

Panoramica di CX Cloud Agent v2.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Accesso ai domini critici](#)

[Prerequisiti per l'aggiornamento a CX Cloud Agent v2.0](#)

[Versioni certificate di Cisco DNA Center](#)

[Browser supportati](#)

[Distribuisci agente cloud CX](#)

[Connetti agente cloud CX a CX Cloud](#)

[Implementazione e configurazione della rete](#)

[Implementazione dell'OVA](#)

[Installazione del thick client ESXi 5.5/6.0](#)

[Installazione del client Web ESXi 6.0](#)

[Installazione del client Web vCenter](#)

[Installazione di Oracle Virtual Box 5.2.30](#)

[Installazione di Microsoft Hyper-V](#)

[Configurazione della rete](#)

[Approccio alternativo per generare il codice di accoppiamento tramite CLI](#)

[Configurazione di Cisco DNA Center per l'inoltro del syslog all'agente cloud CX](#)

[Prerequisito](#)

[Configurazione dell'inoltro di syslog](#)

[Abilita impostazioni syslog livello informazioni](#)

[Sicurezza](#)

[Sicurezza fisica](#)

[Accesso utente](#)

[Sicurezza dell'account](#)

[Sicurezza della rete](#)

[Autenticazione](#)

[Protezione avanzata](#)

[Sicurezza dei dati](#)

[Trasmissione dati](#)

[Log e monitoraggio](#)

[Riepilogo delle funzionalità di sicurezza](#)

[Domande frequenti](#)

[CX Cloud Agent](#)

[Implementazione](#)

[Release e patch](#)

[Autenticazione e configurazione del proxy](#)

[Secure Shell \(SSH\)](#)

[Porte e servizi](#)

[Rapporto tra CX Cloud Agent e Cisco DNA Center](#)

[Analisi diagnostica di CX Cloud Agent](#)

[Log di sistema di CX Cloud Agent](#)

[Risoluzione dei problemi](#)

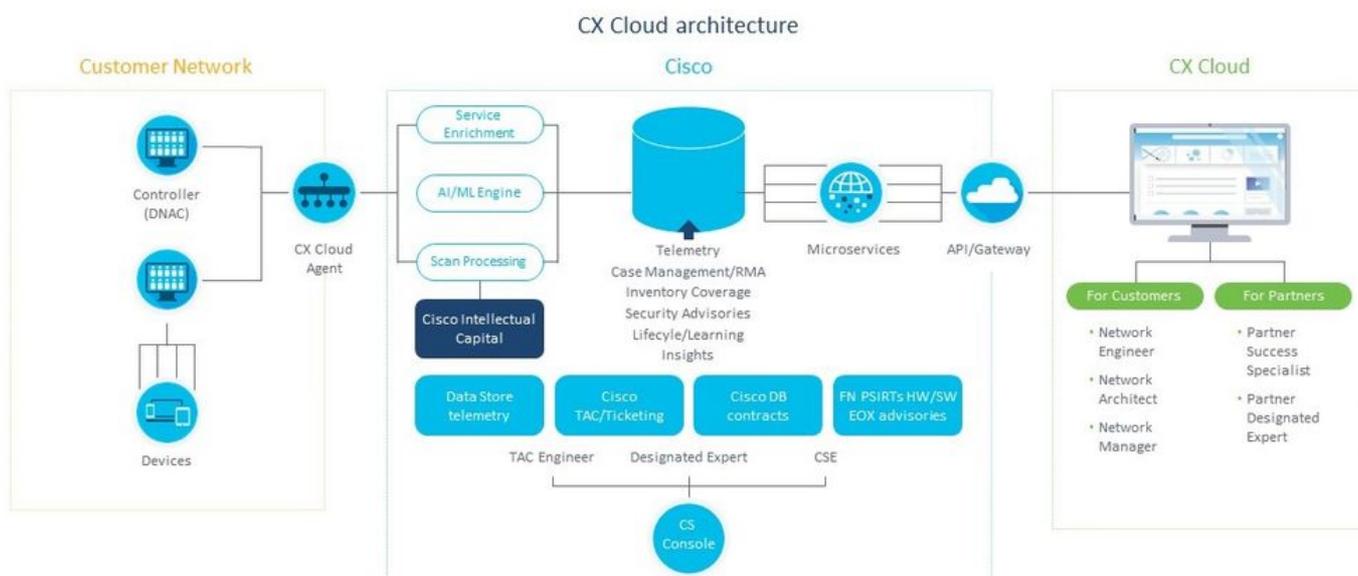
[Risoluzione degli errori di raccolta](#)

[Risoluzione degli errori di analisi diagnostica](#)

Introduzione

Questo documento descrive Cisco's Customer Experience (CX) Cloud Agent. Cisco (CX) Cloud Agent è una piattaforma software on-premise modulare modernizzata che ospita funzionalità di microservizi container leggere. I microservizi possono essere installati, configurati e gestiti direttamente in locale dal cloud. CX Cloud Agent accelera la monetizzazione di nuove offerte, scala le funzionalità e aiuta a sviluppare servizi di nuova generazione guidati da big data, analisi, automazione, Machine Learning/Artificial Intelligence (ML/AI) e streaming.

Nota: Questa guida è destinata agli utenti di CX Cloud Agent v2.0. Fare riferimento a [Cisco CX Cloud Agent](#) per altre informazioni correlate.



Architettura di CX Cloud Agent

Nota: Le immagini (e il contenuto al loro interno) in questa guida hanno solo scopo di riferimento. Il contenuto effettivo può variare.

Prerequisiti

CX Cloud Agent viene eseguito come macchina virtuale (VM) e può essere scaricato come OVA (Open Virtual Appliance) o VHD (Virtual Hard Disk).

Requisiti da distribuire:

- Uno dei seguenti hypervisor: VMware ESXi versione 5.5 o successiva Oracle Virtual Box 5.2.30 Windows Hypervisor versione 2012-2016
- L'hypervisor può ospitare una VM che richiede: 8 core di CPU 16 GB di memoria/RAM 200 GB

di spazio su disco

- Per i clienti che utilizzano i data center Cisco USA designati come area dati principale per l'archiviazione dei dati di CX Cloud:
L'agente cloud CX deve essere in grado di connettersi ai server mostrati qui, utilizzando l'FQDN e HTTPS sulla porta TCP 443:
FQDN: agent.us.cisco.cloud
FQDN: ng.acs.agent.us.cisco.cloud
FQDN: cloudsso.cisco.com
FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati Cisco Europe designati come area dati principale per l'archiviazione dei dati di CX Cloud:
L'agente cloud CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando l'FQDN e utilizzando HTTPS sulla porta TCP 443:
FQDN: agent.us.cisco.cloud
FQDN: agente.emea.cisco.cloud
FQDN: ng.acs.agent.emea.cisco.cloud
FQDN: cloudsso.cisco.com
FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati Cisco Asia Pacifico designati come area dati principale per l'archiviazione dei dati di CX Cloud:
L'agente cloud CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando l'FQDN e utilizzando HTTPS sulla porta TCP 443:
FQDN: agent.us.cisco.cloud
FQDN: agente.apjc.cisco.cloud
FQDN: ng.acs.agent.apjc.cisco.cloud
FQDN: cloudsso.cisco.com
FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati Cisco Europa e Cisco Asia Pacifico designati come regione dati principale, la connettività all'FQDN: agent.us.cisco.cloud è richiesto solo per la registrazione dell'agente CX Cloud con CX Cloud durante la configurazione iniziale. Una volta completata la registrazione dell'agente di CX Cloud con CX Cloud, questa connessione non è più necessaria.
- Per la gestione locale dell'agente cloud CX, la porta 22 deve essere accessibile.

Ulteriori caratteristiche di CX Cloud Agent:

- Se il protocollo DHCP (Dynamic Host Configuration Protocol) è abilitato nell'ambiente VM, verrà rilevato automaticamente un indirizzo IP. In caso contrario, devono essere disponibili un indirizzo IPv4 libero, una subnet mask, un indirizzo IP predefinito del gateway e un indirizzo IP del server DNS.
- È supportato solo IPv4, non IPv6.
- Sono richieste le versioni certificate del centro DNA (Digital Network Architecture) per cluster a nodo singolo e ad alta disponibilità (HA) Cisco da 1.2.8 a 1.3.3.9 e da 2.1.2.0 a 2.2.3.5.
- Se la rete dispone di un'intercettazione SSL, fornire l'indirizzo IP dell'agente cloud CX.

Accesso ai domini critici

Per iniziare il percorso di CX Cloud, gli utenti devono accedere a questi domini.

Domini principali	Altri domini
cisco.com	mixpanel.com
cisco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

Domini specifici dell'area:

AMERICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	m
agent.us.cisco.cloud	agent.us.cisco.cloud	api-cx.cisco.com
ng.acs.agent.us.cisco.cloud	agent.us.cisco.cloud	agent.us.cisco.cloud
	agente.emea. cisco.cloud	d
	ng.acs.agent.emea. cisco.cloud	agente.apjc. cisco.cloud
		ng.acs.agent.apjc.cisco.cloud

Prerequisiti per l'aggiornamento a CX Cloud Agent v2.0

I prerequisiti descritti in questa sezione devono essere soddisfatti prima dell'aggiornamento a CX Cloud Agent v2.0.

1. Prima di avviare l'aggiornamento, verificare che CX Cloud Agent v1.12.x e versioni successive sia installato.
2. Eseguire la procedura seguente per configurare il server dei nomi di dominio se non è già configurato:
Accedere alla console Command Line Interface (CLI) della macchina virtuale dell'agente cloud CX. Eseguire il comando `cxcli agent configureDNS`. Immettere l'indirizzo IP DNS. Clic Exit.
3. Verificare che la rete del cliente consenta ai nomi di dominio in [Accesso al dominio critico di](#) completare la nuova registrazione dell'agente cloud durante la migrazione. L'agente cloud CX deve essere in grado di raggiungere questi domini e anche i domini devono essere risolvibili dal server DNS. Se un dominio non è raggiungibile, contattare il team di rete.
4. Eseguire uno snapshot della macchina virtuale dell'agente cloud prima di avviare l'aggiornamento v2.0 (è necessario l'accesso appropriato).

Nota: Le versioni precedenti alla 1.10 devono prima eseguire l'aggiornamento alla versione 1.10, quindi gli aggiornamenti incrementali alla versione 1.12.x e infine alla versione 2.0. Gli utenti possono eseguire l'aggiornamento da Impostazioni di amministrazione > Origini dati nel portale CX Cloud. Clic `View Update` per completare l'aggiornamento.

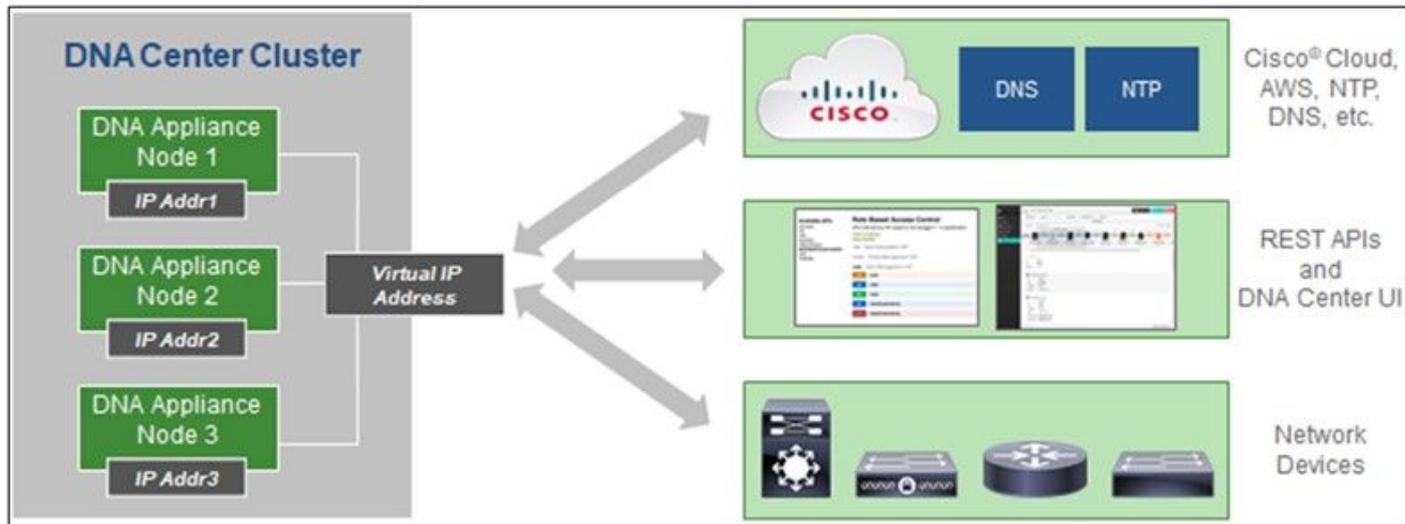
Condizioni da soddisfare per la corretta installazione:

1. Elenco di DNAC e relative credenziali
2. Utente DNAC con accesso al ruolo **Admin** o **Observer**

3. Indirizzo IP virtuale o indirizzo IP fisico/autonomo per il cluster DNAC
4. Raggiungibilità tra Cloud Agent e DNAC
5. DNAC deve avere almeno 1 (uno) dispositivo gestito

Versioni certificate di Cisco DNA Center

Le versioni certificate supportate di Cisco DNA Center a nodo singolo e cluster HA vanno dalla 1.2.8 alla 1.3.3.9 e dalla 2.1.2.0 alla 2.2.3.5.



Cisco DNA Center con cluster HA a più nodi

Browser supportati

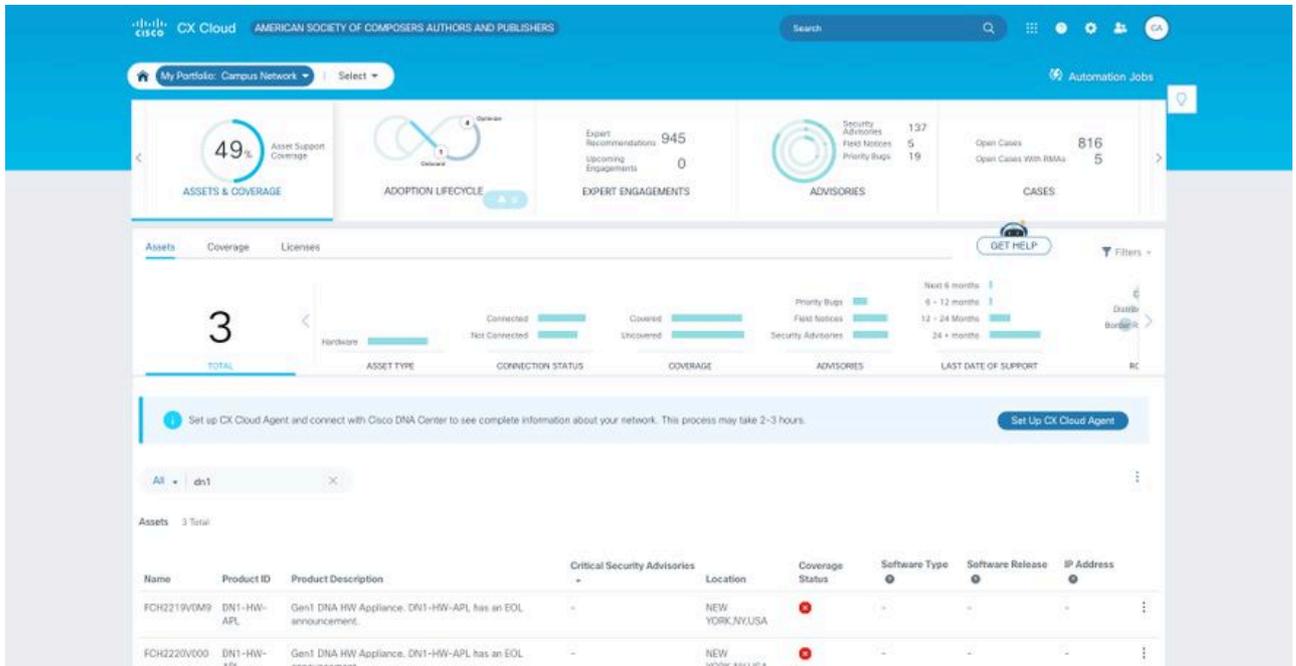
Per un'esperienza ottimale su Cisco.com, si consiglia l'ultima versione ufficiale di questi browser:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Distribuisci agente cloud CX

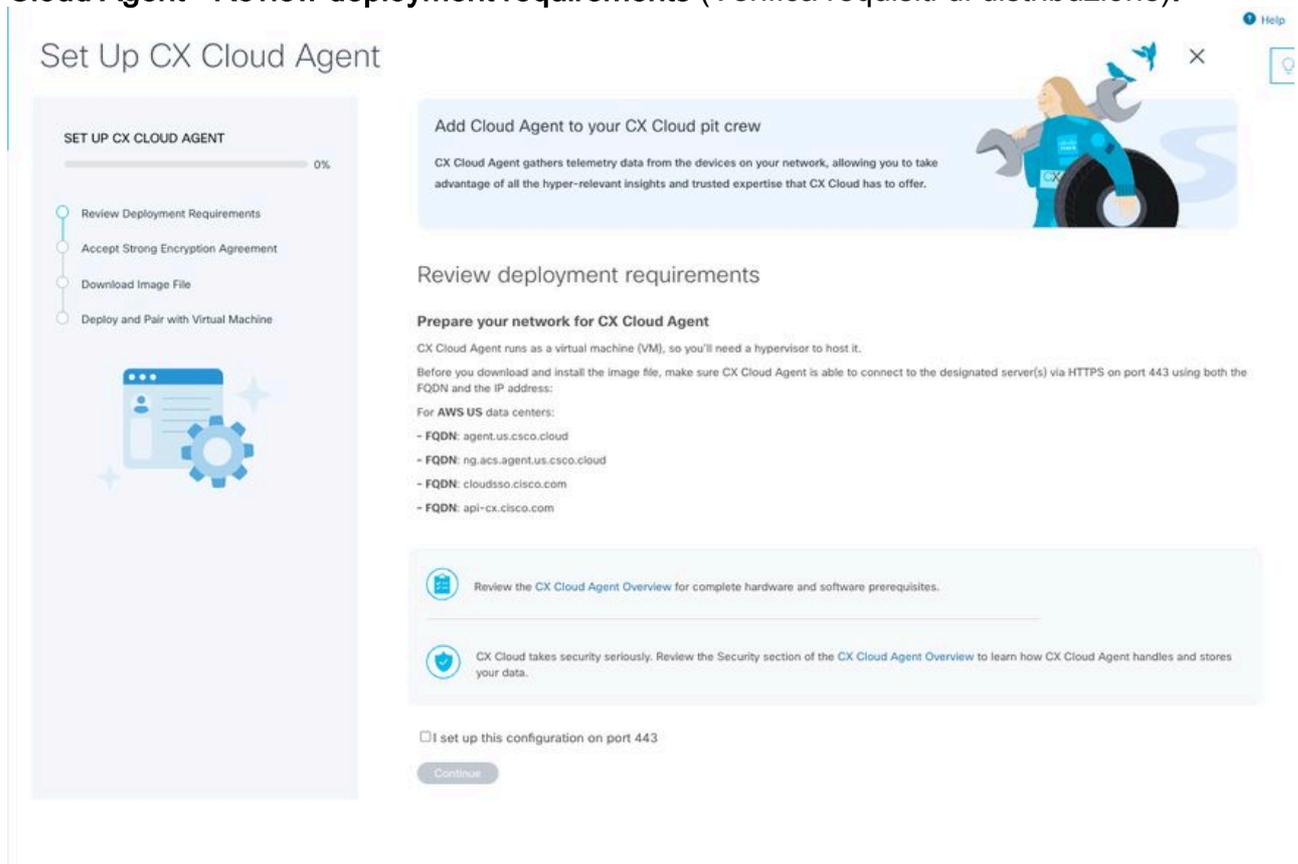
Per implementare CX Cloud Agent:

1. Fare clic su cx.cisco.com per accedere a CX Cloud.
2. Seleziona Campus Network e passare a ASSETS & COVERAGE piastrella.



Home page

- Fare clic su **Set Up CX Cloud Agent** nel banner. Viene visualizzata la finestra **Set Up CX Cloud Agent - Review deployment requirements** (Verifica requisiti di distribuzione).



Verifica requisiti di distribuzione

- Leggere i prerequisiti in **Verifica requisiti di distribuzione** e selezionare la casella di controllo **I set up this configuration on port 443**.

Nota: Le immagini (e il contenuto al loro interno) in questa guida hanno solo scopo di riferimento. Il contenuto effettivo può variare.

- Fare clic su **Continua**. Viene visualizzata la finestra **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

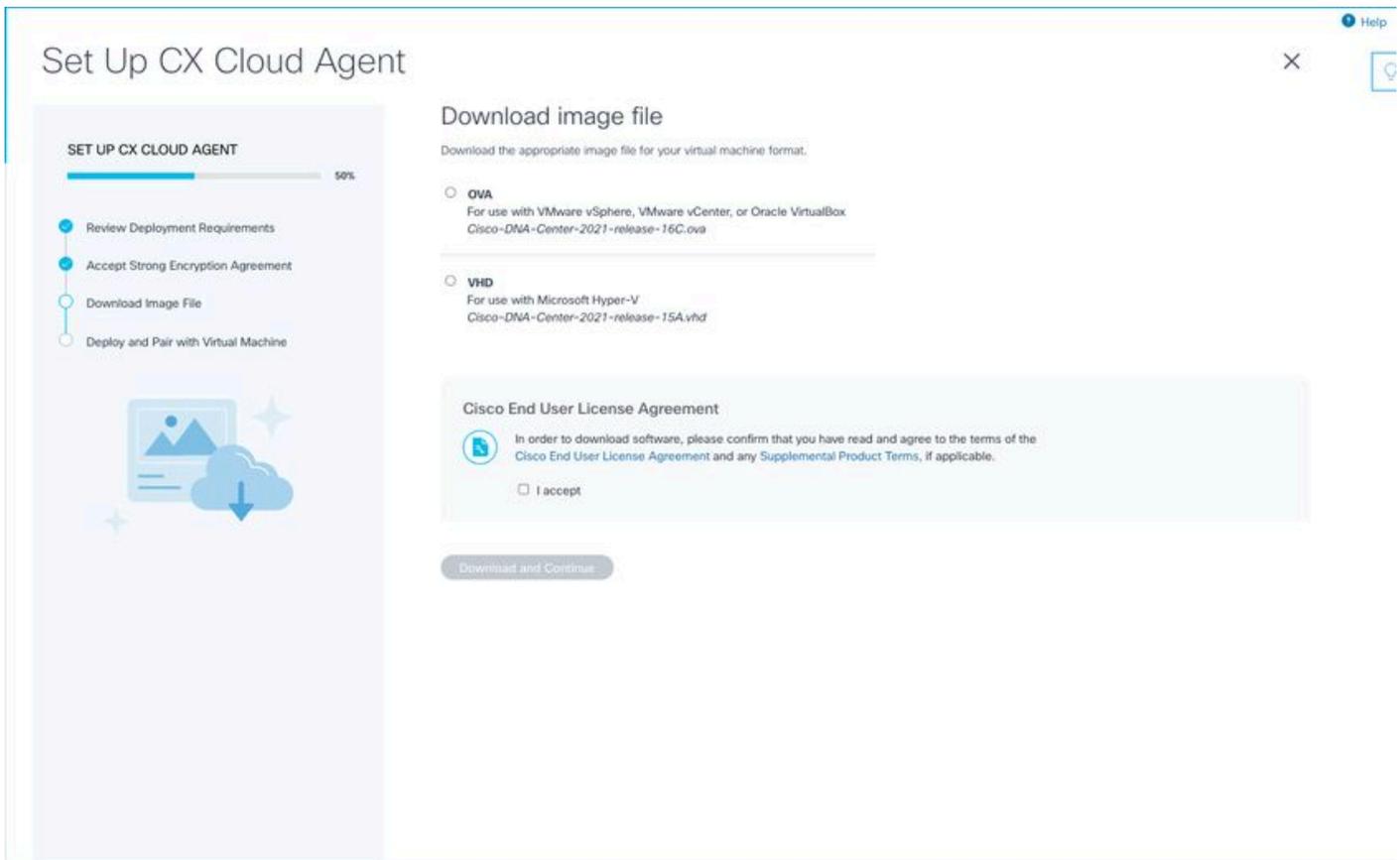
Confirmation

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

Contratto di crittografia

6. Verificare le informazioni precompilate nei campi **Nome, Cognome, Posta elettronica e ID utente CCO**.
7. Selezionare la scheda **Business division's function**.
8. Selezionare il **Confirmation** per accettare le condizioni di utilizzo.
9. Fare clic su **Continua**. Viene visualizzata la finestra **Set Up CX Cloud Agent - Download file immagine**.



Scarica immagine

10. Selezionare il formato di file appropriato per scaricare il file di immagine necessario per l'installazione.

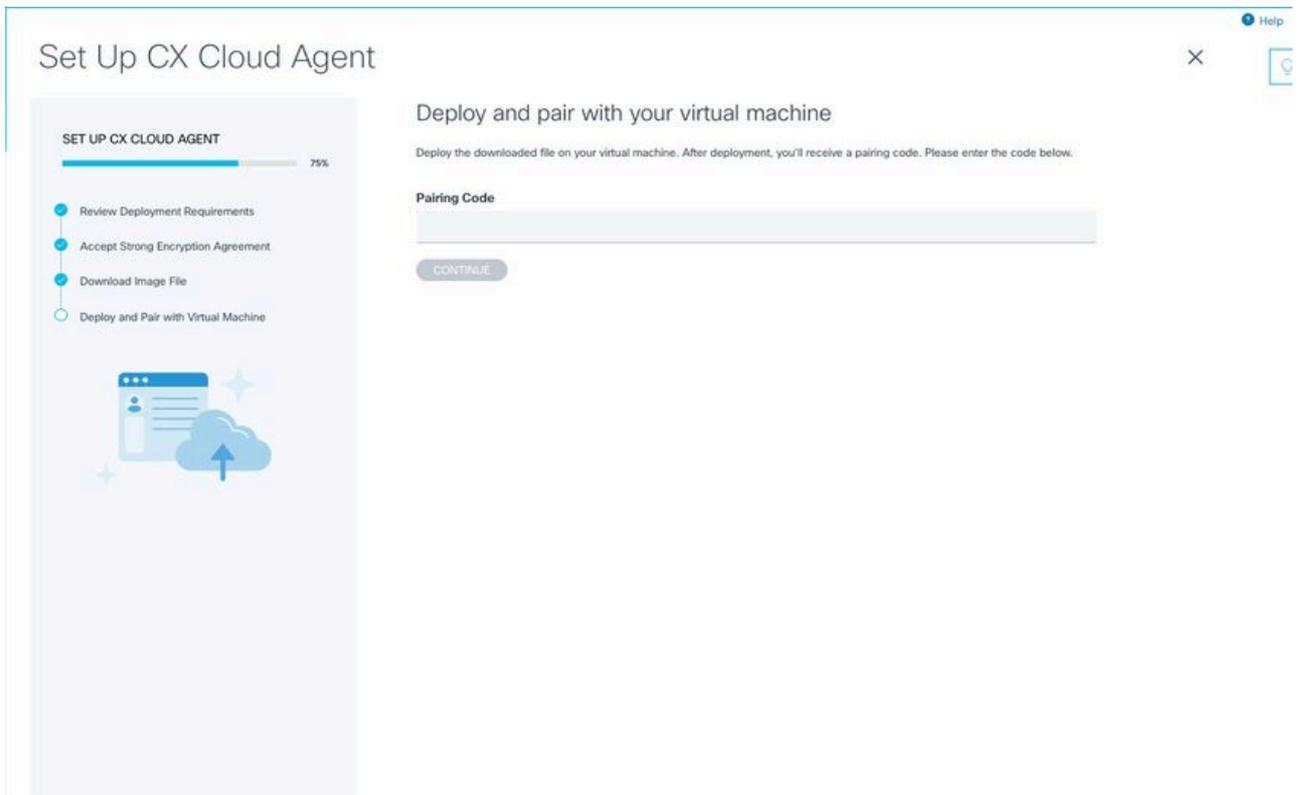
11. Selezionare la casella di controllo **Accetto** per accettare il contratto di licenza con l'utente finale Cisco.

12. Fare clic su **Download e Continua**. Viene visualizzata la finestra **Imposta agente cloud CX - Distribuisci e associa alla macchina virtuale**.

13. Fare riferimento a [Network Configuration](#) per l'installazione di OVA e passare alla sezione successiva per installare l'agente cloud CX.

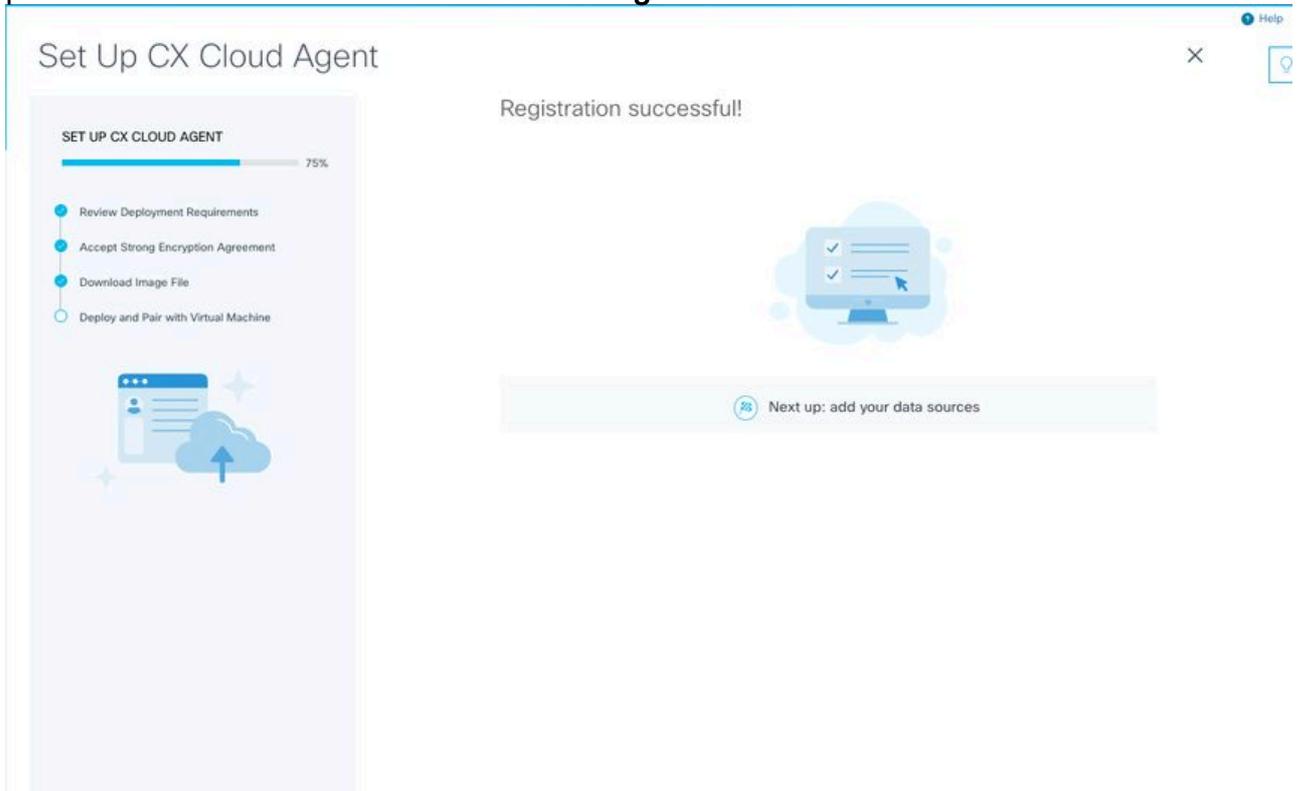
Connetti agente cloud CX a CX Cloud

1. Immettere il **codice di associazione** fornito nella finestra di dialogo della console o nell'interfaccia della riga di comando (CLI).



Codice di associazione

2. Fare clic su **Continue** (Continua) per registrare l'agente cloud CX. La finestra **Imposta agente cloud CX - Registrazione riuscita** viene visualizzata per alcuni secondi prima di passare automaticamente alla finestra **Configura connessione a CX Cloud**



Registrazione completata

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](#)

Configura connessione

3. Immettere i dati e fare clic su **Connetti origine dati**. Viene visualizzato il messaggio di conferma "Connesso correttamente".

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](#)

Aggiunta DNAC completata

Nota: Clic Add Another Cisco DNA Center per aggiungere più 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

Aggiunta di più DNAC

4. Fare clic su **Fine connessione origini dati**. Verrà visualizzata la finestra **Origini dati**.

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

Origini dei dati

Implementazione e configurazione della rete

Per distribuire l'agente cloud CX è possibile selezionare una delle seguenti opzioni:

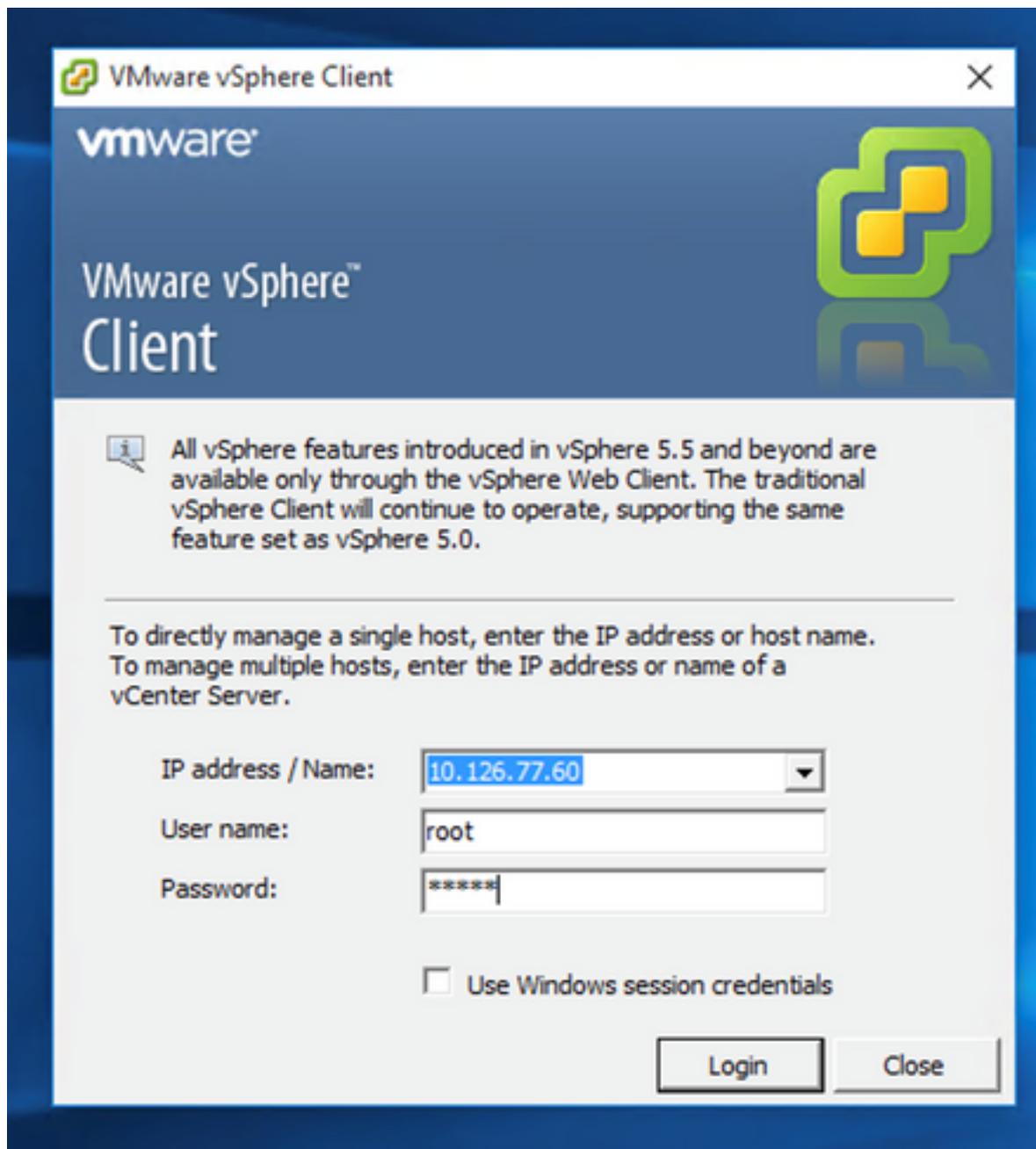
- Se si sceglie il thick client ESXi 5.5/6.0 di VMware vSphere/vCenter, andare a [Thick Client](#).
- Se si sceglie il client Web ESXi 6.0 di VMware vSphere/vCenter, andare a [Web Client vSphere](#) o [Center](#).
- Se si sceglie Oracle Virtual Box 5.2.30, andare a [Oracle VM](#).
- Se si sceglie Microsoft Hyper-V, andare a [Hyper-V](#).

Implementazione dell'OVA

Installazione del thick client ESXi 5.5/6.0

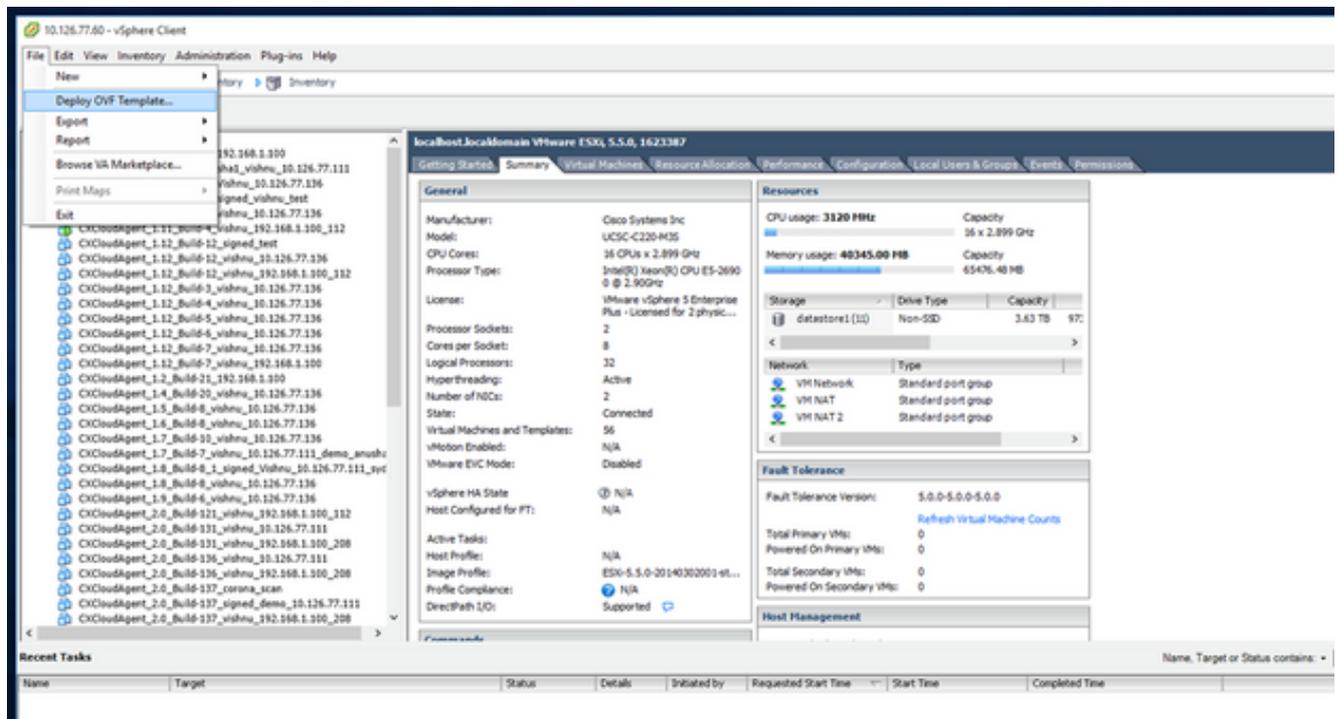
Questo client consente la distribuzione di VSA agente cloud CX mediante il client thick vSphere.

1. Dopo aver scaricato l'immagine, avviare il client VMware vSphere ed eseguire il login.



Accesso

2. Passa a File > Deploy OVF Template.



Client vSphere

3. Selezionare il file OVA e fare clic su Next.

Source

Select the source location.

Source

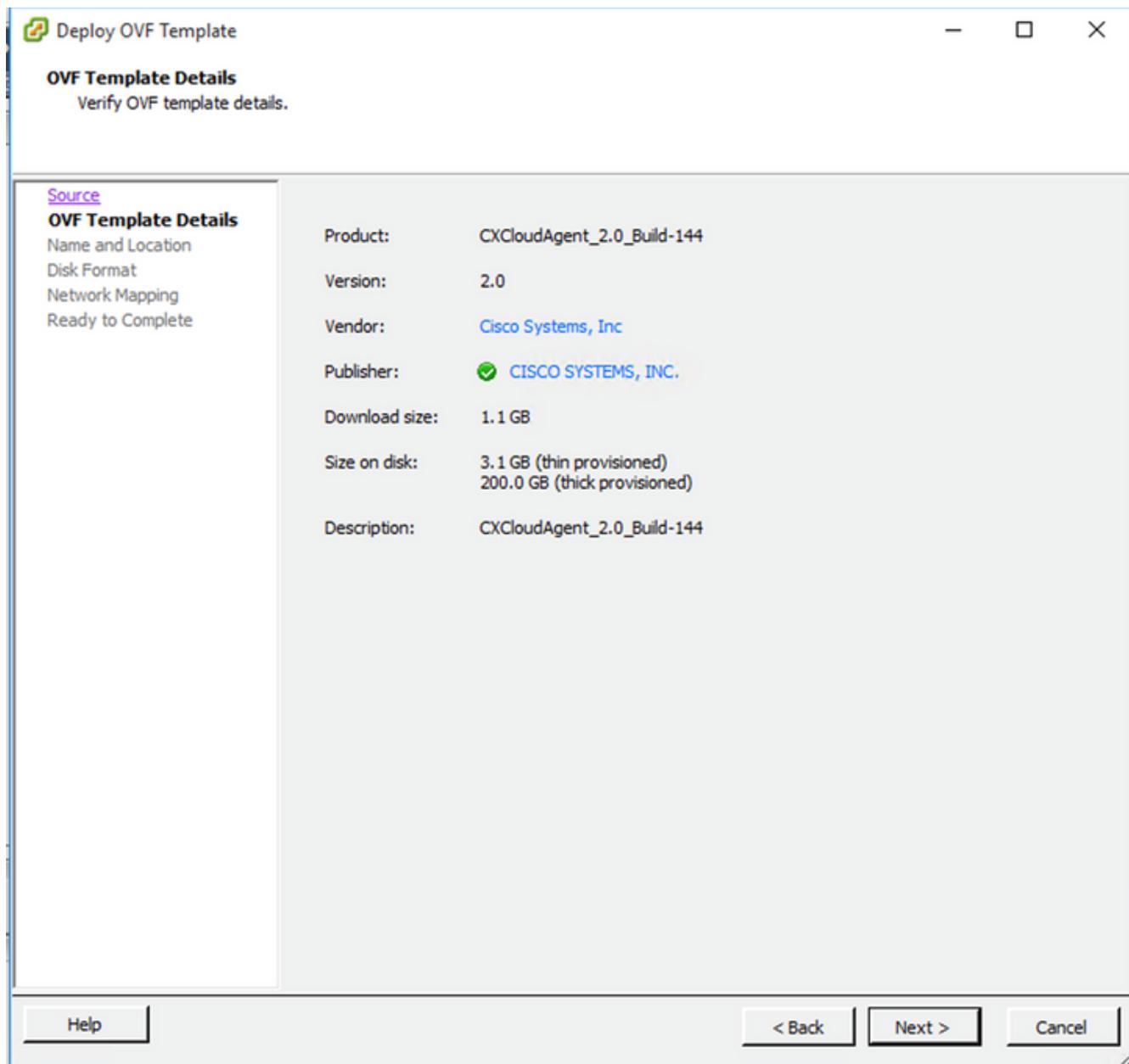
- OVF Template Details
- Name and Location
- Disk Format
- Ready to Complete

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.

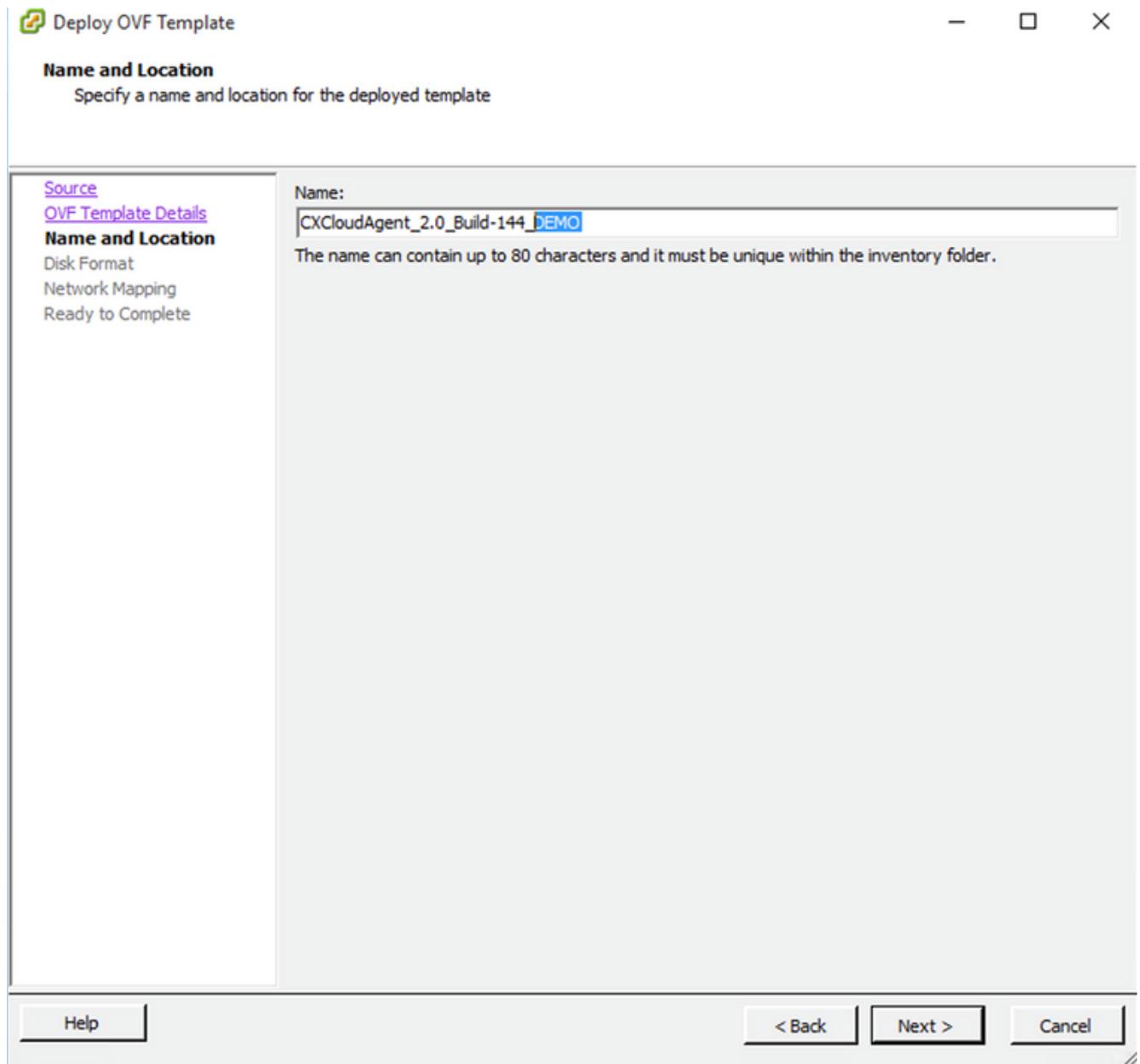
Percorso OVA

4. Verificare OVF Details e fare clic su Next.



Dettagli del modello

5. Immettere un Unique Name e fare clic su Next.



Nome e posizione

6. Seleziona un Disk Format e fare clic su Next (si consiglia Thin Provision).

Disk Format

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

Source OVF Template Details Name and Location Disk Format 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 del disco

7. Selezionare il Power on after deployment e fare clic su 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:

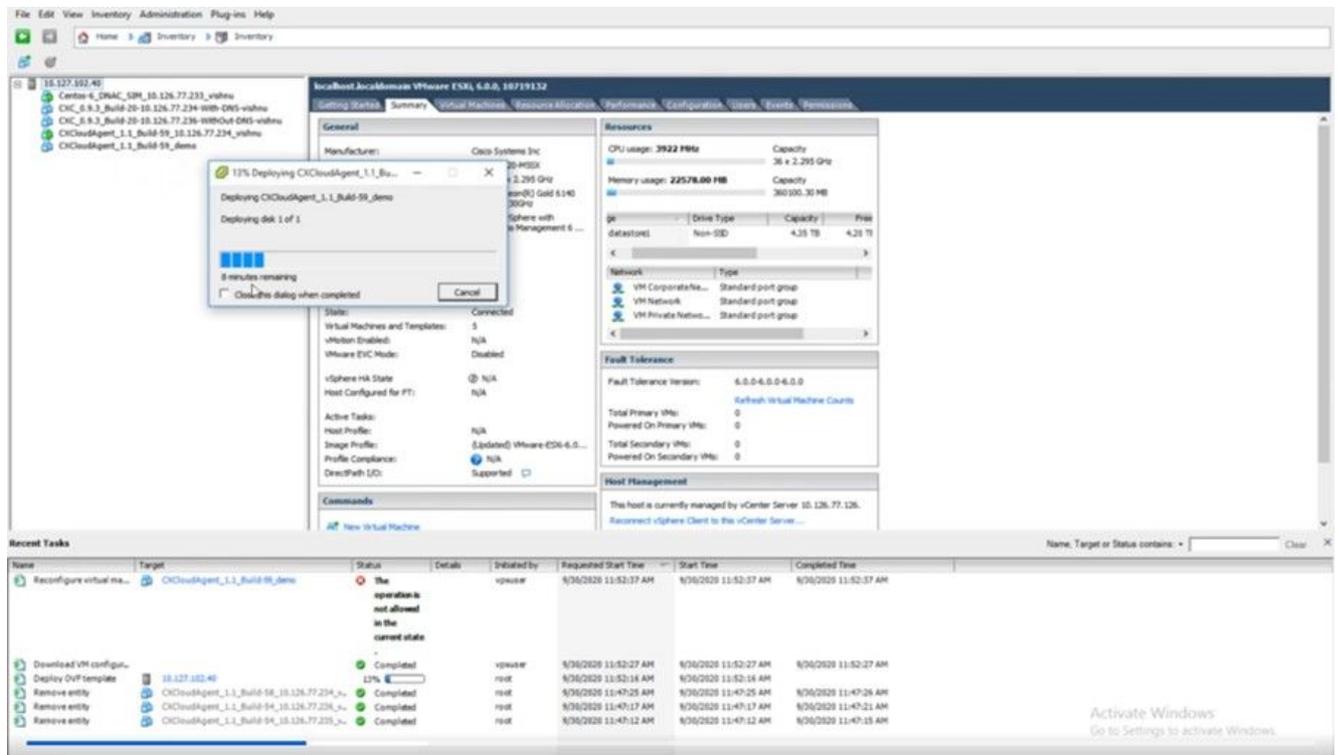
OVF file:	C:\Users\oxcadmin\Downloads\OVA\CXCloudAgent_2.0...
Download size:	1.1 GB
Size on disk:	3.1 GB
Name:	CXCloudAgent_2.0_Build-144_DEMO
Host/Cluster:	localhost
Datastore:	datastore1 (11)
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"

Power on after deployment

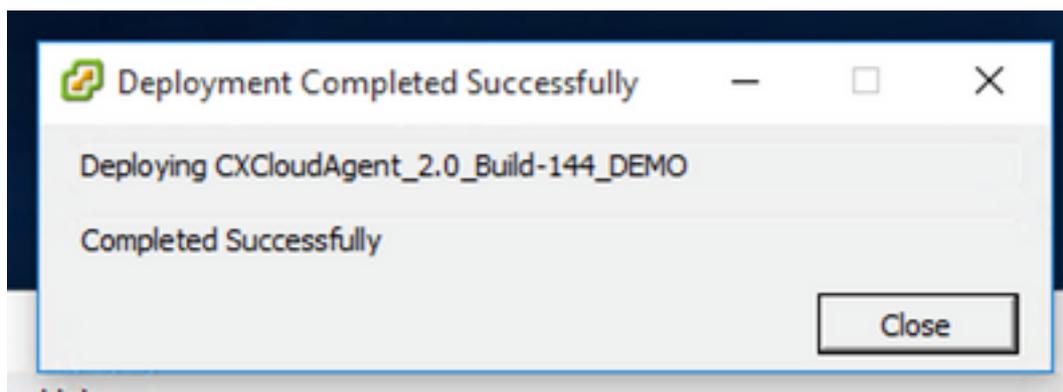
Help < Back Finish Cancel

Pronto per il completamento

La distribuzione può richiedere alcuni minuti. Attendere finché non viene visualizzato un messaggio di completamento.



Implementazione in corso



Implementazione completata

8. Selezionare la VM appena distribuita, aprire la console e passare a [Configurazione di rete](#).

Installazione del client Web ESXi 6.0

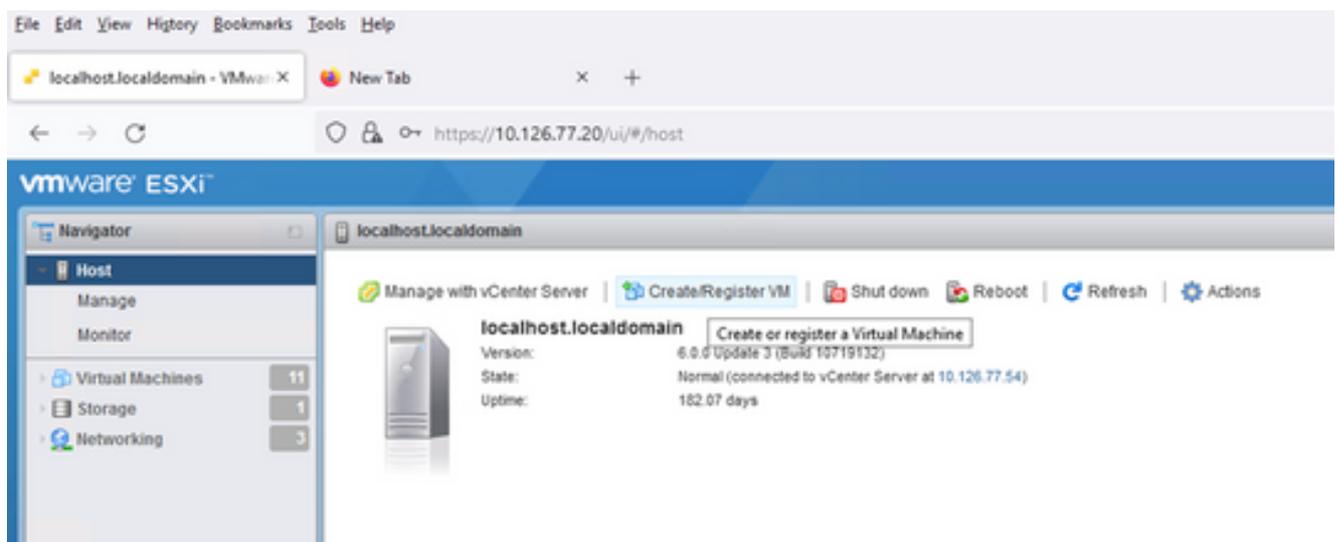
Questo client distribuisce l'agente cloud CX tramite il Web vSphere.

1. Accedere all'interfaccia utente di VMWare con le credenziali ESXi/hypervisor utilizzate per l'installazione della VM.

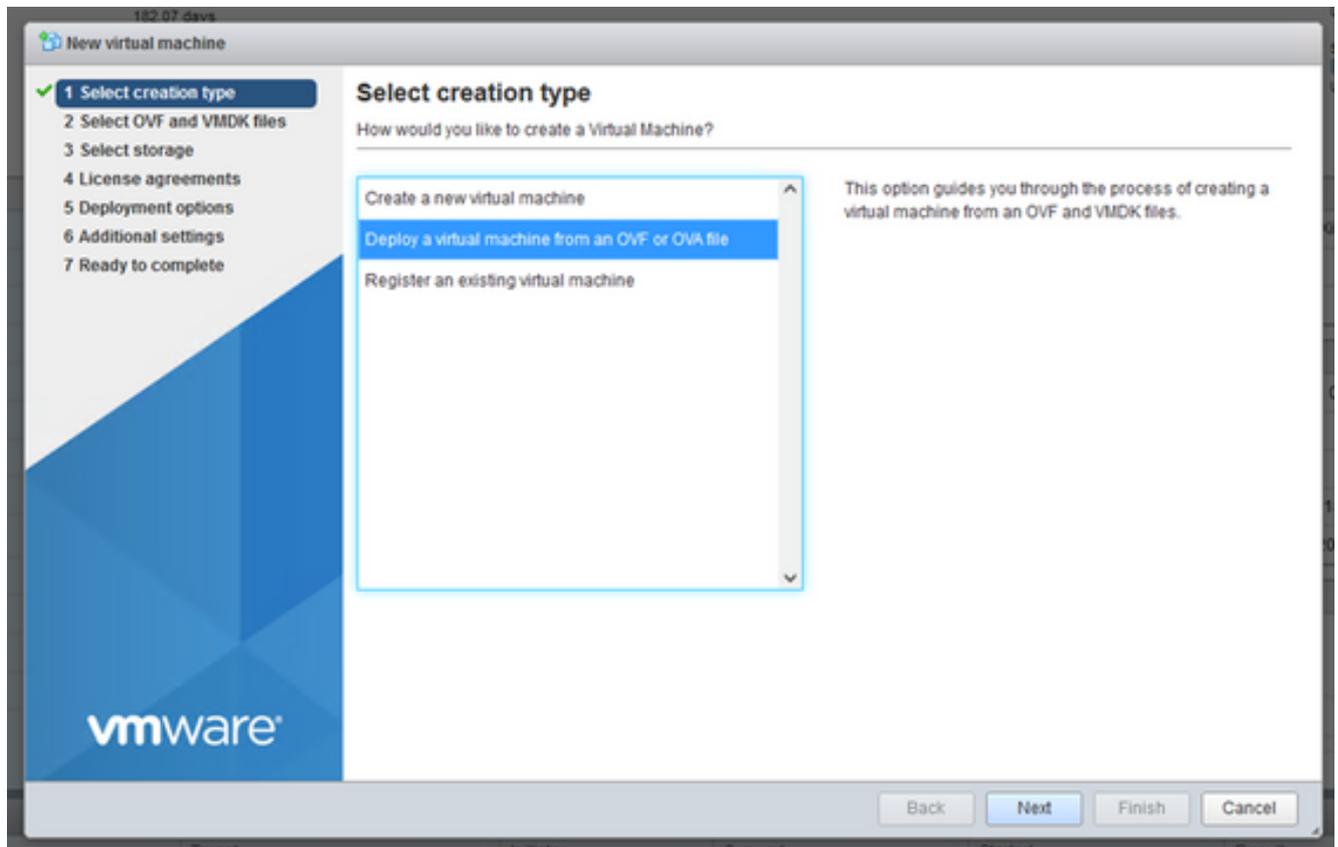


Accesso a VMware ESXi

2. Seleziona Virtual Machine > Create / Register VM.

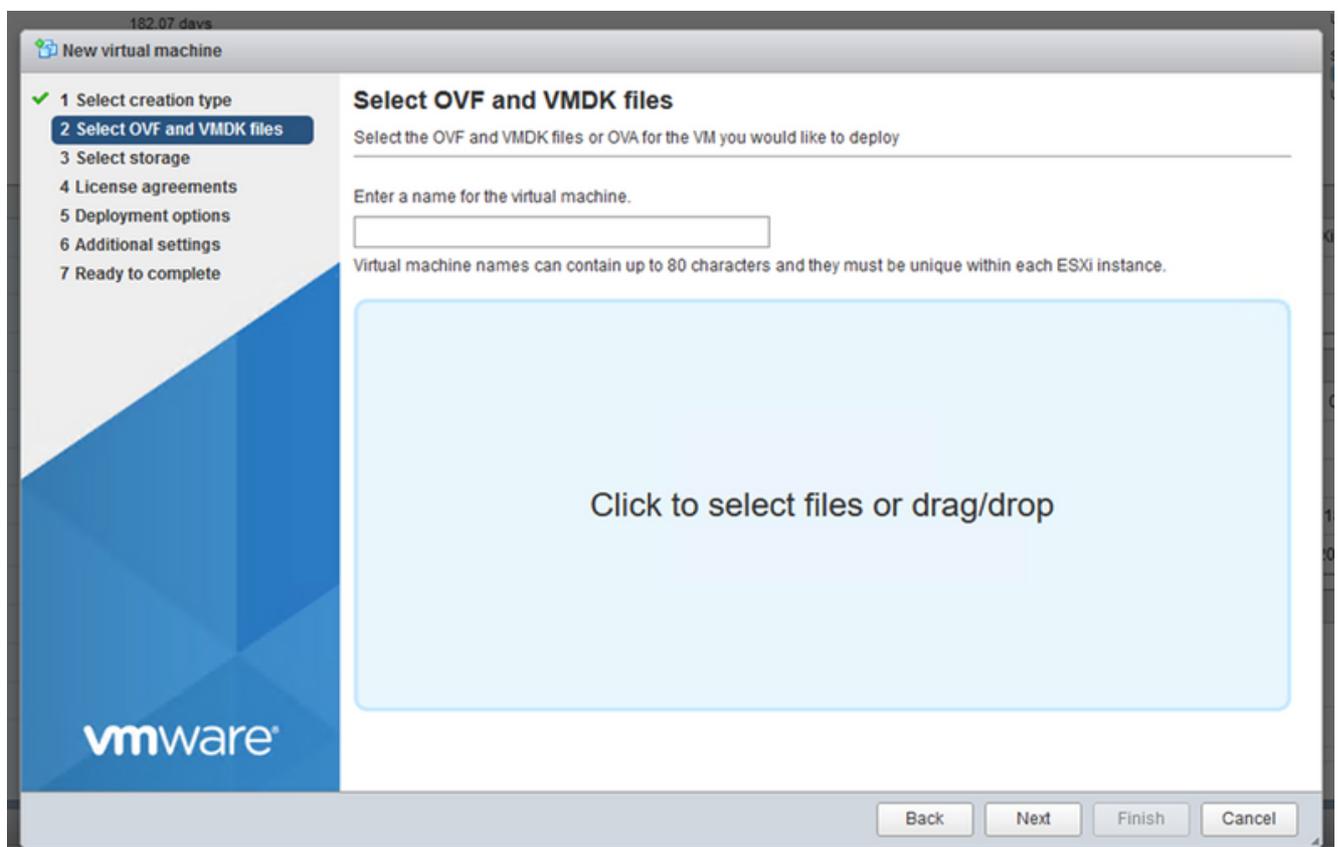


Creazione della VM



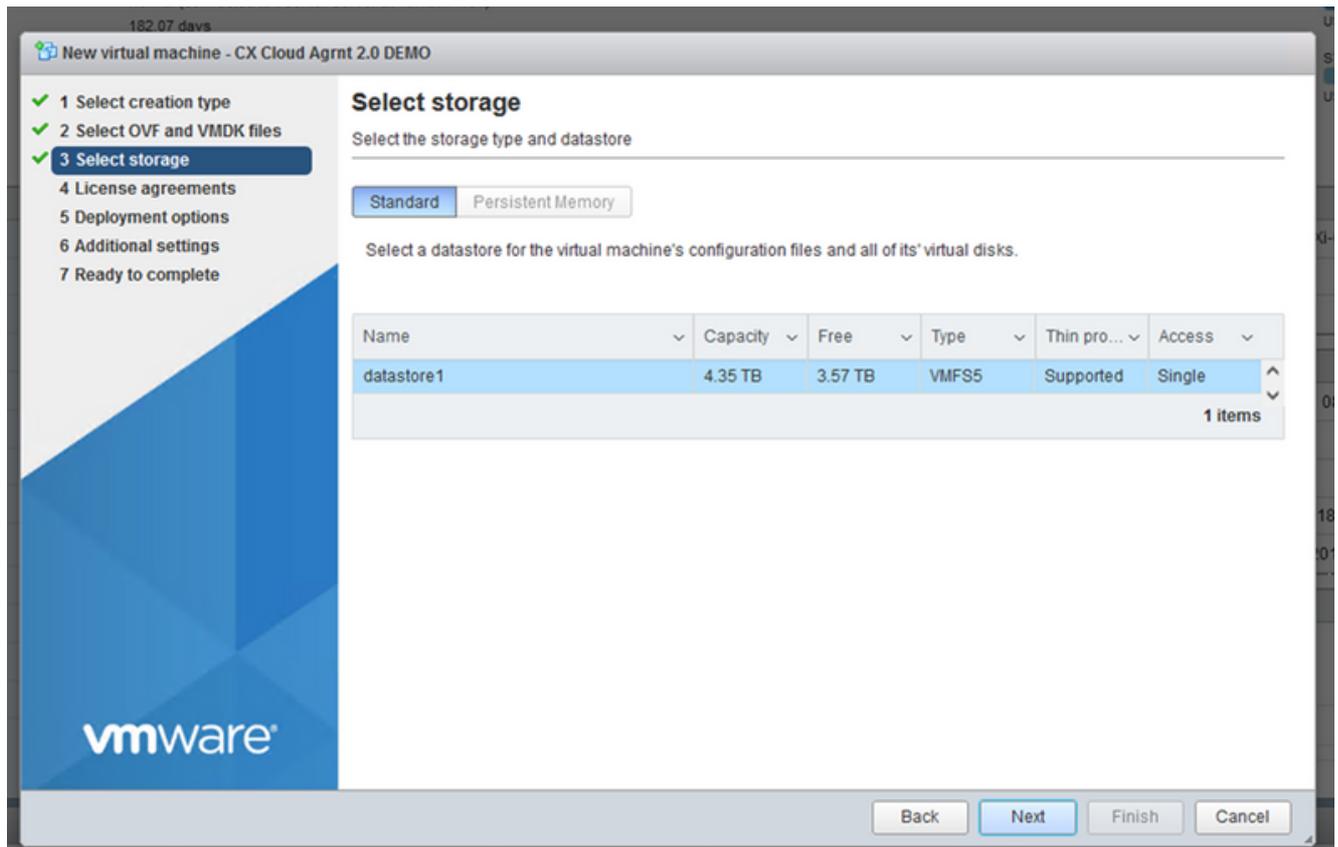
Implementazione dell'OVA

3. Seleziona Deploy a virtual machine from an OVF or OVA file e fare clic su Next.
4. Immettere il nome della VM, selezionare il file o trascinare il file OAV scaricato.
5. Clic Next.

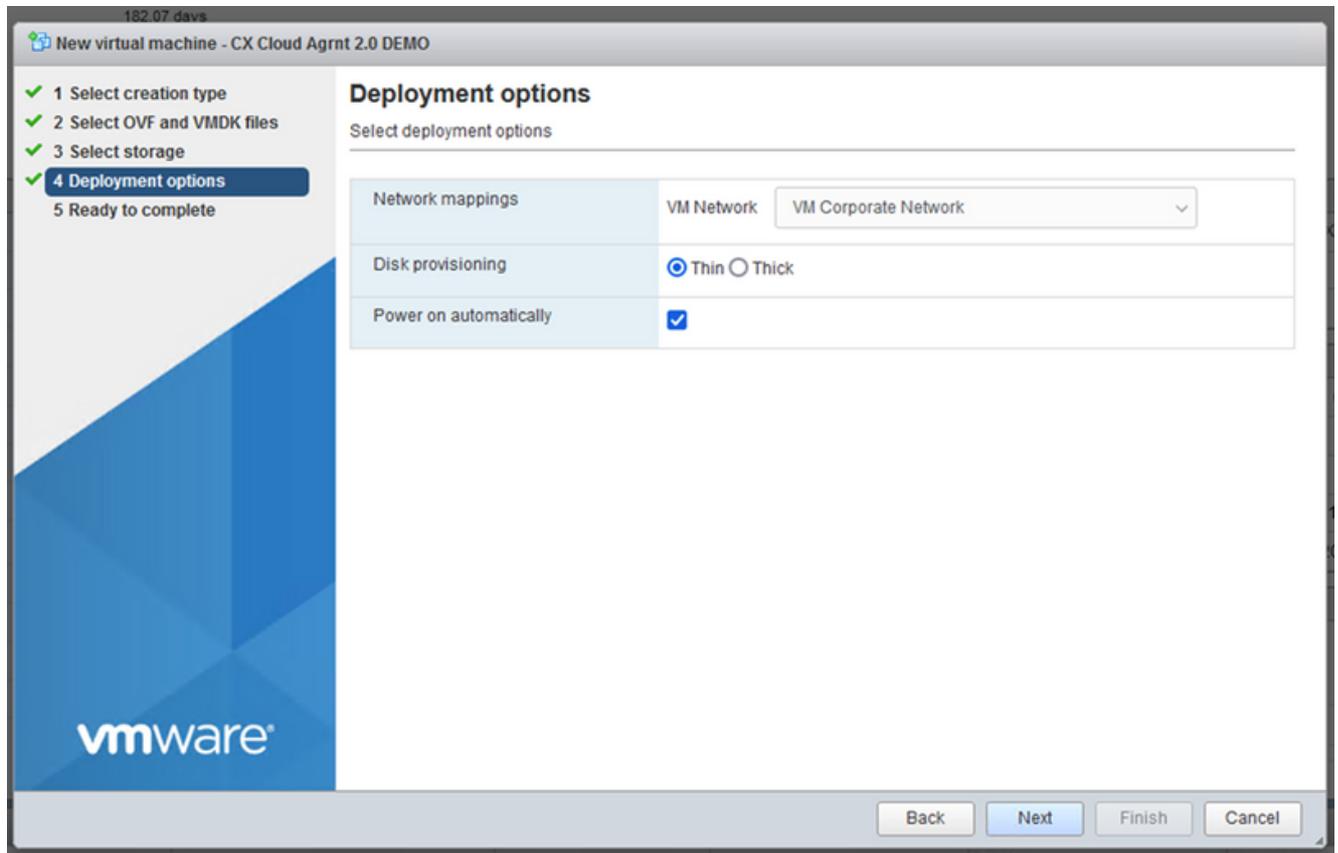


Selezione dell'OVA

6. Seleziona Standard Storage e fare clic su Next.

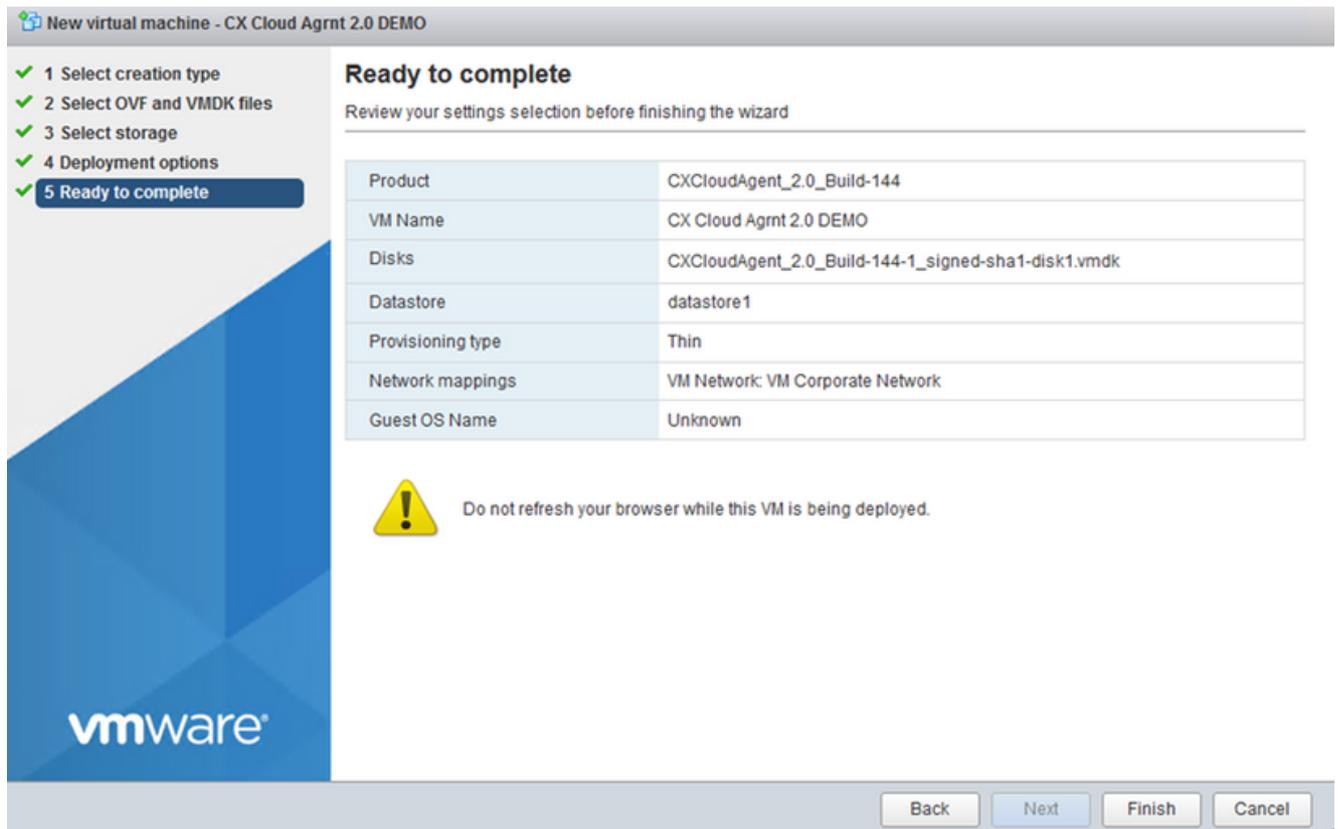


Selezione dell'archivio

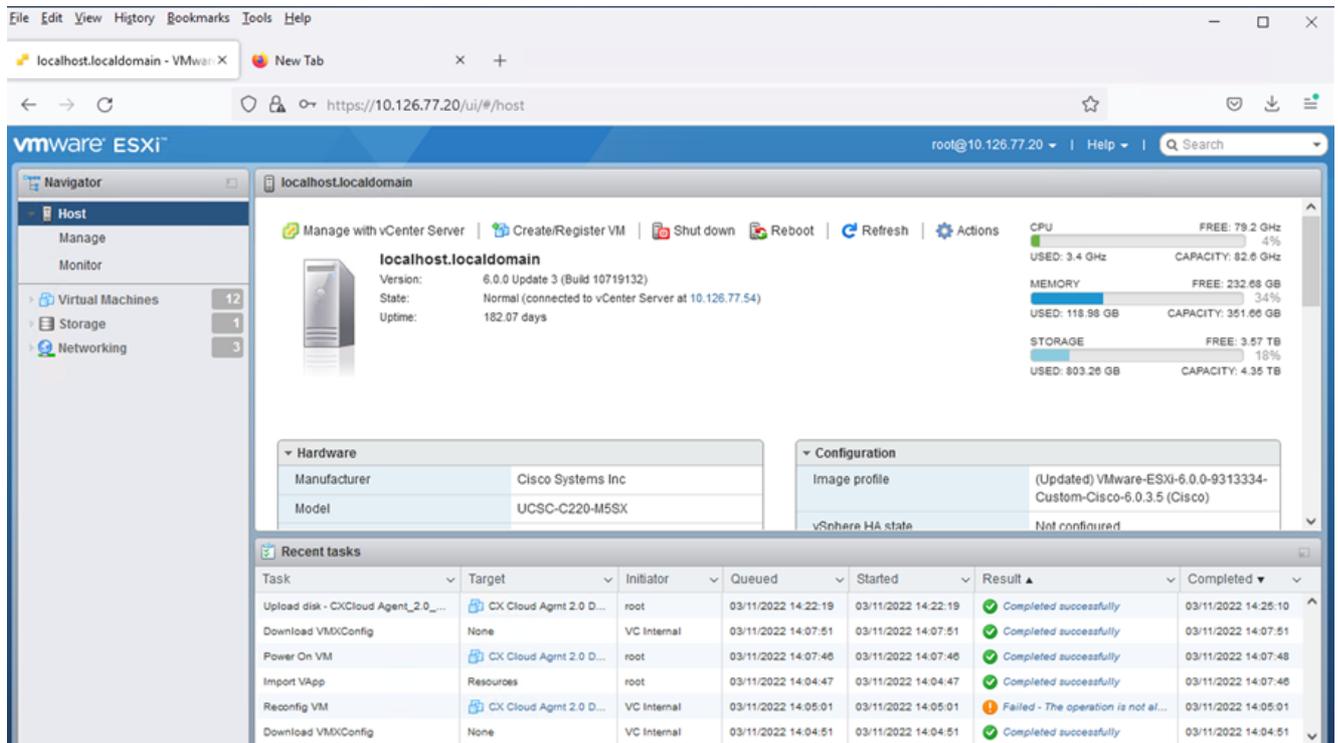


Opzioni di implementazione

7. Selezionare le opzioni di distribuzione appropriate e fare clic su Next.

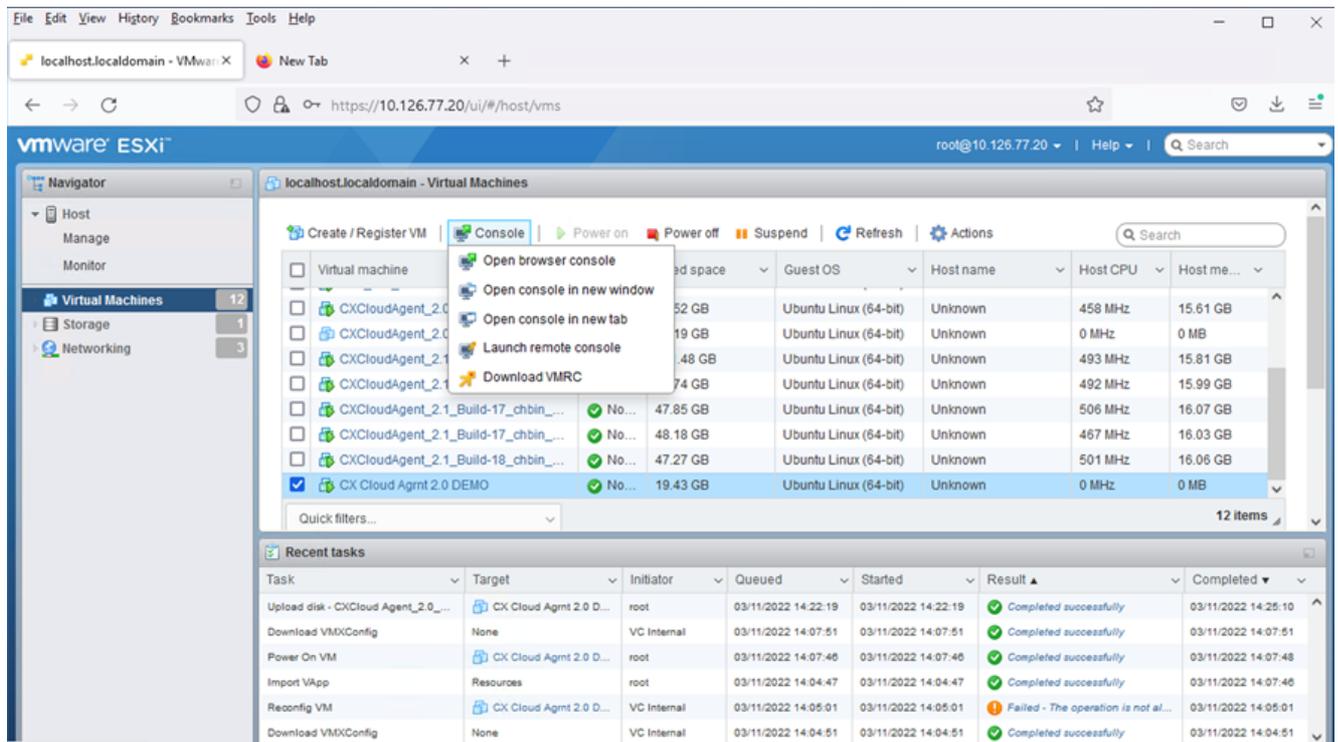


Pronto per il completamento



Procedura completata

8. Controllare le impostazioni e fare clic su Finish.
9. Selezionare la VM appena distribuita e scegliere Console > Open browser console.



Apertura della console

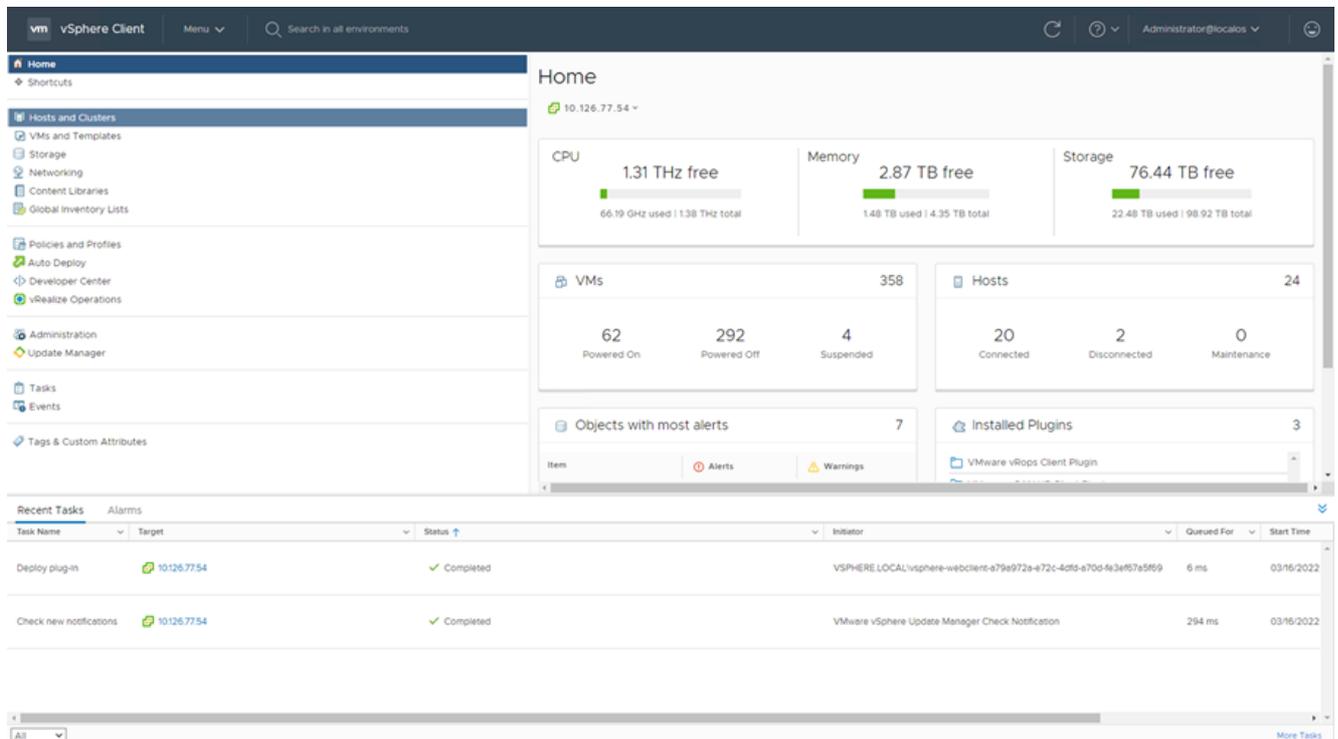
10. Andare a [Network Configuration](#) (Configurazione della rete).

Installazione del client Web vCenter

1. Accedere al client vCenter utilizzando le credenziali ESXi/hypervisor.

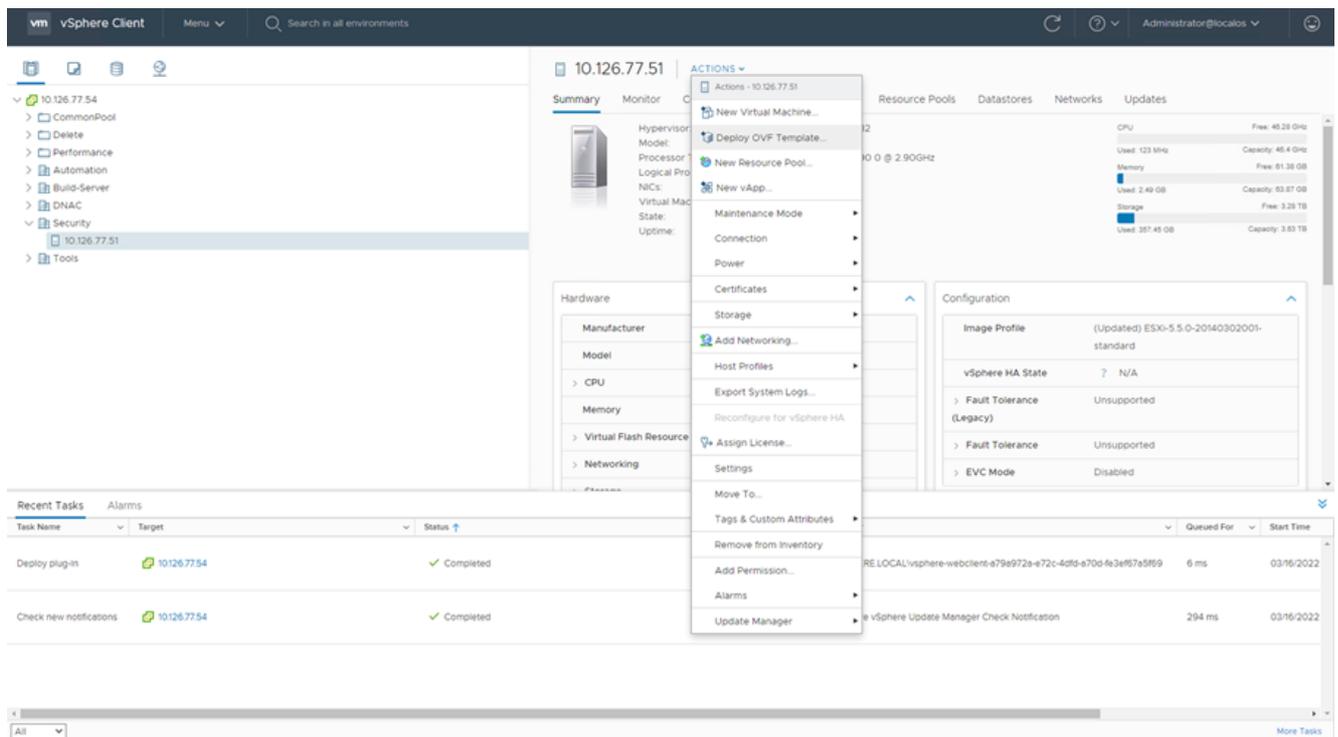


Accesso

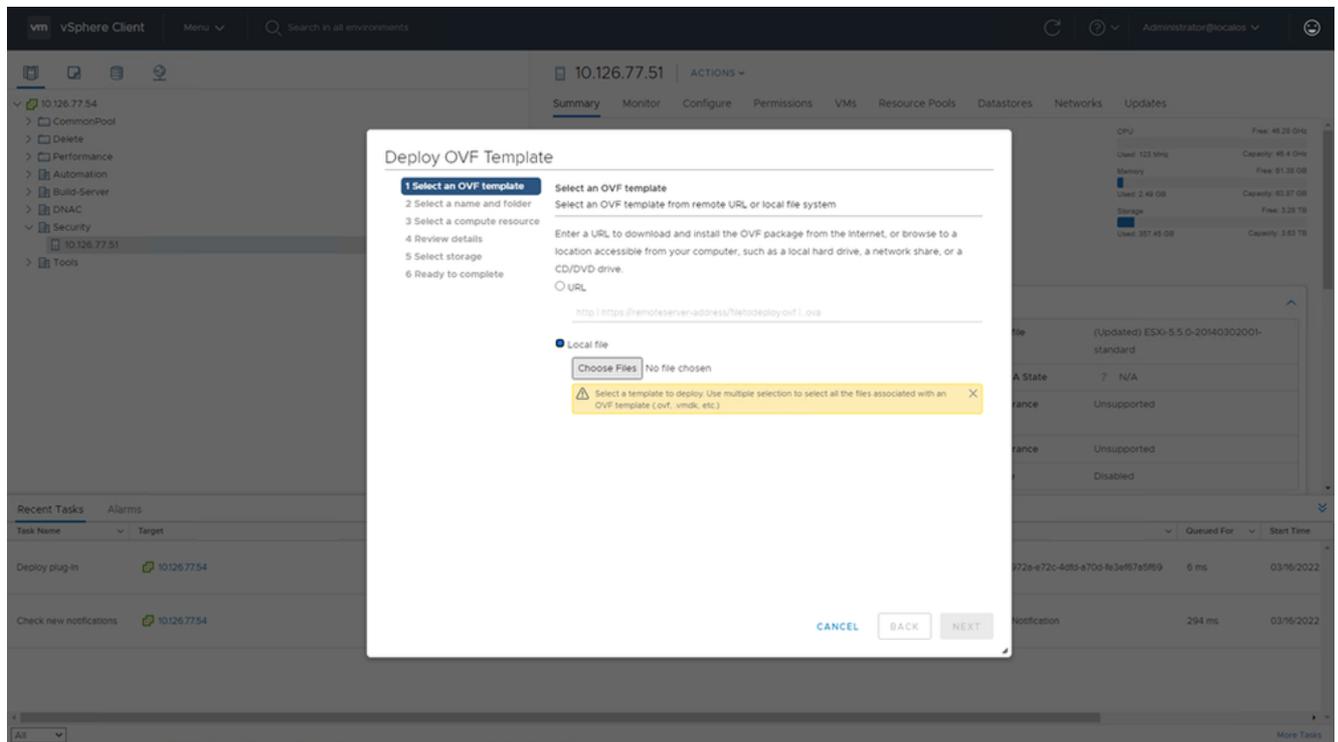


Schermata principale

2. Nella home page fare clic su Hosts and Clusters.
3. Selezionare la VM e fare clic su Action > Deploy OVF Template.



Azioni



Selezione del modello

4. Aggiungere l'URL direttamente o selezionare il file OVA e fare clic su Next.
5. Immettere un nome univoco e selezionare la posizione, se necessario.
6. 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

Nome e cartella

7. Selezionare la risorsa di calcolo e fare clic su 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

Seleziona risorsa di calcolo

8. Rivedere i dettagli e fare clic su 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)

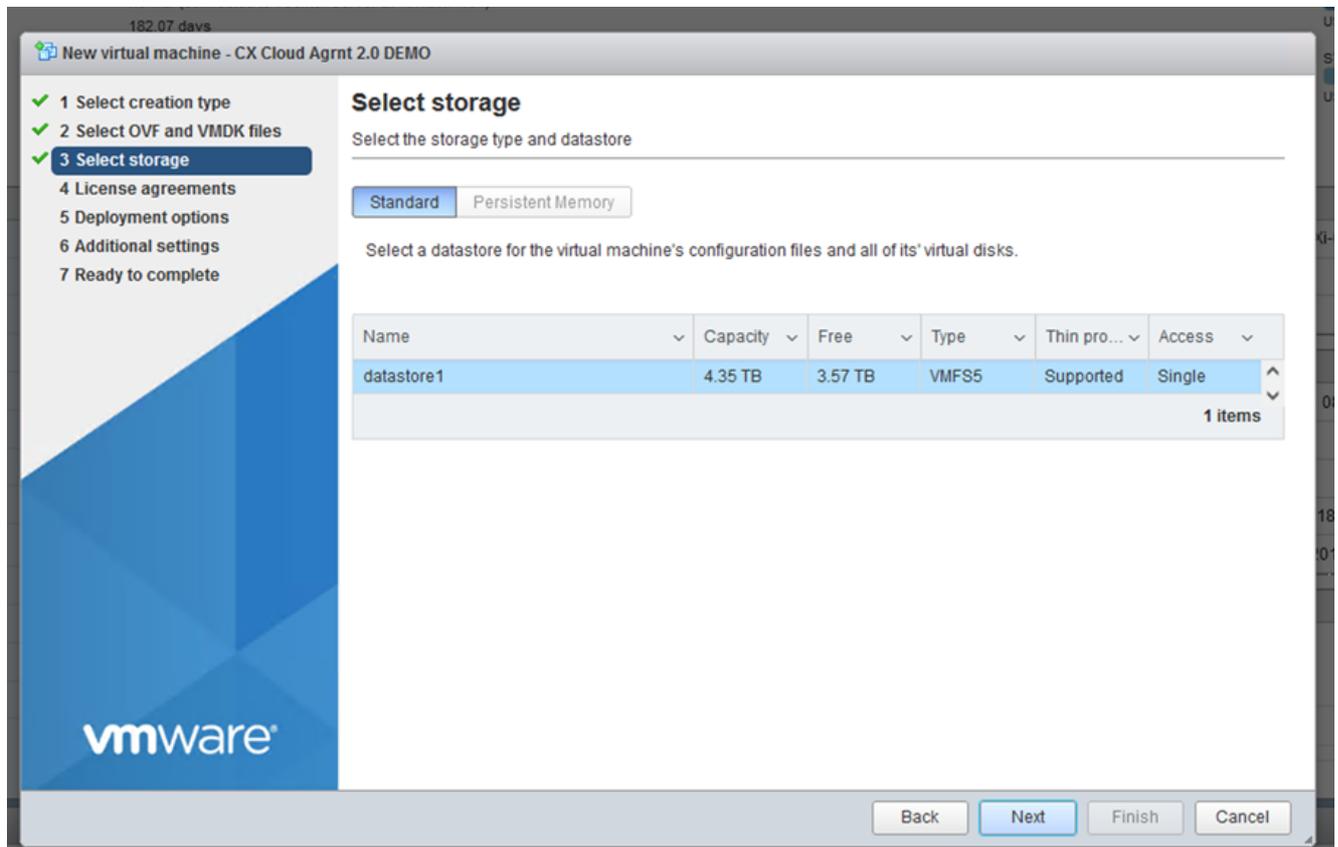
CANCEL

BACK

NEXT

Riesame dei dettagli

9. Selezionare il formato del disco virtuale e fare clic su Next.



Selezione dell'archivio

10. 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

Selezione delle reti

11. 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

Pronto per il completamento

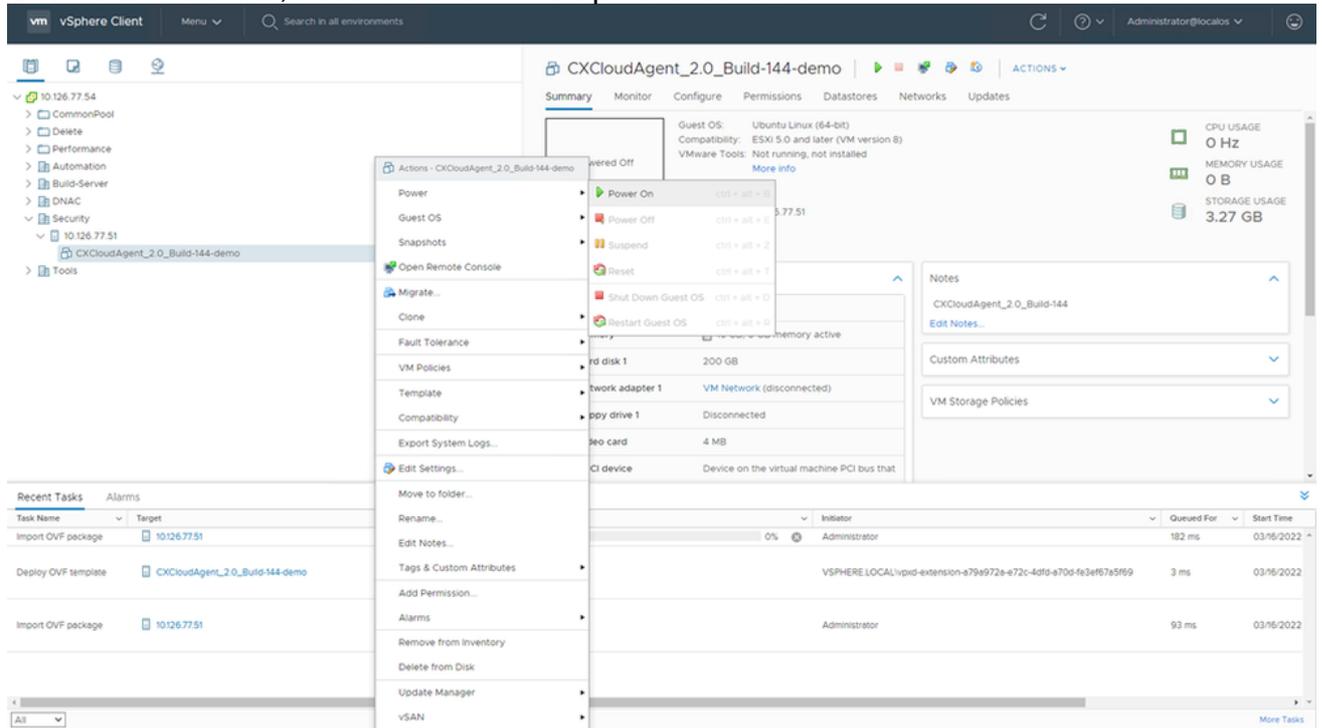
12. Viene aggiunta una nuova VM. Fare clic sul nome per visualizzare lo stato.

The screenshot shows the vSphere Client interface. The left sidebar displays a folder hierarchy 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, 200 GB hard disk, VM Network (disconnected), Floppy drive 1 (Disconnected), Video card (4 MB), 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 aggiunta

13. Una volta installata, accendere la VM e aprire la console.



Apertura della console

14. Andare a [Network Configuration](#) (Configurazione della rete).

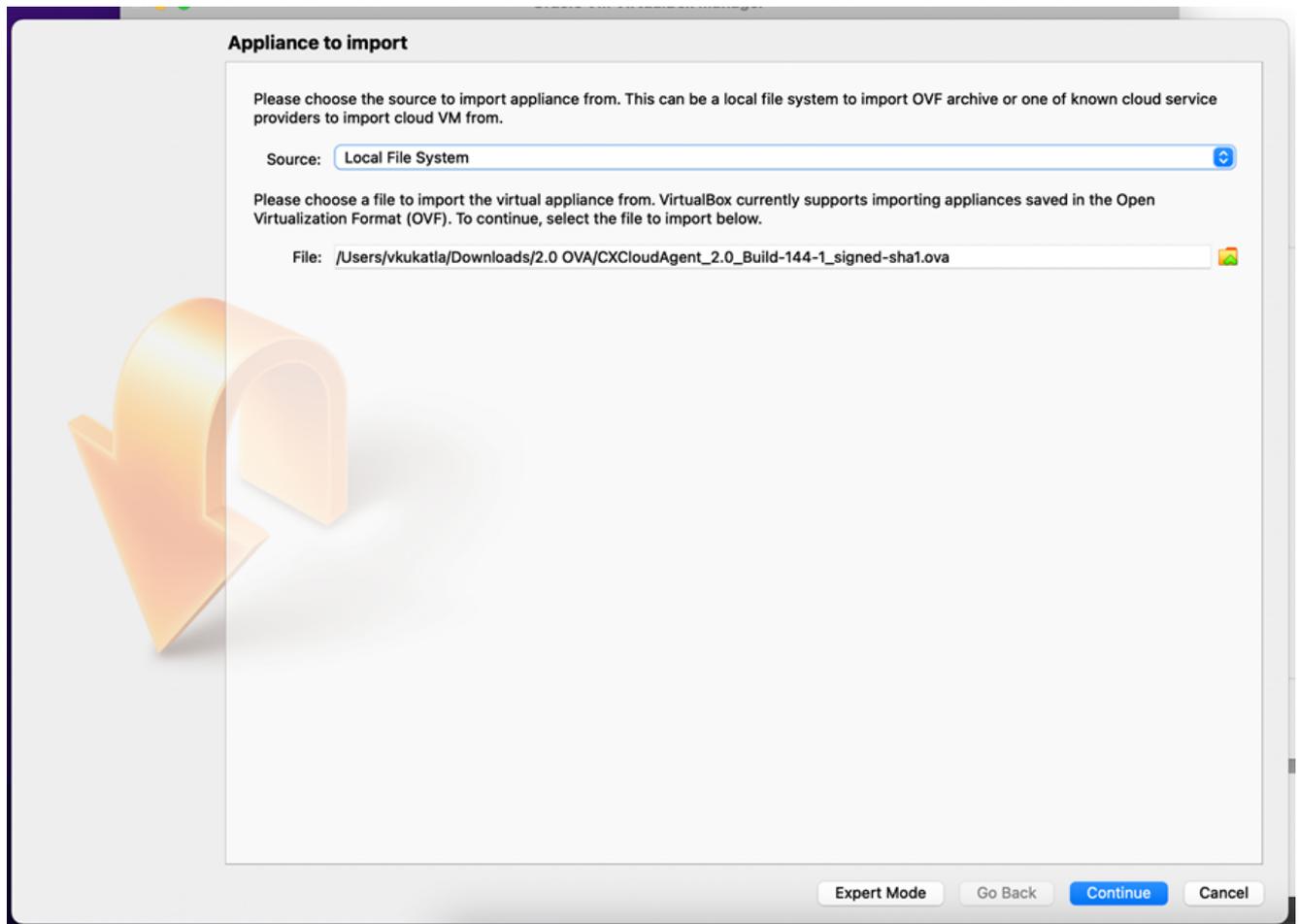
Installazione di Oracle Virtual Box 5.2.30

Questo client distribuisce l'OAV dell'agente cloud CX tramite Oracle Virtual Box.



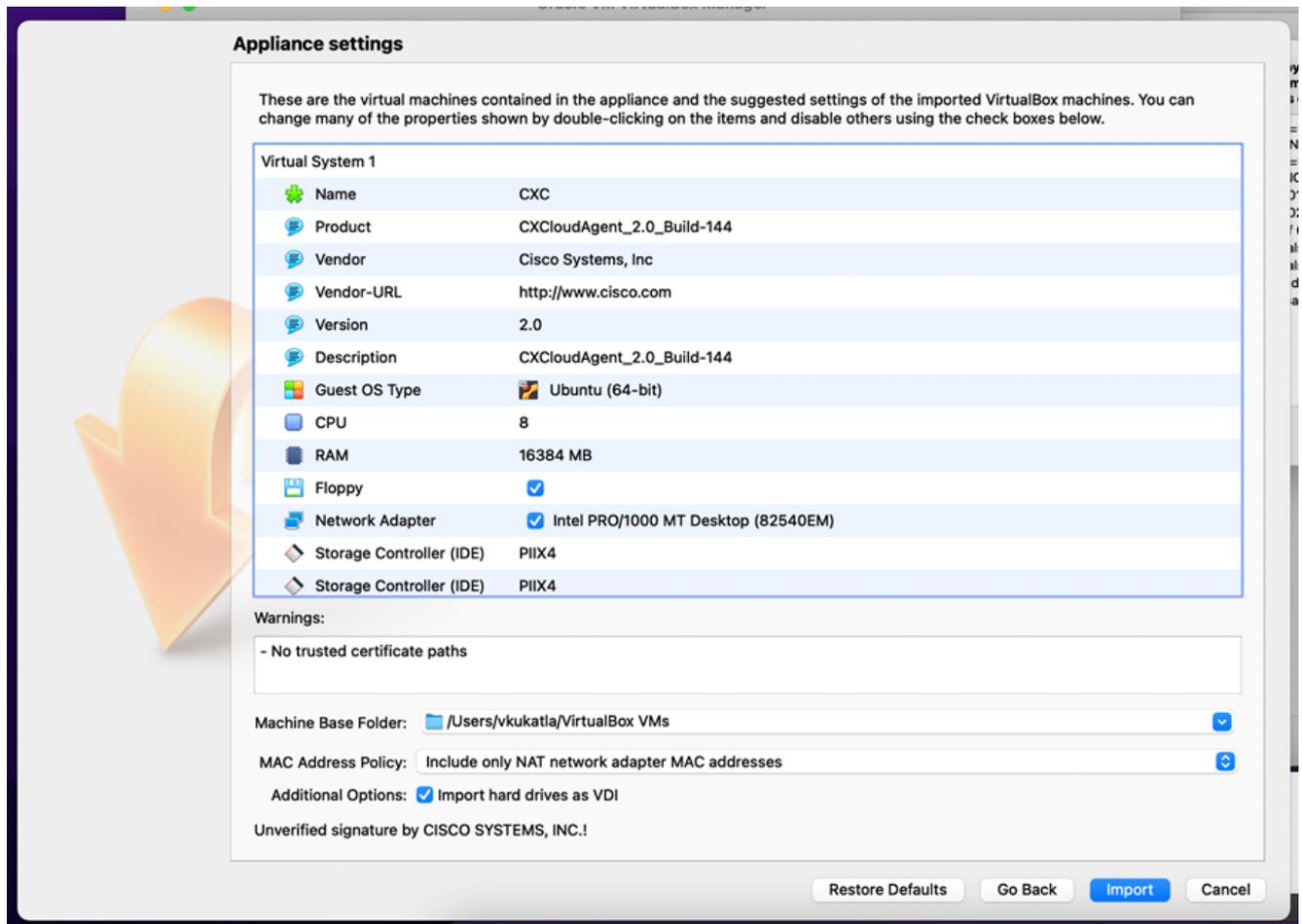
Oracle VM

1. Aprire l'interfaccia utente di Oracle VM e selezionare File > Import Appliance.
2. Individuare il file OVA e importarlo.



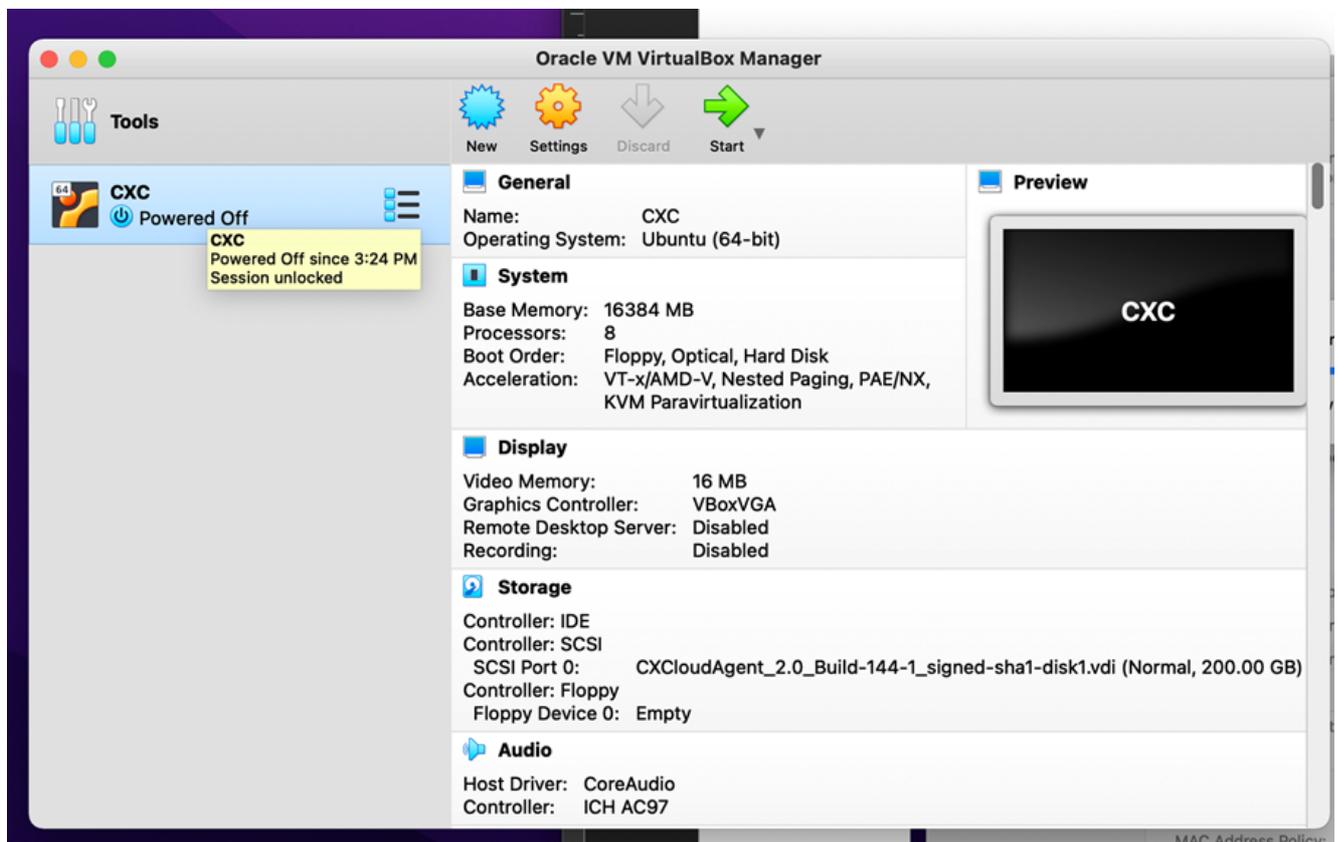
Selezione del file

3. Clic Import.

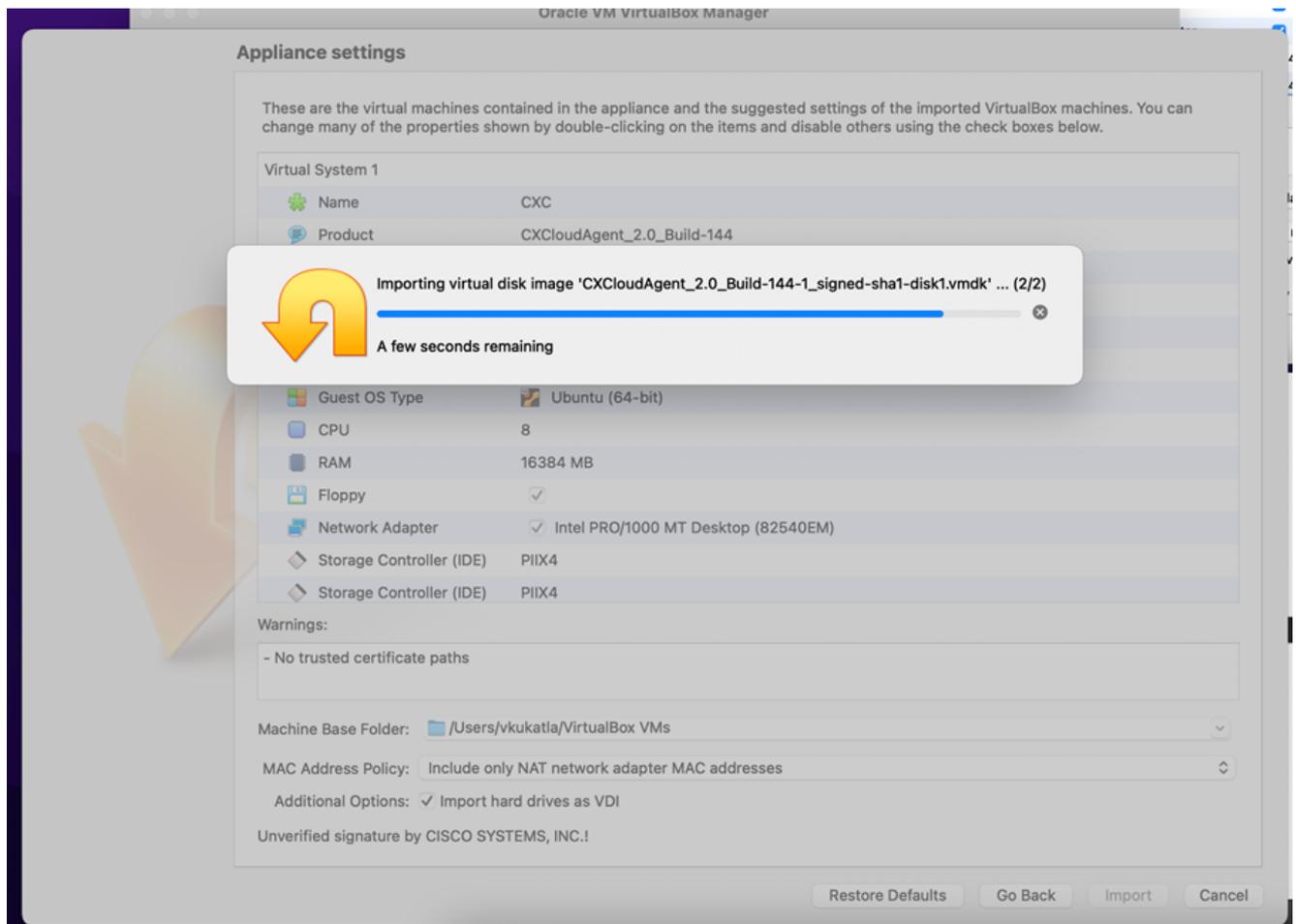


Importazione del file

4. Selezionare la VM appena distribuita e fare clic su Start.

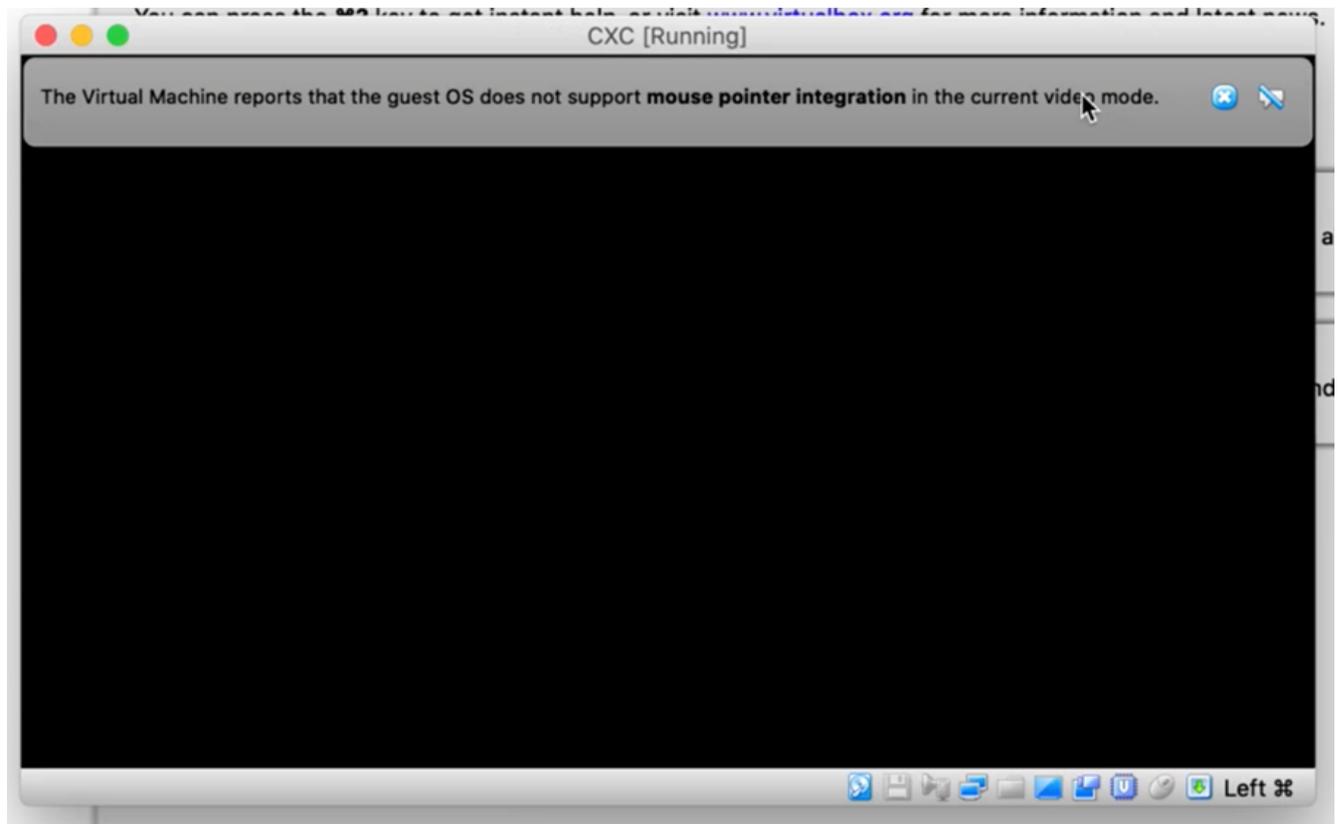


Avvio della console VM



Importazione in corso

5. Accendere la VM. Sulla console viene visualizzato.

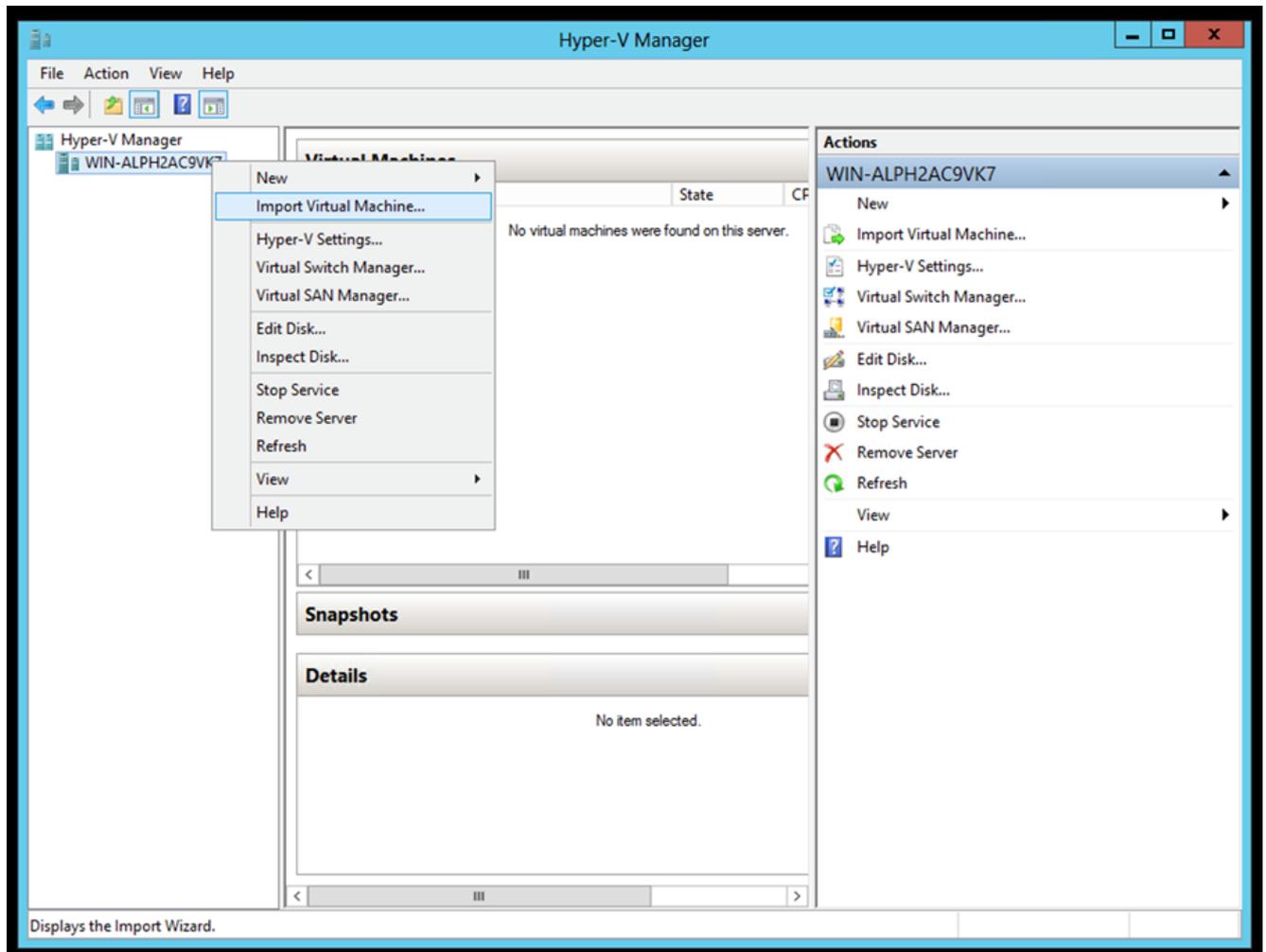


Apertura della console

6. Andare a [Network Configuration](#) (Configurazione della rete).

Installazione di Microsoft Hyper-V

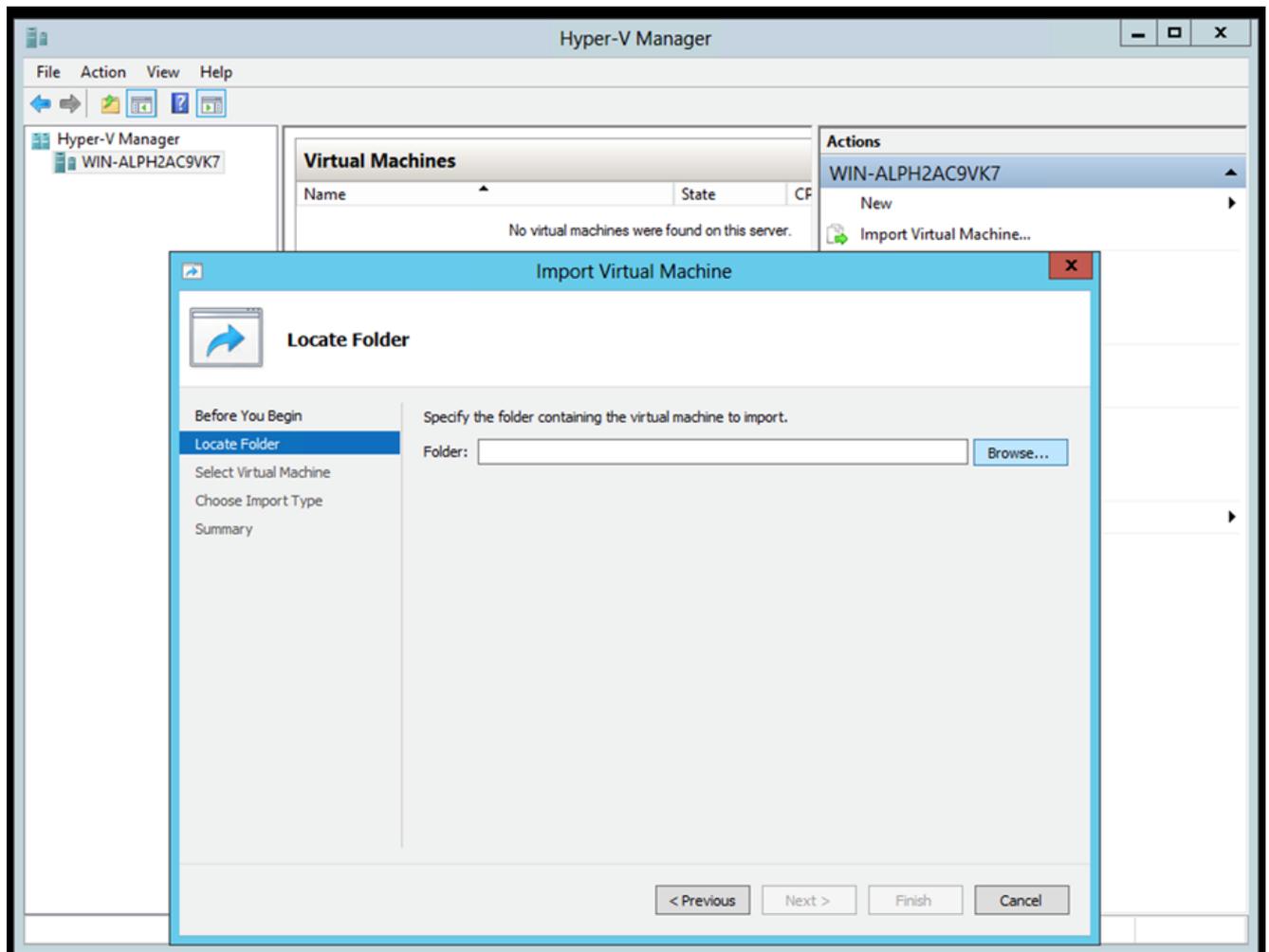
1. Seleziona Import Virtual Machine.



Hyper-V Manager

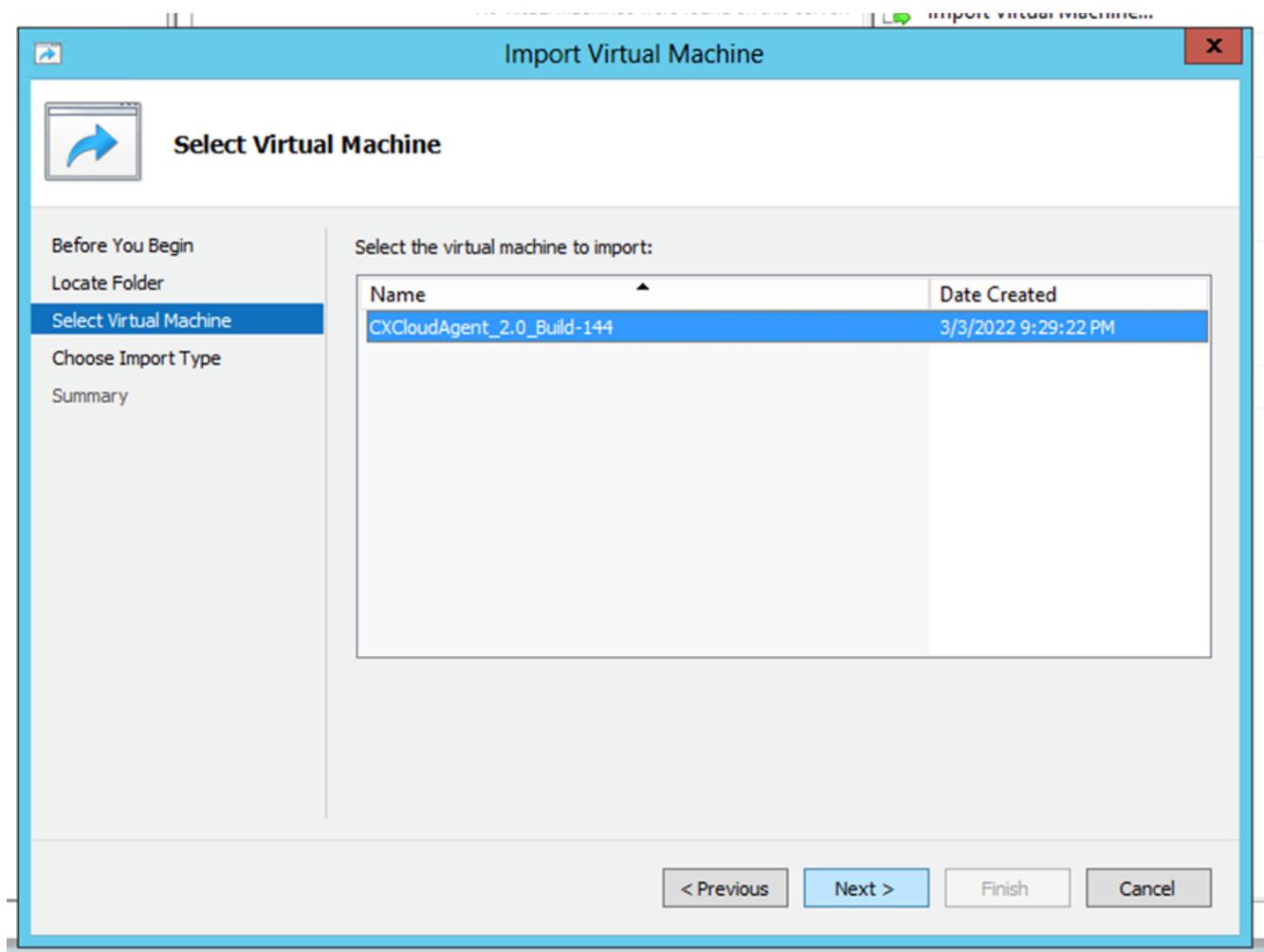
2. Individuare la cartella di download e selezionarla.

3. Clic Next.



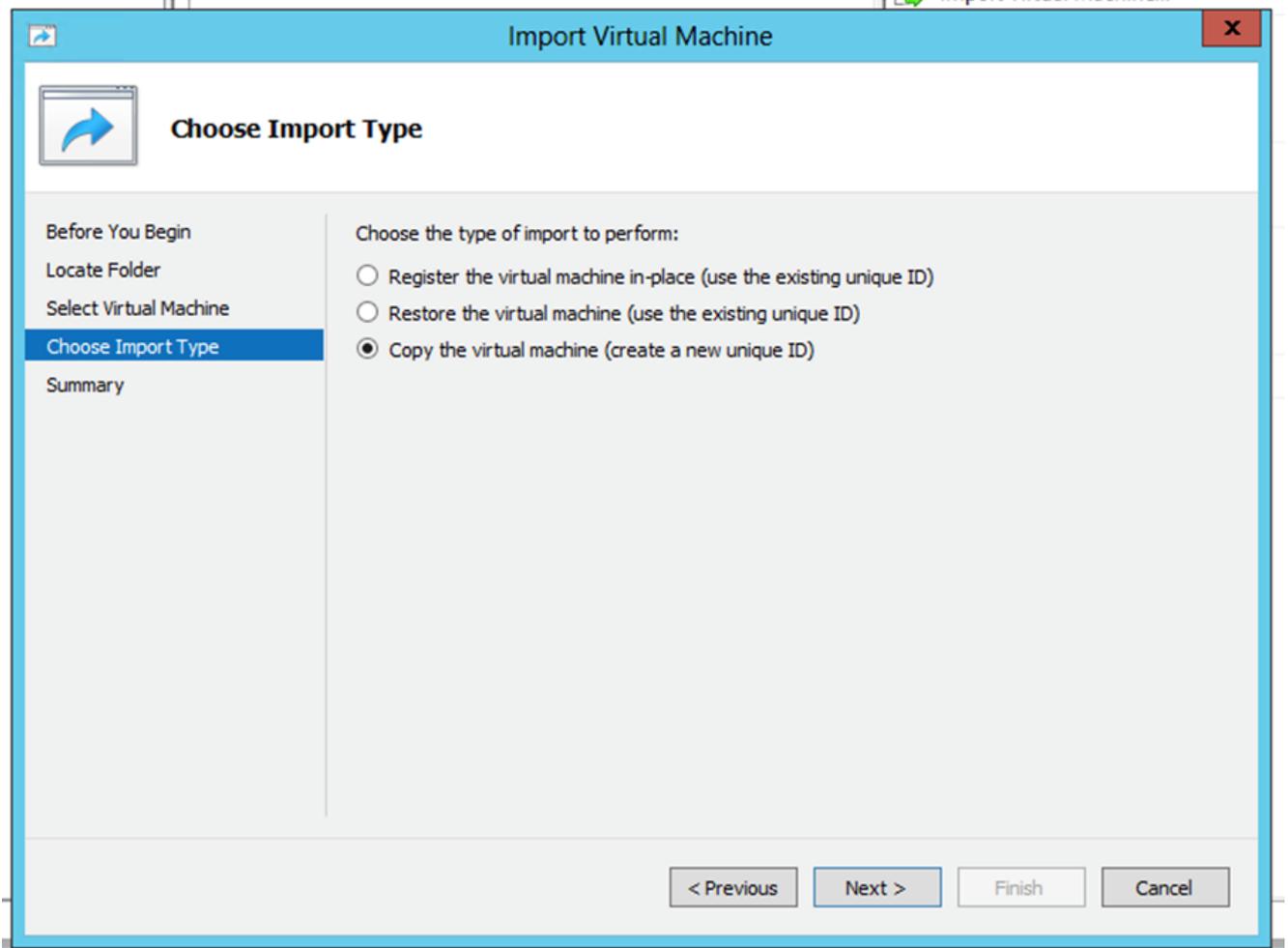
Cartella per l'importazione

4. Selezionare la VM e fare clic su Next.



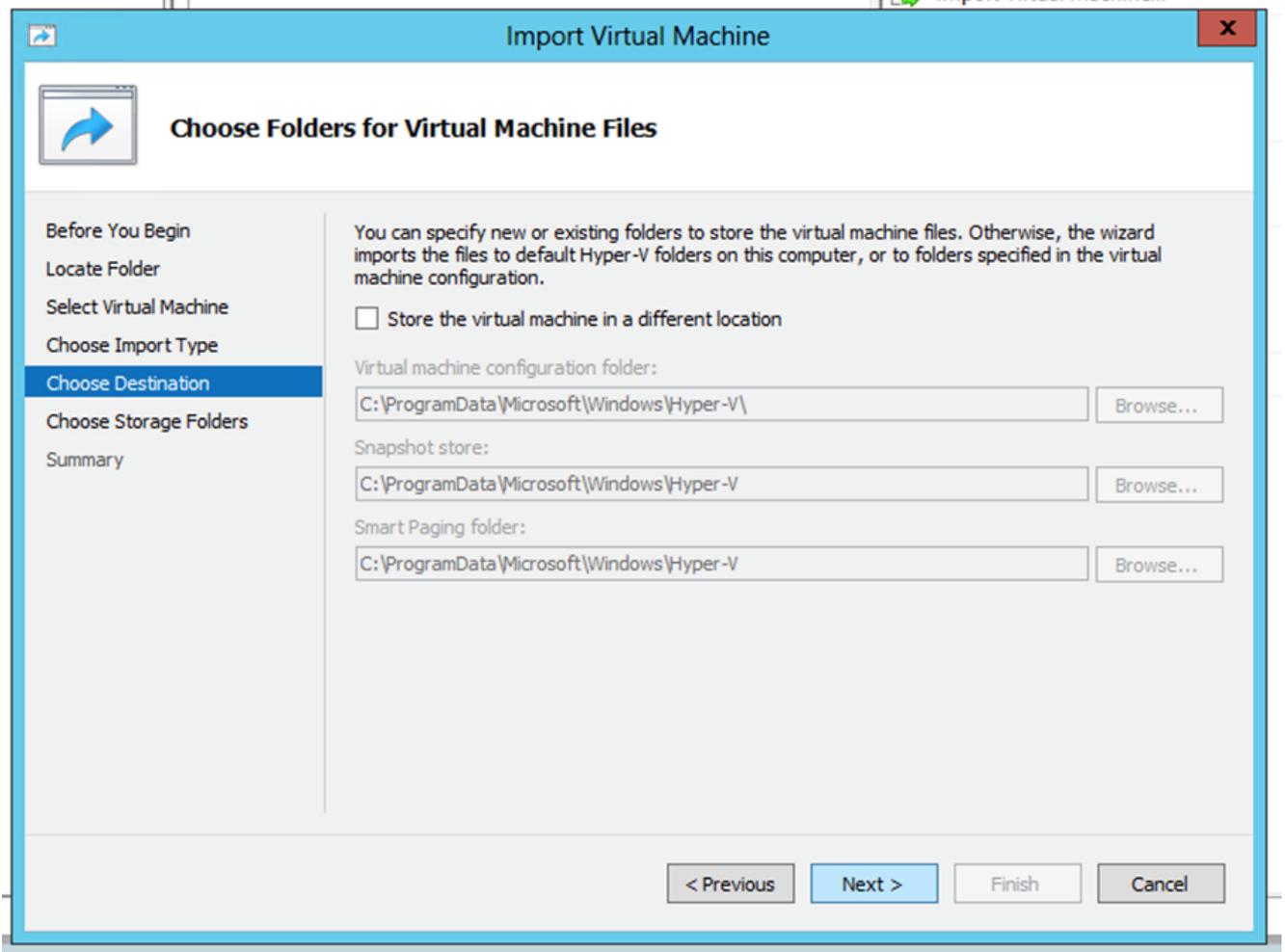
Selezione della VM

5. Selezionare il Copy the virtual machine (create a new unique ID) e fare clic su Next.



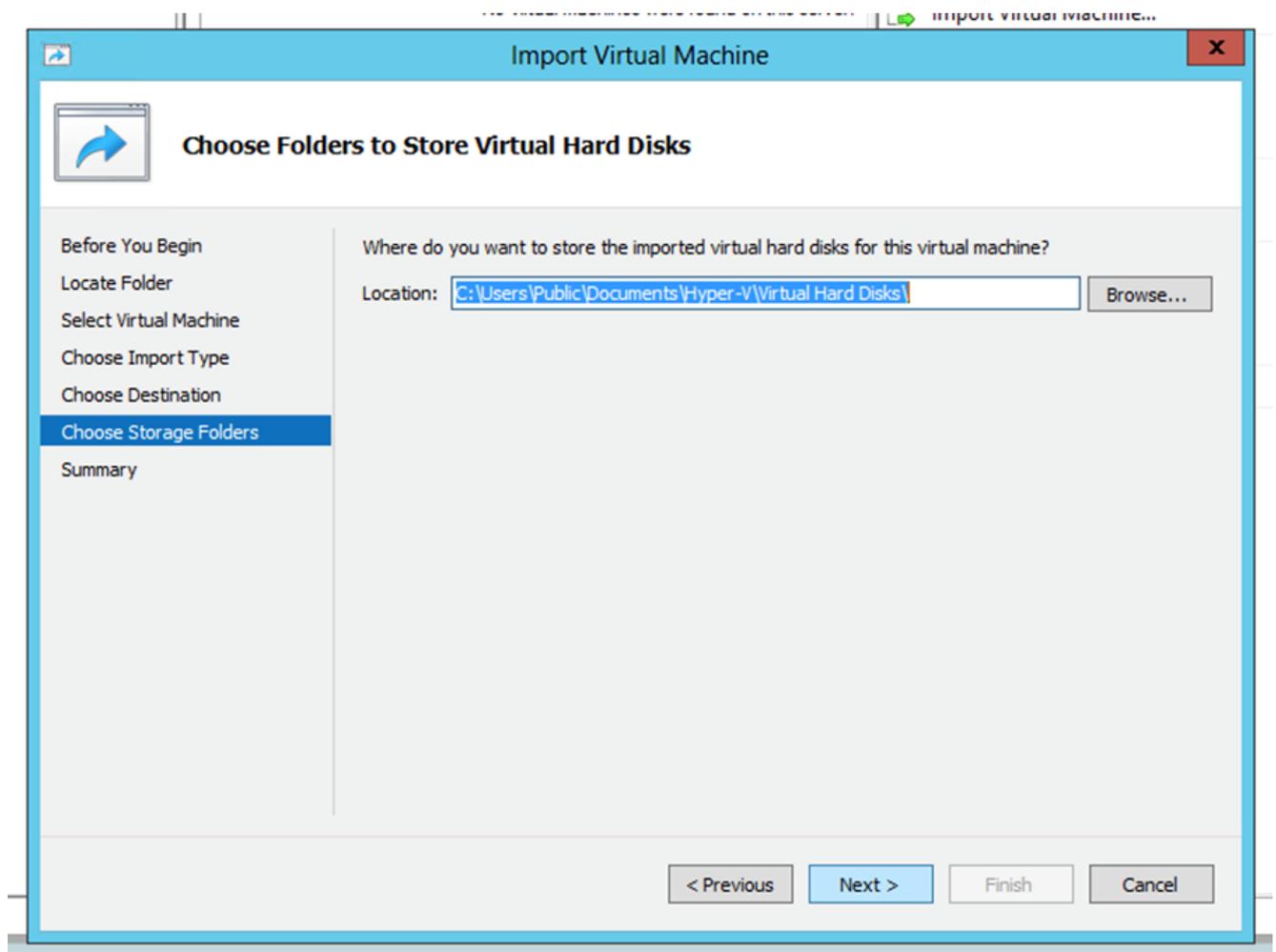
Tipo di importazione

6. Individuare la cartella dei file VM e selezionarla È consigliabile utilizzare percorsi predefiniti.
7. Clic Next.



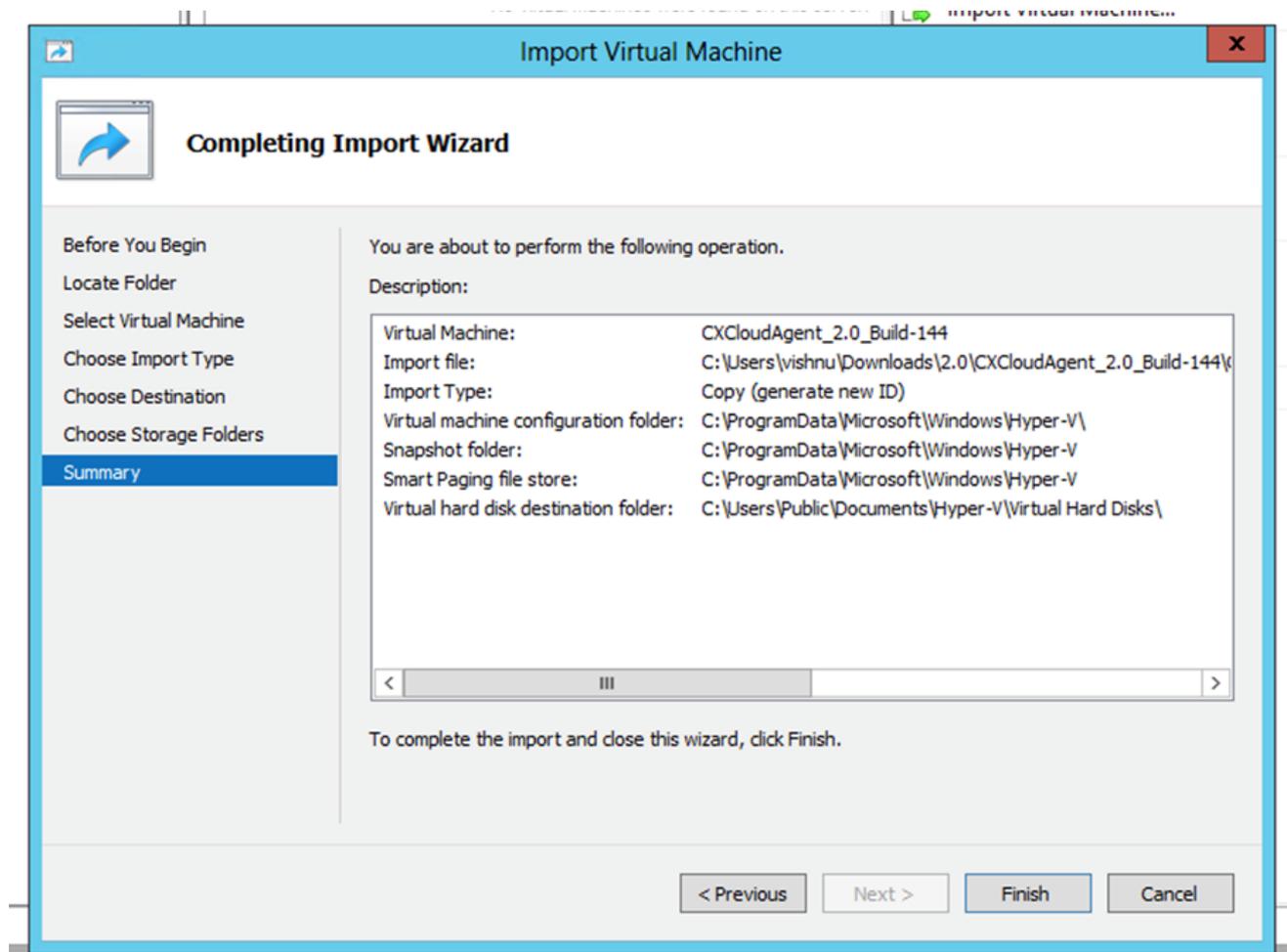
Scegli cartella

8. Individuare la cartella in cui archiviare il disco rigido della VM È consigliabile utilizzare percorsi predefiniti.
9. Clic Next.



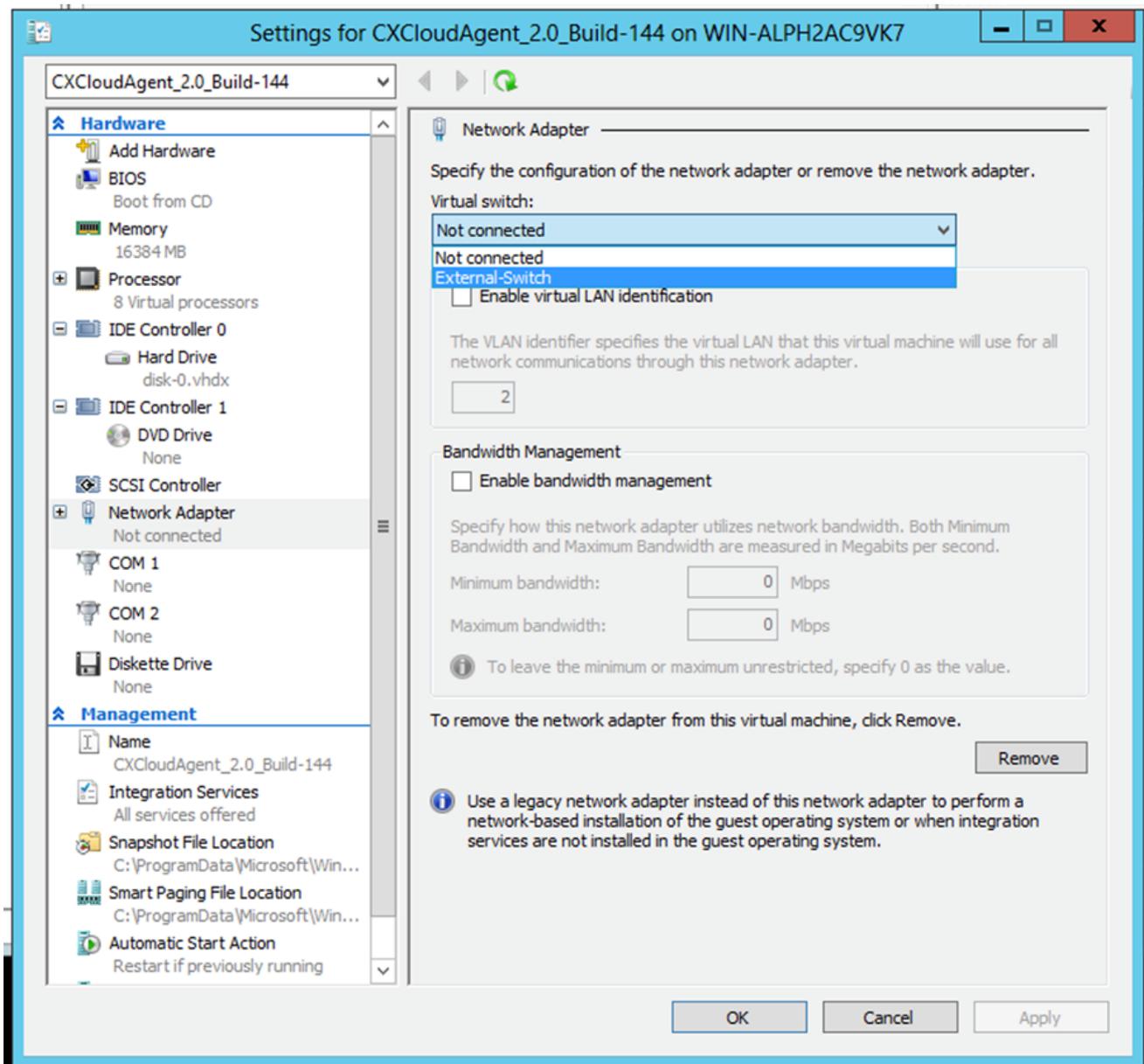
Cartella in cui archiviare i dischi rigidi virtuali

10. Viene visualizzato il riepilogo della VM. Verificare tutti gli input e fare clic su Finish.



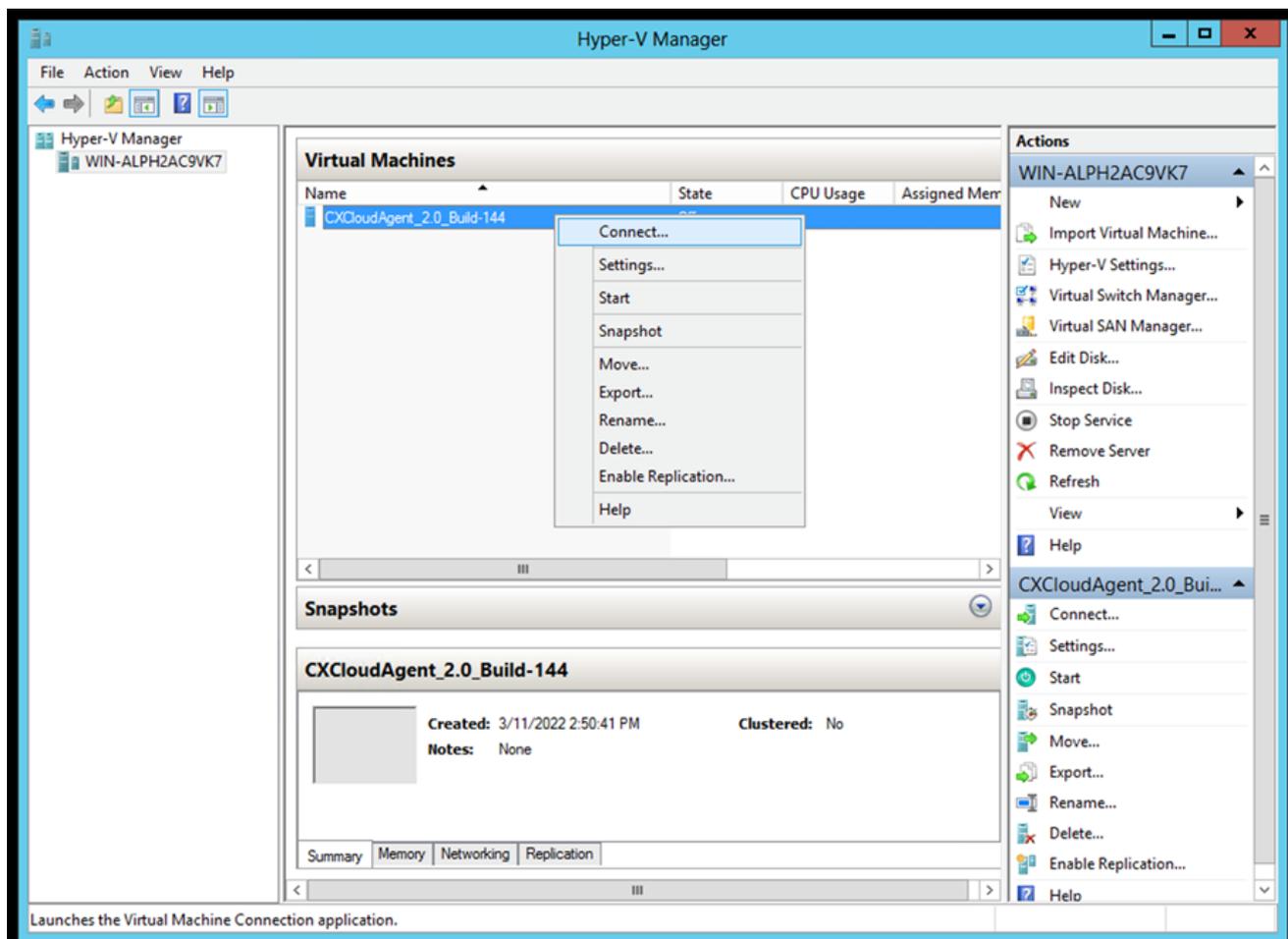
Riepilogo

11. Al termine dell'importazione, viene creata una nuova macchina virtuale in Hyper-V. Aprire l'impostazione della macchina virtuale.
12. Selezionare la scheda di rete nel riquadro sinistro e scegliere la scheda Virtual Switch dall'elenco a discesa.



Switch virtuale

13. Seleziona Connect per avviare la VM.



Avvio della VM

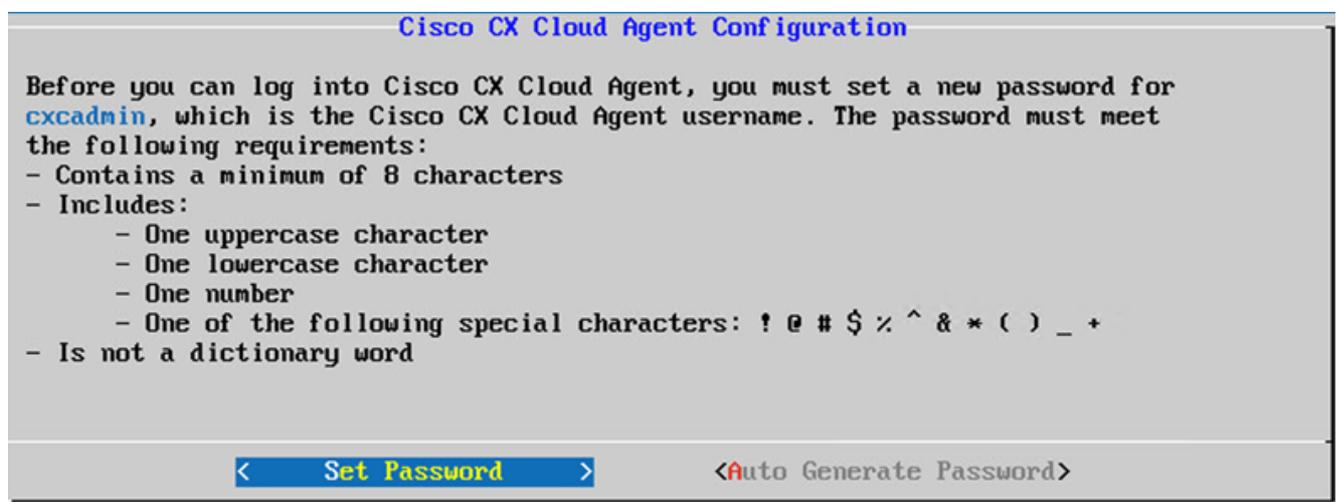
14. Andare a [Network Configuration](#) (Configurazione della rete).

Configurazione della rete



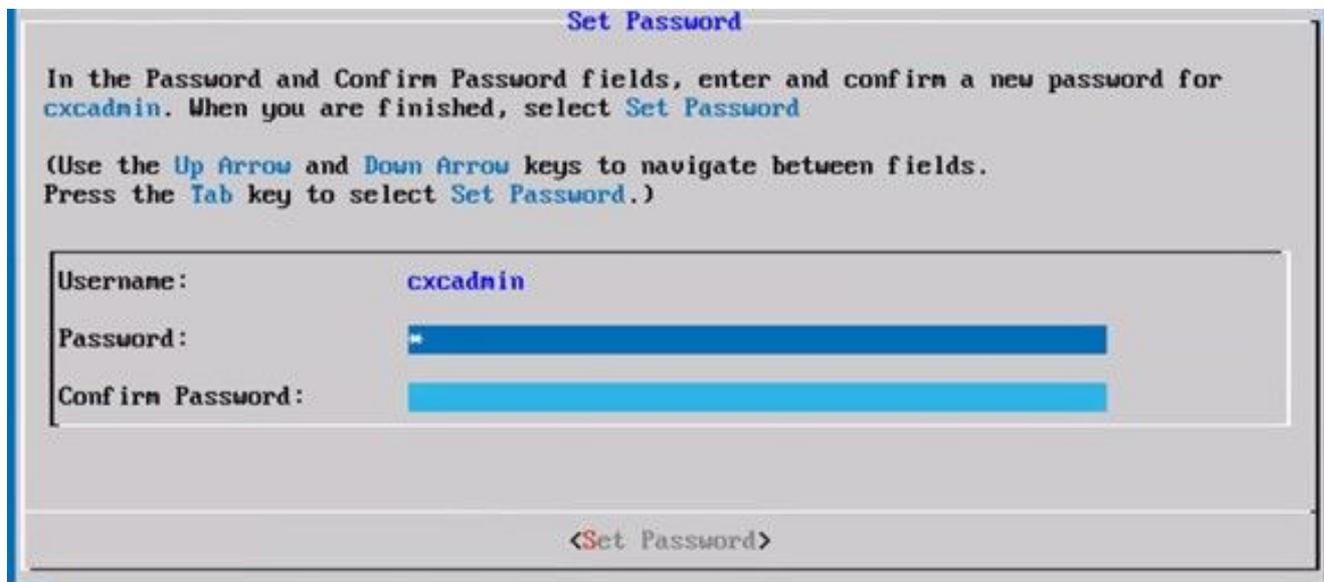
Console VM

1. Clic Set Password per aggiungere una nuova password per cxcadmin OPPURE fare clic su Auto Generate Password per ottenere una nuova password.



Imposta password

2. Se Set Password immettere la password per cxcadmin e confermarla. Clic Set Password e andare al Passaggio 3.



Nuova password

O se Auto Generate Password è selezionata, copiare la password generata e memorizzarla per utilizzarla in futuro. Clic Save Password e andare al Passaggio

4.



Password generata automaticamente

3. Clic Save Password per l'autenticazione.



Salva password

4. Immettere il IP Address, Subnet Mask, Gateway, e DNS Server e fare clic su 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>

Configurazione della rete

5. Confermare le voci e fare clic su 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 >

Conferma

6. Per impostare i dettagli del proxy, fare clic su Yes, Set Up Proxy o fare clic su No, Continue to Configuration per completare la configurazione e andare al passo 8.

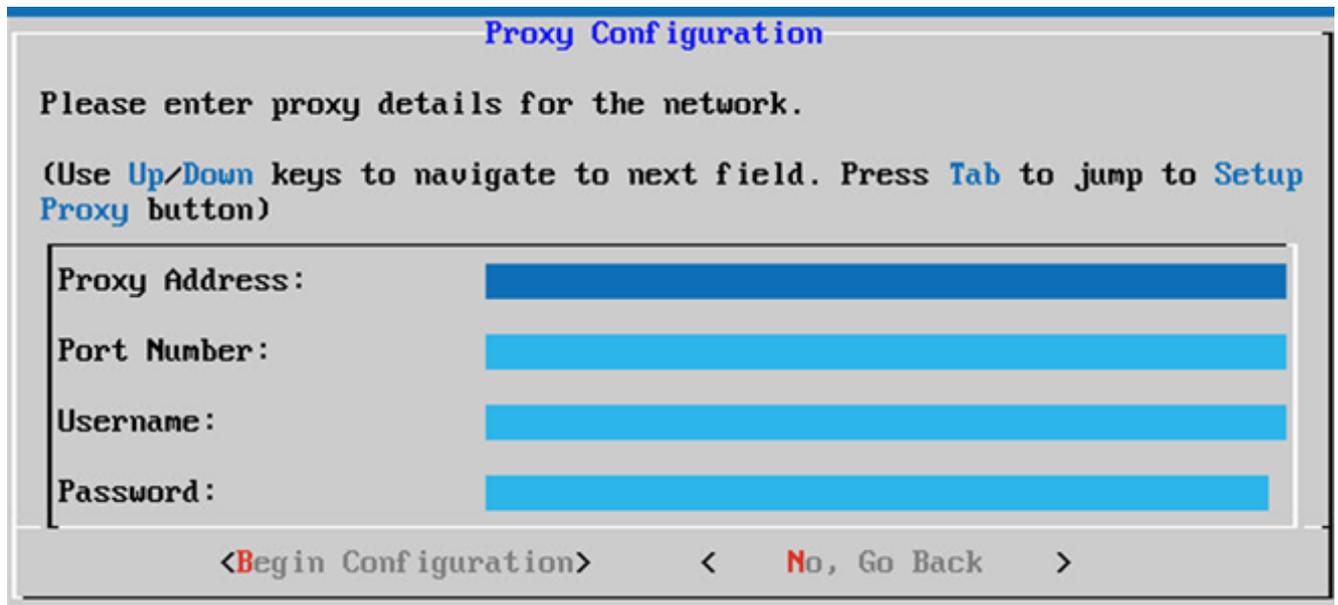
Proxy Set Up Confirmation

Do you want to add proxy details?

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

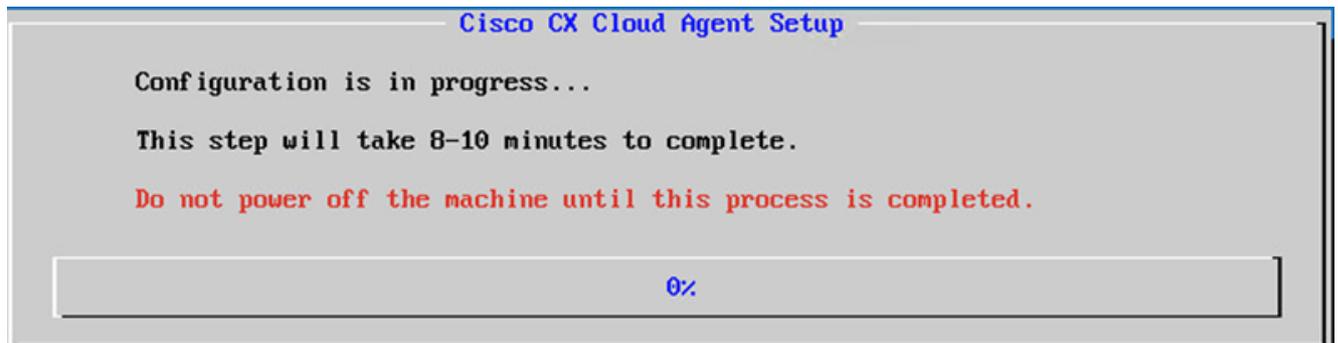
Impostazione del proxy

7. Immettere il Proxy Address, Port Number, Username, e Password.



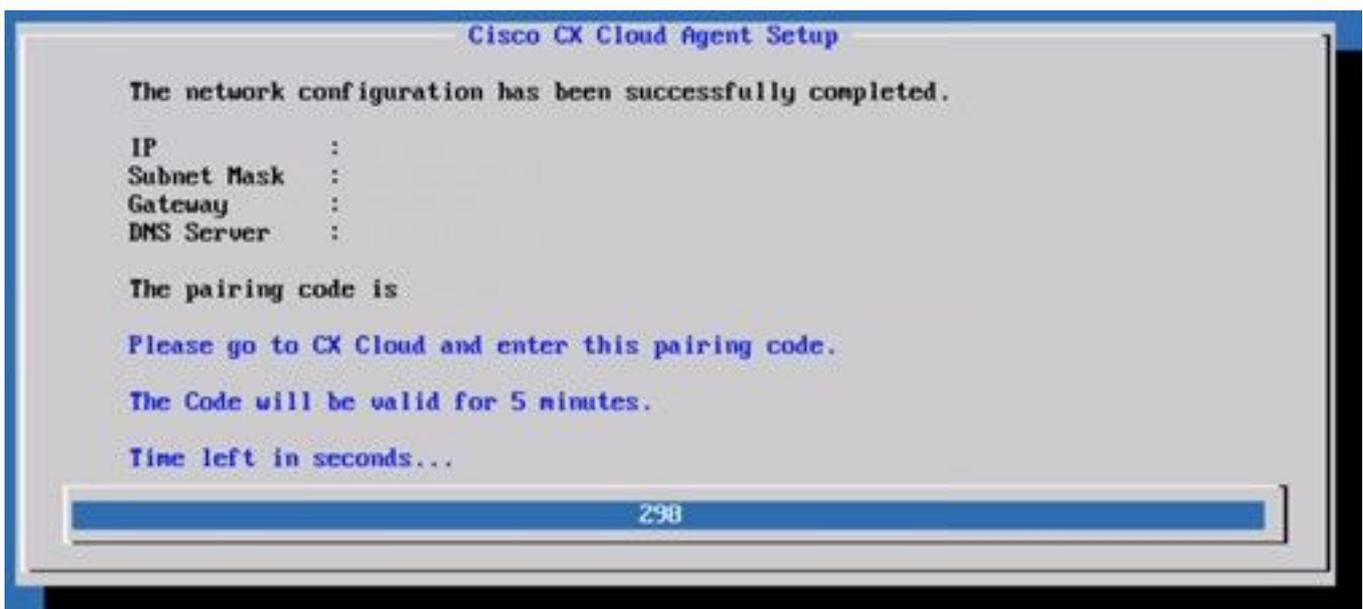
Configurazione del proxy

8. Clic Begin Configuration. Il completamento della configurazione può richiedere alcuni minuti.



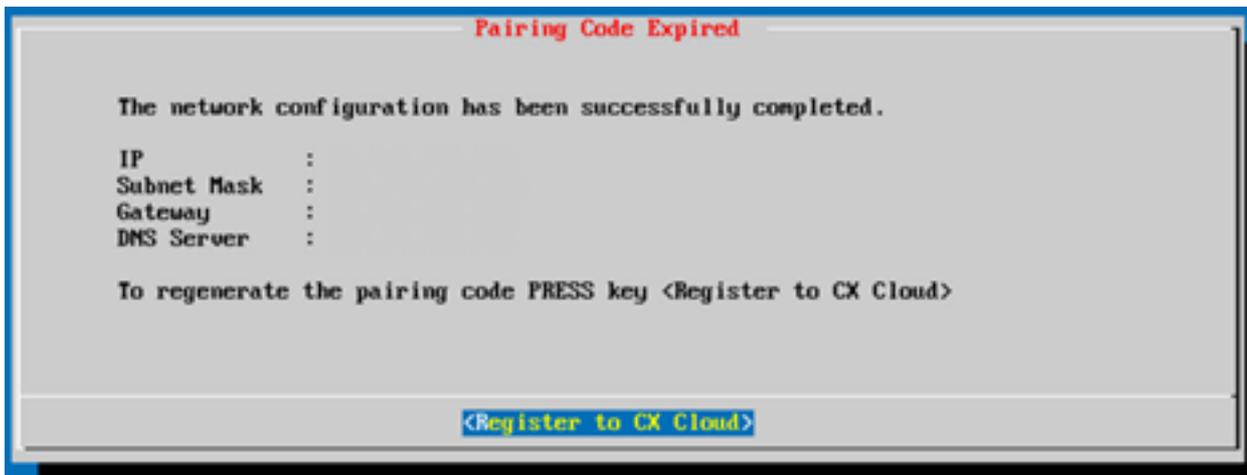
Configurazione in corso

9. Copia Pairing Code e tornare a CX Cloud per continuare l'installazione.



Codice di associazione

10. Se il codice di associazione scade, fare clic su Register to CX Cloud per ottenere nuovamente il codice.



Codice scaduto

11. Fare clic su OK.



Registrazione completata

12. Tornare alla sezione [Connessione dell'agente cloud CX a CX Cloud](#) ed eseguire i passi elencati.

Approccio alternativo per generare il codice di accoppiamento tramite CLI

Gli utenti possono anche generare un codice di associazione utilizzando le opzioni CLI.

Per generare un codice di associazione tramite CLI:

1. Accedere all'agente cloud tramite SSH utilizzando le credenziali utente cxcadmin.
2. Generare il codice di associazione con il 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:~$
```

Generazione del codice di associazione dalla CLI

3. Copia Pairing Code e tornare a CX Cloud per continuare l'installazione. Per ulteriori informazioni, fare riferimento a Connessione al portale clienti.

Configurazione di Cisco DNA Center per l'inoltro del syslog all'agente cloud CX

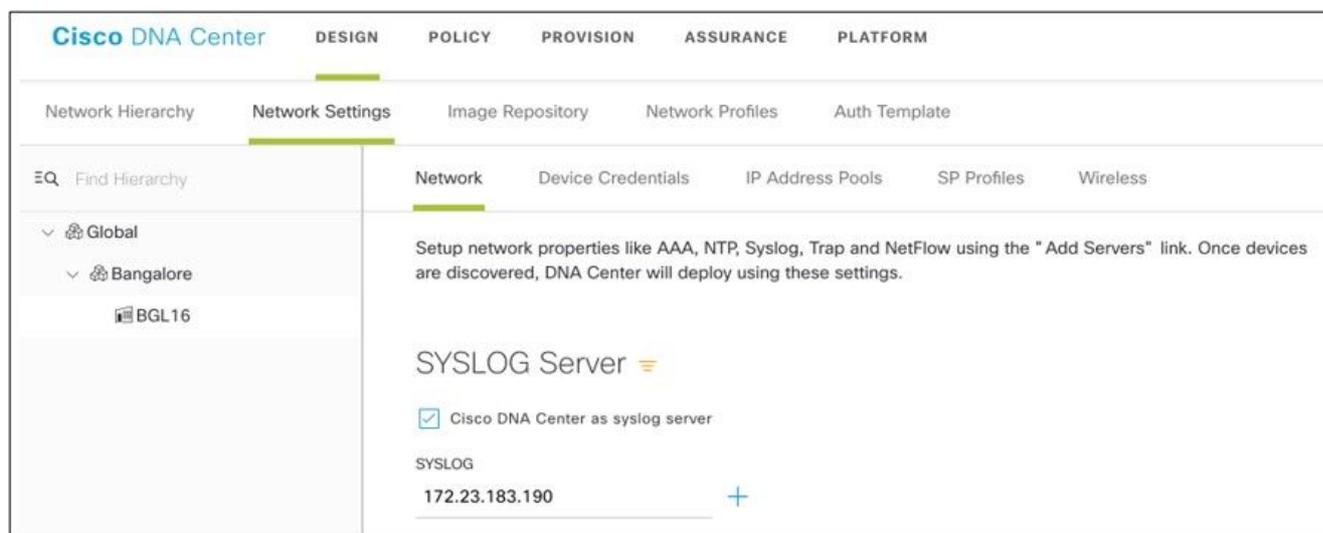
Prerequisito

Le versioni supportate di Cisco DNA Center sono dalla 1.2.8 alla 1.3.3.9 e dalla 2.1.2.0 alla 2.2.3.5.

Configurazione dell'inoltro di syslog

Per configurare l'inoltro Syslog all'agente cloud CX in Cisco DNA Center tramite l'interfaccia utente, attenersi alla seguente procedura:

1. Avviare Cisco DNA Center.
2. Vai a Design > Network Settings > Network.
3. Per ciascuna sede, aggiungere l'IP di CX Cloud Agent come server Syslog.



Server Syslog

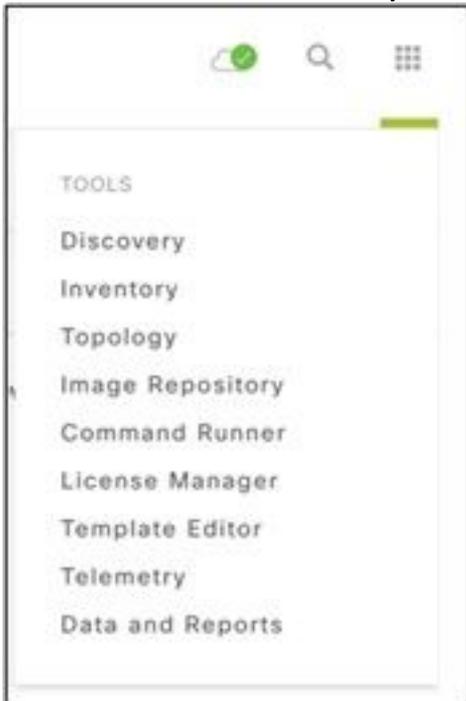
Note:

- Una volta configurati, tutti i dispositivi associati al sito sono configurati per inviare syslog con il livello critico all'agente cloud CX.
- I dispositivi devono essere associati a un sito per abilitare l'inoltro syslog dal dispositivo all'agente cloud CX.
- Quando si aggiorna l'impostazione di un server syslog, tutti i dispositivi associati al sito vengono automaticamente impostati sul livello critico predefinito.

Abilita impostazioni syslog livello informazioni

Per rendere visibile il livello Informazioni syslog, effettuare le seguenti operazioni:

1. Passa a Tools > Telemetry.



Menu Strumenti

2. Selezionare ed espandere la Site View e selezionare un sito dalla gerarchia dei siti.



Vista della sede

3. Selezionare il sito richiesto e selezionare tutti i dispositivi che utilizzano Device name casella di controllo.

4. A decorrere dal Actions a discesa, selezionare Optimal Visibility.



Azioni

Sicurezza

CX Cloud Agent garantisce al cliente la sicurezza completa. La connessione tra CX Cloud e CX Cloud Agent è crittografata. SSH (Secure Socket Shell) di CX Cloud Agent supporta 11 cifrari diversi.

Sicurezza fisica

Distribuire l'immagine OAV dell'agente cloud CX in un'azienda server VMware protetta. L'OVA viene condivisa in modo sicuro dal centro di download del software Cisco. Per il bootloader (modalità utente singolo) viene impostata una password univoca scelta casualmente. Gli utenti devono fare riferimento alle [Domande frequenti \(FAQ\)](#) per impostare la password del bootloader (modalità utente singolo).

Accesso utente

Gli utenti di CX Cloud possono solo ottenere l'autenticazione e accedere alle API Cloud Agent.

Sicurezza dell'account

Al momento della distribuzione, viene creato l'account utente cxcadmin. Gli utenti sono obbligati a impostare una password durante la configurazione iniziale. Le credenziali di cxcadmin vengono utilizzate per accedere alle API di CX Cloud Agent e per connettere l'appliance tramite SSH.

L'utente cxcadmin ha limitato l'accesso con i privilegi minimi. La password cxcadmin segue i criteri di protezione ed è sottoposta a hash unidirezionale con un periodo di scadenza di 90 giorni. L'utente cxcadmin può creare un utente cxcroot utilizzando l'utilità denominata remoteaccount. L'utente cxcroot può ottenere i privilegi root. La passphrase scade tra due giorni.

Sicurezza della rete

È possibile accedere alla VM dell'agente cloud CX utilizzando ssh con le credenziali utente cxcadmin. Le porte in arrivo sono limitate a 22 (SSH), 514 (Syslog).

Autenticazione

Autenticazione basata sulla password: l'appliance gestisce un solo utente, "cxcadmin", che permette di autenticarsi e comunicare con CX Cloud Agent.

- Azioni eseguibili sull'appliance con privilegi root tramite SSH l'utente cxcadmin può creare un utente cxcroot utilizzando un'utilità denominata remoteaccount. Questa utility visualizza una password crittografata RSA/ECB/PKCS1v1_5 che può essere decrittografata solo dal portale SWIM (<https://swims.cisco.com/abraxas/decrypt>). Solo il personale autorizzato può accedere al portale. L'utente cxcroot può ottenere privilegi root utilizzando la password decrittata. La passphrase è valida solo due giorni. Una volta scaduta, l'utente cxcadmin deve ricreare l'account e richiedere nuovamente la password sul portale SWIM.

Protezione avanzata

L'appliance CX Cloud Agent rispetta gli standard di protezione avanzata CIS.

Sicurezza dei dati

L'appliance CX Cloud Agent non memorizza le informazioni personali dei clienti.

L'applicazione di gestione delle credenziali del dispositivo (eseguita come uno dei pod) memorizza le credenziali criptate del server Cisco DNA Center in un database protetto. I dati raccolti da Cisco DNA Center non vengono memorizzati in alcun modo nell'appliance. I dati raccolti vengono caricati sul backend subito dopo il completamento della raccolta e vengono eliminati dall'agente.

Trasmissione dati

Il pacchetto di registrazione contiene il codice univoco richiesto [X.509](#) certificato e chiavi del dispositivo per stabilire una connessione sicura con IoT Core. L'utilizzo di tale agente consente di stabilire una connessione protetta tramite MQTT su TLS v1.2

Log e monitoraggio

I log non contengono alcun tipo di informazioni sensibili. I registri di verifica acquisiscono tutte le azioni relative alla sicurezza eseguite sull'appliance CX Cloud Agent.

Riepilogo delle funzionalità di sicurezza

Funzionalità di sicurezza	Descrizione
Password del bootloader	Per il bootloader (modalità utente singolo) viene impostata una password univoca scelta casualmente. Consultare le Domande frequenti (FAQ) per impostare la password del bootloader (modalità utente singolo).
Accesso utente	SSH: <ul style="list-style-type: none"> • Per accedere all'appliance con l'utente cxcadmin, occorre utilizzare le credenziali create durante l'installazione. • L'accesso all'accessorio tramite l'utente cxcroot richiede la decrittografia delle credenziali tramite il portale SWIM da parte di personale autorizzato. • cxcadmin: l'account utente predefinito che viene creato. L'utente può eseguire i comandi dell'applicazione CX Cloud Agent utilizzando cxcli e ha privilegi minimi sull'appliance.
Account utente	L'utente cxcroot e la relativa password criptata vengono generati utilizzando l'utente cxcadmin. <ul style="list-style-type: none"> • cxcroot: un utente che può essere creato da cxcadmin utilizzando l'utility "remoteaccount".

Policy della password di cxcadmin	<p>Con questo account, l'utente può ottenere privilegi root.</p> <ul style="list-style-type: none"> • La password ha un hash unidirezionale che utilizza SHA-256 e viene memorizzata in modo sicuro. • Un minimo di otto (8) caratteri, che contiene tre di queste categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali. • La password di cxcroot è RSA/ECB/PKCS1v1_5 ed è criptata. • La passphrase generata deve essere decriptata nel portale SWIM. • L'utente e la password cxcroot sono validi per massimo due giorni e possono essere rigenerati utilizzando l'utente cxcadmin.
Policy della password cxcroot	<ul style="list-style-type: none"> • La passphrase generata deve essere decriptata nel portale SWIM. • L'utente e la password cxcroot sono validi per massimo due giorni e possono essere rigenerati utilizzando l'utente cxcadmin.
Policy della password di accesso tramite SSH	<ul style="list-style-type: none"> • Un minimo di otto (8) caratteri, che contiene tre di queste categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali. • 5 tentativi di accesso non riusciti bloccheranno la scatola per 30 minuti. La validità della password è 90 giorni.
Porte	Porte in ingresso aperte - 514 (Syslog) e 22 (SSH)
Sicurezza dei dati	<p>Nessuna informazione dei clienti viene memorizzata.</p> <p>Nessun dato dei dispositivi viene memorizzato.</p> <p>Le credenziali del server Cisco DNA Center sono criptate e memorizzate nel database.</p>

Domande frequenti

CX Cloud Agent

Implementazione

D: L'opzione "Reinstalla" permette di implementare il nuovo Cloud Agent con il nuovo indirizzo IP?

R: Sì

D - Quali sono i formati di file disponibili per l'installazione?

R: OVA e VHD

D: Qual è l'ambiente in cui è possibile implementare l'installazione?

R: OVA

VMware ESXi versione 5.5 o successiva

Oracle Virtual Box 5.2.30 o successivo

VHD

Windows Hypervisor da 2012 a 2016

D: CX Cloud Agent può rilevare l'indirizzo IP in un ambiente DHCP?

R: Sì, in un ambiente DHCP, l'indirizzo IP viene assegnato durante la configurazione IP. Tuttavia, tale ambiente non supporta modifiche future dell'indirizzo IP per CX Cloud Agent. Inoltre, si consiglia di prenotare l'IP del Cloud Agent nel proprio ambiente DHCP.

D: CX Cloud Agent supporta entrambe le configurazioni IPv4 e IPv6?

R: No, è supportata solo la configurazione IPV4.

D: Durante la configurazione IP, l'indirizzo IP viene convalidato?

R: Sì, la sintassi dell'indirizzo IP e l'assegnazione dell'indirizzo IP duplicato vengono convalidate.

D: Qual è il tempo approssimativo impiegato per l'implementazione dell'OVA e la configurazione IP?

R: L'implementazione dell'OVA dipende dalla velocità con cui la rete copia i dati. La configurazione IP richiede circa 8-10 minuti e include la creazione di Kubernetes e container.

D: Sono previste limitazioni per qualche tipo di hardware?

A - Il computer host su cui è installato OVA deve soddisfare i requisiti forniti nell'ambito della configurazione del portale CX. L'agente cloud CX viene testato con VMware/Virtual box in esecuzione su un hardware con processori Intel Xeon E5 con rapporto vCPU/CPU impostato su 2:1. Se si utilizza una CPU con minore potenza o un rapporto maggiore, le prestazioni possono peggiorare.

D: È possibile generare il codice di associazione in qualsiasi momento?

R: No, il codice di associazione può essere generato solo se Cloud Agent non è registrato.

D - Quali sono i requisiti di larghezza di banda tra i DNAC (fino a 10 cluster o 20 non cluster) e l'agente?

A - La larghezza di banda non è un vincolo quando l'agente e DNAC si trovano nella stessa rete LAN/WAN nell'ambiente del cliente. La larghezza di banda minima richiesta è 2,7 Mbit/sec per le raccolte di inventario di 5000 dispositivi +13000 Access Point per una connessione da agente a DNAC. Se vengono raccolti i syslog per I2 insights, la larghezza di banda minima richiesta è di 3,5 Mbit/sec per le coperture di 5000 dispositivi +13000 Access Point per l'inventario, 5000 dispositivi syslog e 2000 dispositivi per le scansioni, il tutto eseguito in parallelo dall'agente.

Release e patch

D: Quali sono i diversi tipi di versioni disponibili per l'aggiornamento di CX Cloud Agent?

A - Di seguito sono elencate le versioni rilasciate di CX Cloud Agent:

- A.x.0 (dove x è l'ultima versione della principale funzionalità di produzione, ad esempio, 1.3.0)
- A.x.y (dove A.x.0 è obbligatorio e deve essere avviato l'aggiornamento incrementale, x è l'ultima versione delle funzionalità principali di produzione e y è l'ultima patch di aggiornamento disponibile, ad esempio: 1.3.1).
- A.x.y-z (dove A.x.0 è obbligatorio e deve essere avviato l'aggiornamento incrementale, x è l'ultima versione delle funzionalità principali di produzione e y è l'ultima patch di aggiornamento disponibile e z è la patch spot che è una correzione immediata per un periodo di tempo molto breve, ad esempio: 1.3.1-1)

dove A è una release a lungo termine distribuita su un periodo di 3-5 anni.

D - Dove trovare l'ultima versione rilasciata di CX Cloud Agent e come aggiornare l'agente CX Cloud esistente?

A - Vai a Admin Settings > Data Sources. Fare clic sul pulsante View Update ed eseguire le istruzioni visualizzate sullo schermo.

Autenticazione e configurazione del proxy

D: Qual è l'utente predefinito dell'applicazione CX Cloud Agent?

R: cxcadmin

D - Come viene impostata la password per l'utente predefinito?

R: La password è impostata durante la configurazione della rete.

D: È disponibile un'opzione per reimpostare la password dopo il giorno 0?

R: L'agente non fornisce alcuna opzione specifica per reimpostare la password, ma è possibile utilizzare i comandi Linux per reimpostare la password di cxcadmin.

D: Quali sono le policy delle password per configurare CX Cloud Agent?

R: Le policy delle password sono:

- Durata massima della password impostata a 90 giorni.
- Durata minima della password impostata a 8.
- Lunghezza massima della password 127 caratteri.
- È necessario indicare almeno un carattere maiuscolo e uno minuscolo.
- Deve contenere almeno un carattere speciale, ad esempio !\$%^&*()_+|~-=\`{}[]:":';<>?,/).
- Questi caratteri non sono consentiti Caratteri speciali a 8 bit (ad esempio, ¬£, √Å √', √¥, √ë, ¬ø, √ü)Spazi
- La password non deve essere l'ultima 10 password utilizzata di recente.
- Non deve contenere espressioni regolari, ad esempio
- Non devono contenere queste parole o loro derivati: cisco, sanjose e sanfran

D: Come impostare la password Grub?

A - Per impostare la password Grub, procedere come segue:

1. Immettere il comando ssh come utente cxcroot e fornire il token (rivolgersi al team di supporto per il token cxcroot).
2. Immettere il comando sudo su e fornire lo stesso token.
3. Immettere il comando grub-mkpasswd-pbkdf2 e impostare la password GRUB. Verrà stampato un hash della password fornita, copiare il contenuto.
4. vi nel file /etc/grub.d/00_header. Andare alla fine del file e sostituire l'output dell'hash seguito dal contenuto di password_pbkdf2 root ***** con l'hash ottenuto per la password nel passaggio 3.
5. Salvare il file con il comando: wq!
6. Eseguire il comando update-grub.

D - Qual è il periodo di scadenza per la password di cxcadmin?

R: La password è valida 90 giorni.

D: Il sistema disabilita l'account dopo un certo numero di tentativi di accesso consecutivi non riusciti?

R: Sì, l'account viene disabilitato dopo 5 tentativi consecutivi non riusciti. L'account viene bloccato per 30 minuti.

D: Come posso generare la passphrase?

A - Attenersi alla seguente procedura:

1. Eseguire il comando SSH e accedere come utente `cxcadmin`.
2. Eseguire il comando `remoteaccount cleanup -f`
3. Eseguire il comando `remoteaccount create`

D: L'host proxy supporta sia il nome host che l'IP?

A - Sì, ma per utilizzare il nome host l'utente deve fornire l'indirizzo IP DNS durante la configurazione della rete.

Secure Shell (SSH)

D: Quali sono gli algoritmi di cifratura supportati dalla shell SHH?

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

D: Come si effettua l'accesso alla console?

R: Attenersi alla seguente procedura:

1. Accedere come utente `cxcadmin`.
2. Specificare la password `cxcadmin`.

D: Gli accessi SSH vengono registrati?

R - Sì, sono registrati come parte del `var/logs/audit/audit.log`.

D: Qual è il timeout di una sessione inattiva?

A - Il timeout della sessione SSH si verifica se l'agente cloud rimane inattivo per cinque (5) minuti.

Porte e servizi

D: Quali sono le porte aperte per impostazione predefinita su CX Cloud Agent?

A - Sono disponibili le seguenti porte:

- Outbound port: L'agente cloud CX implementato può connettersi al back-end Cisco come indicato nella tabella sulla porta HTTPS 443 o tramite un proxy per inviare i dati a Cisco. L'agente cloud CX implementato può connettersi a Cisco DNA Center sulla porta HTTPS 443.

AMERICAS

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
agente.emea.[cisco.cloud](#)
ng.acs.agent.emea.[cisco.cl](#)
[oud](#)

APJC

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

Nota: Oltre ai domini elencati, quando i clienti EMEA o APJC reinstallano l'agente cloud, il dominio agent.us.cisco.cloud deve essere consentito nel firewall del cliente.

Il dominio agent.us.cisco.cloud non è più necessario dopo la reinstallazione.

Nota: Verificare che il traffico di ritorno sia consentito sulla porta 443.

- Inbound port: Per la gestione locale dell'agente cloud CX, devono essere accessibili 514 (Syslog) e 22 (ssh). Il cliente deve consentire alla porta 443 nel proprio firewall di ricevere i dati da CX Cloud.

Rapporto tra CX Cloud Agent e Cisco DNA Center

D: Qual è lo scopo e il rapporto tra Cisco DNA Center e CX Cloud Agent?

A - Cisco DNA Center è l'agente cloud che gestisce i dispositivi di rete della sede del cliente. CX Cloud Agent raccoglie le informazioni dell'inventario dei dispositivi dal Cisco DNA Center configurato e carica le informazioni dell'inventario disponibili come vista delle risorse in CX Cloud.

D: Quando è possibile fornire i dettagli di Cisco DNA Center a CX Cloud Agent?

A - Durante il Giorno 0 - Installazione di CX Cloud Agent, l'utente può aggiungere i dettagli di Cisco DNA Center dal portale CX Cloud. Inoltre, durante le operazioni del Giorno N, gli utenti possono aggiungere altri centri DNA da Admin Settings > Data source.

D: Quanti Cisco DNA Center è possibile aggiungere?

A: 10 cluster Cisco DNAC o 20 non cluster DNAC.

D - Quale ruolo può svolgere l'utente di Cisco DNA Center?

A - Il ruolo utente può essere admin o observer.

D - Come riflettere le modifiche apportate all'agente CX a causa delle modifiche delle credenziali di un centro DNA collegato?

A - Eseguire questi comandi dalla console dell'agente cloud CX:

```
cxcli agent modifyController
```

Contattare il supporto tecnico per qualsiasi problema durante l'aggiornamento delle credenziali DNAC.

D: Come vengono memorizzati i dettagli di Cisco DNA Center in CX Cloud Agent?

R: Le credenziali di Cisco DNA Center vengono criptate utilizzando AES-256 e archiviate nel database di CX Cloud Agent. Il database di CX Cloud Agent è protetto da un ID utente e una password sicuri.

D: Quale tipo di crittografia viene utilizzata durante l'accesso all'API di Cisco DNA Center da CX Cloud Agent?

R: Per la comunicazione tra Cisco DNA Center e CX Cloud Agent, viene usato il protocollo HTTPS su TLS 1.2.

D: Quali sono le operazioni eseguite da CX Cloud Agent sul Cisco DNA Center Cloud Agent integrato?

A - L'agente cloud CX raccoglie i dati di Cisco DNA Center sui dispositivi di rete e utilizza l'interfaccia del router dei comandi di Cisco DNA Center per comunicare con i dispositivi terminali ed eseguire i comandi CLI (comando show). Non viene eseguito alcun comando di modifica della configurazione

D: Quali sono i dati predefiniti raccolti da Cisco DNA Center e caricati nel backend?

R:

- Entità di rete
- Moduli
- Show version
- Config
- Informazioni sull'immagine del dispositivo
- Tag

D: Quali sono i dati aggiuntivi raccolti da Cisco DNA Center e caricati nel backend di Cisco?

R: Tutte le informazioni sono disponibili [qui](#).

D: Come vengono caricati i dati dell'inventario sul backend?

R: CX Cloud Agent carica i dati tramite il protocollo TLS 1.2 sul server backend di Cisco.

D: Qual è la frequenza di caricamento dell'inventario?

A - La raccolta viene attivata in base alla pianificazione definita dall'utente e caricata nel back-end Cisco.

D: L'utente può ripianificare l'inventario?

A - Sì, è disponibile un'opzione per modificare le informazioni sulla programmazione da Admin Settings> Data Sources.

D: Quando scade la connessione tra Cisco DNA Center e Cloud Agent?

R: I timeout sono classificati come segue:

- Per la connessione iniziale, il timeout è massimo 300 secondi. Se la connessione tra Cisco DNA Center e Cloud Agent non viene stabilita entro un massimo di 5 minuti, la connessione viene interrotta.
- Per le connessioni ricorrenti, tipiche o per gli aggiornamenti: il timeout della risposta è 1800 secondi. Se la risposta non viene ricevuta o letta entro 30 minuti, la connessione viene interrotta.

Analisi diagnostica di CX Cloud Agent

D: Quali sono i comandi disponibili per eseguire l'analisi sul dispositivo?

A - I comandi che devono essere eseguiti sul dispositivo per la scansione vengono determinati dinamicamente durante il processo di scansione. L'insieme di comandi può cambiare nel tempo, anche per lo stesso dispositivo (e non in controllo di Diagnostic Scan).

D: Dove vengono archiviati e analizzati i risultati dall'analisi?

R: I risultati vengono memorizzati e analizzati sul server backend di Cisco.

R: I duplicati (per nome host o IP) di Cisco DNA Center vengono aggiunti all'analisi diagnostica quando l'origine Cisco DNA Center è collegata?

A - No, i duplicati vengono filtrati e vengono estratti solo i dispositivi univoci.

D: Cosa succede quando uno dei comandi di analisi non viene eseguito correttamente?

R: L'analisi del dispositivo viene interrotta completamente e l'analisi viene contrassegnata come non riuscita.

Log di sistema di CX Cloud Agent

D - Quali informazioni sullo stato vengono inviate al cloud CX?

R: Log delle applicazioni, stato dei pod, dettagli di Cisco DNA Center, log di audit, dettagli di sistema e dettagli hardware.

D: Quali dettagli di sistema e hardware vengono raccolti?

R: Output di esempio:

```
system_details":{
  "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"
  }
}
```

```
"dettagli_hardware":{
"total_cpu":"8",
"cpu_usage":"12,5%",
"total_memory":"16007MB",
"free_memory":"9994 MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}
```

D: Come vengono inviati i dati sull'integrità al backend?

R: con l'agente cloud CX, il servizio di integrità (facilità di manutenzione) invia i dati al back-end Cisco.

D: Qual è la policy di conservazione dei log dei dati sull'integrità di CX Cloud Agent nel server backend?

R: La policy dei log dei dati sull'integrità di CX Cloud Agent nel server backend prevede un periodo di conservazione di 120 giorni.

D: Quali sono i tipi di caricamento disponibili?

A - Tre tipi di caricamento disponibili

1. Caricamento scorte
2. Caricamento syslog
3. Caricamento integrità agente: 3 elementi come parte del caricamento dello stato Integrità dei servizi: ogni 5 minutiPodlog - ogni 1 oraRegistro di controllo - ogni 1 ora

Risoluzione dei problemi

Problema: Impossibile accedere all'IP configurato.

Soluzione: Eseguire il comando SSH con l'IP configurato. In caso di timeout della connessione, è possibile che l'indirizzo IP non sia stato configurato correttamente. In questo caso, eseguire nuovamente l'installazione configurando un indirizzo IP valido. A tale scopo, è possibile utilizzare il portale con l'opzione di reinstallazione fornita nel Admin Setting pagina.

Problema: Come verificare se i servizi sono attivi dopo la registrazione?

Soluzione: Eseguire il comando riportato di seguito e verificare che i pod siano attivi e in esecuzione.

1. Eseguire il comando SSH sull'IP configurato come cxcadmin.
2. Immettere la password.
3. Eseguire il comando *kubectl get pods*.

I pod possono essere in qualsiasi stato, ad esempio in esecuzione, Inizializzazione o Creazione contenitore, ma dopo 20 minuti, i pod devono essere in esecuzione.

Se lo stato *non è in esecuzione* o *Pod Initialization*, controllare la descrizione del pod con il comando mostrato di seguito

```
kubectl descrizione pod <podname>
```

Le informazioni sullo stato del pod vengono restituite nell'output.

Problema: Come verificare se l'intercettore SSL è disabilitato sul proxy del cliente?

Soluzione: Eseguire il comando curl illustrato qui per verificare la sezione del certificato del server. La risposta contiene i dettagli del certificato del server Web concavo.

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

* Certificato server:

* oggetto: C=IT; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

* data di inizio: 16 feb 11:55:11 2021 GMT

* data di scadenza: 16 feb 12:05:00 2022 GMT

* subjectAltName: l'host "concsoweb-prd.cisco.com" corrisponde all'host "concsoweb-prd.cisco.com" del certificato

* emittente: C=IT; O=ID idrante (Avalanche Cloud Corporation); CN=IDRidranteSSL CA G3

* Verifica certificato SSL corretta.

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

Problema: Comandi kubectl non riusciti. L'errore viene visualizzato come "La connessione al server X.X.X:6443 è stata rifiutata - è stato specificato l'host o la porta corretta".

Soluzione:

- Verificare la disponibilità delle risorse, [esempio: CPU, memoria]
- Attendere l'avvio del servizio Kubernetes.

Problema: Come richiamare i dettagli dell'errore di raccolta di un comando o di un dispositivo

Soluzione:

- Immettere il comando `kubectl get pods` e richiamare il nome del pod di raccolta.
- Immettere il comando `kubectl logs` per ottenere i dettagli specifici del comando o del dispositivo.

Problema: Impossibile eseguire il comando `kubectl`; viene visualizzato l'errore "[authentication.go:64] Unable to authenticate the request due to an error: (Impossibile autenticare la richiesta a causa di un errore:) [x509: certificato scaduto o non ancora valido, x509: certificato scaduto o non ancora valido]"

Soluzione: eseguire i comandi visualizzati come utente `cxcroot`

```
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-serving
systemctl restart k3s
```

Risoluzione degli errori di raccolta

L'errore di raccolta può essere causato da qualsiasi vincolo o problema riscontrato nel controller aggiunto o nei dispositivi presenti nel controller.

Nella tabella riportata di seguito è riportato lo snippet di errore relativo ai casi di utilizzo rilevati nel microservizio Collection durante il processo di raccolta.

Scenario d'uso	Frammento di codice nel log del microservizio Collection
Il dispositivo desiderato non viene rilevato in Cisco DNA Center	<pre>{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a" }</pre>
Il dispositivo desiderato non è raggiungibile da Cisco DNA Center	<pre>{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error occurred while executing command: show version\nError connecting to device [Host: 172.21.137.221:22]No route to host : No route to host "</pre>
Il dispositivo desiderato non è raggiungibile da Cisco DNA Center	<pre>{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error ocurred while executing command : show version\nError connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connection out: /X.X.X.X:22"</pre>
Il comando desiderato non è disponibile sul dispositivo	<pre>{ "command": "show run-config", "status": "Success", "commandResponse": " Error ocurred while executing command : show run-config\n\nshow run-config\n ^\n% Invalid input detected at \u0027^\u0027 marker.\n\nXXCT5760#", "errorMessage": "" }</pre>
Se il dispositivo richiesto non dispone di SSHv2 e Cisco DNA Center tenta di	<pre>{ "command": "show version", "status": "Failed",</pre>

connetterlo con SSHv2

```
"commandResponse": "",  
"errorMessage": "Error ocurred while executing command : show version\nSSH2 cl  
closed : Remote party uses incompatible protocol, it is not SSH-2 compatible."  
}
```

Il comando è disabilitato nel microservizio Collection

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

Esecuzione dell'attività Command Runner non riuscita, Cisco DNA Center non restituisce l'URL dell'attività

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

Creazione dell'attività Command Runner non riuscita in Cisco DNA Center

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

Mancata risposta al microservizio Collection in seguito a una richiesta Command Runner di Cisco DNA Center

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

Cisco DNA Center non completa l'attività entro il timeout configurato (5 minuti per comando nel microservizio Collection)

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

Esecuzione dell'attività Command Runner non riuscita, l'ID file dell'attività inviata da Cisco DNA Center è vuoto

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

Esecuzione dell'attività Command Runner non riuscita, Cisco DNA Center non restituisce il tag dell'ID file

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

Command Runner non può essere eseguito sul dispositivo

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

Command Runner non può essere eseguito dall'utente

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

Risoluzione degli errori di analisi diagnostica

L'errore di analisi e la causa possono provenire da uno qualsiasi dei componenti elencati.

Quando si avvia un'analisi dal portale, a volte viene visualizzato un errore del tipo "failed: Internal server error" (non riuscito: errore interno del server).

La causa del problema può essere uno dei componenti elencati

- Punto di controllo
- Gateway dei dati della rete
- Connettore
- Analisi diagnostica
- Microservizio di CX Cloud Agent (devicemanager, collection)
- Cisco DNA Center
- APIX
- Mashery
- Accesso ping
- IRONBANK
- IRONBANK GW
- Big Data Broker (BDB)

Per visualizzare i registri:

1. Accedere alla console di CX Cloud Agent
2. Eseguire il comando SSH come utente cxcadmin e immettere la password
3. Immettere il comando `kubectl get pods`
4. Ottenere il nome pod della raccolta, il connettore e la facilità di manutenzione.
5. Per verificare la raccolta, il connettore e i registri dei microservizi di manutenzione

- Immettere il comando `kubectl logs`
- Immettere il comando `kubectl logs`
- Immettere il comando `kubectl logs`

Nella tabella riportata di seguito viene visualizzato il frammento di codice di errore presente nei registri dei microservizi Raccolta e facilità di manutenzione che si verifica a causa dei problemi o dei vincoli dei componenti.

Scenario d'uso

Il dispositivo può essere raggiungibile e supportato, ma i comandi da eseguire su tale dispositivo sono elencati a blocchi nel microservizio Collection

Il dispositivo che si sta tentando di analizzare non è disponibile.

In questo scenario si è verificato un errore di sincronizzazione tra i componenti, ad esempio portale, scansione diagnostica, componente CX e Cisco DNA Center.

Il dispositivo che si sta tentando di analizzare è occupato, in uno scenario in cui lo stesso dispositivo fa parte di un altro processo e Cisco DNA Center non gestisce richieste parallele per il dispositivo.

Frammento di codice nel log del microservizio Collection

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

```
No device found with id 02eb08be-b13f-4d25-9eaf4e882f71a
```

```
All requested devices are already being queried by another command runner in another session. Please try again with different devices".
```

```
Requested devices are not in inventory, try with
```

Il dispositivo non supporta la funzionalità di analisi

Se il dispositivo che si è tentato di analizzare non è raggiungibile

Cisco DNA Center non è raggiungibile dal Cloud Agent oppure il microservizio Collection del Cloud Agent non riceve risposta in seguito a una richiesta Command Runner di Cisco DNA Center

```
devices available in inventory
"Error occurred while executing command: show
udi\nError connecting to device [Host: x.x.x.x:2
route to host : No route to host
{
"command": "show version",
"status": "Failed",
"commandResponse": "",
"errorMessage": "The command runner task fa
device %s, RequestURL: %s."
}
```

Scenario d'uso

Nella richiesta di analisi mancano i dettagli della pianificazione

Nella richiesta di analisi mancano i dettagli del dispositivo

Connettività al CPA assente

Il dispositivo da analizzare non supporta le analisi diagnostiche

Frammento di codice nel log del microservizio Control Po Agent

Failed to execute request

```
{"message": "23502: null value in column \"schedule\" violates not-null const
```

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\"}
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).