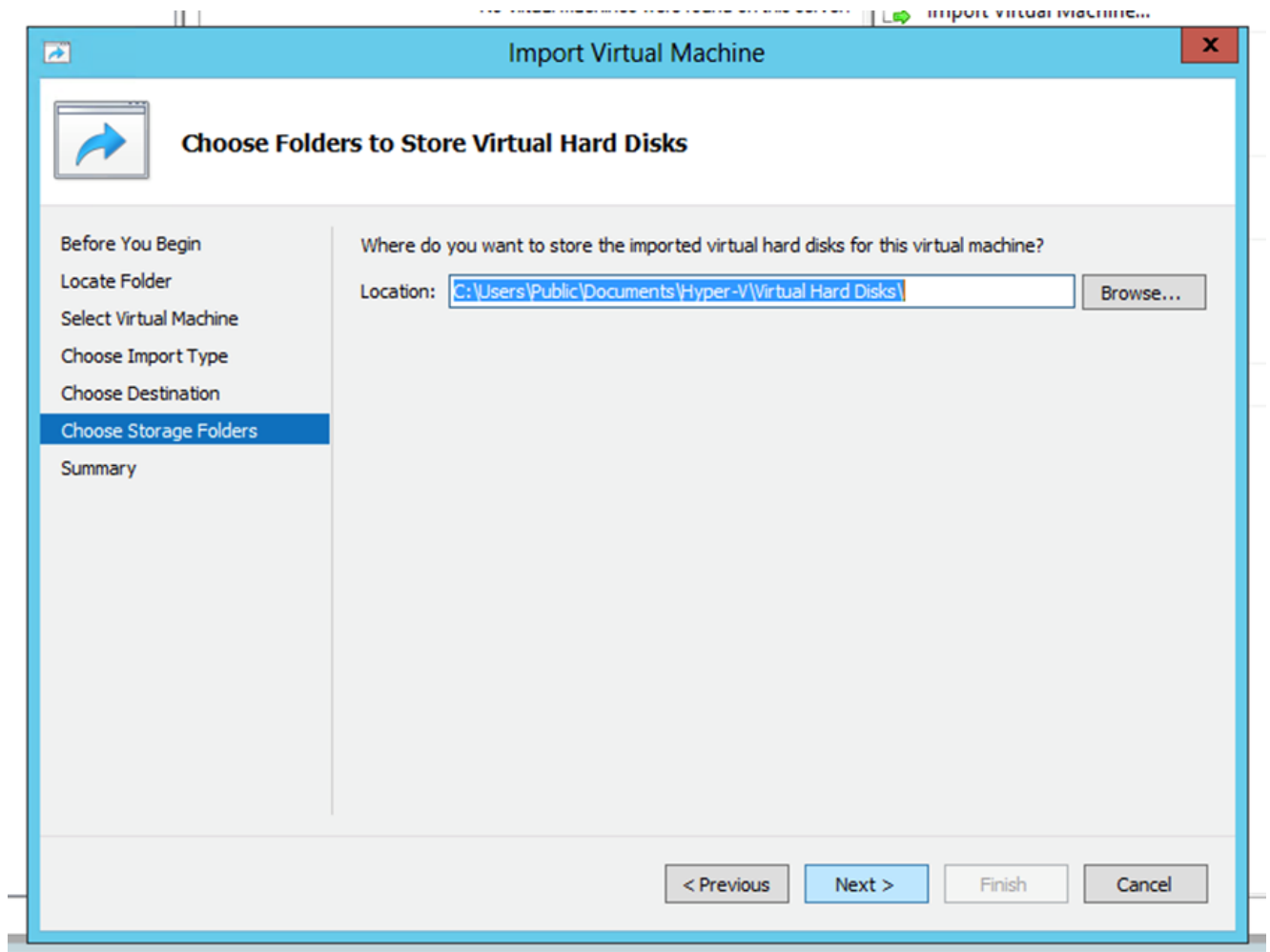
Tipo de importación

6. Busque la carpeta para los archivos de VM. Se recomienda utilizar rutas predeterminadas.
7. Haga clic Next.



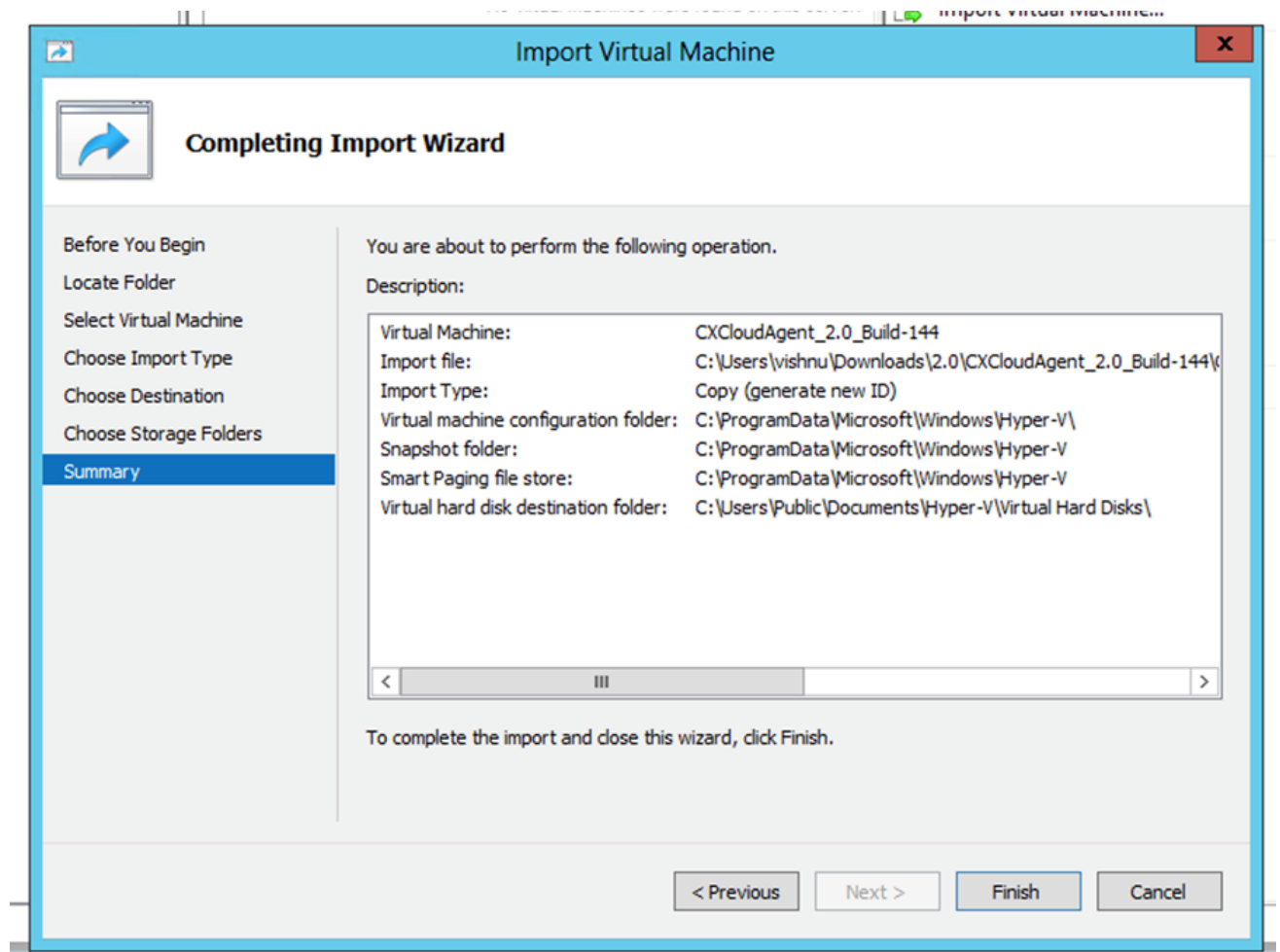
Elegir carpeta

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 Next.



Carpeta para almacenar discos duros virtuales

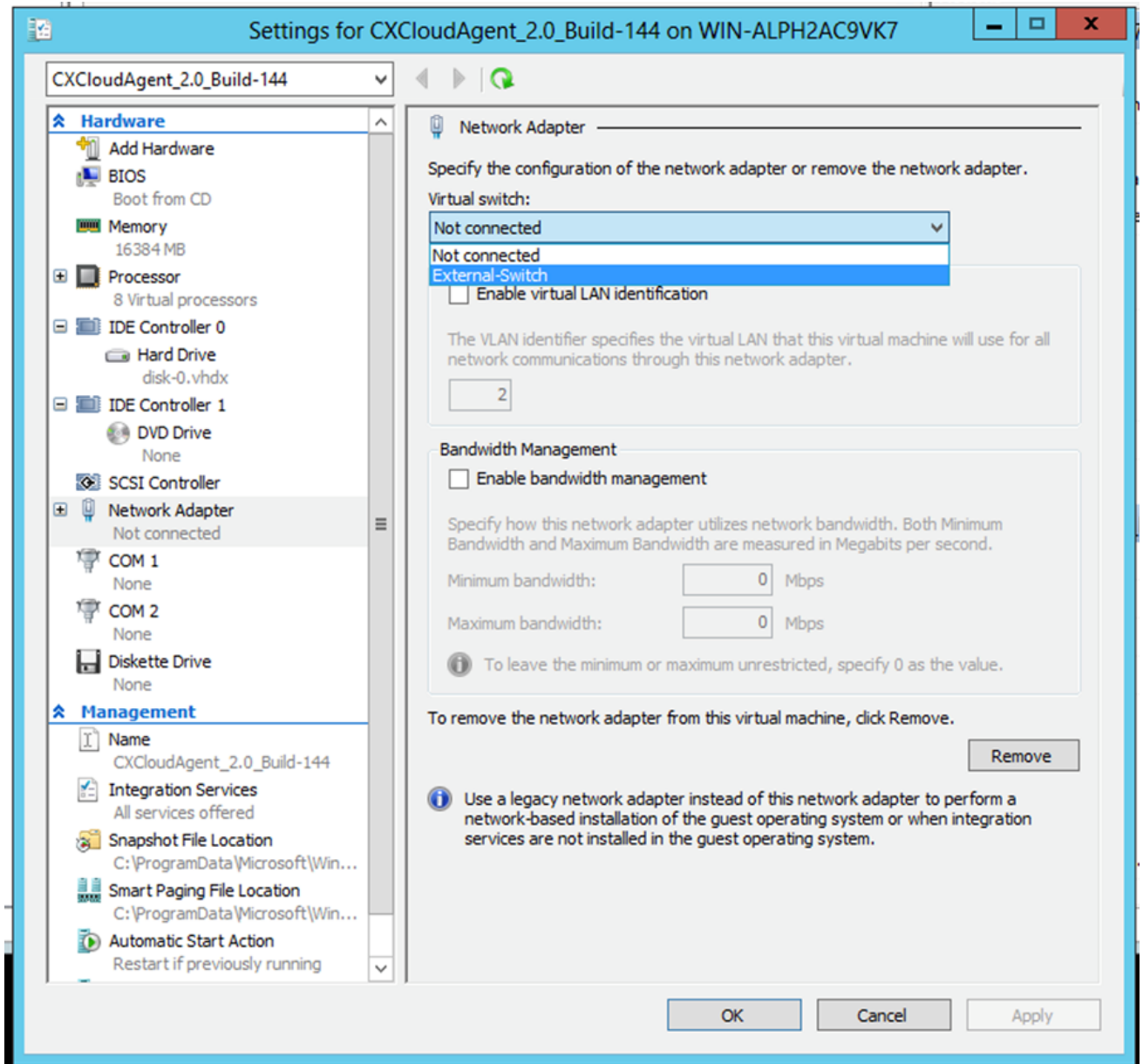
10. Se muestra el resumen de VM. Verifique todas las entradas y haga clic en Finish.



## Summary

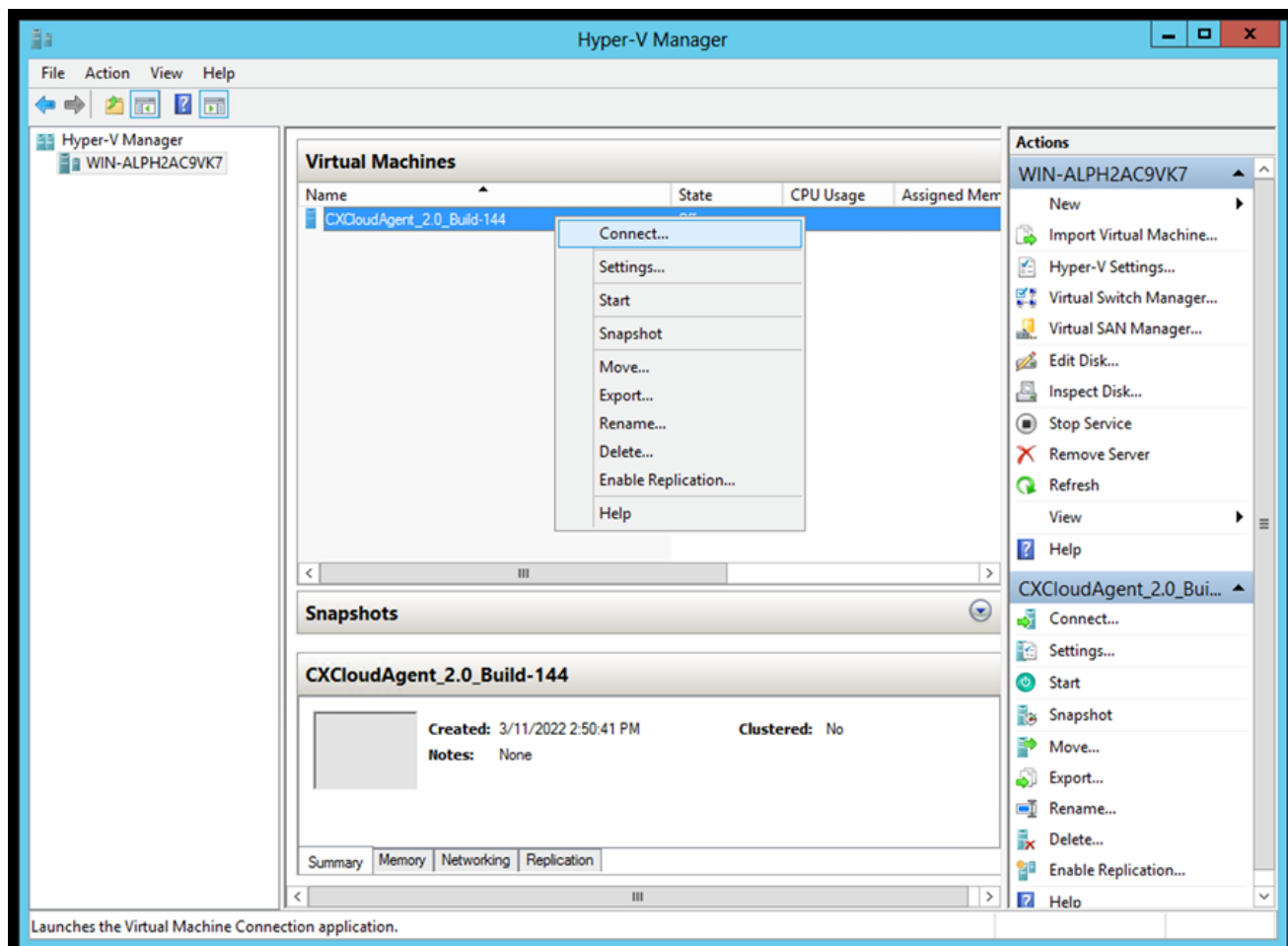
11. Una vez completada correctamente la importación, se crea una nueva máquina virtual en Hyper-V. Abra la configuración de la máquina virtual.
12. Seleccione el adaptador de red en el panel izquierdo y elija la Virtual Switch en el menú desplegable.





Switch virtual

13. Seleccionar Connect para iniciar la máquina virtual.



VM inicial

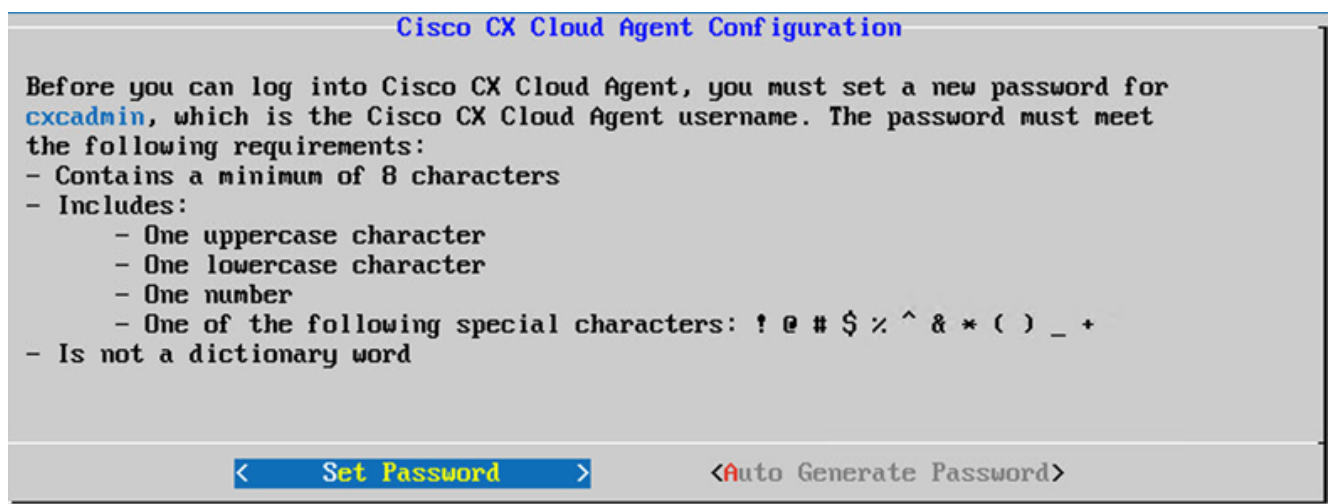
14. Vaya a [Network Configuration](#).

**Configuración de red**



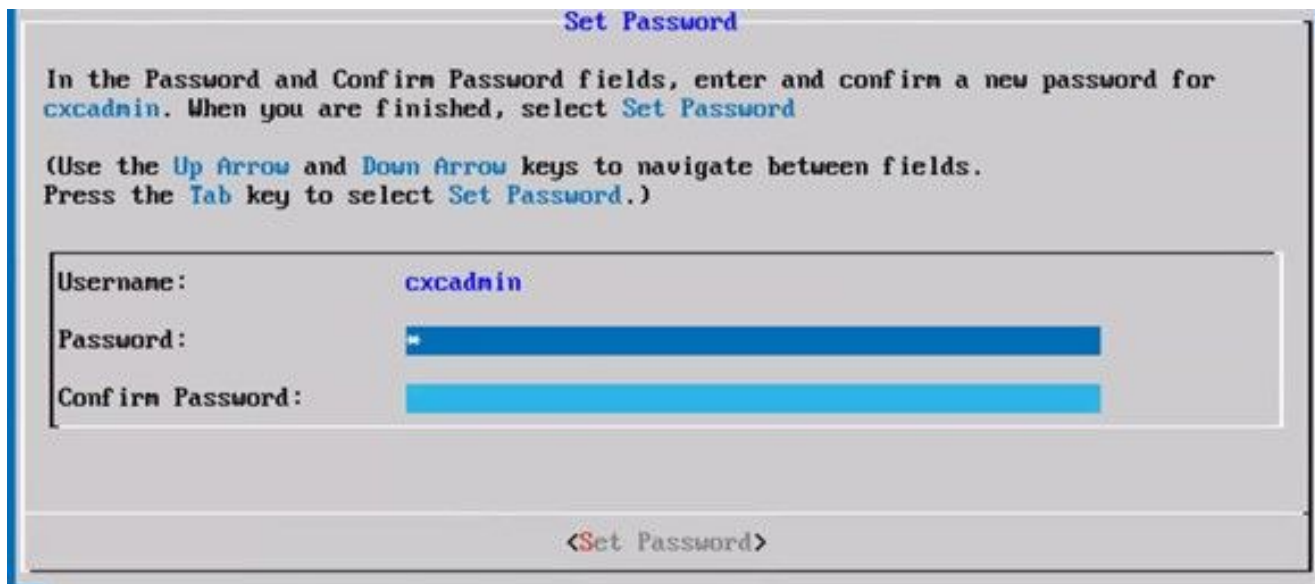
Consola de VM

1. Haga clic 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 Set Password , introduzca la contraseña de cxcadmin y confírmela. Haga clic Set Password y vaya al paso 3.



Nueva contraseña

O Si Auto Generate Password está seleccionado, copie la contraseña generada y guárdela para su uso futuro. Haga clic Save Password y vaya al paso

4.



Contraseña generada automáticamente

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



Guardar contraseña

4. Escriba el IP Address, Subnet Mask, Gateway, y DNS Server y haga clic en Continue.

**Network Configuration**

Please enter an IPv4 address and corresponding network configuration for the appliance.

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

IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Gateway:	<input type="text"/>
DNS Servers:	<input type="text"/>

\*Maximum 3 IPs with comma separator.

**<Continue>**

Configuración de red

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

**Confirmation**

Are these entries correct?

IP Address:	192.168.0.100
Subnet Mask:	255.255.255.0
Gateway:	192.168.0.1
DNS:	192.168.0.64

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

Confirmación

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.

**Proxy Set Up Confirmation**

Do you want to add proxy details?

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

Configuración de proxy

7. Escriba el Proxy Address, Port Number, Username,y Password.

**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:	<input type="text"/>
Port Number:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>

<Begin Configuration>      < **No, Go Back** >

Configuración de proxy

8. Haga clic Begin Configuration. La configuración puede tardar varios minutos en completarse.

**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.**

0%

Configuración en curso

9. Copie el Pairing Code y volver a CX Cloud para continuar con la configuración.

**Cisco CX Cloud Agent Setup**

The network configuration has been successfully completed.

IP :  
 Subnet Mask :  
 Gateway :  
 DNS Server :

The pairing code is

Please go to CX Cloud and enter this pairing code.

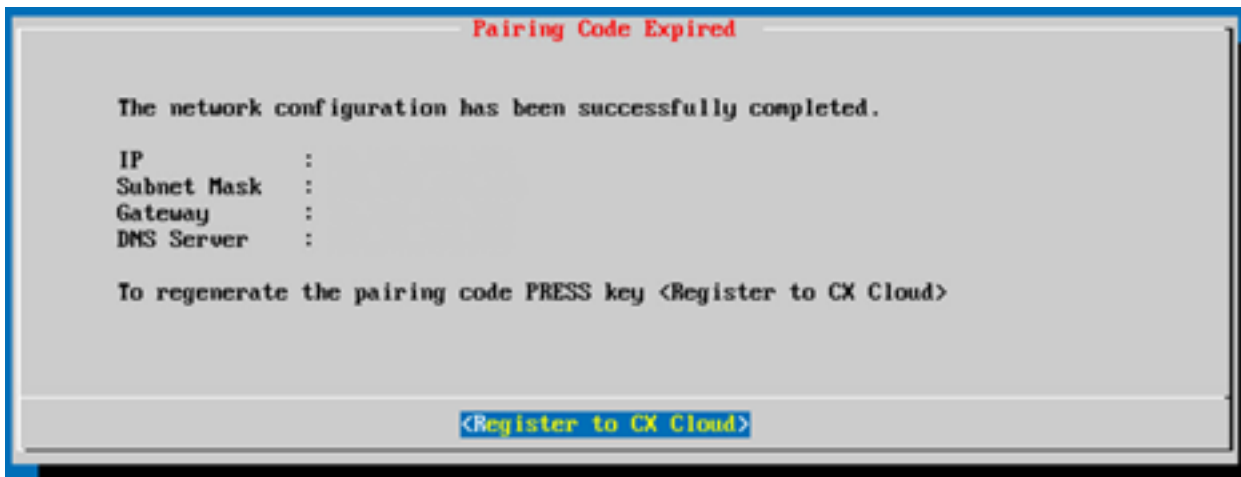
The Code will be valid for 5 minutes.

Time left in seconds...

298

Código de vinculación

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



Código caducado

11. Haga clic en OK.



Registro correcto

12. Vuelva a la sección [Conexión del agente de nube CX a la nube CX](#) y realice los pasos que se indican.

## 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`.

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

Pairing Code : x37I0P
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 emparejamiento



3. Copie el Pairing Code y volver a CX Cloud para continuar con la configuración. Para obtener más información, consulte Conexión al portal del cliente.

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

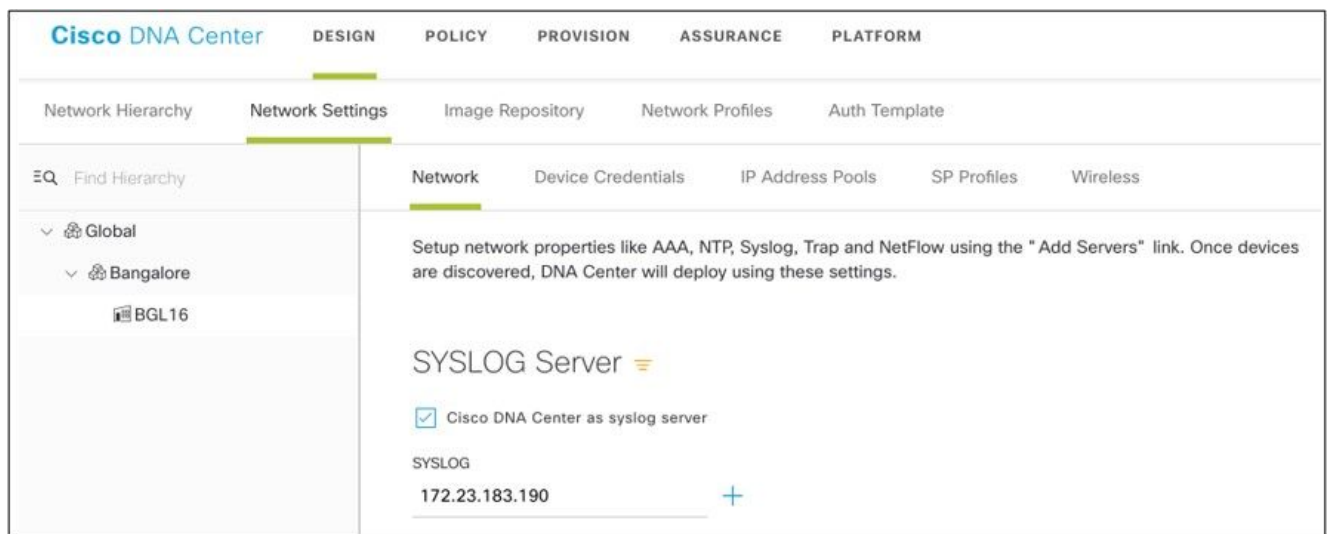
### Requisito previo

Las versiones compatibles de Cisco DNA Center son de 1.2.8 a 1.3.3.9 y de 2.1.2.0 a 2.2.3.5.

### Configuración de Syslog Forwarding

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

1. Inicie Cisco DNA Center.
2. Vaya a Design > Network Settings > Network.
3. Para cada sitio, agregue la IP del agente de nube CX como servidor Syslog.



#### Servidor Syslog

#### Notas:

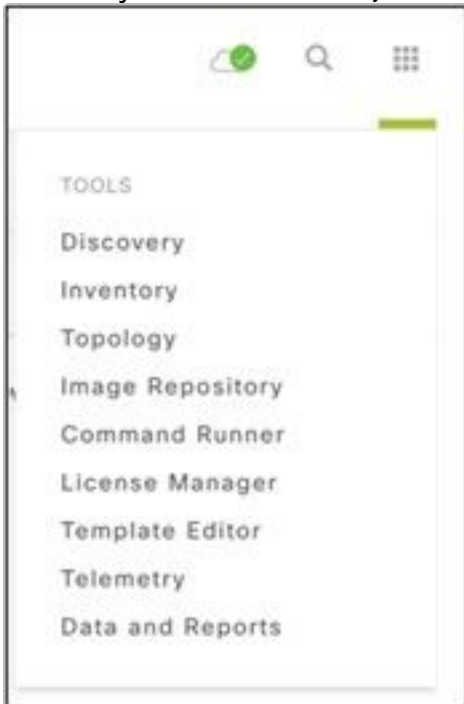
- Una vez configurados, todos los dispositivos asociados con ese sitio se configuran para enviar syslog con nivel crítico a CX Cloud Agent.
- Los dispositivos deben estar asociados a un sitio para habilitar el reenvío de syslog desde el dispositivo a CX Cloud Agent.
- Cuando se actualiza una configuración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

### Habilitar configuración de Syslog de nivel de información



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

1. Vaya a Tools > Telemetry.



Menú Herramientas

2. Seleccione y amplíe el Site View y seleccione un sitio en la jerarquía de sitios.



Vista del sitio

3. Seleccione el sitio necesario y seleccione todos los dispositivos mediante el Device name casilla de verificación.

4. Desde el Actions desplegable, seleccione Optimal Visibility.



Acciones

## Security

CX Cloud Agent garantiza al cliente una seguridad integral. La conexión entre CX Cloud y CX Cloud Agent está cifrada. Secure Socket Shell (SSH) del agente en la nube de CX admite 11 cifrados diferentes.

### Seguridad Física

Implemente la imagen OVA de CX Cloud Agent 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 [FAQ](#) para establecer esta contraseña del cargador de arranque (modo de usuario único).

### Acceso de usuario

Los usuarios de la nube de CX solo pueden obtener autenticación y acceso a las API de Cloud Agent.

### Seguridad de cuentas

Durante la implementación, se crea la cuenta de usuario cxcadmin. Los usuarios deben establecer una contraseña durante la configuración inicial. Las credenciales/usuarios de cxcadmin se utilizan para acceder a las API del agente de nube CX y para conectar el dispositivo a través de SSH.

El usuario cxcadmin ha restringido el acceso con los privilegios mínimos. La contraseña cxcadmin sigue la política de seguridad y se trocea unidireccionalmente con un período de caducidad de 90 días. El usuario cxcadmin puede crear un usuario cxcroot mediante la utilidad denominada remoteaccount. El usuario cxcroot puede obtener privilegios de root. La frase de paso caduca en dos días.

### 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 el usuario cxcadmin puede crear el usuario cxcroot mediante una utilidad denominada remotaaccount. Esta utilidad muestra una contraseña cifrada RSA/ECB/PKCS1v1\_5 que sólo se puede descifrar desde el portal SWIM (<https://swims.cisco.com/abraxas/decrypt>). Solo el personal autorizado tiene acceso a este portal. el usuario cxcroot puede obtener privilegios de root con esta contraseña descifrada. La frase de paso sólo es válida durante dos días. El usuario cxcadmin necesita volver a crear la cuenta y obtener la contraseña del portal SWIM tras el vencimiento de la contraseña.

## Endurecimiento

El dispositivo CX Cloud Agent sigue los estándares de refuerzo de CIS.

## 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 de Cisco DNA Center en una base de datos segura. Los datos recopilados de Cisco DNA Center no se almacenan de ninguna forma dentro del dispositivo. Los datos recopilados se cargan en la copia de seguridad poco después de que se complete la recopilación y los datos se depuran del agente.

## Transmisión de datos

El paquete de registro contiene los datos únicos necesarios [X.509](#) certificado de dispositivo y claves para establecer una conexión segura con IoT Core. El uso de ese agente establece una conexión segura mediante MQTT sobre TLS v1.2

## Registros y supervisión

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

## Resumen de seguridad

### Funciones de seguridad

Funciones de seguridad	Descripción
Contraseña del cargador de arranque (modo de usuario único)	La contraseña del cargador de arranque (modo de usuario único) se establece con una contraseña aleatoria única. El usuario debe consultar <a href="#">FAQ</a> para establecer su contraseña 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 credenciales creadas durante la instalación.</li><li>• El acceso al dispositivo mediante el usuario cxcroot requiere que el personal autorizado</li></ul>
-------------------	---

	descifre las credenciales mediante el portal SWIM.
Cuentas de usuario	<ul style="list-style-type: none"> <li>• cxcadmin: Se trata de una cuenta de usuario predeterminada creada. El usuario puede ejecutar los comandos de la aplicación Agente en la nube de CX mediante cxcli y tiene menos privilegios en el dispositivo. cxcroot user y su contraseña cifrada se generan mediante cxcadmin user</li> <li>• cxcroot: cxcadmin puede crear este usuario mediante la utilidad "remoteaccount". El usuario puede obtener privilegios de root con esta cuenta.</li> </ul>
cxcadmin password policy	<ul style="list-style-type: none"> <li>• La contraseña se codifica en un solo sentido mediante SHA-256 y se almacena de forma segura.</li> <li>• Ocho (8) caracteres como mínimo, que contengan tres de estas categorías: mayúsculas, minúsculas, números y caracteres especiales</li> </ul>
cxcroot password policy	<ul style="list-style-type: none"> <li>• cxcroot password está encriptado 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 un máximo de dos días y se pueden regenerar usando cxcadmin user.</li> </ul>
ssh login password policy	<ul style="list-style-type: none"> <li>• Ocho (8) caracteres como mínimo, que contengan tres de estas categorías: mayúsculas, minúsculas, números y caracteres especiales.</li> <li>• 5 intentos de inicio de sesión fallidos bloquearán 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	<p>No se almacena información del cliente.</p> <p>No hay datos del dispositivo almacenados.</p> <p>Credenciales de servidor de Cisco DNA Center cifradas y almacenadas en la base de datos</p>

## Preguntas Frecuentes

### Agente de nube CX

#### Implementación

P: Con la opción "Reinstalar", ¿puede el usuario implementar el nuevo Cloud Agent con una nueva dirección IP?

A - Sí

P - ¿Cuáles son los formatos de archivo disponibles para la instalación?

A - OVA y VHD

P: ¿En qué entorno se puede implementar el instalador?

A - ÓVULOS

VMWare ESXi versión 5.5 o posterior

Oracle Virtual Box 5.2.30 o posterior

VHD

## Hipervisor de Windows 2012 a 2016

P - ¿Puede CX Cloud Agent detectar la dirección IP en un entorno DHCP?

R - Sí, en el caso del entorno DHCP, se tiene cuidado con la asignación de la dirección IP durante la configuración IP. Sin embargo, no se admite el cambio de dirección IP esperado para el agente en la nube de CX en ningún momento futuro. Además, se recomienda que el cliente reserve la IP para el Cloud Agent en su entorno DHCP.

P: ¿Es el agente en la nube de CX compatible con la configuración de IPv4 e IPv6?

R: No, solo se admite IPV4.

P: ¿Se valida la dirección IP durante la configuración IP?

R: Sí, se validará la sintaxis de la dirección IP y la asignación de direcciones IP duplicadas.

P: ¿Cuál es el tiempo aproximado que se tarda en implementar OVA y configurar IP?

R: La implementación de OVA depende de la velocidad de la red para copiar los datos. La configuración IP tarda aproximadamente de 8 a 10 minutos, lo que incluye la creación de Kubernetes y contenedores.

P: ¿Existe alguna limitación con respecto a cualquier tipo de hardware?

R: La máquina host en la que se implementa OVA debe cumplir los requisitos proporcionados como parte de la configuración del portal CX. El agente en la nube CX se prueba con VMware/Virtual Box en un hardware con procesadores Intel Xeon E5 con una proporción vCPU/CPU establecida en 2:1. Si se utiliza una CPU de procesador menos potente o una proporción mayor, el rendimiento puede disminuir.

P - ¿Podemos generar el código de emparejamiento en cualquier momento?

R - No, el código de emparejamiento solo se puede generar si el Cloud Agent no está registrado.

P: ¿Cuáles son los requisitos de ancho de banda entre los DNAC (para hasta 10 clústeres o 20 no clústeres) y el agente?

R: El ancho de banda no es una restricción cuando el agente y DNAC se encuentran en la misma red LAN/WAN en el entorno del cliente. El ancho de banda de red mínimo requerido es de 2,7 Mbits/seg para las colecciones de inventario de 5000 dispositivos +13000 Puntos de acceso para una conexión de agente a DNAC. Si se recopilan registros del sistema para obtener información de nivel 2, el ancho de banda mínimo necesario es de 3,5 Mbits/seg. para cubrir 5000 dispositivos +13000 puntos de acceso para inventario, 5000 dispositivos registros del sistema y 2000 dispositivos para análisis; todos se ejecutan en paralelo desde el agente.

### Versiones y parches

P. - ¿Cuáles son los diferentes tipos de versiones que aparecen para la actualización de CX Cloud Agent?

R: Aquí se muestra el conjunto de versiones lanzadas de CX Cloud Agent que se enumeran a

continuación:

- A.x.0 (donde x es la última versión de la función principal de producción, por ejemplo:1.3.0)
- A.x.y (donde A.x.0 es obligatorio y debe iniciarse una actualización incremental), x es la última versión de la función principal de producción e y es la última revisión de actualización activa, por ejemplo: 1.3.1).
- A.x.y-z (donde A.x.0 es obligatorio y debe iniciarse una actualización incremental), x es la última versión de la función principal de producción, y y es la última revisión de actualización activa, y z es la corrección instantánea durante un período de tiempo muy corto, por ejemplo: 1.3.1-1)

donde A es una versión a largo plazo distribuida en un período de 3 a 5 años.

P: ¿Dónde se encuentra la última versión de CX Cloud Agent y cómo actualizar la versión existente de CX Cloud Agent?

A - Vaya a Admin Settings > Data Sources. Haga clic en el View Update y siga las instrucciones que aparecen en pantalla.

### Autenticación y configuración de proxy

P: ¿Cuál es el usuario predeterminado de la aplicación CX Cloud Agent?

A - cxcadmin

P: ¿Cómo se establece la contraseña para el usuario predeterminado?

R: La contraseña se establece durante la configuración de la red.

P - ¿Hay alguna opción disponible para restablecer la contraseña después del Día-0?

R - El agente no proporciona ninguna opción específica para restablecer la contraseña, pero puede utilizar los comandos de linux para restablecer la contraseña de cxcadmin.

P: ¿Cuáles son las políticas de contraseñas para configurar CX Cloud Agent?

R: Las políticas de contraseñas son:

- Antigüedad máxima (longitud) de la contraseña establecida en 90 días
- Antigüedad mínima (longitud) de la contraseña establecida en 8
- La longitud máxima de la contraseña es de 127 caracteres.
- Se debe incluir al menos una mayúscula y una minúscula.
- Debe contener al menos un carácter especial (por ejemplo, !\$%^&\*()\_+|~-=\`{}[]:"';<>?,/).
- Estos caracteres no están permitidos Caracteres especiales de 8 bits (por ejemplo, \£, √Å √', √¥, √ë,, √ü)Espacios
- La contraseña no debe ser la última de las 10 contraseñas utilizadas recientemente.
- No debe contener expresiones regulares, p. ej.
- No debe contener estas palabras ni sus derivados: cisco, sanjose y sanfran

P - ¿Cómo establecer la contraseña de Grub?

R - Para establecer la contraseña de Grub, siga estos pasos:

1. Ejecute ssh como cxcroot y proporcione el token [Póngase en contacto con el equipo de soporte técnico para obtener el token cxcroot]
2. Ejecute sudo su, proporcione el mismo token
3. Ejecute el comando grub-mkpasswd-pbkdf2 y establezca la contraseña de GRUB. Se imprimirá el hash de la contraseña proporcionada, copie el contenido.
4. vi al archivo /etc/grub.d/00\_header. Navegue hasta el final del archivo y reemplace la salida hash seguida por el contenido password\_pbkdf2 root \*\*\*\*\* con el hash obtenido para la contraseña que obtuvo en el paso 3
5. Guarde el archivo con el comando :wq!
6. Ejecute el comando update-grub

P: ¿Cuál es el período de caducidad de la contraseña de cxcadmin?

R: La contraseña caducará en 90 días.

P - ¿El sistema inhabilita la cuenta después de intentos consecutivos de inicio de sesión fallidos?

R - Sí, la cuenta se inhabilita después de 5 intentos consecutivos fallidos. El periodo de bloqueo es de 30 minutos.

P - ¿Cómo generar una frase de contraseña?

R: Realice estos pasos:

1. Ejecute ssh e inicie sesión como usuario cxcadmin
2. Ejecute el comando *remoteaccount cleanup -f*
3. Ejecute el comando *remoteaccount create*

P - ¿El host proxy soporta el nombre de host y la IP?

R: Sí, pero para utilizar el nombre de host, el usuario debe proporcionar la IP DNS durante la configuración de la red.

## SSH de Secure Shell

P - ¿Cuáles son los cifrados soportados por el shell ssh?

A: chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr

P - ¿Cómo iniciar sesión en la consola?

R: Siga los pasos para iniciar sesión:

1. Inicie sesión como usuario cxcadmin.
2. Proporcione la contraseña cxcadmin.

P - ¿Están registrados los logins SSH?

R - Sí, se registran como parte de la carpeta var/logs/audit/audit.log.

P - ¿Cuál es el tiempo de espera de la sesión inactiva?

R: El tiempo de espera de la sesión SSH se produce si el Cloud Agent está inactivo durante cinco (5) minutos.

## Puertos y servicios

P: ¿Cuáles son los puertos que se mantienen abiertos de forma predeterminada en el agente en la nube de CX?

R: Estos puertos están disponibles:

- Outbound port: El agente en la nube CX implementado puede conectarse al backend de Cisco como se indica en la tabla del puerto HTTPS 443 o a través de un proxy para enviar datos a Cisco. El agente en la nube CX implementado puede conectarse a Cisco DNA Center en el puerto HTTPS 443.

### AMÉRICA

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

### EMEA

cloudsso.cisco.com  
api-cx.cisco.com  
agent.emea.[cisco.cloud](#)  
ng.acs.agent.emea.[cisco.cloud](#)

### Asia Pacífico, Japón y China

cloudsso.cisco.com  
api-cx.cisco.com  
agent.apjc.[cisco.cloud](#)  
ng.acs.agent.apjc.cisco.  
cloud

**Nota:** Además de los dominios enumerados, cuando los clientes de EMEA o APJC reinstalan el Cloud Agent, se debe permitir el dominio agent.us.cisco.cloud en el firewall del cliente.

El dominio agent.us.cisco.cloud ya no es necesario después de una reinstalación correcta.

**Nota:** Asegúrese de que se permita el tráfico de retorno en el puerto 443.

- Inbound port: Para la gestión local de CX Cloud Agent, se debe poder acceder a 514 (Syslog) y 22 (ssh). El cliente debe permitir que el puerto 443 de su firewall reciba datos de CX Cloud.

## Conexión del agente en la nube CX con Cisco DNA Center

P: ¿Cuál es el propósito y la relación de Cisco DNA Center con CX Cloud Agent o?

R: Cisco DNA Center es el agente en la nube que gestiona los dispositivos de red de las instalaciones del cliente. CX Cloud Agent recopila la información de inventario de los dispositivos del Cisco DNA Center configurado y carga la información de inventario que está disponible como "Vista de recursos" en CX Cloud.

P: ¿Dónde puede el usuario proporcionar los detalles de Cisco DNA Center sobre el agente de nube CX?

R - Durante la configuración del Día 0 - Agente en la nube CX, el usuario puede agregar los detalles del Cisco DNA Center desde el portal de nube CX. Además, durante las operaciones del día N, los usuarios pueden añadir centros de DNA adicionales desde Admin Settings > Data source.



P - ¿Cuántos Cisco DNA Centers se pueden añadir?

R: 10 clústeres de Cisco DNAC o 20 clústeres que no sean de DNAC.

P: ¿Qué función puede desempeñar el usuario del Cisco DNA Center?

R: La función de usuario puede ser admin or observer.

P - ¿Cómo reflejar las modificaciones en el agente CX debido a los cambios en las credenciales del centro DNA conectado?

R: Ejecute estos comandos desde la consola de CX Cloud Agent:

```
cxcli agent modifyController
```

Póngase en contacto con el soporte técnico para cualquier problema durante la actualización de credenciales de DNAC.

P: ¿Cómo se almacenan los datos de Cisco DNA Center en CX Cloud Agent?

R: Las credenciales de Cisco DNA Center se cifran mediante AES-256 y se almacenan en la base de datos de CX Cloud Agent. La base de datos de CX Cloud Agent está protegida con una ID de usuario y una contraseña seguras.

P: ¿Qué tipo de cifrado se utilizará al acceder a la API de Cisco DNA Center desde CX Cloud Agent?

R - HTTPS sobre TLS 1.2 se utiliza para la comunicación entre Cisco DNA Center y CX Cloud Agent.

P - ¿Cuáles son las operaciones realizadas por CX Cloud Agent en el Cisco DNA Center Cloud Agent integrado?

R - El agente en la nube de CX recopila los datos que Cisco DNA Center posee sobre los dispositivos de red y utiliza la interfaz de ejecución de comandos de Cisco DNA Center para comunicarse con los dispositivos finales y ejecutar los comandos CLI (comando show). No se ejecutan comandos de cambio de configuración

P: ¿Qué datos predeterminados se recopilan de Cisco DNA Center y se cargan en el back-end?

R-

- Entidad de red
- Módulos
- show version
- Config
- Información de imagen del dispositivo
- Etiquetas

P: ¿Qué datos adicionales se recopilan de Cisco DNA Center y se cargan en el back-end de Cisco?

R - Obtienes toda la información [aquí](#).

P: ¿Cómo se cargan los datos de inventario en el back-end?

R - El agente de nube CX carga los datos a través del protocolo TLS 1.2 en el servidor backend de Cisco.

P - ¿Cuál es la frecuencia de carga de inventario?

R: La recopilación se activa según la programación definida por el usuario y se carga en el back-end de Cisco.

P: ¿Puede el usuario volver a programar el inventario?

R: Sí, hay una opción disponible para modificar la información de programación de `Admin Settings> Data Sources`.

P - ¿Cuándo se produce el tiempo de espera de conexión entre Cisco DNA Center y Cloud Agent?

A - Los tiempos de espera se clasifican de la siguiente manera:

- Para la conexión inicial, el tiempo de espera es de 300 segundos como máximo. Si no se establece la conexión entre Cisco DNA Center y Cloud Agent en un máximo de 5 minutos, la conexión finaliza.
- Para actualizaciones periódicas, habituales o periódicas: el tiempo de espera de respuesta es de 1800 segundos. Si no se recibe la respuesta o no se puede leer en 30 minutos, la conexión finaliza.

## **Análisis de diagnóstico de CX Cloud Agent utilizado**

P - ¿Cuáles son los comandos ejecutados en el dispositivo para escanear?

R: Los comandos que deben ejecutarse en el dispositivo para el análisis se determinan dinámicamente durante el proceso de análisis. El conjunto de comandos puede cambiar con el tiempo, incluso para el mismo dispositivo (y que no esté bajo el control del Análisis de diagnóstico).

P: ¿Dónde se almacenan y se crean perfiles de los resultados del análisis?

R: Los resultados escaneados se almacenan y perfilan en el backend de Cisco.

P - ¿Los duplicados (por nombre de host o IP) en el Centro de ADN de Cisco, se agregan al Análisis de diagnóstico cuando el origen del Centro de ADN de Cisco está conectado?

R: No, los duplicados se filtrarán y solo se extraerán los dispositivos únicos.

P - ¿Qué sucede cuando falla uno de los escaneos de comando?

R: El análisis del dispositivo se detendrá por completo y se marcará como fallido.

## **Registros del sistema de agentes en la nube CX**

P: ¿Qué información de estado se envía a la nube de CX?

R: Registros de aplicaciones, estado de Pod, detalles de Cisco DNA Center, registros de auditoría, detalles del sistema y detalles del hardware.

P: ¿Qué detalles del sistema y del hardware se recopilan?

A - Ejemplo de salida:

```
detalles_del_sistema":{
  "os_details":{
    "containerRuntimeVersion":"docker://19.3.12",
    "kernelVersion":"5.4.0-47-generic",
    "kubeProxyVersion":"v1.15.12",
    "kubeletVersion":"v1.15.12",
    "machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
    "operatingSystem":"linux",
    "osImage":"Ubuntu 20.04.1 LTS",
    "systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
  },
  "hardware_details":{
    "total_cpu":"8",
    "cpu_utilization":"12.5%",
    "total_memory":"16007MB",
    "free_memory":"994 MB",
    "hdd_size":"214G",
    "free_hdd_size":"202G"
  }
}
```

P - ¿Cómo se envían los datos de estado al backend?

R: Con CX Cloud Agent, el servicio de mantenimiento transfiere los datos al servidor de Cisco.

P: ¿Cuál es la política de retención de registros de datos de estado del agente en la nube de CX en el backend?

R: La política de retención de datos de estado del agente en la nube de CX en el back-end es de 120 días.

P - ¿Cuáles son los tipos de cargas disponibles?

A - Tres tipos de cargas disponibles,

1. Carga del inventario
2. Carga de Syslog
3. Carga de estado del agente: 3 cosas como parte de la carga de estado Estado de los servicios: cada 5 minutos Podlog: cada 1 hora Registro de auditoría: cada 1 hora

## Resolución de problemas

**Problema:** No se puede acceder a la IP configurada.

**Solución:** Ejecute ssh usando la IP configurada. Si se agota el tiempo de espera de la conexión, la razón posible es una configuración incorrecta de IP. En este caso, reinstale configurando una dirección IP válida. Esto se puede realizar a través del portal con la opción de reinstalación proporcionada en el Admin Setting página.

**Problema:** ¿Cómo se verifica si los servicios están en funcionamiento después del registro?

**Solución:** Ejecute el comando que se muestra aquí y verifique si las vainas están funcionando.

1. ssh a la IP configurada como cxcadmin.
2. Proporcione la contraseña.
3. Ejecute el comando `kubectf get pods`.

Las vainas pueden estar en cualquier estado, como en ejecución, Inicializando o Creación de contenedor, pero después de 20 minutos, las vainas deben estar en estado de ejecución.

Si el estado es *no está en ejecución* o *Inicializando POD*, verifique la descripción del POD con el comando que se muestra aquí

```
kubectf describe pod <podname>
```

El resultado tendrá la información sobre el estado del grupo de dispositivos.

**Problema:** ¿Cómo verificar si el interceptor SSL está inhabilitado en el proxy del cliente?

**Solución:** Ejecute el comando curl que se muestra aquí para verificar la sección del certificado del servidor. La respuesta tiene los detalles del certificado del servidor web de concsoweb.

```
curl -v --header 'Autorización: Basic xxxxxx' https://concsoweb-prd.cisco.com/
```

\* Certificado de servidor:

\* asunto: C=US; ST=California; L=San José; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

\* fecha de inicio: 16 de febrero 11:55:11 2021 GMT

\* fecha de caducidad: 16 de febrero 12:05:00 2022 GMT

\* subjectAltName: el host "concsoweb-prd.cisco.com" coincidió con "concsoweb-prd.cisco.com" de cert

\* emisor: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL, CA G3

\* Certificado SSL verificado de acuerdo.

```
>GET / HTTP/1.1
```

**Problema:** Los comandos kubectl fallaron y muestran el error como "La conexión al servidor X.X.X.X:6443 fue rechazada - ¿especificó el host o puerto correcto?"

**Solución:**

- Compruebe la disponibilidad de los recursos. [ejemplo: CPU, Memoria]
- Espere a que comience el servicio Kubernetes

**Problema:** Cómo obtener los detalles de la falla de recolección para un comando/dispositivo

**Solución:**

- Ejecutar `kubectl get pods` y obtenga el nombre del grupo de dispositivos de recopilación.
- Ejecutar `kubectl logs` para obtener los detalles específicos del comando/dispositivo.

**Problema:** El comando kubectl no funciona con el error "[authentication.go:64] No se puede autenticar la solicitud debido a un error: [x509: el certificado ha caducado o aún no es válido, x509: el certificado ha caducado o todavía no es válido]"

**Solución:** Ejecute los comandos que se muestran aquí como usuario `cxroot`

```
rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl --insecure-skip-tls-verify=true delete secret -n kube-system k3s-serve
systemctl restart k3s
```

## Respuestas de fallos de recopilación

La causa de la falla de recolección puede ser cualquier restricción o problema que se observe con el controlador o los dispositivos agregados presentes en el controlador.

La tabla que se muestra aquí tiene el fragmento de error para los casos prácticos vistos en el microservicio de recopilación durante el proceso de recopilación.

### caso de uso

Si el dispositivo solicitado no se encuentra en Cisco DNA Center

Si el dispositivo solicitado no es accesible desde Cisco DNA Center

### Fragmento de registro en microservicio de recopilación

```
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a "
}
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "Error occurred while executing command: show version\nconnecting to device [Host: 172.21.137.221:22]No route to host : No route to host"
```

Si el dispositivo solicitado no es accesible desde Cisco DNA Center

```
}  
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "Error ocurred while executing command : show version\nconnecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 :  
Connection timed out: /X.X.X.X:22"  
}
```

Si el comando solicitado no está disponible en el dispositivo

```
{  
  "command": "show run-config",  
  "status": "Success",  
  "commandResponse": " Error ocurred while executing command : show ru  
config\n\nshow run-config\n      ^\n% Invalid input detected at \u0027^\u0027  
marker.\n\nXXCT5760#",  
  "errorMessage": ""  
}
```

Si el dispositivo solicitado no tiene SSHv2 y Cisco DNA Center intenta conectar el dispositivo con SSHv2

```
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "Error ocurred while executing command : show version\nchannel closed : Remote party uses incompatible protocol, it is not SSH-2  
compatible."  
}
```

Si el comando está deshabilitado en el microservicio de recopilación

```
{  
  "command": "config paging disable",  
  "status": "Command_Disabled",  
  "commandResponse": "Command collection is disabled",  
  "errorMessage": ""  
}
```

Si el Command Runner Task falló y la URL de la tarea no es devuelta por Cisco DNA Center

```
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "The command runner task failed for device %s. Task UR  
empty."  
}
```

Si la tarea Command Runner no se pudo crear en el centro de DNA de Cisco

```
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "The command runner task failed for device %s, Request  
%s. No task details."  
}
```

Si el microservicio de recopilación no recibe respuesta para una solicitud de Command Runner de Cisco DNA Center

```
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "The command runner task failed for device %s, Request  
%s."  
}
```

Si Cisco DNA Center no está completando la tarea dentro del tiempo de espera configurado (5 minutos por comando en el microservicio de recopilación)

```
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "Operation Timedout. The command runner task failed for  
%s, RequestURL: %s. No progress details."  
}
```

Si la tarea Command Runner Task falló y el ID de archivo está vacío para la tarea enviada por Cisco DNA Center

```
{  
  "command": "show version",  
  "status": "Failed",  
  "commandResponse": "",  
  "errorMessage": "The command runner task failed for device %s, Request
```

Si la tarea Command Runner ha fallado y Cisco DNA Center no devuelve la etiqueta de ID de archivo

```
%s. File id is empty."
}
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "The command runner task failed for device %s, Request
%s. No file id details."
}
{
```

Si el dispositivo no es apto para la ejecución del ejecutor de comandos

```
  "command": "config paging disable",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "Requested devices are not in inventory,try with other de
available in inventory"
}
{
```

Si el ejecutor de comandos está deshabilitado para el usuario

```
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "{\nmessage\": \"Role does not have valid permissions to ac
the API\"\n}"
}
```

## Respuestas de error de análisis de diagnóstico

El fallo del análisis y la causa pueden provenir de cualquiera de los componentes enumerados

Cuando el usuario inicia una exploración desde el portal, ocasionalmente se muestra como "failed: Error interno del servidor"

La causa del problema puede ser cualquiera de los componentes enumerados

- Punto de control
- Gateway de datos de red
- Conector
- Análisis de diagnóstico
- CX Cloud Agent Microservice [administrador de dispositivos, recopilación]
- Cisco DNA Center
- APIX
- Mashería
- Ping Access
- BANCO DE HIERRO
- IRONBANK GW
- Big Data Broker (BDB)

Para ver los registros:

1. Inicie sesión en la consola de CX Cloud Agent
2. ssh a cxcadmin y proporcione la contraseña
3. Ejecutar `kubectl get pods`
4. Obtenga el nombre de la recopilación, el conector y la facilidad de mantenimiento del grupo de dispositivos.
5. Para comprobar los registros de microservicios de recopilación, conector y mantenimiento

- Ejecutar `kubectl logs`
- Ejecutar `kubectl logs`
- Ejecutar `kubectl logs`

La tabla que se muestra aquí muestra el fragmento de error que se ve en los registros de microservicio de recopilación y microservicio de mantenimiento que se produce debido a problemas o restricciones con los componentes.

## Caso de uso

El dispositivo puede ser accesible y compatible, pero los comandos que se ejecutan en ese dispositivo se enumeran en bloques en el microservicio de recopilación

Si el dispositivo que se intenta analizar no está disponible. Se produce en un escenario, cuando hay un problema de sincronización entre los componentes, como el portal, la exploración de diagnóstico, el componente CX y Cisco DNA Center

Si el dispositivo que se intenta escanear está ocupado, (en un escenario) en el que el mismo dispositivo ha sido parte de otro trabajo y no se manejan solicitudes paralelas desde Cisco DNA Center para el dispositivo.

Si el dispositivo no es compatible con el análisis

Si el dispositivo que se ha intentado analizar no está accesible

Si no se puede acceder a Cisco DNA Center desde el microservicio Cloud Agent o Collection del Cloud Agent no está recibiendo respuesta para una solicitud Command Runner de Cisco DNA Center

## Fragmento de registro en microservicio de recopilación

```
{
  "command": "config paging disable",
  "status": "Command_Disabled",
  "commandResponse": "Command collection disabled",
}
```

```
No device found with id 02eb08be-b13f-4d2e-eaf4e882f71a
```

```
All requested devices are already being queued for command runner in another session. Please wait for other devices".
```

```
Requested devices are not in inventory, try with other devices available in inventory
"Error occurred while executing command: s...
ud\nError connecting to device [Host: x.x.x.x]
route to host : No route to host
```

```
{
  "command": "show version",
  "status": "Failed",
  "commandResponse": "",
  "errorMessage": "The command runner task failed for device %s, RequestURL: %s."
}
```

## caso de uso

Si la solicitud de análisis tiene detalles de programación que faltan

Si la solicitud de análisis tiene detalles del dispositivo que faltan

Si la conexión entre el CPA y la conectividad está inactiva

Si el dispositivo para análisis solicitado no está disponible en Análisis de diagnóstico

## Fragmento de registro en el microservicio Agent punto de control

Failed to execute request

```
{"message":"23502: null value in column \"schedule\" violates not null constraint"}
```

Failed to create scan policy. No valid devices in the request

Failed to execute request.

```
Failed to submit the request to scan. Reason = {"message":"Device with Hostname=x.x.x.x' was not found"}
```



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).