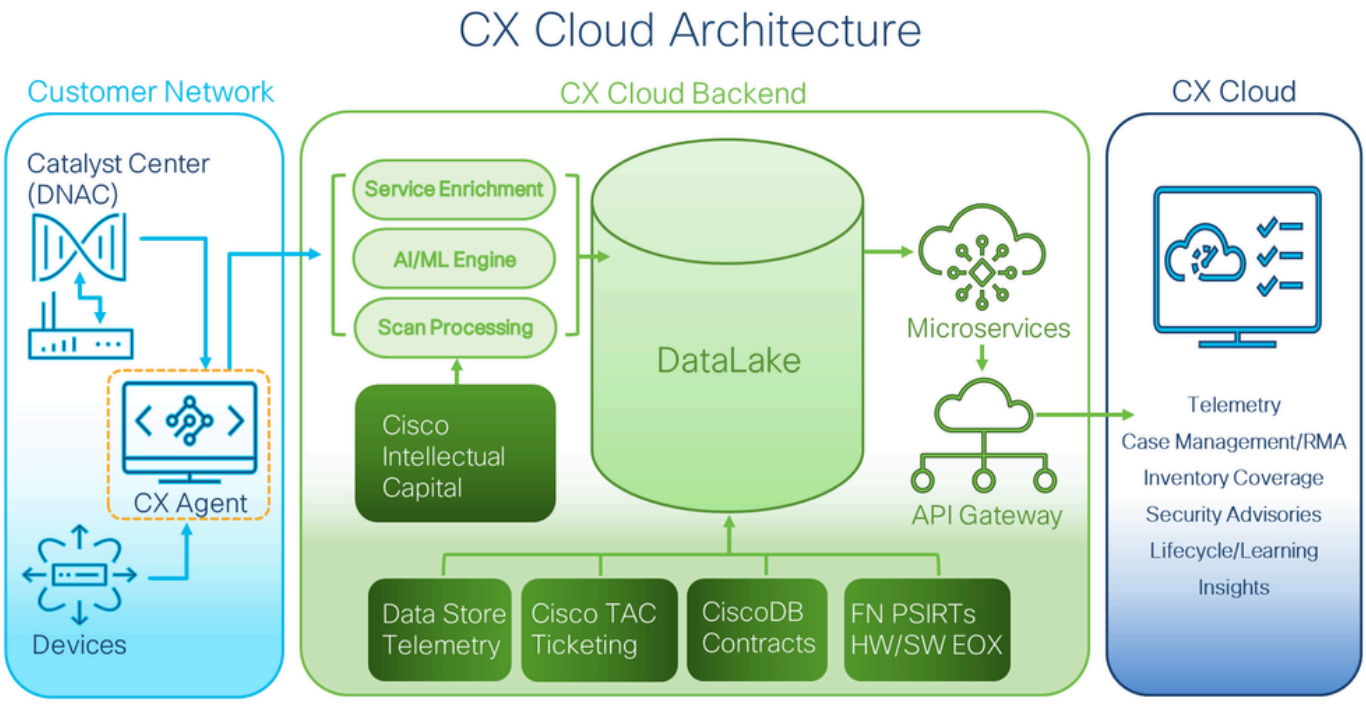
Panoramica di CX Cloud Agent v2.4

Sommario

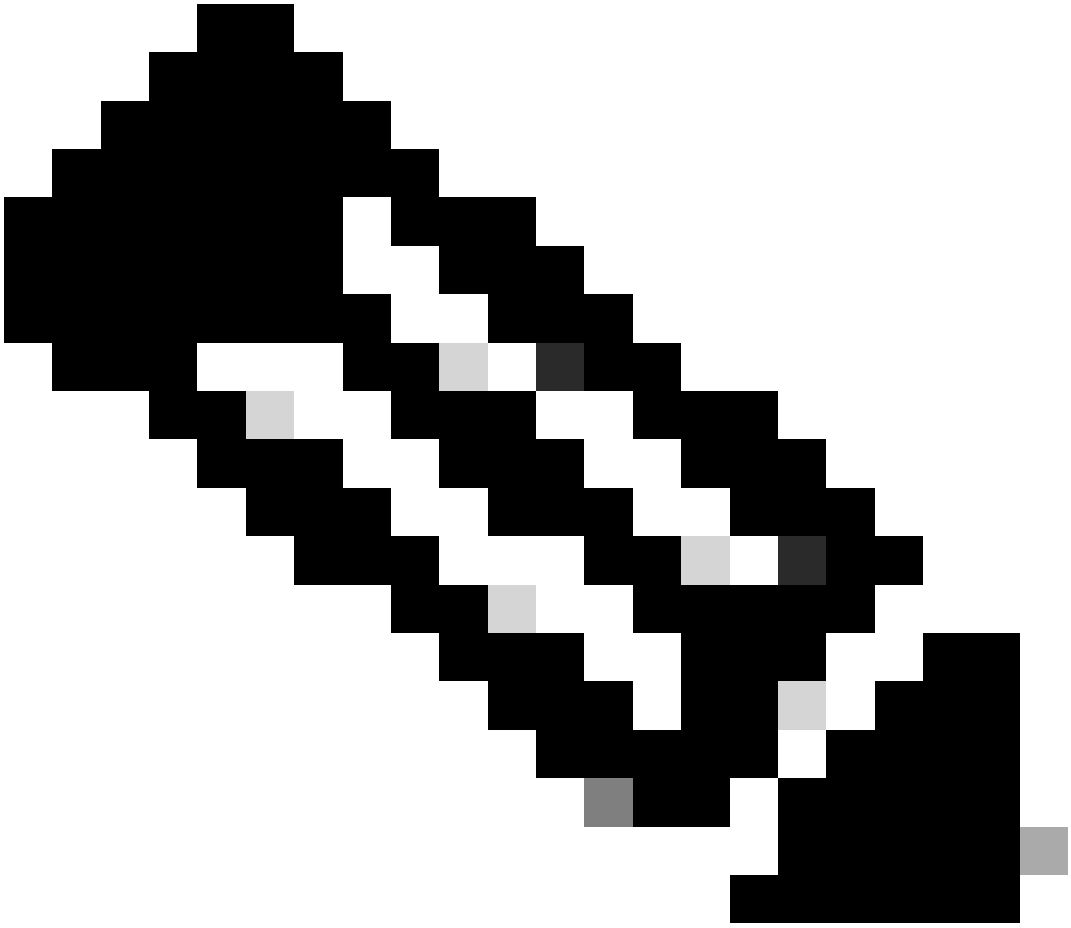
Introduzione

Questo documento descrive Cisco's Customer Experience (CX) Cloud Agent. Cisco CX Cloud Agent è una piattaforma altamente scalabile che raccoglie dati di telemetria dai dispositivi di rete dei clienti per fornire informazioni pratiche ai clienti. CX Cloud Agent consente di trasformare l'intelligenza artificiale (AI)/Machine Learning (ML) dei dati di configurazione in esecuzione attiva in informazioni proattive e predittive visualizzate in CX Cloud.



Architettura di CX Cloud

Questa guida è specifica di CX Cloud Agent v2.4. Per accedere alle versioni precedenti, consultare la pagina Cisco CX Cloud Agent.



Nota: le immagini di questa guida sono solo a scopo di riferimento. Il contenuto effettivo può variare.

Prerequisiti

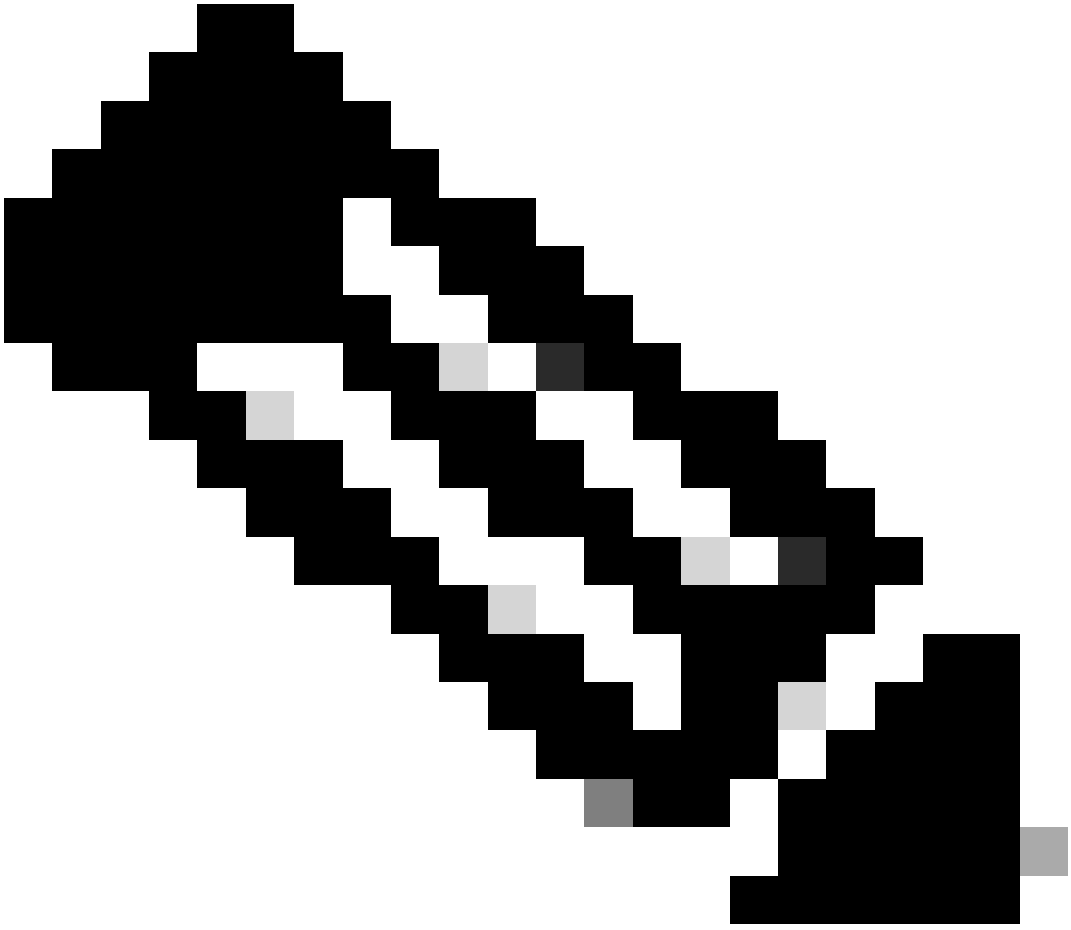
CX Cloud Agent viene eseguito come macchina virtuale (VM) e può essere scaricato come OVA (Open Virtual Appliance) o VHD (Virtual Hard Disk).

Requisiti di distribuzione

- Per una nuova installazione è necessario uno dei seguenti hypervisor:
  - VMware ESXi versione 5.5 o successiva
  - Oracle Virtual Box 5.2.30 o successivo
  - Windows Hypervisor versione 2012-2022
- Per la distribuzione della macchina virtuale sono necessarie le configurazioni riportate nella tabella seguente:

Tipo di distribuzione agente cloud CX	Numero di core CPU	RAM	Disco rigido	*Numero massimo di asset collegati direttamente all'agente cloud CX
OAV piccolo	8C	16 GB	200 GB	10,000
OVULI medi	16°C	32 GB	600 GB	20,000
OVULI grandi	32 quater	64 GB	1.200 GB	50,000:

*Oltre a collegare 20 non-cluster Cisco DNA Center o 10 cluster Cisco DNA Center per ogni istanza di CX Cloud Agent.



Nota: la patch flessibile OVA/Patch 2.4 per configurazioni medie e grandi è disponibile solo per VM VM VMware ESXi. Impossibile utilizzare Oracle VirtualBox e Windows Hyper-

---

V per configurazioni medie e grandi.

- Per i clienti che utilizzano i centri dati statunitensi designati come area dati principale per l'archiviazione dei dati del cloud CX, l'agente cloud CX deve essere in grado di connettersi ai server mostrati qui, utilizzando il nome di dominio completo (FQDN) e utilizzando HTTPS sulla porta TCP 443:
  - FQDN: agent.us.csco.cloud
  - FQDN: ng.acs.agent.us.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati europei designati come area dati principale per l'archiviazione dei dati del cloud CX: l'agente cloud CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando il nome di dominio completo (FQDN) e utilizzando HTTPS sulla porta TCP 443:
  - FQDN: agent.us.csco.cloud
  - FQDN: agent.emea.cisco.cloud
  - FQDN: ng.acs.agent.emea.cisco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati dell'Asia Pacifico designati come area dati principale per l'archiviazione dei dati del cloud CX: l'agente cloud CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando il nome di dominio completo (FQDN) e utilizzando HTTPS sulla porta TCP 443:
  - FQDN: agent.us.csco.cloud
  - FQDN: agent.apjc.cisco.cloud
  - FQDN: ng.acs.agent.apjc.cisco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati designati per l'Europa e l'Asia Pacifico come regione dati principale, la connettività all'FQDN: agent.us.csco.cloud è richiesta solo per la registrazione dell'agente cloud CX 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.
- Nella tabella seguente viene fornito un riepilogo delle porte e dei protocolli che devono essere aperti e abilitati per il corretto funzionamento dell'agente cloud CX:

CX Cloud Agent Traffic

Source	Destination	Protocol	Port	Purpose	Type
CX Cloud Agent	All regions: cloudsso.cisco.com api-cx.cisco.com agent.us.csco.cloud DNA Center AMER region: ng.acs.agent.us.csco.cloud EMEA region: agent.emea.csco.cloud ng.acs.agent.emea.csco.cloud APJC region: agent.apjc.csco.cloud ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers	Bi-directional to Cisco AWS regional data centers and DNA Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- Se nell'ambiente VM è abilitato il protocollo DHCP (Dynamic Host Configuration Protocol), viene rilevato automaticamente un indirizzo IP. In caso contrario, devono essere disponibili un indirizzo IPv4, una subnet mask, l'indirizzo IP del gateway predefinito e l'indirizzo IP del server DNS (Domain Name Service).
- Solo IPv4 è supportato.
- Le versioni certificate di Cisco DNA Center per cluster a nodo singolo e ad alta disponibilità (HA) sono comprese tra 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x e di Cisco Catalyst Center Virtual Appliance e Cisco DNA Center Virtual Appliance.
- Se la rete dispone di un'intercettazione SSL, autorizzare-elencare l'indirizzo IP dell'agente cloud CX.
- Per tutti gli asset con connessione diretta, è richiesto il livello di privilegio SSH 15.
- Utilizzare solo i nomi host forniti. Impossibile utilizzare indirizzi IP statici.

Accesso ai domini critici

Per iniziare il percorso di CX Cloud, gli utenti devono accedere a questi domini. Utilizzare solo i nomi host forniti. Non utilizzare indirizzi IP statici.

Domini specifici del portale agenti cloud CX

Domini principali	Altri domini
csco.cloud	cloudfront.net
	eum-appdynamics.com

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

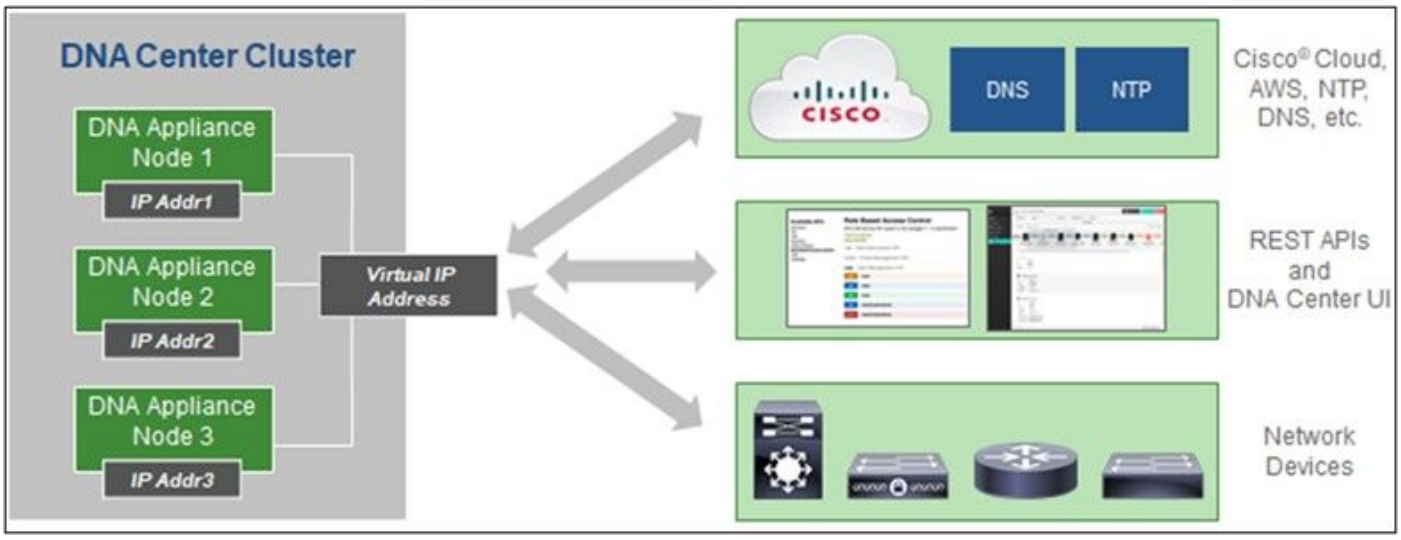
Domini specifici per l'agente cloud CX

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

Nota: l'accesso in uscita deve essere consentito con il reindirizzamento abilitato sulla porta 443 per i nomi di dominio completo (FQDN) specificati.

Versione supportata di Cisco DNA Center

Le versioni supportate di Cisco DNA Center a nodo singolo e cluster HA sono comprese tra 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x e di Cisco Catalyst Center Virtual Appliance e Cisco DNA Center Virtual Appliance.



Cisco DNA Center con cluster HA a più nodi

Browser supportati

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

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Elenco dei prodotti supportati

Per visualizzare l'elenco dei prodotti supportati da CX Cloud Agent, fare riferimento all'elenco dei prodotti supportati.

Aggiornamento/installazione di CX Cloud Agent v2.4

- I clienti esistenti che eseguono l'aggiornamento alla nuova versione devono fare riferimento alla sezione Aggiornamento dell'agente cloud CX v2.4.
- I nuovi clienti che implementano una nuova installazione flessibile di OAV v2.4 devono fare riferimento all'aggiunta dell'agente cloud CX come origine dati.

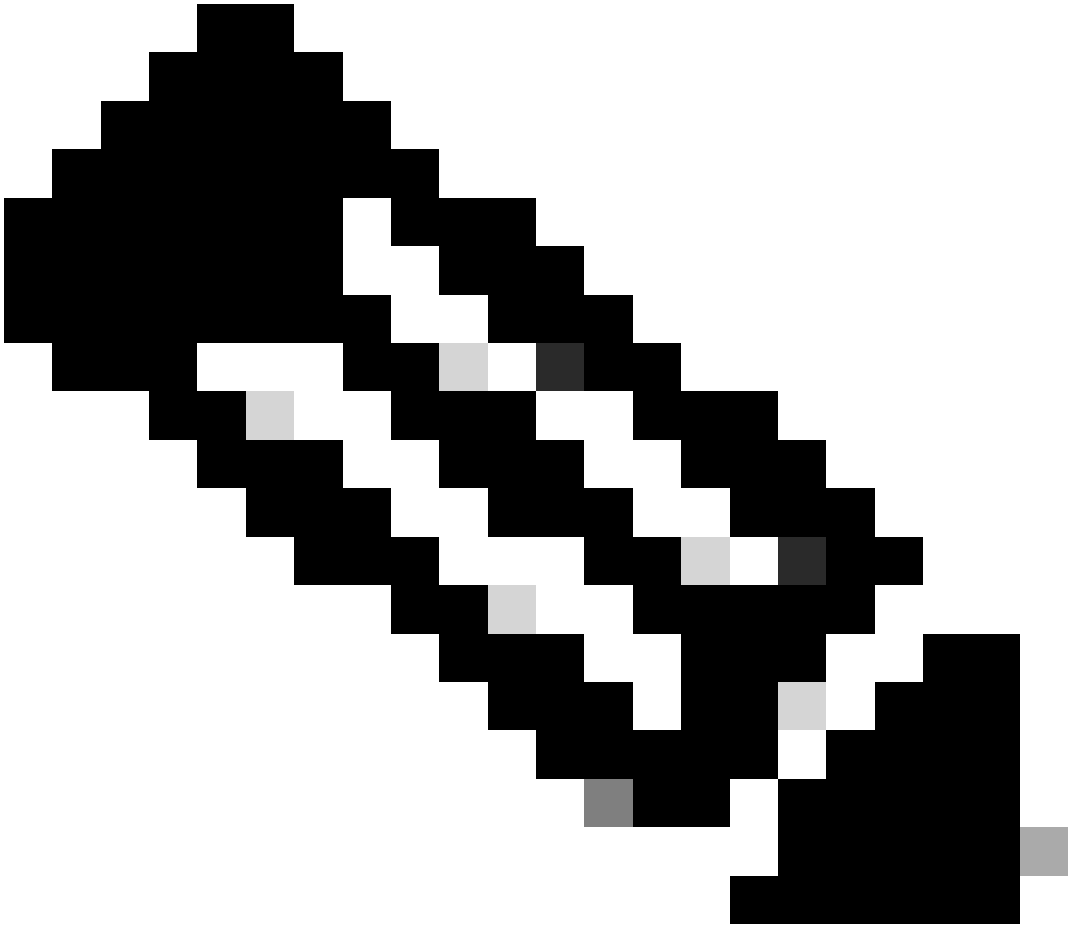
Aggiornamento delle VM esistenti alla configurazione grande e media

I clienti possono aggiornare la configurazione VM esistente a sistemi di medie o grandi dimensioni utilizzando le opzioni di virtualizzazione flessibile in base alle dimensioni e alla complessità della rete.

Per aggiornare la configurazione VM esistente da piccole a medie o grandi, fare riferimento alla sezione Aggiornamento delle VM dell'agente cloud CX alla configurazione media e grande.

Aggiornamento di CX Cloud Agent v2.4

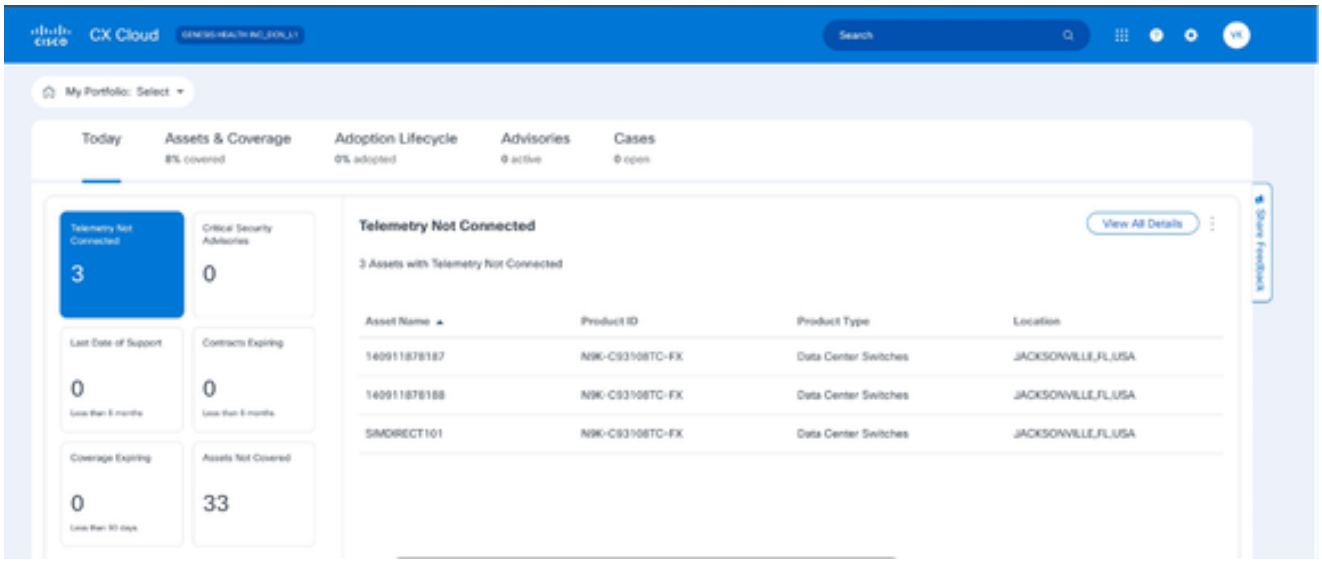
I clienti che eseguono CX Cloud Agent v2.3.x e versioni successive possono seguire i passaggi descritti in questa sezione per eseguire direttamente l'aggiornamento alla versione v2.4.



> Nota: i clienti di CX Cloud Agent v2.2.x devono eseguire l'aggiornamento alla versione 2.3.x prima di eseguire l'aggiornamento alla versione 2.4 o installare la versione 2.4 come nuova installazione di OAV.

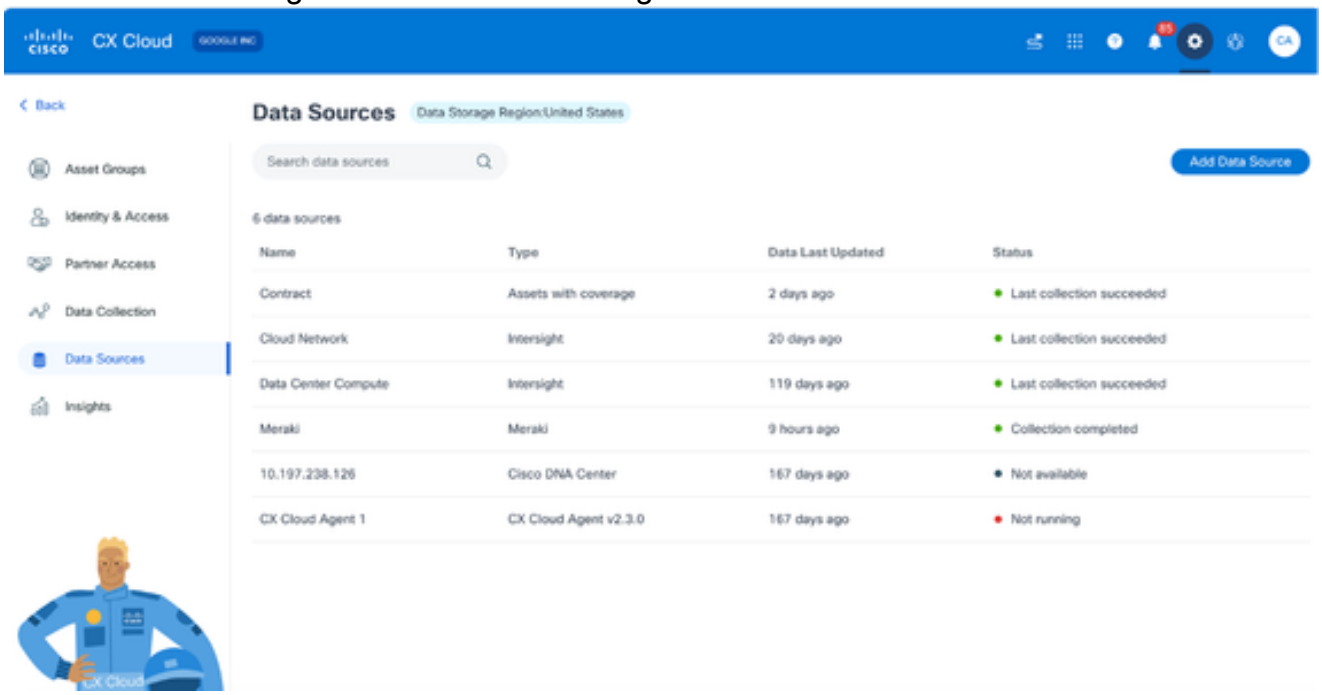
Per installare l'aggiornamento di CX Cloud Agent v2.4 da CX Cloud:

1. Accedere a CX Cloud. Verrà visualizzata la home page.



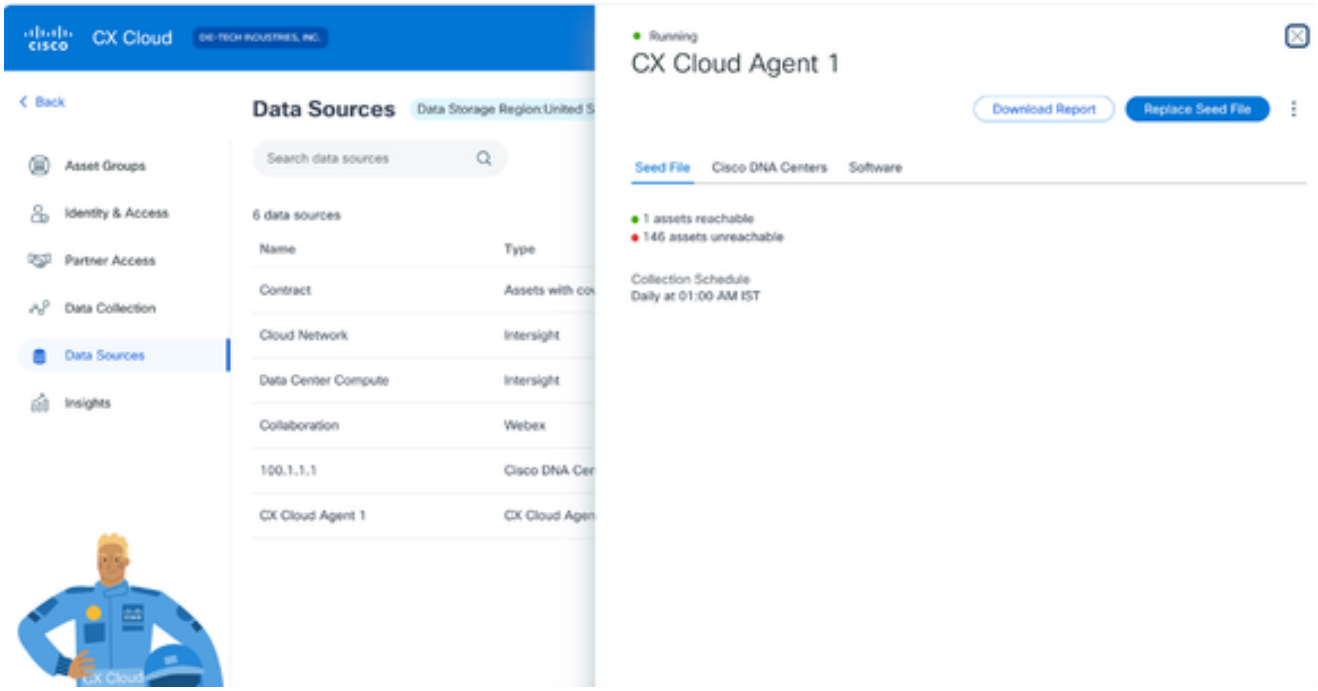
Home page di CX Cloud

2. Fare clic sull'icona Admin Center. Viene visualizzata la finestra Data Sources (Origini dati)in cui è visualizzato l'agente cloud CX come origine dati esistente.



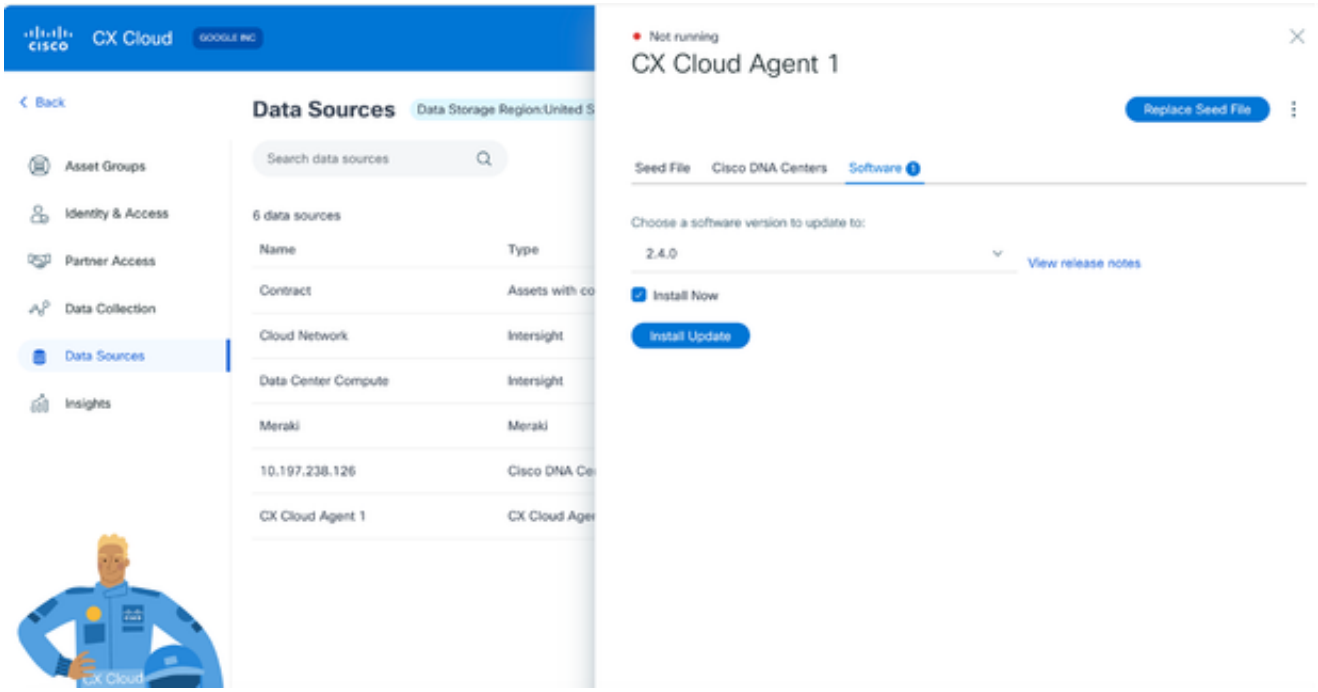
Origini dei dati

3. Fare clic sull'origine dati CX Cloud Agent. Viene visualizzata la finestra dei dettagli di CX Cloud Agent.



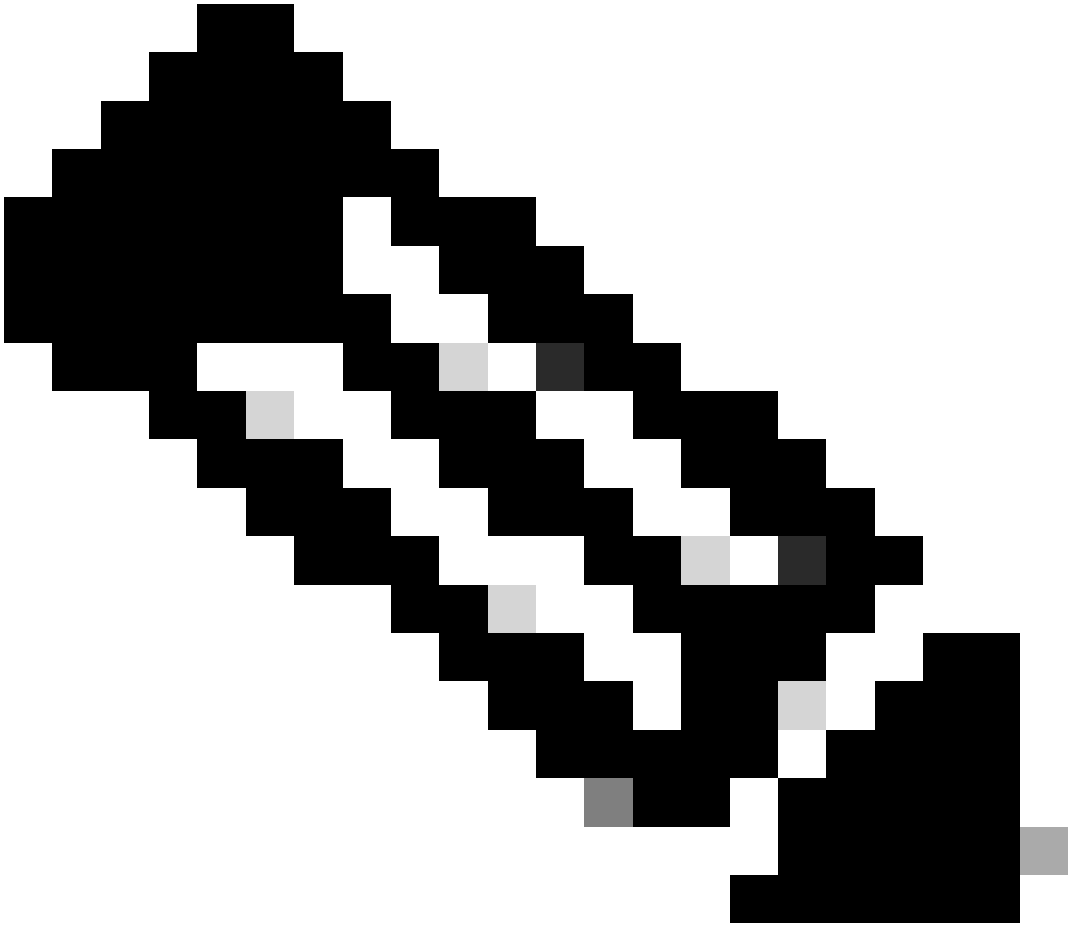
Visualizzazione dettagli origini dati

4. Fare clic sulla scheda Software.



Vista dei dettagli dell'agente cloud CX

5. Selezionare la versione del software 2.4.0 dall'elenco a discesa Scegliere una versione del software da aggiornare.
6. Fare clic su Installa aggiornamento per installare CX Cloud Agent v2.4.0.



Nota: i clienti possono pianificare l'aggiornamento per un secondo momento deselezionando la casella di controllo Installa ora che visualizza le opzioni di programmazione.

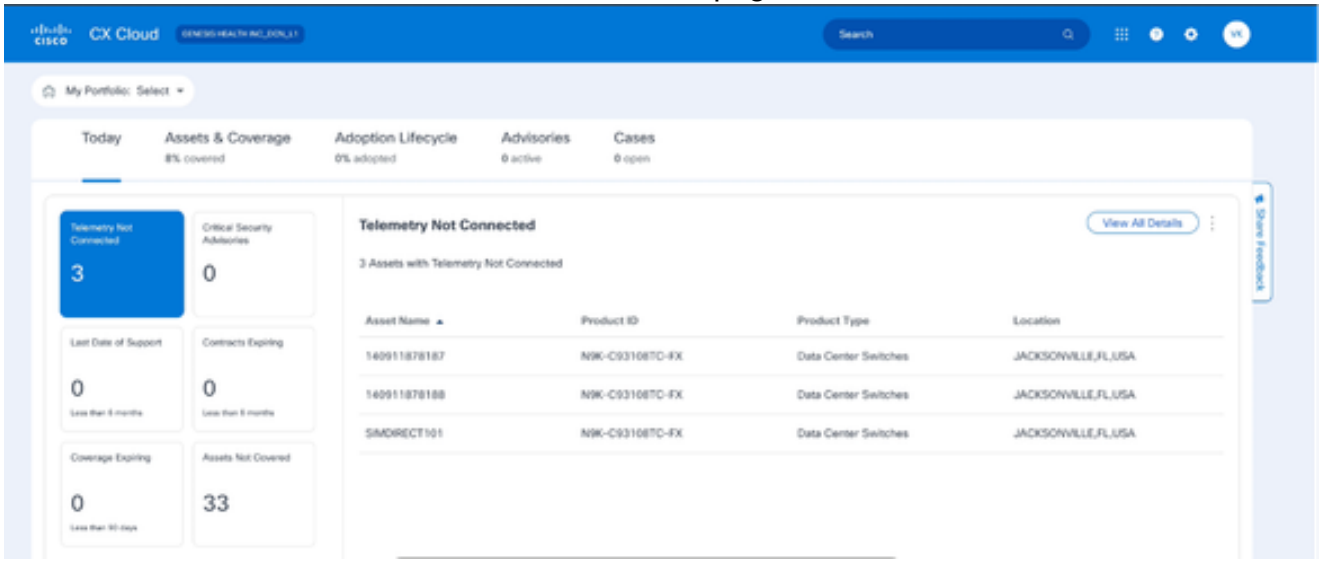
Aggiunta dell'agente cloud CX

I clienti possono aggiungere fino a venti (20) istanze di CX Cloud Agent in CX Cloud.

Per aggiungere un agente cloud CX:

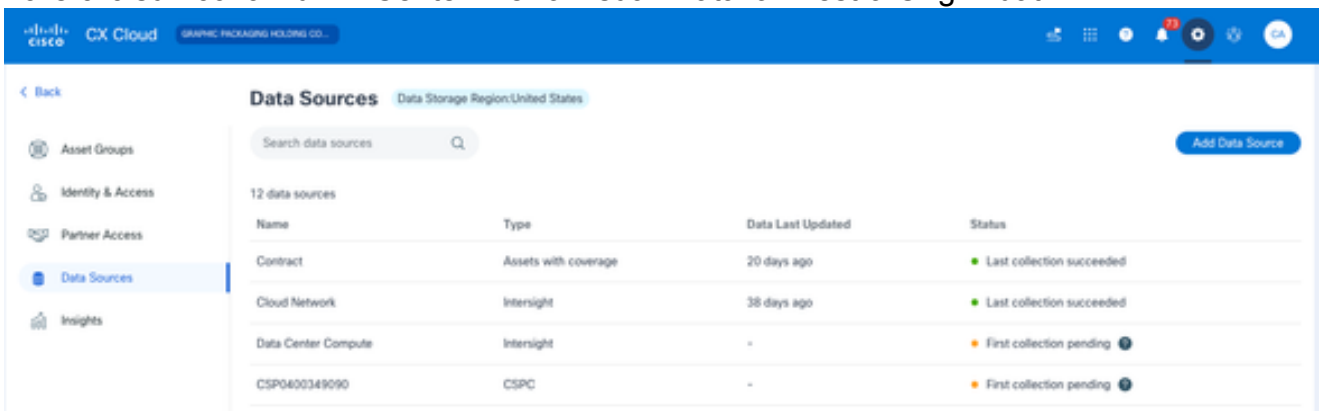
Nota: ripetere i passaggi seguenti per aggiungere ulteriori istanze dell'agente cloud CX come origine dati.

1. Accedere a CX Cloud. Verrà visualizzata la home page.



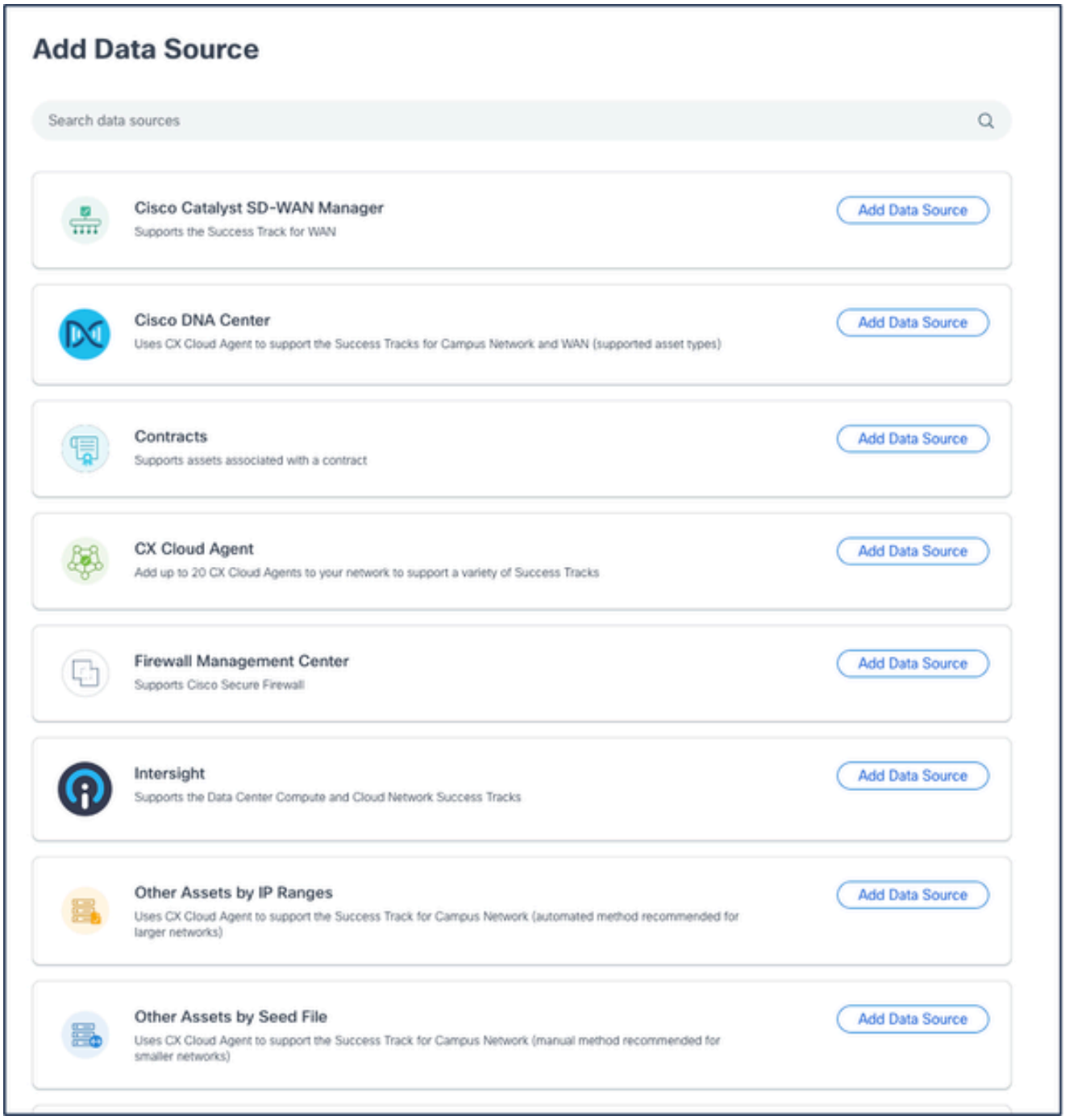
Home page di CX Cloud

2. Fare clic sull'icona Admin Center. Verrà visualizzata la finestra Origini dati.



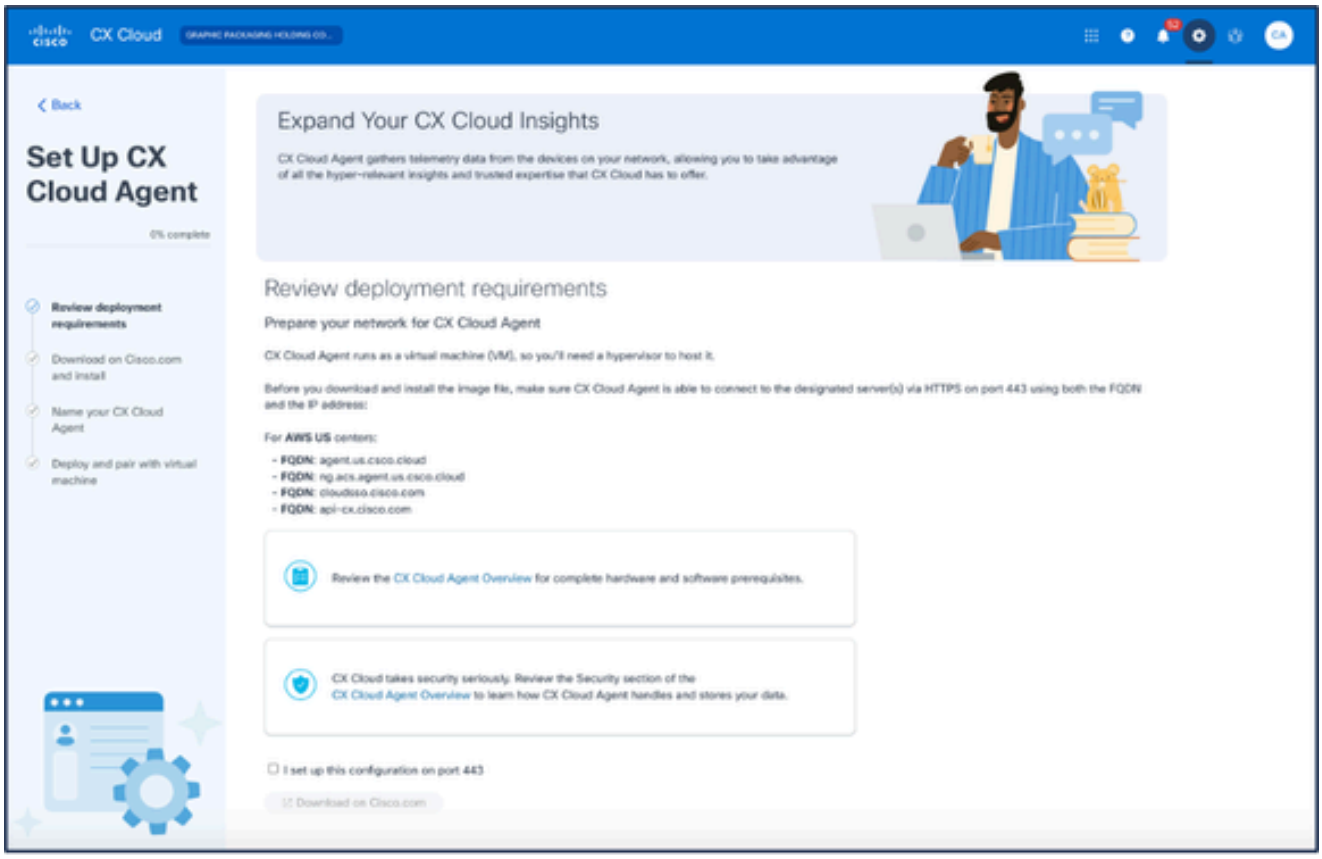
Origini dei dati

3. Fare clic su Aggiungi origine dati. Verrà visualizzata la finestra Aggiungi origine dati. Le opzioni visualizzate variano in base alle sottoscrizioni dei clienti.



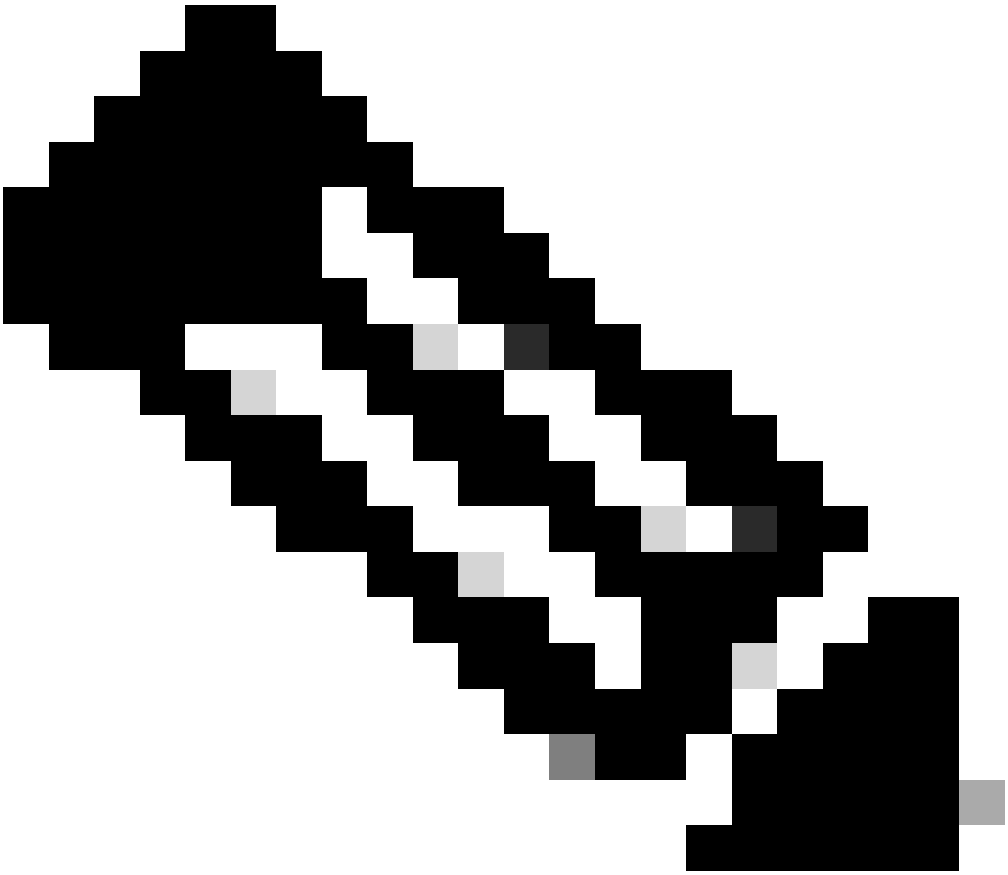
Aggiungi origine dati

4. Fare clic su Add Data Source (Aggiungi origine dati) dall'opzione CX Cloud Agent. Viene visualizzata la finestra Set Up CX Cloud Agent.



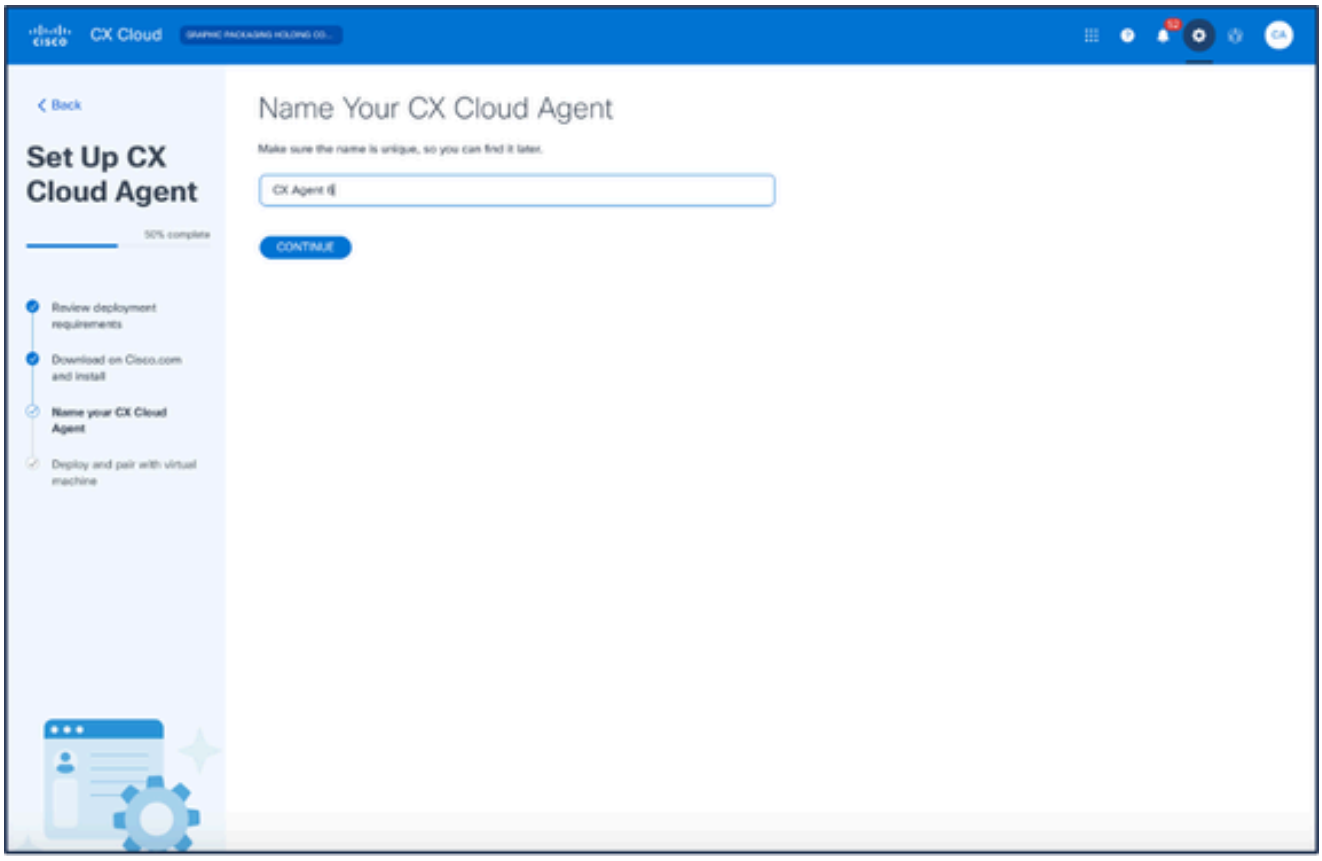
Configura agente cloud CX

5. Esaminare la sezione Verifica dei requisiti di distribuzione e selezionare la casella di controllo I set up this configuration on port 443.
6. Fare clic su Download (Scarica) sul sito Cisco.com. Si apre la pagina Software Download.
7. Scaricare il file OAV di CX Cloud Agent v2.4.



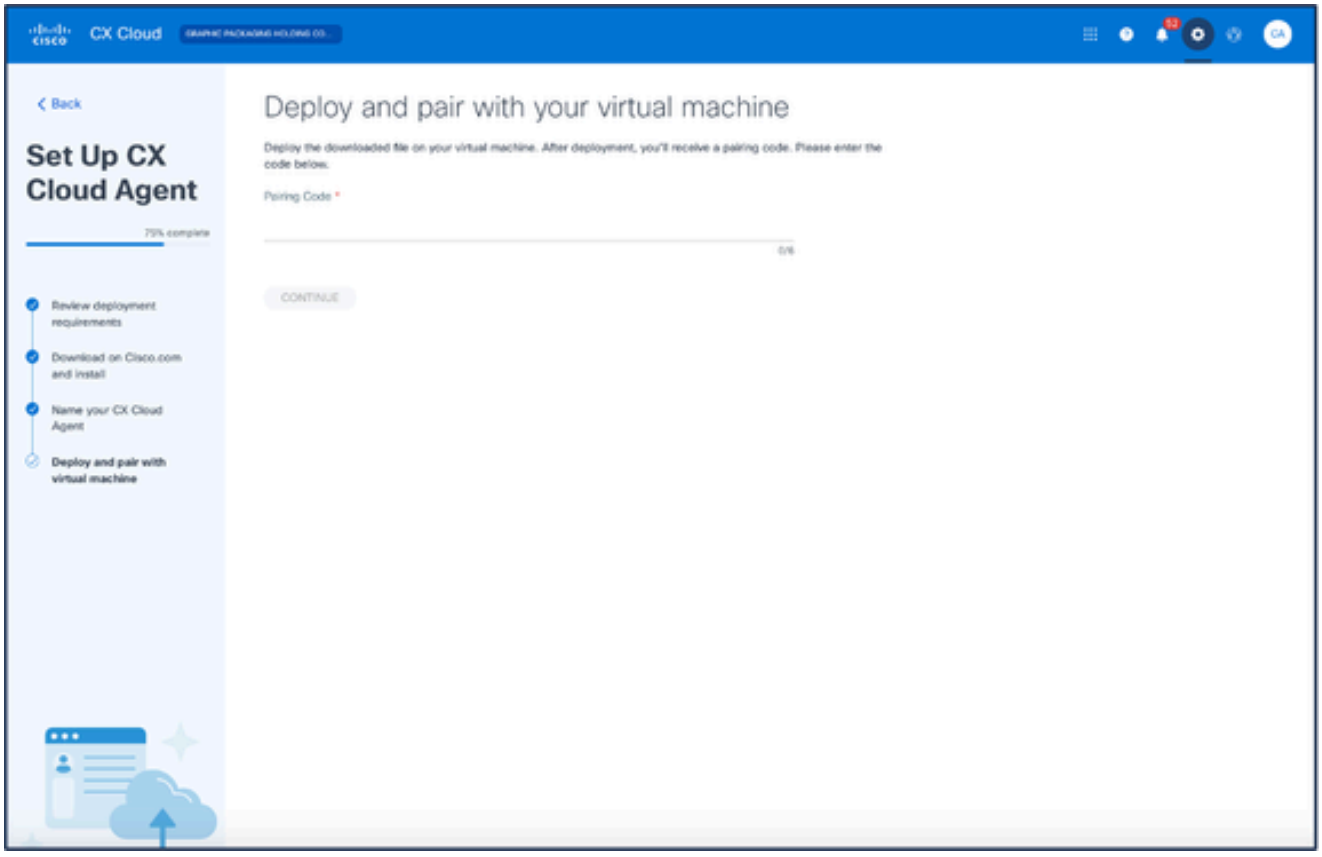
Nota: dopo la distribuzione del file OVA viene generato un codice di associazione, necessario per completare la configurazione dell'agente cloud CX.

8. Immettere il nome dell'agente cloud CX nel campo Name Your CX Cloud Agent.



Denominazione agente cloud CX

9. Fare clic su Continue (Continua). Verrà visualizzata la finestra Distribuisci e associa a macchina virtuale.



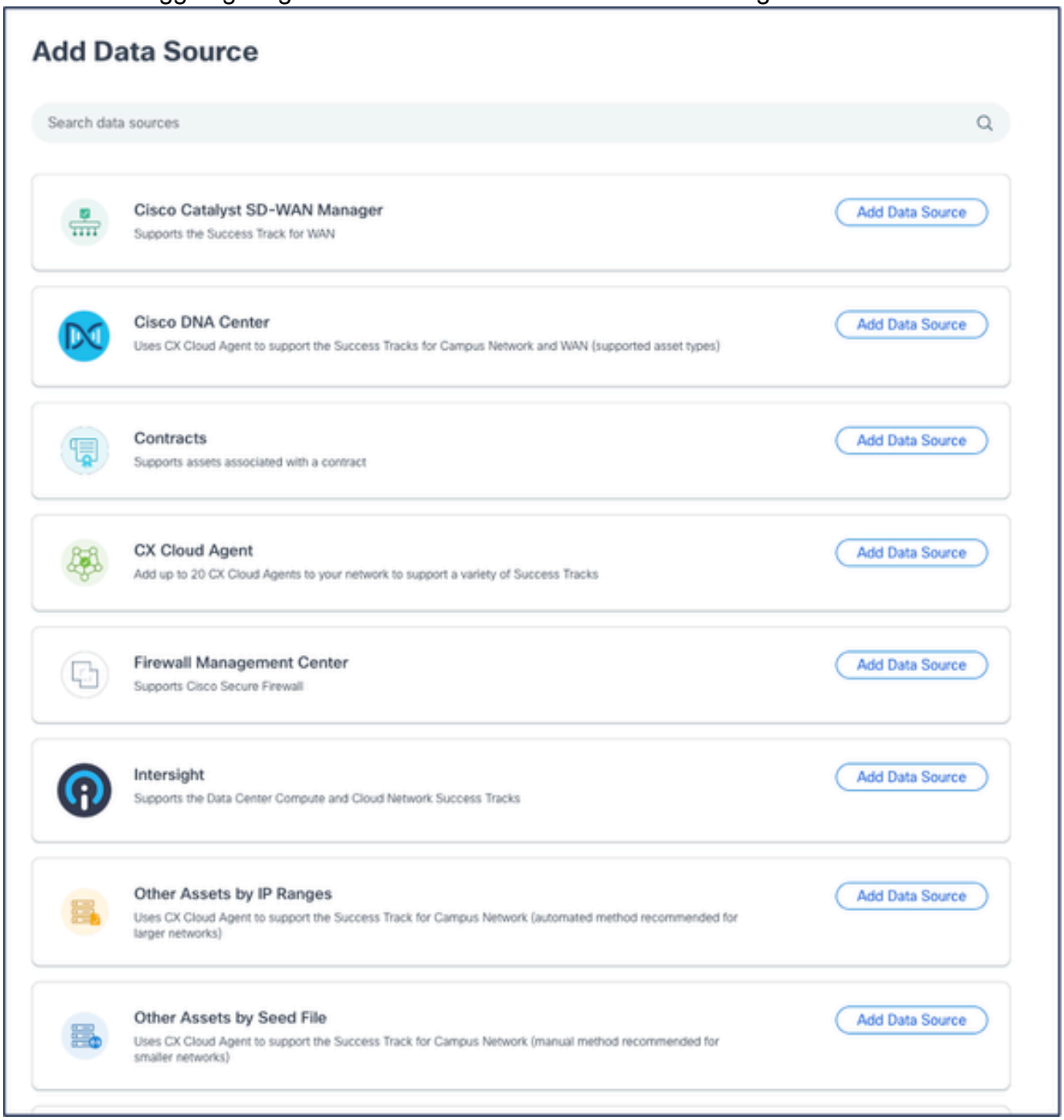
Installazione e associazione con la macchina virtuale

10. Immettere il codice di associazione ricevuto dopo la distribuzione del file OVA scaricato.
11. Fare clic su Continue (Continua). Viene visualizzato lo stato della registrazione, seguito da una conferma.

Aggiunta di Cisco DNA Center come origine dati

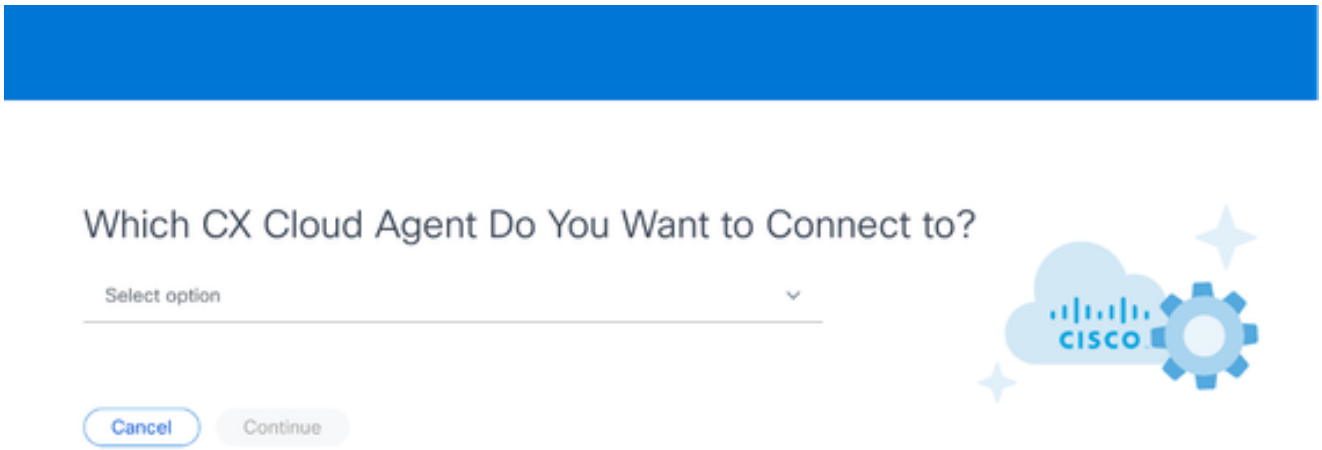
Per aggiungere Cisco DNA Center come origine dati:

1. Fare clic su Aggiungi origine dati nella finestra Admin Center > Origini dati.



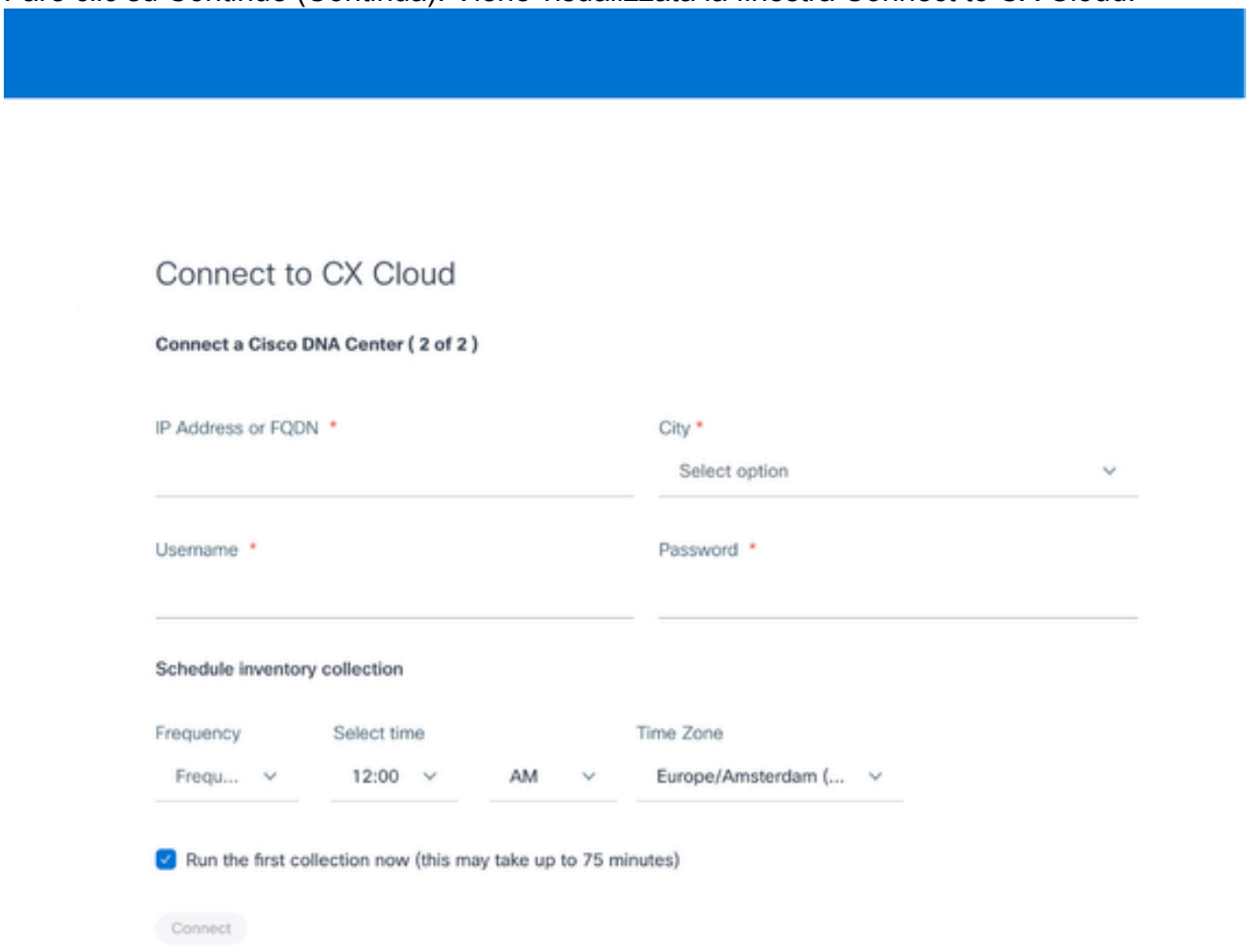
Aggiungi origine dati

2. Fare clic su Add Data Source (Aggiungi origine dati) dall'opzione Cisco DNA Center.



Seleziona agente cloud CX

3. Selezionare l'agente cloud CX dall'elenco a discesa Quale agente cloud CX si desidera connettere a.
4. Fare clic su Continue (Continua). Viene visualizzata la finestra Connect to CX Cloud.



Connetti a CX Cloud

5. Immettere quanto segue in Connect a Cisco DNA Center:
    - Indirizzo IP virtuale o FQDN (ad esempio, indirizzo IP di Cisco DNA Center),
    - Città (ossia la località del Cisco DNA Center),
    - Username
    - Password
    - Frequenza, ora e fuso orario per indicare la frequenza con cui l'agente cloud CX deve eseguire scansioni di rete nelle sezioni Pianifica raccolta inventario
      Nota: selezionare la casella di controllo Esegui la prima raccolta adesso per eseguire la raccolta adesso.

6. Fare clic su Connetti. Viene visualizzata una conferma con l'indirizzo IP del Cisco DNA Center.

Aggiunta di altri cespiti come origini dati

La raccolta di dati di telemetria è stata estesa ai dispositivi non gestiti dal Cisco DNA Center, consentendo ai clienti di visualizzare e interagire con dati di analisi e informazioni derivati dalla telemetria per una gamma più ampia di dispositivi. Dopo la configurazione iniziale dell'agente cloud CX, gli utenti hanno la possibilità di configurare l'agente cloud CX per la connessione a 20 ulteriori Cisco DNA Center all'interno dell'infrastruttura monitorata da CX Cloud.

Gli utenti possono identificare i dispositivi da incorporare in CX Cloud identificando in modo univoco tali dispositivi utilizzando un file di inizializzazione o specificando un intervallo IP, che può essere analizzato dall'agente di CX Cloud. Entrambi gli approcci si basano sul protocollo SNMP (Simple Network Management Protocol) per il rilevamento (SNMP) e su SSH (Secure Shell) per la connettività. Questi devono essere configurati correttamente per abilitare la raccolta di telemetria.

Per aggiungere altri cespiti come origini dati:

- Caricare un file di origine utilizzando un modello di file di origine.
- Specificare un intervallo di indirizzi IP.

Protocolli di rilevamento

Sia il rilevamento diretto di dispositivi basato su file che il rilevamento basato su intervalli IP si basano sul protocollo SNMP come protocollo di rilevamento. Esistono diverse versioni di SNMP, ma l'agente cloud CX supporta SNMPV2c e SNMP V3 ed è possibile configurare una o entrambe le versioni. Le stesse informazioni, descritte più avanti in dettaglio, devono essere fornite dall'utente per completare la configurazione e abilitare la connettività tra il dispositivo gestito da SNMP e il gestore del servizio SNMP.

SNMPV2c e SNMPV3 differiscono in termini di sicurezza e modello di configurazione remota. SNMPV3 utilizza un sistema avanzato di protezione crittografica che supporta la crittografia SHA per autenticare i messaggi e garantirne la privacy. Si consiglia di utilizzare il protocollo SNMPv3 su tutte le reti pubbliche e connesse a Internet per proteggere il sistema da rischi e minacce alla sicurezza. Su CX Cloud, è preferibile configurare SNMPv3 e non SNMPv2c, ad eccezione dei

dispositivi legacy meno recenti che non dispongono del supporto integrato per SNMPv3. Se entrambe le versioni di SNMP sono configurate dall'utente, l'agente cloud CX può, per impostazione predefinita, tentare di comunicare con ciascun dispositivo utilizzando SNMPv3 e tornare a SNMPv2c se la comunicazione non può essere negoziata correttamente.

Protocolli di connettività

Nell'ambito della configurazione della connettività diretta del dispositivo, gli utenti devono specificare i dettagli del protocollo di connettività del dispositivo: SSH (o, in alternativa, telnet). È possibile usare SSHv2, tranne nel caso di singoli asset legacy che non dispongono del supporto integrato appropriato. Tenere presente che il protocollo SSHv1 contiene vulnerabilità fondamentali. In assenza di ulteriore sicurezza, i dati di telemetria e le attività sottostanti possono essere compromessi a causa di queste vulnerabilità quando ci si affida a SSHv1. Anche Telnet non è sicuro. Le informazioni sulle credenziali (nomi utente e password) inviate tramite telnet non vengono crittografate e pertanto possono essere compromesse in assenza di ulteriore protezione.

Limitazione dell'elaborazione telematica per i dispositivi

Di seguito sono riportate le limitazioni relative all'elaborazione dei dati di telemetria per i dispositivi:

- Alcuni dispositivi possono essere visualizzati come raggiungibili nel Riepilogo raccolta ma non sono visibili nella pagina Risorse cloud CX. Le limitazioni della strumentazione del dispositivo impediscono l'elaborazione della telemetria di tali dispositivi.
- Se un dispositivo delle raccolte di file di origine o di intervalli IP fa anche parte dell'inventario di Cisco DNA Center, il dispositivo viene segnalato solo una volta per la voce di Cisco DNA Center. I rispettivi dispositivi all'interno della voce del file di inizializzazione/intervallo IP vengono ignorati per evitare la duplicazione.

Aggiunta di altri cespiti mediante un file di inizializzazione

Un file di origine è un file con estensione csv in cui ogni riga rappresenta un record di dati di sistema. In un file di inizializzazione, ogni record del file di inizializzazione corrisponde a un dispositivo univoco dal quale la telemetria può essere raccolta dall'agente cloud CX. Tutti i messaggi di errore o di informazione relativi a ciascuna voce di dispositivo del file di origine da importare vengono acquisiti come parte dei dettagli del log del processo. Tutti i dispositivi in un file di inizializzazione sono considerati dispositivi gestiti, anche se non sono raggiungibili al momento della configurazione iniziale. Nel caso in cui venga caricato un nuovo file di origine per sostituire un file precedente, la data dell'ultimo caricamento viene visualizzata in CX Cloud.

L'agente cloud CX può tentare di connettersi ai dispositivi, ma non può elaborarli singolarmente per visualizzarli nelle pagine Asset nei casi in cui non è in grado di determinare i PID o i numeri di serie. Qualsiasi riga nel file di origine che inizia con un punto e virgola viene ignorata. La riga di intestazione nel file di origine inizia con un punto e virgola e può essere mantenuta invariata (opzione consigliata) o eliminata durante la creazione del file di origine del cliente.

È importante che il formato del file di inizializzazione di esempio, incluse le intestazioni di colonna, non venga alterato in alcun modo. Fare clic sul collegamento fornito per visualizzare un file di

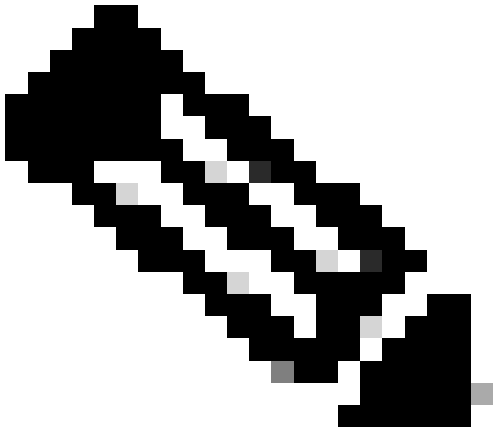
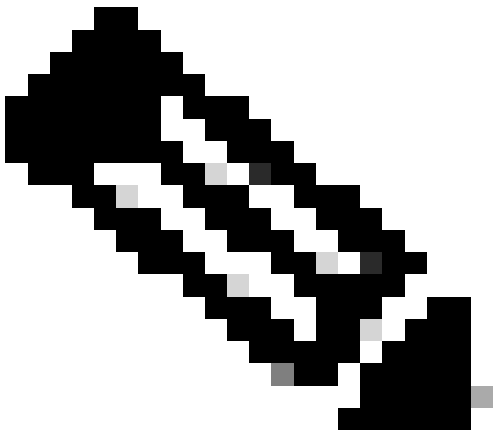
origine in formato PDF. Questo PDF è solo a scopo di riferimento e può essere utilizzato per creare un file di origine che deve essere salvato in formato .csv.

Fare clic su questo collegamento per visualizzare un file di origine che può essere utilizzato per creare un file di origine in formato CSV.

Nota: questo PDF è solo a scopo di riferimento e può essere utilizzato per creare un file di origine che deve essere salvato in formato CSV.

Questa tabella identifica tutte le colonne necessarie del file di partenza e i dati da includere in ogni colonna.

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
A	Indirizzo IP o nome host	Specificare un indirizzo IP o un nome host valido e univoco per il dispositivo.
B	Versione protocollo SNMP	Il protocollo SNMP è richiesto dall'agente cloud CX e viene utilizzato per il rilevamento dei dispositivi all'interno della rete del cliente. I valori possono essere snmpv2c o snmpv3, ma per motivi di sicurezza è consigliabile utilizzare snmpv3.
C	snmpRo : obbligatorio se col#=3 è selezionato come 'snmpv2c'	Se la variante legacy di SNMPv2 è selezionata per un dispositivo specifico, è necessario specificare le credenziali snmpRO (sola lettura) per la raccolta SNMP del dispositivo. In caso contrario, l'immissione può essere vuota.
D	snmpv3UserName : obbligatorio se col#=3 è selezionato come 'snmpv3'	Se si seleziona SNMPv3 per comunicare con un dispositivo specifico, è necessario fornire il nome utente per l'accesso.
S	snmpv3AuthAlgorithm: i valori possono essere MD5 o SHA	Il protocollo SNMPv3 consente l'autenticazione tramite l'algoritmo MD5 o SHA. Se il dispositivo è configurato con l'autenticazione protetta, è necessario fornire il rispettivo algoritmo di autenticazione.

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
		 Nota: MD5 è considerato non sicuro e può essere utilizzato su tutti i dispositivi che lo supportano.
F	snmpv3AuthPassword: password	Se sul dispositivo è configurato un algoritmo di crittografia MD5 o SHA, è necessario fornire la password di autenticazione appropriata per l'accesso al dispositivo.
G	snmpv3PrivAlgorithm: i valori possono essere DES, 3DES	Se il dispositivo è configurato con l'algoritmo per la privacy SNMPv3 (questo algoritmo viene utilizzato per crittografare la risposta), è necessario fornire il rispettivo algoritmo. 

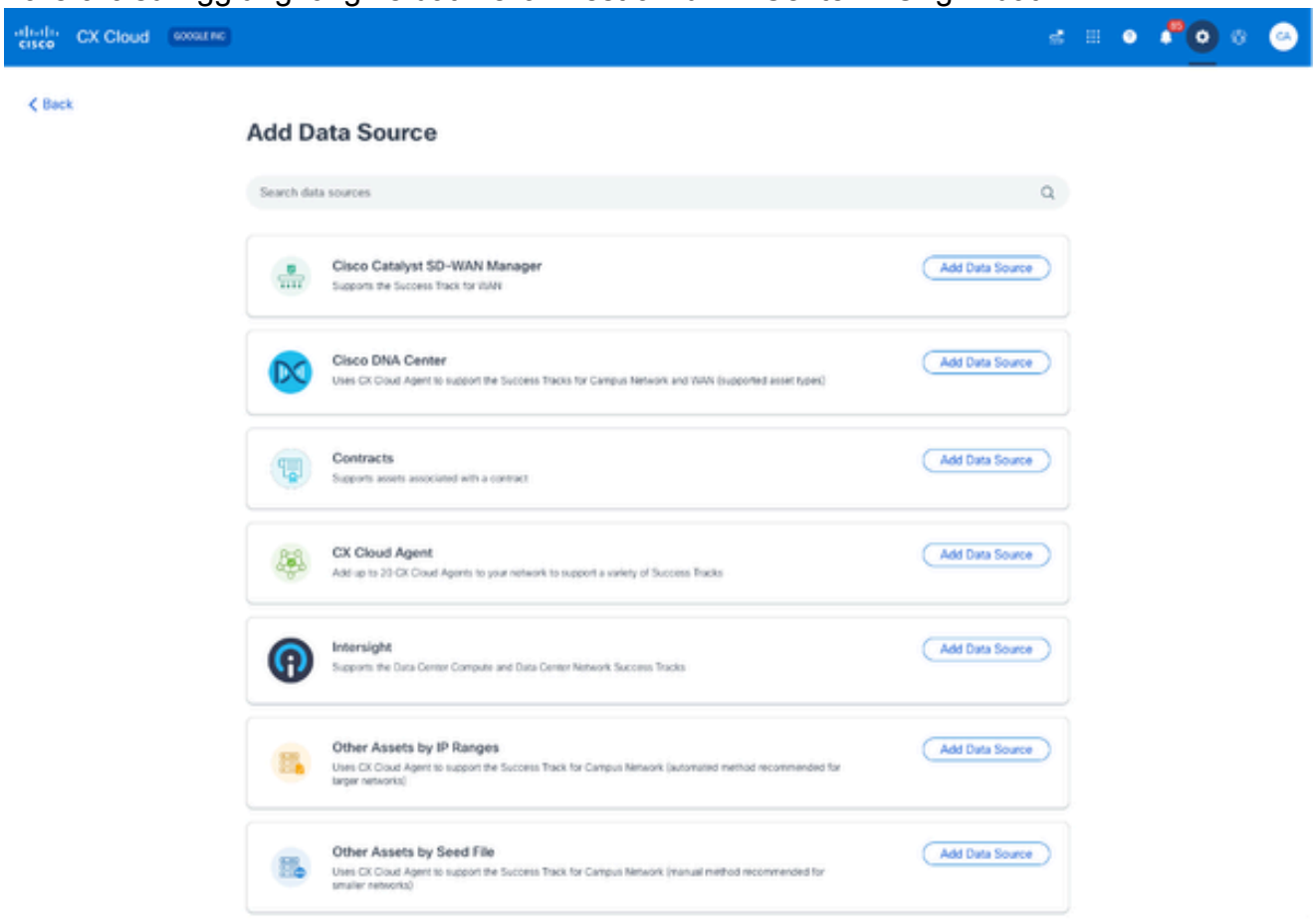
Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
		Nota: le chiavi a 56 bit utilizzate da DES sono considerate troppo brevi per garantire la protezione crittografica e 3DES può essere utilizzato su tutti i dispositivi che lo supportano.
H	snmpv3PrivPassword: password	Se l'algoritmo per la privacy SNMPv3 è configurato sul dispositivo, è necessario fornire la rispettiva password per la privacy per la connessione al dispositivo.
I	snmpv3EngineId : engineID, ID univoco che rappresenta il dispositivo. Specificare l'ID del motore se configurato manualmente nel dispositivo	L'ID motore SNMPv3 è un ID univoco che rappresenta ciascun dispositivo. Questo ID motore viene inviato come riferimento durante la raccolta dei dataset SNMP da parte dell'agente cloud CX. Se il cliente configura il EngineID manualmente, è necessario fornire il relativo EngineID.
J	cliProtocol: i valori possono essere 'telnet', 'sshv1', 'sshv2'. Se vuoto, è possibile impostare 'sshv2' per impostazione predefinita	La CLI ha lo scopo di interagire direttamente con il dispositivo. CX Cloud Agent utilizza questo protocollo per la raccolta CLI per un dispositivo specifico. Questi dati di raccolta CLI vengono utilizzati per il reporting di asset e altre informazioni approfondite all'interno di CX Cloud. Si consiglia SSHv2; in assenza di altre misure di sicurezza della rete, i protocolli SSHv1 e Telnet non garantiscono un'adeguata sicurezza del trasporto.
K	cliPort : numero porta protocollo CLI	Se si seleziona un protocollo CLI, è necessario fornire il relativo numero di porta. Ad esempio, 22 per SSH e 23 per telnet.
L	cliUser : nome utente CLI (è possibile specificare nome	È necessario fornire il nome utente CLI corrispondente del dispositivo. Viene utilizzato

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
	utente/password CLI o ENTRAMBI, MA le colonne (col#=12 e col#=13) non possono essere vuote.)	dall'agente cloud CX al momento della connessione al dispositivo durante la raccolta CLI.
M	cliPassword : password utente CLI (è possibile specificare nome utente/password CLI o BOTH, MA le colonne (col#=12 e col#=13) non possono essere vuote.)	È necessario fornire la password CLI corrispondente del dispositivo. Viene utilizzato dall'agente cloud CX al momento della connessione al dispositivo durante la raccolta CLI.
N	cliAttivaUtente	Se sul dispositivo è configurato enable, è necessario fornire il valore enableUsername del dispositivo.
O	cliAttivaPassword	Se sul dispositivo è configurato enable, è necessario fornire il valore enablePassword del dispositivo.
P	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro
Q	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro
R	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro
S	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro

Aggiunta di altri cespiti mediante un nuovo file di origine

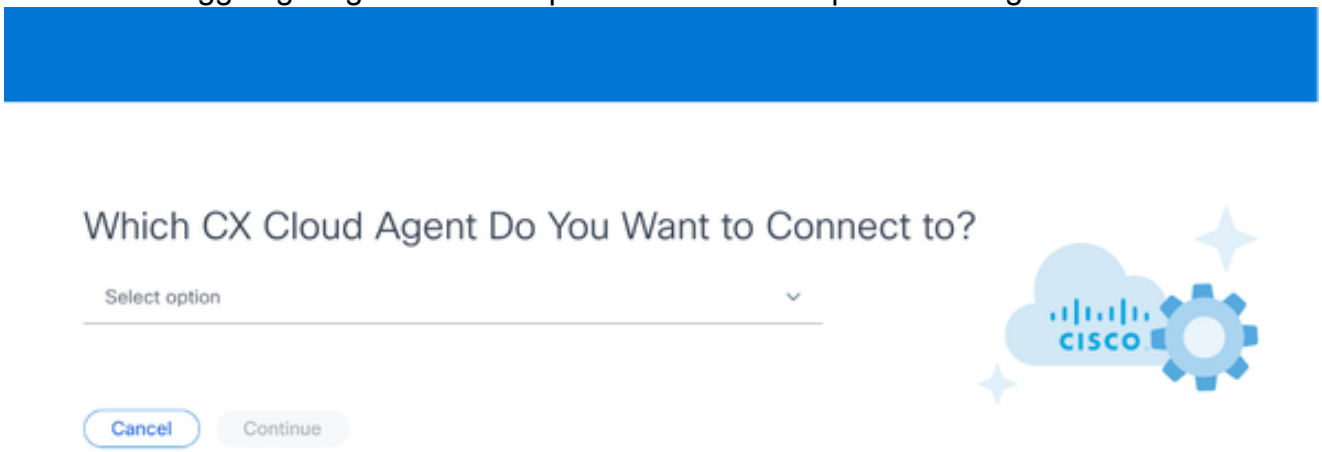
Per aggiungere altri cespiti utilizzando un nuovo file di origine:

1. Fare clic su Aggiungi origine dati nella finestra Admin Center > Origini dati.



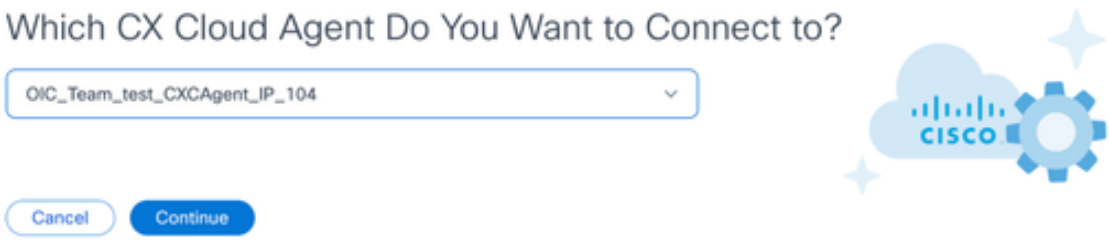
Aggiungi origine dati

2. Fare clic su Aggiungi origine dati dall'opzione Altre risorse per file di origine.



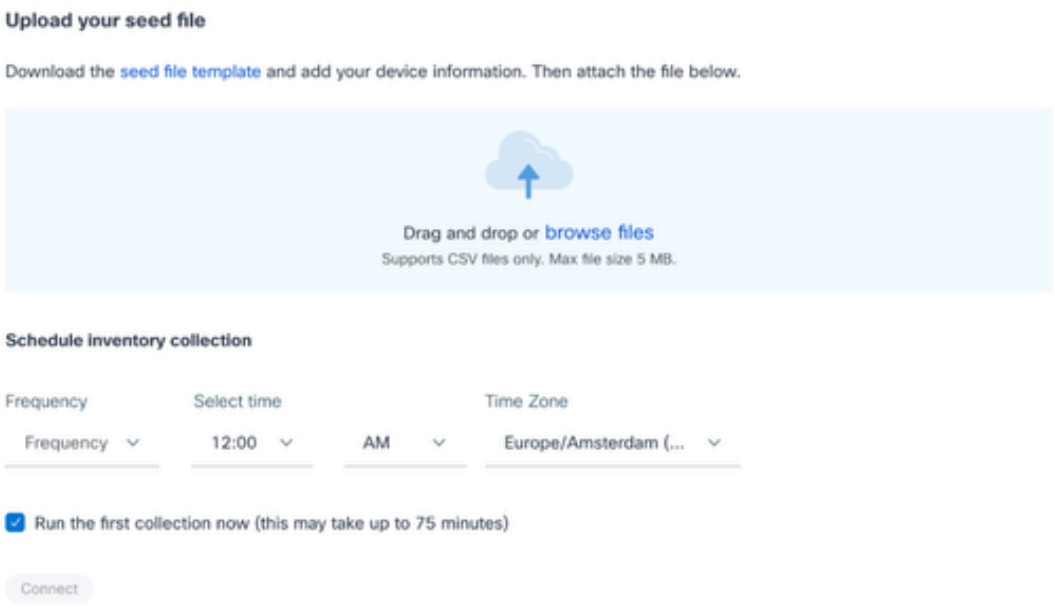
Seleziona agente cloud CX

3. Selezionare l'agente cloud CX dall'elenco a discesa Quale agente cloud CX si desidera connettere a.



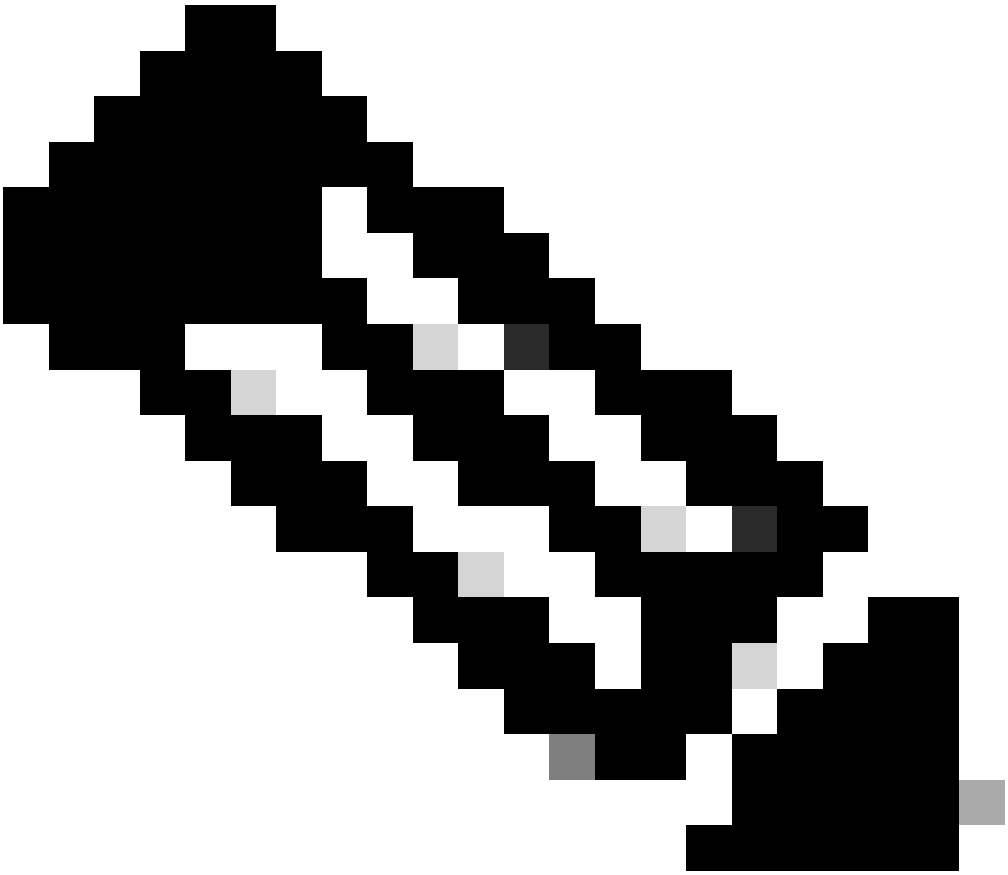
Continua

4. Fare clic su Continue (Continua). Viene visualizzata la pagina Carica file di inizializzazione.



Carica il file di inizializzazione

5. Fare clic sul modello di file di origine con collegamenti ipertestuali per scaricarlo.
6. Immettere o importare manualmente i dati nel file. Al termine, salvare il modello come file .csv per importare il file in CX Cloud Agent.
7. Trascinare o fare clic su Sfoglia file per caricare il file CSV.
8. Completare la sezione Pianifica raccolta scorte.



Nota: prima che la configurazione iniziale di CX Cloud sia completata, l'agente deve eseguire la prima raccolta di telemetria elaborando il file di inizializzazione e stabilendo la connessione con tutti i dispositivi identificati. La raccolta può essere avviata su richiesta o eseguita in base a una pianificazione definita qui. Gli utenti possono eseguire la prima connessione di telemetria selezionando la casella di controllo Esegui la prima raccolta. A seconda del numero di voci specificate nel file di inizializzazione e di altri fattori, questo processo può richiedere molto tempo.

9. Fare clic su Connetti. Viene visualizzata la finestra Origini dati, contenente un messaggio di conferma.

Aggiunta di altri cespiti mediante un file di partenza modificato

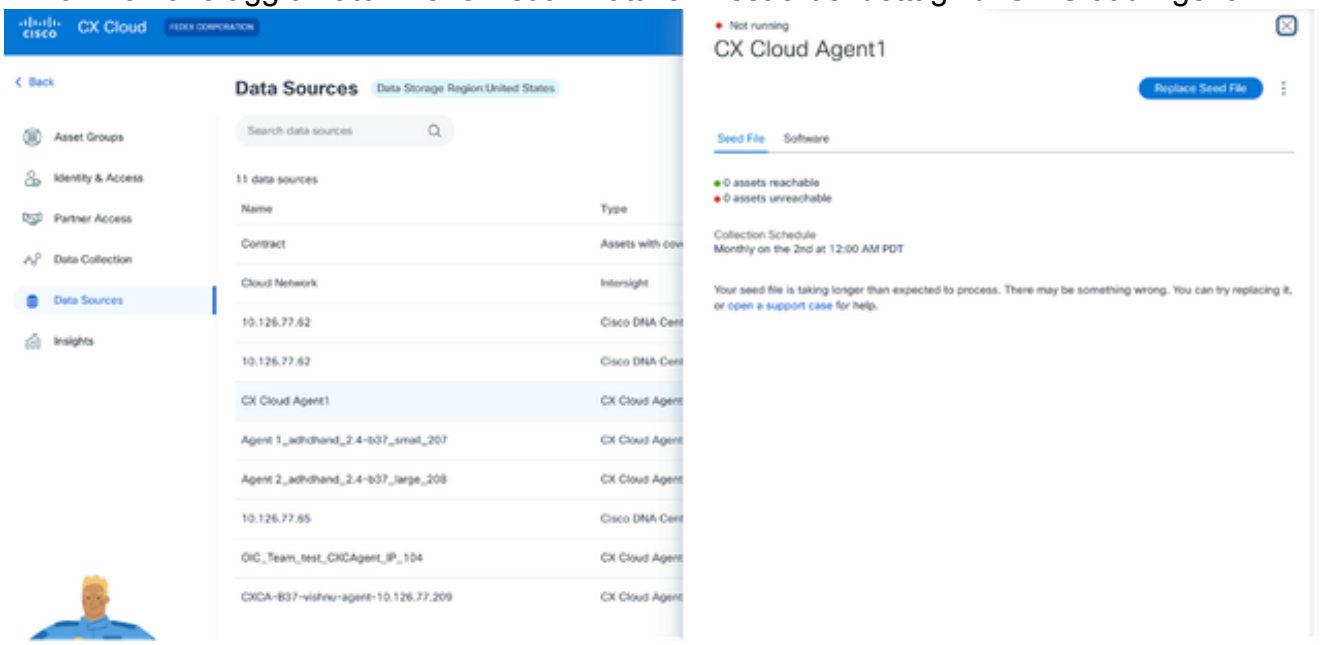
Per aggiungere, modificare o eliminare dispositivi utilizzando il file di origine corrente:

1. Aprite il file di origine creato in precedenza, apportate le modifiche necessarie e salvate il file.

Nota: per aggiungere cespiti al file di origine, aggiungete tali cespiti al file di origine

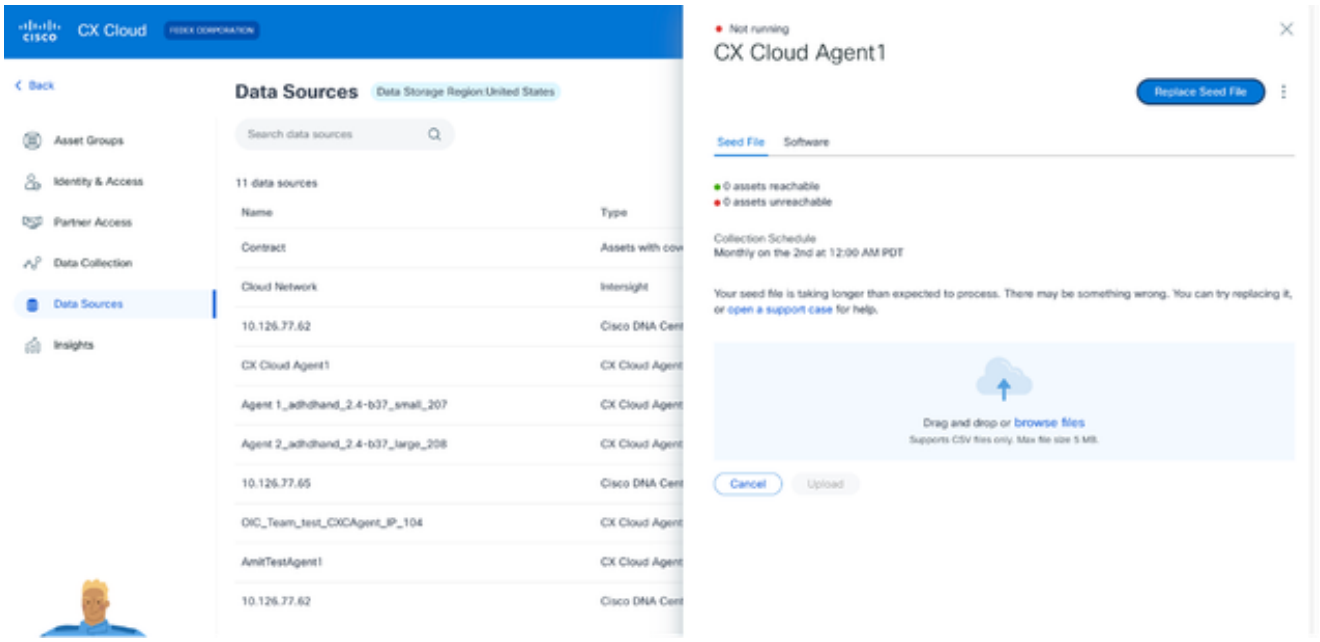
creato in precedenza e ricaricate il file. Questa operazione è necessaria in quanto il caricamento di un nuovo file di inizializzazione sostituisce il file di inizializzazione corrente. Per l'individuazione e la raccolta viene utilizzato solo l'ultimo file di inizializzazione caricato.

2. Dalla pagina Origini dati, fare clic sull'origine dati dell'agente cloud CX che richiede un file di inizializzazione aggiornato. Viene visualizzata la finestra dei dettagli di CX Cloud Agent.



Finestra Dettagli agente cloud CX

3. Fare clic su Sostituisci file di inizializzazione.



Finestra di CX Cloud Agent

4. Trascinare o fare clic su Sfoglia file per caricare il file di origine modificato.
5. Fare clic su Upload.

Aggiungi altre risorse utilizzando gli intervalli IP

Gli intervalli IP consentono agli utenti di identificare le risorse hardware e, di conseguenza, di raccogliere la telemetria da tali dispositivi in base agli indirizzi IP. I dispositivi per la raccolta di telemetria possono essere identificati in modo univoco specificando un singolo intervallo IP a livello di rete, che può essere analizzato dall'agente cloud CX utilizzando il protocollo SNMP. Se l'intervallo IP viene scelto per identificare un dispositivo connesso direttamente, gli indirizzi IP a cui si fa riferimento possono essere il più restrittivi possibile, consentendo al tempo stesso la copertura per tutti gli asset necessari.

- È possibile specificare indirizzi IP specifici oppure utilizzare caratteri jolly per sostituire gli ottetti di un indirizzo IP e creare un intervallo.
- Se uno specifico indirizzo IP non è incluso nell'intervallo IP identificato durante l'installazione, l'agente cloud CX non tenta di comunicare con un dispositivo che dispone di tale indirizzo IP, né raccoglie dati di telemetria da tale dispositivo.
- L'immissione di *.*.*.* consente all'agente cloud CX di utilizzare le credenziali fornite dall'utente con qualsiasi IP. Ad esempio: 172.16.*.* consente di utilizzare le credenziali per tutti i dispositivi della subnet 172.16.0.0/16.
- In caso di modifiche alla rete o alla base installata, è possibile modificare l'intervallo IP. Fare riferimento alla sezione Modifica degli intervalli IP

L'agente cloud CX tenterà di connettersi ai dispositivi, ma potrebbe non essere in grado di elaborarli singolarmente per visualizzarli nella visualizzazione Asset nei casi in cui non è in grado di determinare i PID o i numeri di serie.

Note:
Facendo clic su Modifica intervallo indirizzi IP viene avviato il rilevamento dei dispositivi su richiesta. Quando un nuovo dispositivo viene aggiunto o eliminato (all'interno o all'esterno) a un intervallo IP specificato, il cliente deve sempre fare clic su Modifica intervallo indirizzi IP (fare riferimento alla sezione Modifica degli intervalli IP) e completare i passaggi richiesti per avviare il rilevamento dei dispositivi su richiesta per includere qualsiasi dispositivo appena aggiunto all'inventario della raccolta dell'agente cloud CX.

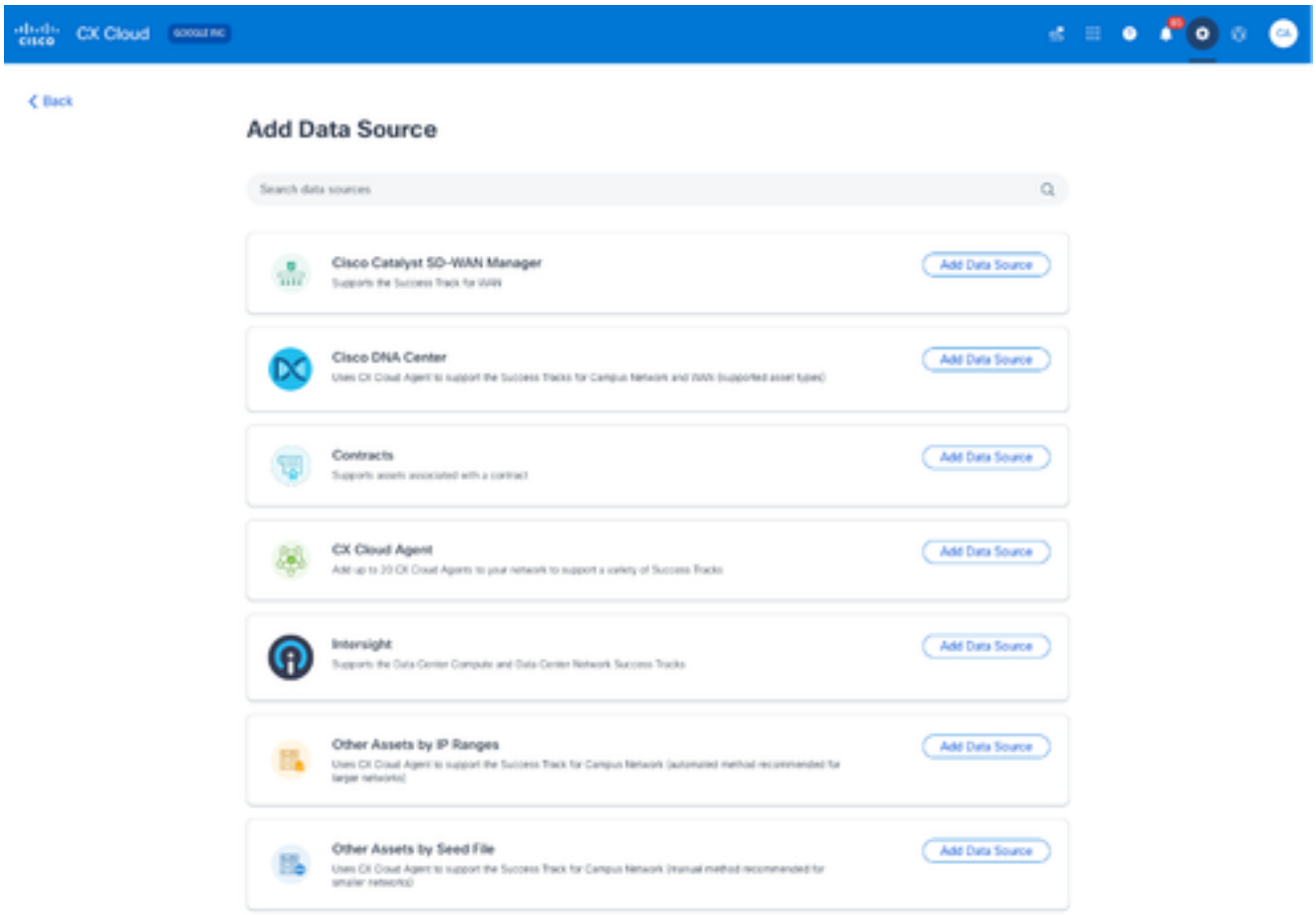
L'aggiunta di dispositivi tramite un intervallo IP richiede che gli utenti specifichino tutte le credenziali applicabili tramite l'interfaccia utente di configurazione. I campi visibili variano a seconda dei protocolli selezionati nelle finestre precedenti. Se si selezionano più protocolli per lo stesso protocollo, ad esempio SNMPv2c e SNMPv3 o SSHv2 e SSHv1, l'agente cloud CX negozia automaticamente la selezione del protocollo in base alle funzionalità del singolo dispositivo.

Quando si collegano i dispositivi con indirizzi IP, il cliente deve accertarsi che tutti i protocolli pertinenti nell'intervallo IP, insieme alle versioni SSH e alle credenziali Telnet, siano validi o che le connessioni non riescano.

Aggiunta di altre risorse in base agli intervalli IP

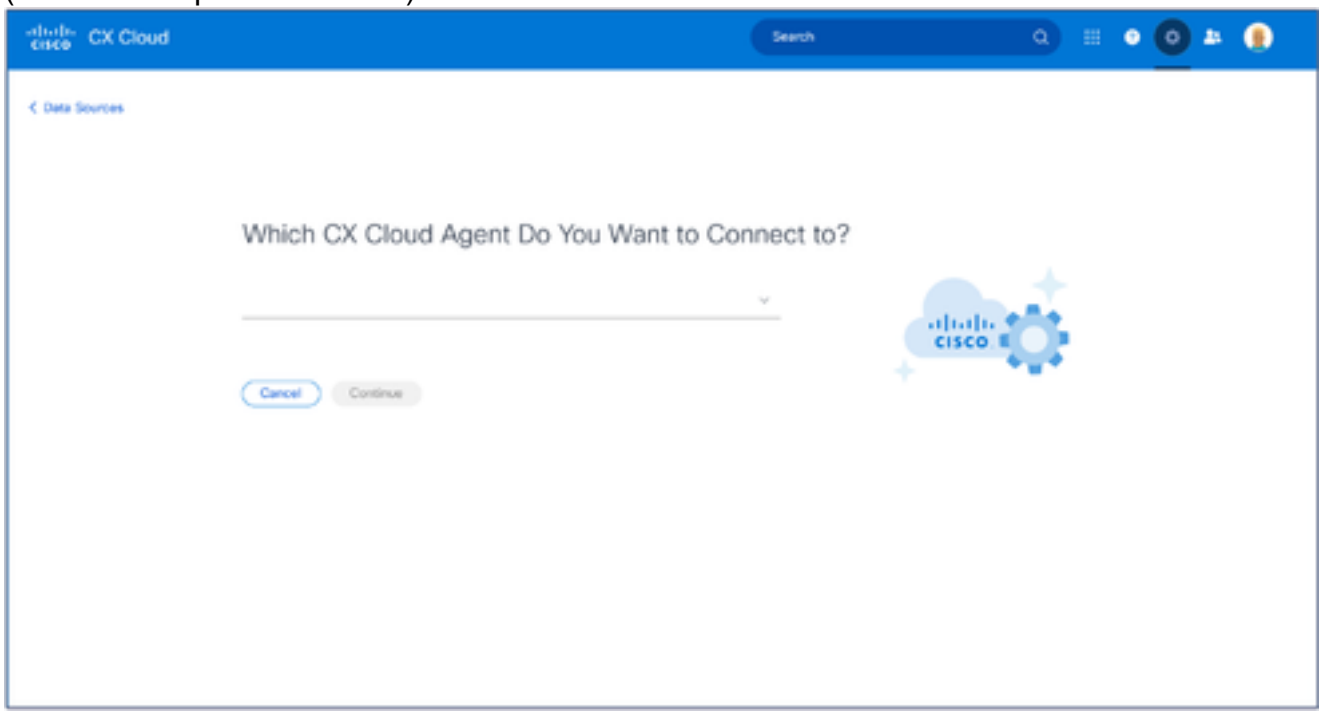
Per aggiungere dispositivi utilizzando l'intervallo IP:

1. Fare clic su Aggiungi origine dati nella finestra Admin Center > Origini dati.



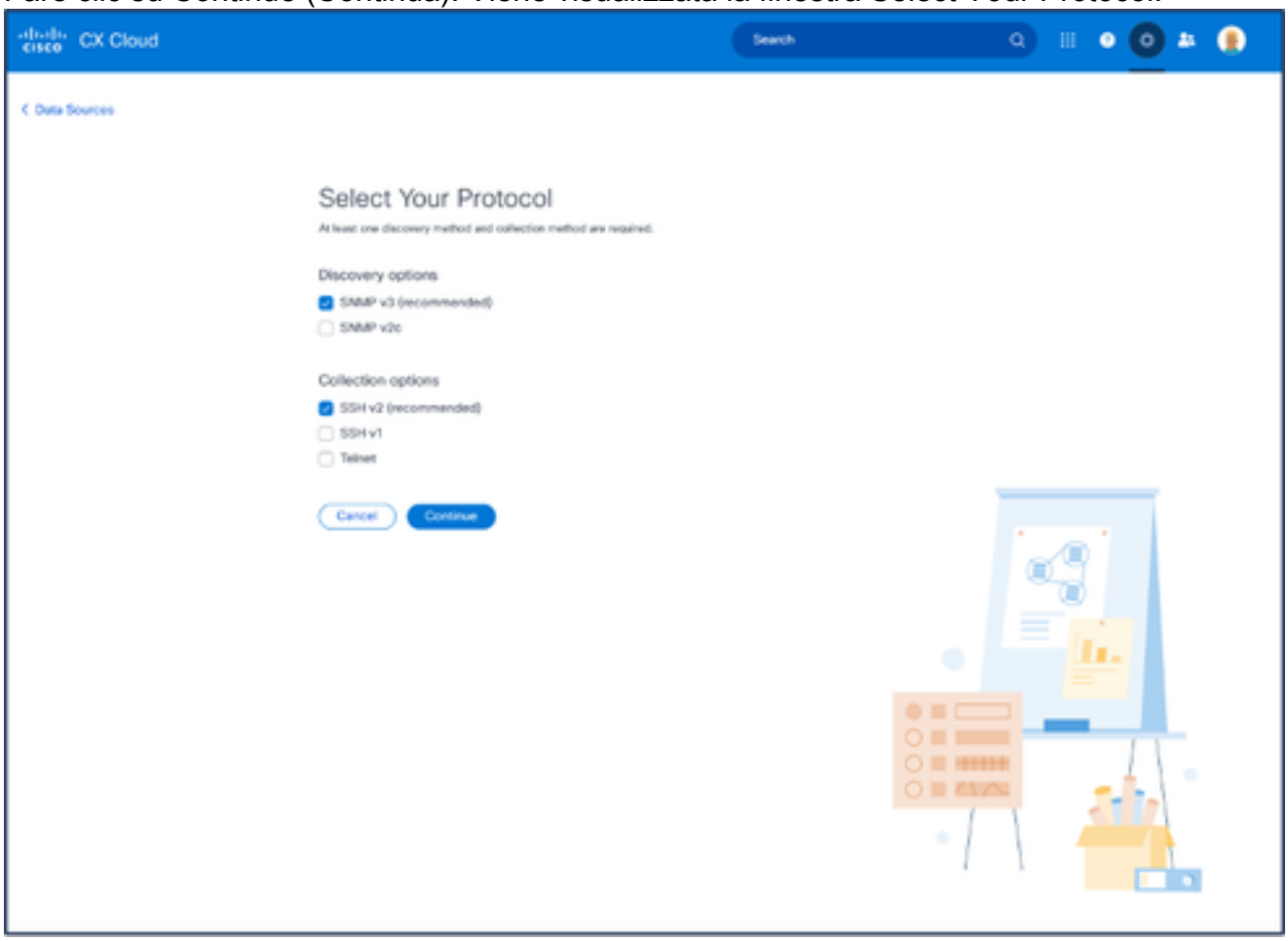
Aggiungi origini dati

2. Fare clic su Add Data Source (Aggiungi origine dati) nell'opzione Other Assets by IP Ranges (Altre risorse per intervalli IP).



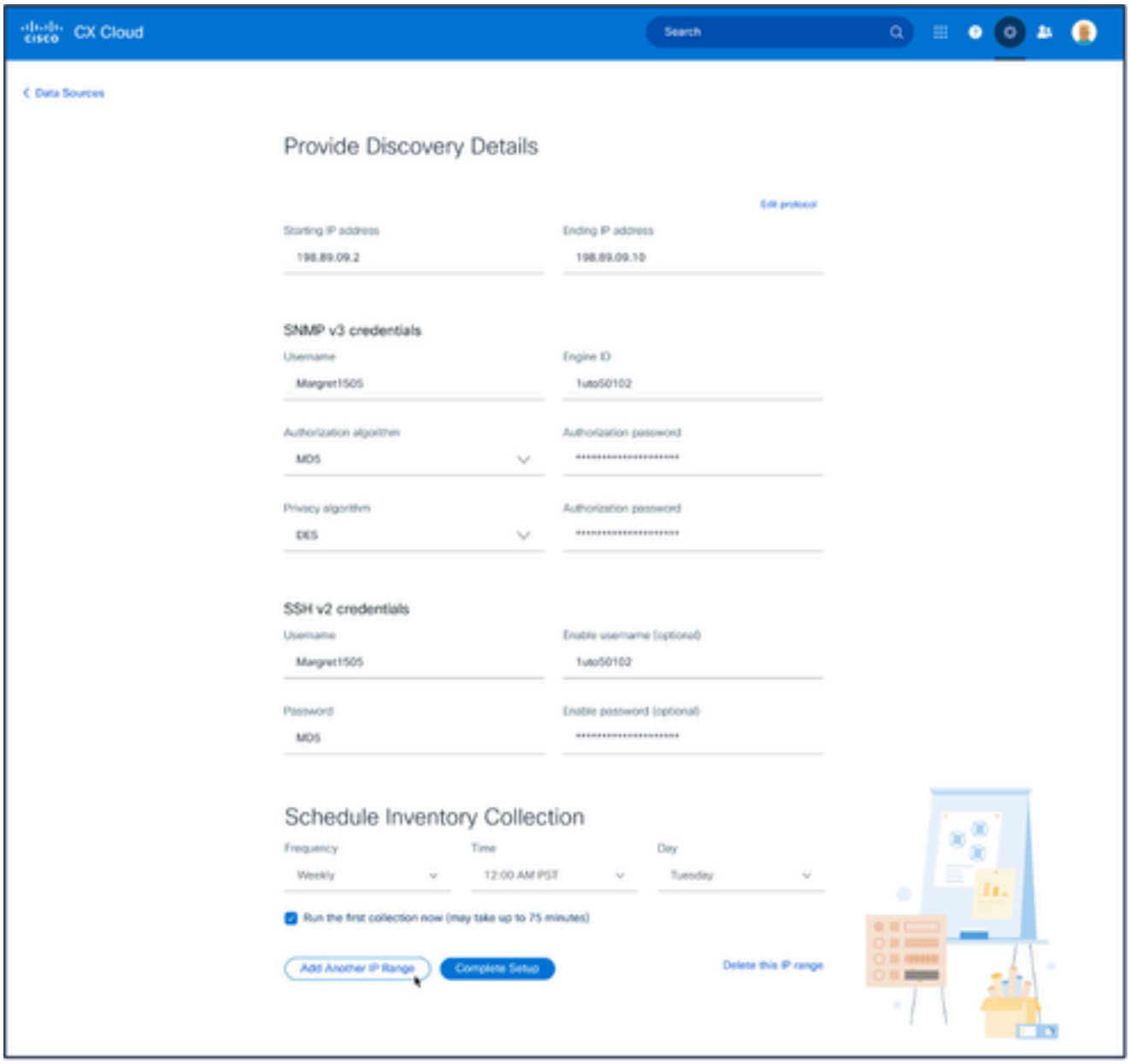
Seleziona agente cloud CX

3. Selezionare l'agente cloud CX dall'elenco a discesa Quale agente cloud CX si desidera connettere a.
4. Fare clic su Continue (Continua). Viene visualizzata la finestra Select Your Protocol.



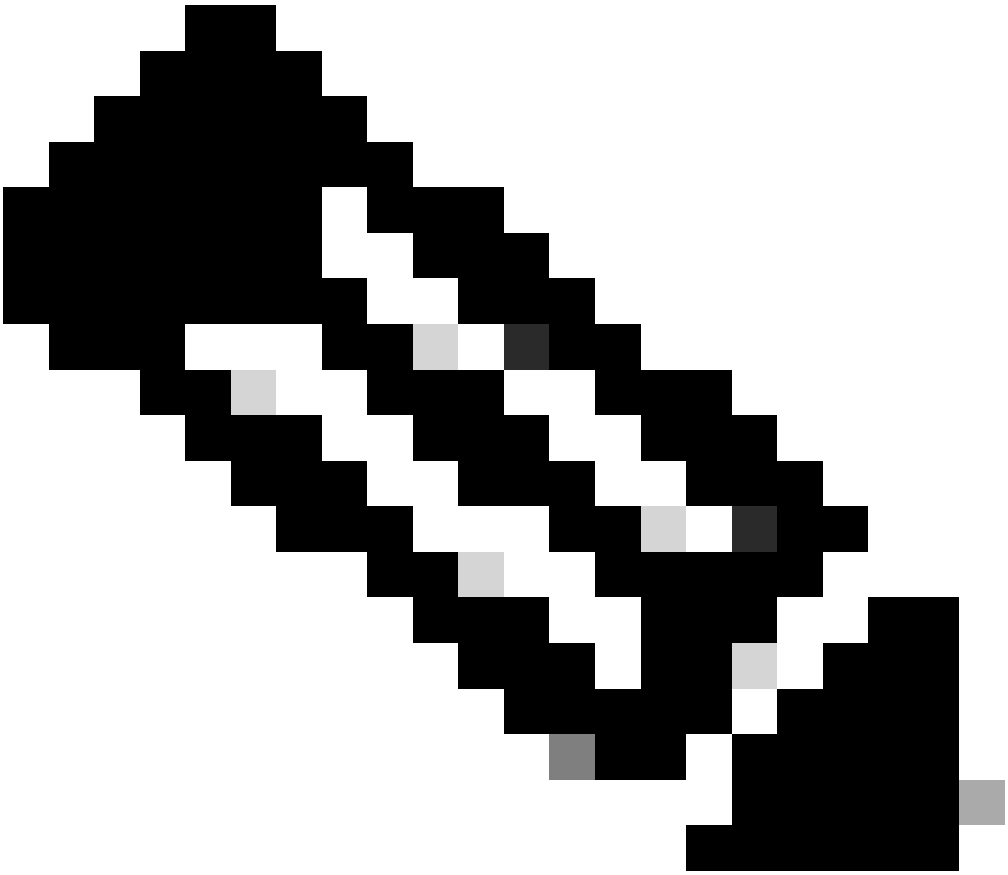
Selezionare il protocollo

5. Selezionare le caselle di controllo appropriate per le opzioni di individuazione e raccolta.
6. Fare clic su Continue (Continua).



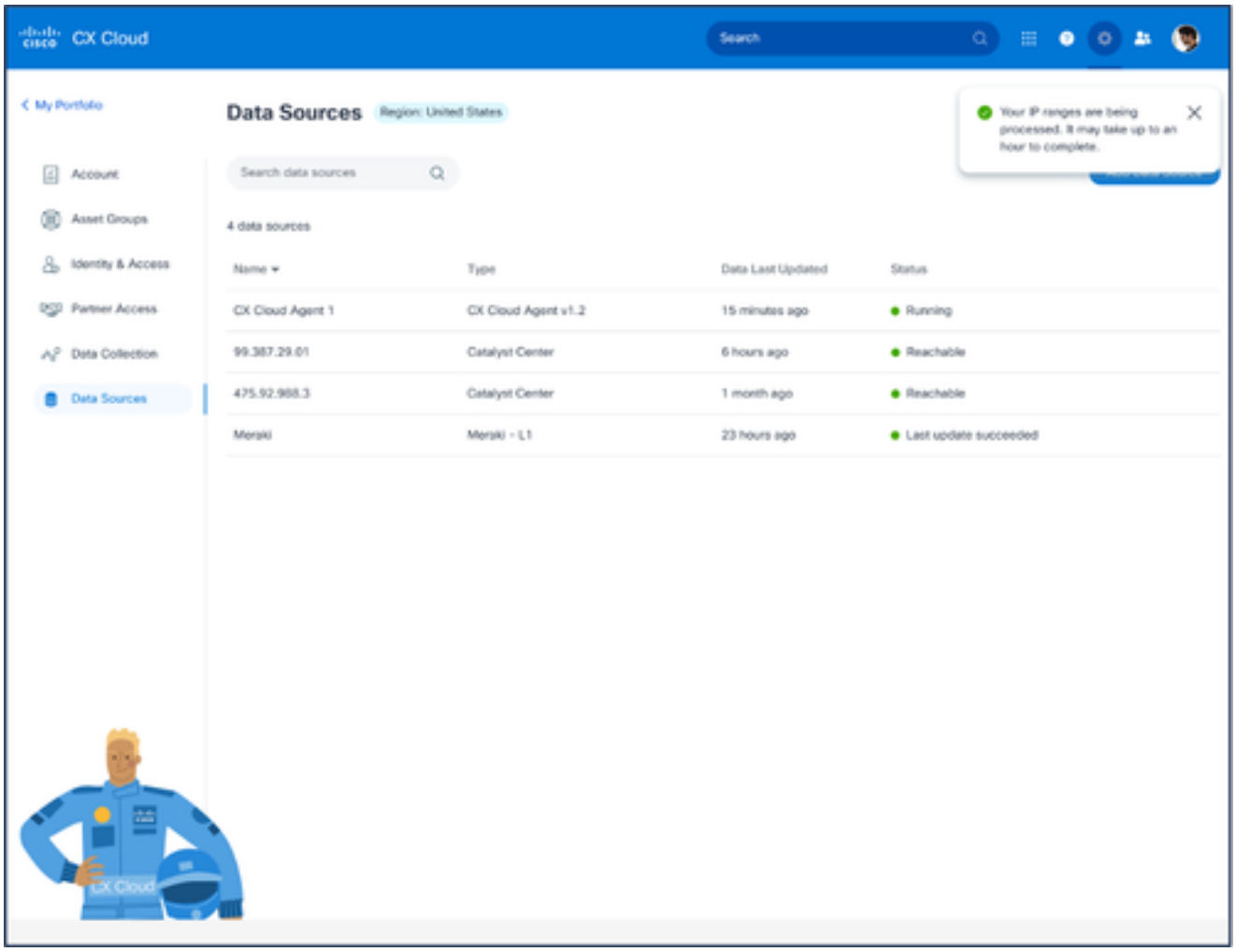
Fornire i dettagli di individuazione e pianificare le sezioni di raccolta dell'inventario

7. Immettere i dettagli richiesti nelle sezioni Specifica dettagli individuazione e Pianifica raccolta scorte.



Nota: per aggiungere un altro intervallo IP per l'agente cloud CX selezionato, fare clic su Aggiungi un altro intervallo IP per tornare alla finestra Imposta protocollo e ripetere i passaggi descritti in questa sezione.

8. Fare clic su Completa impostazione. Una volta completata la distribuzione, viene visualizzata una conferma.

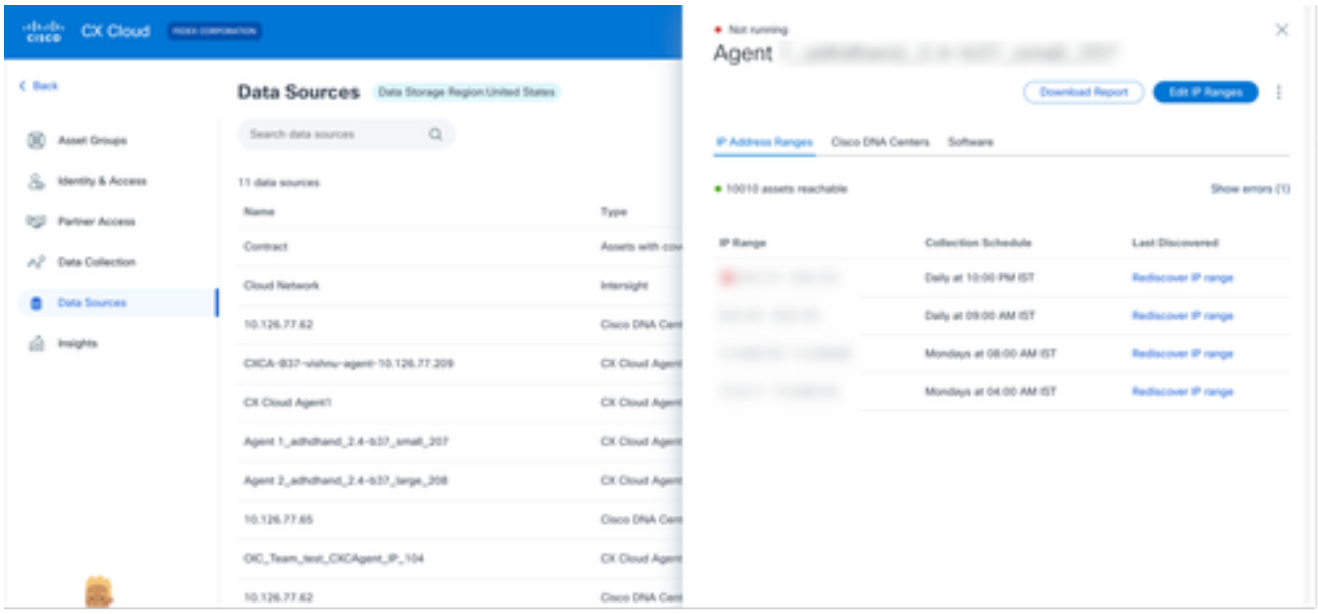


Messaggio di conferma

Modifica degli intervalli IP

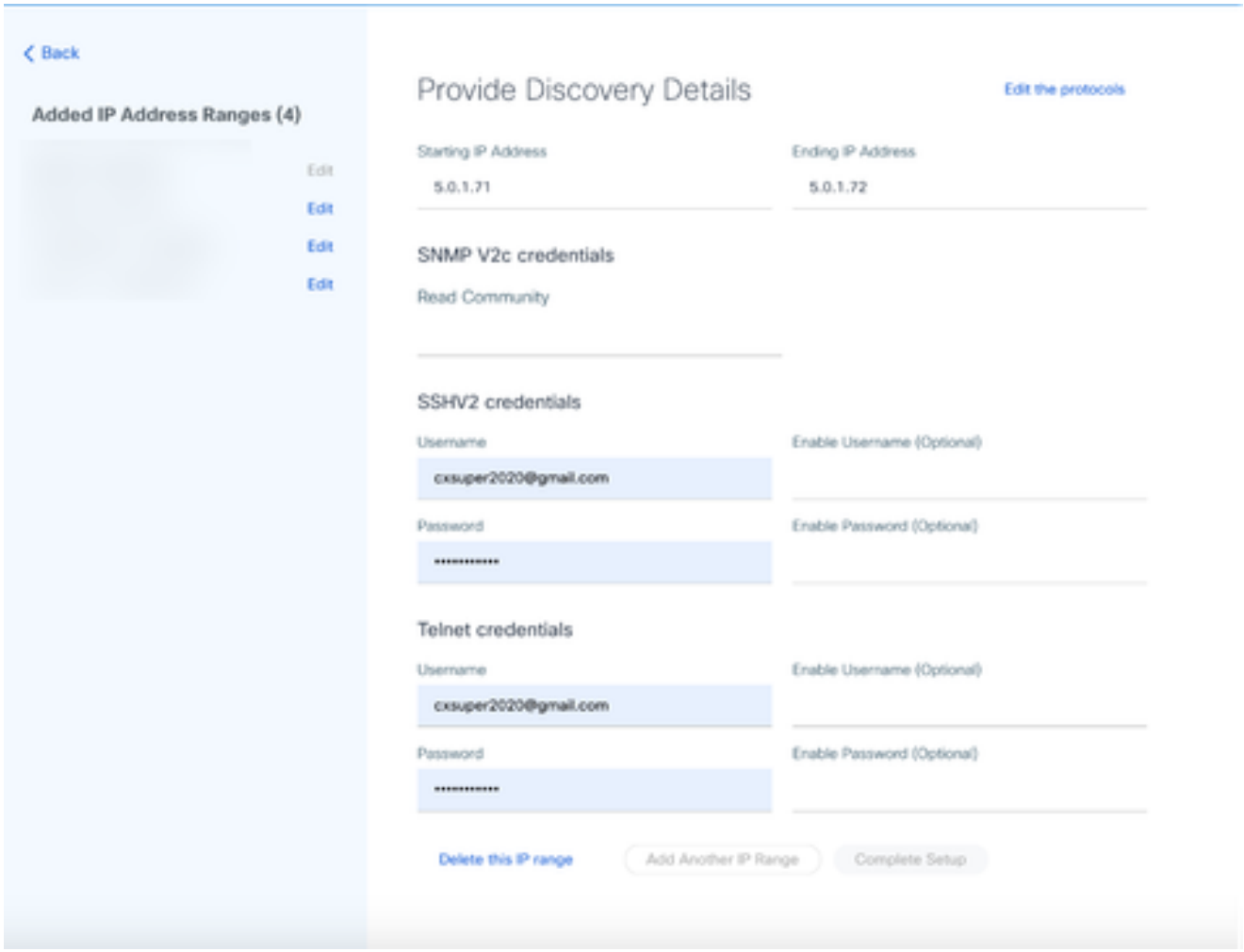
Per modificare un intervallo IP:

1. Passare alla finestra Origini dati.
2. Fare clic sull'agente cloud CX che richiede la modifica dell'intervallo IP nelle origini dati. Viene visualizzata la finestra dei dettagli.



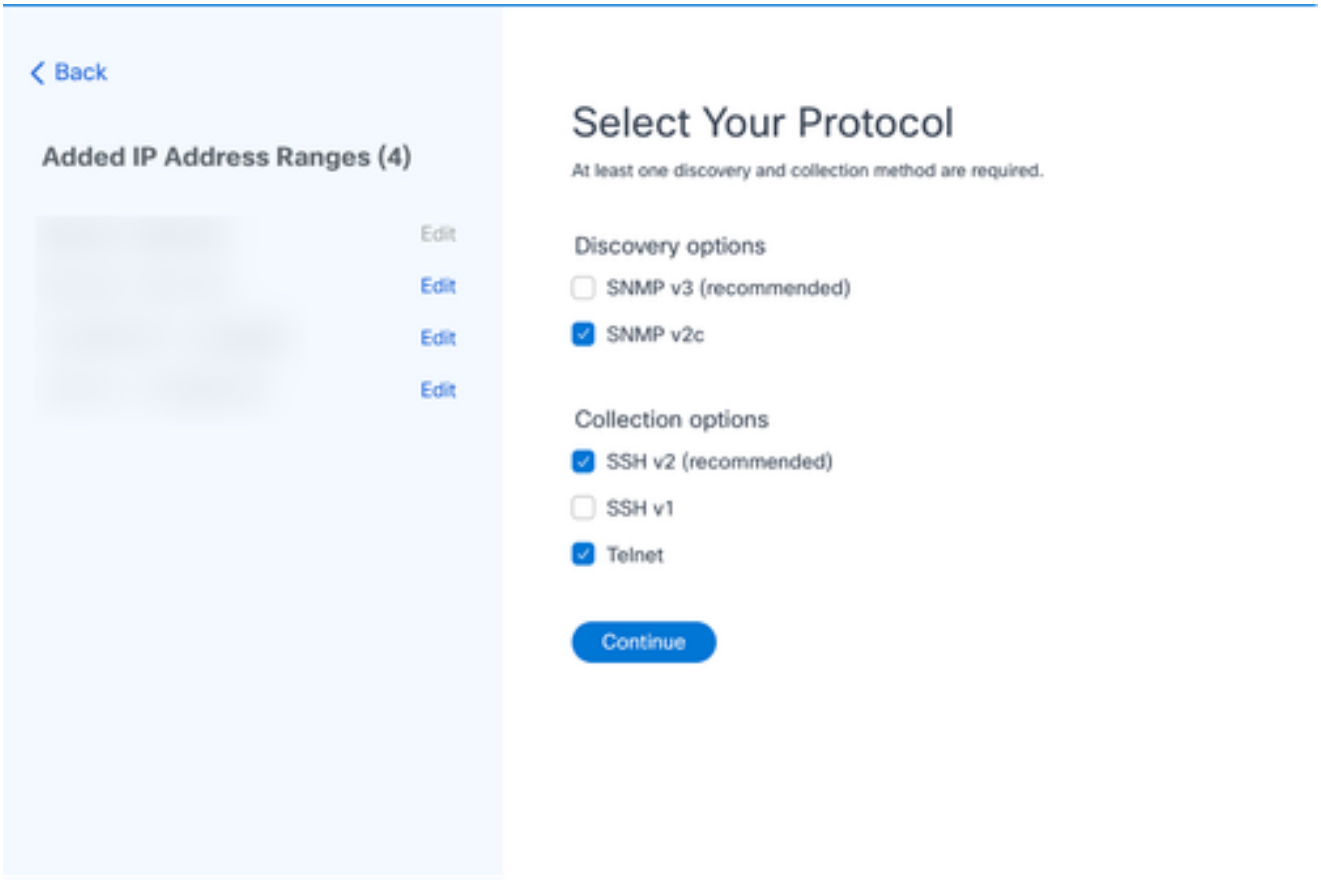
Origini dei dati

3. Fare clic su Modifica intervallo di indirizzi IP. Viene visualizzata la finestra Connetti a CX Cloud.



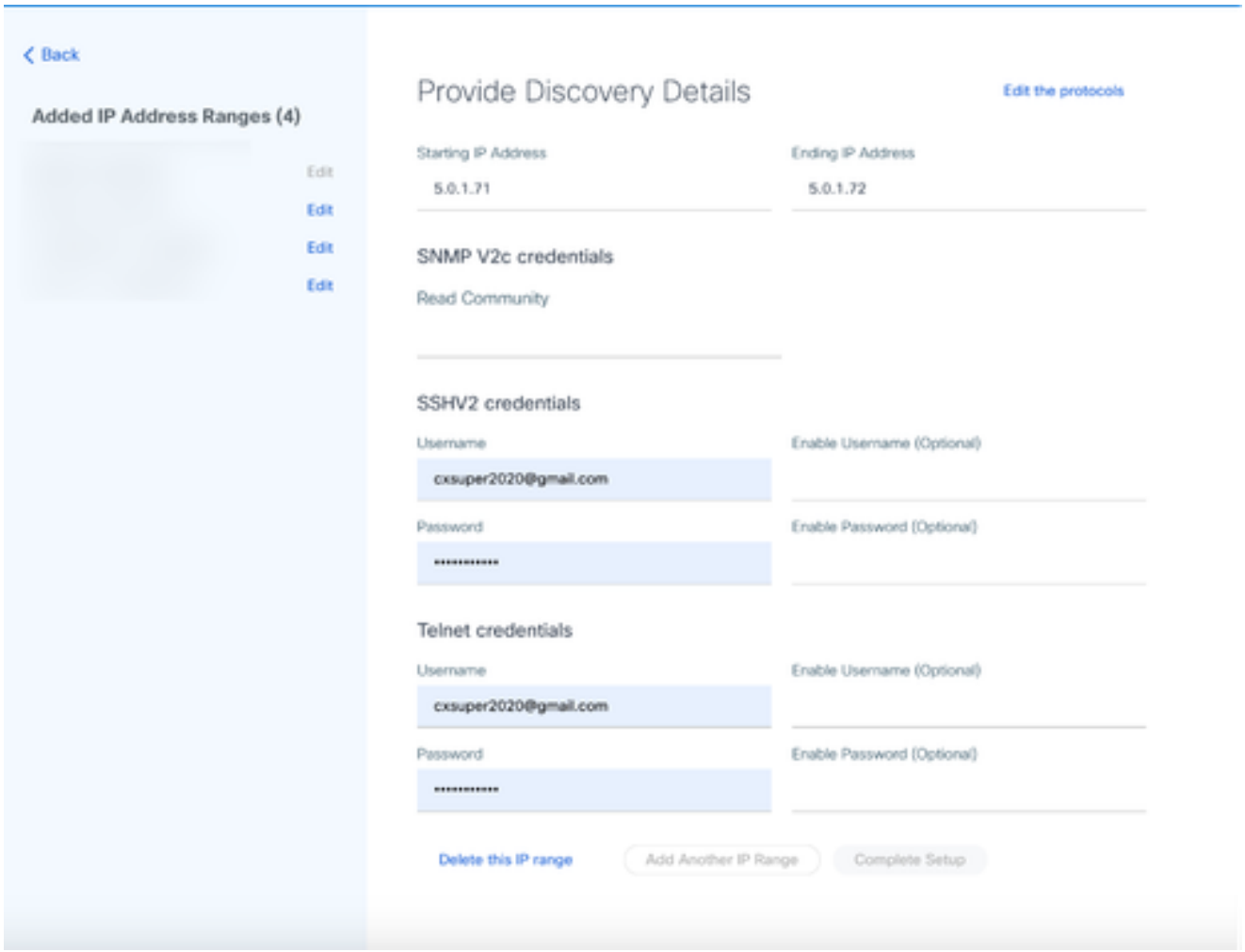
Fornire i dettagli di individuazione

4. Fare clic su Modifica i protocolli. Viene visualizzata la finestra Select Your Protocol.



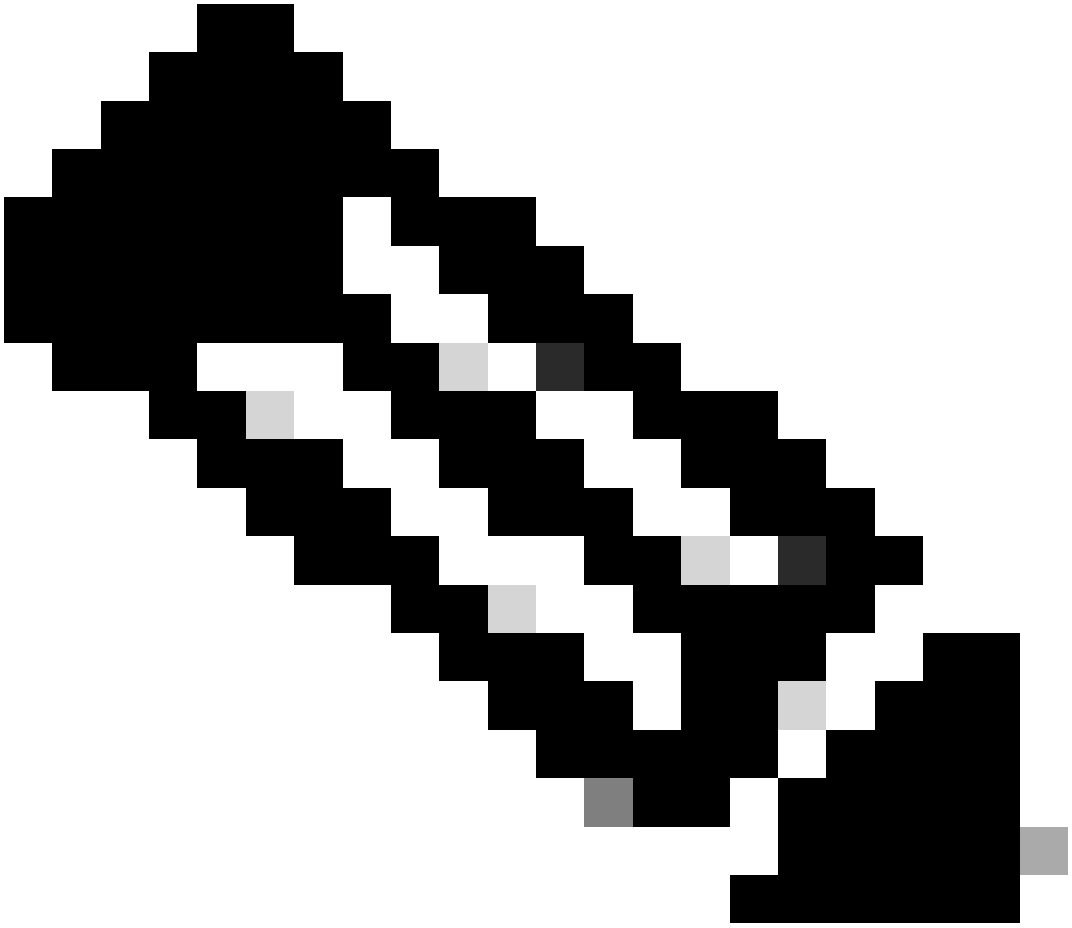
Selezionare il protocollo

5. Selezionare le caselle di controllo appropriate per scegliere i protocolli applicabili e fare clic su Continua per tornare alla finestra Specifica dettagli individuazione.



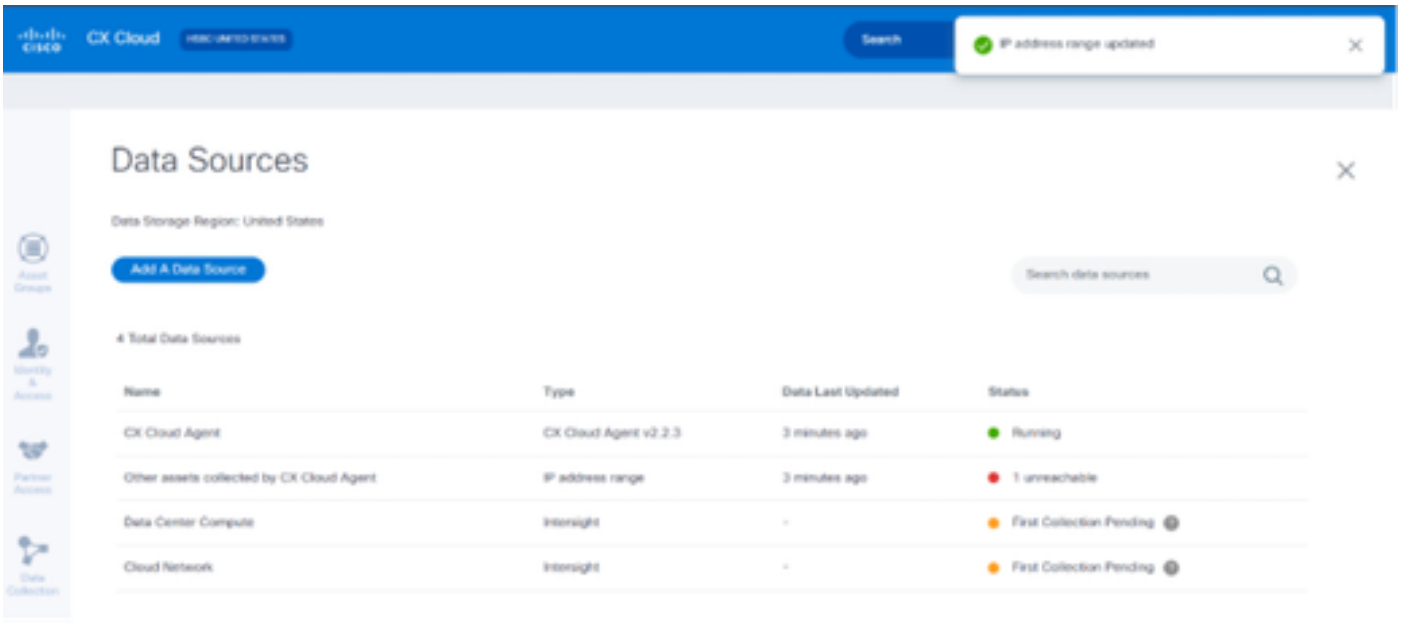
Fornire i dettagli di individuazione

6. Modificare i dettagli come richiesto e fare clic su Completa impostazione. Si apre la finestra Data Sources (Origini dati), in cui viene visualizzato un messaggio di conferma dell'aggiunta degli intervalli di indirizzi IP appena aggiunti.



Nota: questo messaggio di conferma non verifica se i dispositivi nell'intervallo modificato sono raggiungibili o se le loro credenziali vengono accettate. Questa conferma viene eseguita quando il cliente avvia il processo di individuazione.

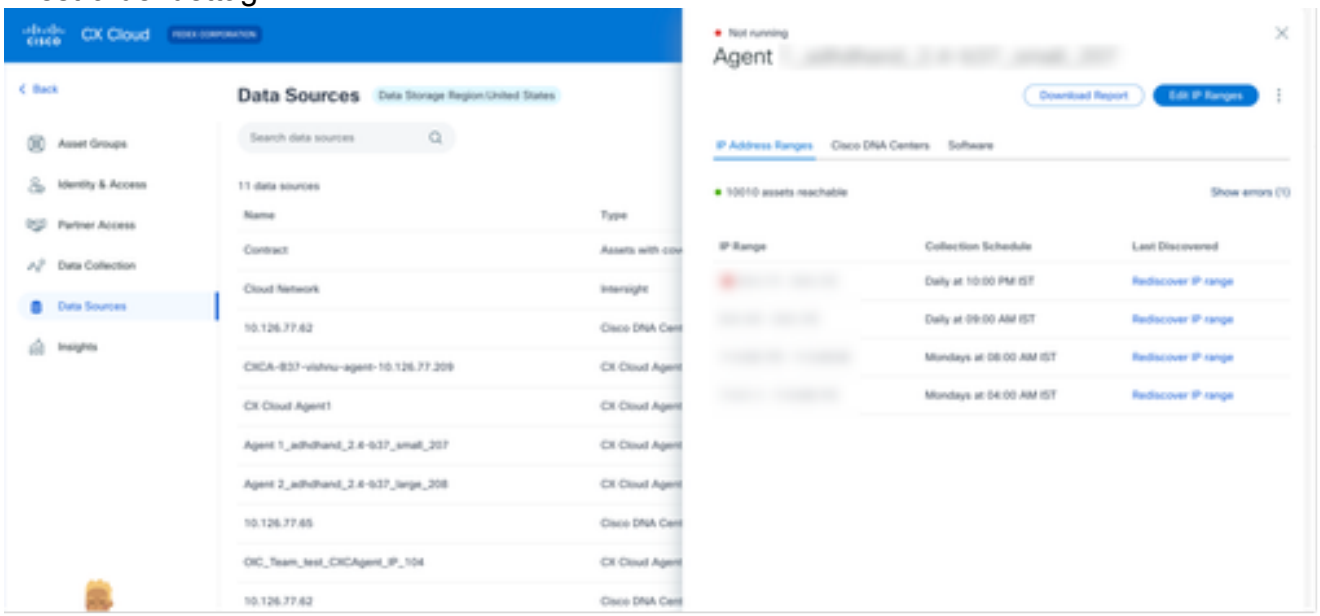
.



Eliminazione intervallo IP

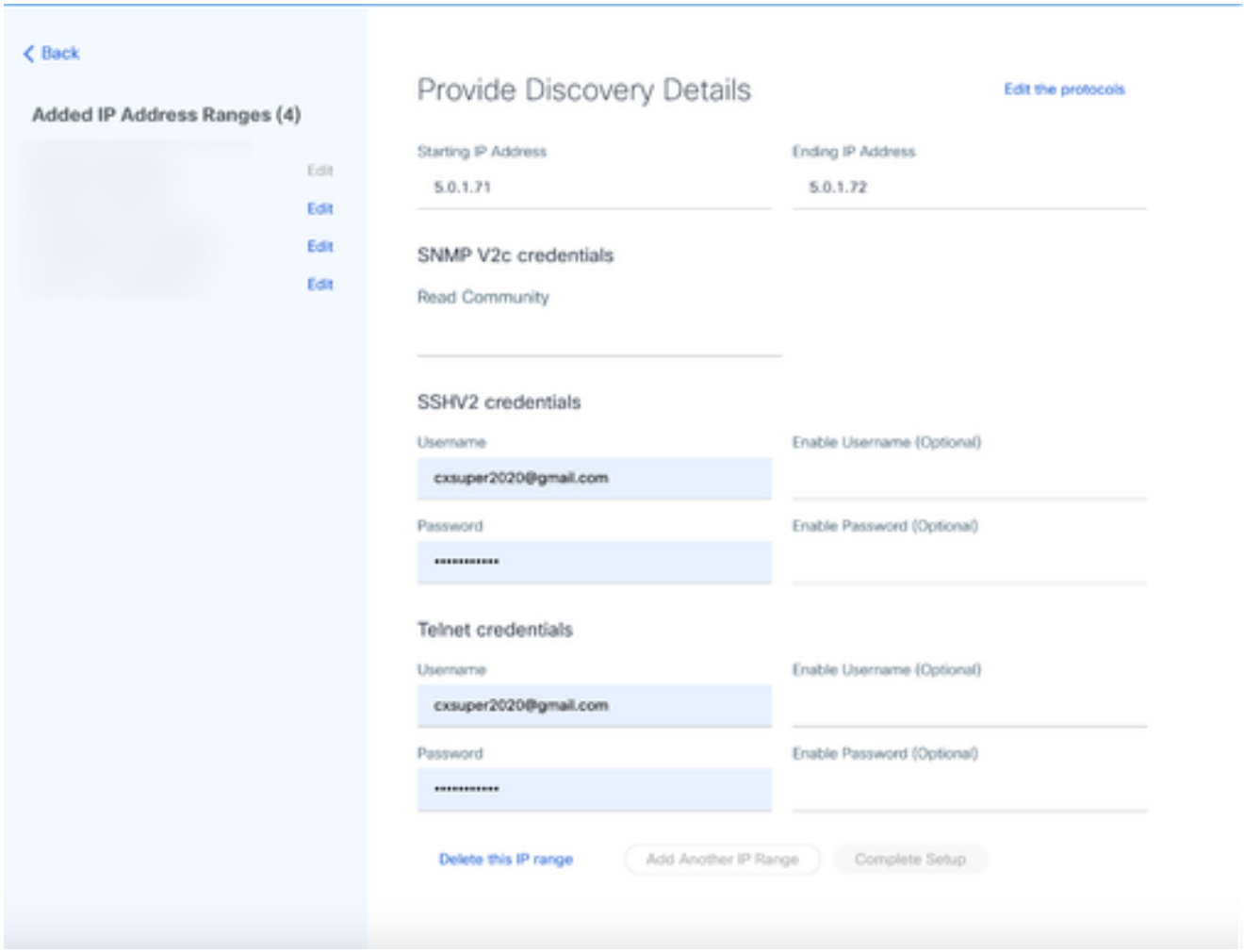
Per eliminare un intervallo IP:

1. Passare alla finestra Origini dati.
2. Selezionare il rispettivo agente cloud CX con l'intervallo IP da eliminare. Viene visualizzata la finestra dei dettagli.



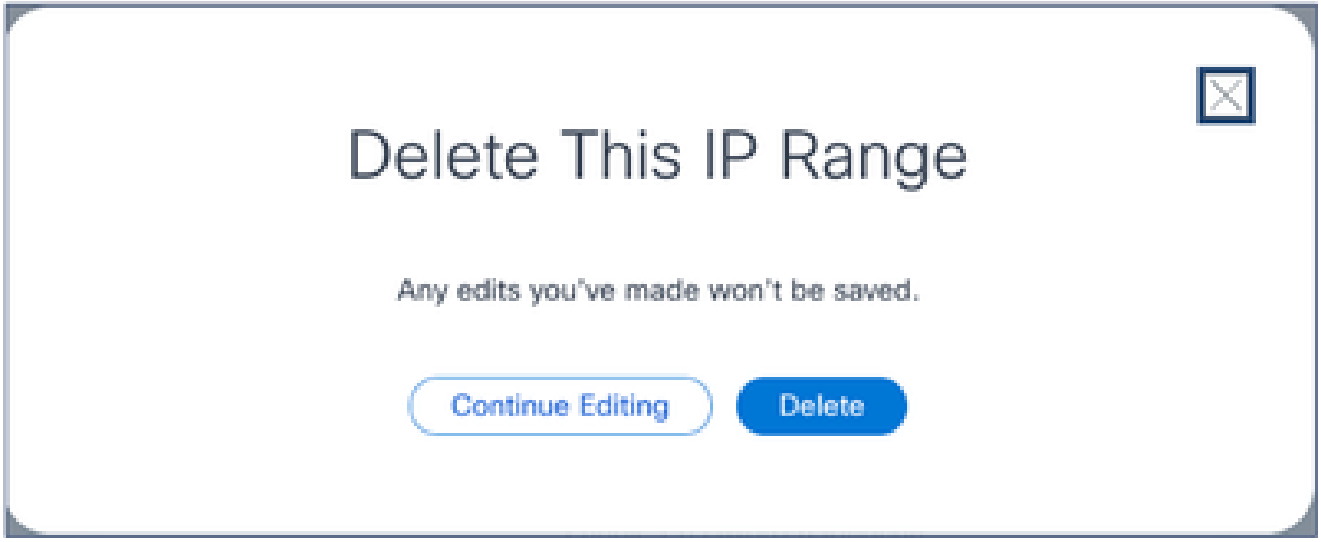
Origini dei dati

3. Fare clic su Modifica intervalli IP. Viene visualizzata la finestra Fornisci dettagli individuazione.



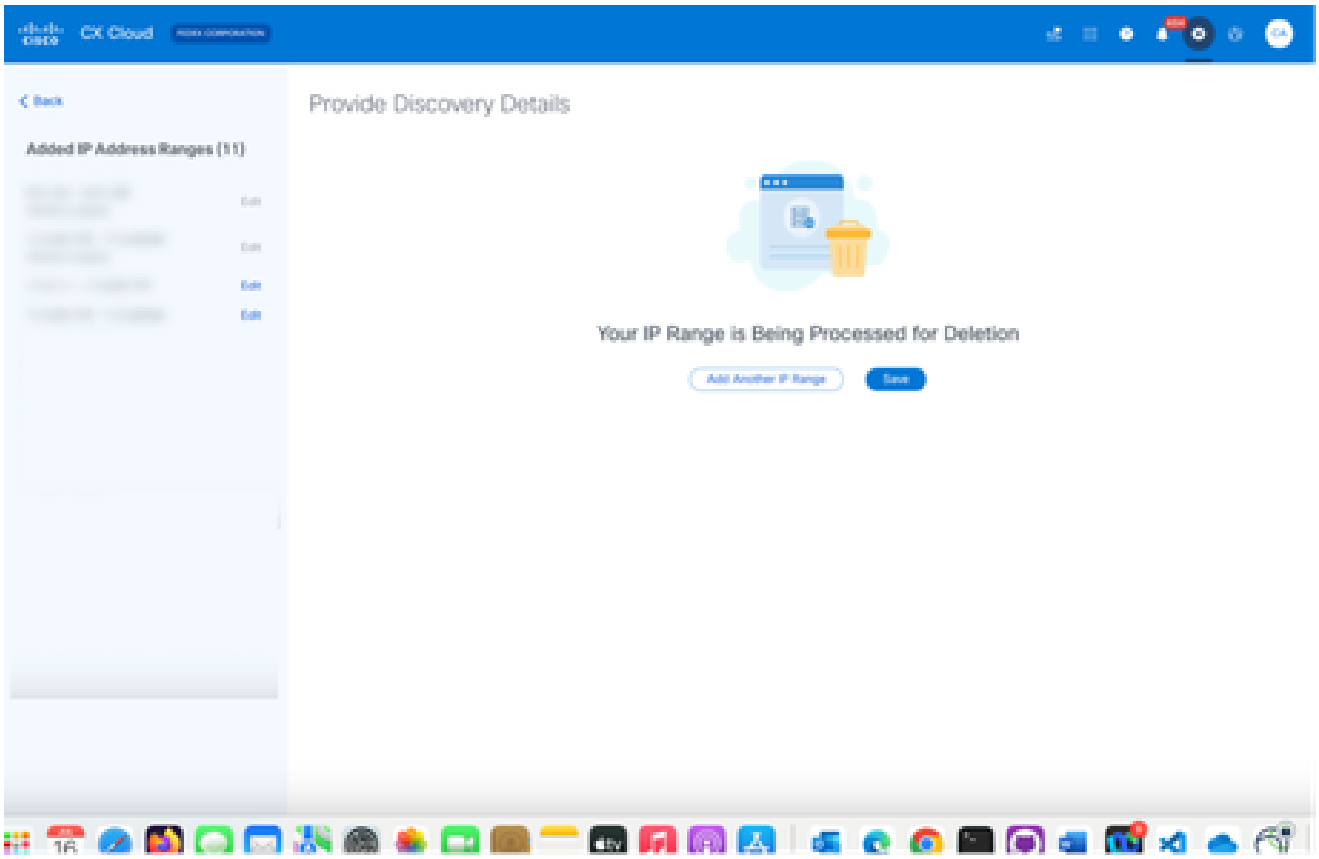
Fornire i dettagli di individuazione

4. Fare clic sul collegamento Elimina intervallo IP. Viene visualizzato il messaggio di conferma.



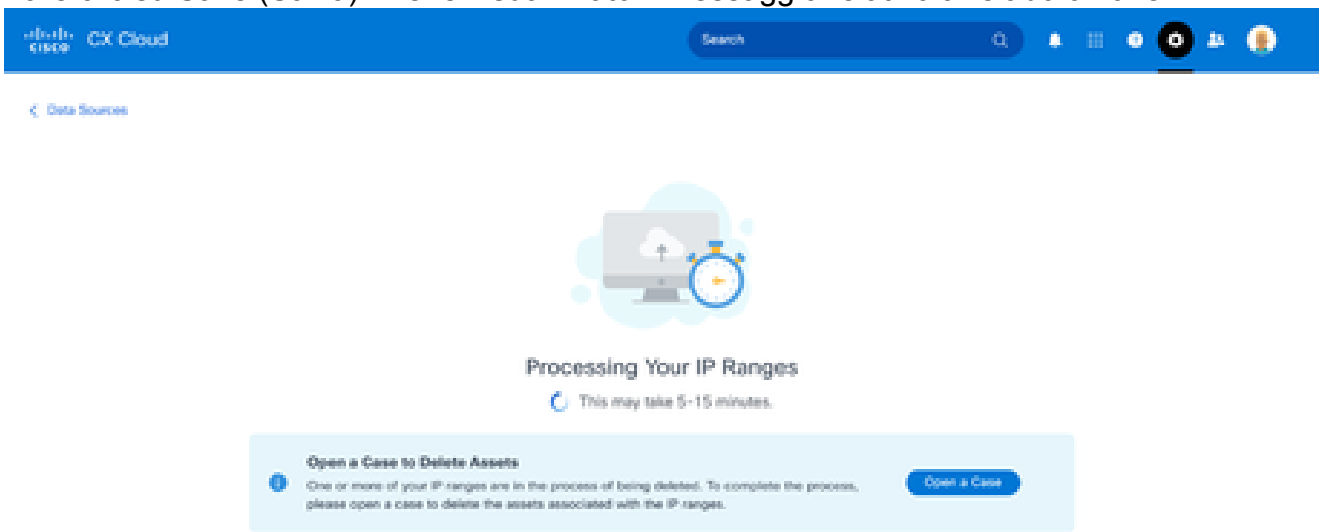
Messaggio eliminazione conferma

5. Fare clic su Elimina.



Eliminazione intervallo IP

6. Fare clic su Save (Salva). Viene visualizzato il messaggio relativo all'elaborazione.



7. Fare clic su Apri richiesta per creare una richiesta per eliminare gli asset associati all'intervallo IP. Viene visualizzata la finestra Origini dati, contenente un messaggio di conferma.

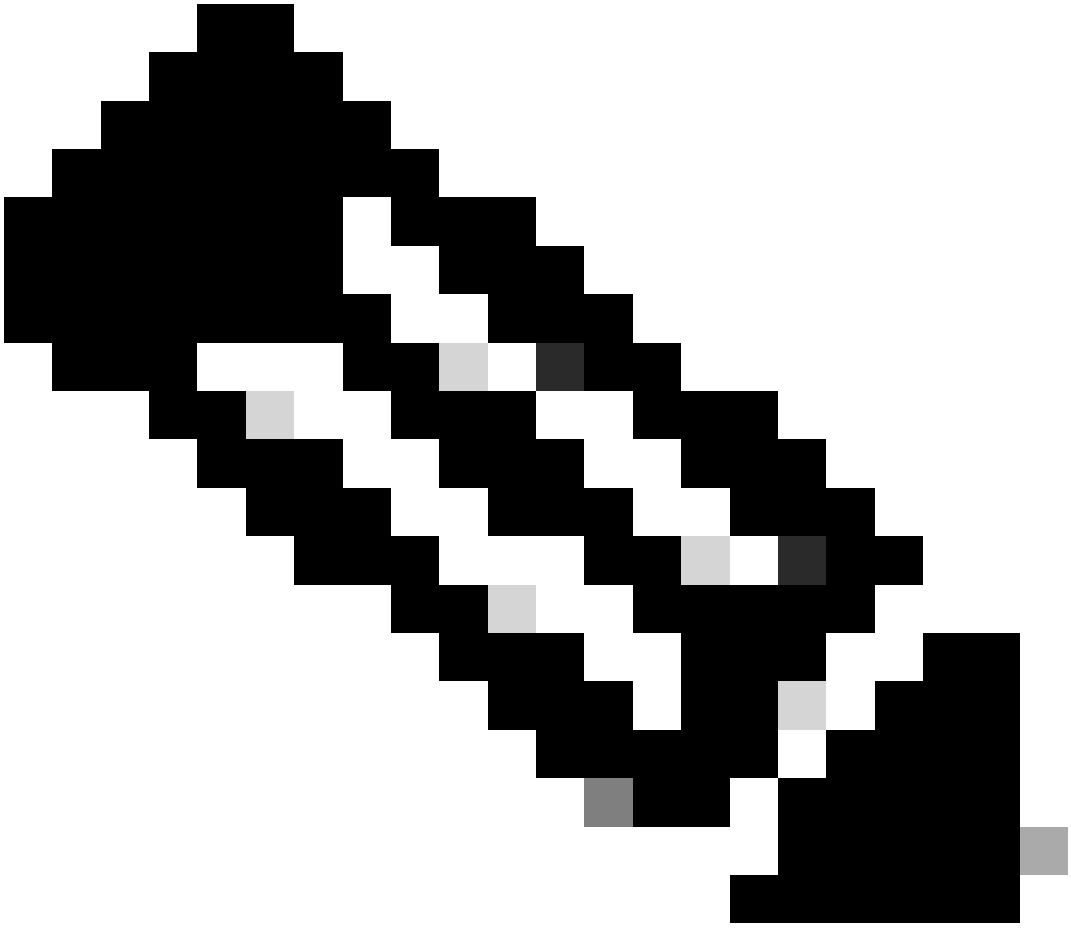
Informazioni sui dispositivi rilevati da più controller

È possibile che alcuni dispositivi possano essere individuati sia da Cisco DNA Center che dalla connessione diretta dei dispositivi all'agente cloud CX, causando la raccolta di dati duplicati da tali dispositivi. Per evitare la raccolta di dati duplicati e la gestione dei dispositivi da parte di un solo controller, è necessario determinare una precedenza per la gestione dei dispositivi da parte dell'agente cloud CX.

- Se un dispositivo viene individuato per la prima volta da Cisco DNA Center e quindi riscoperto tramite connessione diretta (utilizzando un file di inizializzazione o un intervallo IP), Cisco DNA Center ha la precedenza nel controllo del dispositivo.
- Se un dispositivo viene individuato per la prima volta tramite connessione diretta al dispositivo all'agente cloud CX e quindi riscoperto da Cisco DNA Center, Cisco DNA Center ha la precedenza nel controllo del dispositivo.

Pianificazione delle analisi diagnostiche

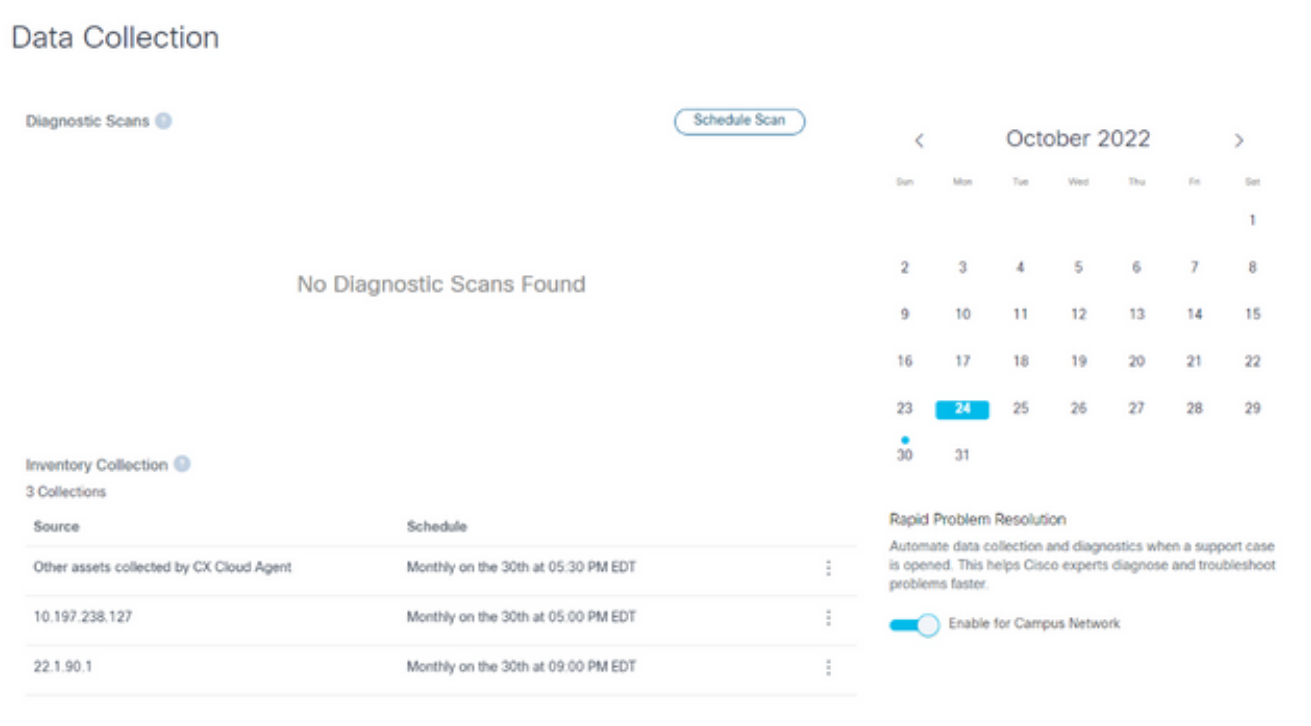
I clienti possono pianificare scansioni diagnostiche su richiesta in CX Cloud.



Nota: Cisco consiglia di pianificare le analisi diagnostiche o di avviare le analisi su richiesta almeno 6-7 ore prima dei programmi di raccolta delle scorte in modo che non si sovrappongano. L'esecuzione simultanea di più scansioni diagnostiche può rallentare il processo di scansione e potenzialmente causare errori di scansione.

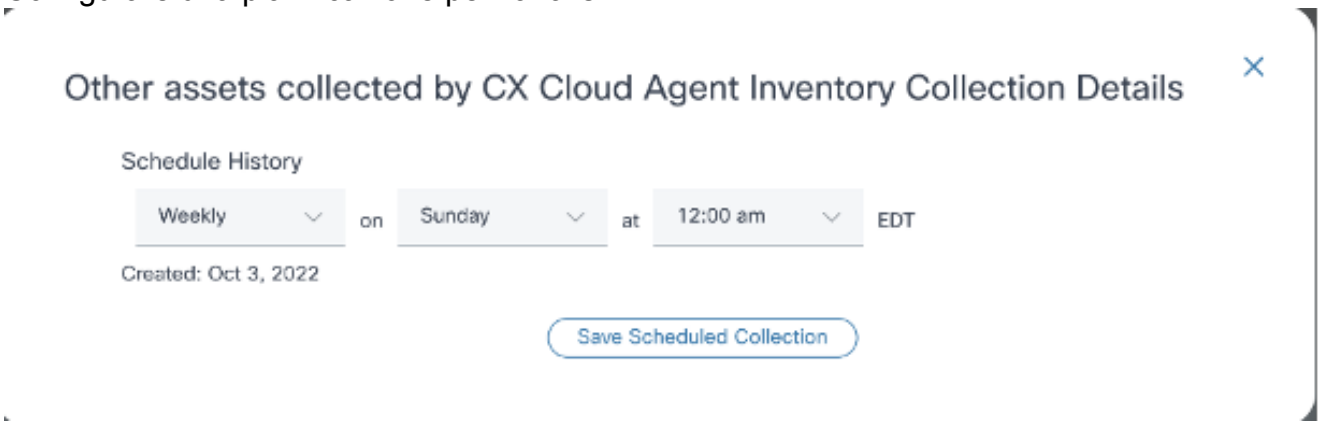
Per pianificare le analisi diagnostiche:

1. Nella pagina Home fare clic sull'icona Impostazioni (ingranaggio).
2. Nella pagina Origini dati selezionare Raccolta dati nel riquadro sinistro.
3. Fare clic su Pianifica scansione.



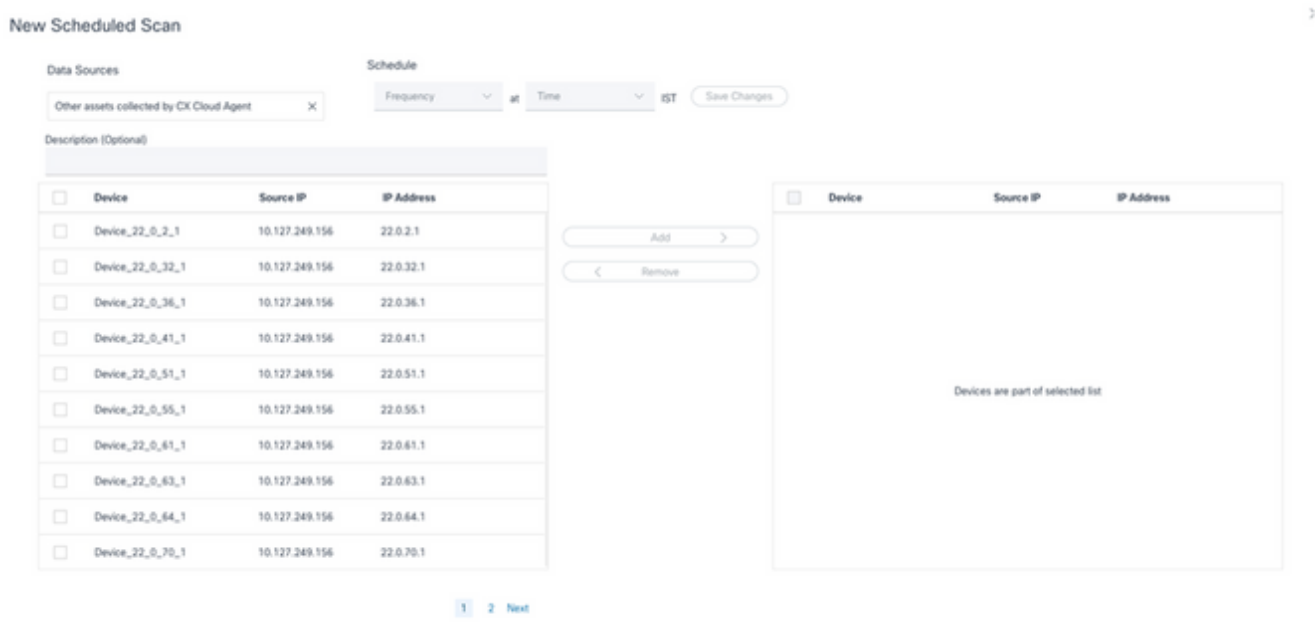
Raccolta dati

4. Configurare una pianificazione per l'analisi.



Configura pianificazione analisi

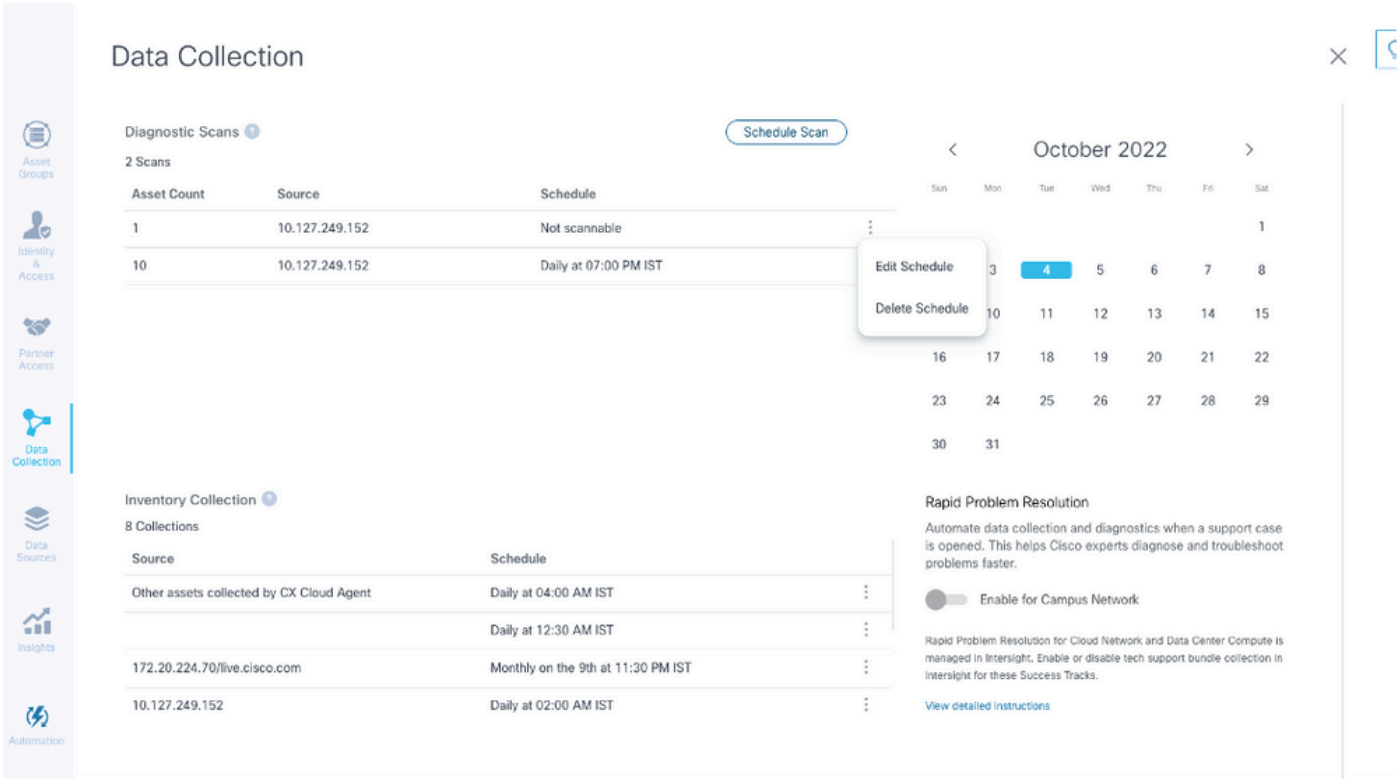
5. Nell'elenco delle periferiche, selezionare tutte le periferiche per la scansione e fare clic su Aggiungi.



Pianifica analisi

6. Al termine della programmazione, fare clic su Salva modifiche.

Le pianificazioni delle analisi diagnostiche e della raccolta dei dati di inventario possono essere modificate ed eliminate dalla pagina Raccolta dati.



Raccolta dei dati con le opzioni di pianificazione Modifica ed Elimina

Aggiornamento delle VM dell'agente cloud CX a configurazioni medie e grandi

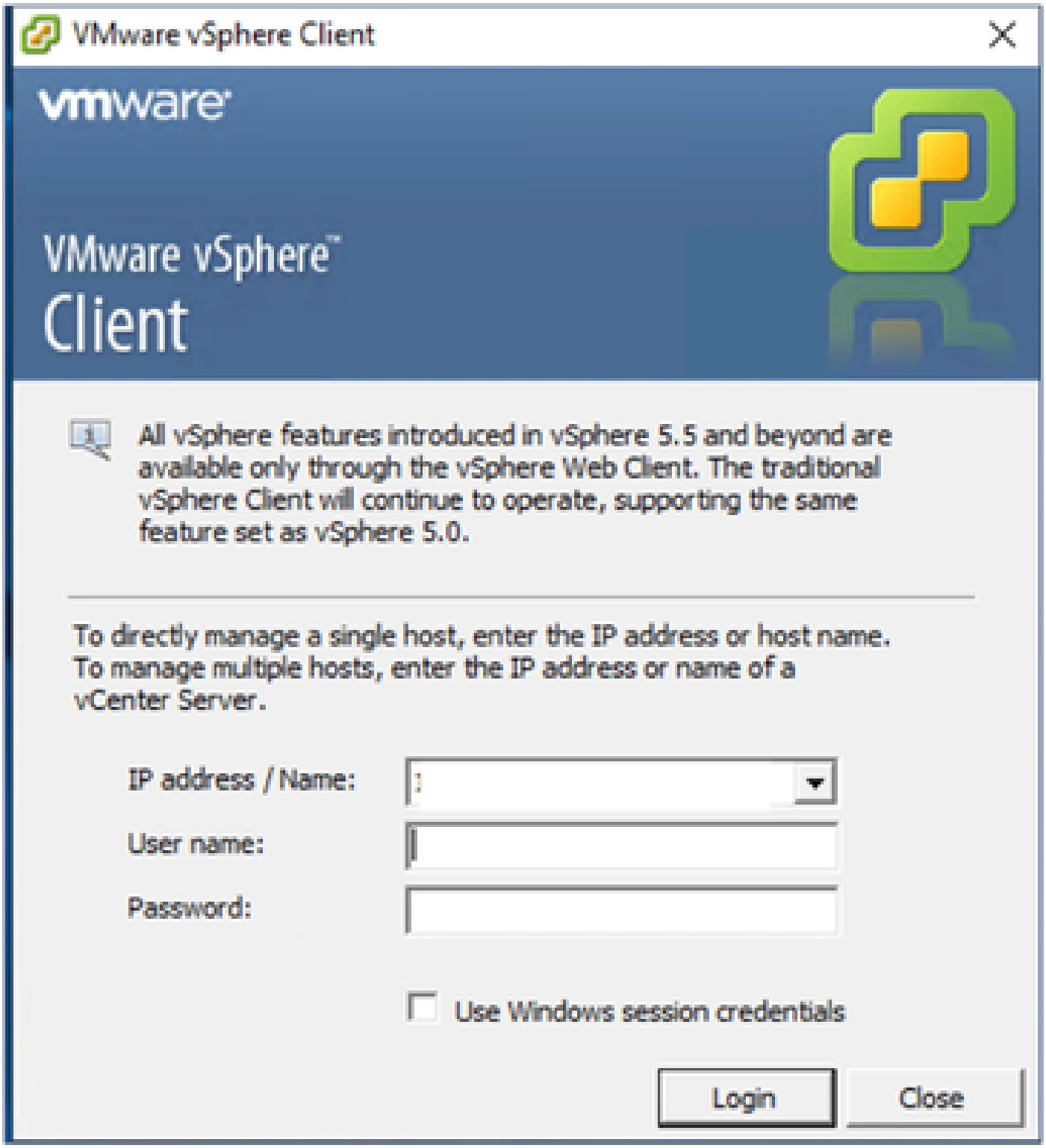
Dopo l'aggiornamento delle VM, non è possibile:

- Scalabilità da una configurazione grande o media a una configurazione piccola
- Scalabilità da una configurazione di grandi dimensioni a una media
- Aggiornamento da una configurazione di medie dimensioni a una di grandi dimensioni

Prima di aggiornare la VM, Cisco consiglia di creare un'istantanea a scopo di ripristino in caso di guasto. Per ulteriori informazioni, fare riferimento a Backup e ripristino della VM cloud CX.

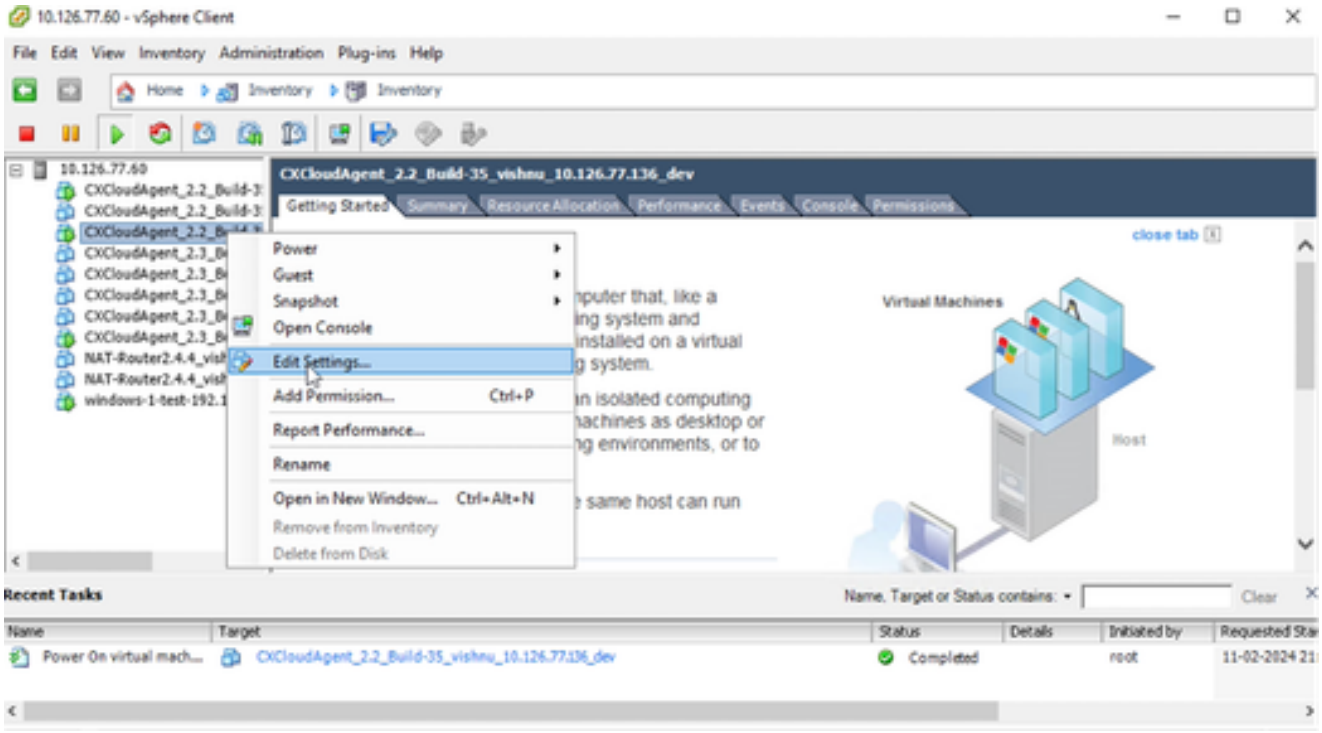
Riconfigurazione con VMware vSphere Thick Client

Per aggiornare la configurazione della VM utilizzando VMware vSphere Thick Client esistente:



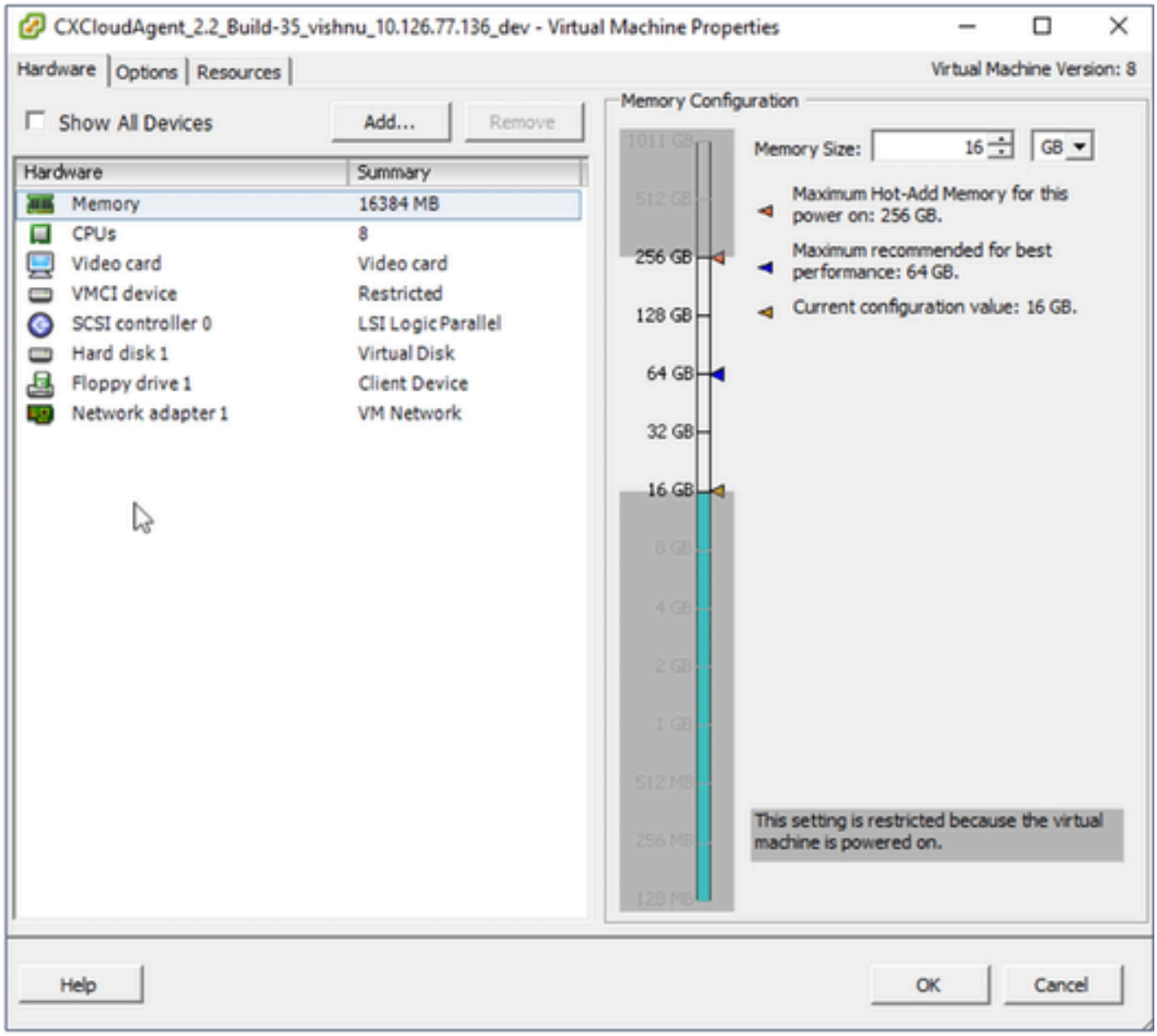
Client vSphere

1. Accedere al client VMware vSphere. Nella home page viene visualizzato un elenco di VM.



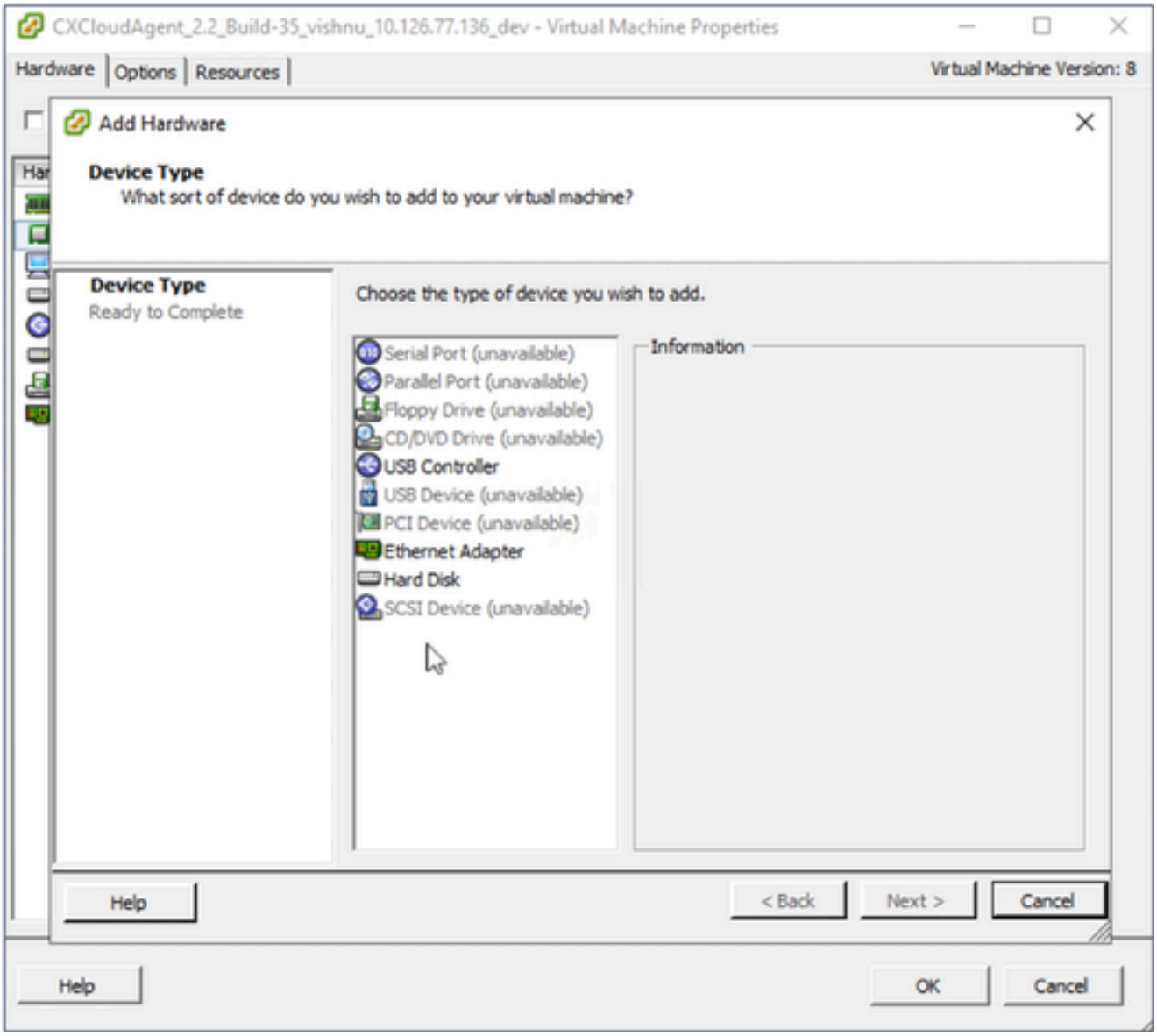
Modifica impostazioni

2. Fare clic con il pulsante destro del mouse sulla VM di destinazione e selezionare Modifica impostazioni dal menu. Viene visualizzata la finestra Proprietà VM.



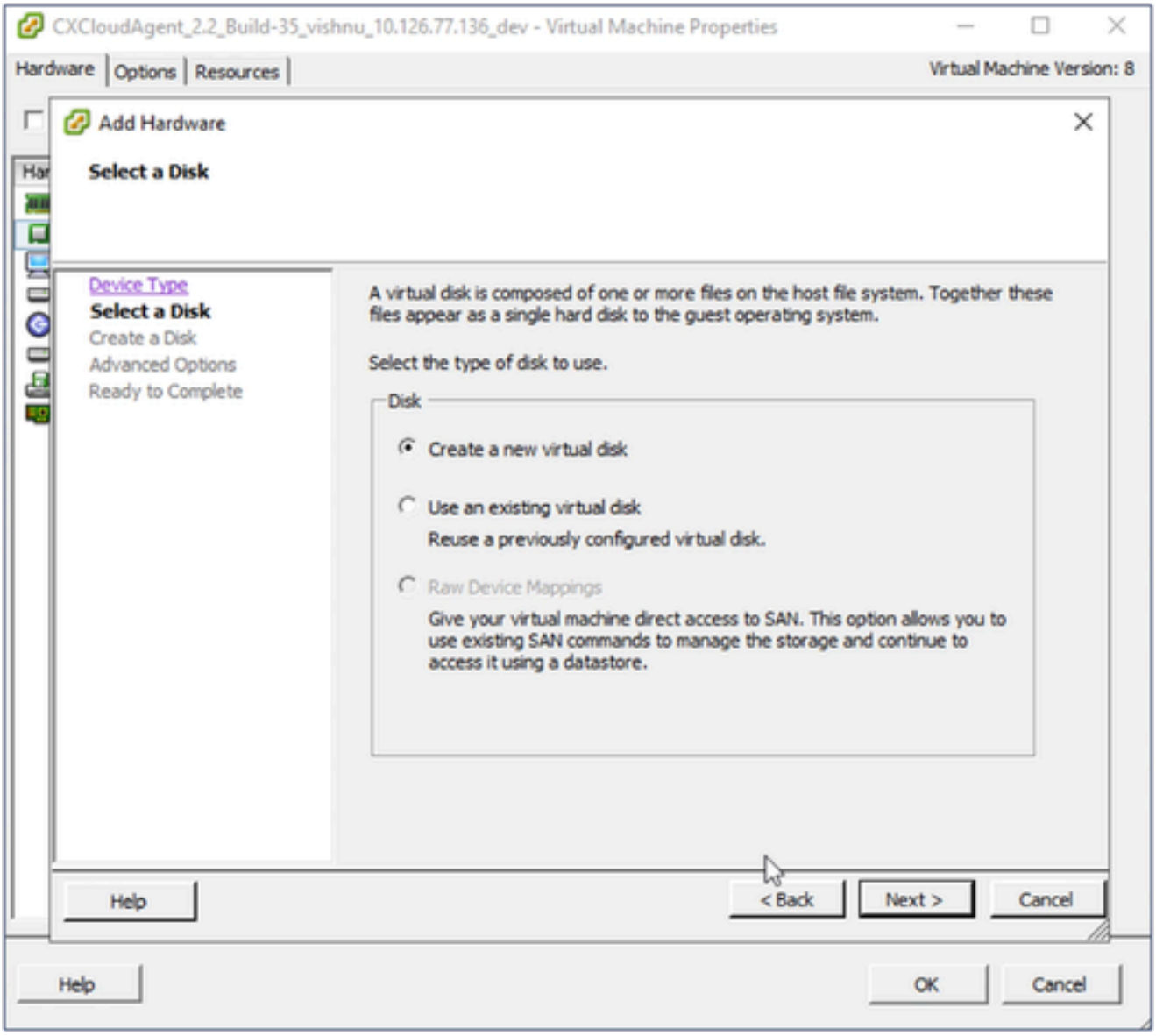
Proprietà macchina virtuale

3. Aggiornare i valori di Dimensione memoria come specificato:
   Media: 32 GB (32.768 MB)
   Grandi: 64 GB (65.536 MB)
4. Selezionare le CPU e aggiornare i valori come specificato:
   Medio: 16 core (8 socket *2 core/socket)
   Grande: 32 core (16 socket *2 core/socket)
5. Fare clic su Add. Viene visualizzata la finestra Installazione hardware.



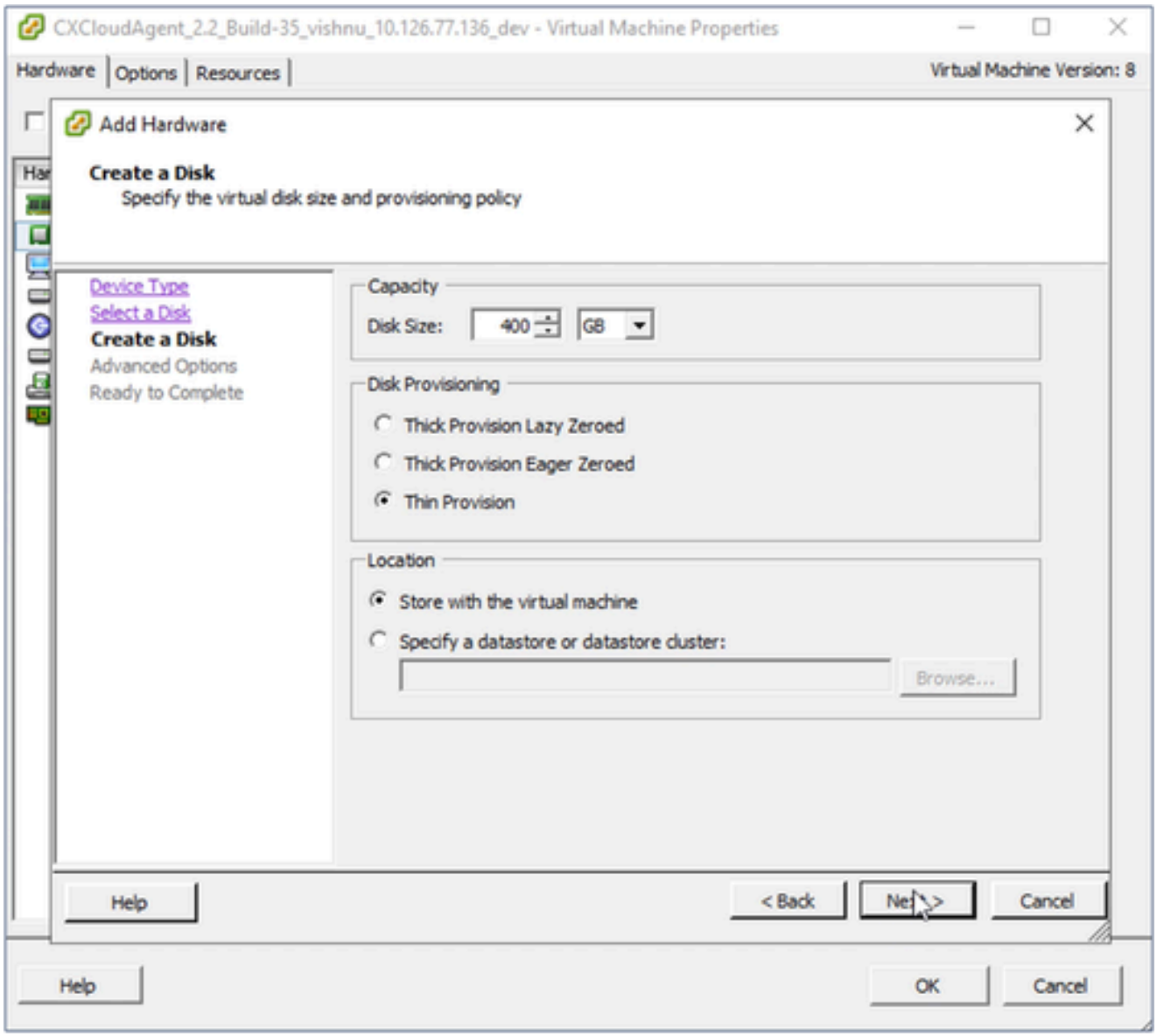
Tipo di dispositivo

6. Selezionare Hard Disk come Tipo di dispositivo.
7. Fare clic su Next (Avanti).



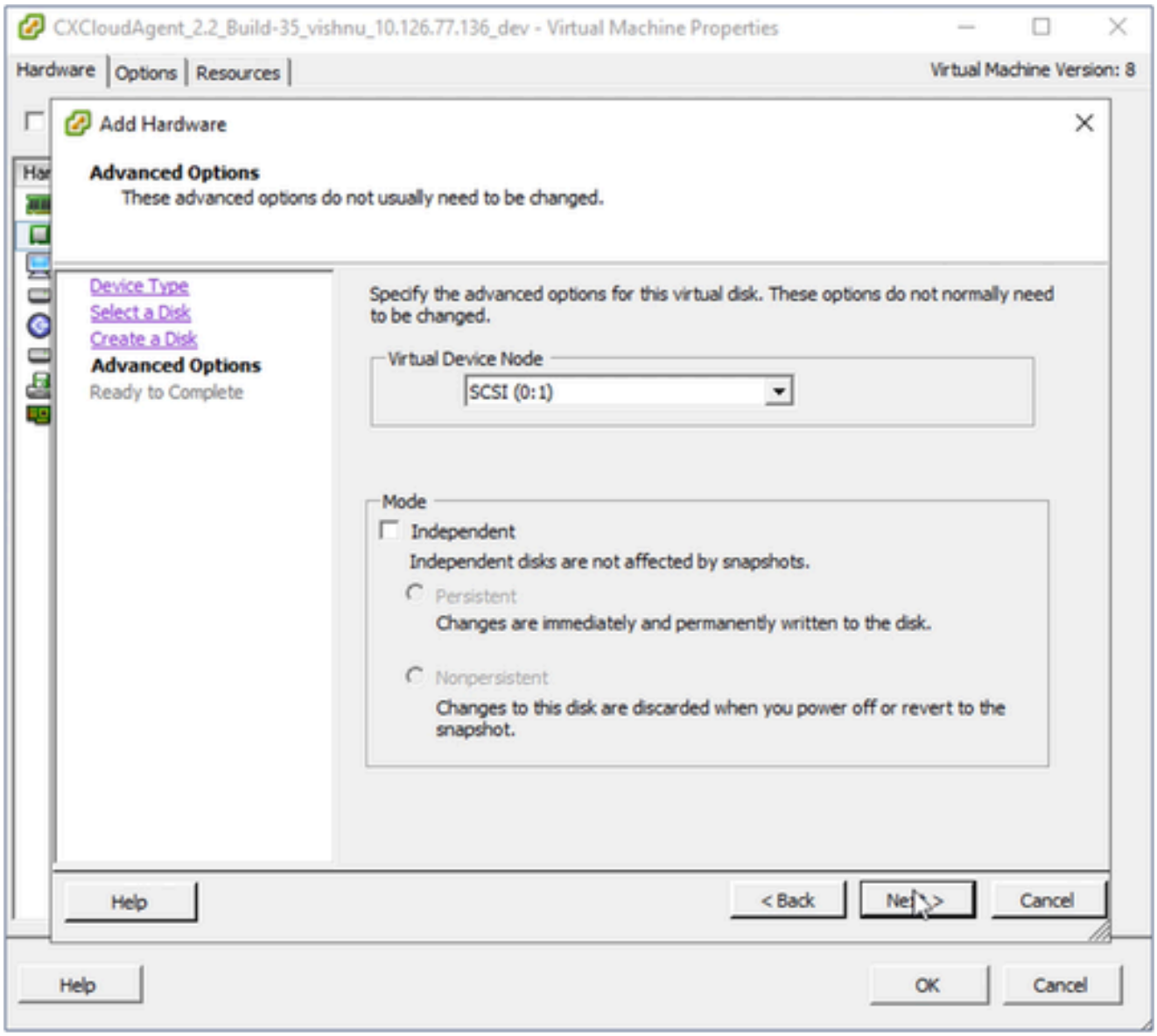
Seleziona disco

8. Selezionare il pulsante di scelta Crea nuovo disco virtuale e fare clic su Avanti.



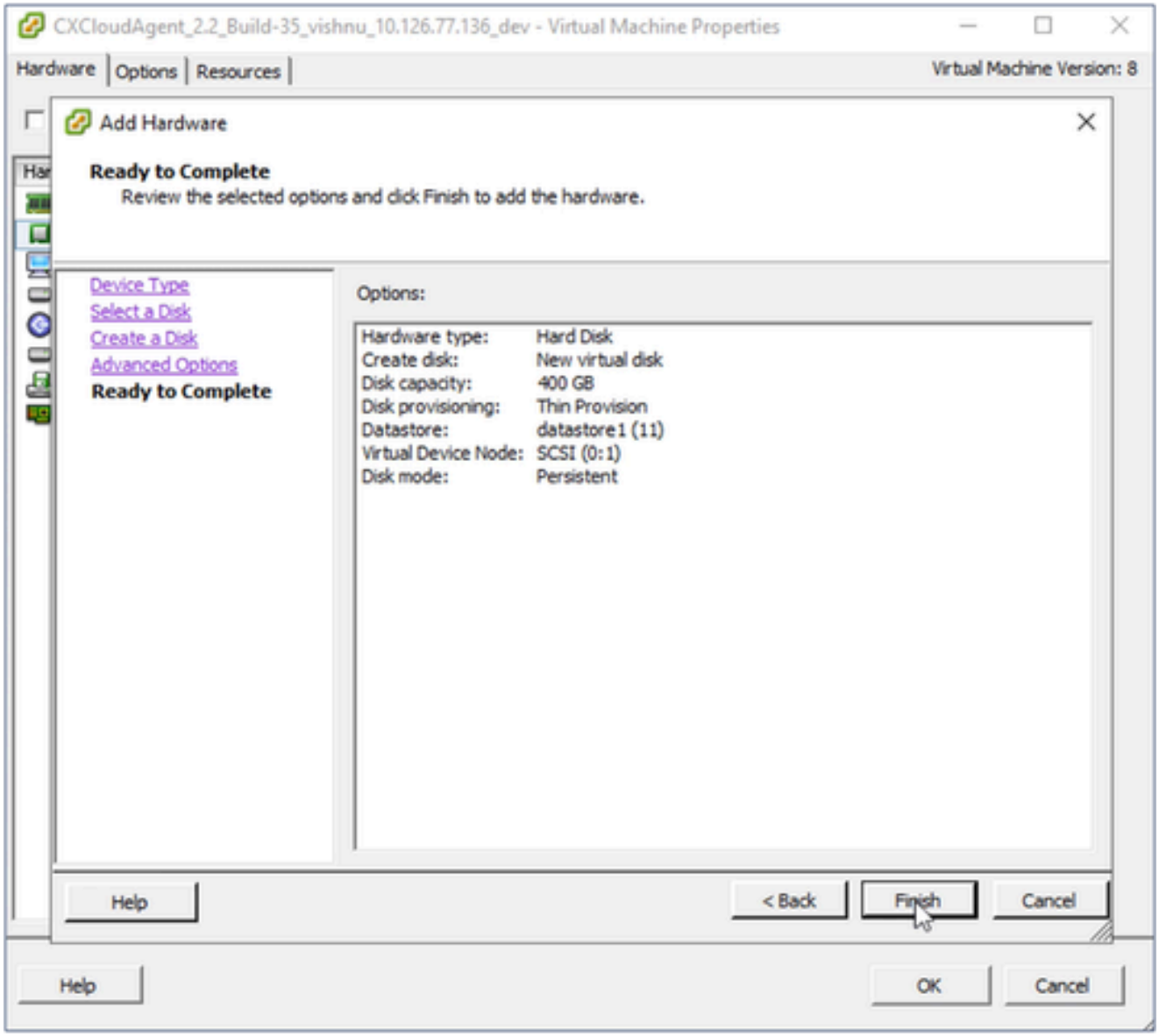
Crea disco

9. Aggiornare Capacity > Disk Size come specificato:
   Piccole e medie: 400 GB (dimensioni iniziali 200 GB, aumento dello spazio totale a 600 GB)
   Piccole e grandi: 1.000 GB (dimensioni iniziali 200 GB, aumento dello spazio totale a 1.200 GB)
10. Selezionare il pulsante di opzione Thin Provision per Disk Provisioning.
11. Fare clic su Next (Avanti). Viene visualizzata la finestra Opzioni avanzate.



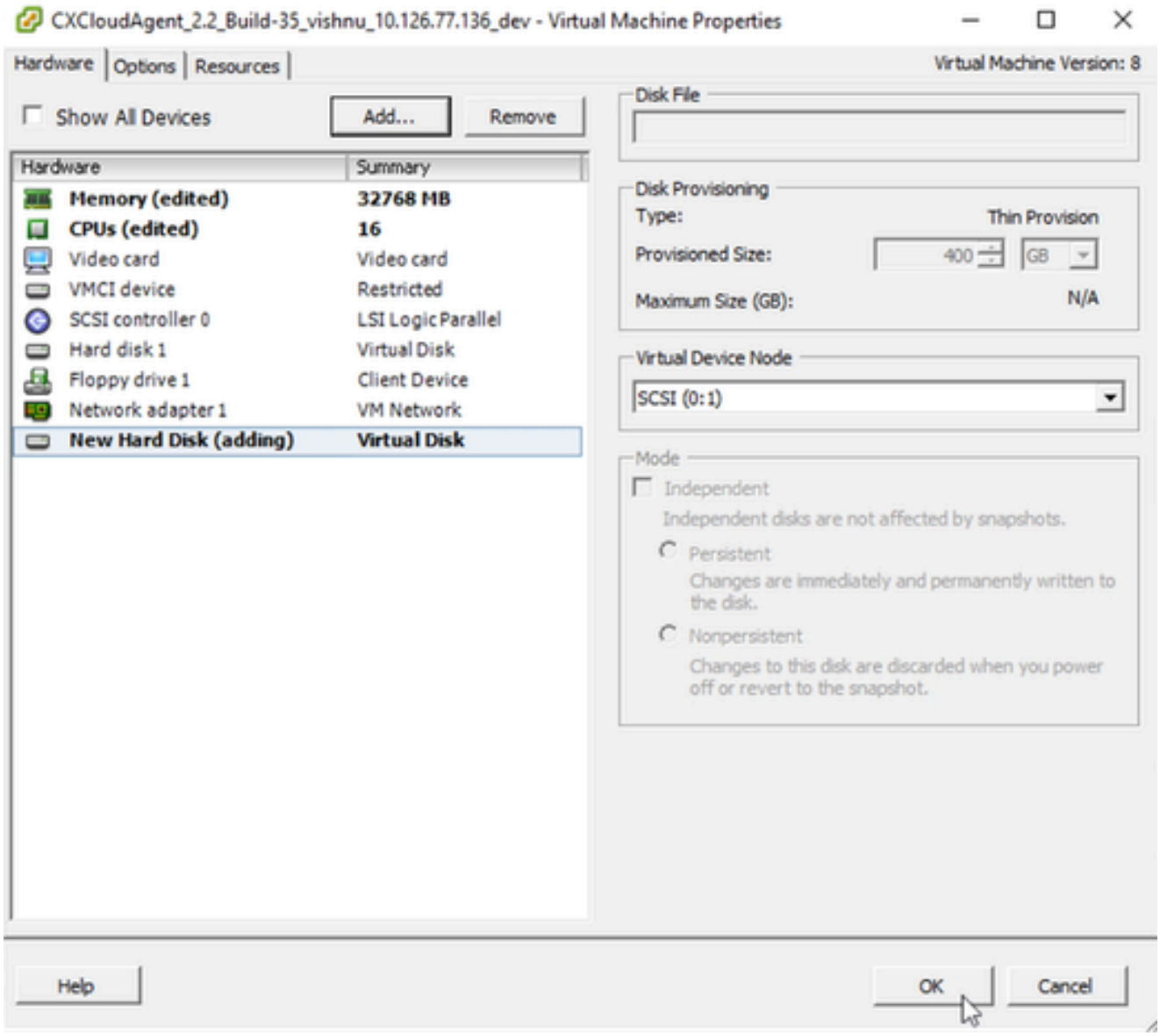
Opzioni avanzate

12. Non apportare modifiche. Fare clic su Avanti per continuare.



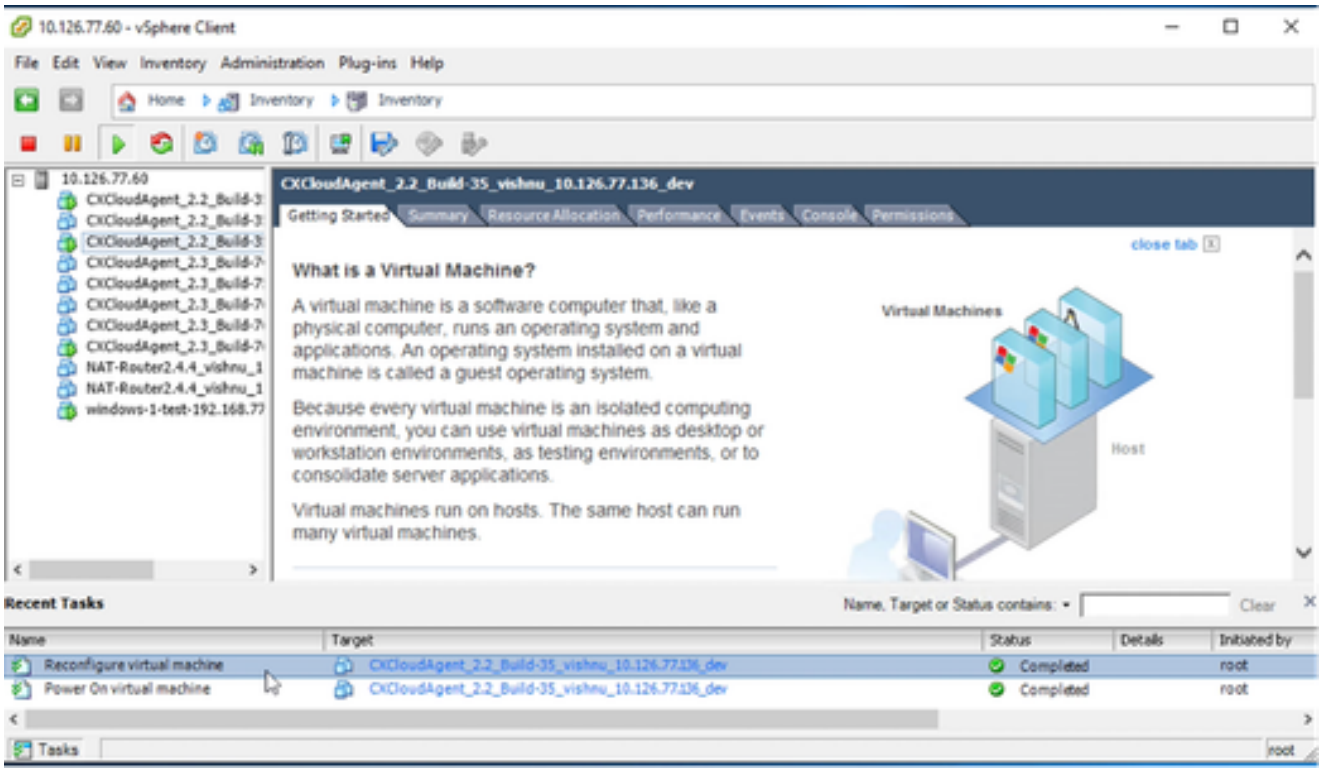
Pronto per il completamento

13. Fare clic su Finish (Fine).

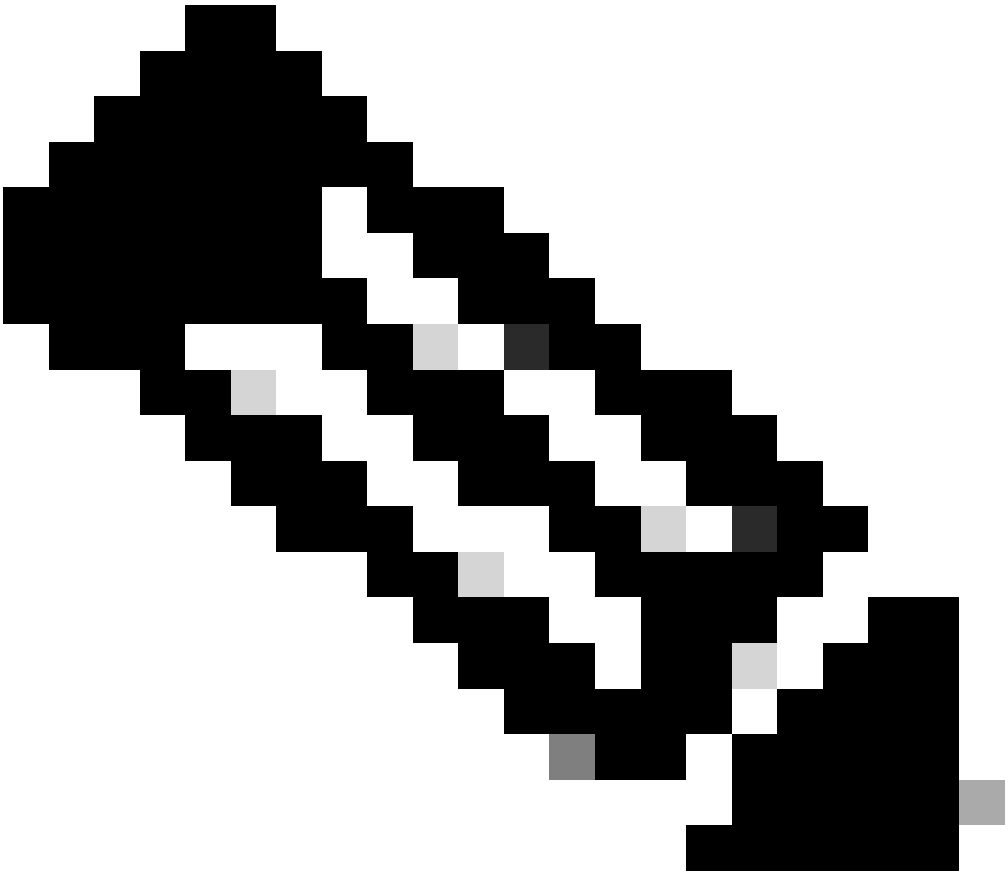


Hardware

14. Scegliere OK per completare la riconfigurazione. La riconfigurazione completata viene visualizzata nel pannello Attività recenti.



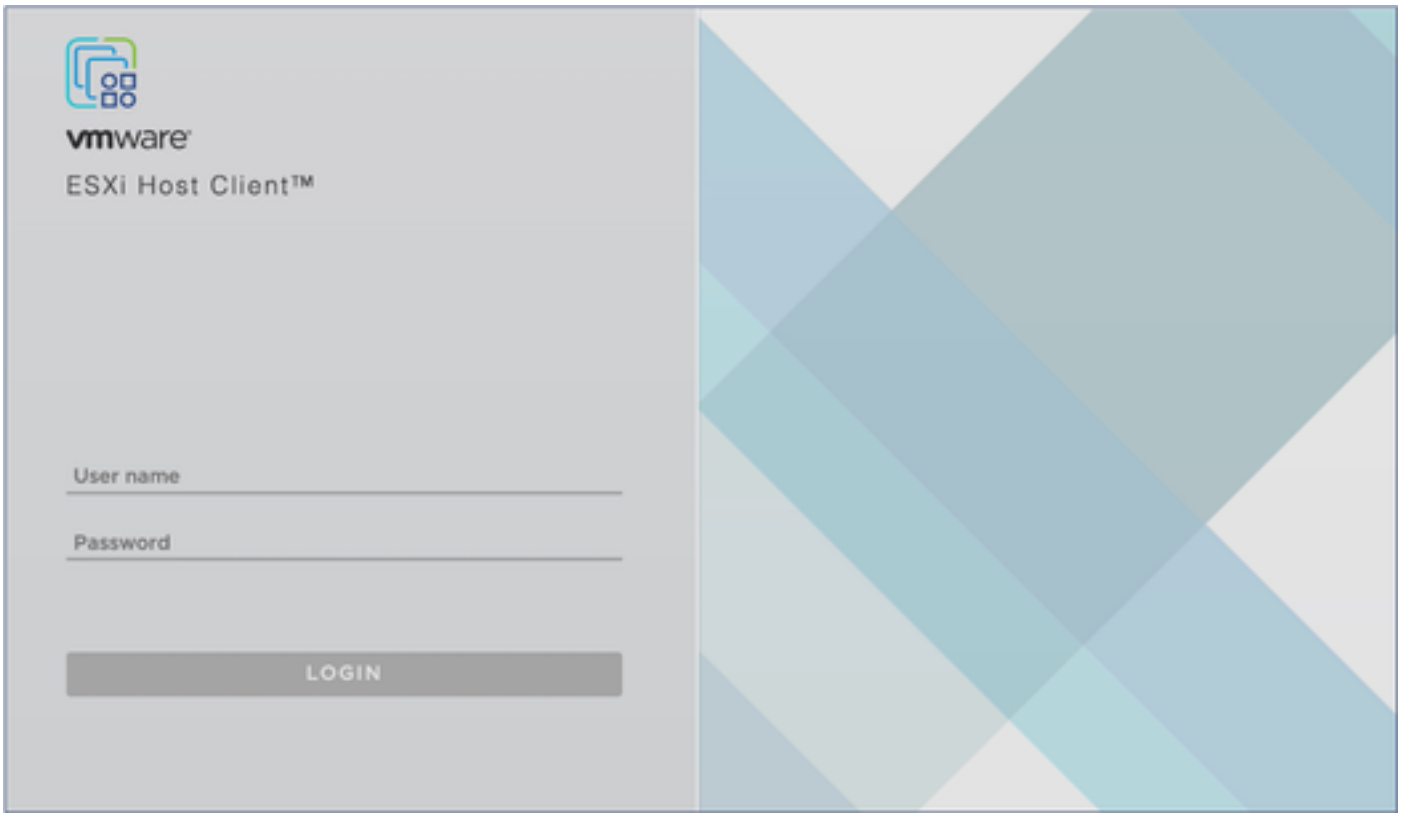
Attività recenti



Nota: il completamento delle modifiche alla configurazione richiede circa cinque minuti.

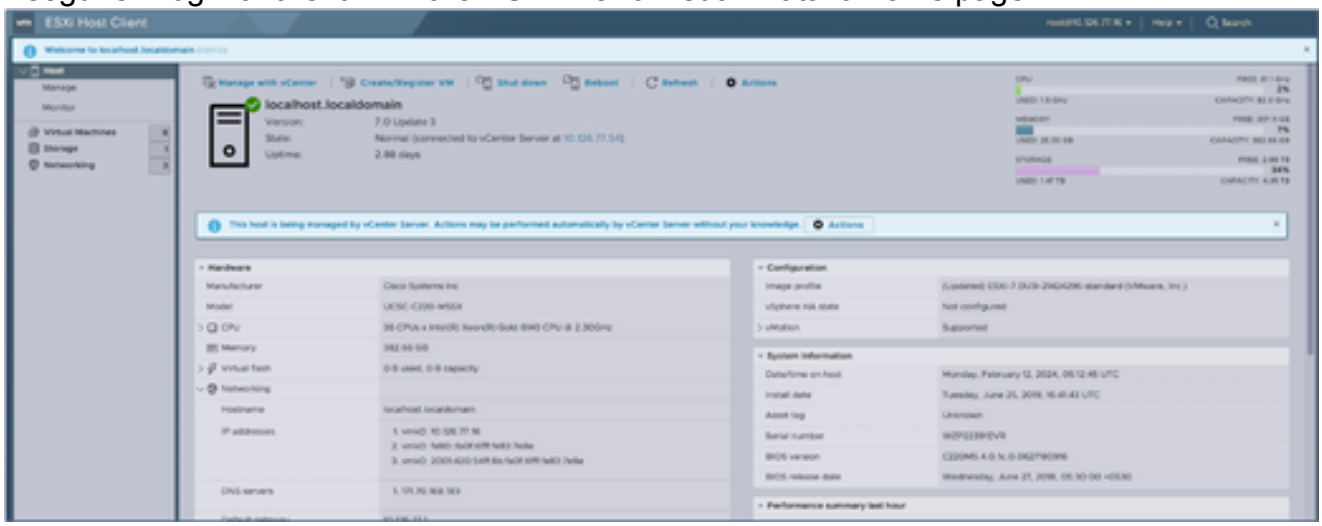
Riconfigurazione con il client Web ESXi v6.0

Per aggiornare le configurazioni delle macchine virtuali utilizzando il client Web ESXi v6.0:



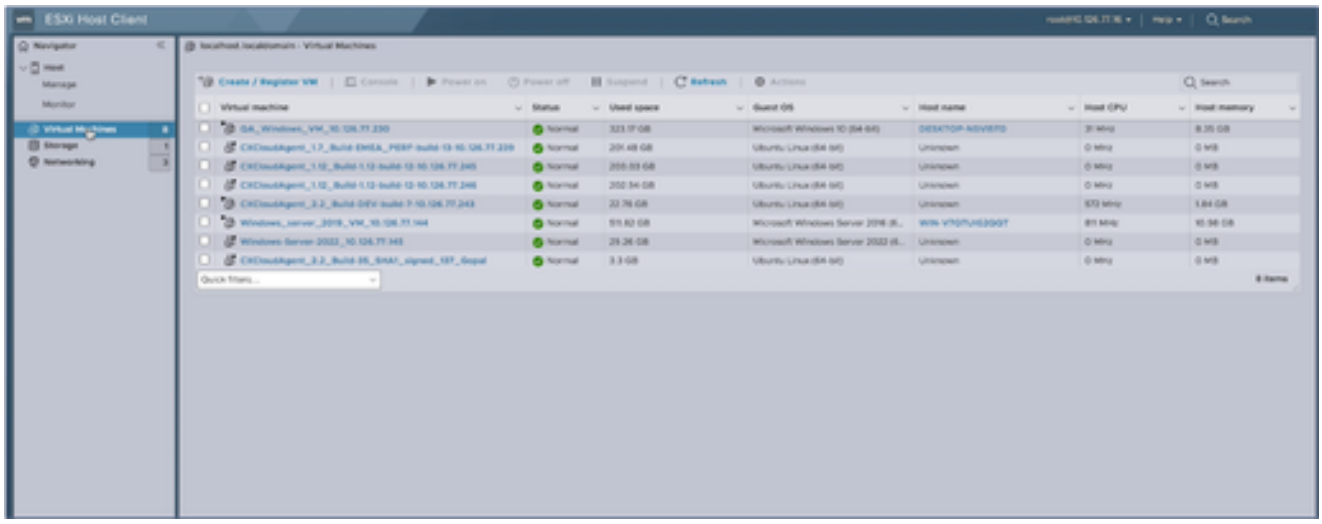
Client ESXi

1. Eseguire il login al client VMware ESXi. Verrà visualizzata la home page.



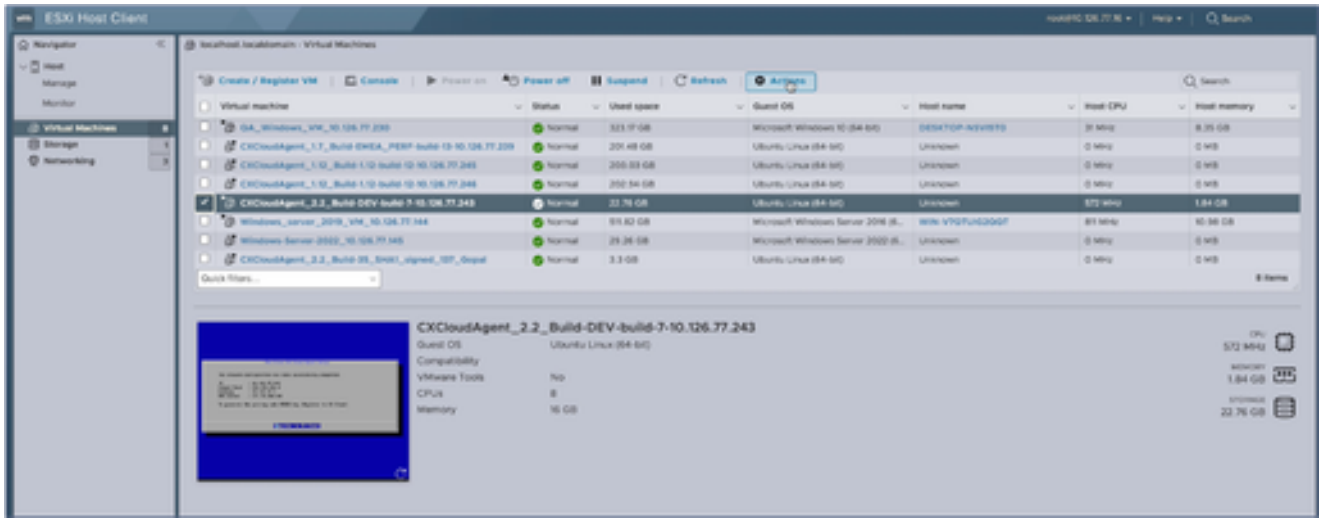
Home page ESXi

2. Fare clic su Macchina virtuale per visualizzare un elenco di macchine virtuali.



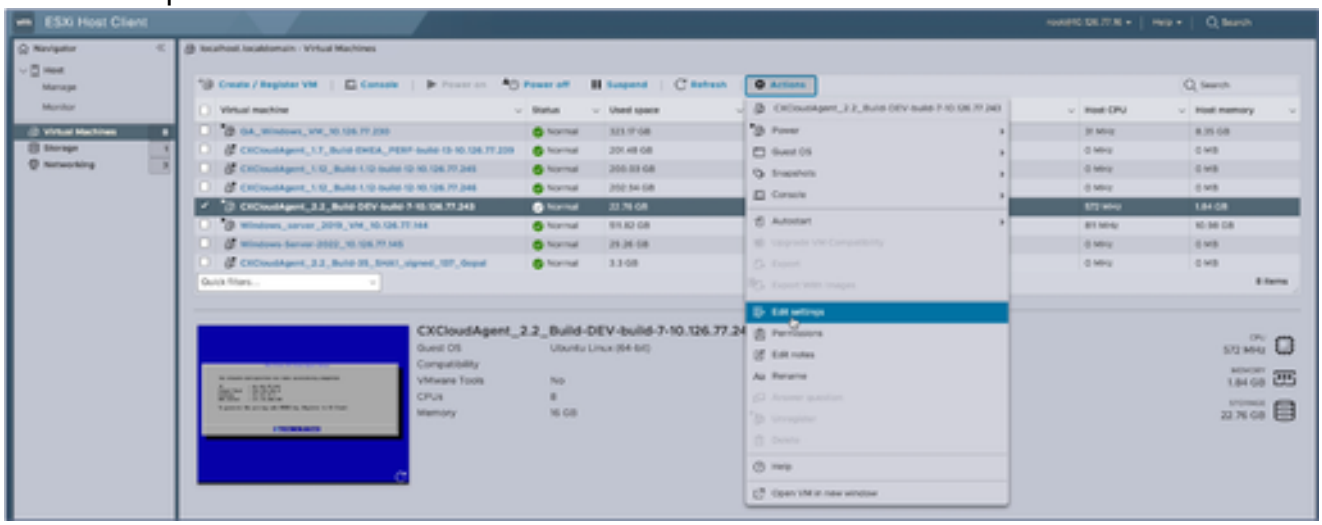
Elenco di macchine virtuali

3. Selezionare la macchina virtuale di destinazione.

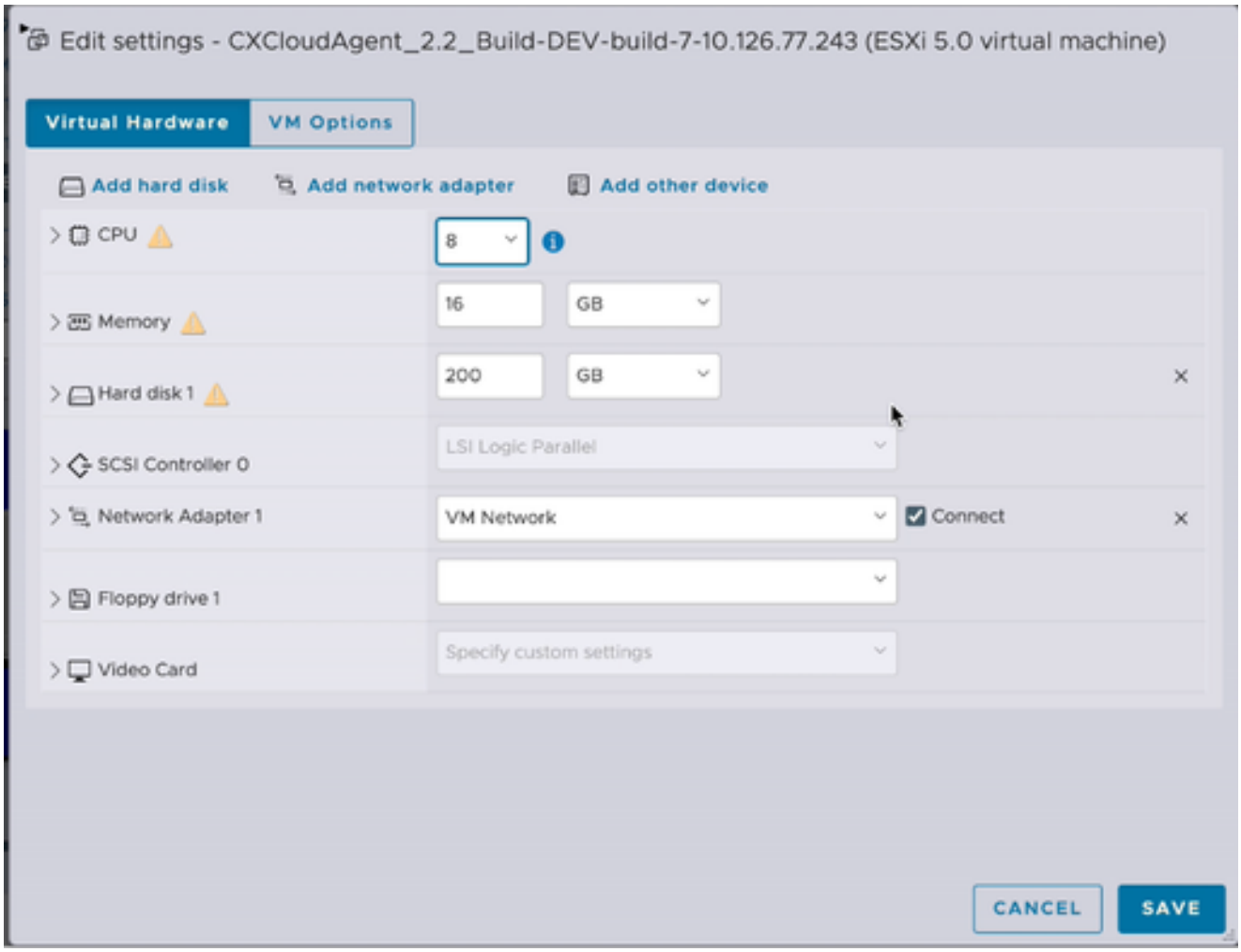


VM di destinazione

4. Fare clic su Azioni e selezionare Modifica impostazioni. Viene visualizzata la finestra Modifica impostazioni.

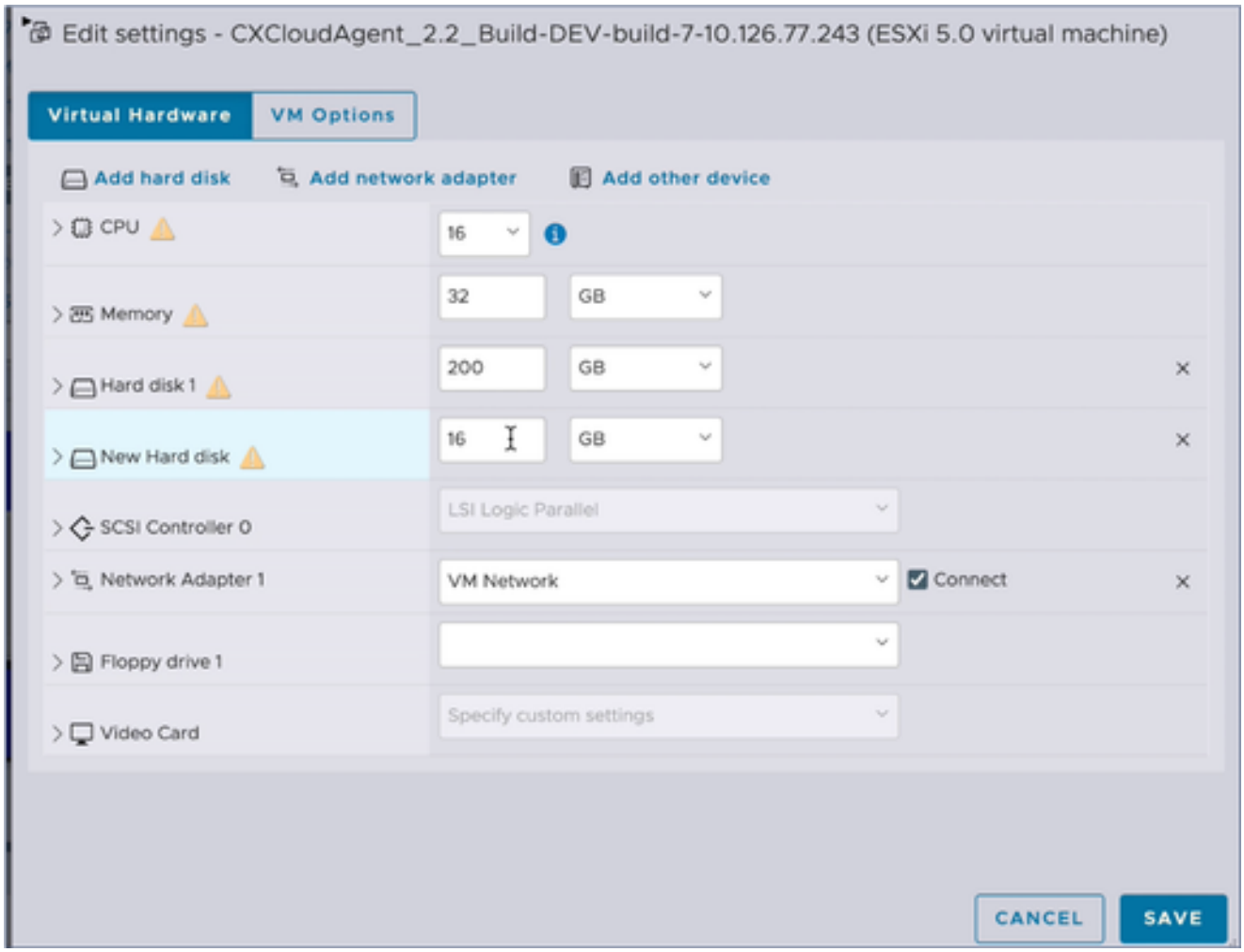


Azioni



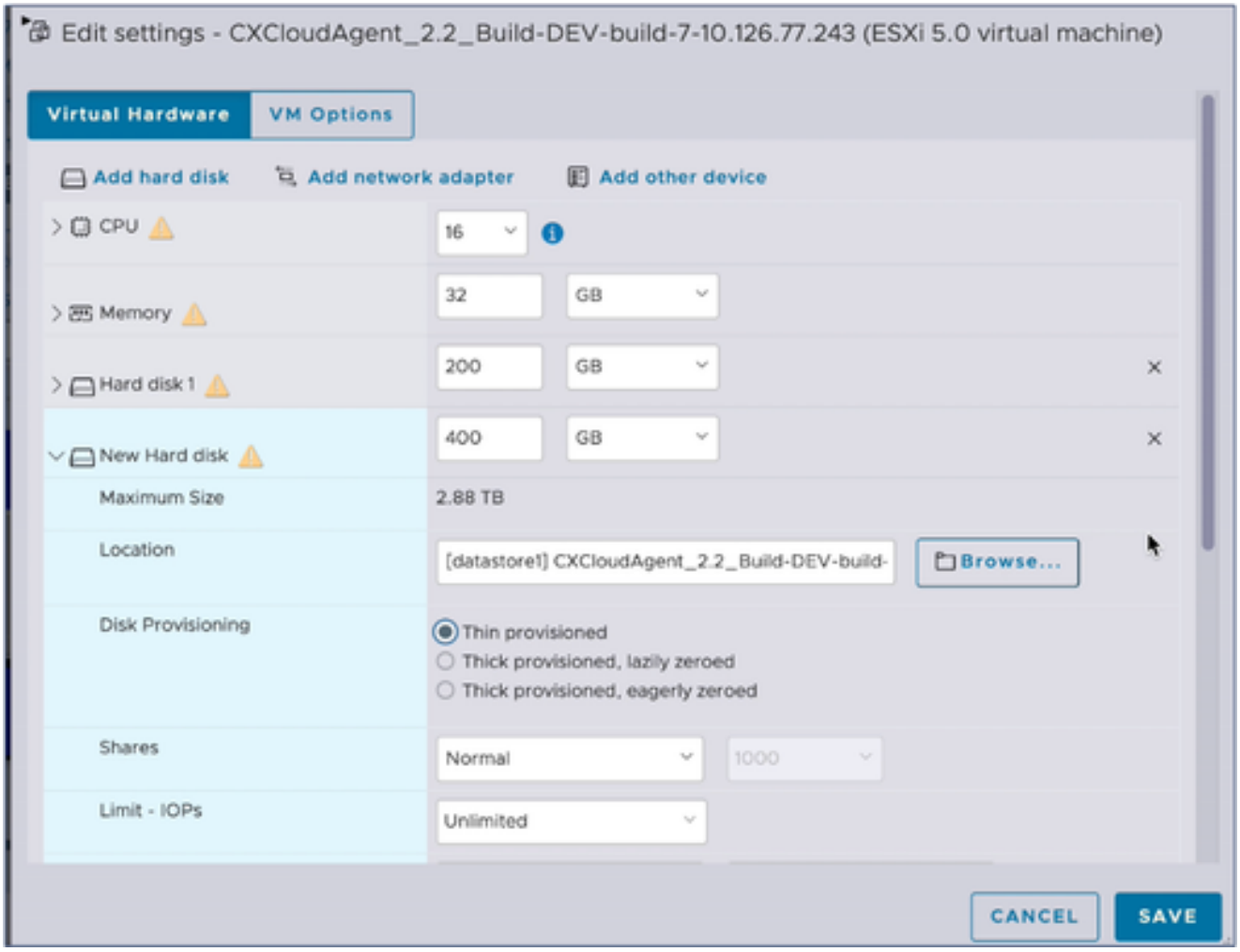
Modifica impostazioni

5. Aggiornare il valore CPU come specificato:
   Medio: 16 core (8 socket *2 core/socket)
   Grande: 32 core (16 socket *2 core/socket)
6. Aggiornare il valore Memory come specificato:
   Media: 32 GB
   Grandi: 64 GB
7. Fare clic su Aggiungi disco rigido > Nuovo disco rigido standard. La nuova voce relativa al disco rigido viene visualizzata nella finestra Modifica impostazioni.



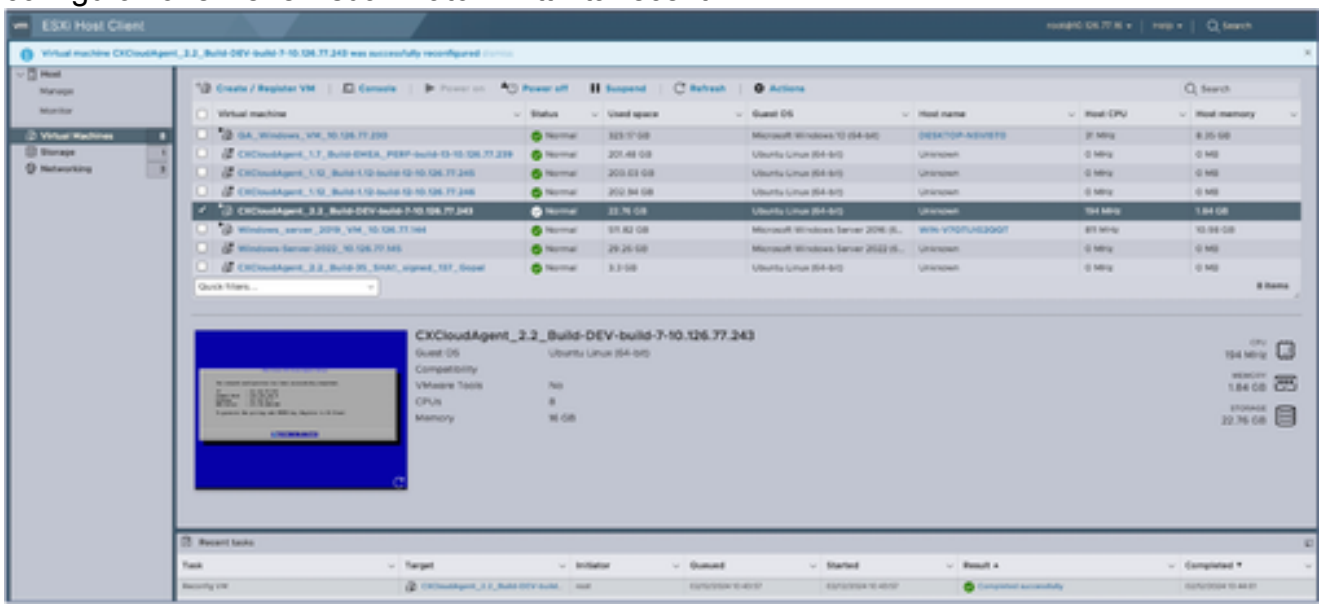
Modifica impostazioni

8. Aggiorna nuovi valori disco rigido come specificato:
   Piccole e medie: 400 GB (dimensioni iniziali 200 GB, aumento dello spazio totale a 600 GB)
   Piccole e grandi: 1.000 GB (dimensioni iniziali 200 GB, aumento dello spazio totale a 1.200 GB)
9. Fare clic sulla freccia per espandere Nuovo disco rigido. Vengono visualizzate le proprietà.



Modifica impostazioni

10. Selezionare il pulsante di opzione Thin provisioning.
11. Fare clic su Save (Salva) per completare la configurazione. L'aggiornamento della configurazione viene visualizzato in Attività recenti.



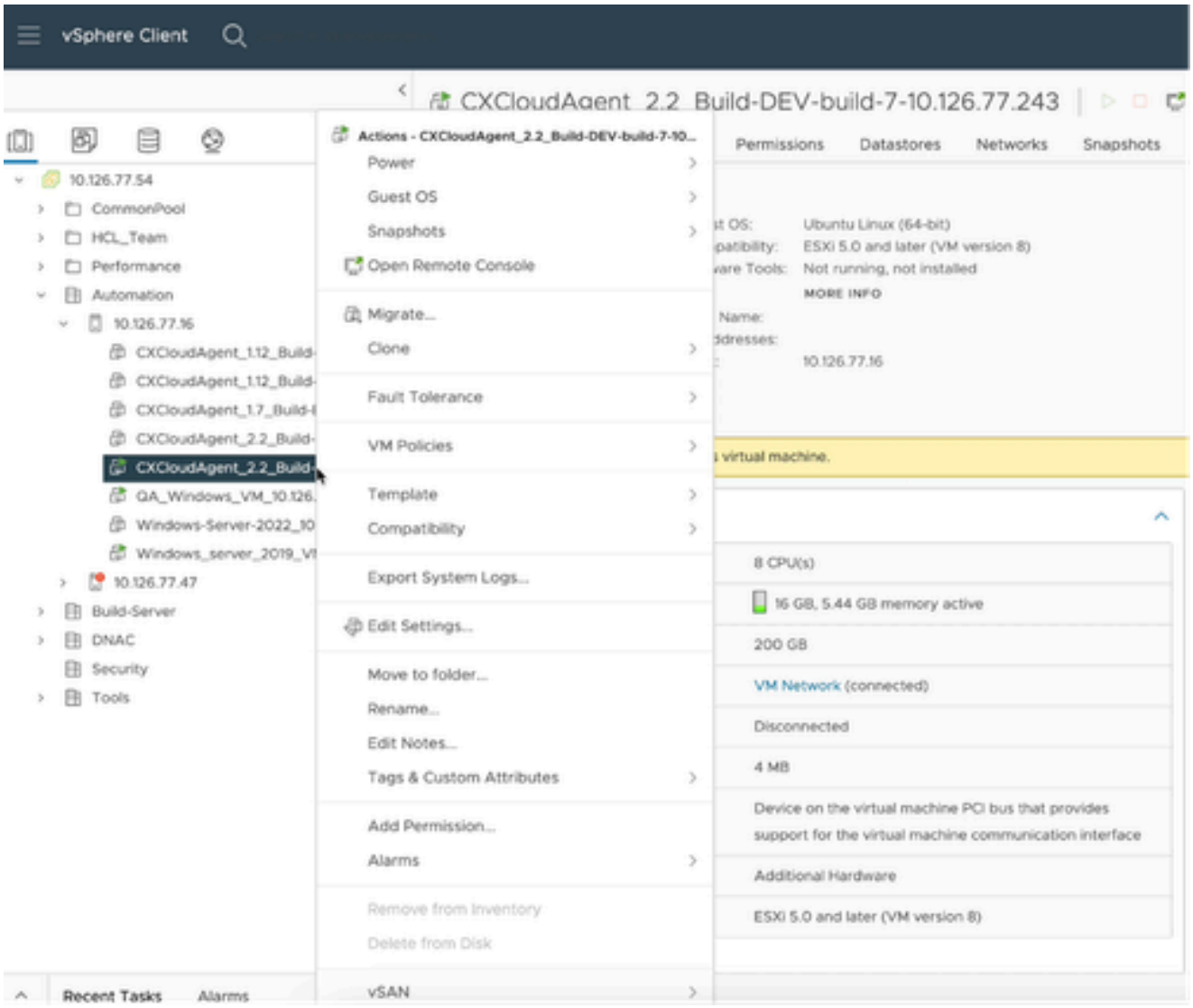
Attività recenti

Riconfigurazione mediante Web Client vCenter

Per aggiornare le configurazioni delle macchine virtuali utilizzando Web Client vCenter:

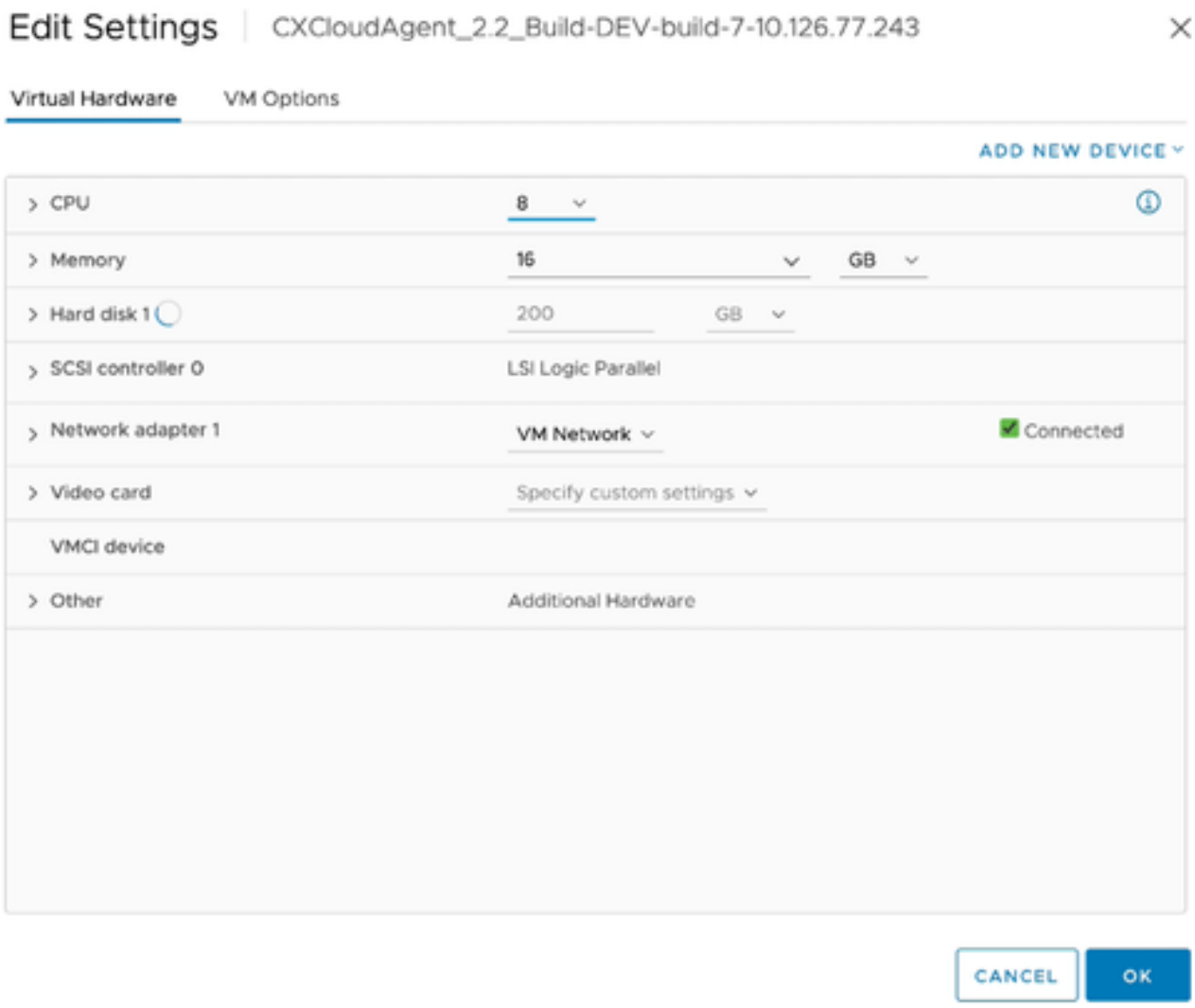
vCenter

1. Accedere a vCenter. Verrà visualizzata la home page.



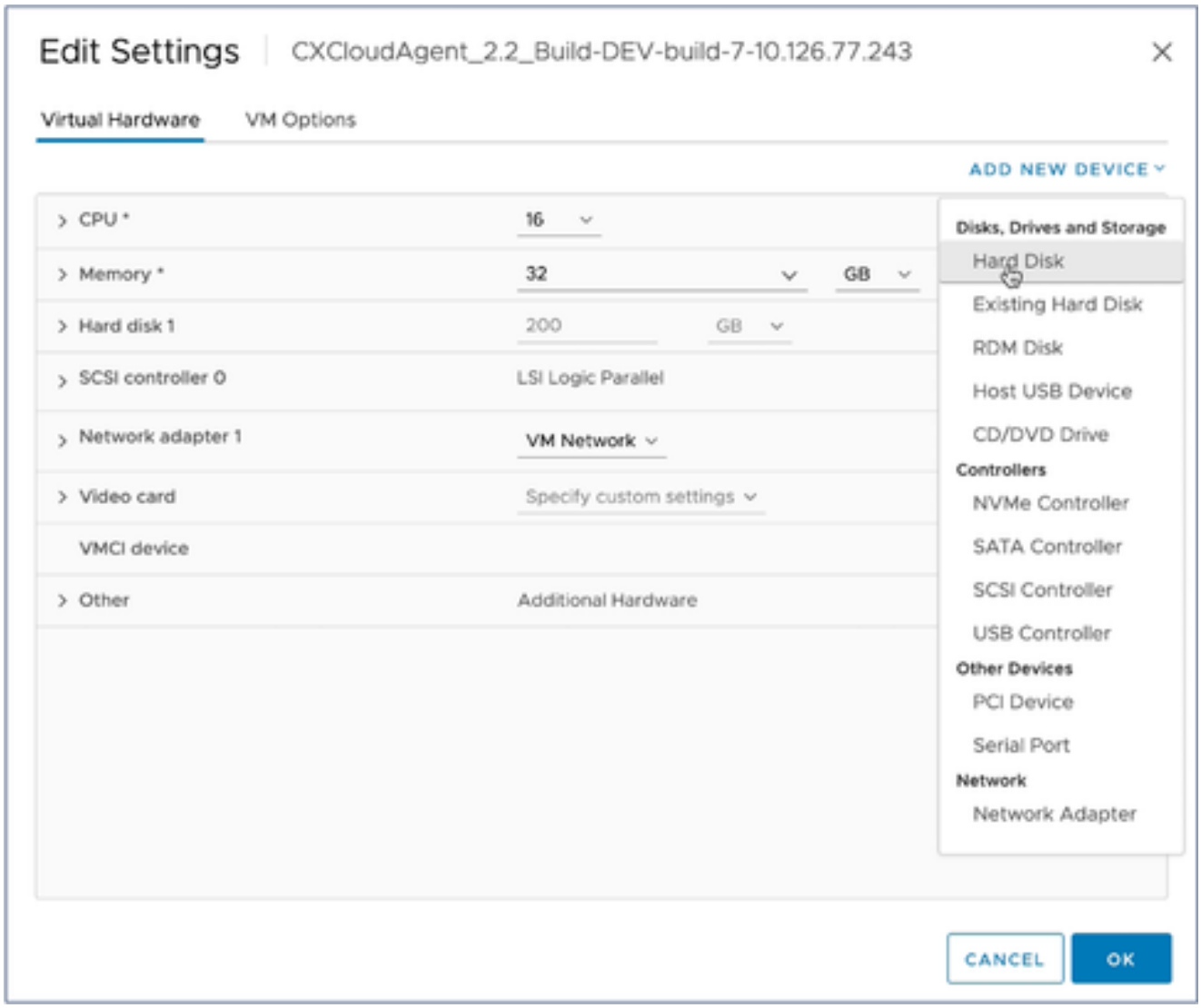
Elenco di macchine virtuali

2. Fare clic con il pulsante destro del mouse sulla VM di destinazione e selezionare Modifica impostazioni dal menu. Viene visualizzata la finestra Modifica impostazioni.



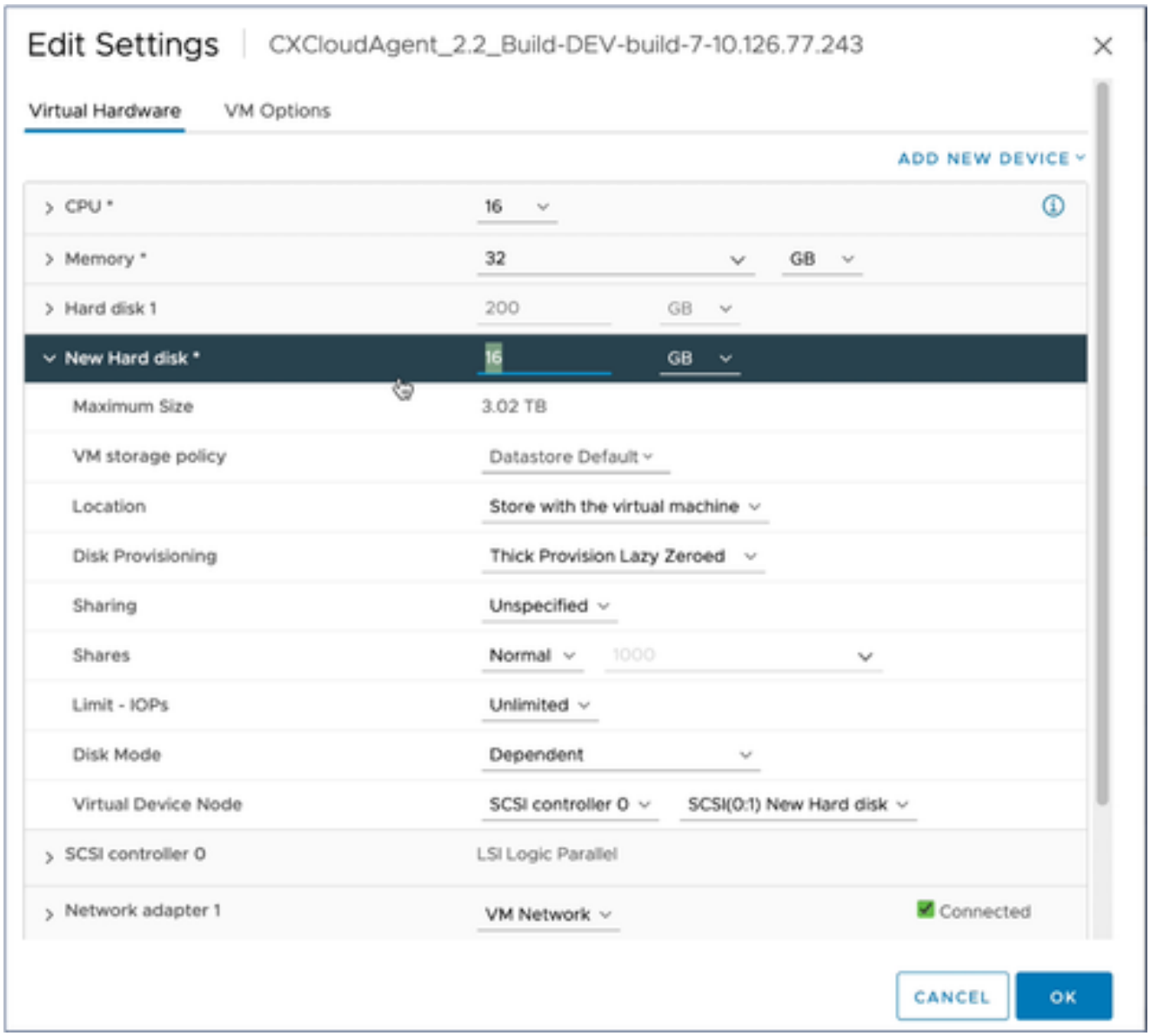
Modifica impostazioni

3. Aggiornare i valori CPU come specificato:
   Medio: 16 core (8 socket *2 core/socket)
   Grande: 32 core (16 socket *2 core/socket)
4. Aggiornare i valori di Memory come specificato:
   Media: 32 GB
   Grandi: 64 GB



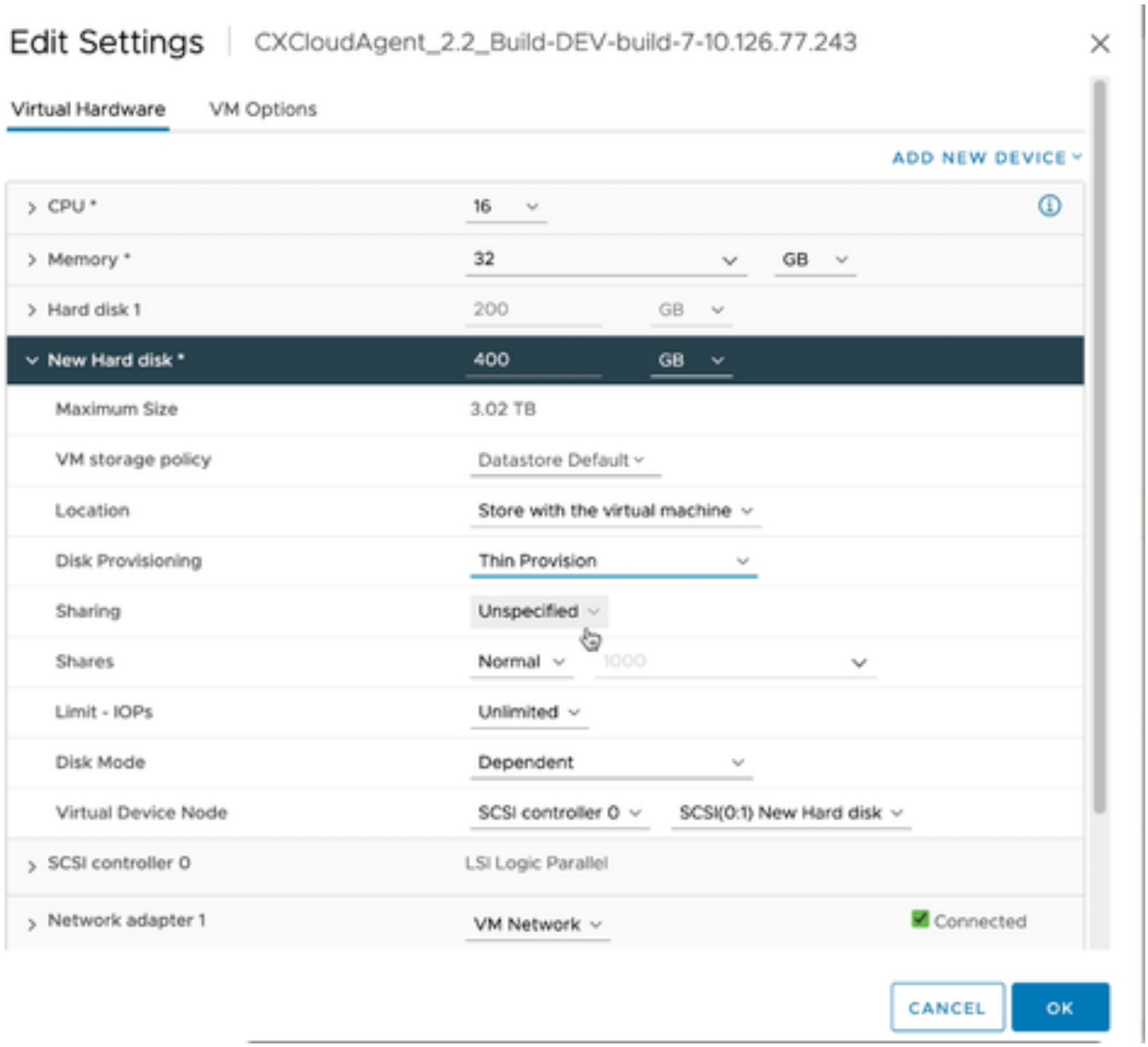
Modifica impostazioni

5. Fare clic su Add New Device (Aggiungi nuova periferica) e selezionare Hard Disk (Disco rigido). Viene aggiunta la voce Nuovo disco rigido.



Modifica impostazioni

6. Aggiorna nuova memoria disco rigido come specificato:
   Piccole e medie: 400 GB (dimensioni iniziali 200 GB, aumento dello spazio totale a 600 GB)
   Piccole e grandi: 1.000 GB (dimensioni iniziali 200 GB, aumento dello spazio totale a 1.200 GB)



Modifica impostazioni

7. Selezionare Thin Provision dall'elenco a discesa Disk Provisioning.
8. Fare clic su OK per completare l'aggiornamento.

Implementazione e configurazione della rete

Selezionare una delle seguenti opzioni per distribuire l'agente cloud CX:

- Per selezionare VMware vSphere/vCenter Thick Client ESXi 5.5/6.0, passare a Thick Client
- Per selezionare VMware vSphere/vCenter Web Client ESXi 6.0, passare a Web Client o vSphere Center
- Per selezionare Oracle Virtual Box 5.2.30, passare a Oracle VM
- Per selezionare Microsoft Hyper-V, passare a Hyper-V

Implementazione dell'OVA

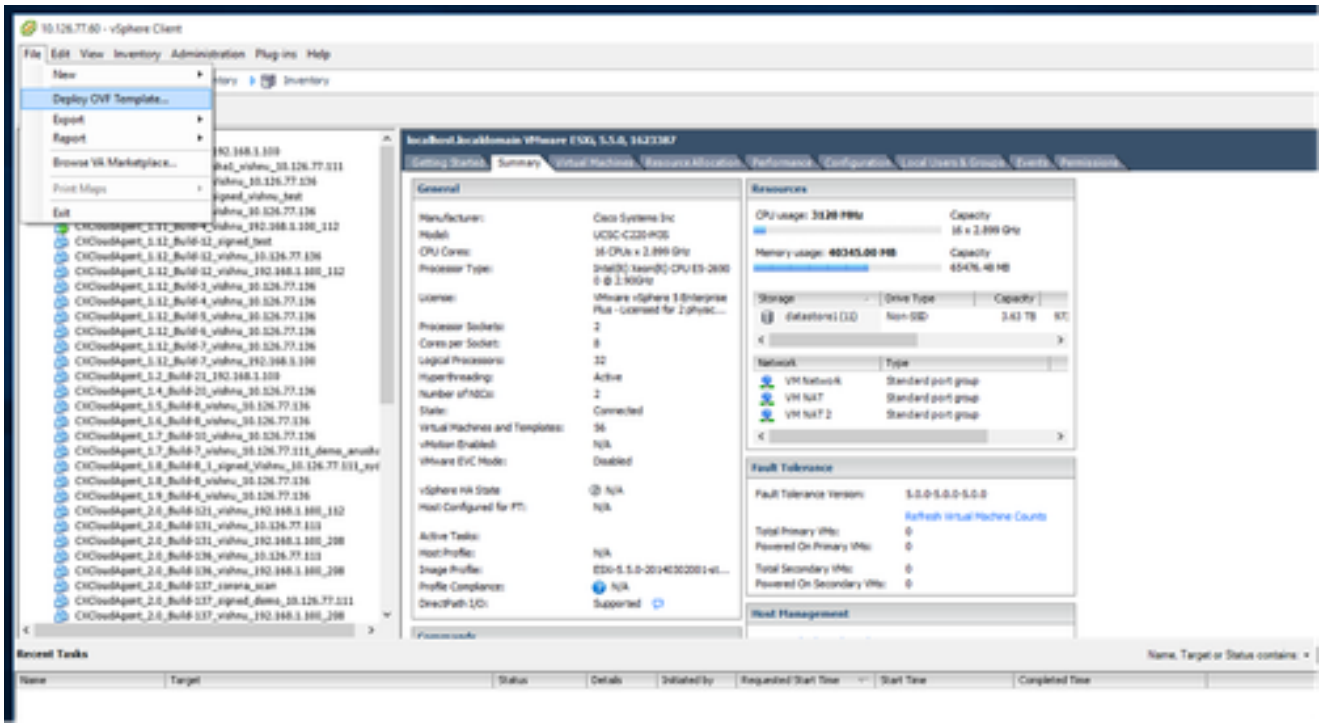
Installazione del thick client ESXi 5.5/6.0

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.

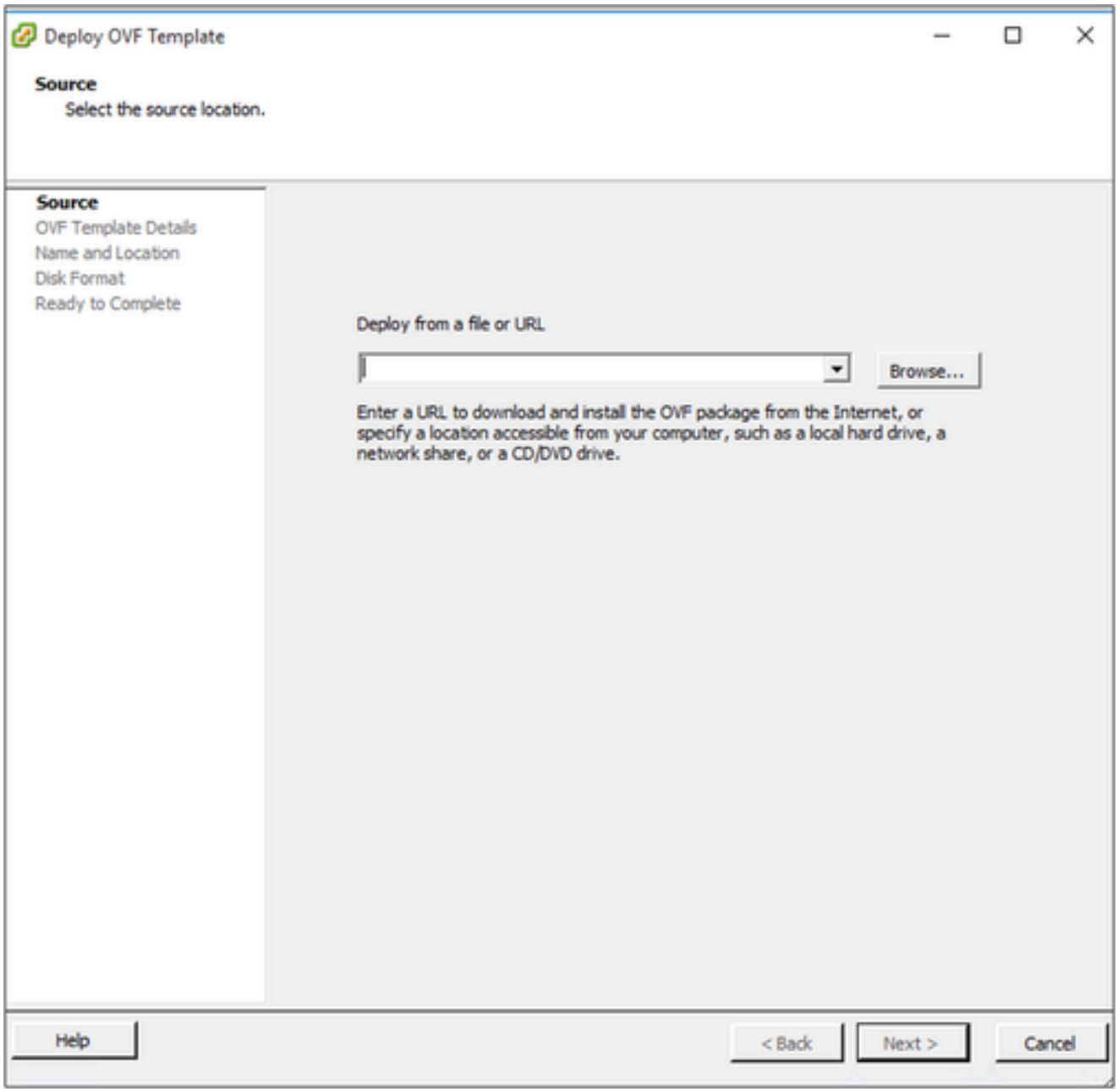
Accesso

2. Dal menu, selezionare File > Distribuisci modello OVF.



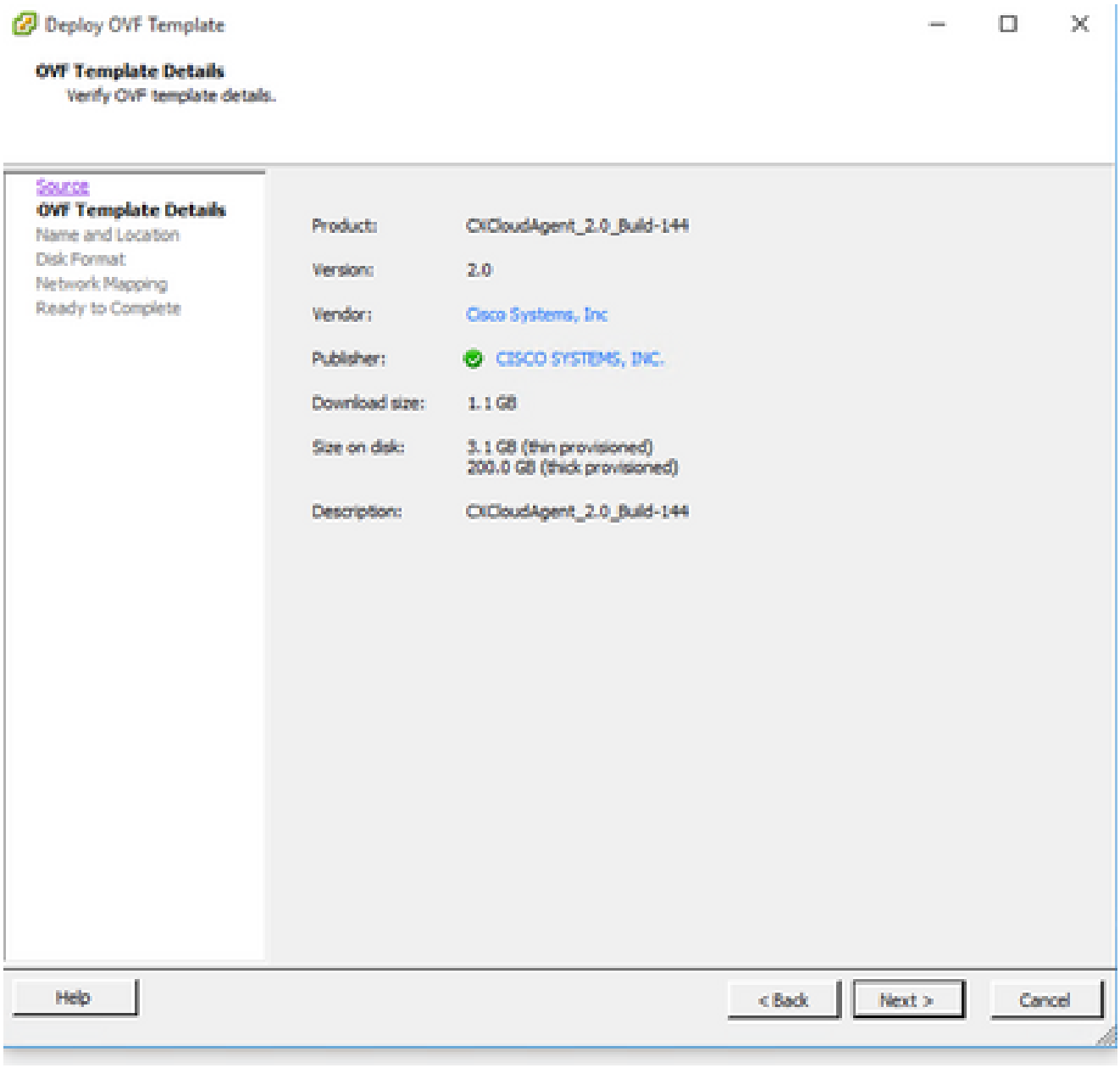
Client vSphere

3. Individuare e selezionare il file OVA e fare clic su Avanti.



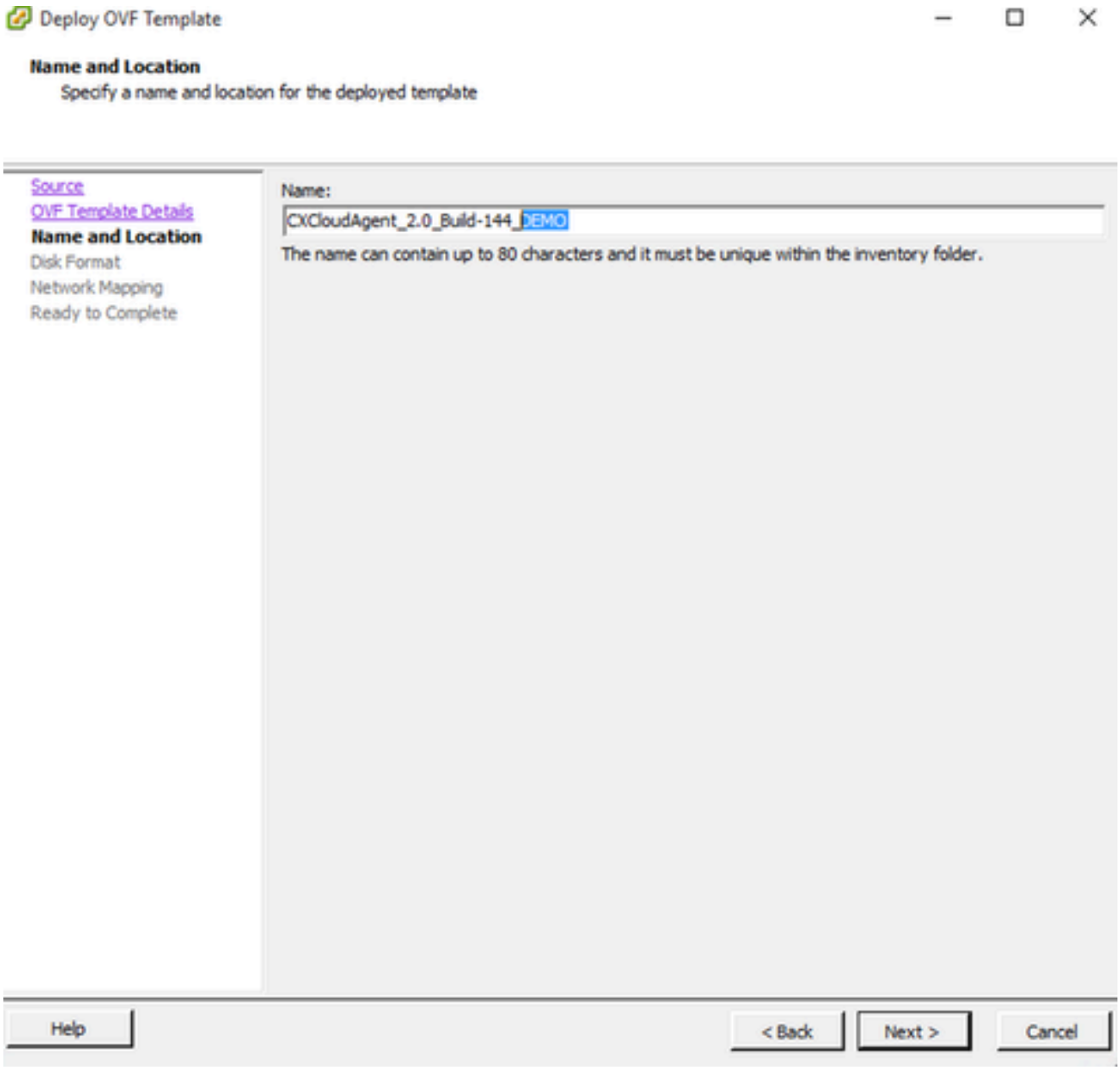
Percorso OVA

4. Verificare i dettagli OVF e fare clic su Avanti.



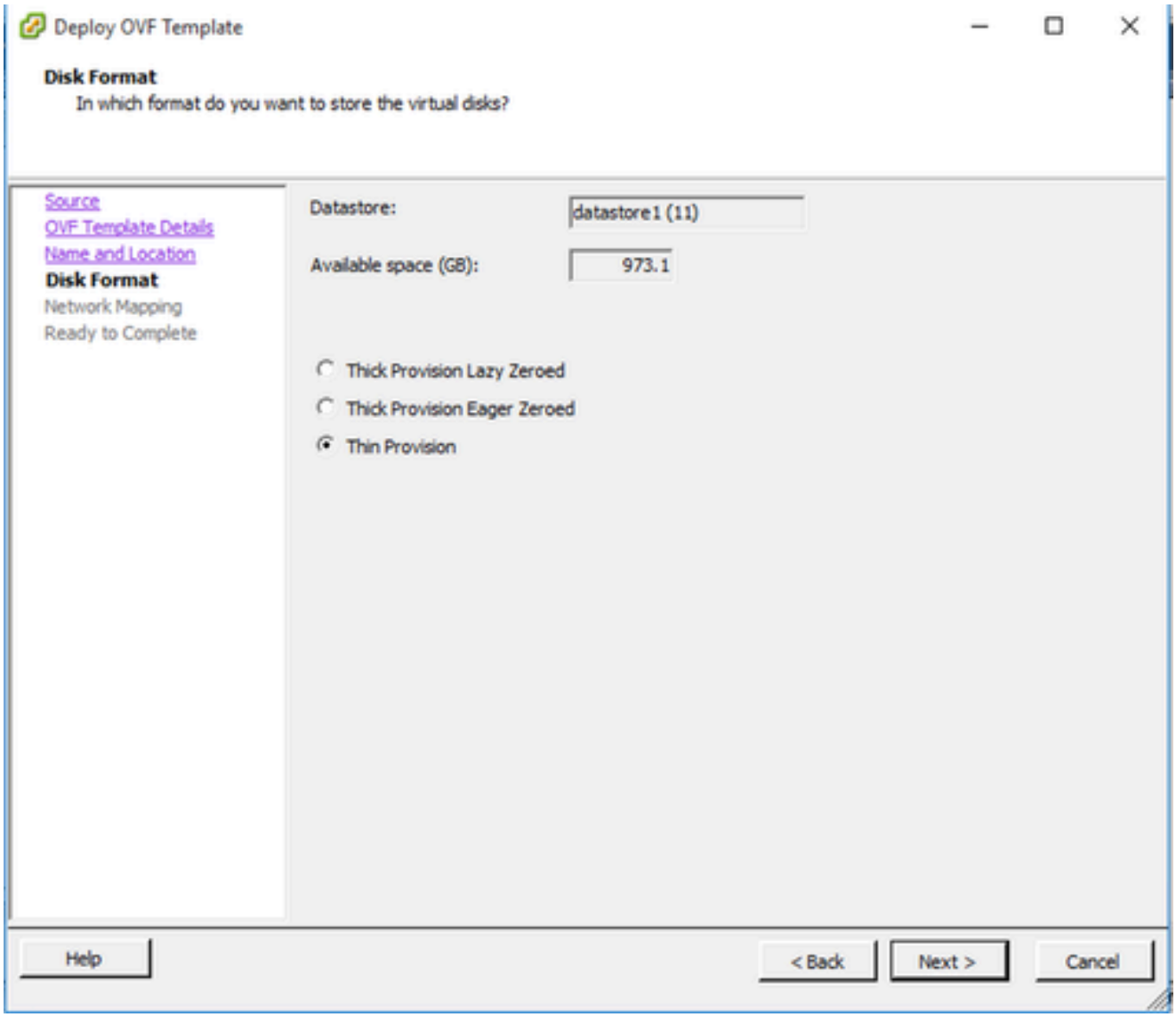
Dettagli del modello

5. Immettere un nome univoco e fare clic su Avanti.



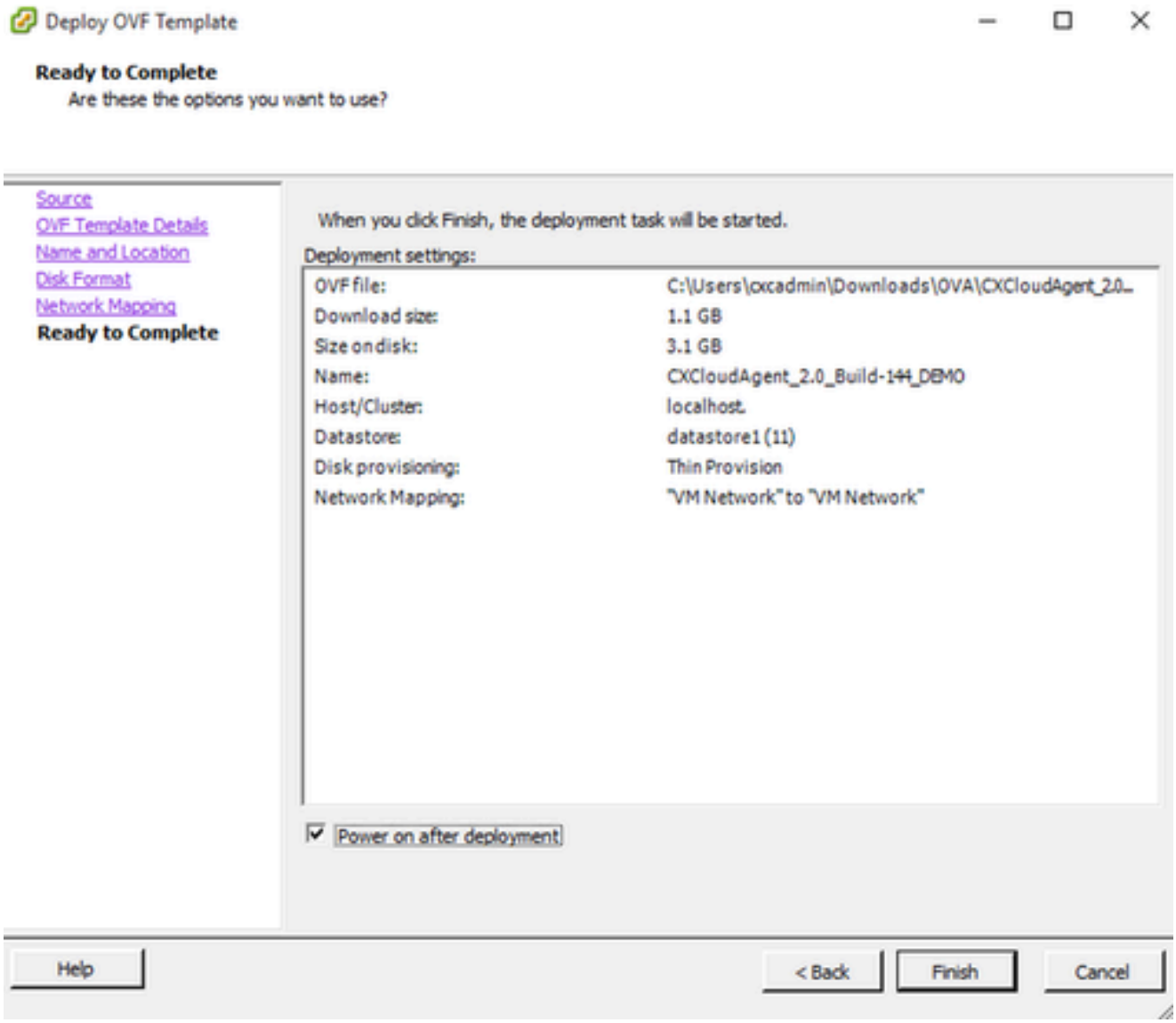
Nome e posizione

6. Selezionare un formato disco e fare clic su Avanti (si consiglia il thin provisioning).



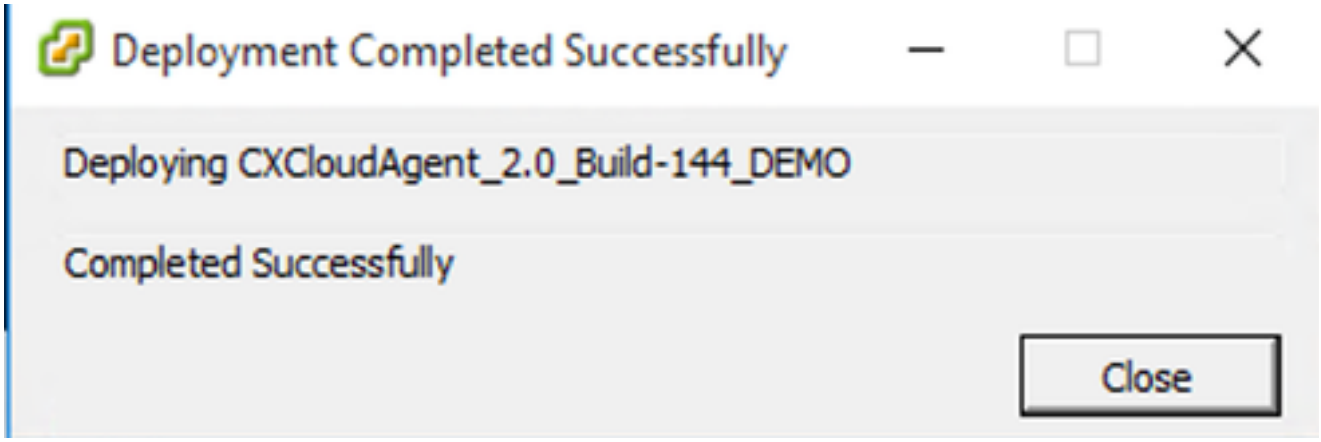
Formato del disco

7. Selezionare la casella di controllo Accendi dopo la distribuzione e fare clic su Chiudi.



Pronto per il completamento

L'installazione può richiedere alcuni minuti. Al completamento della distribuzione viene visualizzata la conferma.



Distribuzione completata

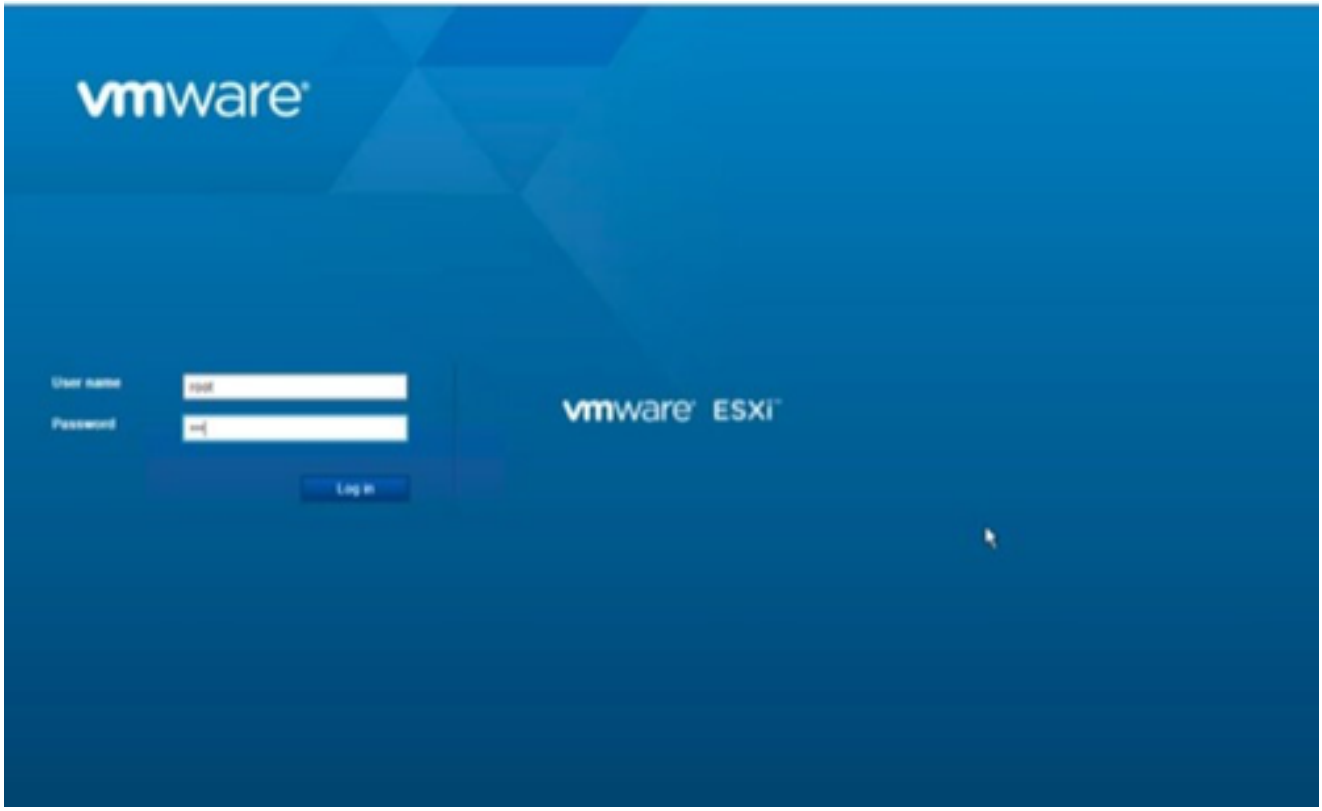
8. Selezionare la VM distribuita, aprire la console e passare a Configurazione di rete per

procedere con i passaggi successivi.

Installazione del client Web ESXi 6.0

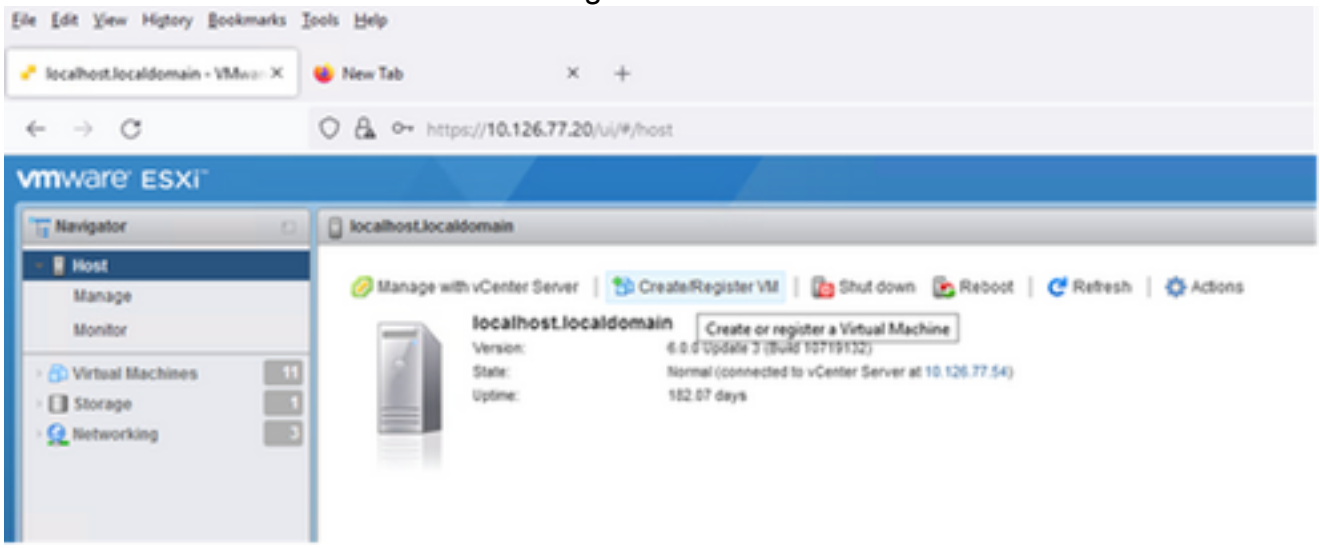
Questo client distribuisce l'agente cloud CX tramite il Web vSphere.

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



Accesso a VMware ESXi

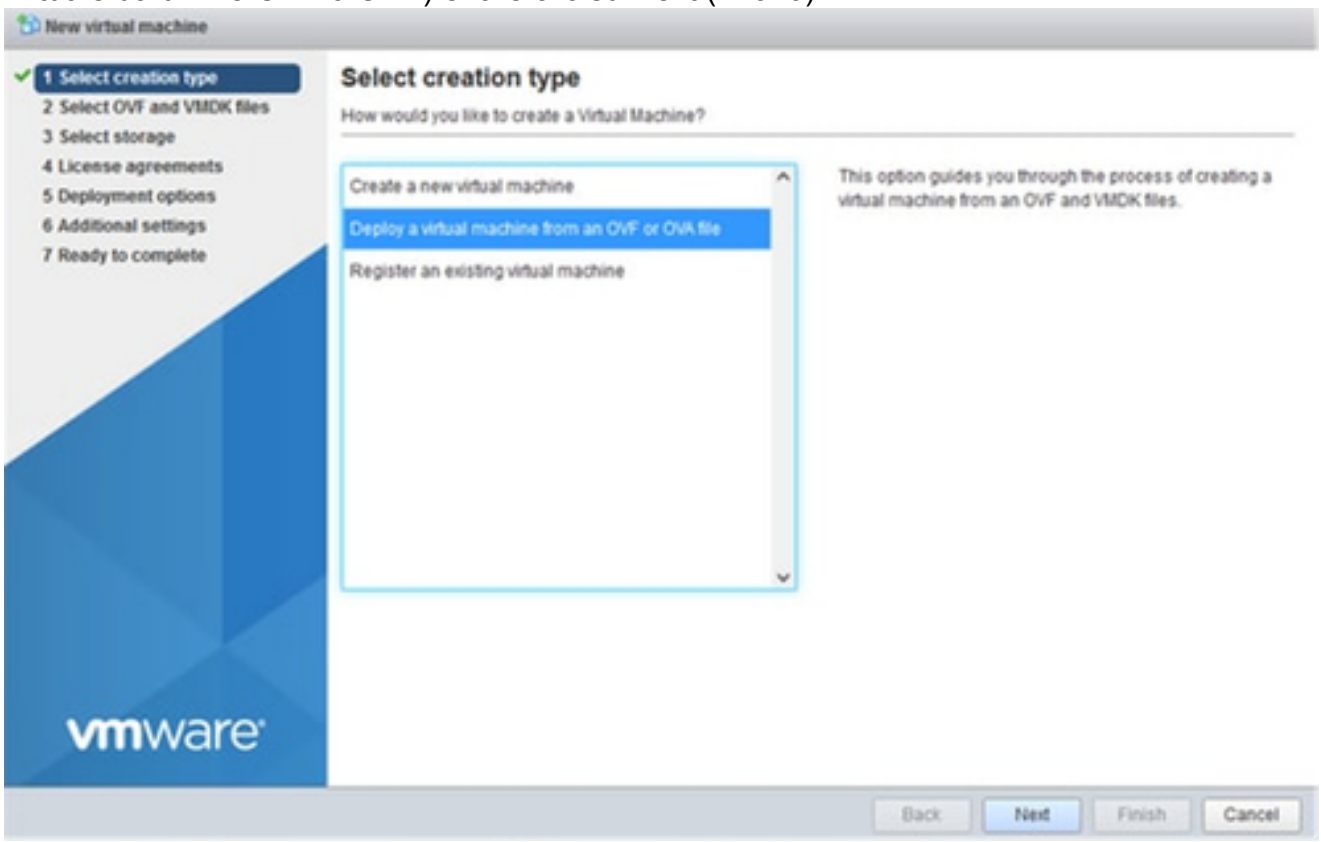
2. Selezionare Virtual Machine > Create/Register VM.



Creazione della VM

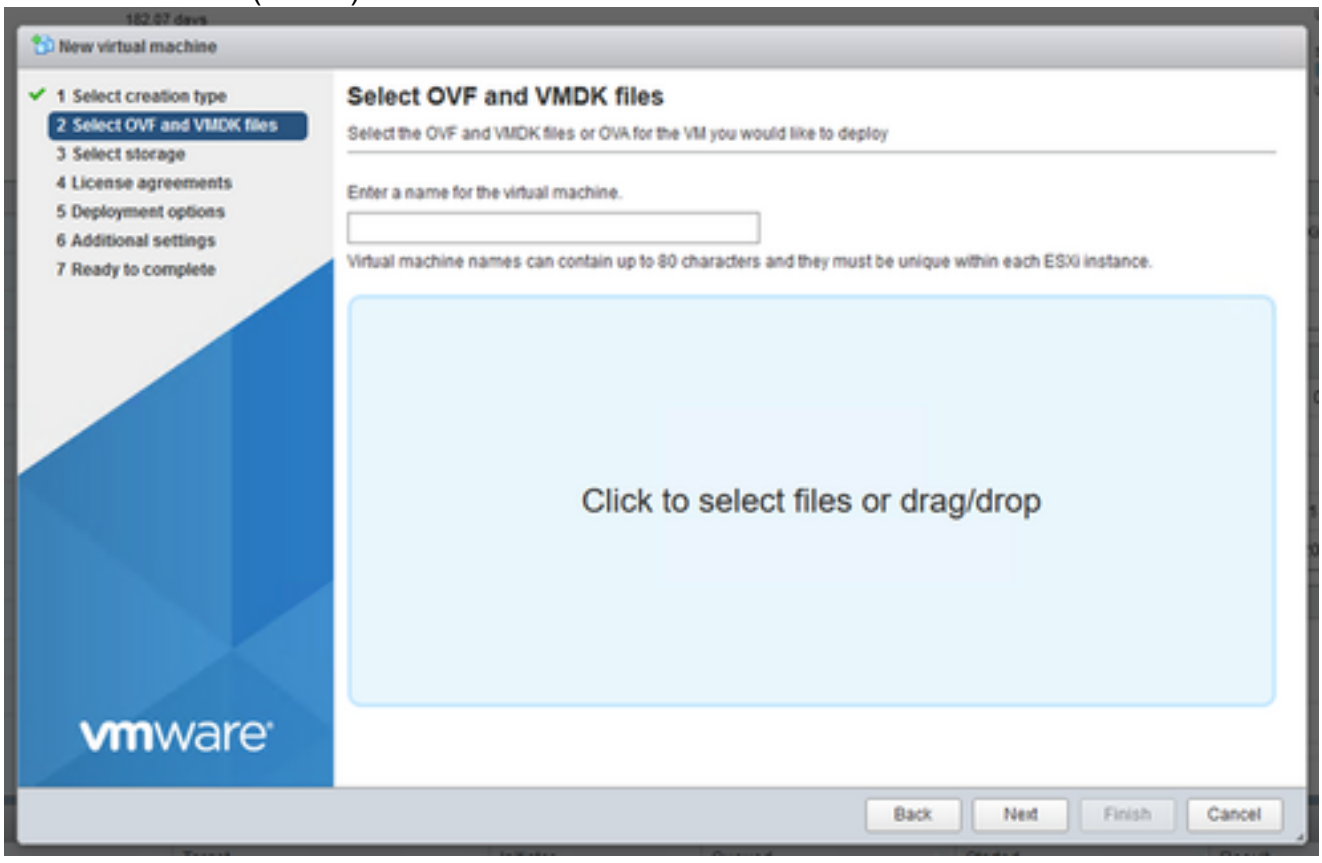
3. Selezionare Deploy a virtual machine from an OVF or OVA file (Implementa una macchina

virtuale da un file OVF o OVA) e fare clic su Next (Avanti).



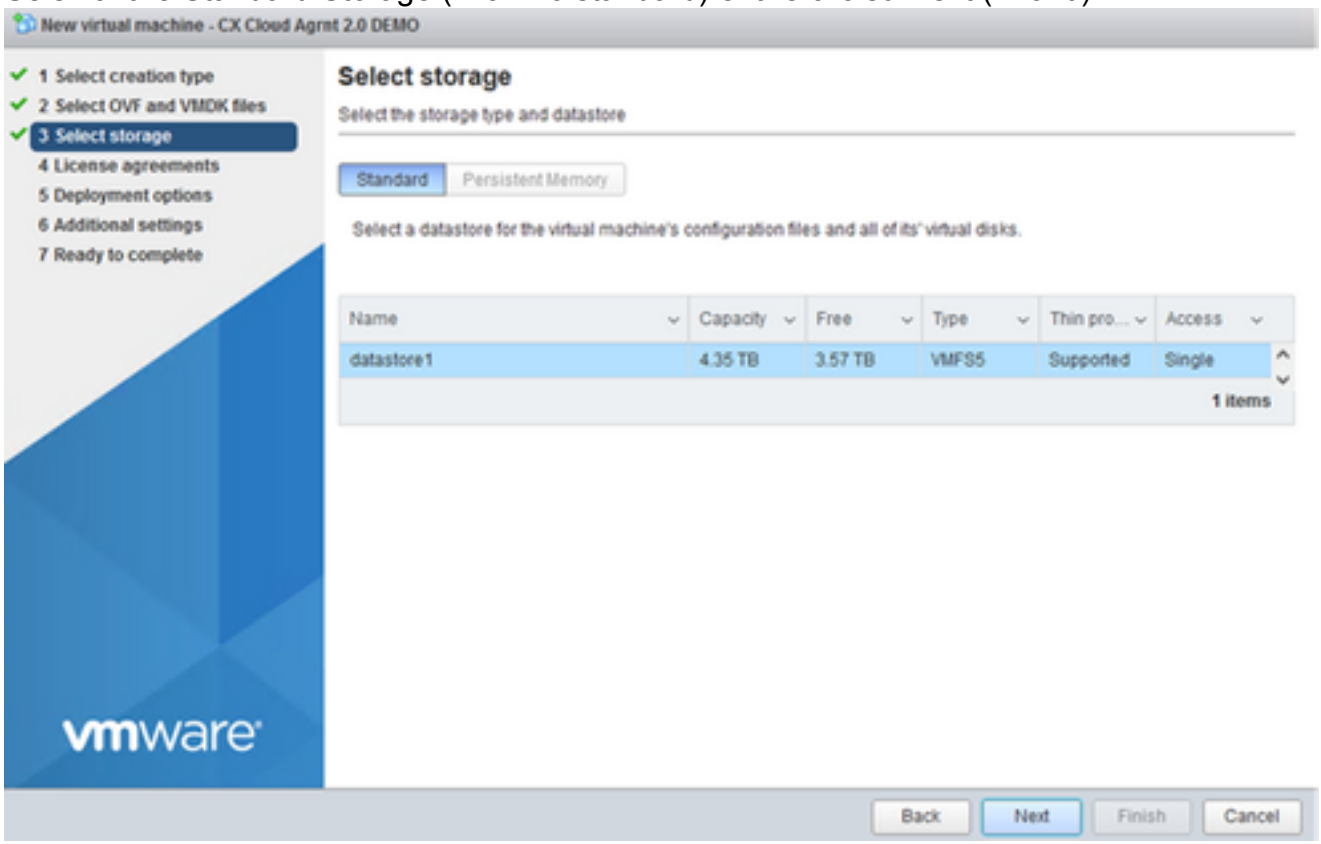
Seleziona tipo di creazione

4. Immettere il nome della macchina virtuale, selezionare il file o trascinare il file OAV scaricato.
5. Fare clic su Next (Avanti).



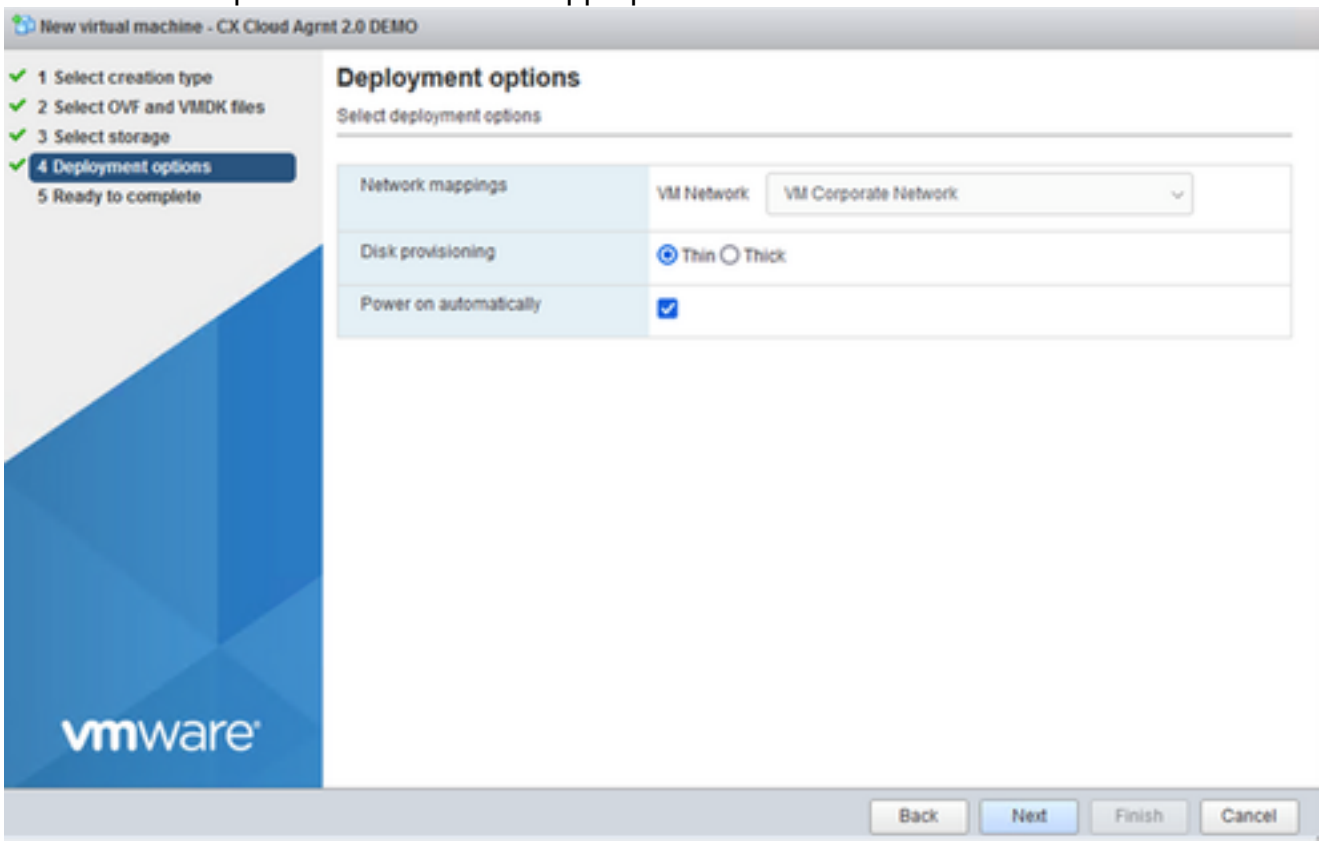
Selezione dell'OVA

6. Selezionare Standard Storage (Archivio standard) e fare clic su Next (Avanti).

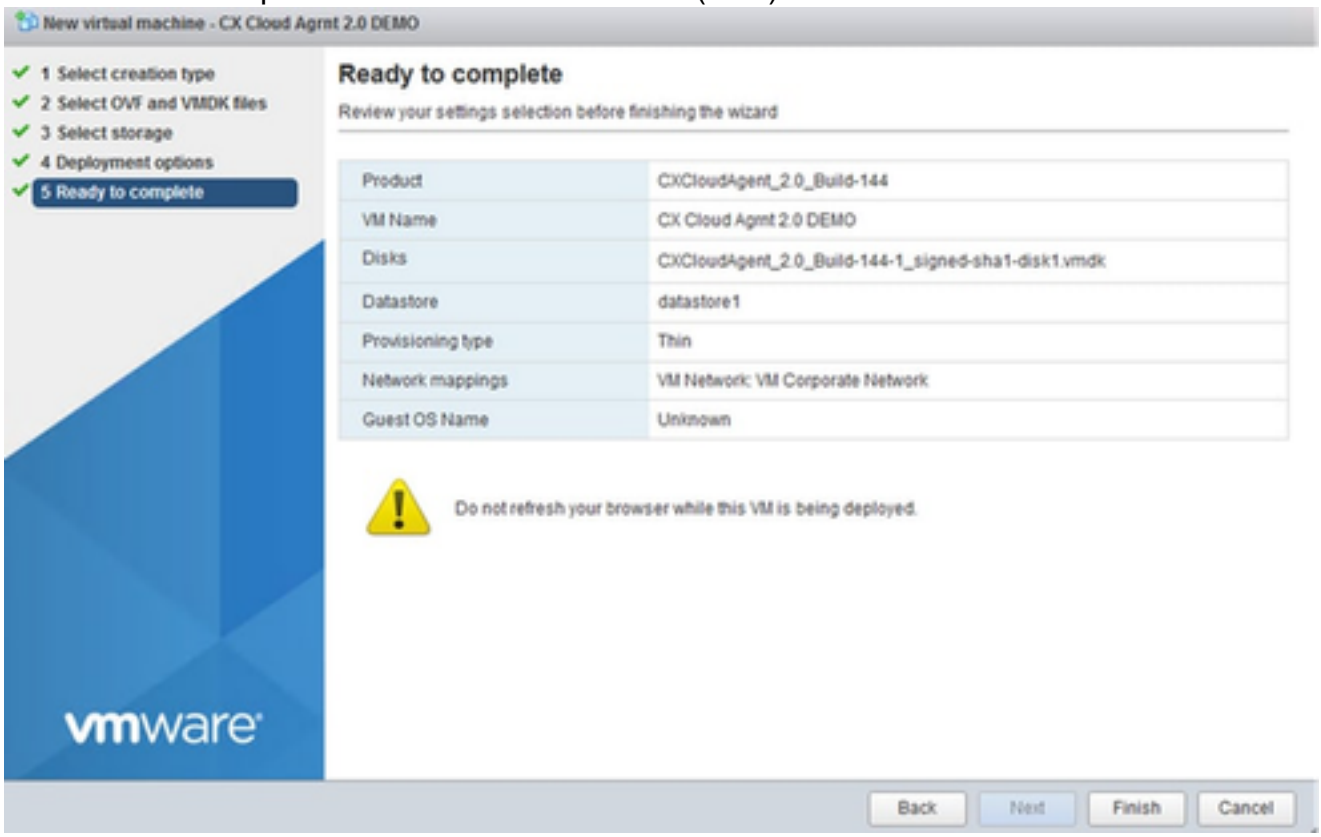


Selezione dell'archivio

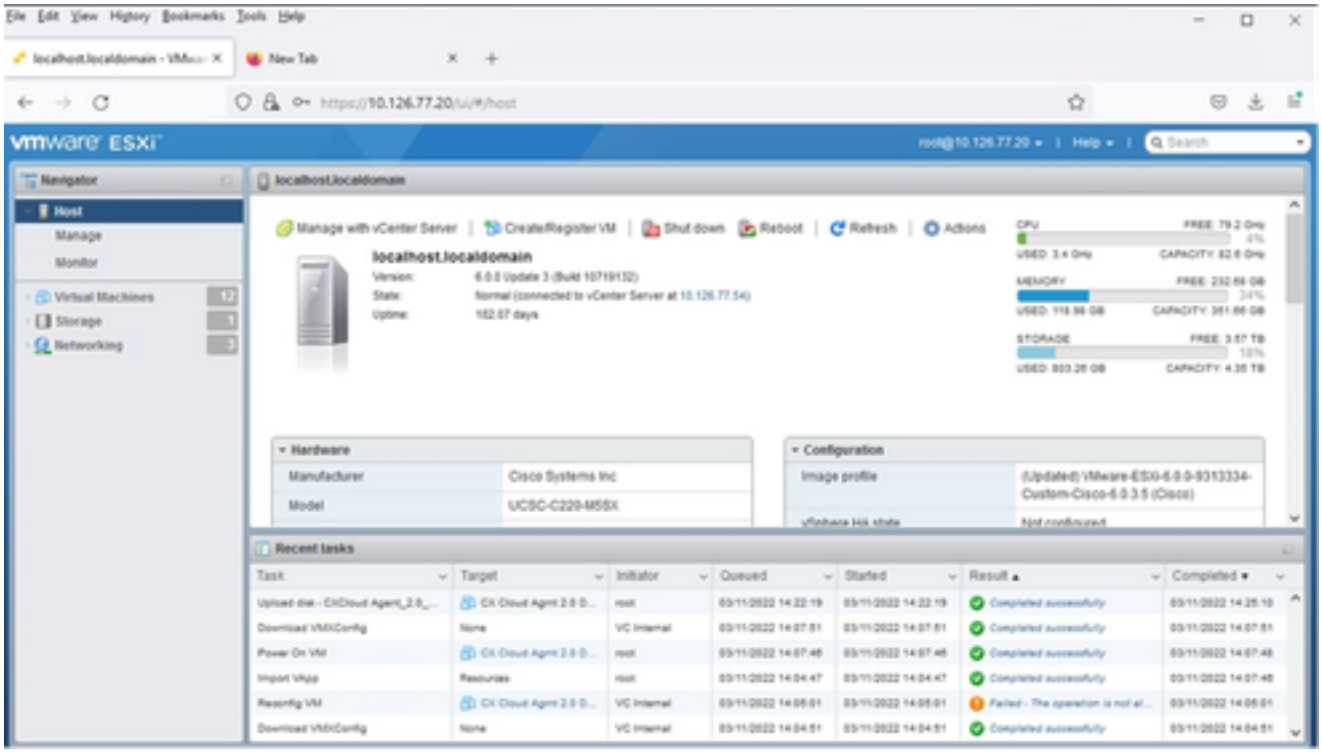
7. Selezionare le opzioni di distribuzione appropriate e fare clic su Avanti.



8. Riesaminare le impostazioni e fare clic su Finish (Fine).

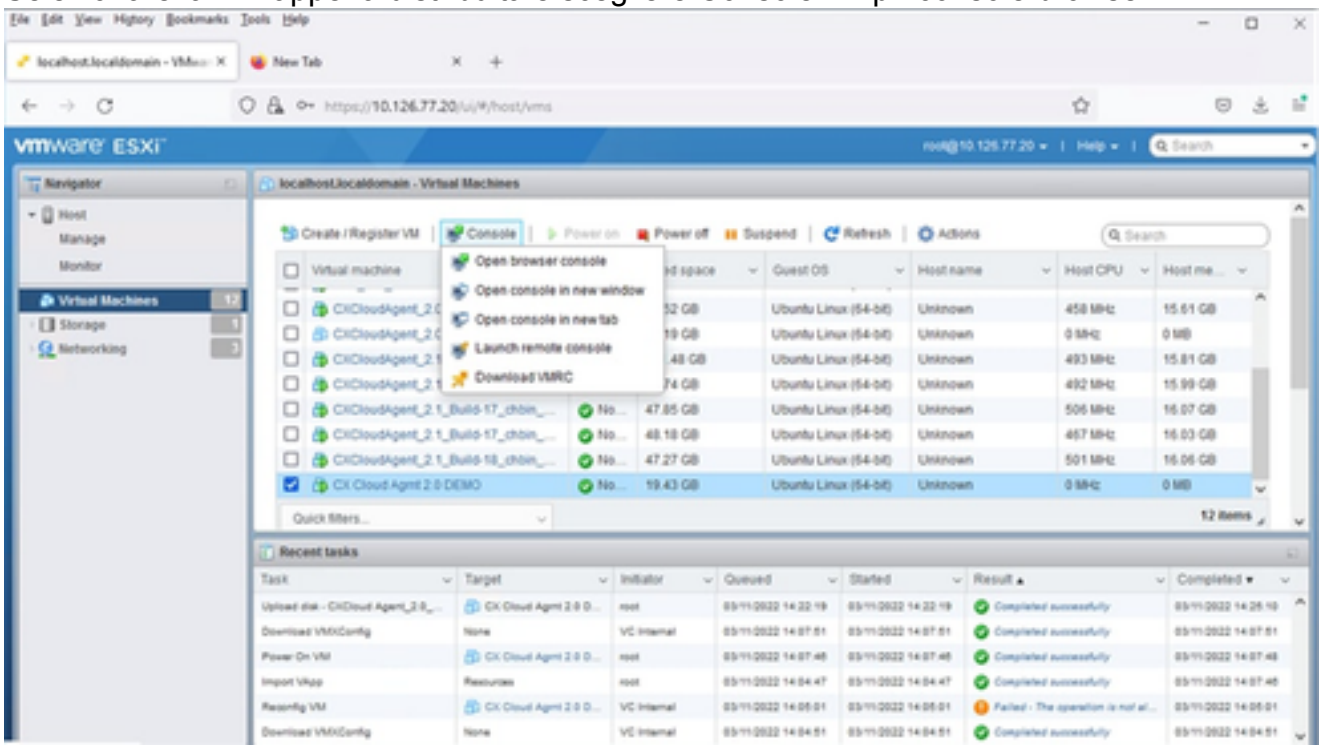


Pronto per il completamento



Procedura completata

9. Selezionare la VM appena distribuita e scegliere Console > Apri console browser.



Console

10. Passare a Configurazione di rete per continuare con i passaggi successivi.

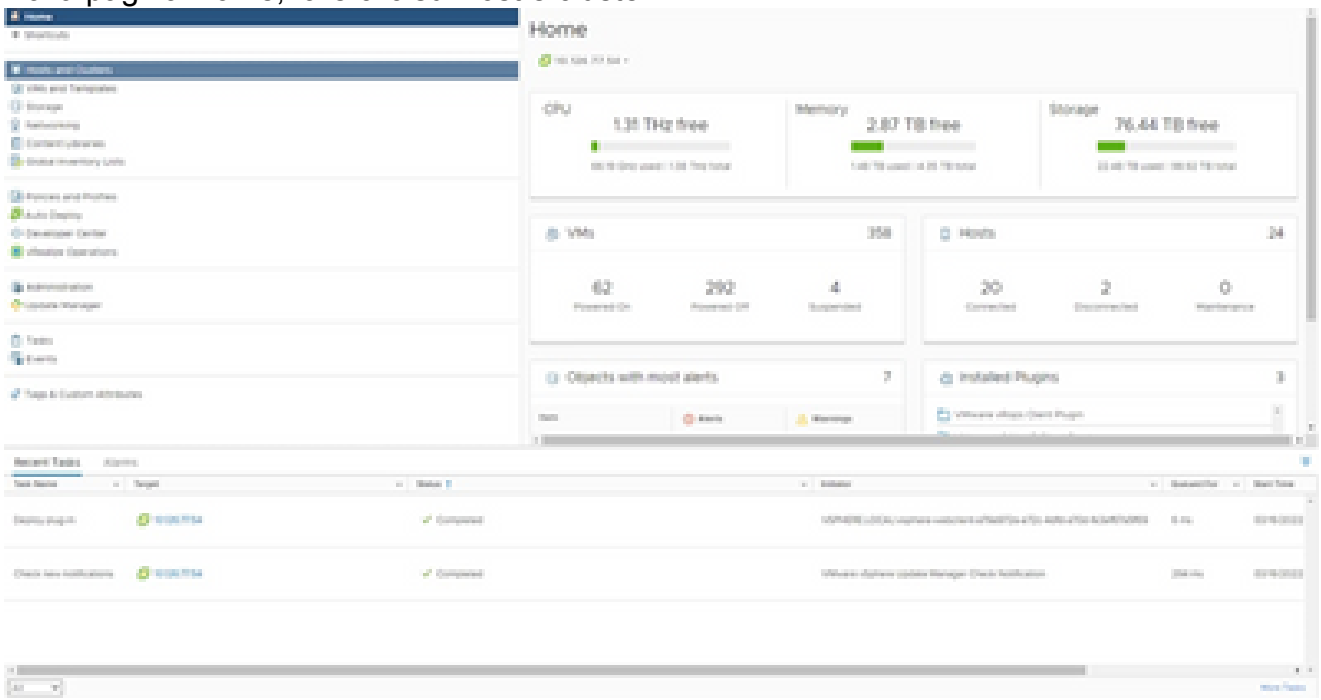
Installazione del client Web vCenter

Eseguire questa procedura:

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

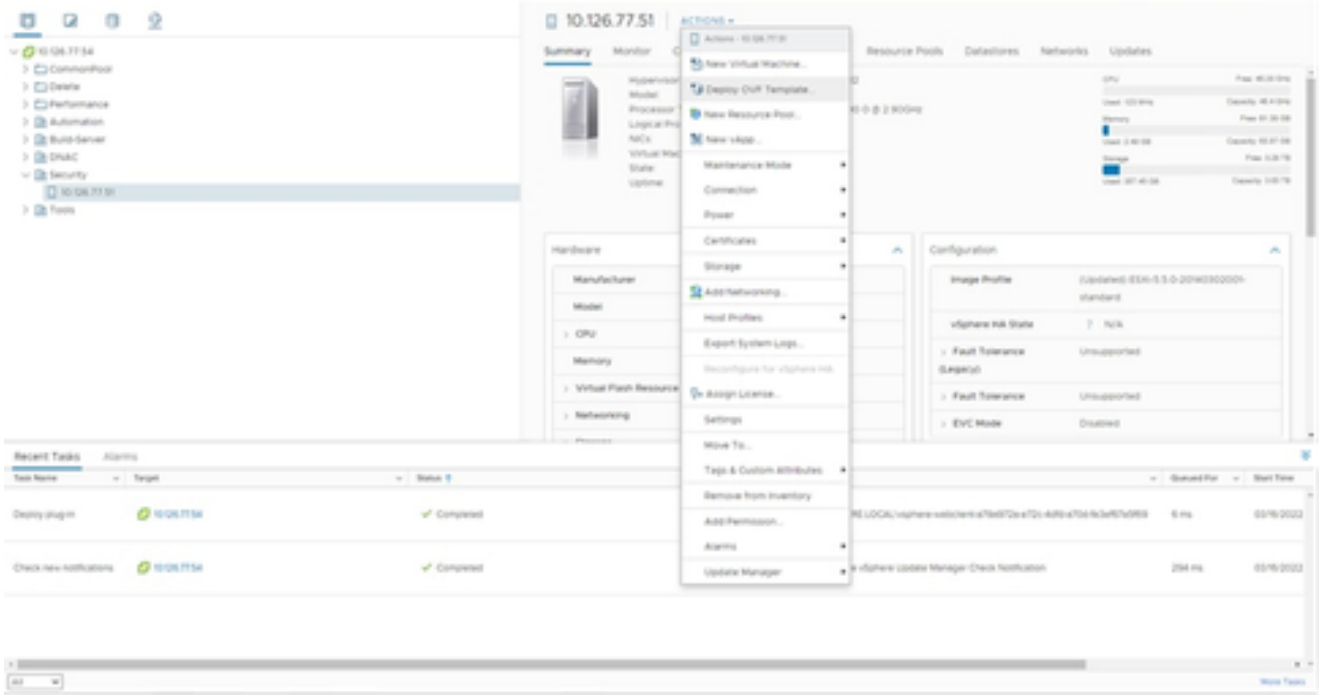
Accedi

2. Dalla pagina Home, fare clic su Host e cluster.

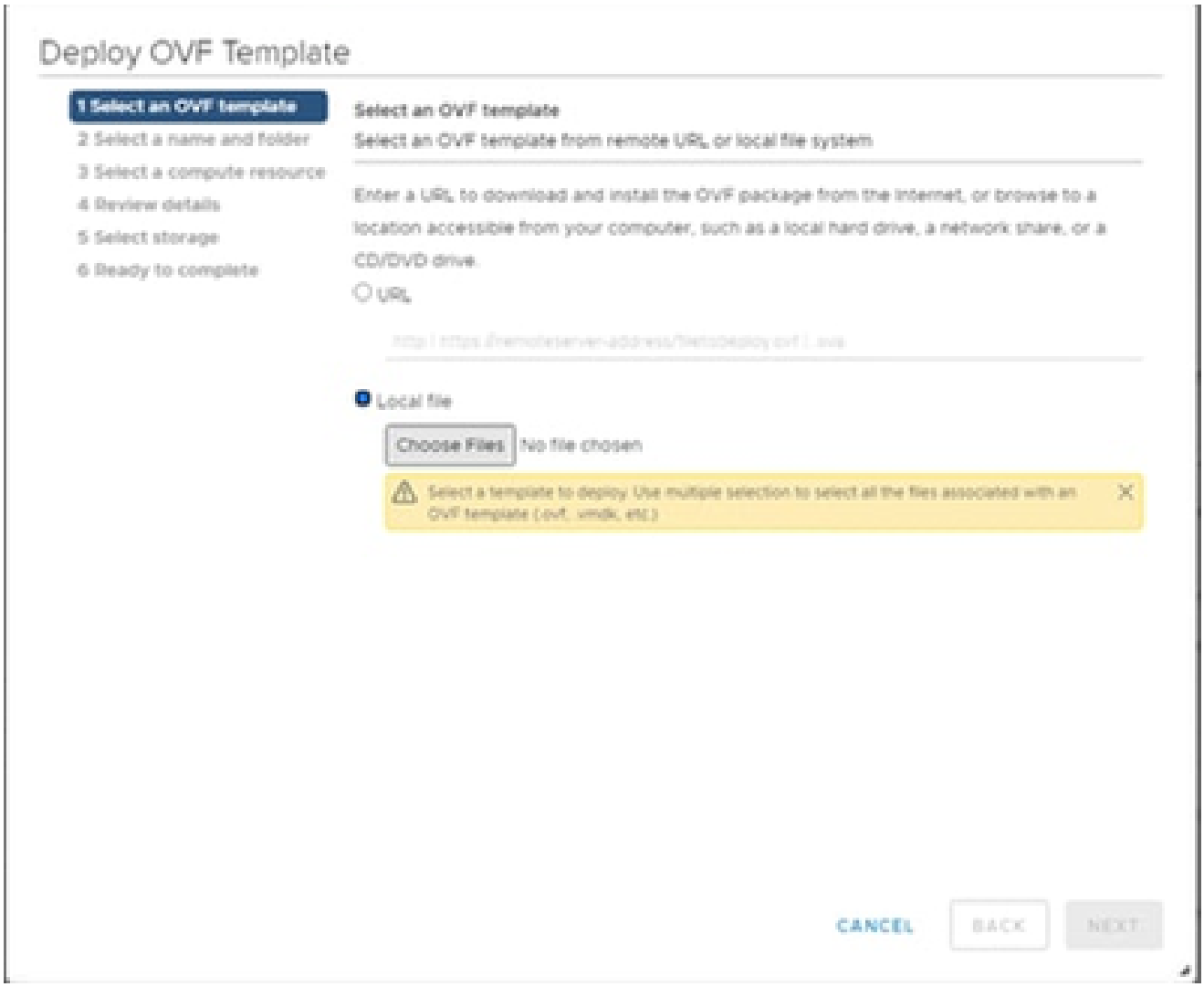


Home page

3. Selezionare la macchina virtuale e fare clic su Action > Deploy OVF Template (Azione > Implementa il modello OVF).

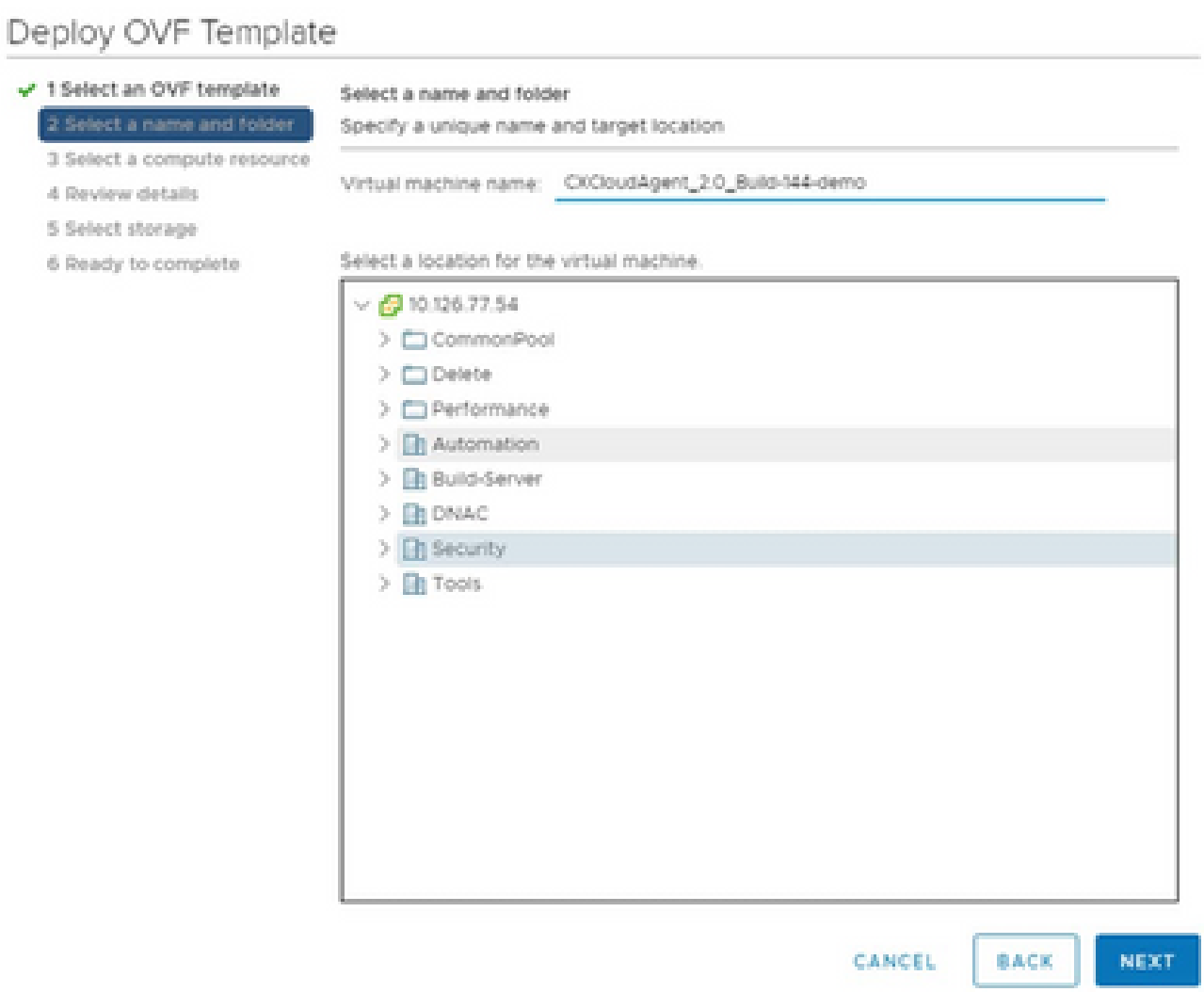


Azioni



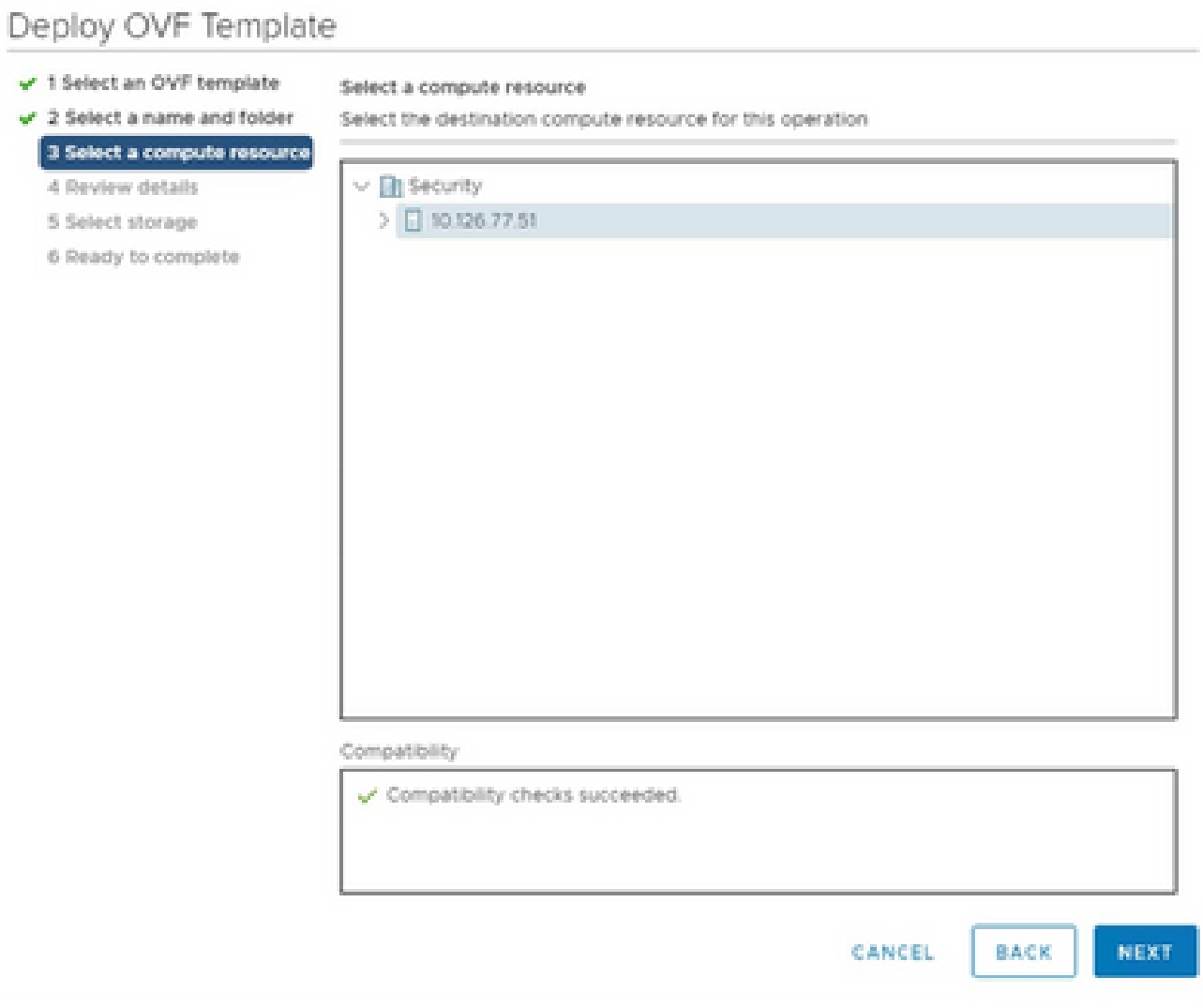
Selezione del modello

4. Aggiungere l'URL direttamente o selezionare il file OVA e fare clic su Avanti.
5. Se necessario, immettere un nome univoco e selezionare la posizione.
6. Fare clic su Next (Avanti).



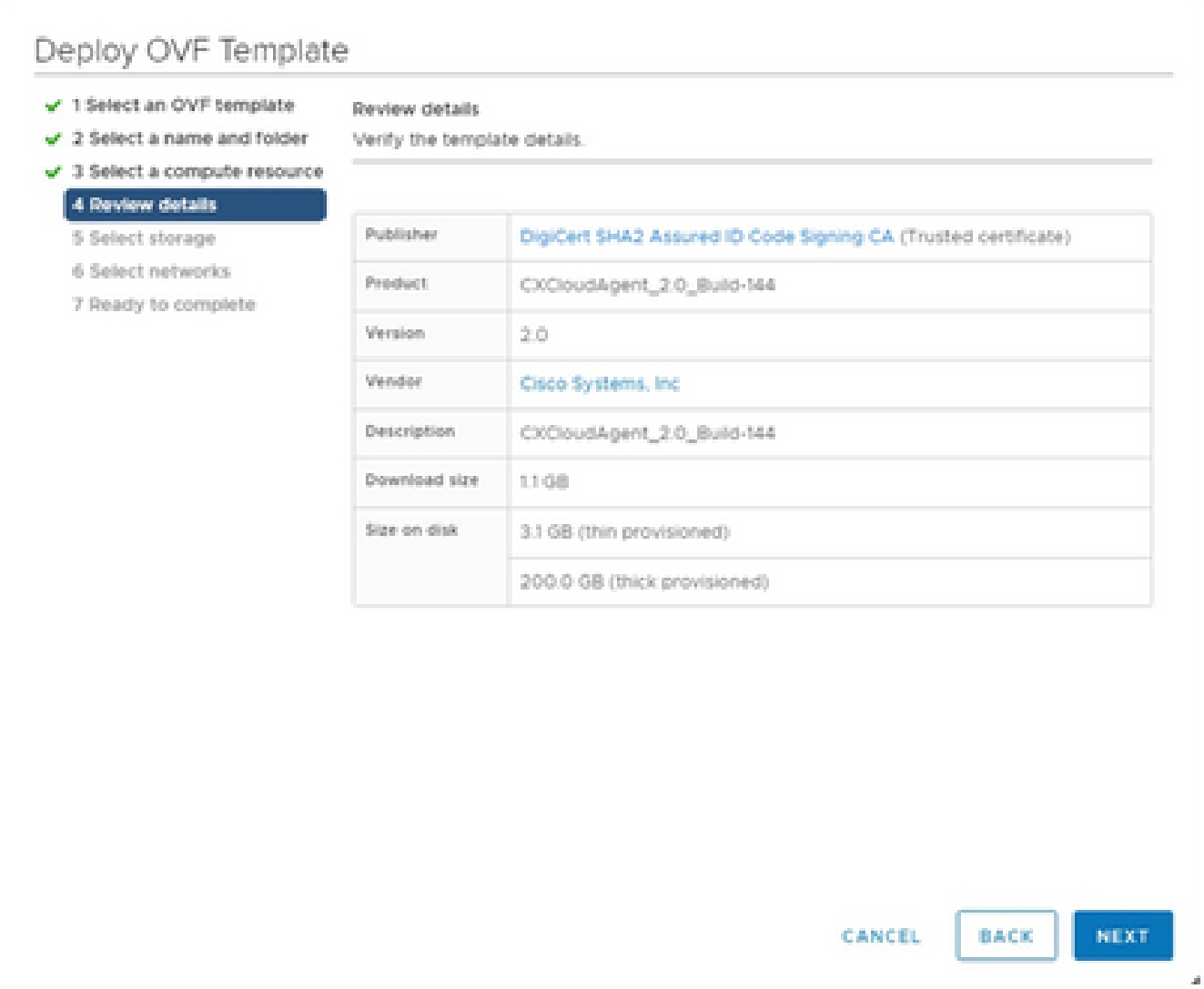
Nome e cartella

7. Selezionare una risorsa di calcolo e fare clic su Avanti.



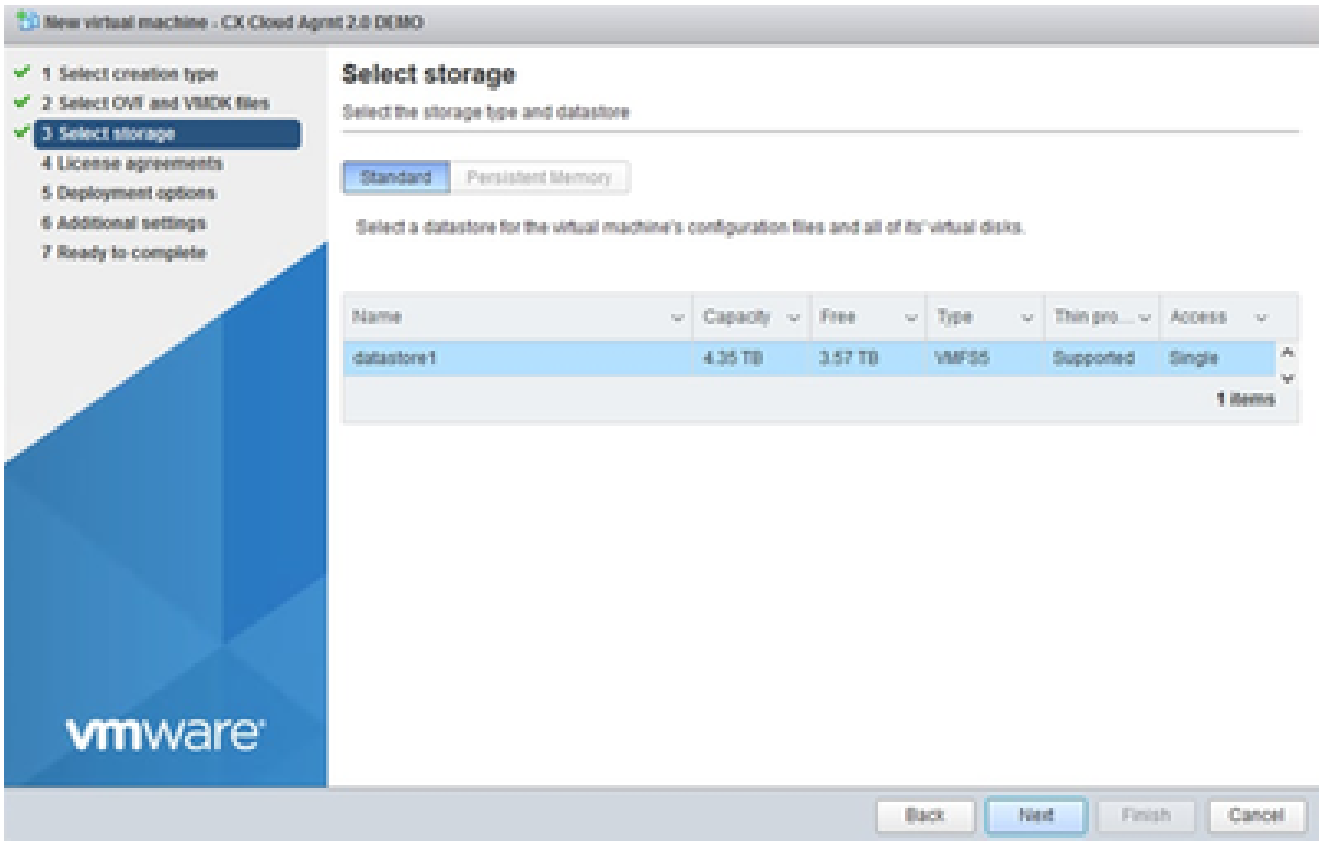
Seleziona risorsa computer

8. Riesaminare i dettagli e fare clic su Next (Avanti).



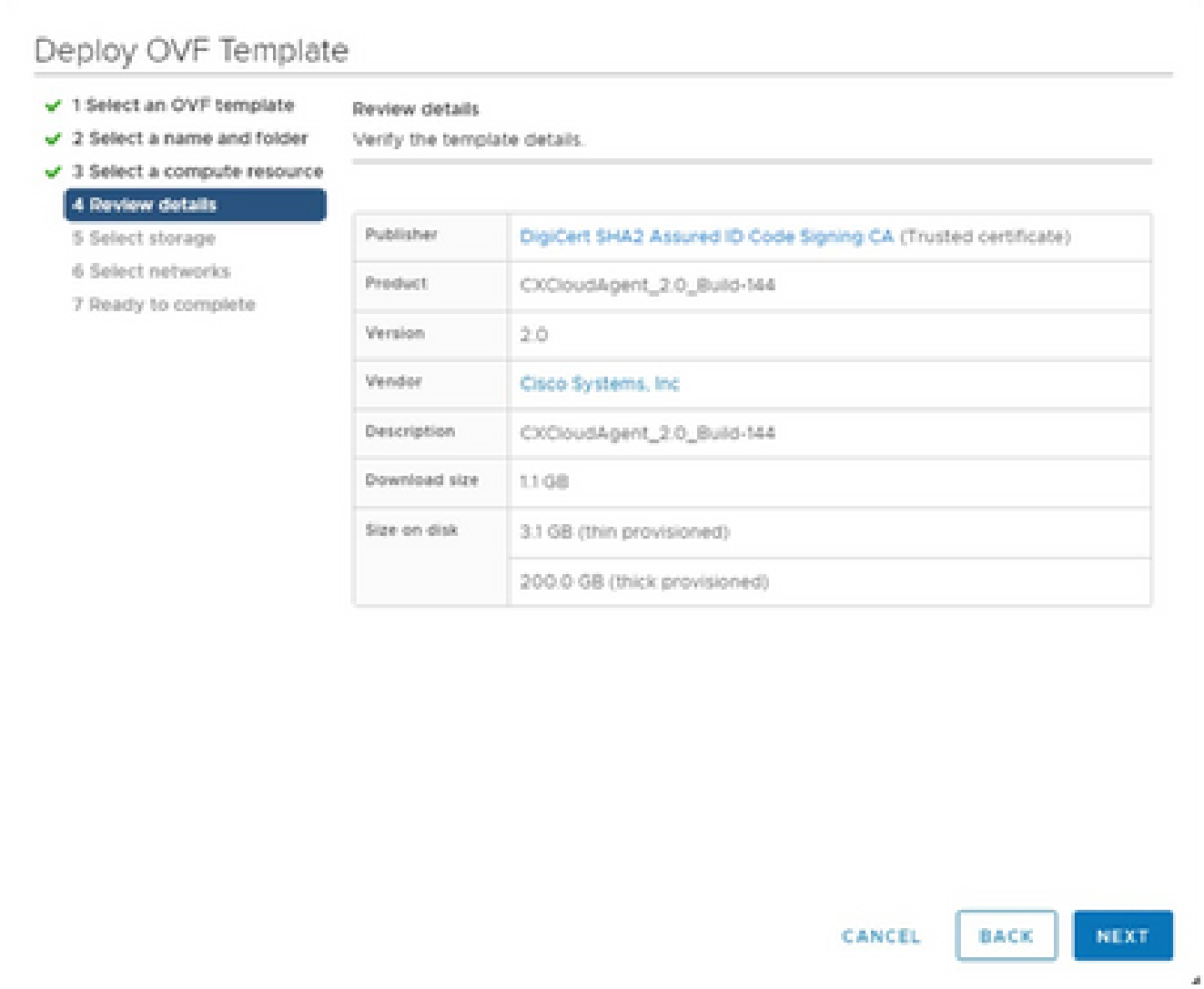
Riesame dei dettagli

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



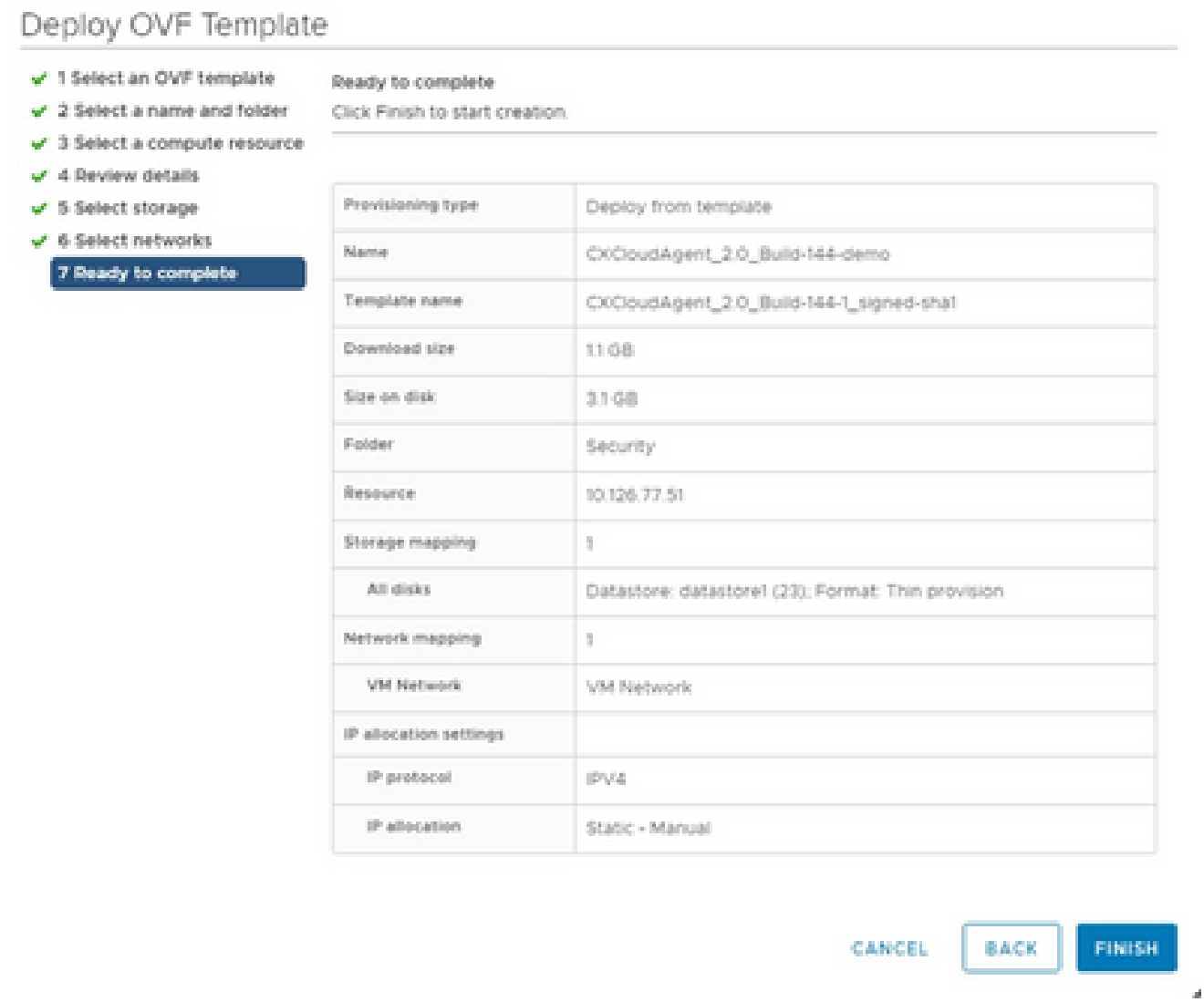
Selezione dell'archivio

10. Fare clic su Next (Avanti).



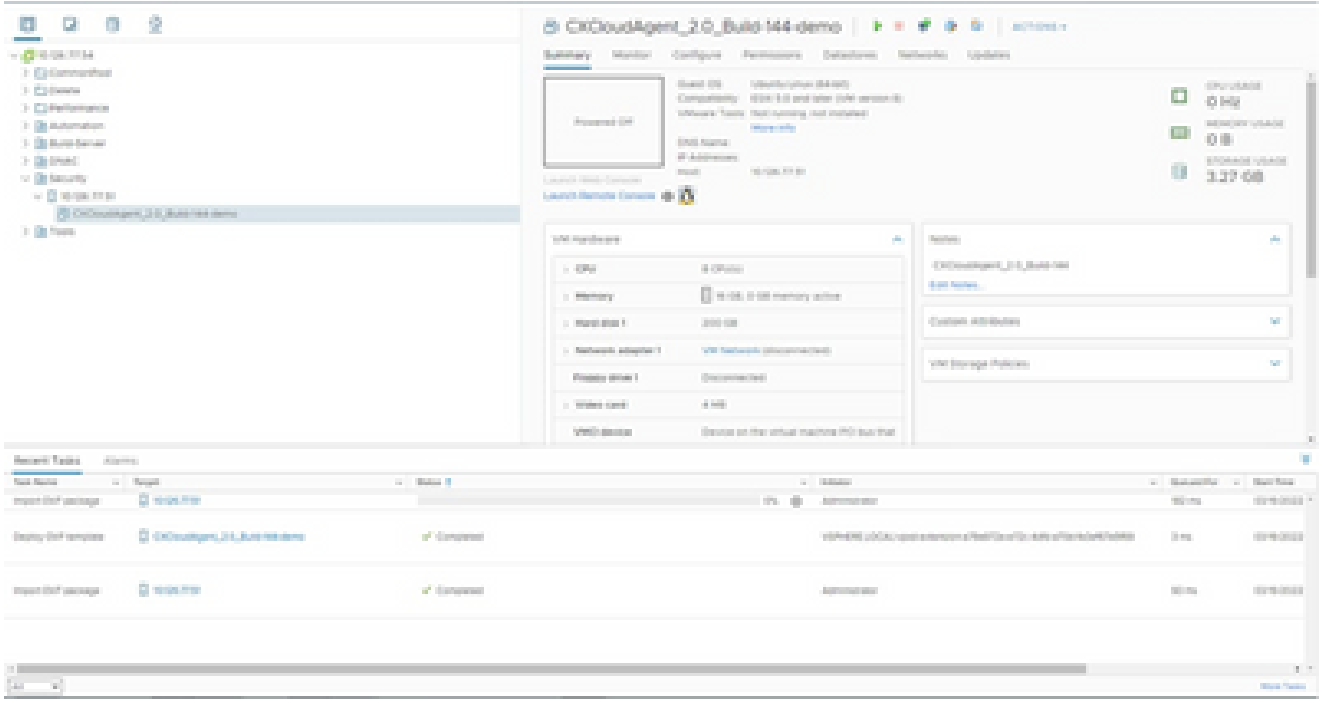
Seleziona rete

11. Fare clic su Finish (Fine).



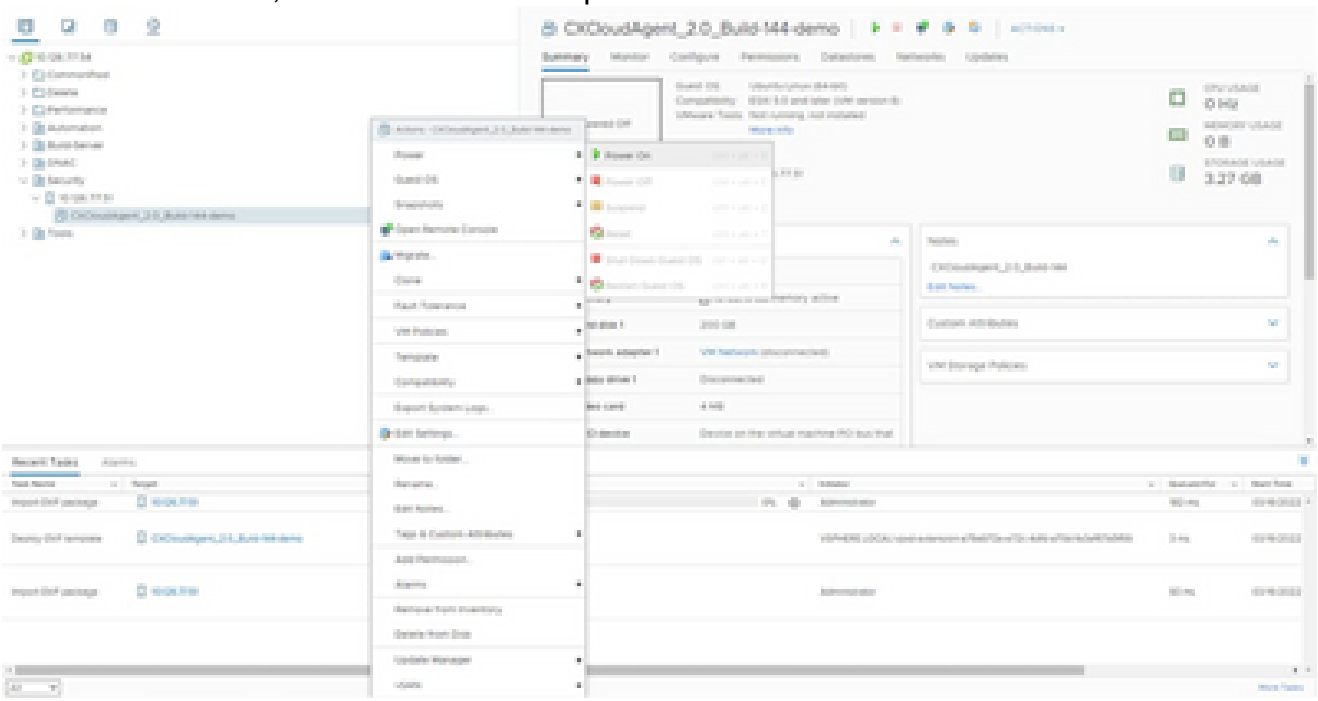
Pronto per il completamento

12. Fare clic sul nome della VM appena aggiunta per visualizzare lo stato.



VM aggiunta

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



Apertura della console

14. Passare a Configurazione di rete per continuare con i passaggi successivi.

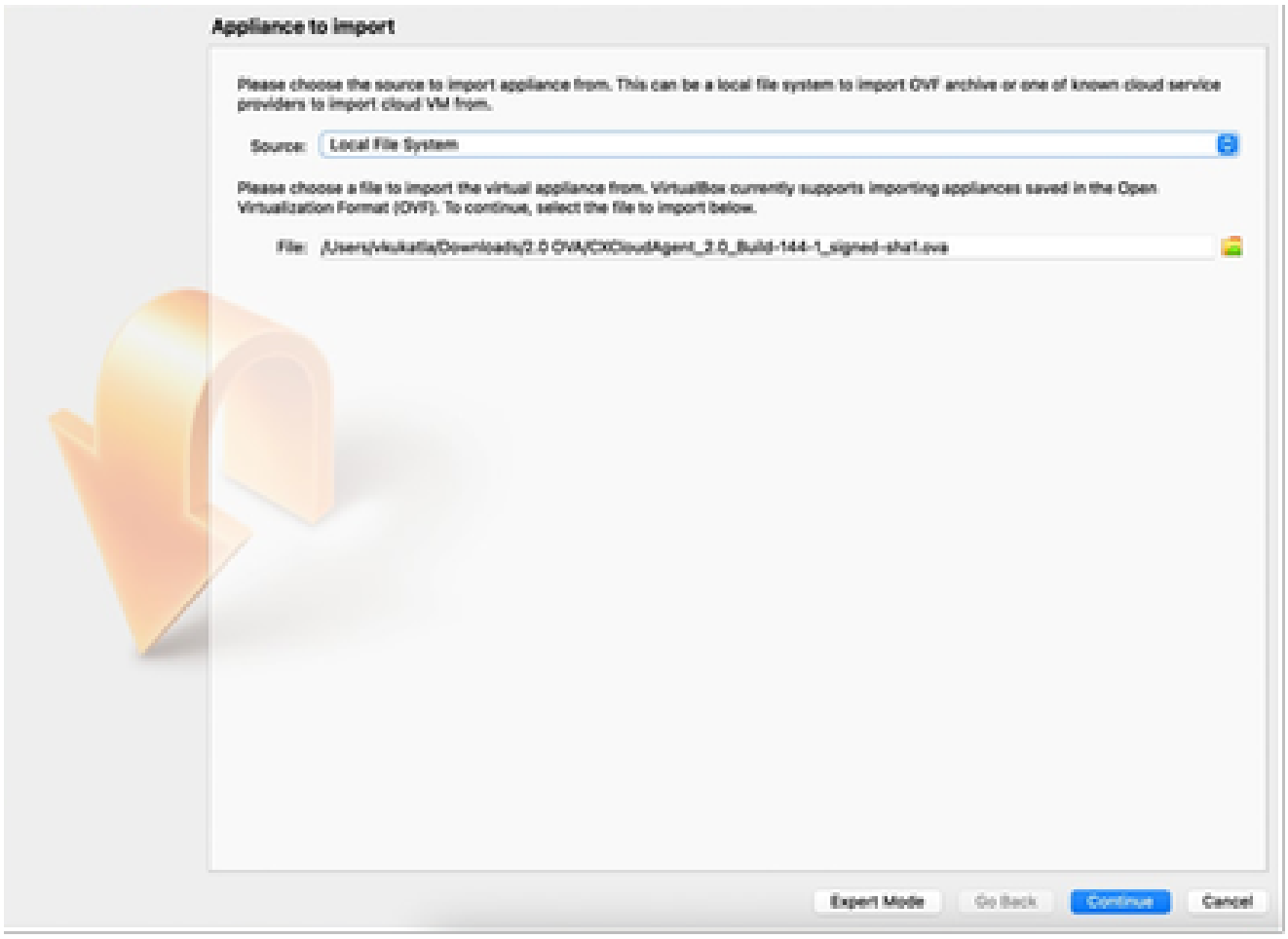
Installazione di Oracle Virtual Box 5.2.30

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

1. Aprire l'interfaccia utente di Oracle VM e selezionare File> Importa accessorio.

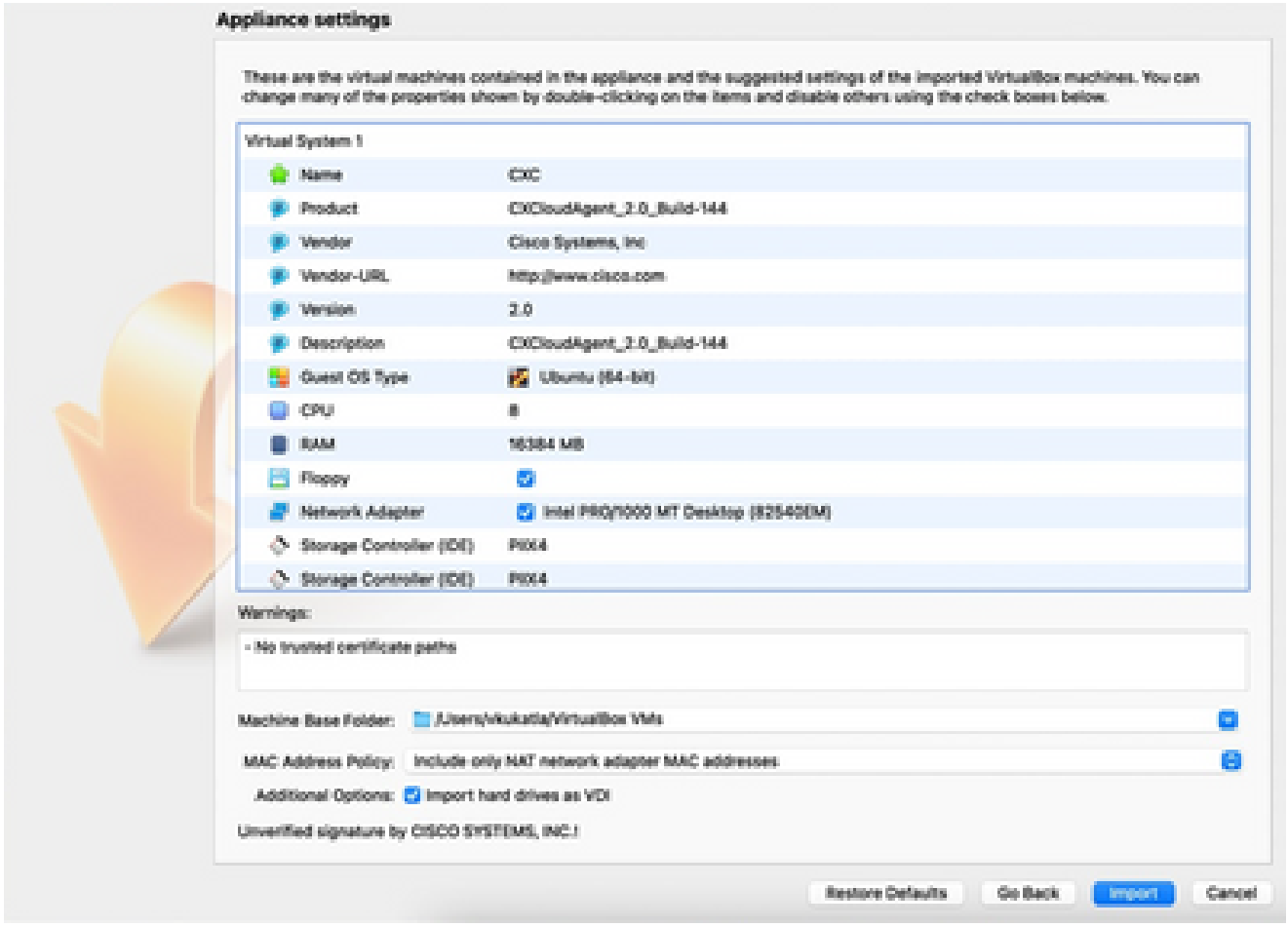
Oracle VM

2. Individuare il file OVA e importarlo.



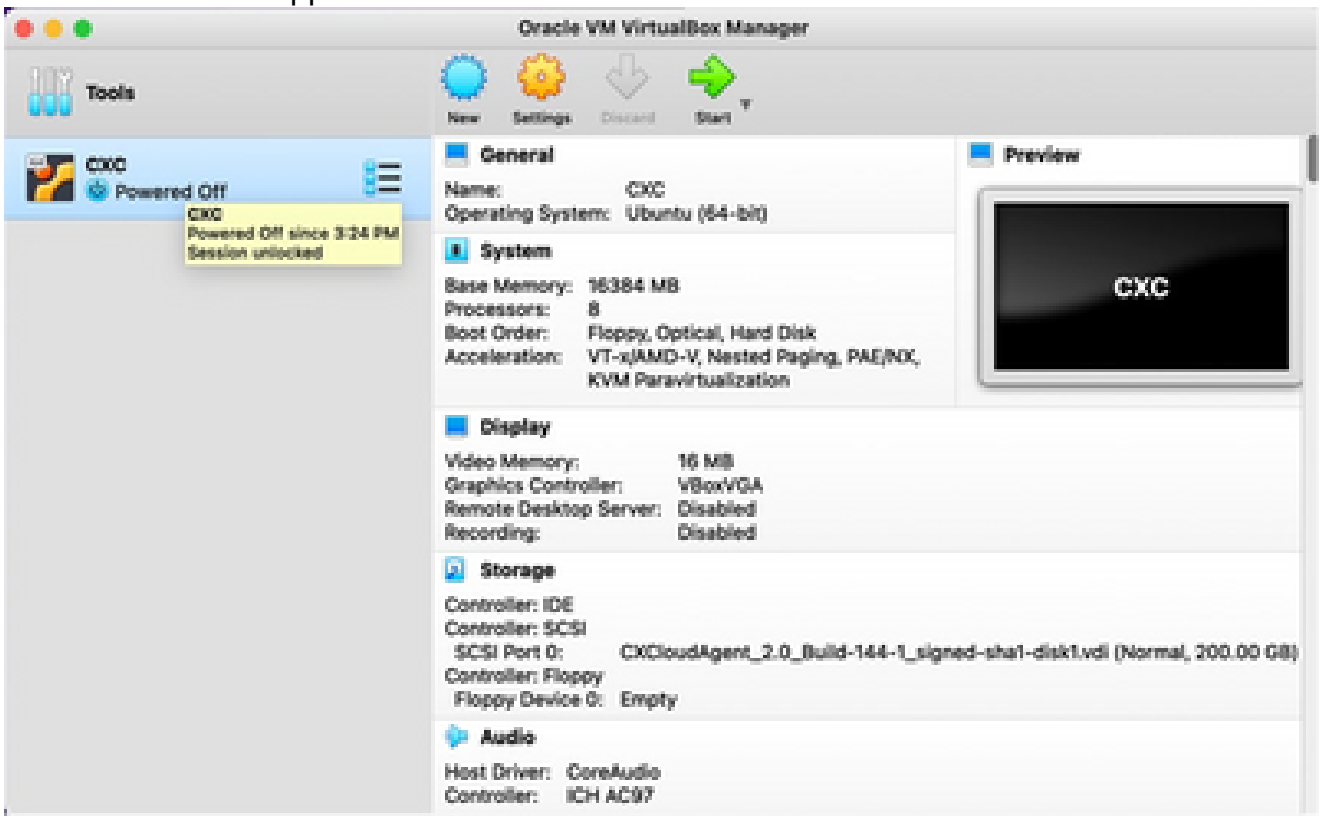
Selezione del file

3. Fare clic su Import (Importa).

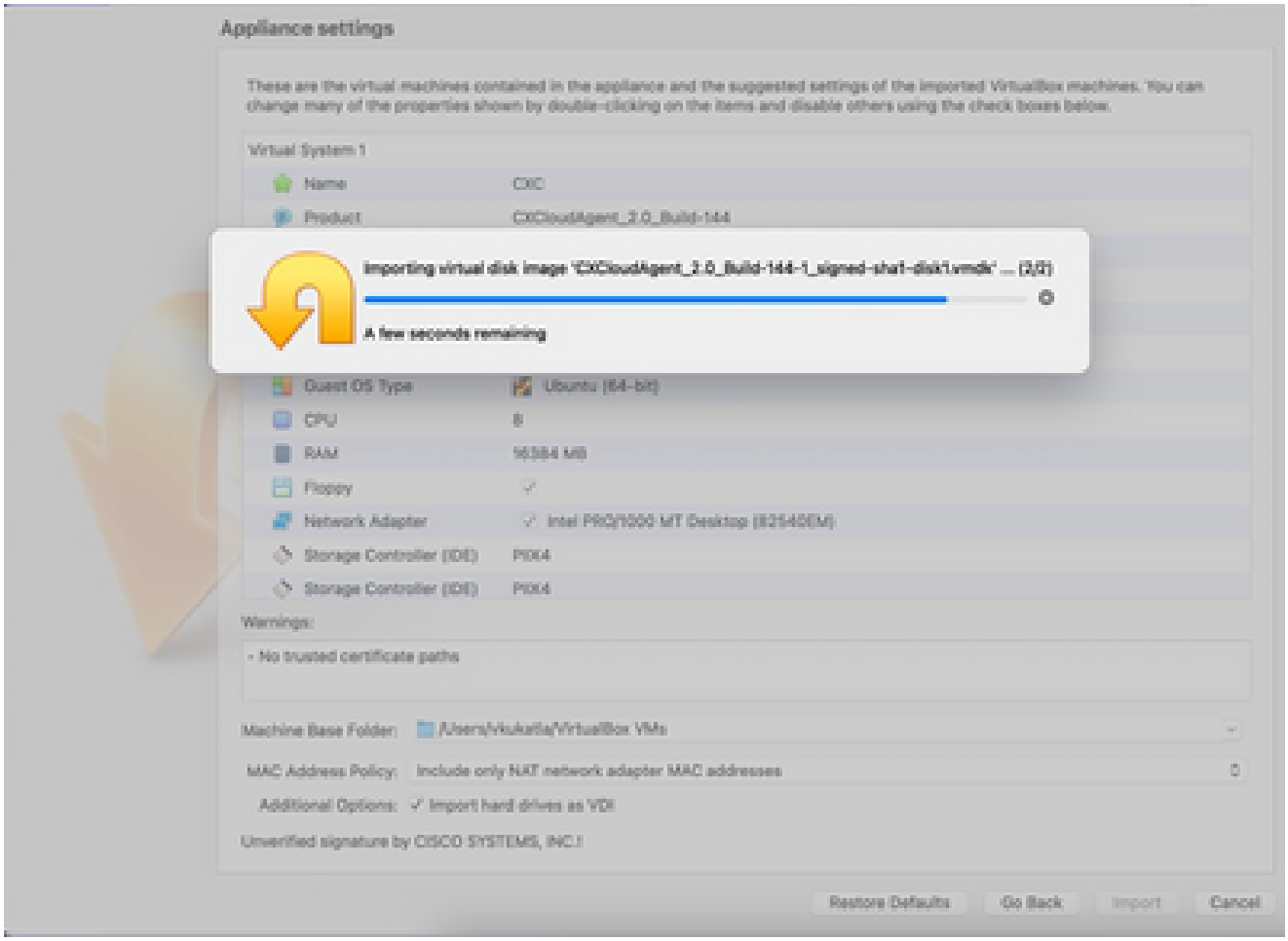


Importazione del file

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

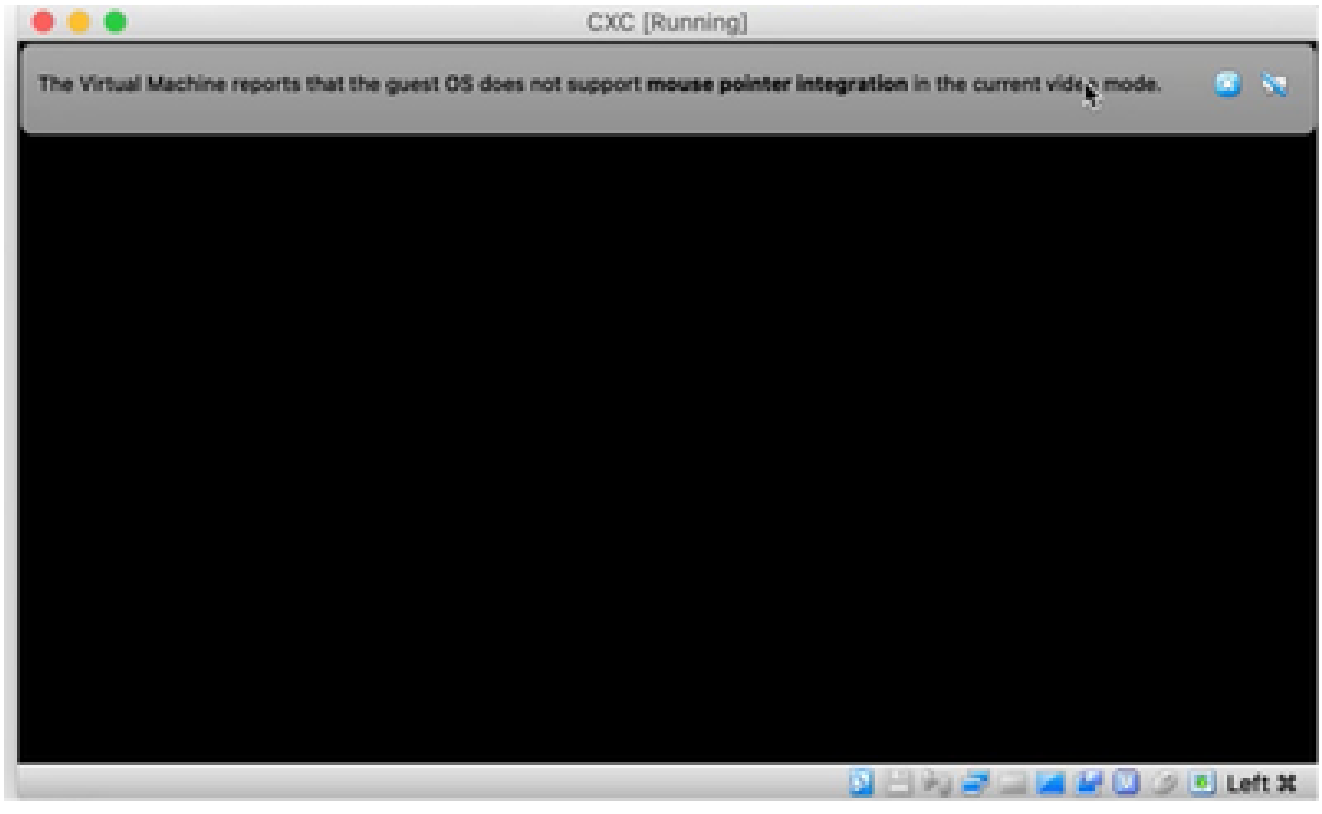


Avvio della console VM



Importazione in corso

5. Accendere la VM. Sulla console viene visualizzato.



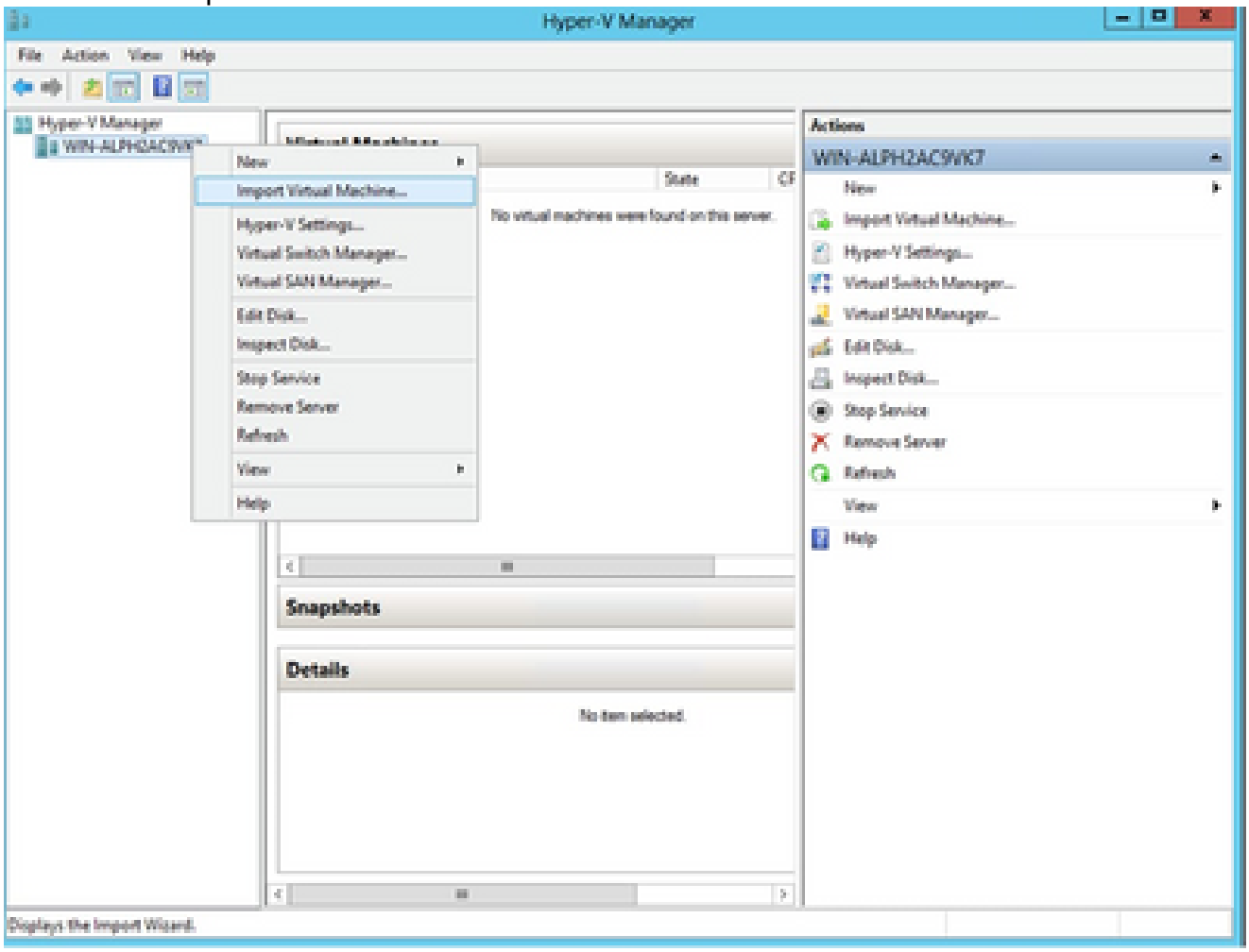
Apertura della console

6. Passare a Configurazione di rete per continuare con i passaggi successivi.

Installazione di Microsoft Hyper-V

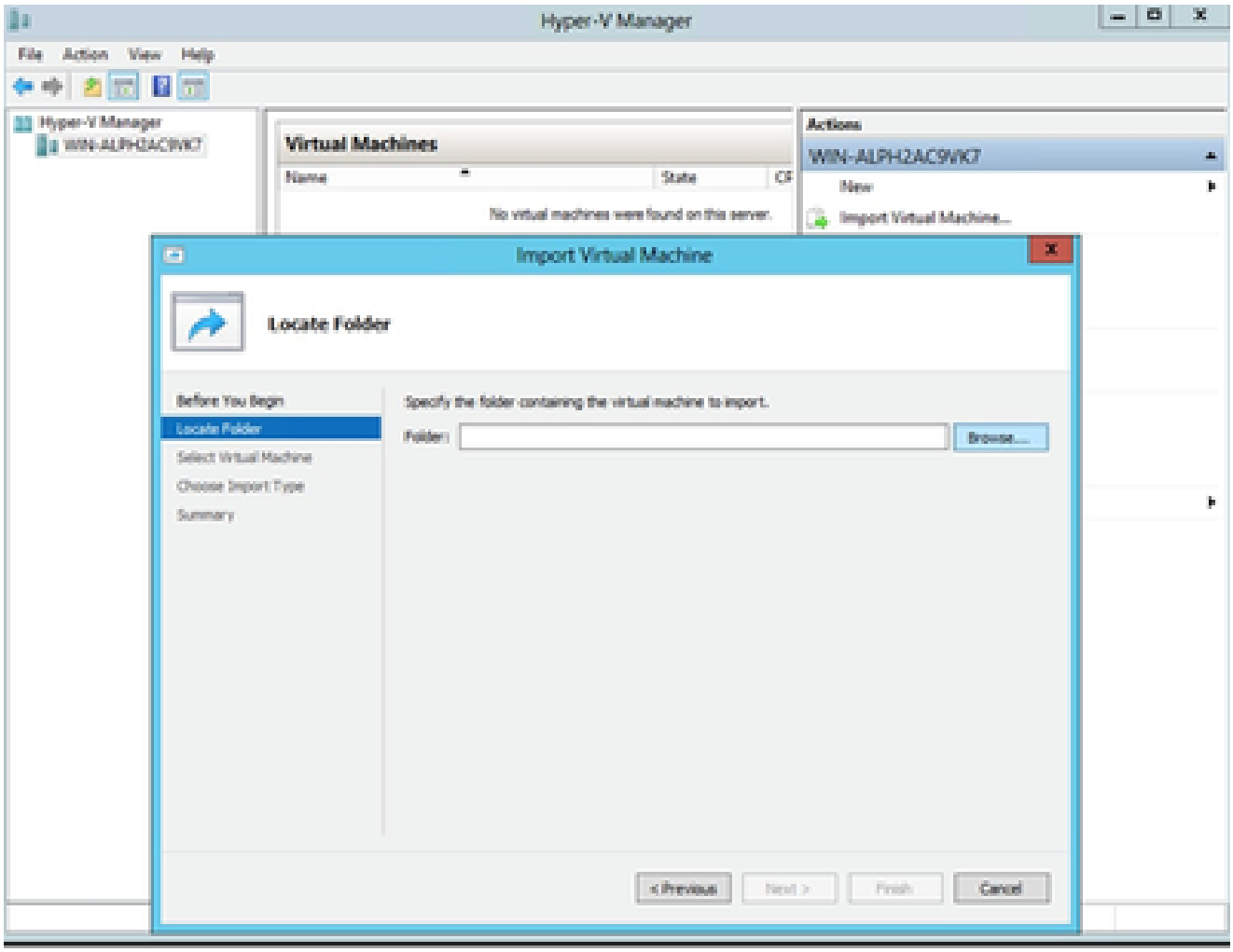
Eseguire questa procedura:

1. Selezionare Importa macchina virtuale.



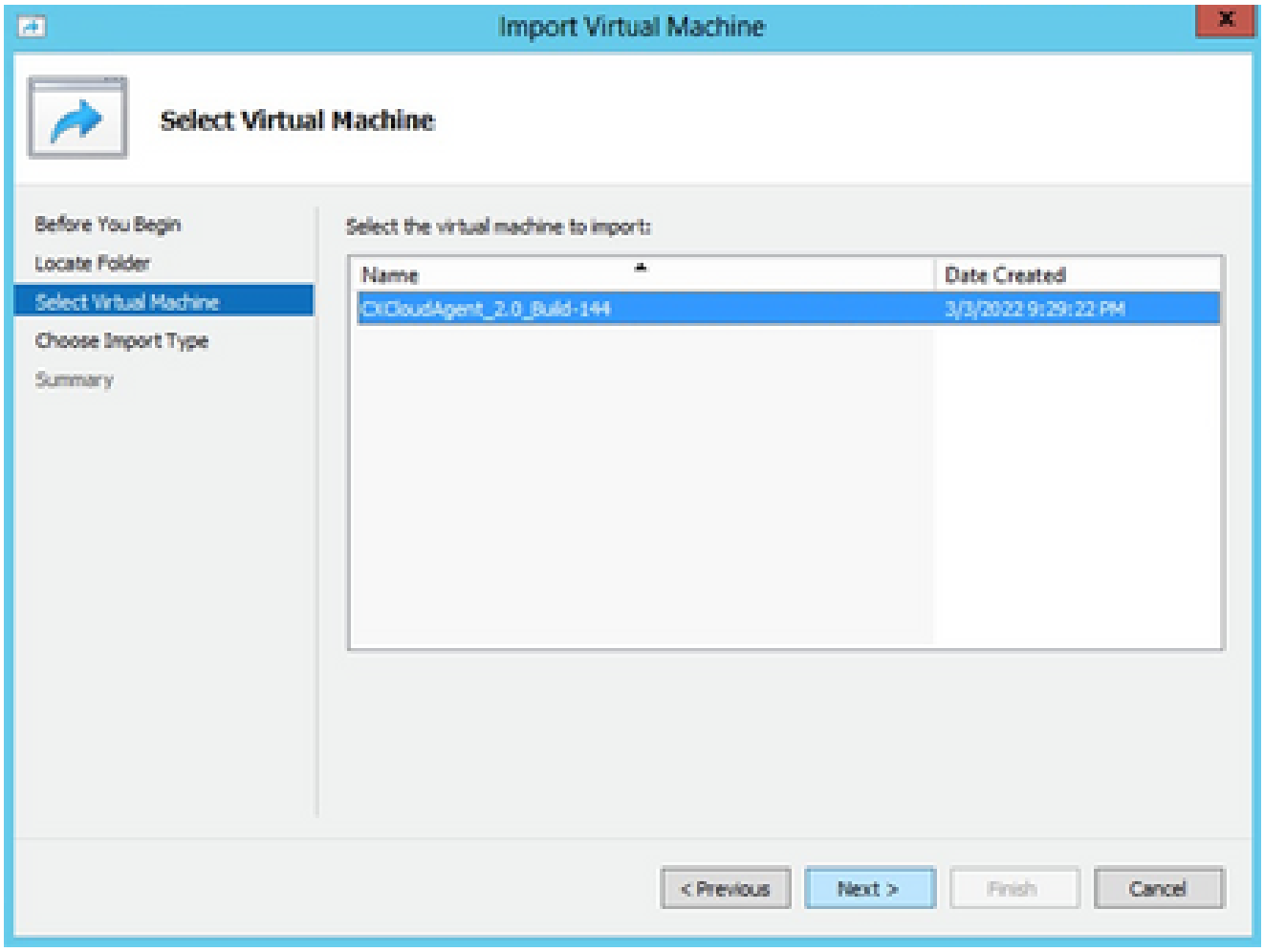
Gestione Hyper-V

2. Individuare la cartella di download e selezionarla.
3. Fare clic su Next (Avanti).



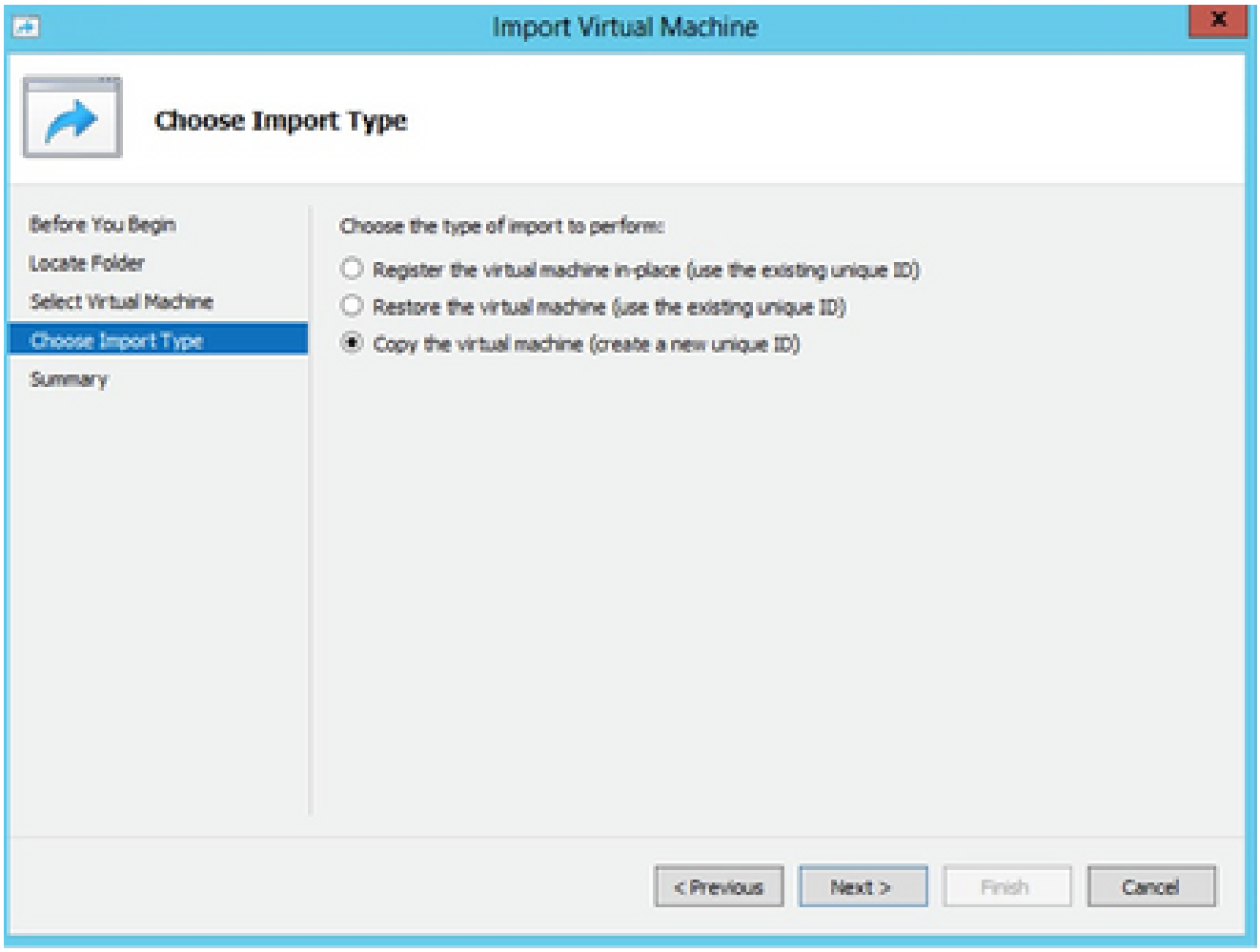
Cartella per l'importazione

4. Selezionare la VM e fare clic su Avanti.



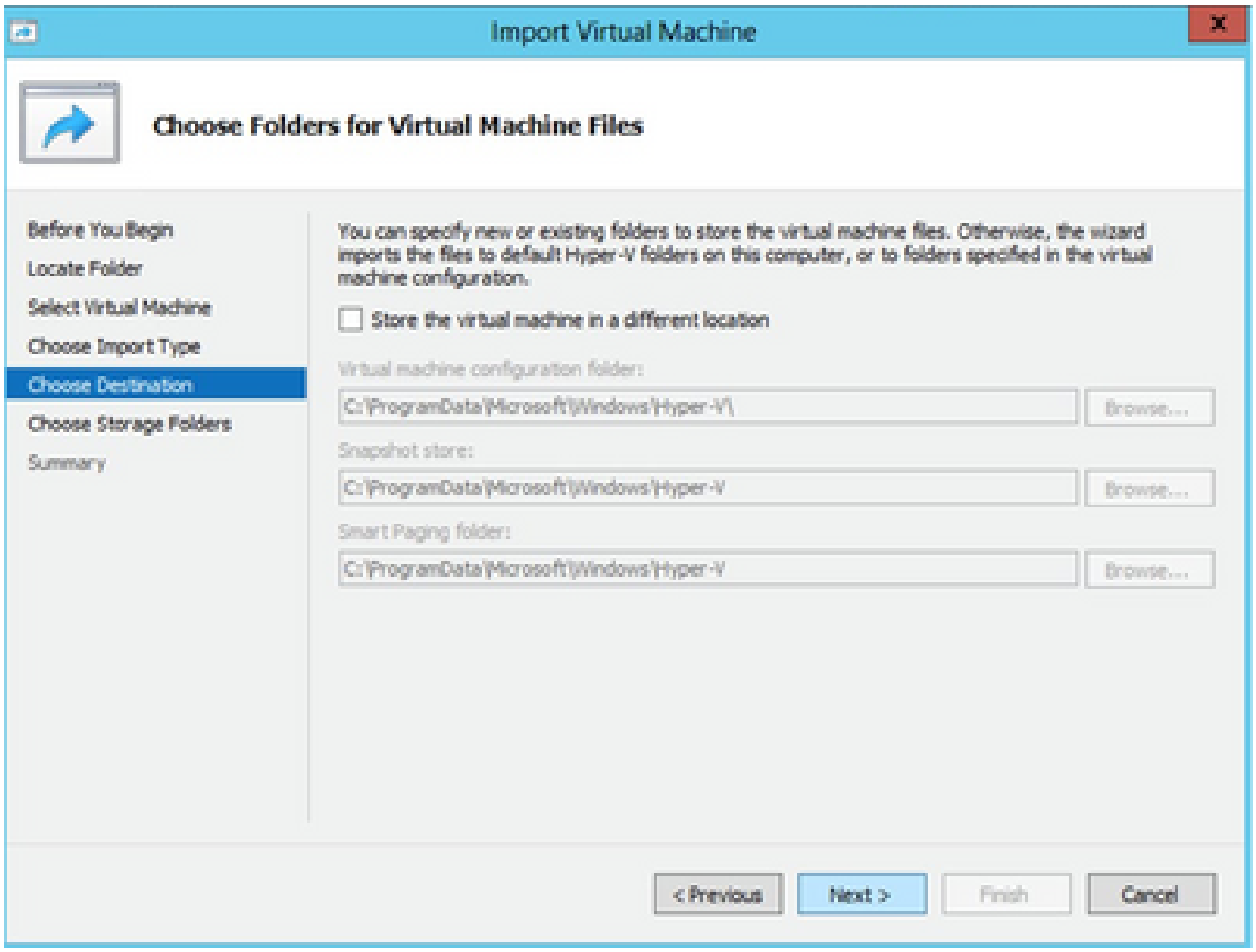
Selezione della VM

5. Selezionare il pulsante di opzione Copia la macchina virtuale (crea un nuovo ID univoco) e fare clic su Avanti.



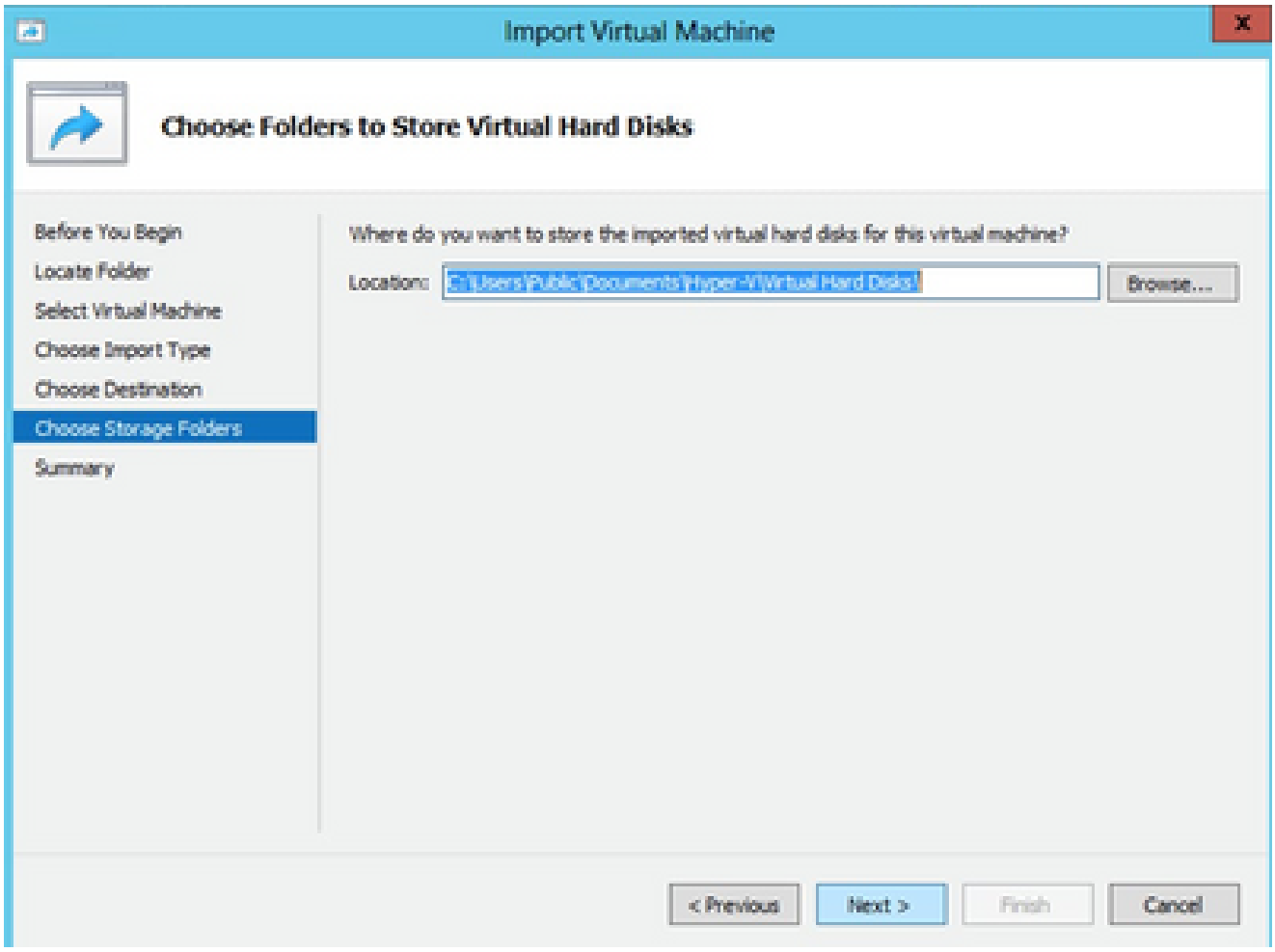
Tipo di importazione

6. Individuare la cartella dei file VM e selezionarla Si consiglia di utilizzare i percorsi predefiniti.
7. Fare clic su Next (Avanti).



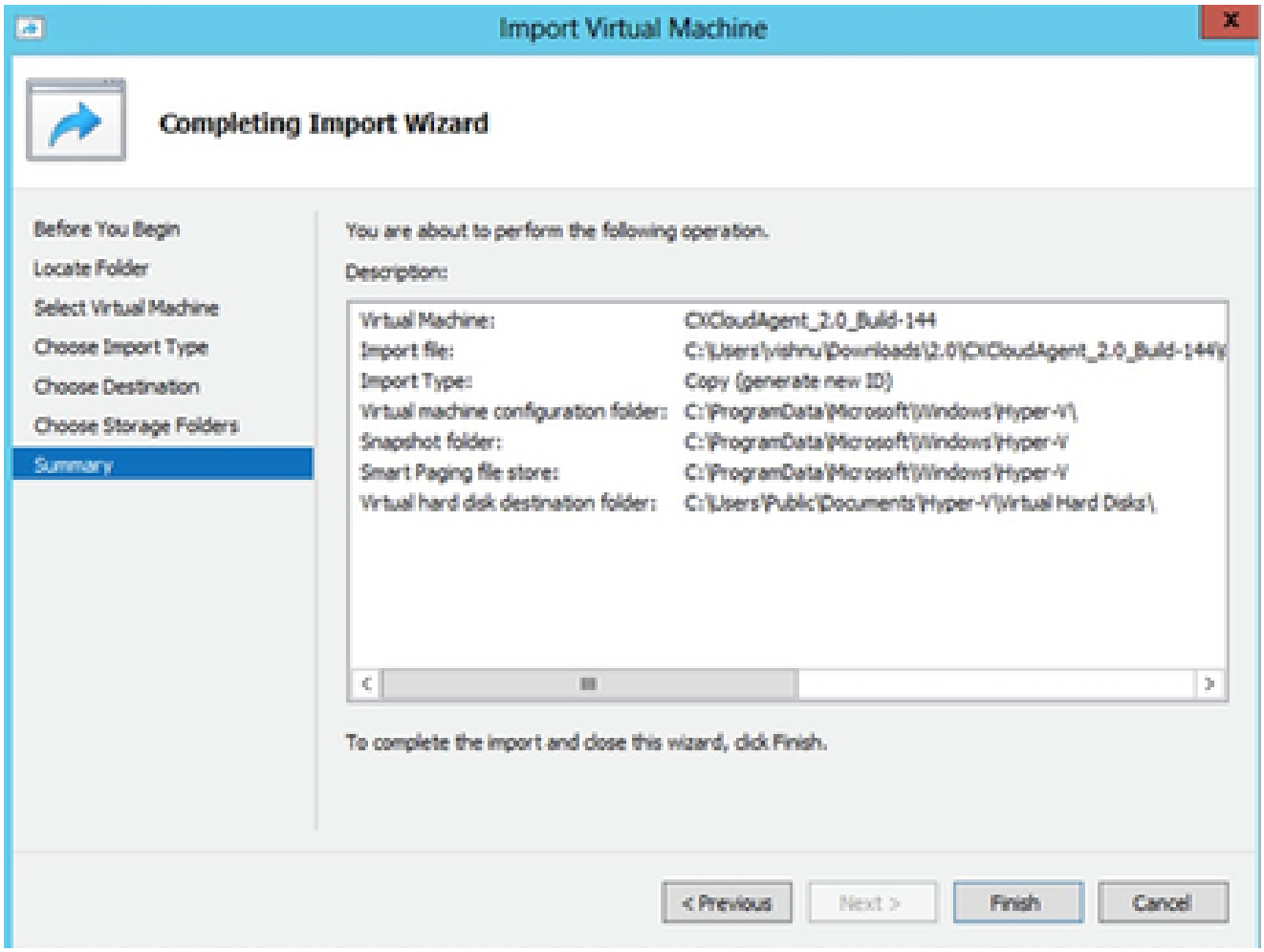
Scegliere le cartelle per i file delle macchine virtuali

8. Individuare la cartella in cui archiviare il disco rigido della VM Si consiglia di utilizzare i percorsi predefiniti.
9. Fare clic su Next (Avanti).



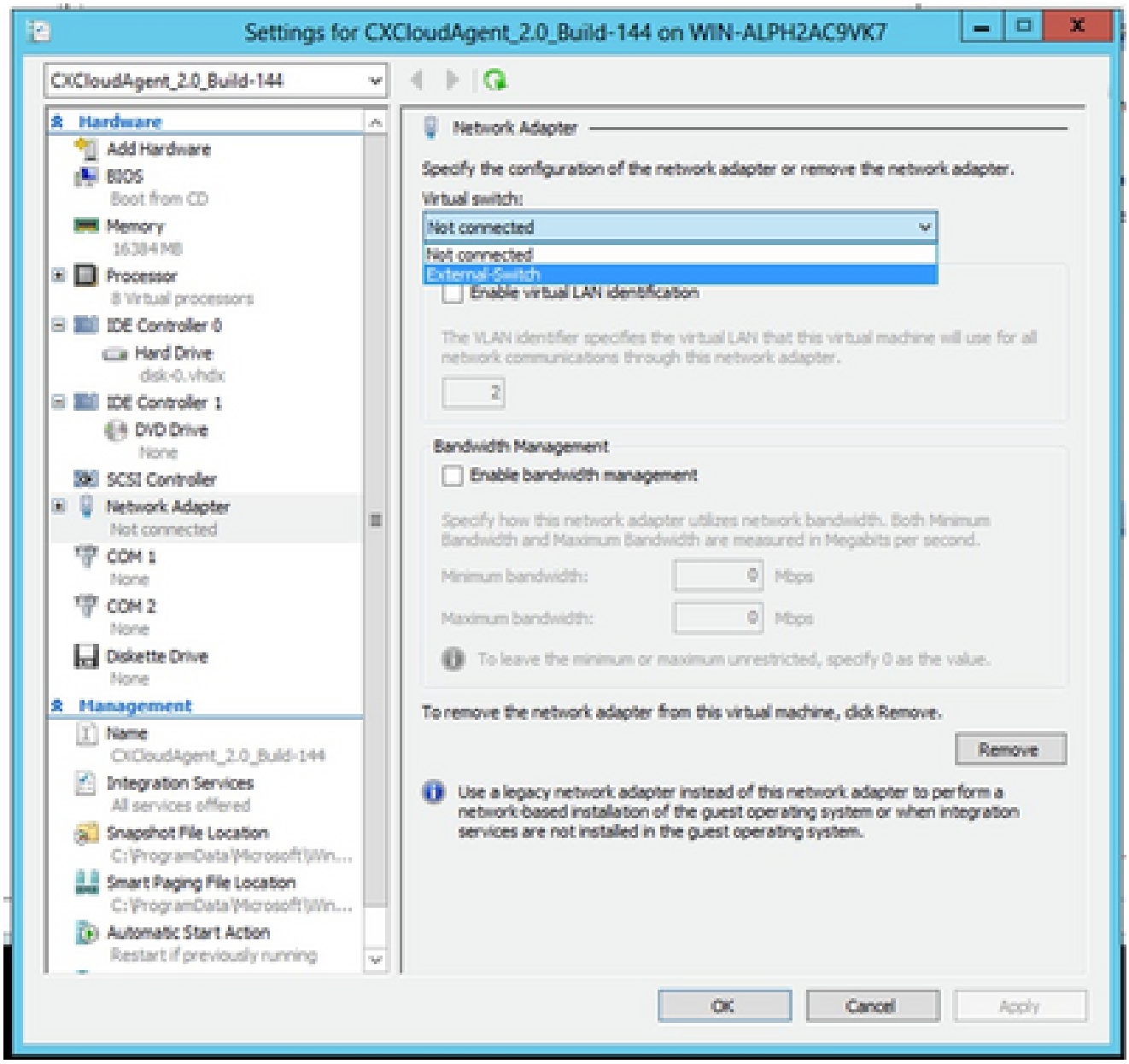
Cartella per l'archiviazione dei dischi rigidi virtuali

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



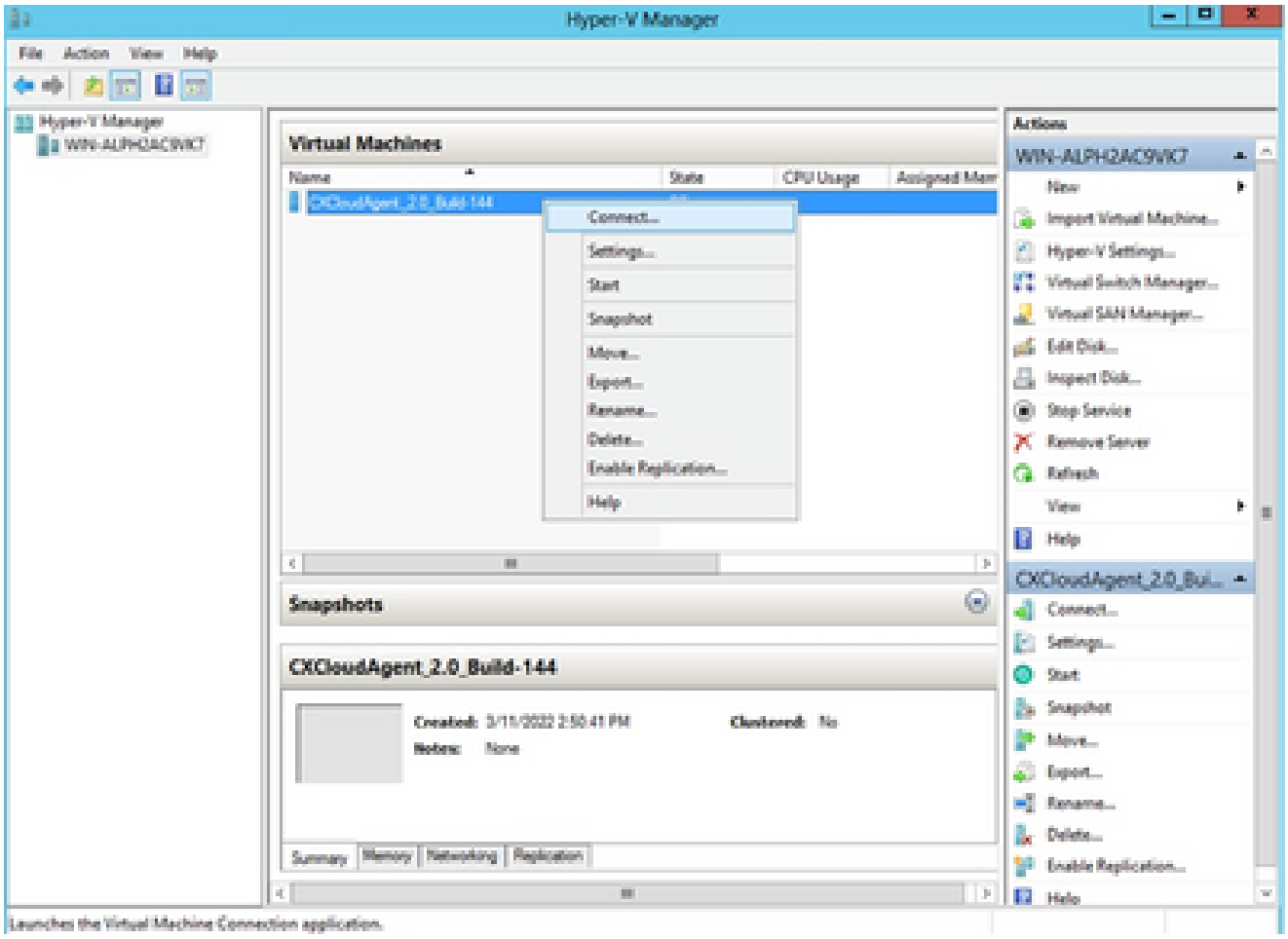
Riepilogo

11. Al termine dell'importazione, viene creata una nuova VM in Hyper-V. Aprire l'impostazione della VM.
12. Selezionare la scheda di rete sul riquadro a sinistra e selezionare Virtual Switch (Switch virtuale) dall'elenco a discesa.



Switch virtuale

13. Selezionare Connect (Connetti) per avviare la VM.

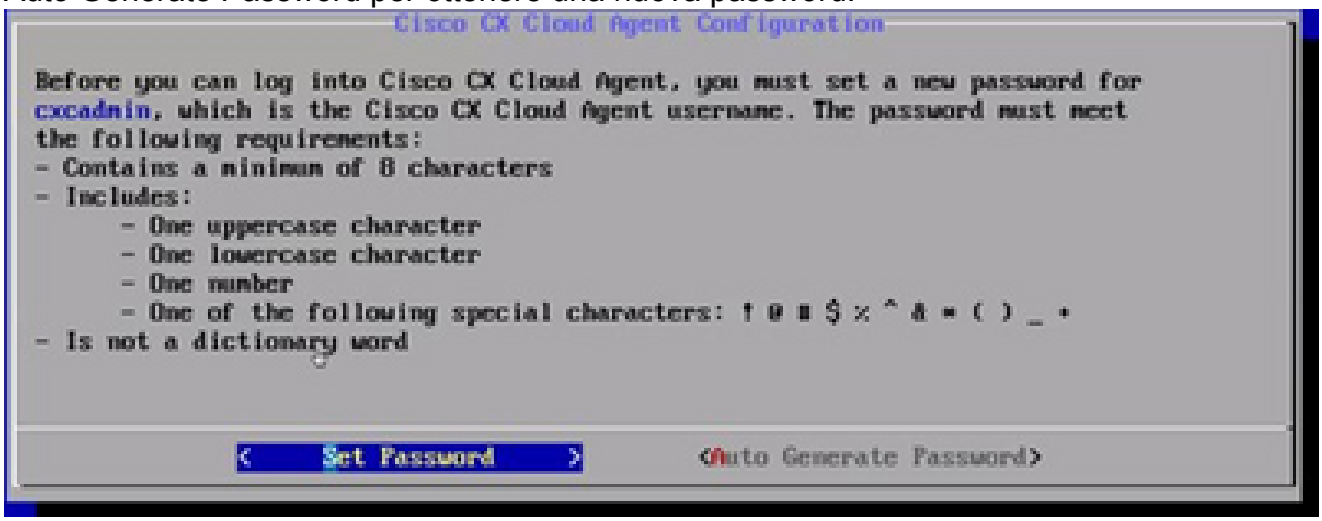


Avvio della VM

14. Passare a Configurazione di rete per continuare con i passaggi successivi.

Configurazione della rete

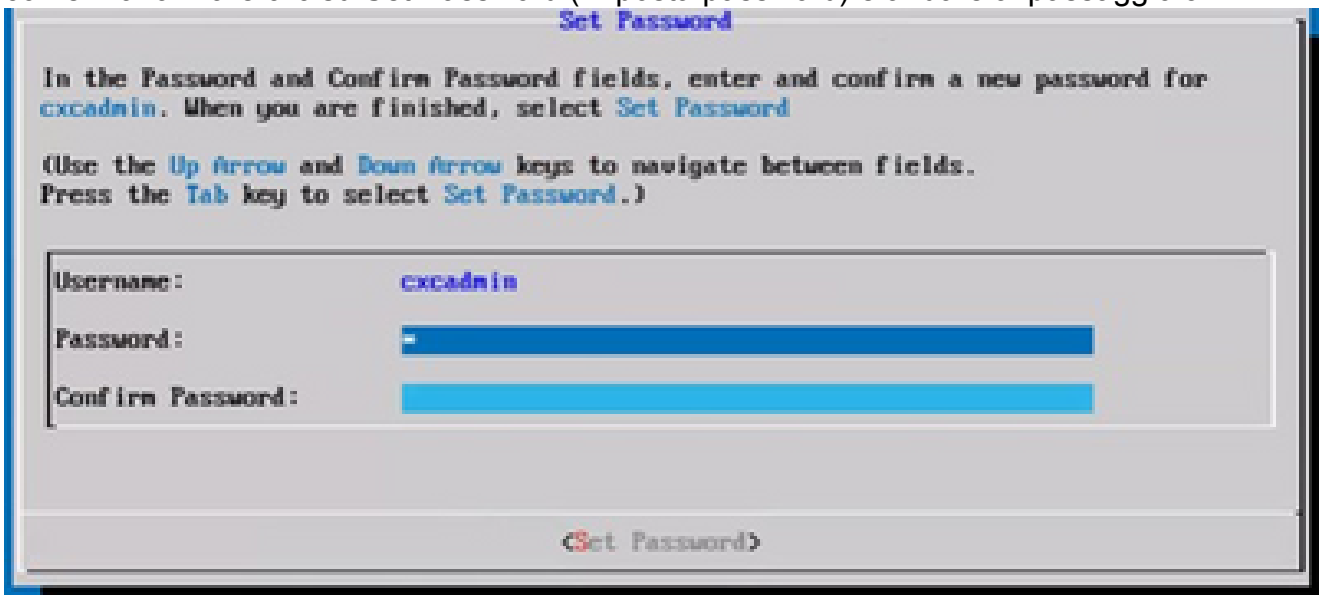
1. Fare clic su Set Password per aggiungere una nuova password per cxcadmin OPPURE su Auto Generate Password per ottenere una nuova password.



Imposta password

2. Se si seleziona Set Password (Imposta password), immettere la password per cxcadmin e

confermarla. Fare clic su Set Password (Imposta password) e andare al passaggio 3.



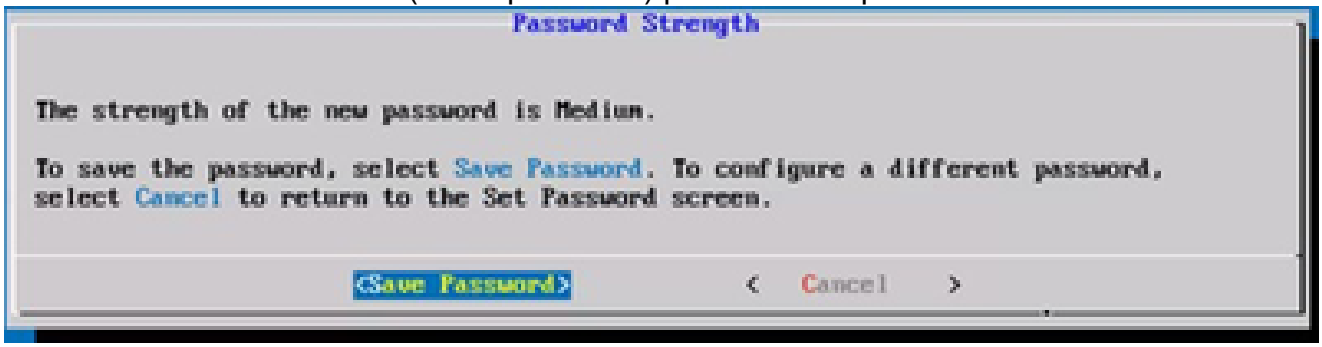
Nuova password

O

Se è selezionata l'opzione Generazione automatica password, copiare la password generata e memorizzarla per utilizzarla in futuro. Fare clic su Save Password (Salva password) e andare al passaggio 4.

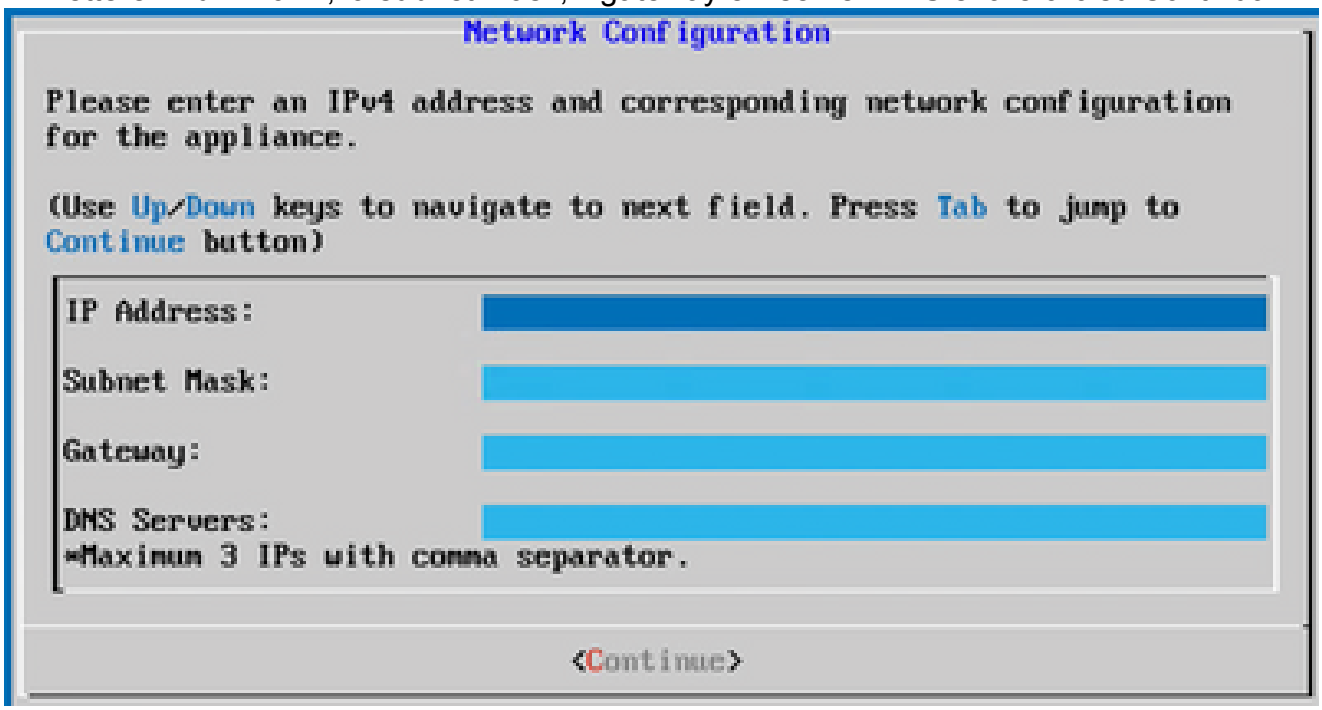
Password generata automaticamente

3. Fare clic su Save Password (Salva password) per utilizzarla per l'autenticazione.



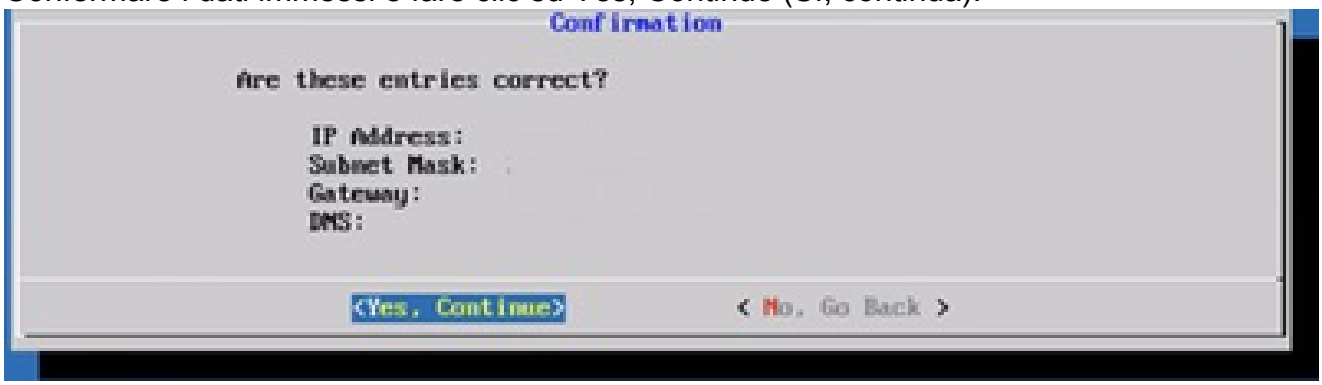
Salva password

4. Immettere l'indirizzo IP, la subnet mask, il gateway e il server DNS e fare clic su Continua.



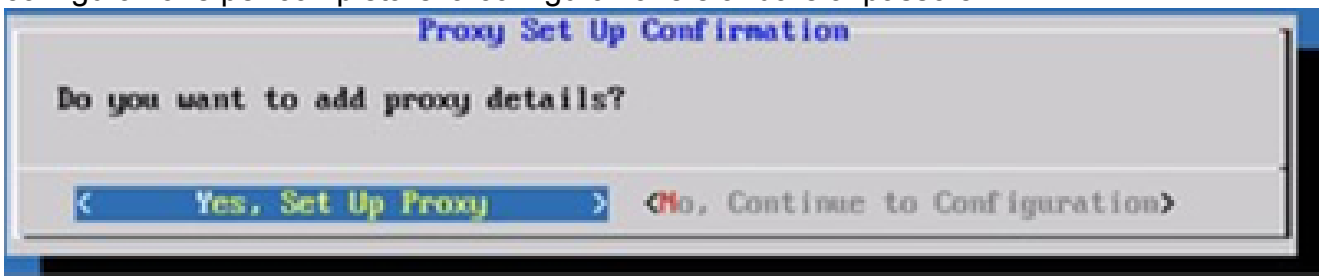
Configurazione della rete

5. Confermare i dati immessi e fare clic su Yes, Continue (Sì, continua).



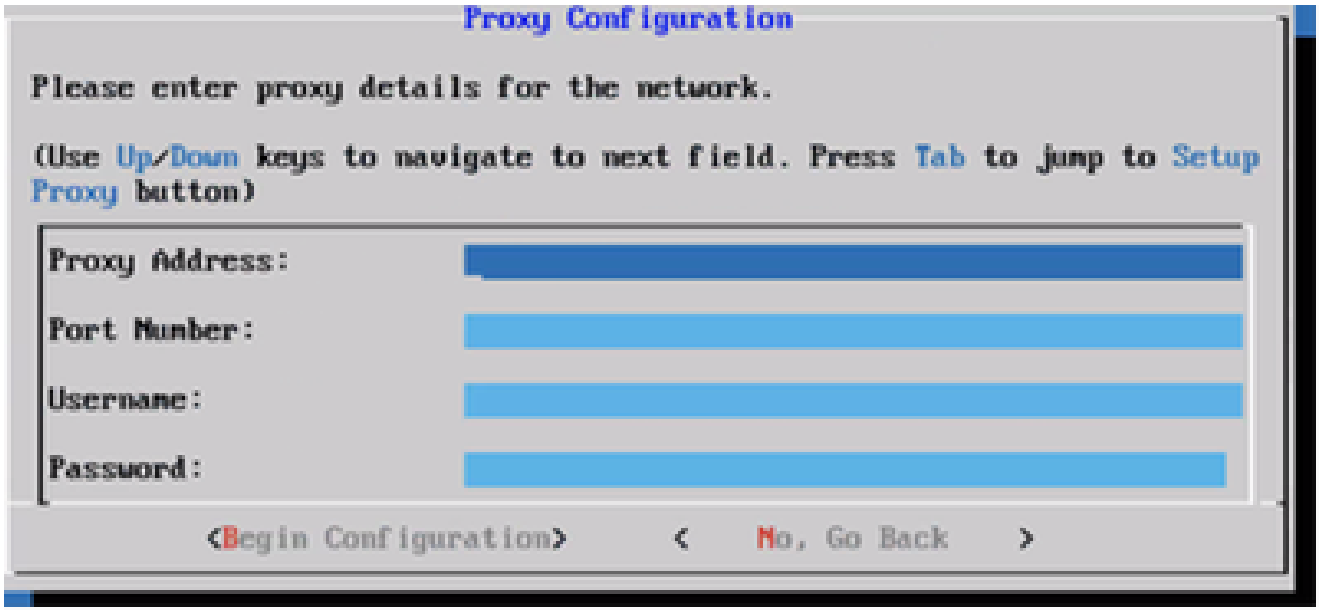
Configurazione

6. Per impostare i dettagli del proxy, fare clic su Sì, Configura proxy o su No, Continua con la configurazione per completare la configurazione e andare al passo 8.



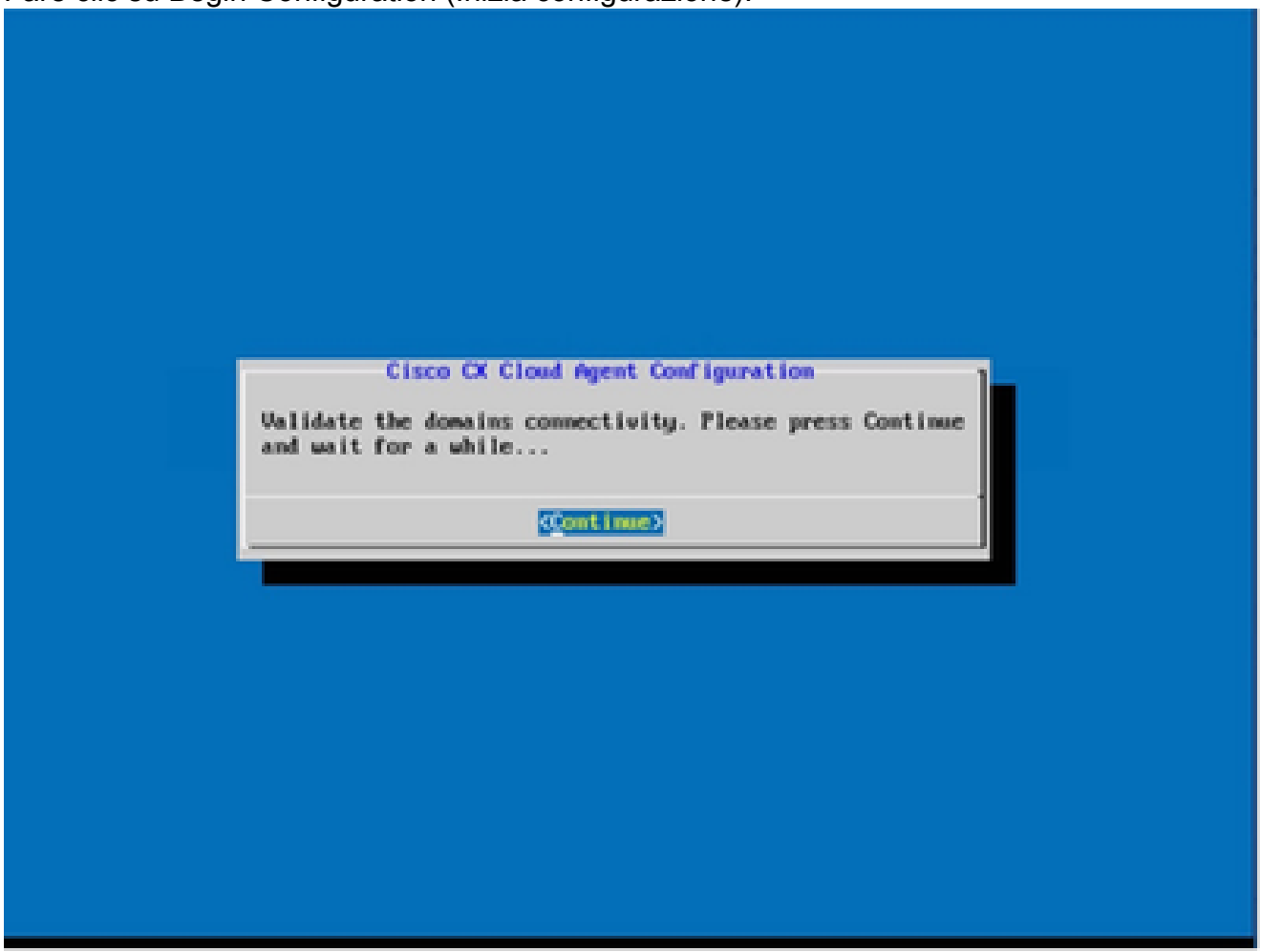
Impostazione del proxy

7. Immettere l'indirizzo proxy, il numero di porta, il nome utente e la password.



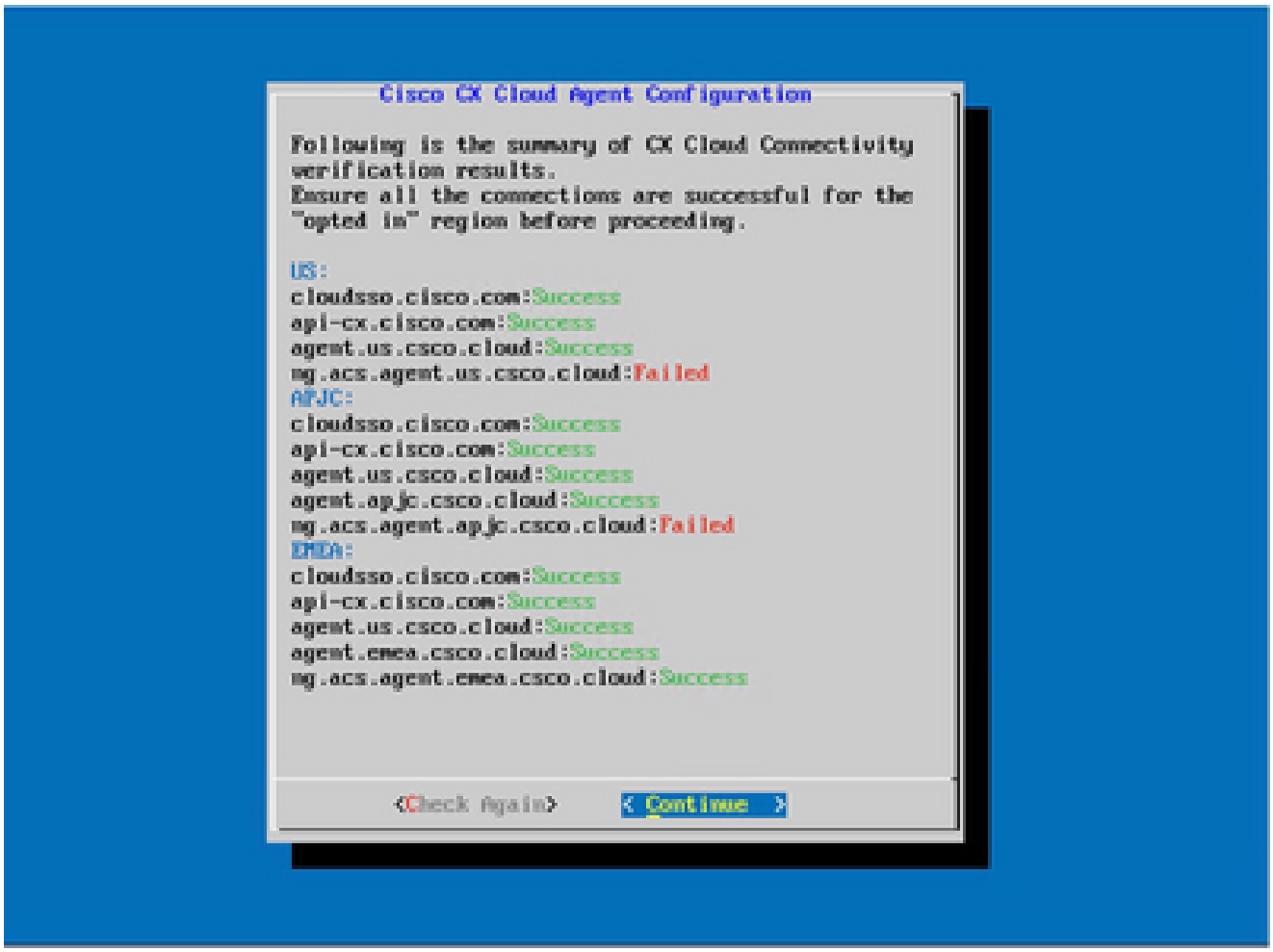
Configurazione del proxy

8. Fare clic su Begin Configuration (Inizia configurazione).



Inizio configurazione

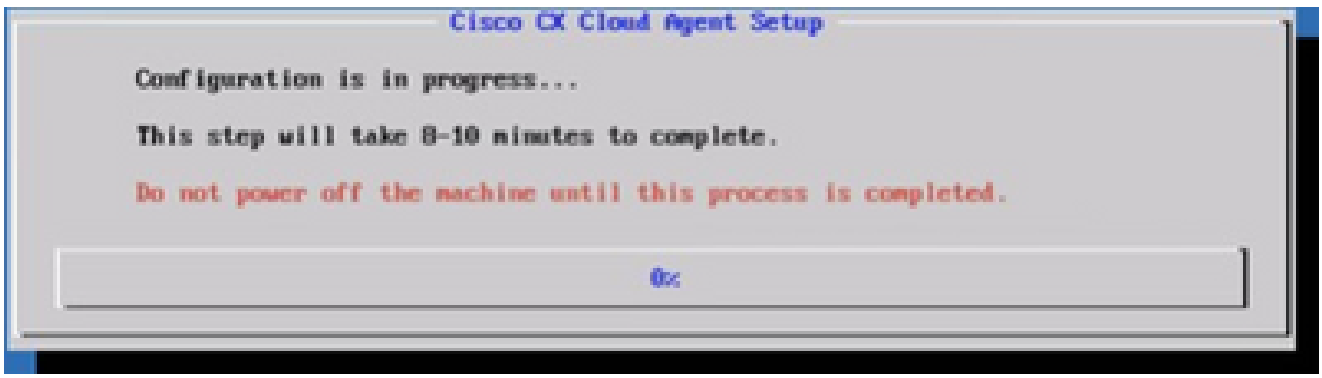
9. Fare clic su Continue (Continua).



Configurazione continua

10. Fare clic su Continue (Continua) per procedere con la configurazione in modo che il dominio raggiunga correttamente il dominio. Il completamento della configurazione può richiedere alcuni minuti.

Nota: se i domini non possono essere raggiunti correttamente, il cliente deve correggere la raggiungibilità del dominio apportando modifiche nel firewall per assicurare che i domini siano raggiungibili. Fare clic su Controlla di nuovo dopo aver risolto il problema di raggiungibilità dei domini.

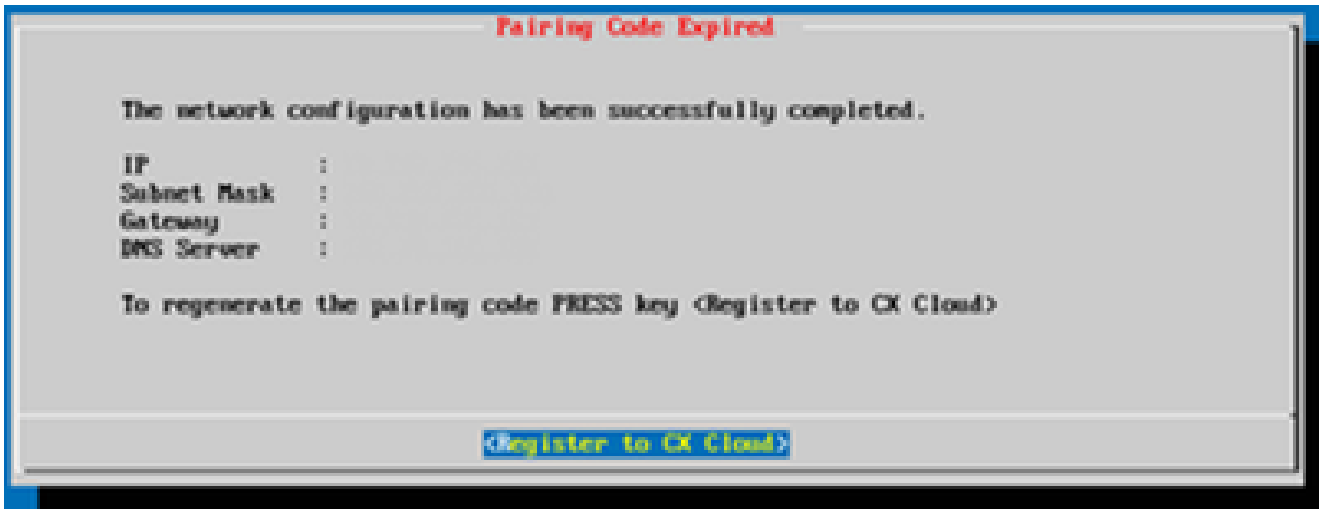


Configurazione in corso

11. Copiare il codice di associazione e tornare a CX Cloud per proseguire.

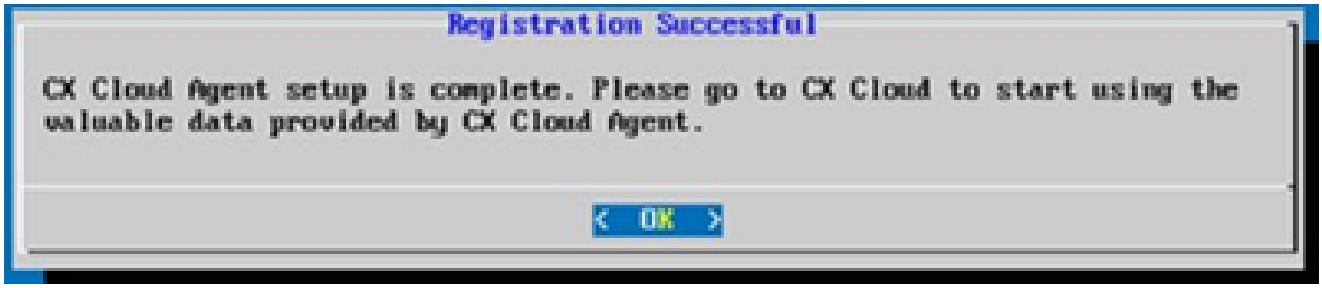
Codice di associazione

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



Codice scaduto

13. Fare clic su OK.



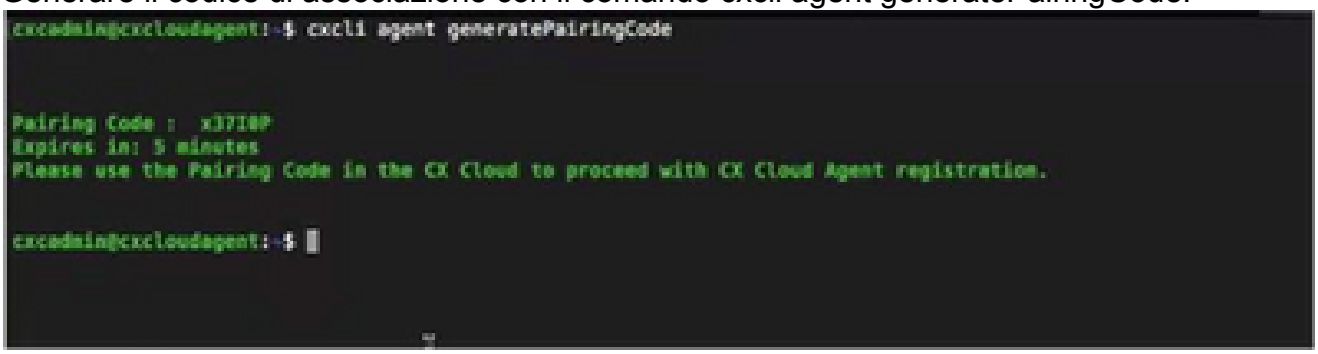
Registrazione completata

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 utilizzando 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.



Generazione del codice di associazione dalla CLI

3. Copiare il codice di associazione e tornare a CX Cloud per proseguire.

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

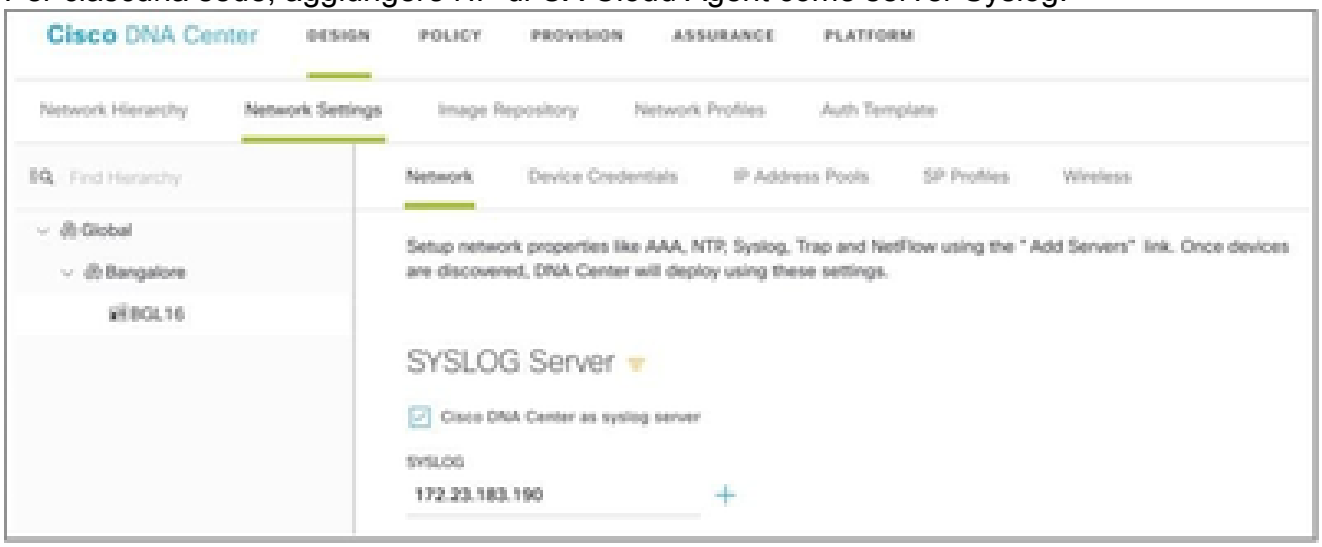
Prerequisiti

Le versioni supportate di Cisco DNA Center sono dalla 2.1.2.0 alla 2.2.3.5, dalla 2.3.3.4 alla 2.3.3.6, dalla 2.3.5.0 e da Cisco DNA Center Virtual Appliance

Configura impostazione inoltro syslog

Per configurare l'inoltro Syslog all'agente cloud CX nel Cisco DNA Center, attenersi alla seguente procedura:

1. Avviare Cisco DNA Center.
2. Andare a Design > Network Settings > Network (Progetto > Impostazioni di rete > Rete).
3. Per ciascuna sede, aggiungere l'IP di CX Cloud Agent come server Syslog.



Server Syslog

Note:
Una volta configurati, tutti i dispositivi associati a quel 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 impostati automaticamente sul livello critico predefinito.

Configurazione di altre risorse per l'inoltro del syslog all'agente cloud CX

I dispositivi devono essere configurati in modo da inviare messaggi Syslog all'agente cloud CX per utilizzare la funzione Fault Management di CX Cloud.

Nota: solo i dispositivi Campus Success Track di livello 2 possono configurare altre risorse per l'inoltro del syslog.

Server Syslog esistenti con funzionalità di inoltro

Eseguire le istruzioni di configurazione per il software del server syslog e aggiungere l'indirizzo IP dell'agente cloud CX come nuova destinazione.

Nota: quando si inoltrano i syslog, assicurarsi che l'indirizzo IP di origine del messaggio syslog originale venga mantenuto.

Server Syslog esistenti senza funzionalità di inoltro O senza server Syslog

Configurare ciascun dispositivo in modo che invii i syslog direttamente all'indirizzo IP dell'agente del cloud CX. Per i passaggi di configurazione specifici, consultare la documentazione.

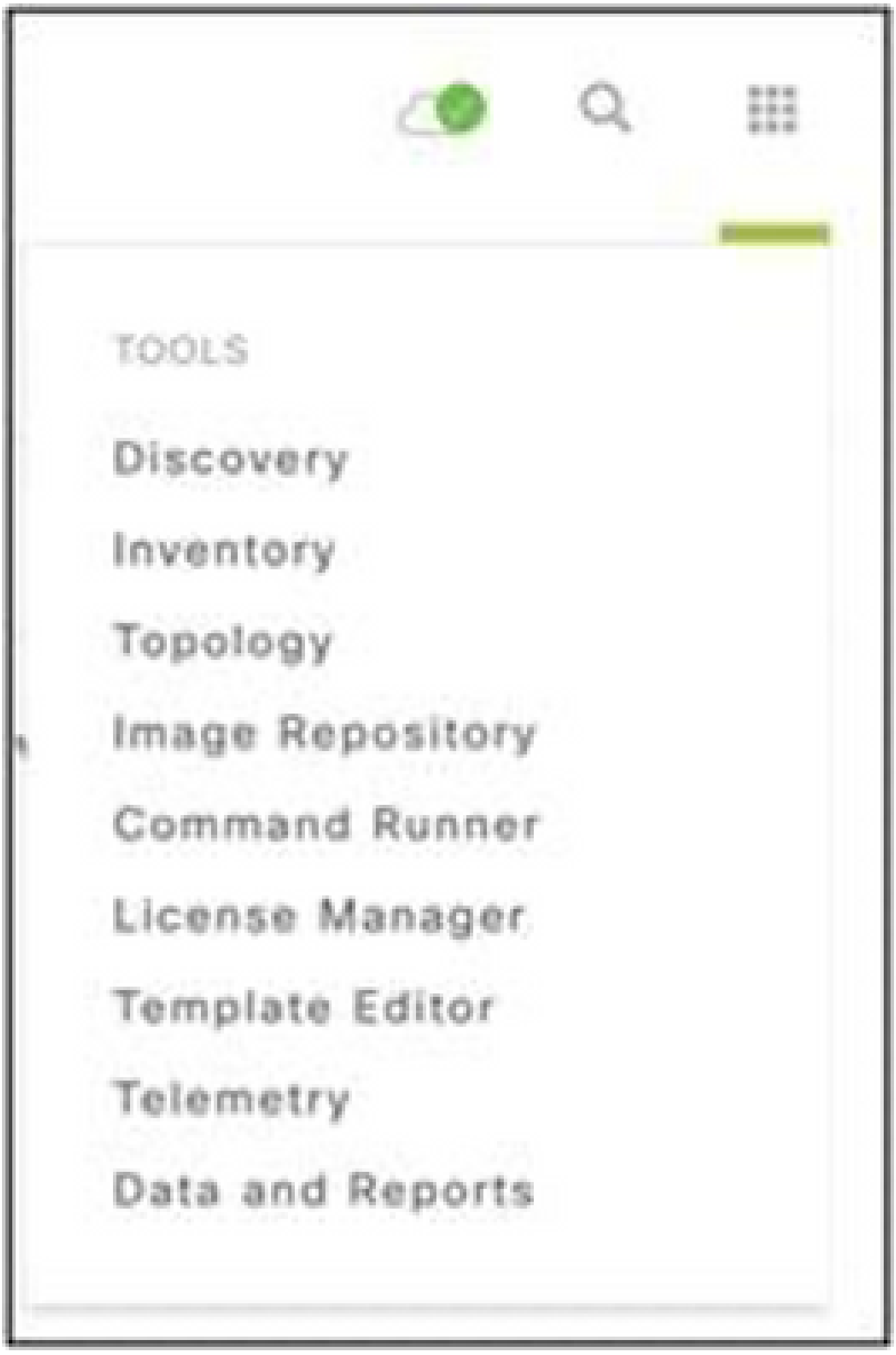
Guida alla configurazione di Cisco IOS® XE

Guida alla configurazione di AireOS Wireless Controller

Abilita impostazioni syslog livello informazioni

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

1. Selezionare Strumenti>Telemetria.


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

Menu Strumenti

2. Selezionare ed espandere la visualizzazione Sito e selezionare un sito dalla gerarchia.

Vista della sede

3. Selezionare il sito desiderato e selezionare tutte le periferiche che utilizzano la casella di controllo Nome periferica.

4. Selezionare Visibilità ottimale dall'elenco a discesa Azioni.

Azioni

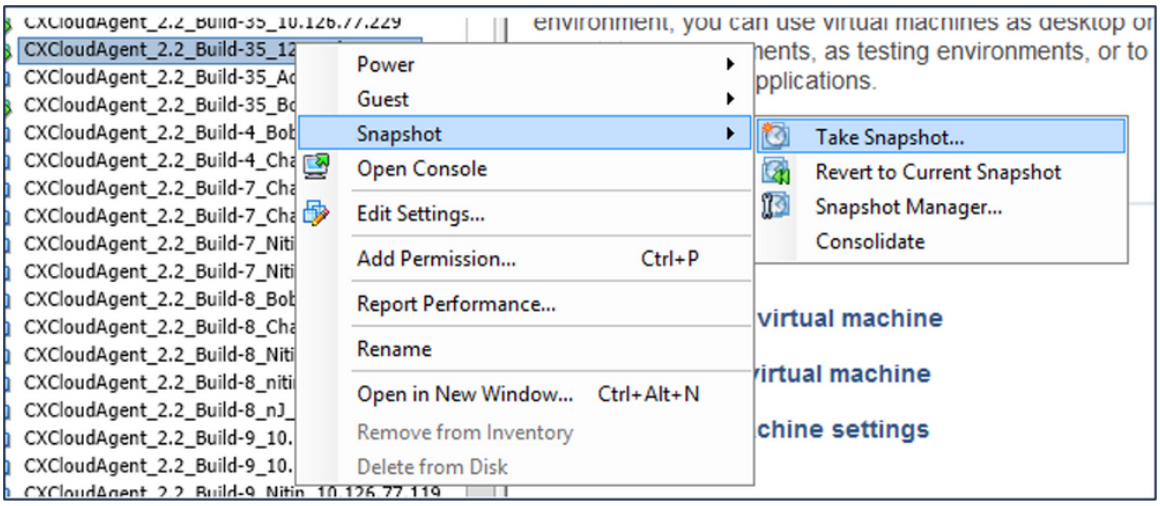
Backup e ripristino della VM cloud CX

Si consiglia di conservare lo stato e i dati di una VM agente cloud CX in un determinato point in time utilizzando la funzione di istantanea. Questa funzione facilita il ripristino della VM del cloud CX fino all'ora specifica in cui viene eseguita la copia istantanea.

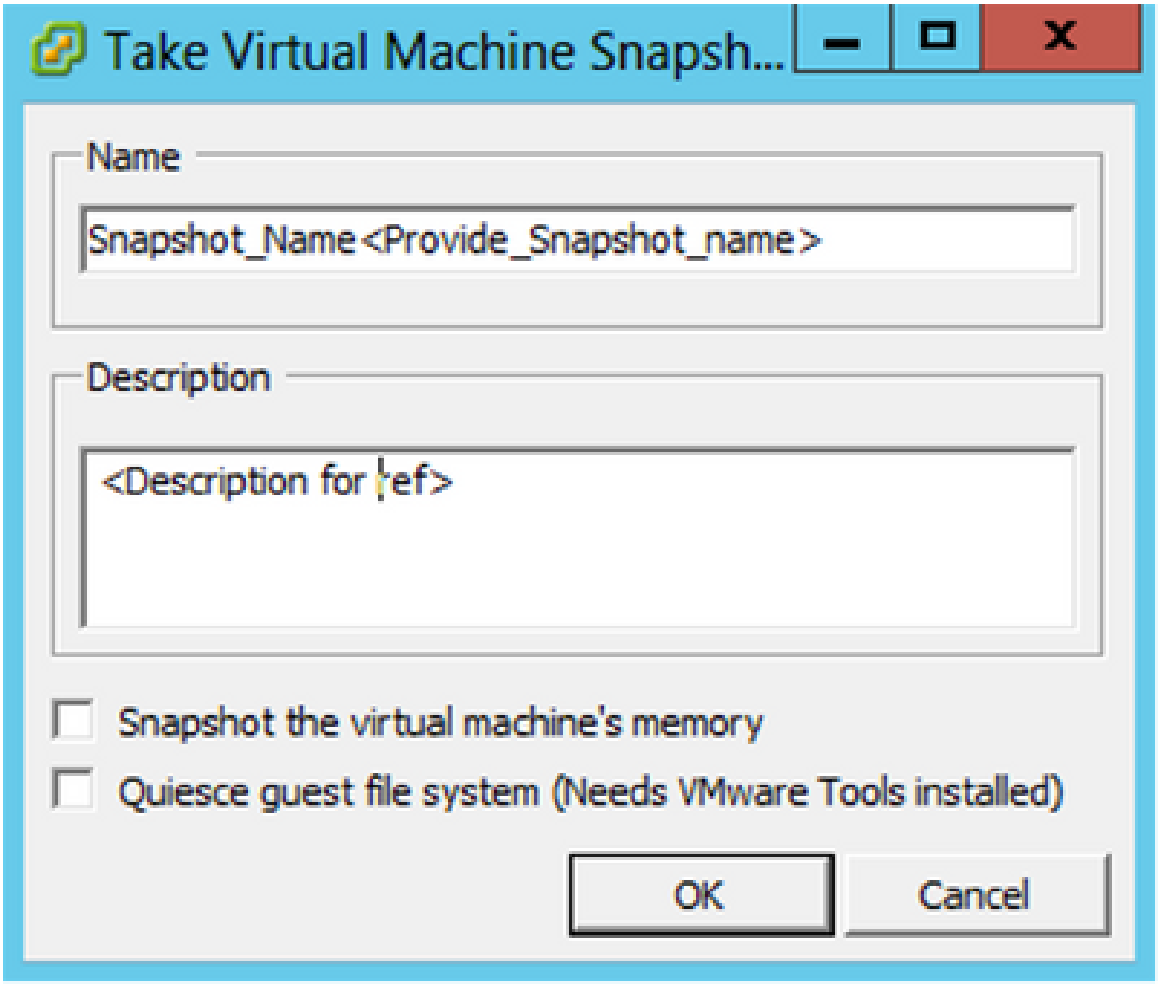
Backup

Per eseguire il backup della VM del cloud CX:

1. Fare clic con il pulsante destro del mouse sulla VM e selezionare Istantanea > Crea istantanea. Viene visualizzata la finestra Crea snapshot macchina virtuale.



Selezione della VM

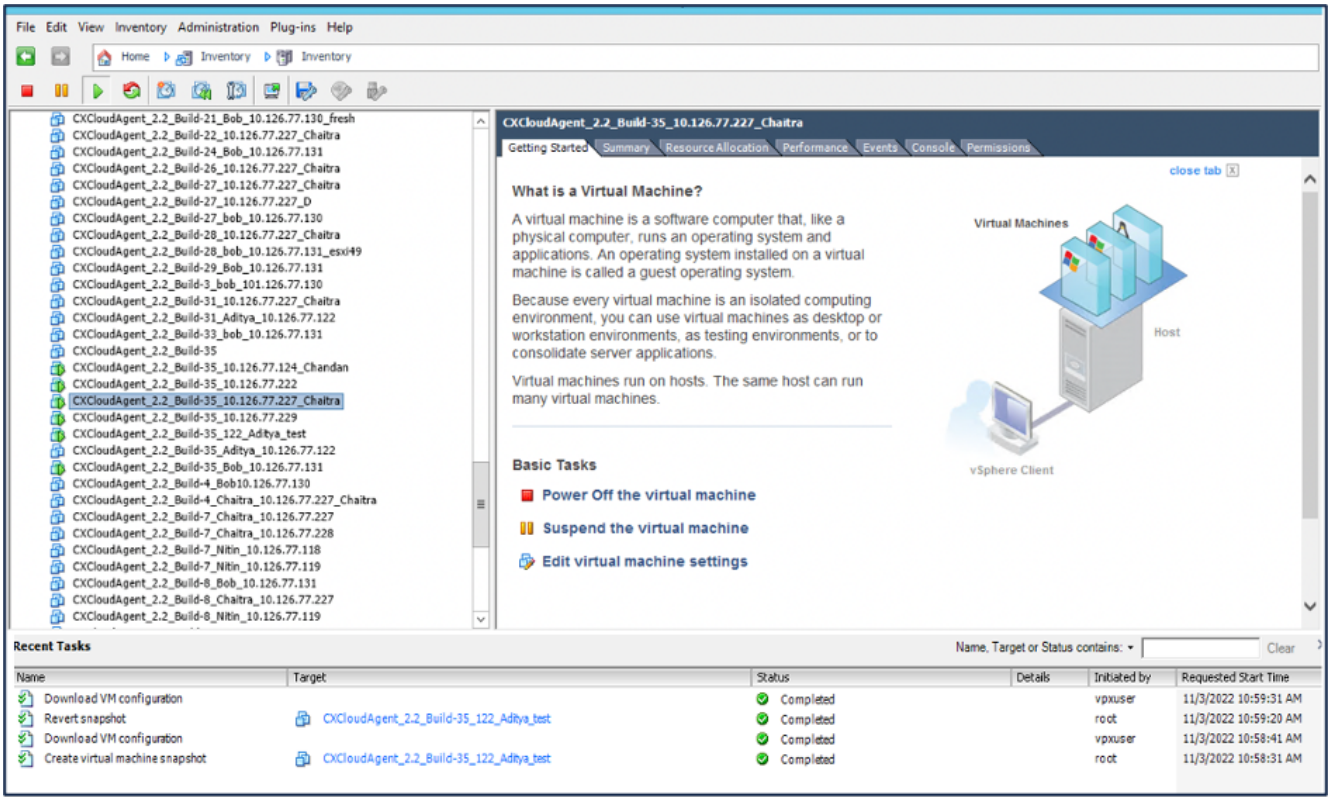


Crea snapshot macchina virtuale

2. Immettere Nome e Descrizione.

Nota: verificare che la casella di controllo Esegui snapshot della memoria della macchina virtuale sia deselezionata.

3. Fare clic su OK. Lo stato Crea snapshot macchina virtuale viene visualizzato come Completato nell'elenco Attività recenti.

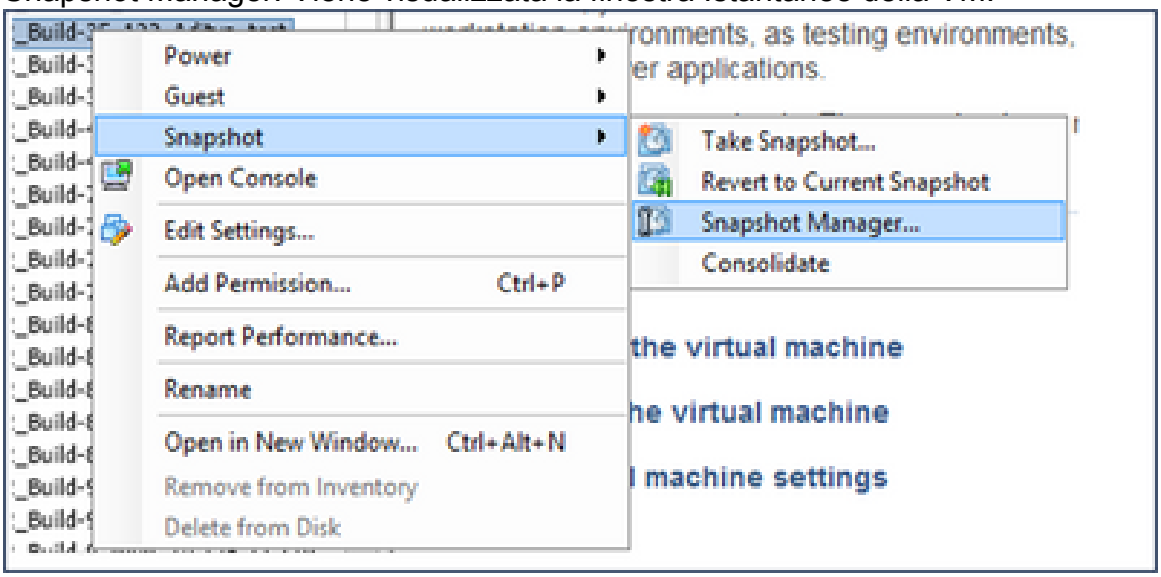


Attività recenti

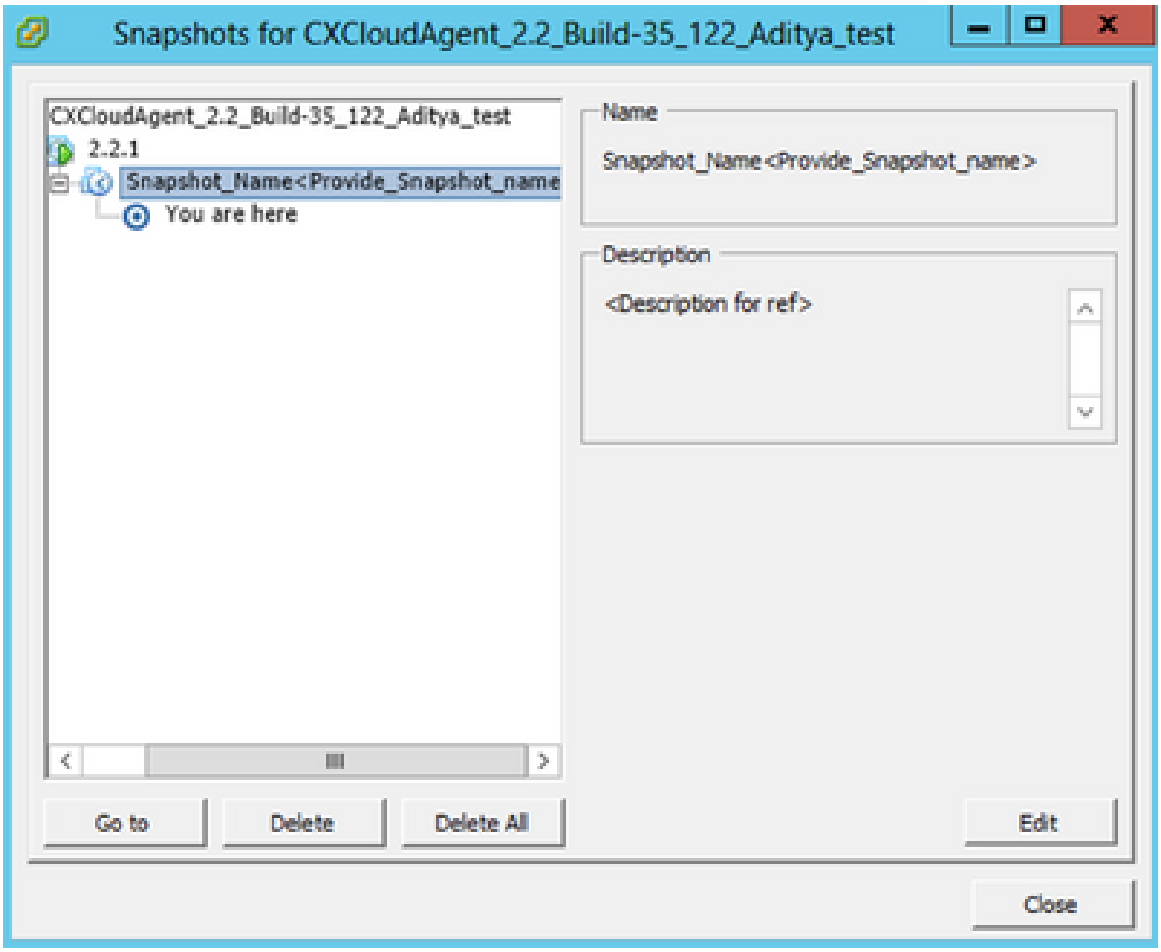
Ripristina

Per ripristinare la VM del cloud CX:

1. Fare clic con il pulsante destro del mouse sulla VM e selezionare Snapshot > Snapshot Manager. Viene visualizzata la finestra Istantanee della VM.

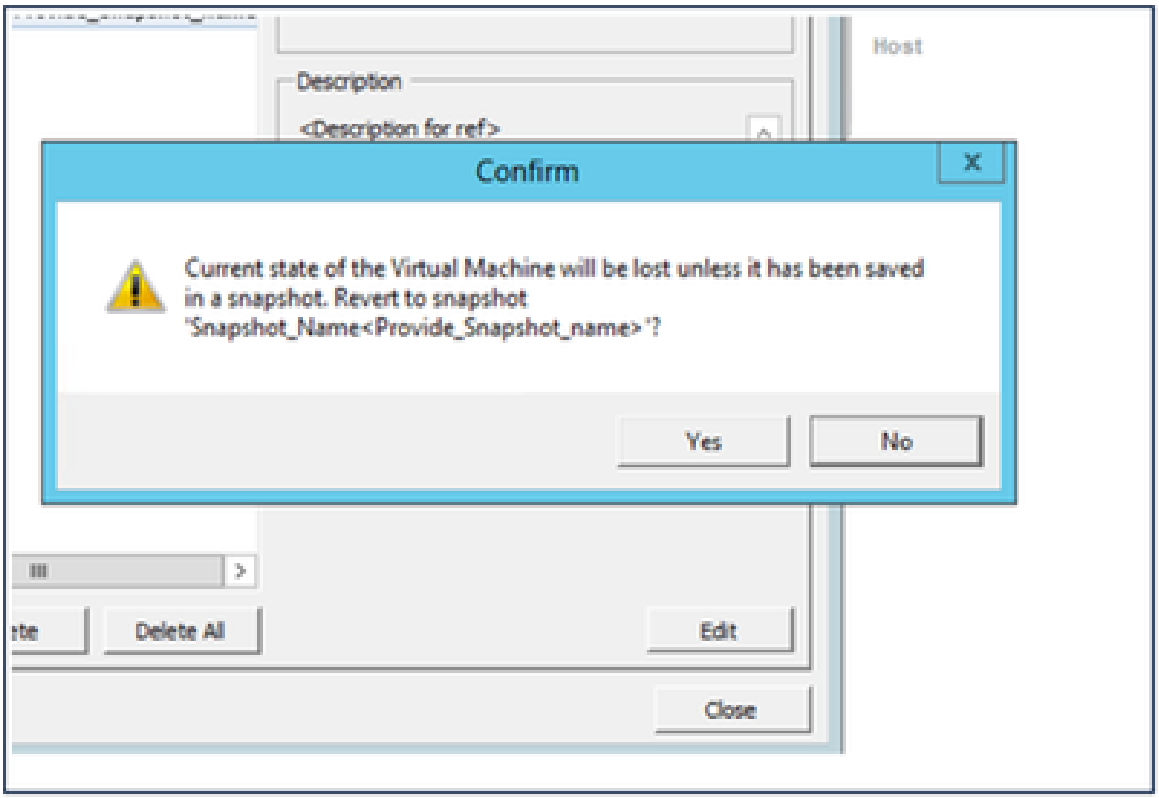


Finestra Seleziona VM



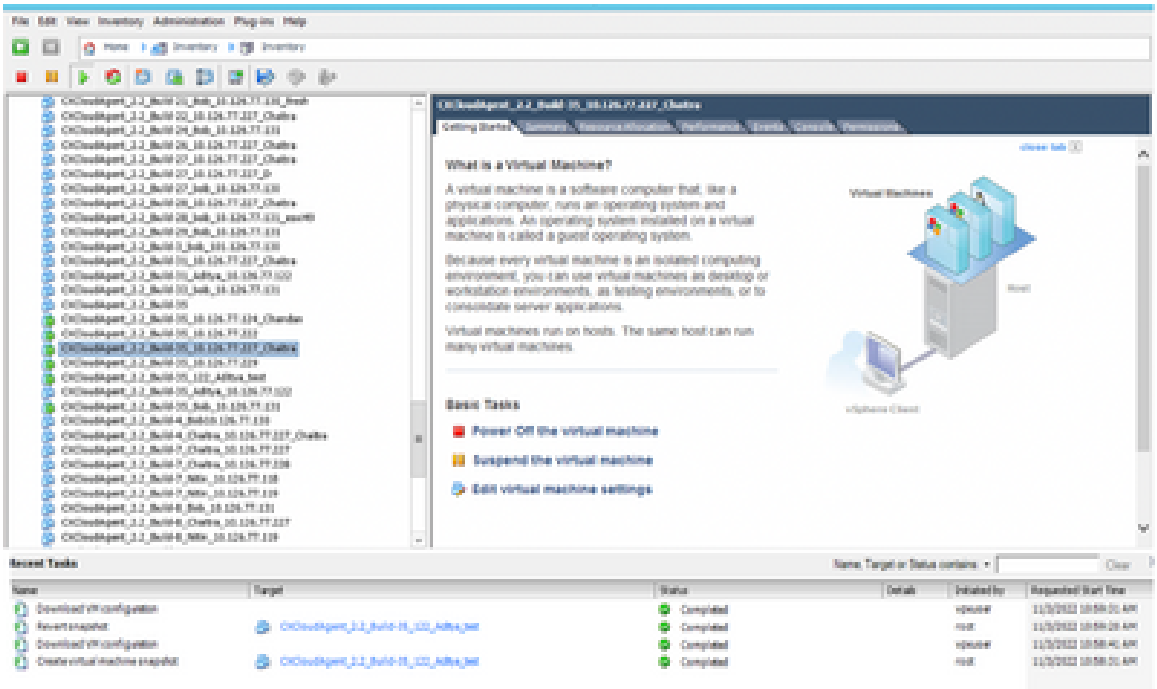
Finestra Snapshot

2. Fare clic su Vai a. Viene visualizzata la finestra Conferma.



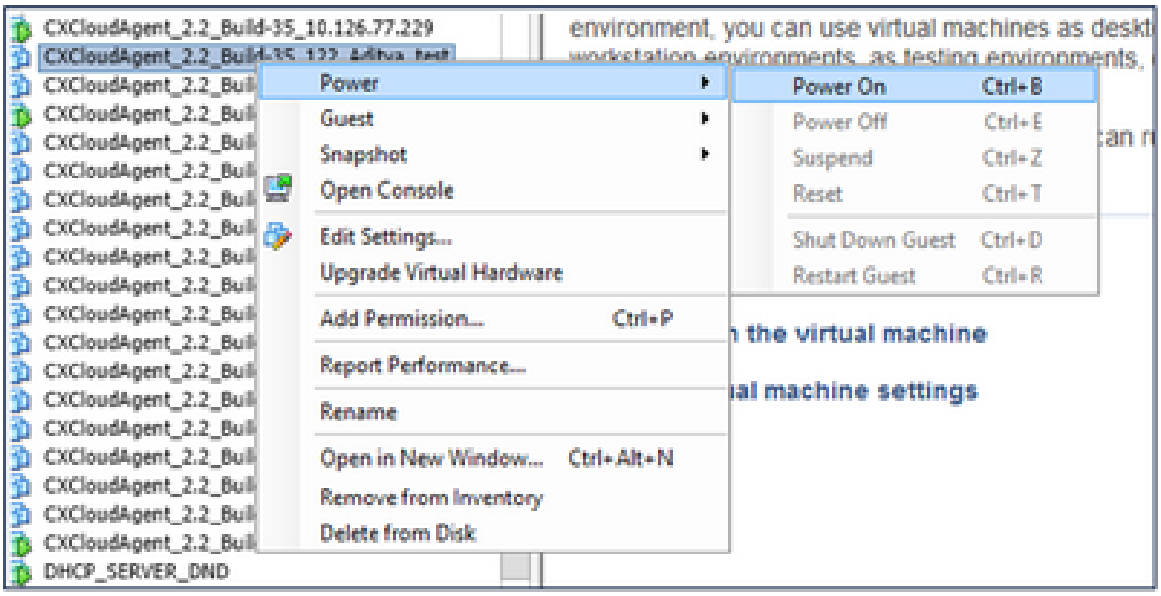
Finestra Conferma

3. Fare clic su Sì. Lo stato Ripristina snapshot viene visualizzato come Completato nell'elenco Attività recenti.



Attività recenti

4. Fare clic con il pulsante destro del mouse sulla VM e selezionare Accensione > Accendi per accendere la VM.



Sicurezza

CX Cloud Agent garantisce la sicurezza end-to-end. La connessione tra CX Cloud e CX Cloud Agent è protetta da TLS. L'utente SSH predefinito dell'agente cloud deve eseguire solo le operazioni di base.

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 a queste domande frequenti per impostare la password del bootloader (modalità utente singolo).

Sicurezza dell'account

Durante la distribuzione, viene creato l'account utente cxcadmin. Gli utenti sono obbligati a impostare una password durante la configurazione iniziale. Le credenziali e gli utenti cxcadmin vengono utilizzati per accedere alle API dell'agente cloud CX e per connettersi all'accessorio tramite SSH.

gli utenti cxcadmin dispongono di un accesso limitato con il minor numero di privilegi. La password cxcadmin segue i criteri di protezione ed è sottoposta a hash unidirezionale con un periodo di scadenza di 90 giorni. Gli utenti cxcadmin possono creare un utente cxcroot utilizzando l'utilità denominata remoteaccount. Gli utenti cxcadmin possono ottenere i privilegi root.

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 su password: l'accessorio gestisce un singolo utente (cxcadmin) che consente all'utente di autenticarsi e comunicare con l'agente cloud CX.

- Azioni eseguibili sull'appliance con privilegi root tramite SSH.

gli utenti cxcadmin possono creare utenti cxcroot utilizzando un'utilità denominata remoteaccount. Questa utility visualizza una password crittografata RSA/ECB/PKCS1v1_5 che può essere decrittografata solo dal portale SWIM (modulo di richiesta DECRYPT). Solo il personale autorizzato può accedere a questo portale. Gli utenti di Cxcroot possono ottenere i privilegi di root utilizzando questa password decrittografata. La passphrase è valida solo per due giorni. Gli utenti cxcadmin devono ricreare l'account e ottenere la password dalla scadenza della password del post-portale SWIM.

Protezione avanzata

L'appliance CX Cloud Agent è conforme agli standard di protezione avanzata di Center of Internet Security.

Sicurezza dei dati

L'appliance CX Cloud Agent non memorizza le informazioni personali dei clienti. L'applicazione per le credenziali del dispositivo (in esecuzione come uno dei pod) archivia le credenziali del server crittografato all'interno del database protetto. I dati raccolti non vengono memorizzati in alcun modo all'interno dell'accessorio, se non temporaneamente durante l'elaborazione. I dati di telemetria vengono caricati in CX Cloud appena possibile dopo il completamento della raccolta e vengono immediatamente eliminati dallo storage locale dopo la conferma del corretto caricamento.

Trasmissione dati

Il pacchetto di registrazione contiene il certificato e le chiavi univoci richiesti per il dispositivo X.509 per stabilire una connessione sicura con Iot Core. Tramite tale agente viene stabilita una connessione protetta utilizzando il protocollo MQTT (Message Queuing Telemetry Transport) su TLS (Transport Layer Security) versione 1.2

Log e monitoraggio

I registri non contengono alcun tipo di dati PII (Personal Identifier Information). I registri di verifica acquisiscono tutte le azioni relative alla sicurezza eseguite sull'appliance CX Cloud Agent.

Comandi di telemetria Cisco

CX Cloud recupera la telemetria degli asset utilizzando le API e i comandi elencati nei comandi di telemetria Cisco. Questo documento classifica i comandi in base alla loro applicabilità all'inventario Cisco DNA Center, al Diagnostic Bridge, all'Intersight, alle informazioni sulla

conformità, ai guasti e a tutte le altre fonti di telemetria raccolte dall'agente cloud CX.

Le informazioni sensibili all'interno della telemetria degli asset vengono nascoste prima di essere trasmesse al cloud. L'agente cloud CX maschera i dati sensibili per tutte le risorse raccolte che inviano la telemetria direttamente all'agente cloud CX. ad esempio password, chiavi, stringhe della community, nomi utente e così via. I controller forniscono il masking dei dati per tutte le risorse gestite dai controller prima di trasferire queste informazioni all'agente cloud CX. In alcuni casi, la telemetria delle risorse gestite dai controller può essere ulteriormente anonimizzata. Per ulteriori informazioni sull'anonimizzazione della telemetria (ad esempio, la sezione Anonimizza dati della Cisco DNA Center Administrator Guide), consultare la documentazione di supporto del prodotto corrispondente.

Anche se l'elenco dei comandi di telemetria non può essere personalizzato e le regole di mascheramento dei dati non possono essere modificate, i clienti possono controllare gli accessi di telemetria degli asset a CX Cloud specificando le origini dati come indicato nella documentazione di supporto del prodotto per i dispositivi gestiti da controller o nella sezione Connessione delle origini dati di questo documento (per Altre risorse raccolte da 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. Gli utenti devono fare riferimento alle domande frequenti per impostare la password del bootloader (modalità utente singolo).
Accesso utente	SSH: ·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.
Account utente	· cxcadmin: account utente predefinito creato; l'utente può eseguire i comandi dell'applicazione CX Cloud Agent utilizzando cxcli e dispone dei privilegi minimi sull'accessorio; l'utente cxcadmin e la relativa password crittografata vengono generati utilizzando cxcadmin user. · cxcroot: cxcadmin consente di creare l'utente utilizzando l'account remoto dell'utilità. L'utente può ottenere i privilegi root con questo account.
Policy della	·La password ha un hash unidirezionale che utilizza SHA-256 e viene

password di cxcadmin	memorizzata in modo sicuro. · Almeno otto (8) caratteri, contenenti tre di queste categorie: maiuscole, minuscole, numeri e caratteri speciali.
Policy della password cxcroot	·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 due giorni e possono essere rigenerati utilizzando cxcadmin user.
Policy della password di accesso tramite SSH	· Un minimo di otto caratteri che contengono tre di queste categorie: maiuscole, minuscole, numeri e caratteri speciali. · Cinque tentativi di login non riusciti bloccano la scatola per 30 minuti; la password scade tra 90 giorni.
Porte	Porte in ingresso aperte - 514 (Syslog) e 22 (SSH)
Sicurezza dei dati	·Nessuna informazione dei clienti viene memorizzata. ·Nessun dato dei dispositivi viene memorizzato. ·Le credenziali del server Cisco DNA Center sono criptate e memorizzate nel database.

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).