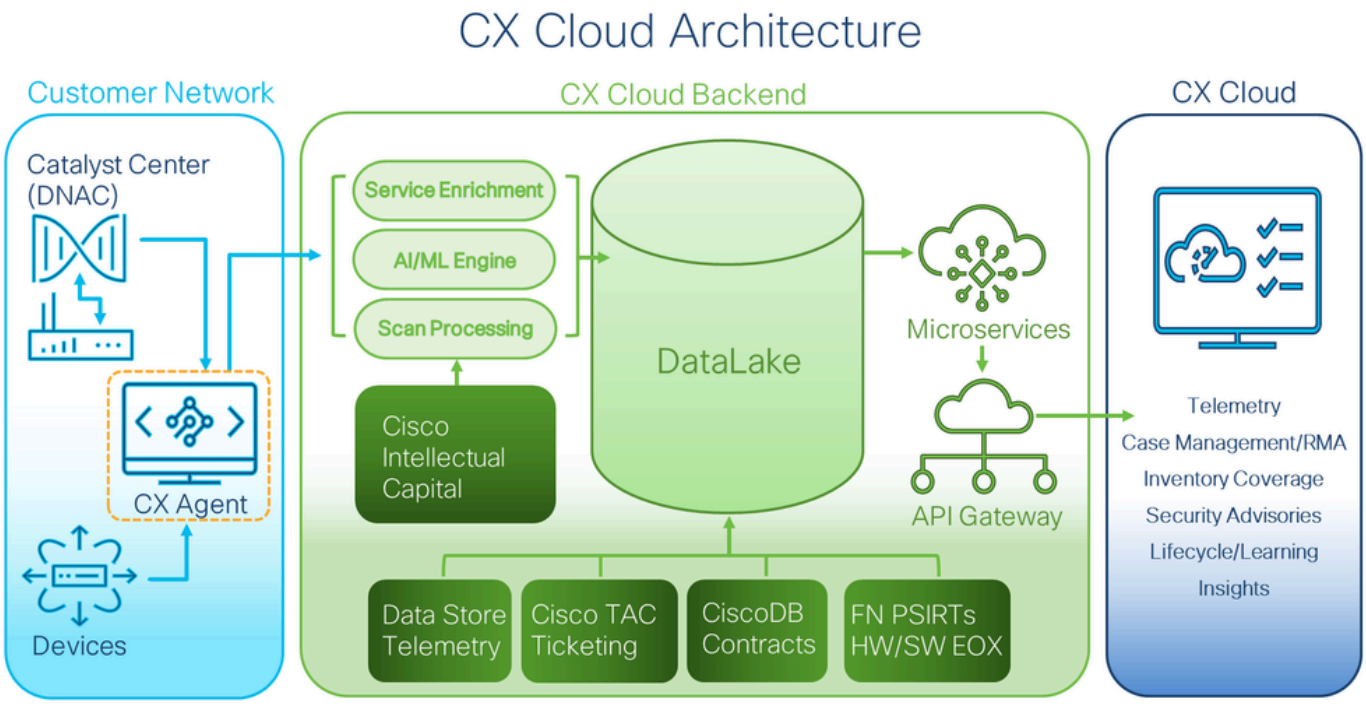
Guida alla panoramica di CX Agent v3.1

Sommario

Introduzione

Questo documento descrive Cisco's Customer Experience (CX) Agent. L'agente CX di Cisco è una piattaforma altamente scalabile che raccoglie dati di telemetria dai dispositivi di rete dei clienti per fornire informazioni pratiche ai clienti. L'agente CX consente la trasformazione di intelligenza artificiale (AI)/Machine Learning (ML) dei dati di configurazione in esecuzione attiva in informazioni proattive e predittive visualizzate in CX Cloud (inclusi Success Tracks, Smart Net Total Care (SNTC) e Business Critical Services (BCS) o Lifecycle Services (LCS)).



Architettura di CX Cloud

Questa guida è destinata esclusivamente agli amministratori di CX Cloud e dei partner. Gli utenti con ruoli di amministratore utenti privilegiati (SUA) e di amministratore dispongono delle autorizzazioni necessarie per eseguire le azioni descritte in questa guida.

Questa guida è specifica di CX Agent v3.1. Fare riferimento alla pagina Cisco CX Agent per accedere alle versioni precedenti.

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

Prerequisiti

L'agente CX viene eseguito come macchina virtuale ed è disponibile per il download come appliance virtuale aperta o disco rigido virtuale.

Requisiti di distribuzione

- Per una nuova installazione è necessario uno dei seguenti hypervisor:
  - VMware ESXi v5.5 o versioni successive
  - Oracle Virtual Box v5.2.30 o versioni successive

    - Windows Hypervisor versione 2012-2022 e versione 2025
- Per la distribuzione della macchina virtuale sono necessarie le configurazioni riportate nella tabella seguente:

Tipo di distribuzione dell'agente CX	Numero di core CPU	RAM	Disco rigido	*Numero massimo di asset direttamente collegato all'agente CX	Hypervisor supportati
OAV piccolo	8C	16 GB	200 GB	10,000	VMware ESXi, Oracle VirtualBox e Windows Hyper-V
OVULI medi	16°C	32 GB	600 GB	20,000	VMWare ESXi
OVULI grandi	32 quater	64 GB	1.200 GB	50,000:	VMWare ESXi

*Oltre a collegare 20 non cluster Cisco Catalyst Center (Catalyst Center) o 10 cluster Catalyst Center per ogni istanza di agente cloud CX.

Nota:il servizio RADKit è disponibile esclusivamente per le distribuzioni dell'agente CX di tipi OVA medi 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 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 di CX Cloud: l'agente CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando l'FQDN e utilizzando HTTPS sulla porta TCP 443:
    - FQDN: agent.us.csco.cloud
    - FQDN: agente.emea.cisco.cloud
    - FQDN: ng.acs.agent.emea.cisco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati dell'area Asia Pacifico designati come area dati principale per l'archiviazione dei dati di CX Cloud: l'agente CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando l'FQDN e utilizzando HTTPS sulla porta TCP 443:

    - FQDN: agent.us.csco.cloud
    - FQDN: agente.apjc.cisco.cloud
    - FQDN: ng.acs.agent.apjc.cisco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati designati per l'Europa e l'Asia Pacifico come regione dati principale, connettività all'FQDN: agent.us.csco.cloud è richiesto solo per la registrazione dell'agente CX Cloud con CX Cloud durante la configurazione iniziale. Una volta completata la registrazione dell'agente di CX Cloud con CX Cloud, questa connessione non è più necessaria.
- Per la gestione locale dell'agente cloud CX, la porta 22 deve essere accessibile.
- Per i clienti che utilizzano RADKit con FQDN e HTTPS sulla porta TCP 443:
    - FQDN USA: radkit.us.csco.cloud
    - FQDN EMEA: radkit.emea.cisco.cloud
    - FQDN APJC: radkit.apjc.cisco.cloud
- Per consentire a RADKit di collegare l'output a una richiesta di servizio, il nome di dominio completo cxd.cisco.com deve essere accessibile per l'agente CX.
- 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 radkit.emea.csco.cloud Catalyst 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 Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- Un indirizzo IP viene rilevato automaticamente se il protocollo DHCP (Dynamic Host Configuration Protocol) è abilitato nell'ambiente VM; In caso contrario, devono essere disponibili un indirizzo IPv4 libero, una subnet mask, un indirizzo IP predefinito del gateway e un indirizzo IP del server DNS (Domain Name Service).
- Solo IPv4 è supportato.
- Le versioni certificate di un singolo nodo e di un cluster ad alta disponibilità (HA, High Availability) Catalyst Center 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 un'appliance virtuale Catalyst Center e di un'appliance virtuale Catalyst Center.
- Se la rete dispone di un'intercettazione SSL, inserire l'indirizzo IP dell'agente CX nell'elenco delle autorizzazioni.

- 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 CX Cloud, gli utenti devono accedere ai seguenti domini. Utilizzare solo i nomi host forniti; non utilizzare indirizzi IP statici.

Domini specifici del portale dell'agente CX

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

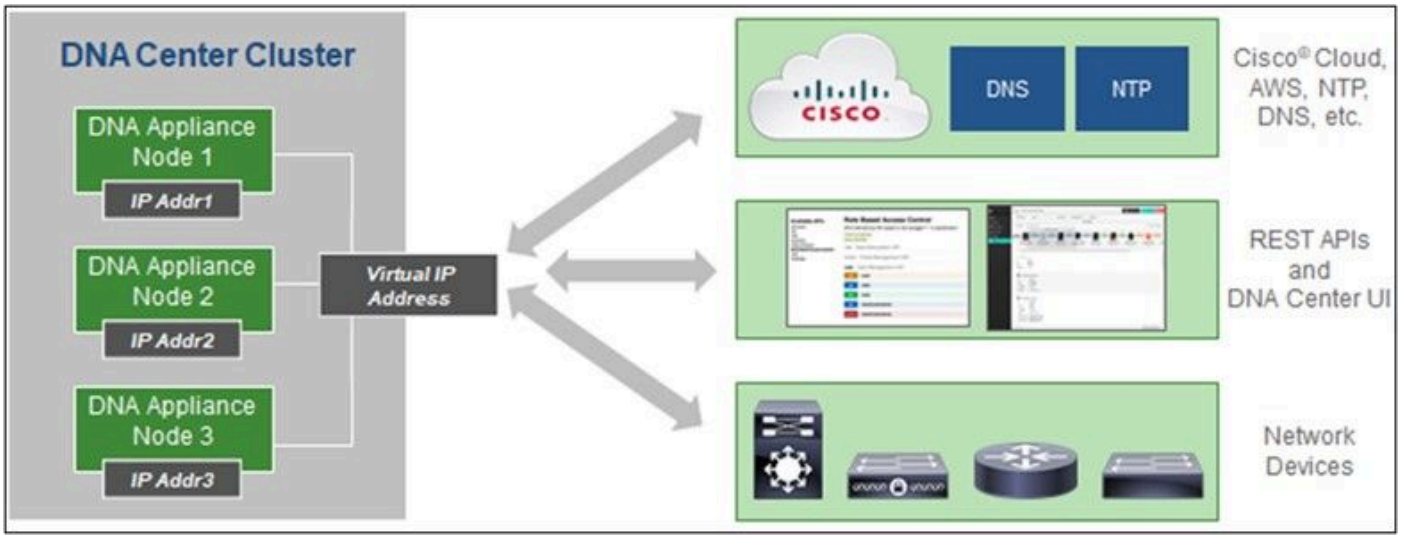
Domini specifici per l'agente CX

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 gli FQDN specificati.

Versioni supportate da Catalyst Center

Le versioni supportate di Catalyst Center a nodo singolo e HA Cluster 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 Catalyst Center Virtual Appliance e Catalyst 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 Agent, consultare l'elenco dei prodotti supportati.

Aggiornamento/installazione di CX Agent v3.1

- I clienti esistenti che eseguono l'aggiornamento alla nuova versione devono fare riferimento alla sezione Aggiornamento di CX Agent v3.1.
- I nuovi clienti che implementano una nuova installazione flessibile di OAV v3.1 devono fare riferimento all'aggiunta dell'agente CX.

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.

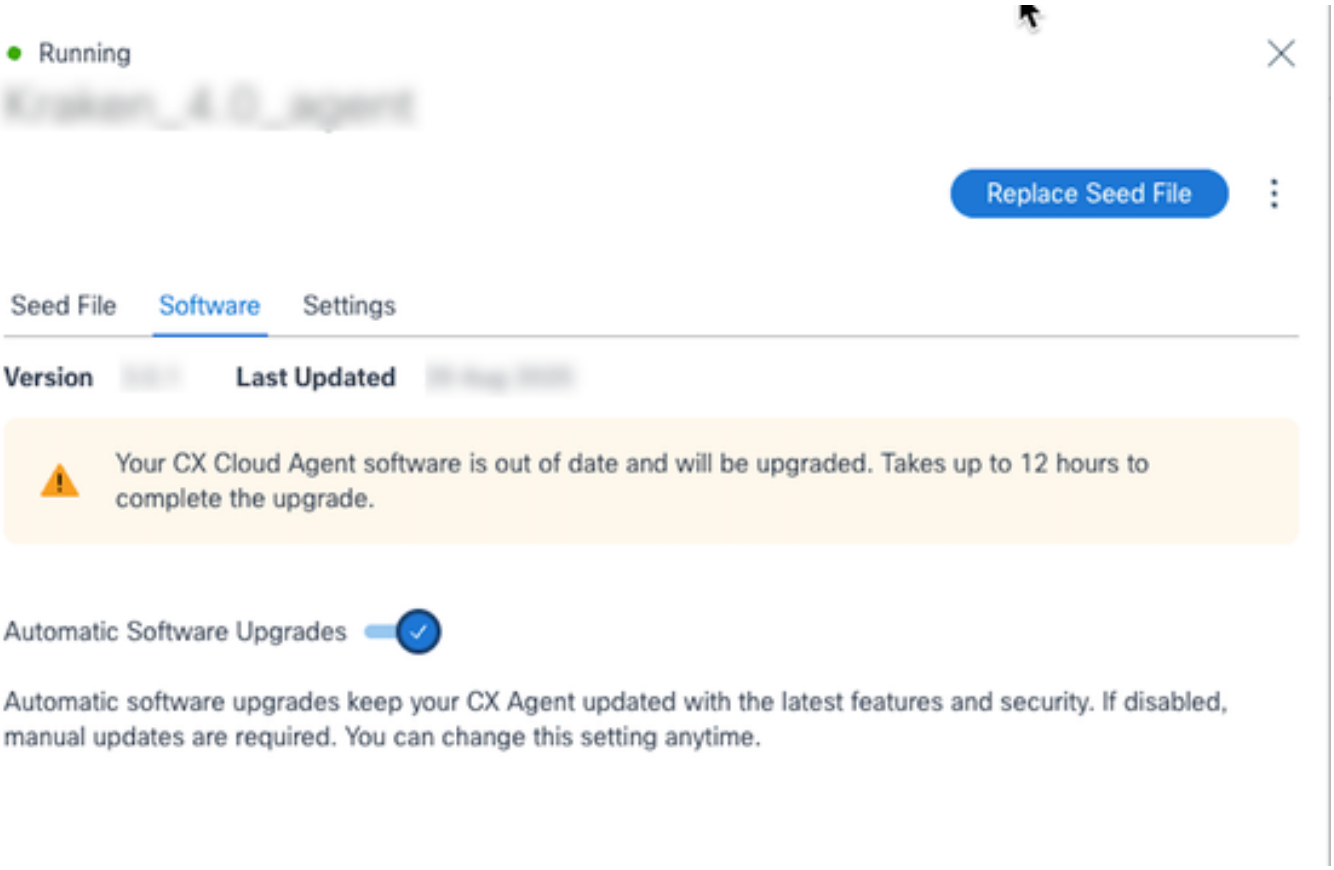
Per aggiornare la configurazione della VM esistente da piccola a media o grande, fare riferimento alla sezione Aggiornamento delle VM dell'agente CX alla configurazione media e grande.

Aggiornamento a CX Agent v3.1

I clienti esistenti possono eseguire l'aggiornamento alla versione più recente attivando gli aggiornamenti automatici o scegliendo di eseguire l'aggiornamento manualmente dalla versione esistente.

Aggiornamenti automatici

I clienti possono attivare l'interruttore Aggiornamento automatico software per assicurarsi che il sistema venga aggiornato quando vengono rilasciate le nuove versioni. Questa opzione è abilitata per impostazione predefinita per le nuove installazioni, ma può essere modificata in qualsiasi momento per allinearla ai criteri aziendali o per pianificare gli aggiornamenti durante le finestre di manutenzione pianificata.



Aggiornamenti automatici

Nota: gli aggiornamenti automatici sono disabilitati per impostazione predefinita per le istanze esistenti dell'agente CX, ma gli utenti possono abilitarli in qualsiasi momento.

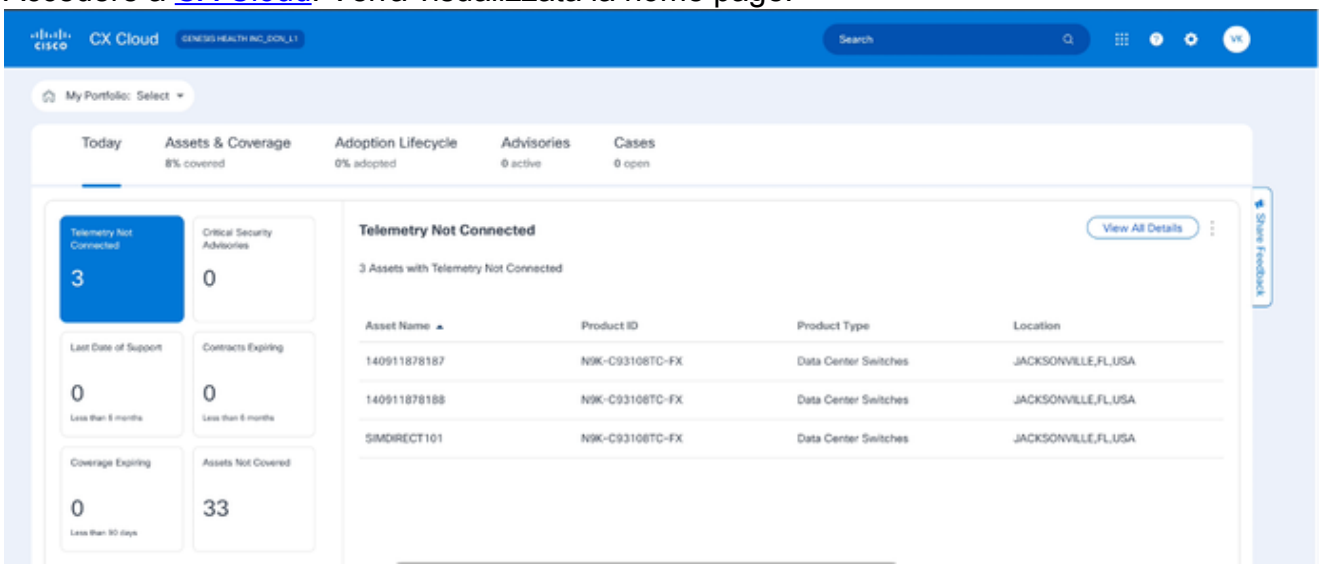
Aggiornamenti manuali

I clienti che preferiscono non utilizzare gli aggiornamenti automatici e che non hanno attivato Aggiornamenti automatici del software possono scegliere di eseguire l'aggiornamento manualmente. CX Agent v2.4.x e versioni successive supportano l'aggiornamento diretto alla versione v3.1 seguendo la procedura descritta in questa sezione.

Nota: i clienti che utilizzano CX Agent v2.3.x e versioni successive devono eseguire l'aggiornamento alla versione v2.4.x in modo incrementale prima di eseguire l'aggiornamento alla versione v3.1 o eseguire una nuova installazione di OAV.

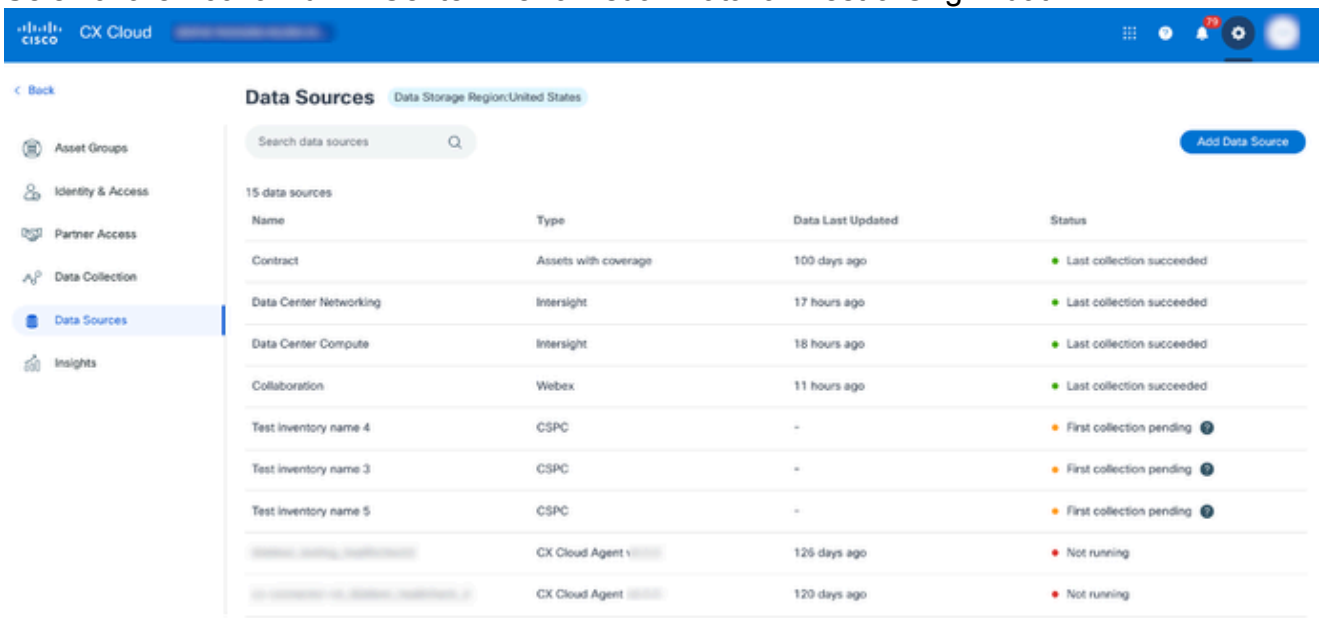
Per installare l'aggiornamento di CX Agent v3.1 da CX Cloud:

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



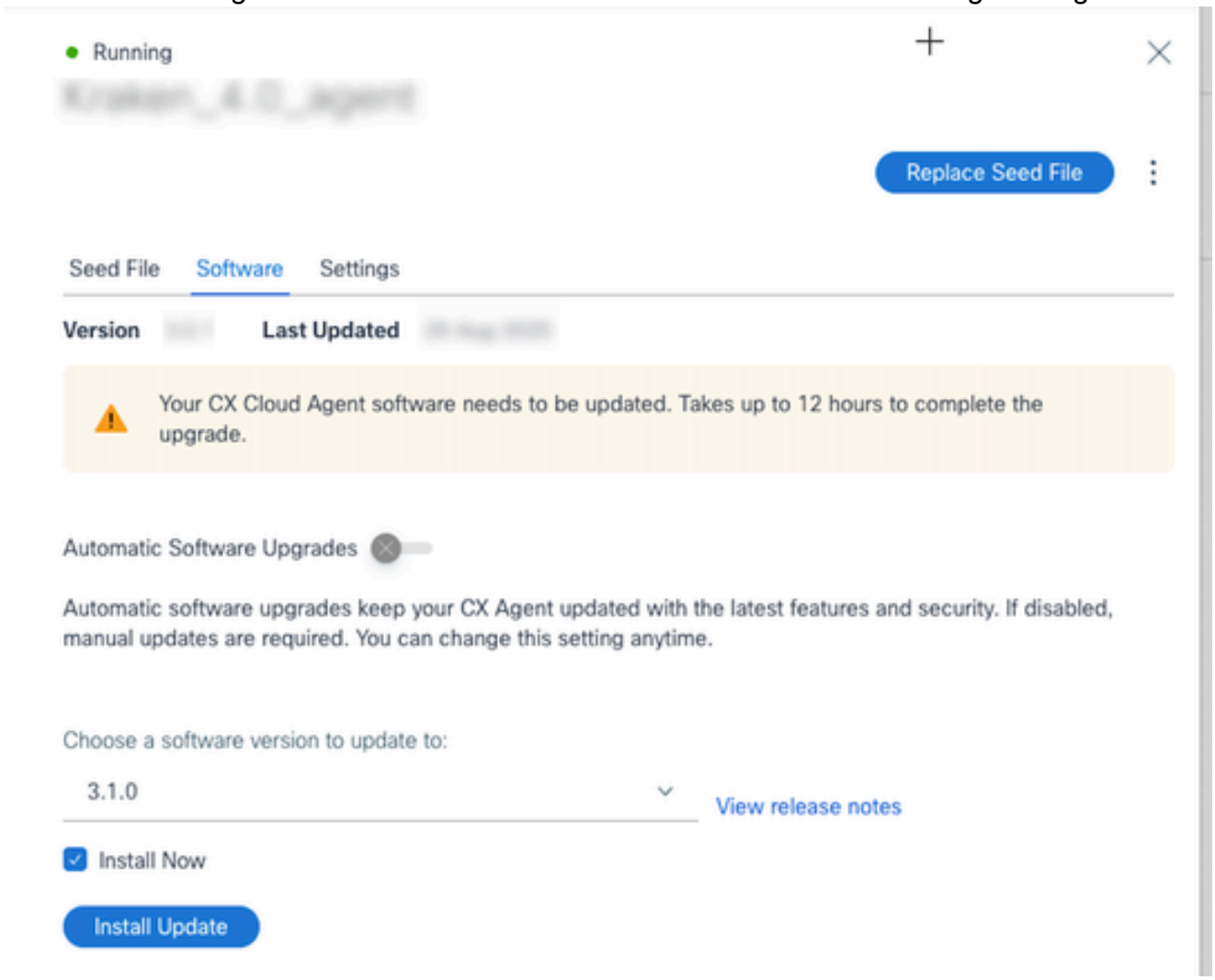
Home page di CX Cloud

2. Selezionare l'icona Admin Center. Verrà visualizzata la finestra Origini dati.



Origini dei dati

3. Fare clic su CX Agent Data Source. Viene visualizzata la finestra dei dettagli dell'agente CX.



Aggiornamenti manuali

4. Selezionare la versione del software 3.1.0 dall'elenco a discesa Scegliere una versione del software da aggiornare.
5. Fare clic su Installa aggiornamento per installare CX Agent v3.1.

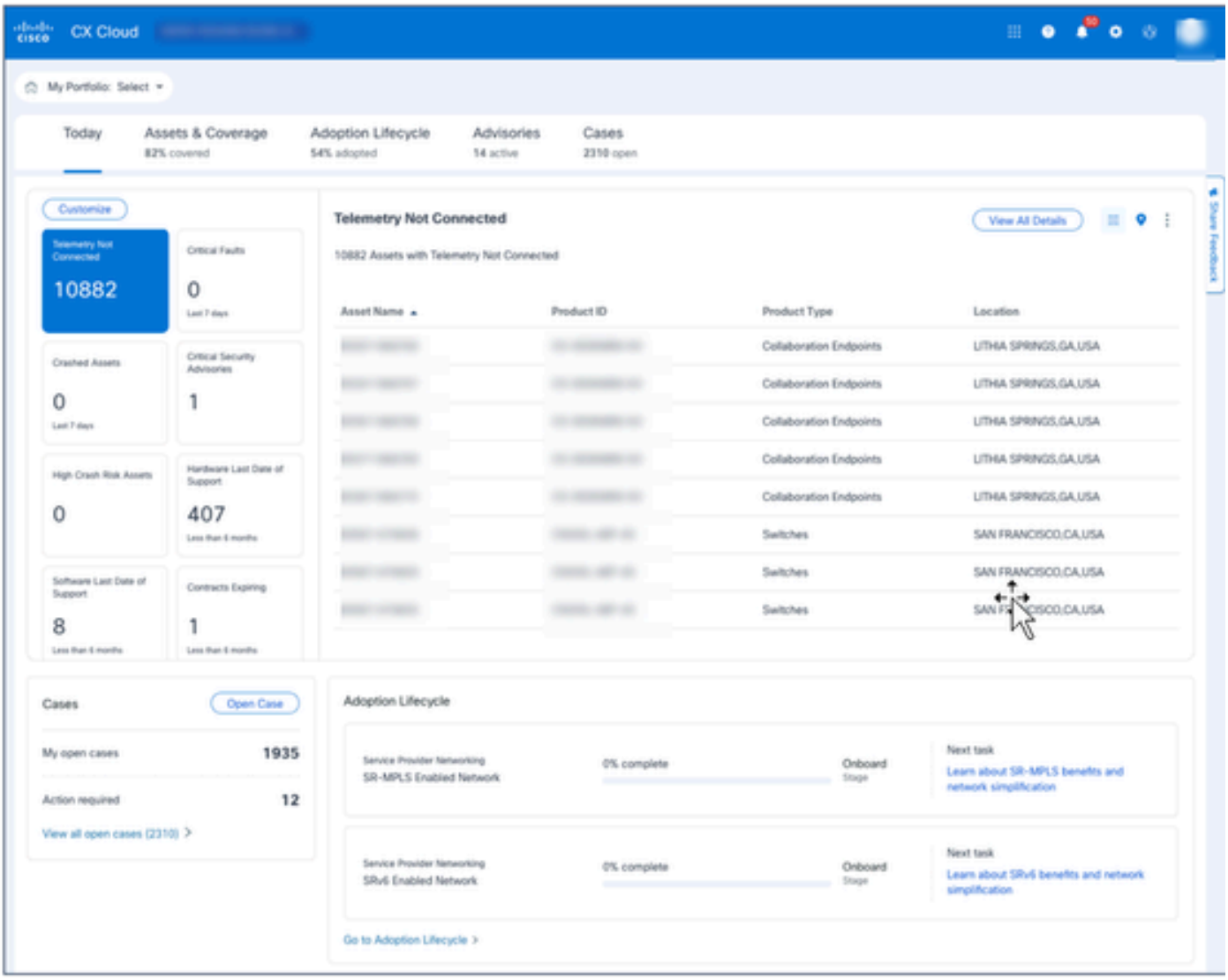
Nota: i clienti possono pianificare l'aggiornamento per un secondo momento deselezionando la casella di controllo Installa ora che visualizza le opzioni di programmazione.

Aggiunta dell'agente CX

I clienti possono aggiungere fino a 20 istanze dell'agente CX in CX Cloud.

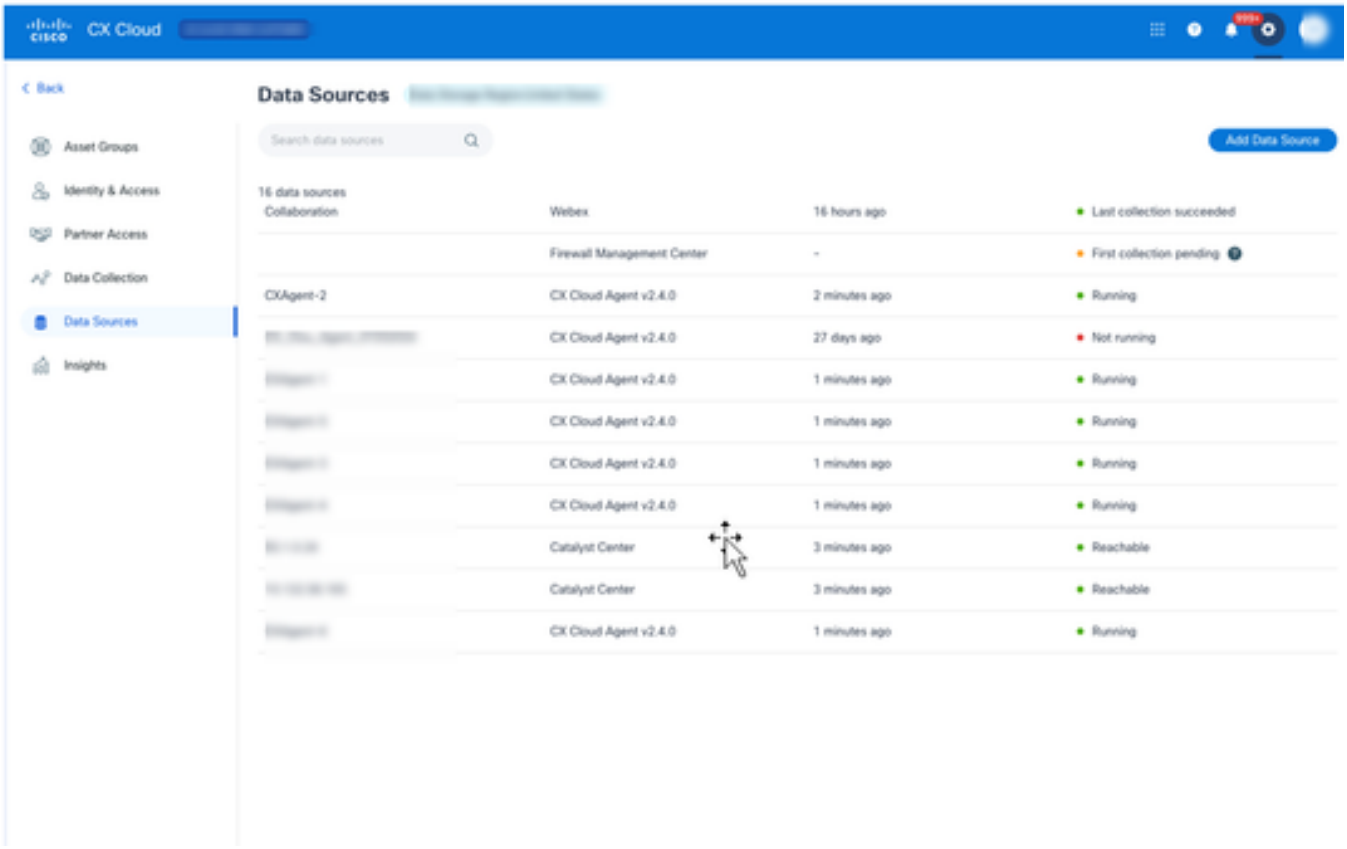
Per aggiungere un agente CX:

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



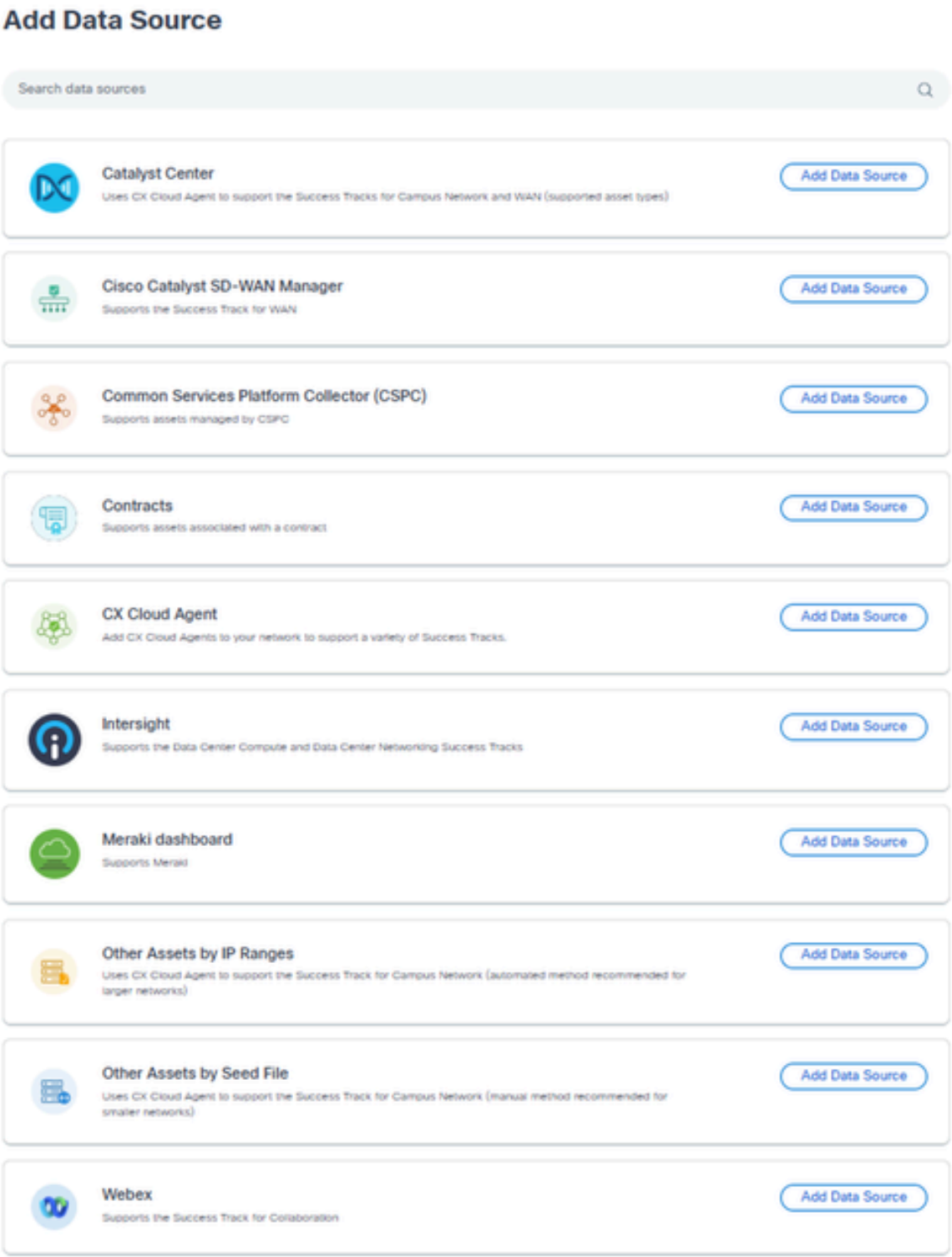
Home page di CX Cloud

2. Selezionare l'icona Admin Center. Verrà visualizzata la finestra Origini dati.



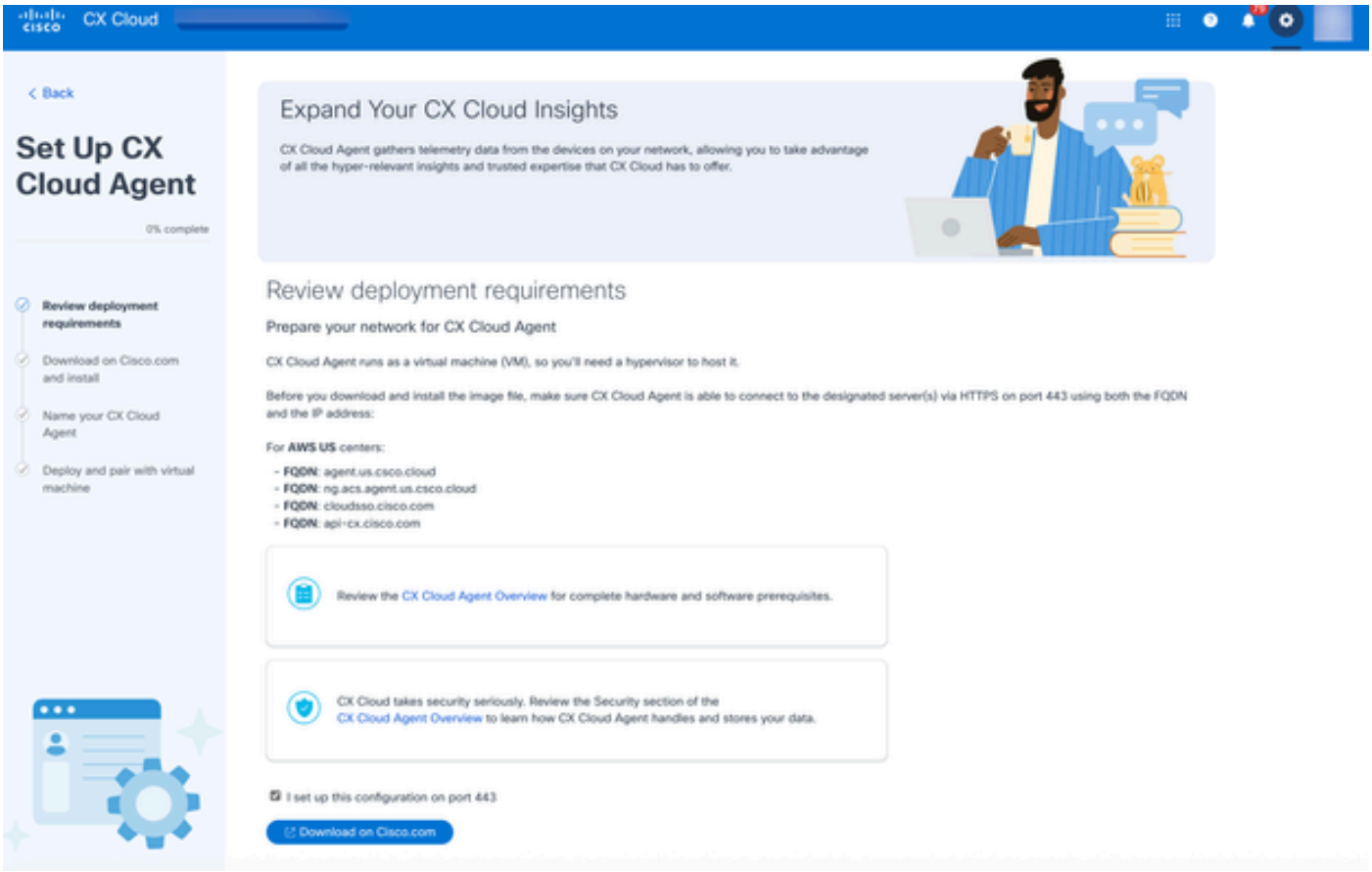
Origini dei dati

3. Fare clic su Aggiungi origine dati. Verrà visualizzata la pagina 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 Agent. Viene visualizzata la finestra Set Up CX Agent.



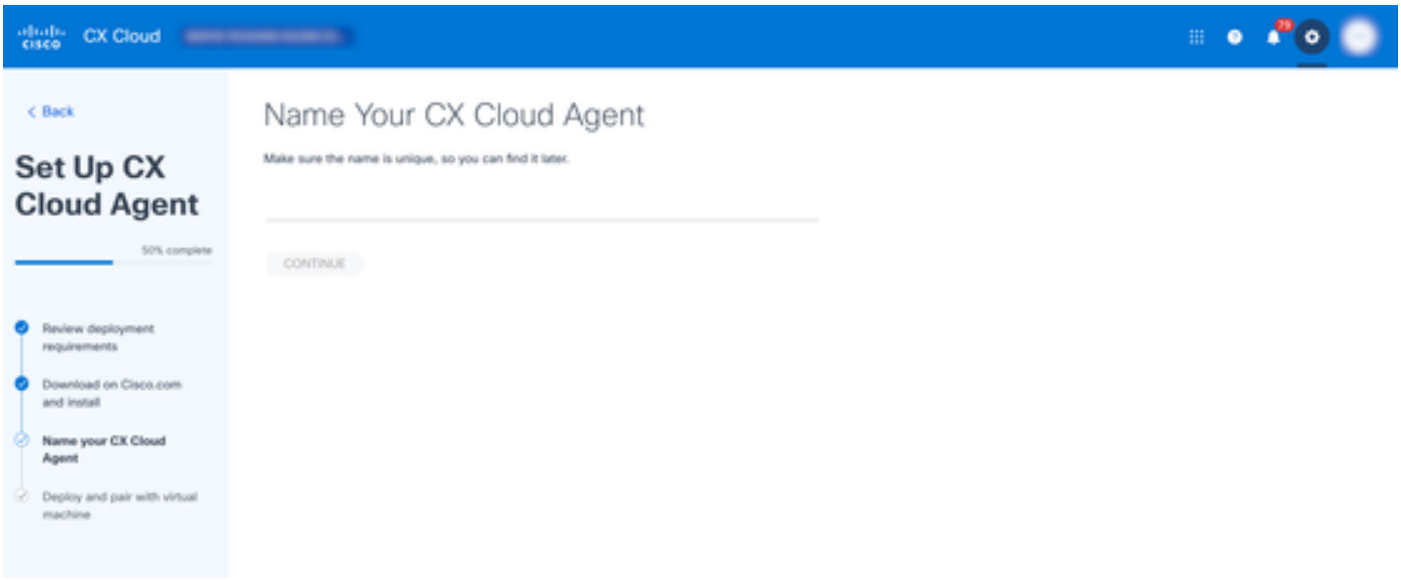
Aggiunta dell'agente CX

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. La finestra Software Download si apre in un'altra scheda.
7. Scaricare il file "CX Agent v3.1.0 OVA".

Nota: dopo la distribuzione del file "OVA" viene generato un codice di associazione necessario per completare l'installazione dell'agente CX.

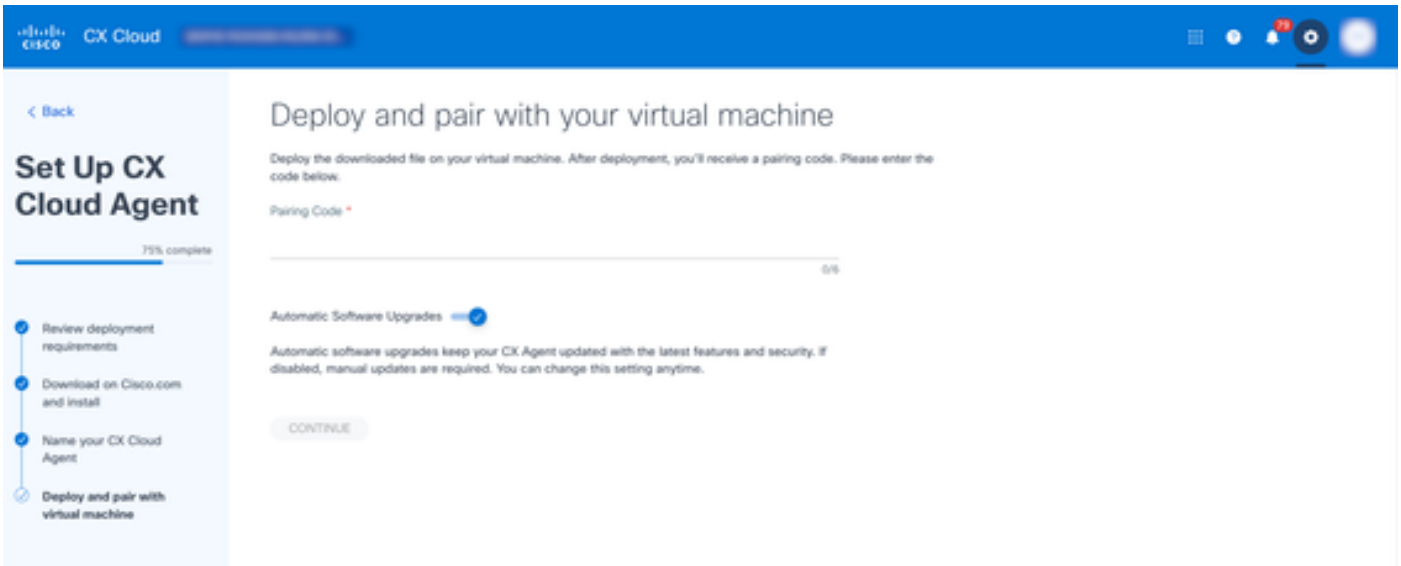
---

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



Agente CX nome

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



Codice di associazione

10. Inserire il codice di accoppiamento ricevuto dopo la distribuzione del file "OVA" scaricato.

11. Fare clic su Continua. Viene visualizzato lo stato della registrazione, seguito da un messaggio di conferma.

Nota: Ripetere i passaggi precedenti per aggiungere altre istanze dell'agente CX come origine dati.

Configurazione dell'agente CX per BCS/LCS

La nuova funzionalità Cisco Converged Collection semplifica la configurazione di CX Agent v3.1 per BCS/LCS, semplificando l'esperienza del cliente.

Nota:questa configurazione è specifica dei tecnici dell'assistenza Cisco responsabili della configurazione del collector per i clienti BCS/LCS.

I clienti BCS/LCS possono visitare la comunità cloud CX per ulteriori informazioni sul caricamento degli utenti e altre informazioni correlate.

Prerequisiti

I tecnici del supporto con accesso utente privilegiato (SUA) e amministratore possono eseguire solo la configurazione dell'agente CX per BCS/LCS.

Configurazione dell'agente CX

Per configurare CX Agent per BCS/LCS, contattare il supporto Cisco.

Configurazione delle funzionalità RADKit

CX Agent v3.1 fornisce una configurazione RADKit opzionale progettata per migliorare la gestione remota e la risoluzione dei problemi dei dispositivi Cisco in CX Cloud. Se abilitato, gli utenti autorizzati possono eseguire in modo sicuro operazioni quali l'acquisizione dei dati, la configurazione e gli aggiornamenti software in remoto. Queste impostazioni possono essere attivate o disattivate in qualsiasi momento in base alle esigenze operative del cliente.

Per dettagli completi su RADKit, fare riferimento a Cisco RADKit.

Integrazione del client RADKit tramite CLI

Per integrare il servizio client RADKit, creare un account amministratore e registrare il servizio completando i passaggi seguenti:

Nota: i passi riportati di seguito richiedono l'accesso root alla macchina virtuale dell'agente CX.

1. Aprire il terminale e Secure Shell (SSH) in una VM utilizzando le credenziali appropriate, ad esempio:

```
ssh your_username@your_vm_ip
```

2. Per abilitare la connettività di rete, eseguire il comando seguente:

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

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

3. Sul computer locale, inviare una richiesta POST all'endpoint di gestione per creare un

account amministratore. L'organismo di richiesta dovrebbe includere:

- admin_name (obbligatorio): Nome utente per l'account amministratore
- email (opzionale): Indirizzo di posta elettronica per l'account amministratore
- full_name (facoltativo): Nome completo dell'amministratore
- descrizione (facoltativa): Descrizione dell'account amministratore

Nell'esempio seguente viene illustrato come inviare la richiesta utilizzando cURL:

```
curl -X POST \

  http://<ip_vm_utente>:30100/radkitmanager/v1/createAdmin \

  -H "Tipo di contenuto: application/json" \

  -d '{

        "nome_amministratore": "admin_user123",

        "email": "admin@example.com"

        "nome_completo": "Utente amministratore",

        "descrizione": "Account amministratore per la gestione del
sistema"

      }'
```

Una volta creato un account amministratore, il server risponde con un messaggio di conferma che indica che l'account amministratore è stato creato correttamente. Questa risposta include anche una password temporanea che deve essere modificata al primo accesso. Tuttavia, se l'account amministratore esiste già, il server restituisce un codice di stato 400 con il messaggio "Admin already created" (Amministratore già creato).

4. Aprire il browser Web e passare all'interfaccia utente Web RADKit: https://<your_vm_ip>:30101/
5. Accedere utilizzando il nome utente dell'amministratore (admin_name) e la password temporanea fornita nella risposta.

 Nota: Al primo accesso, agli utenti viene richiesto di modificare la password. Seguire le istruzioni per impostare una nuova password.

---

6. Eseguire il client RADKit nel computer locale per registrare il servizio.
7. Dopo l'autenticazione, generare una password temporanea eseguendo il comando seguente:

```
grant_service_otp()
```

8. Sul computer locale, inviare una richiesta POST all'endpoint del manager per registrare il

servizio. L'organismo di richiesta dovrebbe includere:

- OTP (obbligatorio): Stringa della password monouso

Nell'esempio seguente viene illustrato come inviare la richiesta utilizzando cURL:

```
curl -X POST \

  http://<ip_vm_utente>:30100/radkitmanager/v1/enrollService \

  -H "Tipo di contenuto: application/json" \

  -d '{

        "one_time_password": "PROD:1234-1234-1234"

      }'
```

Una volta completata la registrazione, viene visualizzato un messaggio di conferma e gli utenti possono gestire il servizio RADKit utilizzando un account amministratore.

Per disabilitare la connettività di rete, eseguire il comando seguente:

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

Configurazione dell'insieme di credenziali per gli agenti CX esistenti

La funzionalità opzionale di configurazione Vault consente a CX Cloud di connettersi in modo sicuro a un servizio di vaulting per l'accesso a dati sensibili, quali token ed elenchi di inventario, utilizzando le credenziali più recenti. Se abilitato, CX Cloud utilizza automaticamente l'indirizzo e il token configurati. Questa impostazione può essere attivata o disattivata in qualsiasi momento. Al momento, è supportata solo la configurazione degli archivi di HashiCorp.

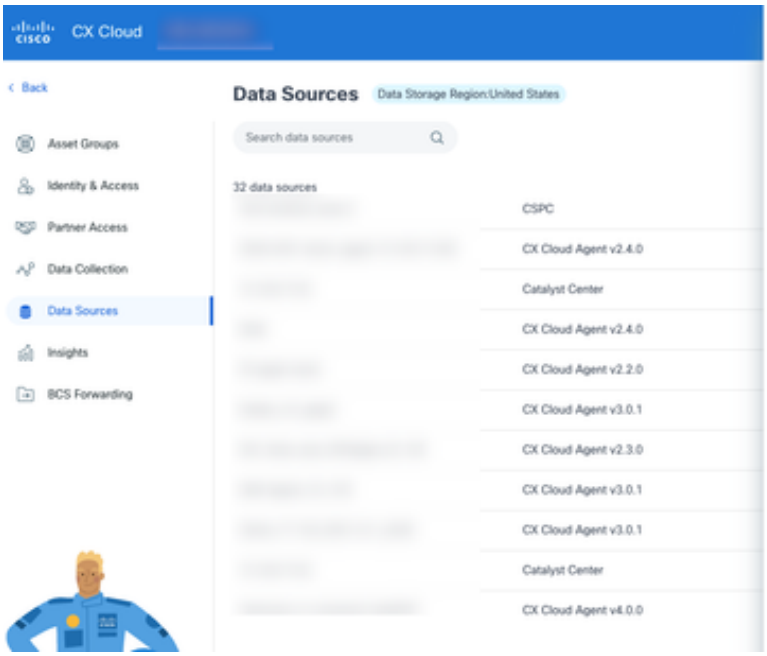
L'archivio può essere configurato in due modi:

- Anche se l'interfaccia utente di CX Cloud
- Tramite CLI

Configurazione di HashiCorp Vault nell'interfaccia utente di CX Cloud

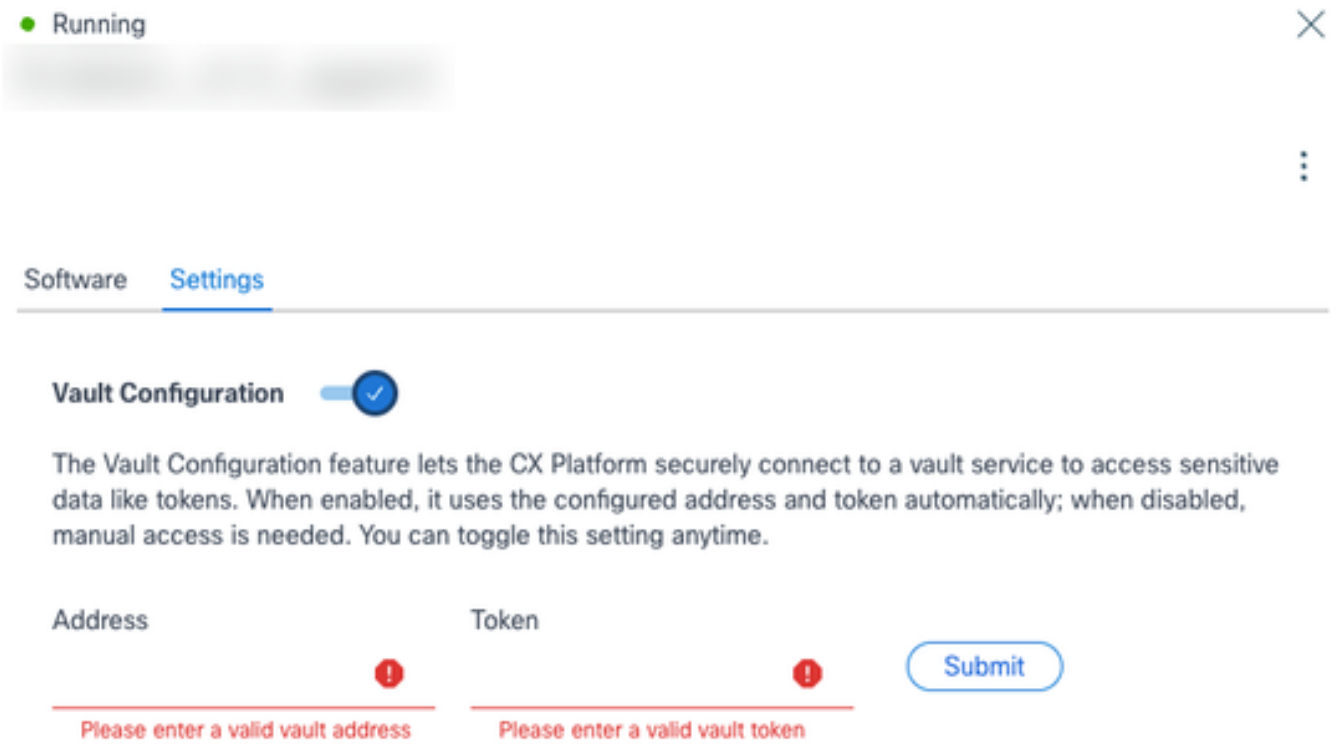
Per configurare l'archivio HashiCorp per un agente CX esistente:

1. Selezionare l'icona Admin Center. Verrà visualizzata la finestra Origini dati.
2. Fare clic sull'origine dati dell'agente CX. Viene visualizzata la finestra dei dettagli dell'agente CX.



Impostazioni

3. Fare clic sulla scheda Impostazioni.
4. Abilitare l'interruttore Configurazione archivi.



Configurazione archivi

5. Inserire i dettagli nei campi Indirizzo e Token.

6. Fare clic su Sottometti. Viene visualizzata una conferma e l'indirizzo IP aggiunto.

I clienti possono rimuovere l'archivio configurato facendo clic su Rimuovi.

Integrazione dell'agente CX con HashiCorp Vault tramite CLI

In questa sezione viene descritta la procedura per la configurazione della connessione tra l'agente Cisco CX e un'istanza di HashiCorp Vault. Questa integrazione consente l'archiviazione sicura e il recupero delle credenziali del dispositivo, migliorando la postura di sicurezza complessiva.

Prerequisiti

- accesso cxcroot alla VM dell'agente CX
- Un'istanza di archivio in esecuzione e accessibile

Integrazione con HashiCorp Vault

- Per abilitare l'integrazione degli archivi, eseguire il comando seguente:

```
cxcli agent vault attivato
```

- Per disabilitare l'integrazione degli archivi, eseguire il comando seguente:

```
cxcli agent vault disattivato
```

- Per controllare lo stato di integrazione dell'insieme di credenziali corrente, eseguire il comando seguente:

```
stato di cxcli agent vault
```

Abilitazione dell'integrazione di HashiCorp Vault

Per abilitare l'integrazione degli archivi:

1. Eseguire il login all'agente CX tramite SSH utilizzando l'account utente cxcroot per accedere all'agente CX.
2. Passare all'utente root per elevare i privilegi eseguendo il comando seguente:

```
sudo su
```

3. Eseguire il seguente comando per controllare lo stato di integrazione dell'insieme di credenziali corrente:

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

integrazione vault disabilitata

4. Eseguire il seguente comando per abilitare l'integrazione degli archivi:

```
cxcli agent vault attivato
```

5. Aggiornare i seguenti campi:

- Indirizzo archivio
- Token radice di archiviazione

6. Per verificare, controllare lo stato dell'integrazione con l'archivio. Il messaggio di risposta deve confermare che l'integrazione è abilitata:

```
root@cxcloudagent: /home/cxcroot# archivio agente cxcli attivato

Immettere l'indirizzo dell'insieme di credenziali HashiCorp:

Immettere il token dell'insieme di credenziali HashiCorp:

integrazione con vault abilitata root@cxcloudagent: /home/cxcroot#
```

Disattivazione integrazione vaulting HashiCorp

Per accedere all'agente CX:

1. Accedere all'agente CX tramite SSH utilizzando l'account utente cxcroot.
2. Passare all'utente root per elevare i privilegi eseguendo il comando seguente:

```
sudo su
```

3. Eseguire il seguente comando per disabilitare l'integrazione dell'insieme di credenziali HashiCorp:

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

integrazione vault disabilitata

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

Hashi Corp Schema credenziali dispositivo di insieme di credenziali

Schema credenziali insieme di credenziali: Per informazioni dettagliate sulle opzioni disponibili e sui campi supportati per le credenziali del dispositivo, scaricare il file dello schema delle credenziali (vault-credentials-schema.json).

Esempio: Di seguito è riportato un esempio di credenziale JSON basata sullo schema:

-

```
{
"targetIp": "5.0.1.*",
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
```

```
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
"password": "*******",
"enableUser": "cisco",
"enablePassword": "*******"
}
}
}
```

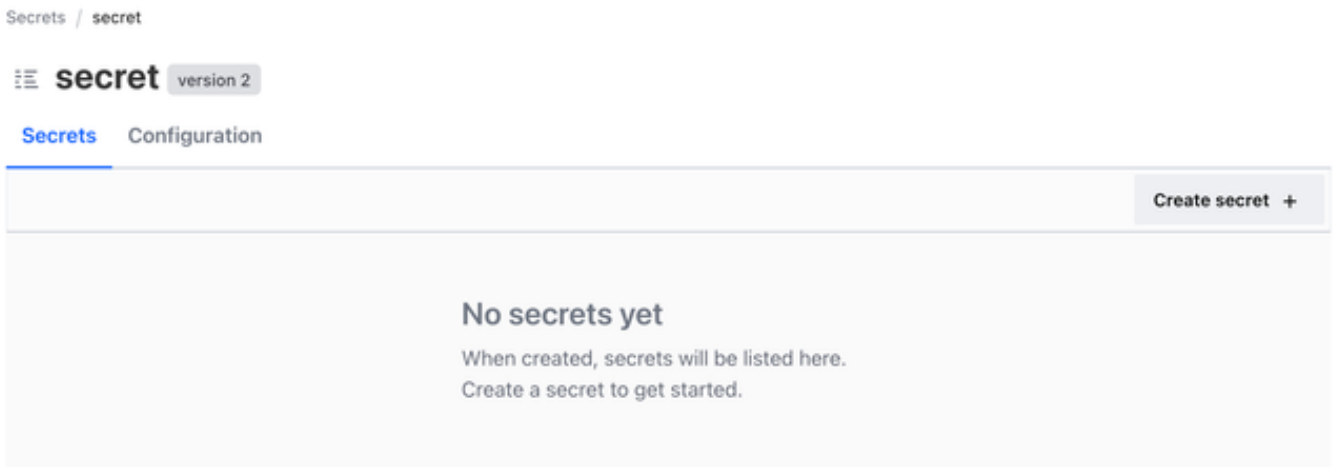
Nota:gli utenti possono specificare più protocolli all'interno di un singolo file JSON delle credenziali. Tuttavia, evitare di includere protocolli duplicati della stessa famiglia (ad esempio, non includere sia SNMPv2c che SNMPv3 nello stesso file di credenziali).

Configurazione delle credenziali del dispositivo nell'insieme di credenziali HashiCorp (prima volta)

1. Accedere a un'istanza di Vault.

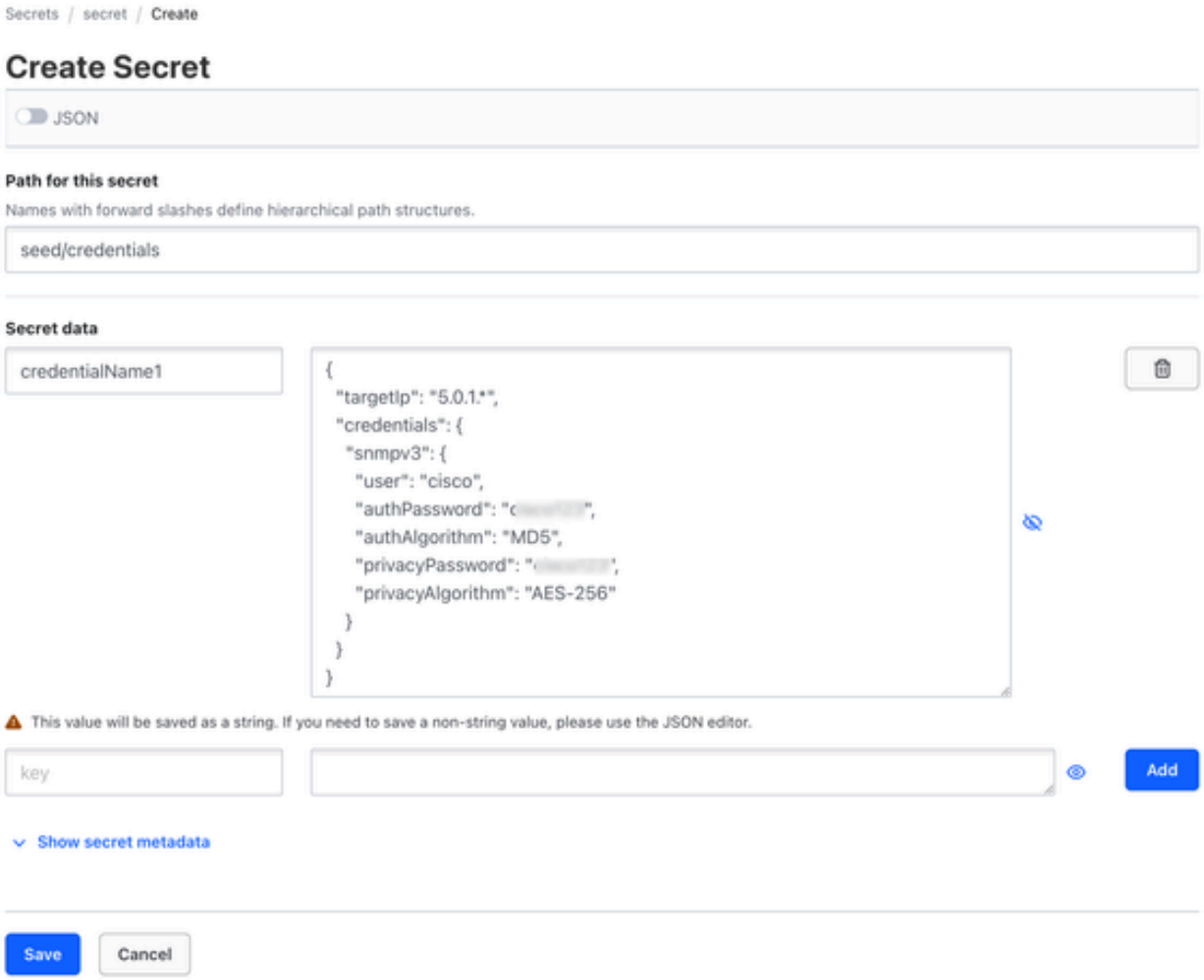
Secret

2. Creare un nuovo segreto chiave-valore utilizzando il percorso seguente: segreto/velocità/credenziali.
3. Scegliere il motore di archiviazione segreta chiave-valore (segreto/).



Segreto valore chiave

4. Fare clic su Crea segreto. Verrà visualizzata la finestra Crea segreto.



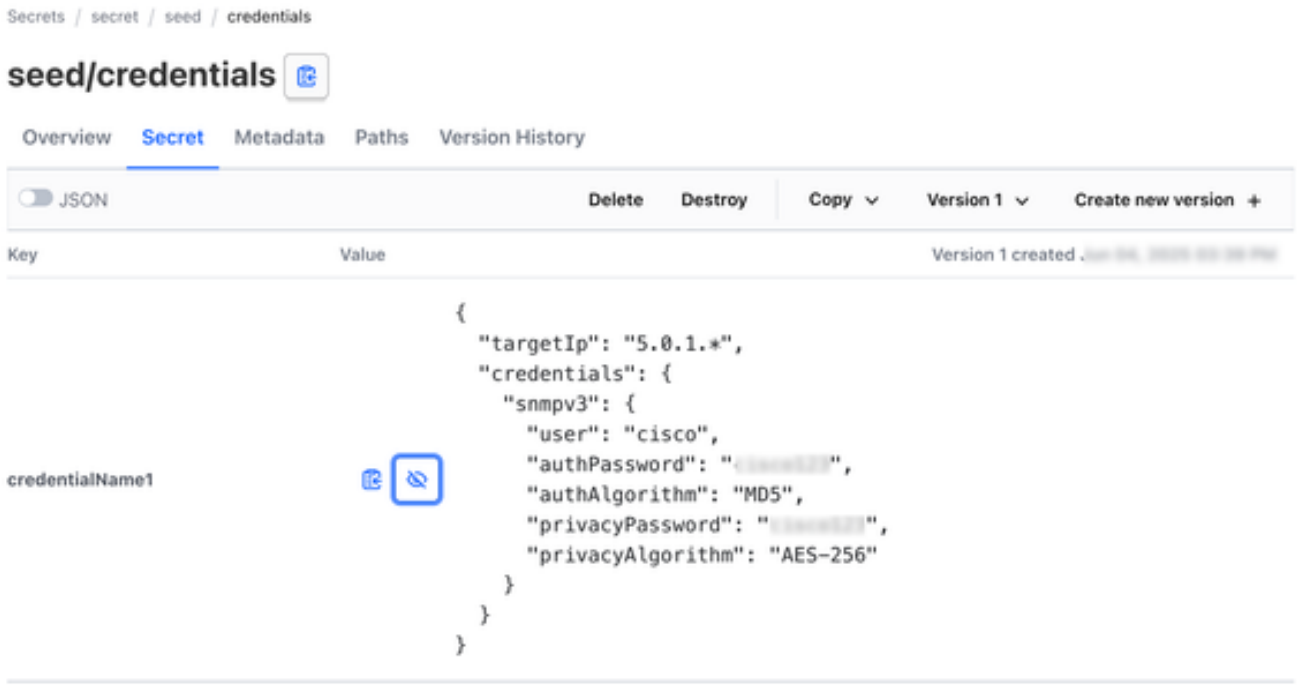
Segreto client

5. Aggiornare i seguenti campi:

- Percorso segreto: valore di inizializzazione/credenziali
- Dati segreti: raccolta di chiavi - segreti dei valori

- chiave: nome credenziali univoche personalizzate
- valore: JSON credenziali

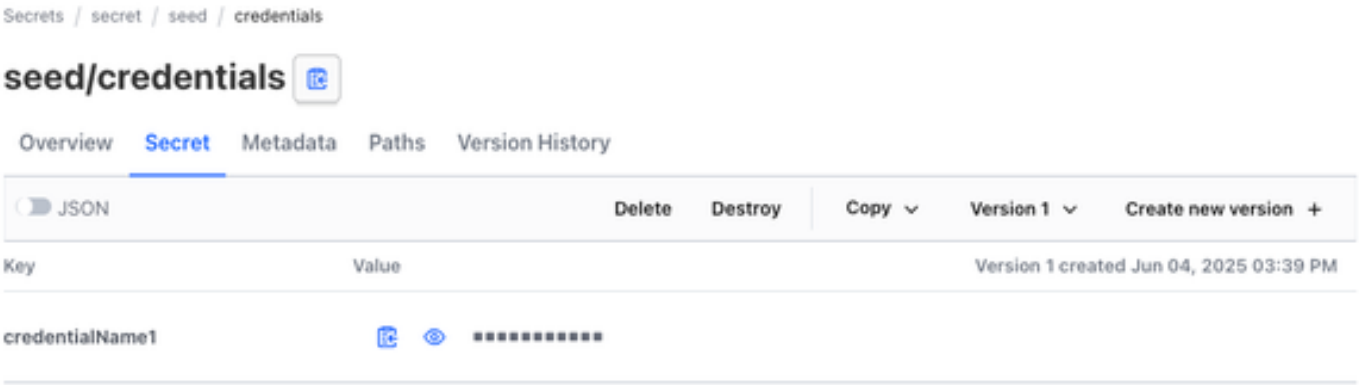
6. Fare clic su Salva. Il segreto dovrebbe essere ora archiviato nell'insieme di credenziali HashiCorp.



Credenziali

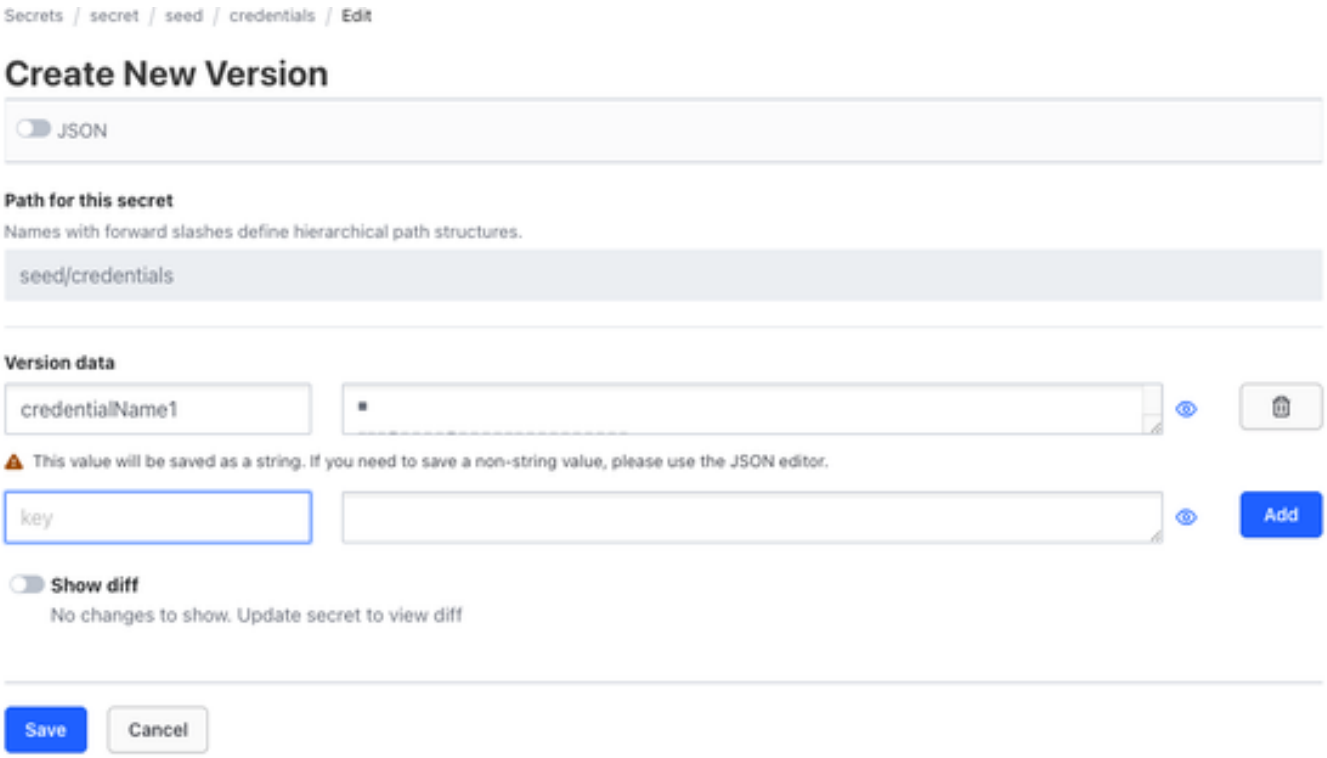
Aggiunta di altre credenziali all'insieme di credenziali HashiCorp

1. Accedere a un'istanza dell'insieme di credenziali HashiCorp.



Aggiungi credenziali

2. Passare al segreto "segreto/velocità/credenziali" già creato.



Crea versione

3. Fare clic su Crea nuova versione.

4. Aggiungere nuovi segreti fornendo un numero qualsiasi di coppie chiave-valore in base alle esigenze.

5. Fare clic su Salva.

File di inizializzazione del cloud CX con credenziali predefinite

- Semplificazione del file di inizializzazione: Se si utilizzano credenziali configurate tramite l'archivio Hashicorp, semplificare il file di inizializzazione omettendo le informazioni riservate
- Specificare solo l'indirizzo IP o il nome host: Gli utenti possono passare solo l'indirizzo IP o il nome host nel file di inizializzazione, lasciando vuoti gli altri campi

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

IP o nome host

- Utilizzare l'archivio HashiCorp e le credenziali del file di inizializzazione: Fornire le credenziali per alcuni dispositivi nel file di inizializzazione utilizzando l'insieme di credenziali per gestire le credenziali per altri dispositivi

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

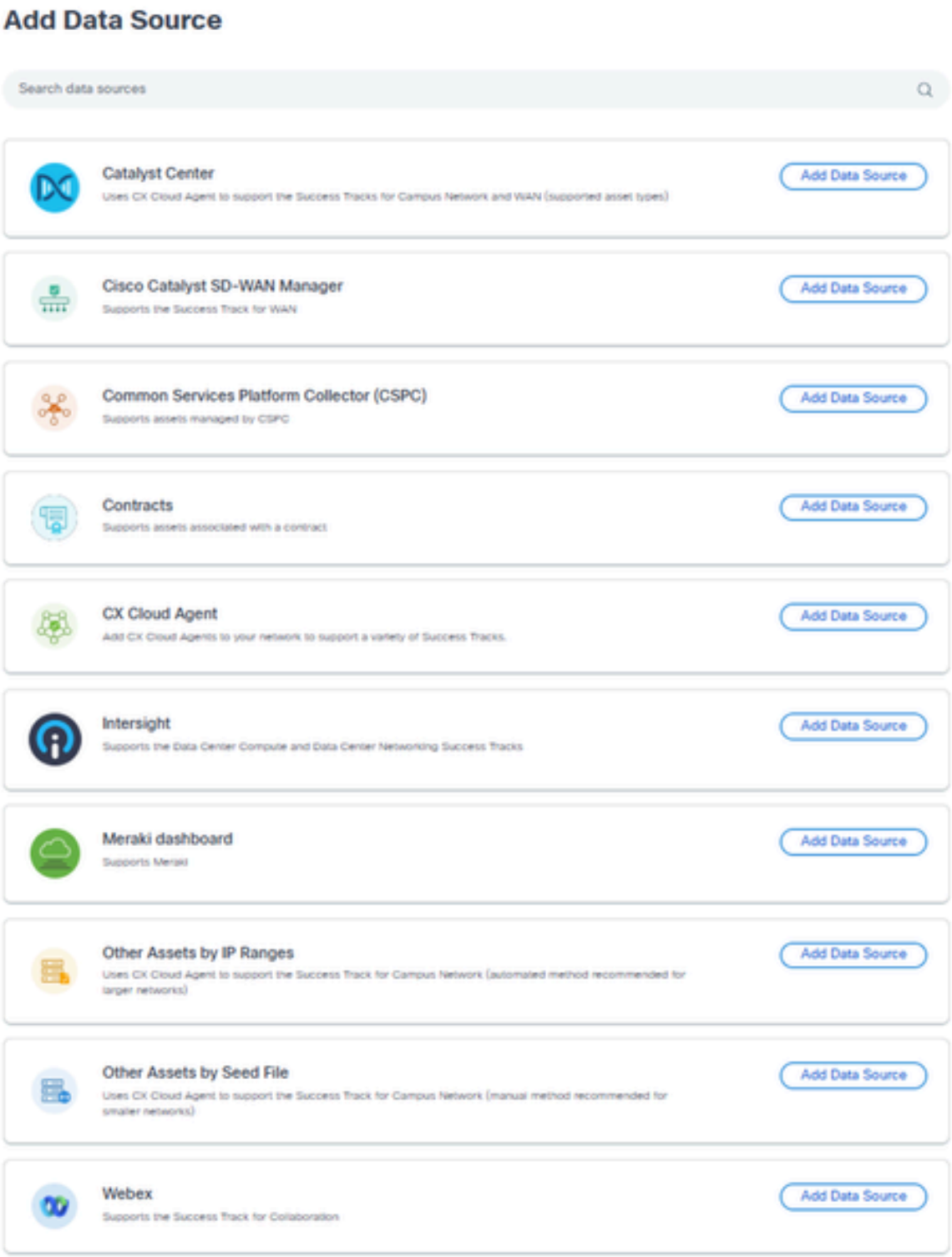
IP o nome host

Aggiunta di Catalyst Center come origine dati

Gli utenti con il ruolo di amministratore privilegiato possono aggiungere l'origine dati Catalyst Center.

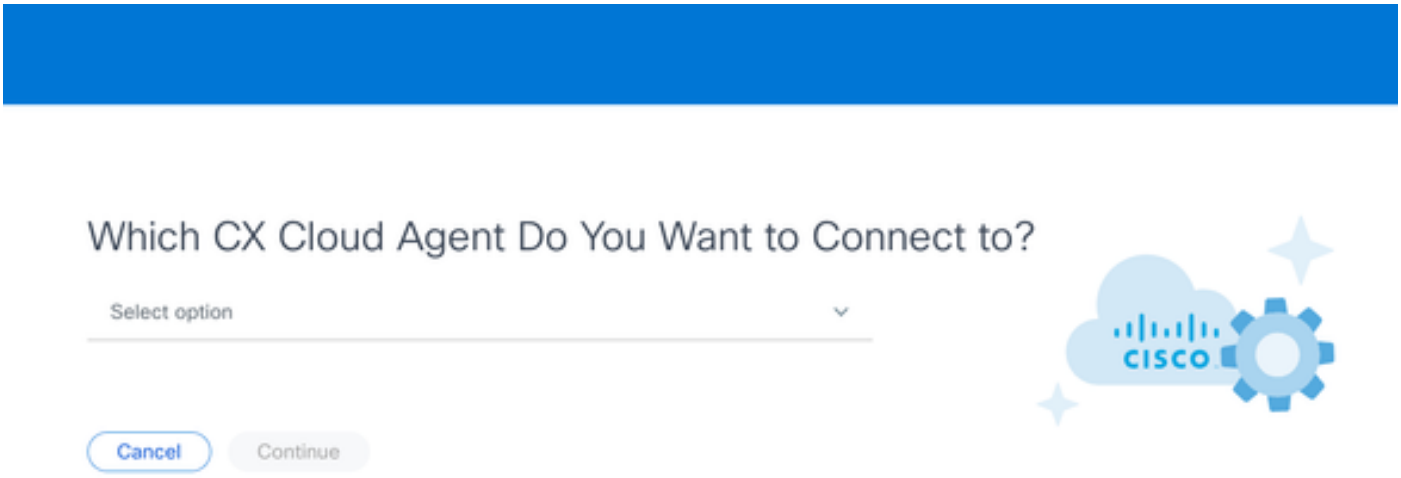
Per aggiungere Catalyst Center come origine dati:

1. Selezionare l'icona Admin Center. Verrà visualizzata la finestra Origini dati.
2. Fare clic su Aggiungi origine dati. Verrà visualizzata la pagina Aggiungi origine dati.



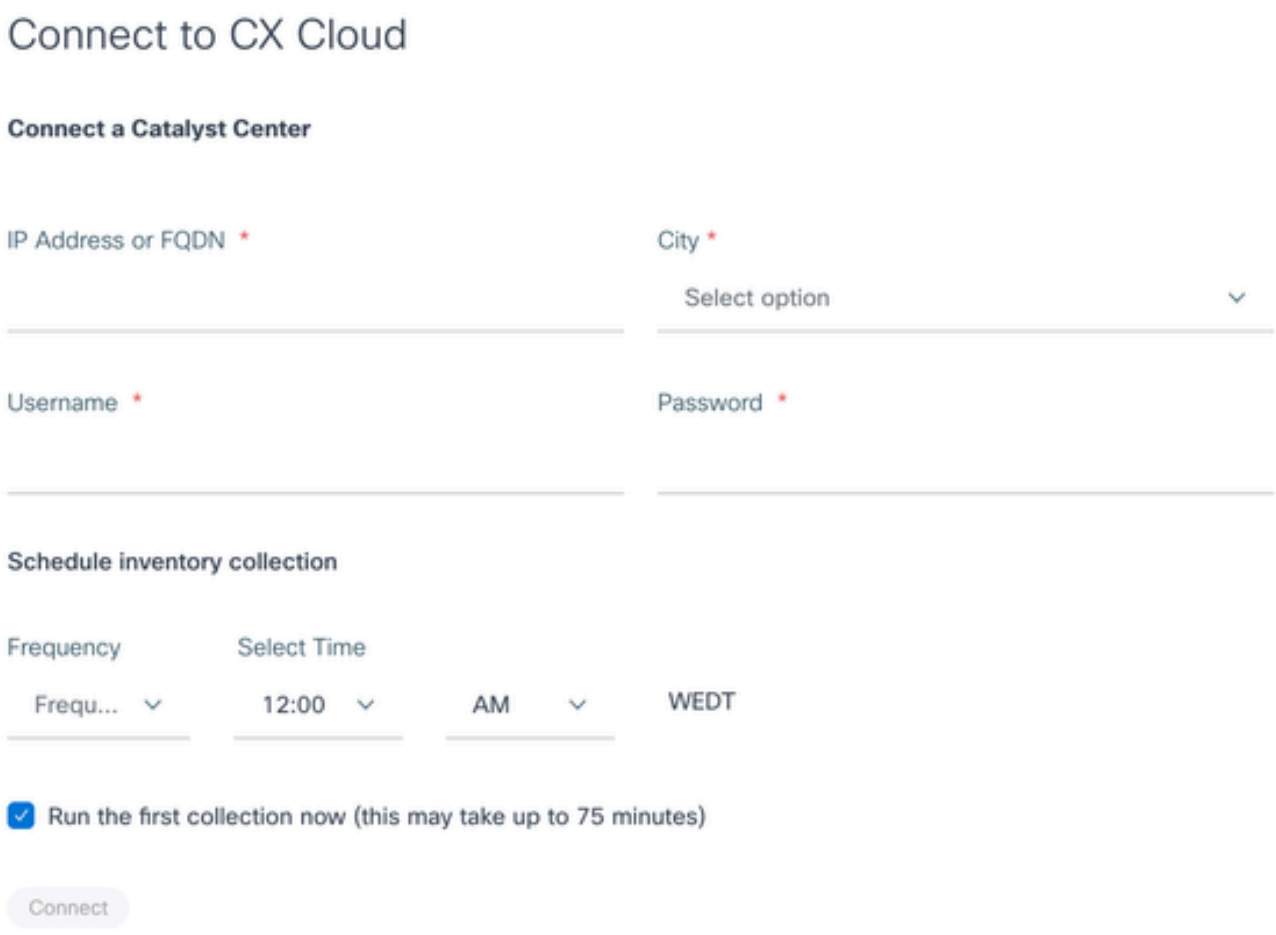
Aggiungi origine dati

3. Fare clic su Aggiungi origine dati dall'opzione Catalyst Center.



Seleziona agente CX

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



Frequenza

6. Immettere i seguenti dettagli:

- Indirizzo IP virtuale o FQDN (ad esempio, indirizzo IP del Catalyst Center)
- Città (ad esempio, ubicazione del Catalyst Center)
- Username
- Password
- Frequenza e Selezionare Tempo per indicare la frequenza con cui l'agente CX deve eseguire le scansioni di rete nelle sezioni Pianifica raccolta inventario

Nota: Selezionare la casella di controllo Esegui la prima raccolta adesso per eseguire la raccolta adesso.

7. Fare clic su Connetti. Viene visualizzata una conferma con l'indirizzo IP del Catalyst Center.

Aggiunta di SolarWinds® come origine dati

Nota: Se è necessario aggiungere l'origine dati SolarWinds®, contattare il supporto Cisco per assistenza.

I clienti BCS/LCS possono ora utilizzare la funzionalità di CX Agent per l'integrazione esterna con SolarWinds®, fornendo maggiore trasparenza, gestibilità migliorata e una migliore esperienza utente grazie a una maggiore automazione. L'agente CX raccoglie l'inventario e altri dati necessari per generare diversi report coerenti in termini di formato, completezza dei dati e accuratezza dei dati per i report correnti generati da Operational Insights Collector. L'agente CX supporta l'integrazione con SolarWinds® consentendo a un cliente BCS/LCS di sostituire OIC con l'agente CX per la raccolta dei dati da Solarwinds®. Questa funzione, inclusa la sorgente dati Solarwinds®, è disponibile esclusivamente per i clienti BCS/LCS.

L'agente CX deve essere configurato in Inoltro BCS prima della prima raccolta. in caso contrario, i file non vengono elaborati. Per ulteriori informazioni sulla configurazione dell'inoltro BCS, consultare la sezione Configurazione dell'agente CX per BCS o LCS.

Note:

- Più raccolte dalla stessa istanza SolarWinds® sovrascrivono i file precedenti (i caricamenti successivi hanno la precedenza)
- Sono supportate più origini, ma ogni istanza di SolarWinds® deve avere un ID IP e un ID accessorio univoci

Aggiunta di altri cespiti come origini dati

La raccolta di dati di telemetria è stata estesa ai dispositivi non gestiti dal Catalyst Center, consentendo agli utenti di visualizzare e interagire con dati di analisi e informazioni derivate dalla telemetria per una gamma più ampia di dispositivi. Dopo la configurazione iniziale dell'agente CX, gli utenti hanno la possibilità di configurare l'agente CX per la connessione a 20 ulteriori Catalyst 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 deve essere analizzato da CX Agent. Entrambi gli approcci si basano sul protocollo SNMP (Simple Network Management Protocol) per il rilevamento e su SSH (Secure Shell) per la connettività. Questi devono essere configurati correttamente per abilitare la raccolta di telemetria.

Per aggiungere altre risorse come origini dati, utilizzare una delle opzioni seguenti:

- Caricare un file di inizializzazione utilizzando un modello di file di inizializzazione
- 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 CX supporta SNMPv2c e SNMPv3 ed è possibile configurare una o entrambe le versioni. Le stesse informazioni, descritte di seguito in modo dettagliato, 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 SNMPv3 su tutte le reti pubbliche e su Internet per proteggere il sistema da rischi e minacce alla sicurezza. In CX Cloud, è preferibile configurare SNMPv3 e non SNMPv2c, ad eccezione dei dispositivi legacy meno recenti che non dispongono del supporto incorporato per SNMPv3. Se entrambe le versioni di SNMP sono configurate dall'utente, l'agente CX tenta, per impostazione predefinita, di comunicare con ciascun dispositivo utilizzando SNMPv3 e ritorna a SNMPv2c se la comunicazione non può essere negoziata correttamente.

Protocolli di connettività

Nell'ambito dell'impostazione della connettività diretta del dispositivo, gli utenti devono specificare i dettagli del protocollo di connettività del dispositivo: SSH (o in alternativa Telnet). Si consiglia di utilizzare SSHv2, ad eccezione dei casi in cui le singole risorse legacy 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 risorse sottostanti possono essere compromessi a causa di queste vulnerabilità quando si fa affidamento su SSHv1. Anche Telnet non è sicuro. Le informazioni sulle credenziali (ad esempio nomi utente e password) inviate tramite telnet non vengono crittografate e pertanto possono essere compromesse se non si garantisce una protezione aggiuntiva.

Limitazioni all'elaborazione della telemetria 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.
- Se anche un dispositivo delle raccolte di intervalli IP o di file di inizializzazione fa parte dell'inventario di Catalyst Center, il dispositivo viene segnalato solo una volta per la voce Catalyst Center. I rispettivi dispositivi all'interno del file di origine o della voce dell'intervallo IP vengono ignorati per evitare la duplicazione.
- I telefoni IP Cisco non sono supportati in CX Cloud per la raccolta dei dati da parte dell'agente CX. Di conseguenza, i telefoni IP Cisco non vengono visualizzati nell'elenco delle risorse.

Aggiunta di altri cespiti mediante un file di inizializzazione

Un file di inizializzazione 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 deve essere raccolta dall'agente 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 CX tenterà di connettersi ai dispositivi, ma potrebbe non essere in grado di elaborarli singolarmente per visualizzarli nelle pagine Asset nei casi in cui non sia 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.

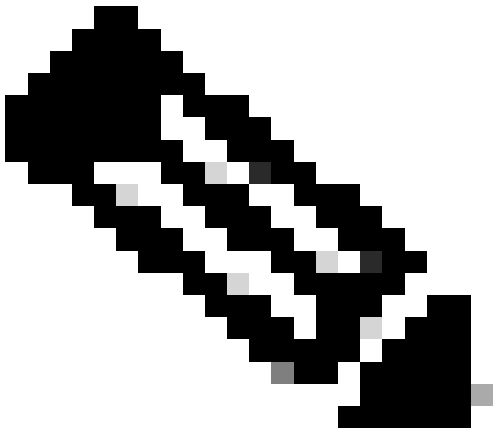
Gli utenti possono caricare un file di inizializzazione CSPC (Common Services Platform Collector) come un file di inizializzazione standard del cloud CX e qualsiasi riformattazione necessaria viene gestita nel cloud CX.

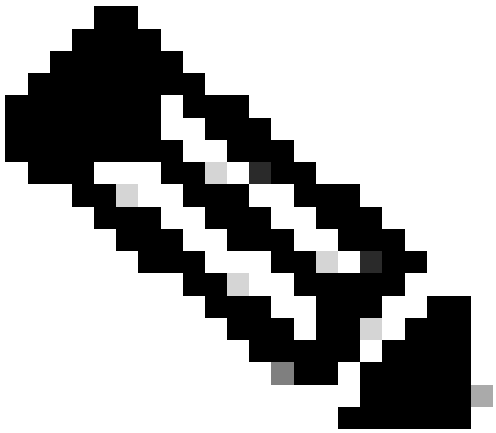
Per CX Agent v3.1 e versioni successive, i clienti possono caricare i file di inizializzazione in formato CSPC o CX; per le versioni precedenti dell'agente CX è supportato solo il file di inizializzazione in formato CX.

È importante che il formato del file di inizializzazione di esempio, incluse le intestazioni di colonna, non venga alterato in alcun modo.

Nella tabella seguente vengono identificate tutte le colonne del file di partenza necessarie 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

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
		valido e univoco per il dispositivo.
B	Versione protocollo SNMP	Il protocollo SNMP è richiesto dall'agente CX e viene utilizzato per il rilevamento dei dispositivi nella 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 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	snmpv3NomeUtente: Obbligatorio se col#=3 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 Message Digest (MD5) o Secure Hash Algorithm (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.  Nota: Le chiavi a 56 bit utilizzate da DES (Data Encryption Standard) sono considerate troppo brevi per garantire la sicurezza crittografica e lo standard 3DES (Triple Data Encryption Standard) 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

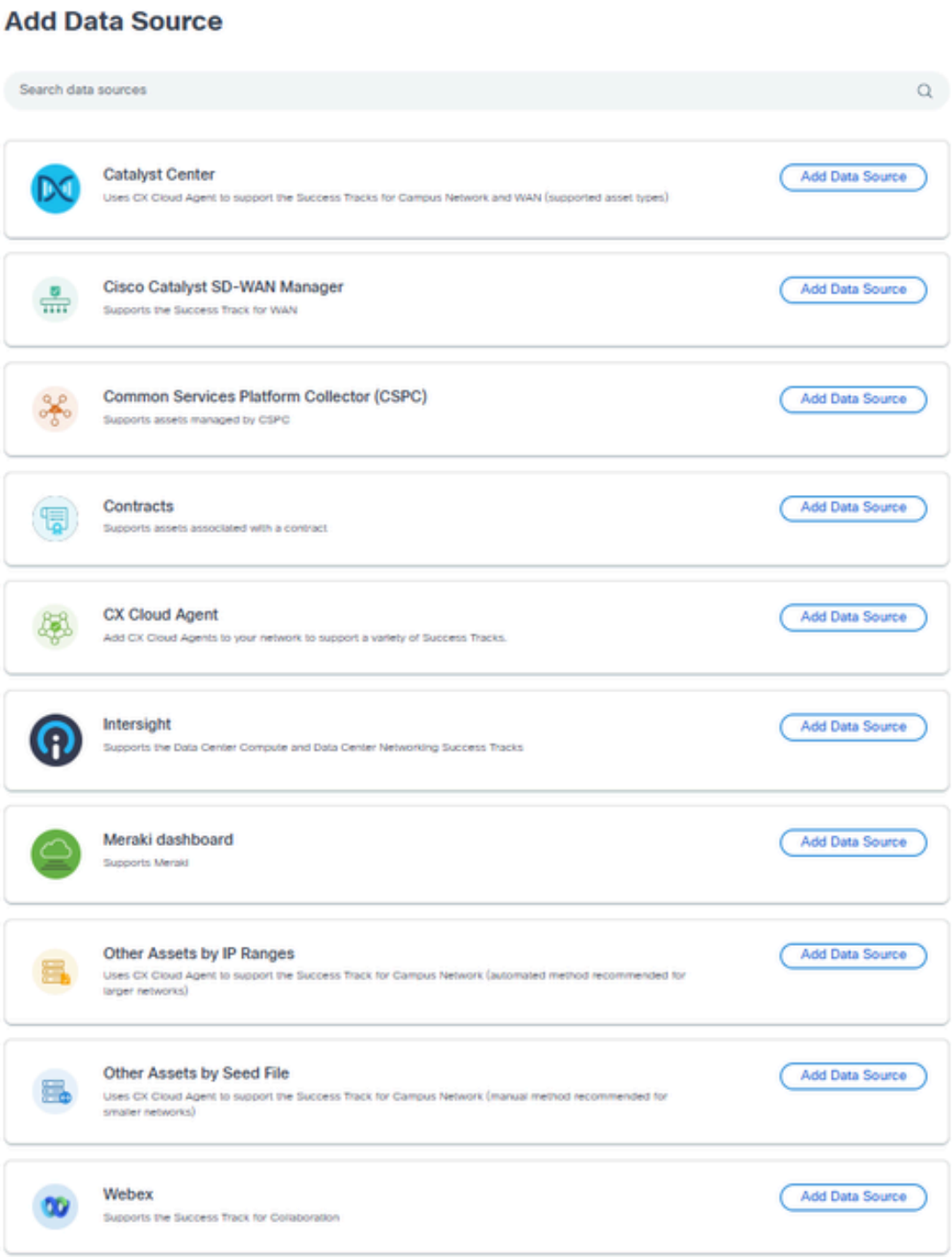
Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
		per la connessione al dispositivo.
I	snmpv3EngineId: engineID, ID univoco che rappresenta il dispositivo, specifica l'ID del motore se configurato manualmente sul dispositivo	L'ID motore SNMPv3 è un ID univoco che rappresenta ciascun dispositivo. Questo ID motore viene inviato come riferimento durante la raccolta dei dataset SNMP da parte dell'agente CX. Se il cliente configura il EngineID manualmente, è necessario fornire il relativo EngineID.
J	Protocollo cli: i valori possono essere 'telnet', 'sshv1', 'sshv2'. Se vuoto, è possibile impostare 'sshv2' per impostazione predefinita	L'interfaccia della riga di comando (CLI) è progettata per interagire direttamente con il dispositivo. L'agente CX utilizza questo protocollo per la raccolta della 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 di per sé non forniscono 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 utente/password CLI o ENTRAMBI, MA entrambe le colonne (col#=12 e col#=13) non possono essere vuote.)	È necessario fornire il nome utente CLI corrispondente del dispositivo. Viene utilizzato dall'agente cloud CX al momento della connessione al dispositivo durante la raccolta CLI.
M	Password cli: Password utente CLI (è possibile specificare nome utente/password CLI o ENTRAMBI, MA le colonne (col#=12 e col#=13) non	È necessario fornire la password CLI corrispondente del dispositivo. Viene utilizzato dall'agente CX al momento della connessione al dispositivo durante la raccolta dalla CLI.

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
	possono essere vuote.)	
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

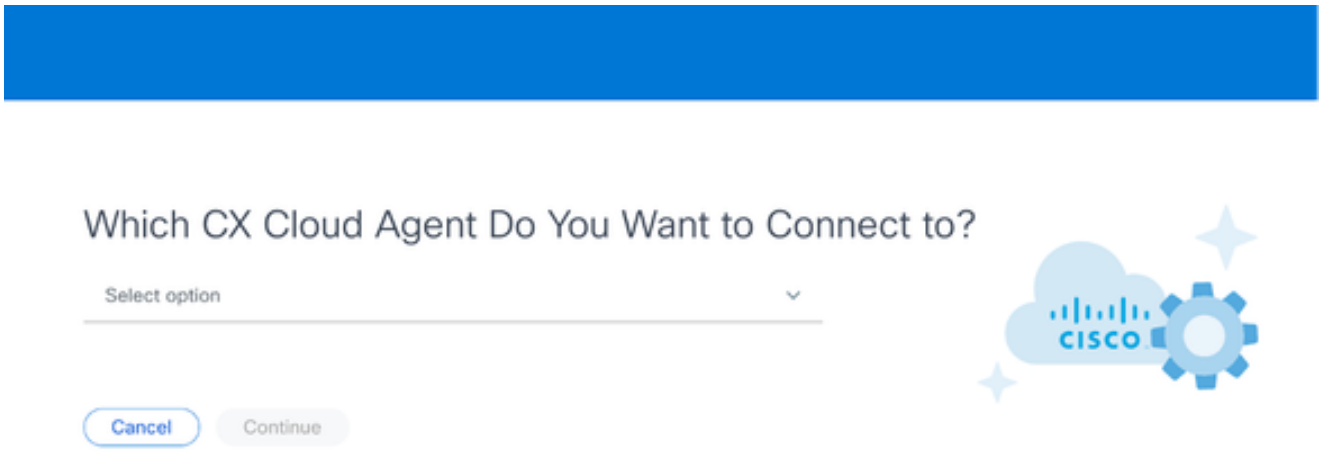
Per aggiungere altri asset utilizzando un nuovo file di inizializzazione:

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



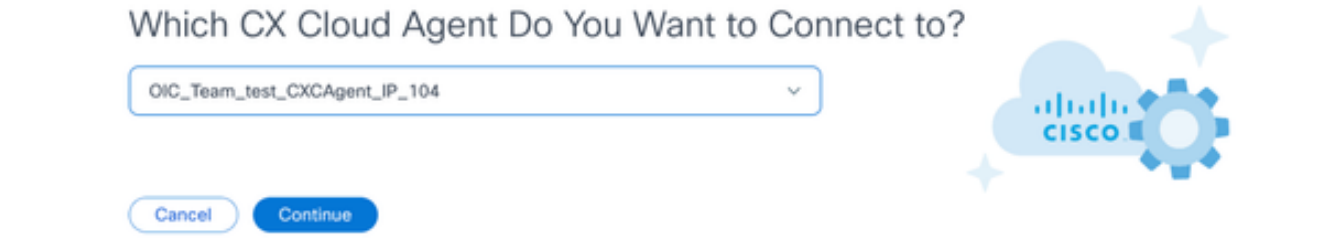
Aggiungi origine dati

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



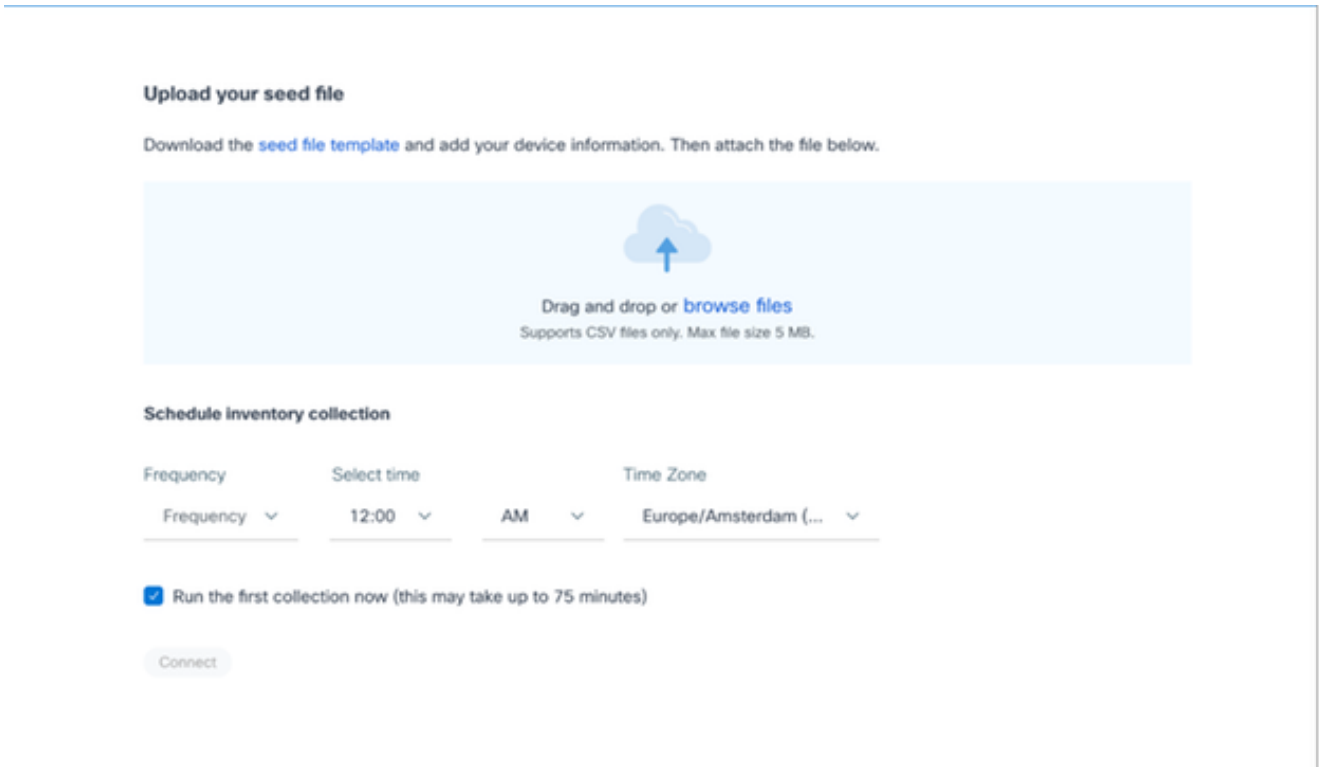
Seleziona agente CX

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



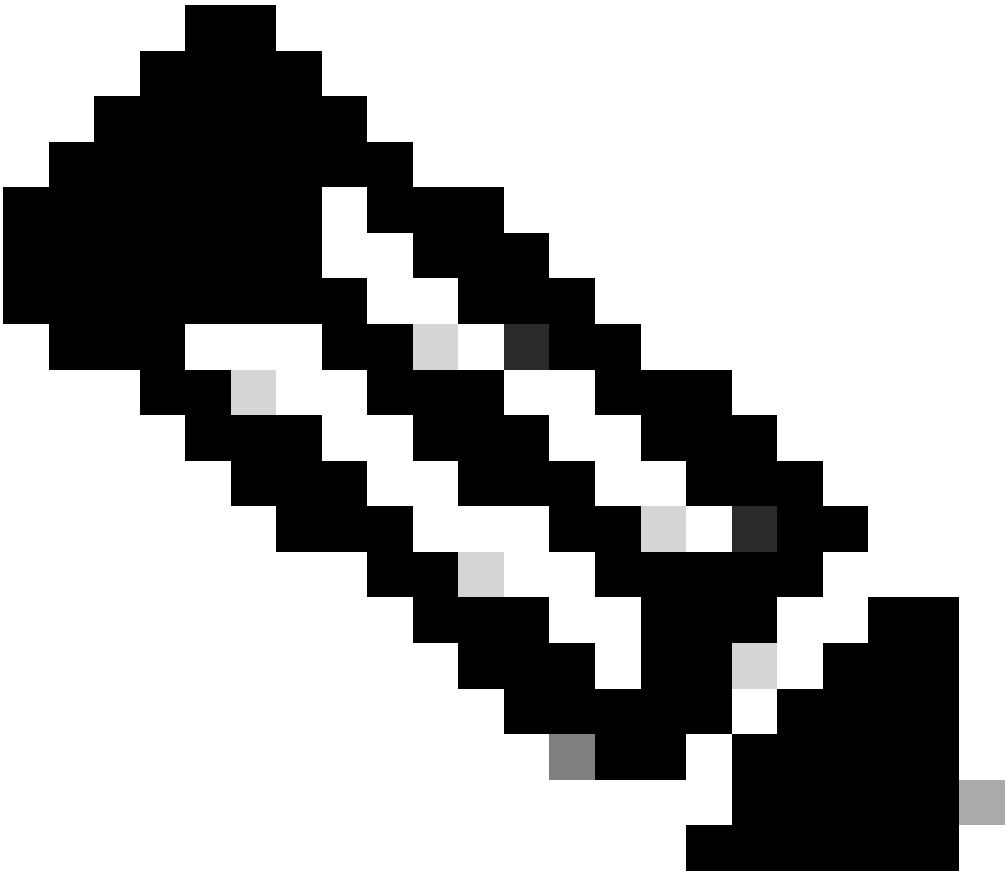
Continua

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 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 di CX Cloud 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.

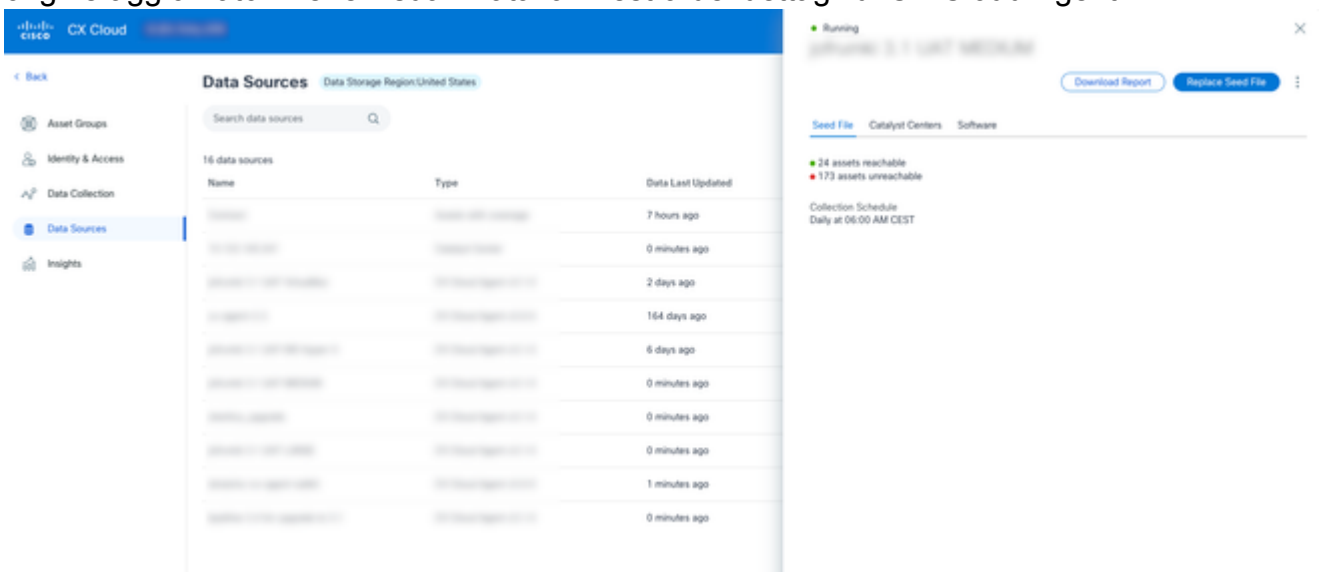
Aggiunta di altri cespiti mediante un file di partenza modificato

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

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

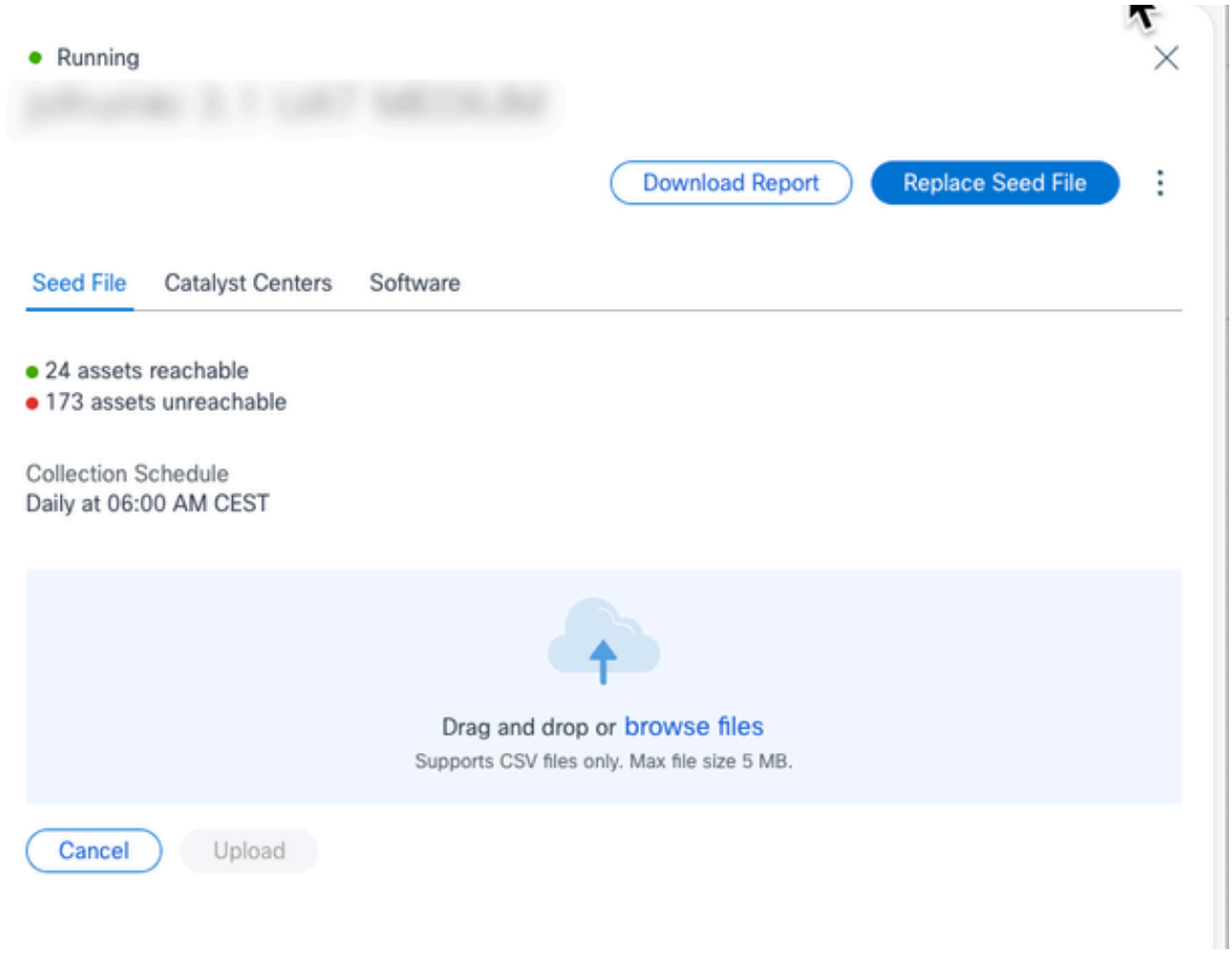
Nota: Per aggiungere risorse al file di origine, aggiungetele al file di origine creato in precedenza e ricaricate il file. Questa operazione è necessaria in quanto il caricamento di un nuovo file di inizializzazione sostituisce il file di inizializzazione corrente. Per l'individuazione e la raccolta viene utilizzato solo l'ultimo file di inizializzazione caricato.

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



File di inizializzazione

3. Fare clic su Sostituisci file di inizializzazione.



Sostituisci file di inizializzazione

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

Credenziali predefinite per il file di inizializzazione

L'agente CX fornisce credenziali predefinite che i clienti possono impostare localmente nell'agente, eliminando la necessità di includere password riservate direttamente nel file di inizializzazione. Ciò migliora la sicurezza riducendo l'esposizione di informazioni riservate, risolvendo un problema chiave per il cliente.

Aggiunta di altre risorse mediante 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 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 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 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 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 si aggiunge o si elimina un nuovo dispositivo (all'interno o all'esterno) a un determinato intervallo IP, il cliente deve sempre fare clic su Modifica intervallo indirizzi IP (vedere la 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 di raccolta dell'agente CX.

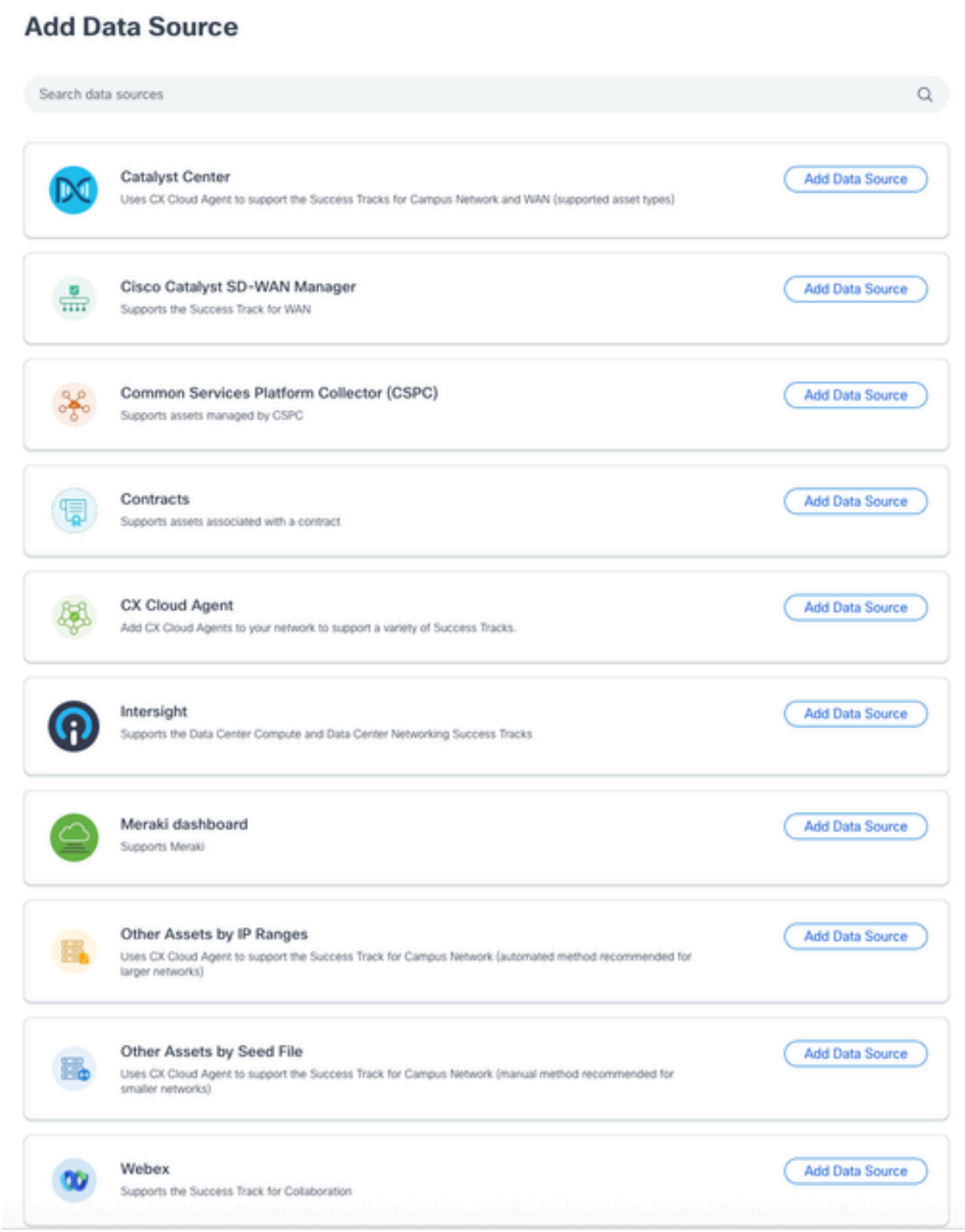
L'aggiunta di dispositivi tramite un intervallo IP richiede che gli utenti specifichino tutte le credenziali applicabili tramite l'interfaccia utente di configurazione. I campi visibili variano a seconda dei protocolli selezionati nelle finestre precedenti. Se si selezionano più protocolli per lo stesso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

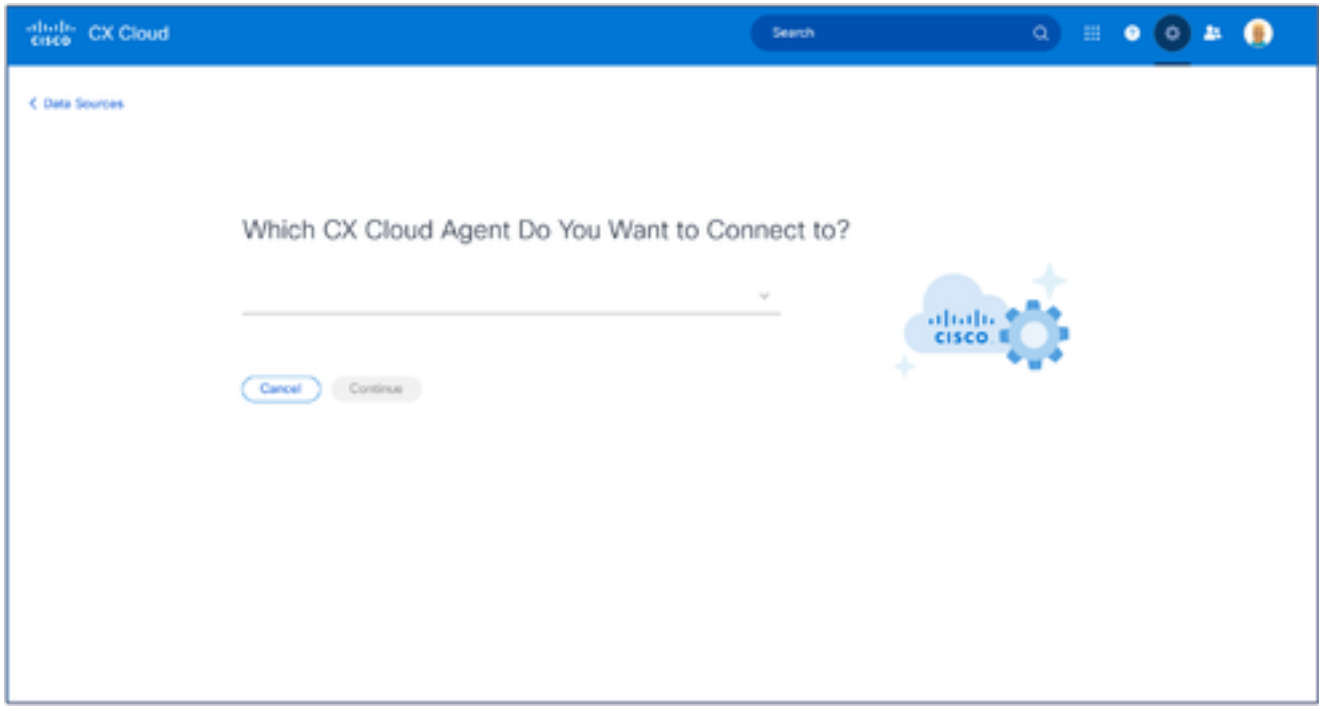
Per aggiungere dispositivi utilizzando l'intervallo IP:

1. Selezionare l'icona Admin Center. Viene visualizzata la finestra Origini dati.
2. Fare clic su Aggiungi origine dati nella finestra Admin Center > Origini dati.



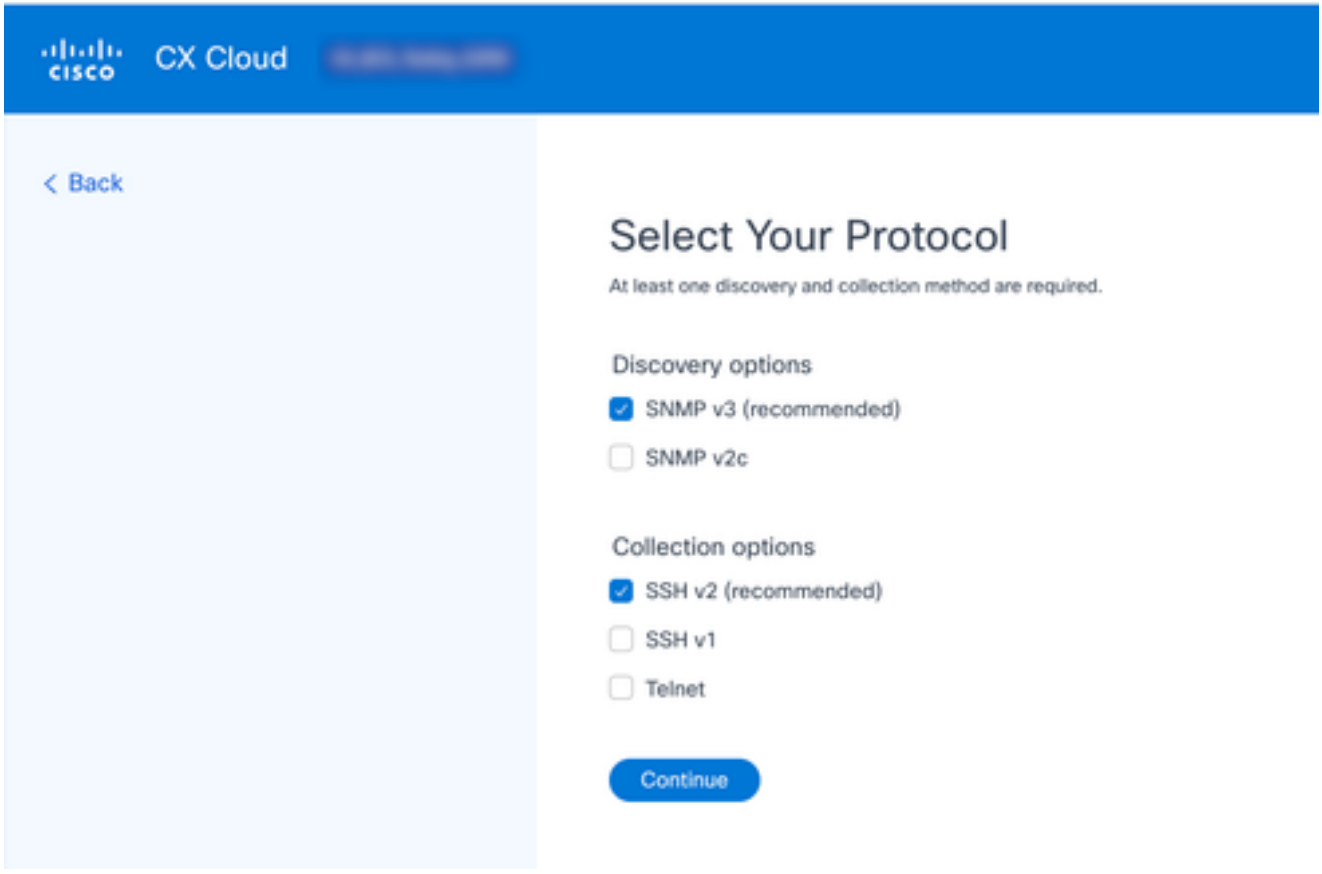
Aggiungi origine dati

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



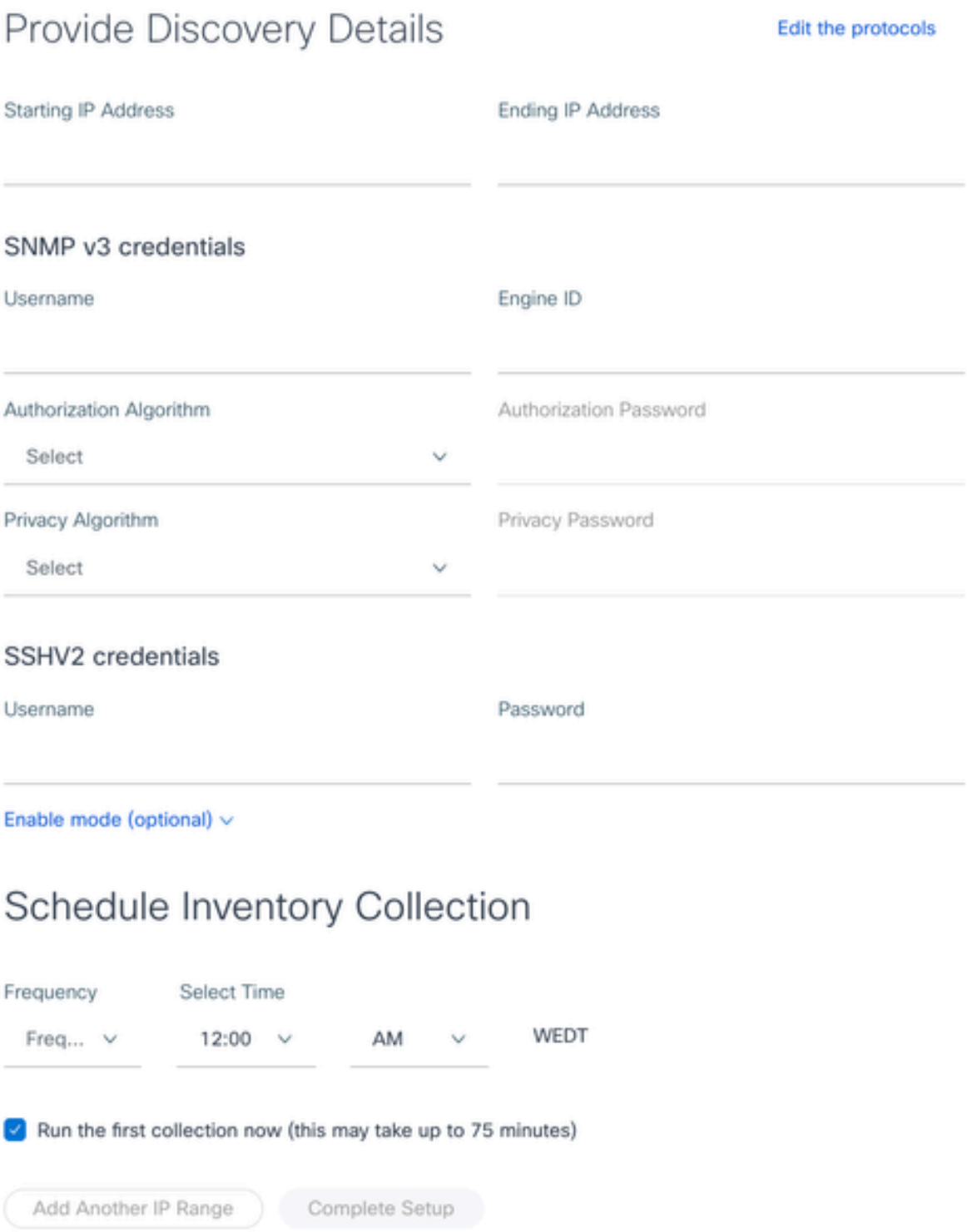
Seleziona agente cloud CX

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



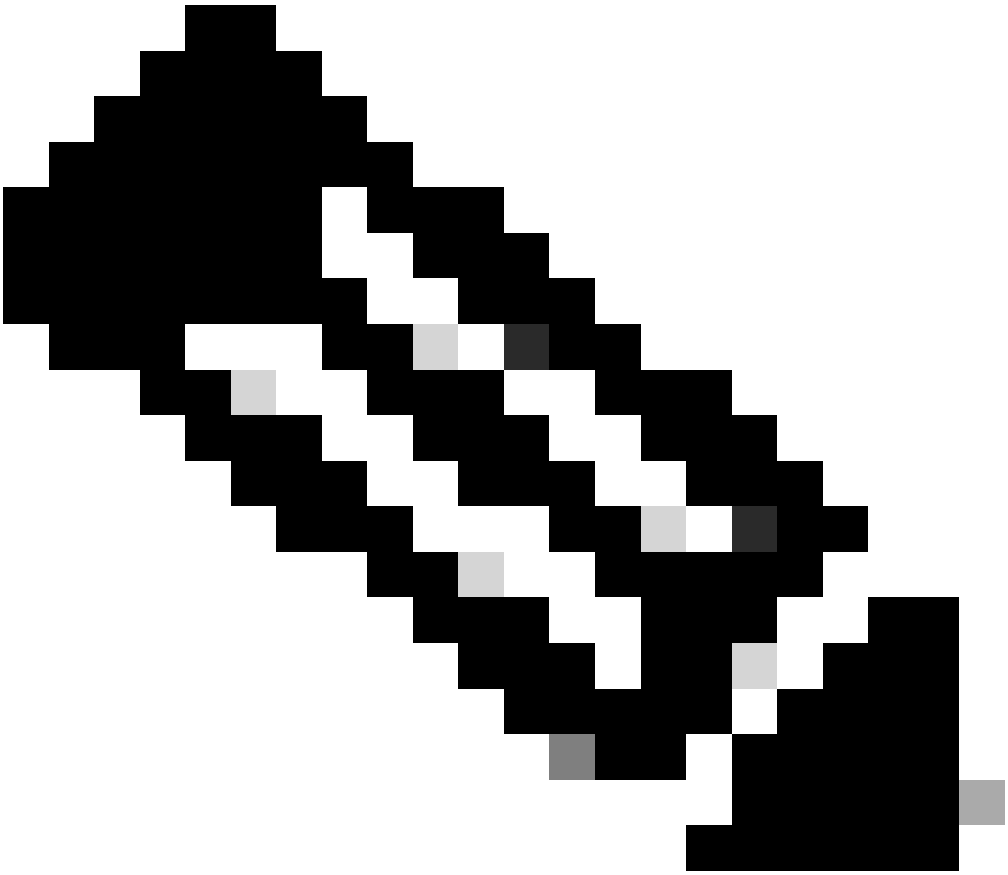
Selezionare il protocollo

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



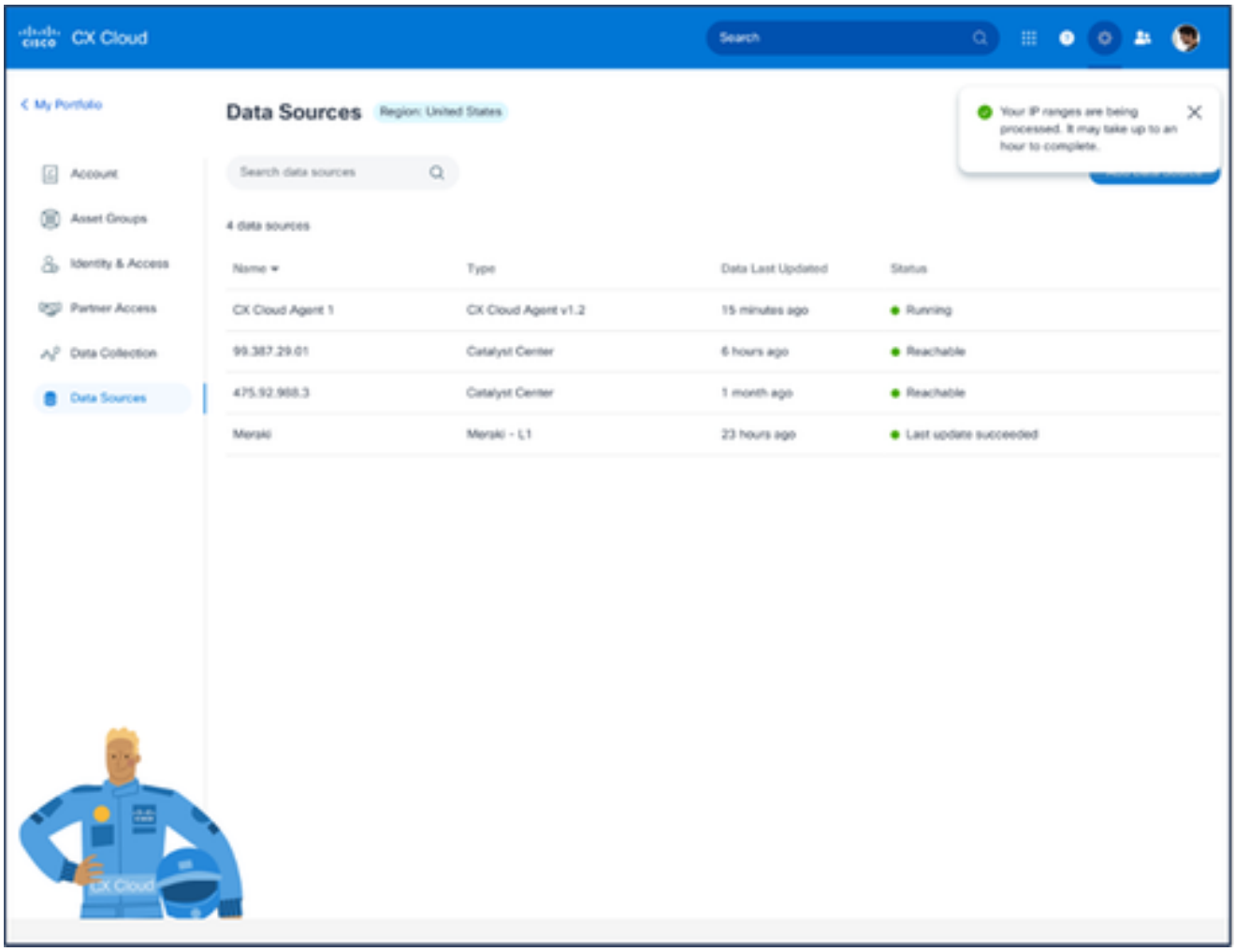
Dettagli individuazione

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



Nota: Per aggiungere un altro intervallo IP per l'agente CX selezionato, fare clic su Add Another IP Range per tornare alla finestra Set Your Protocol e ripetere i passaggi descritti in questa sezione.

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

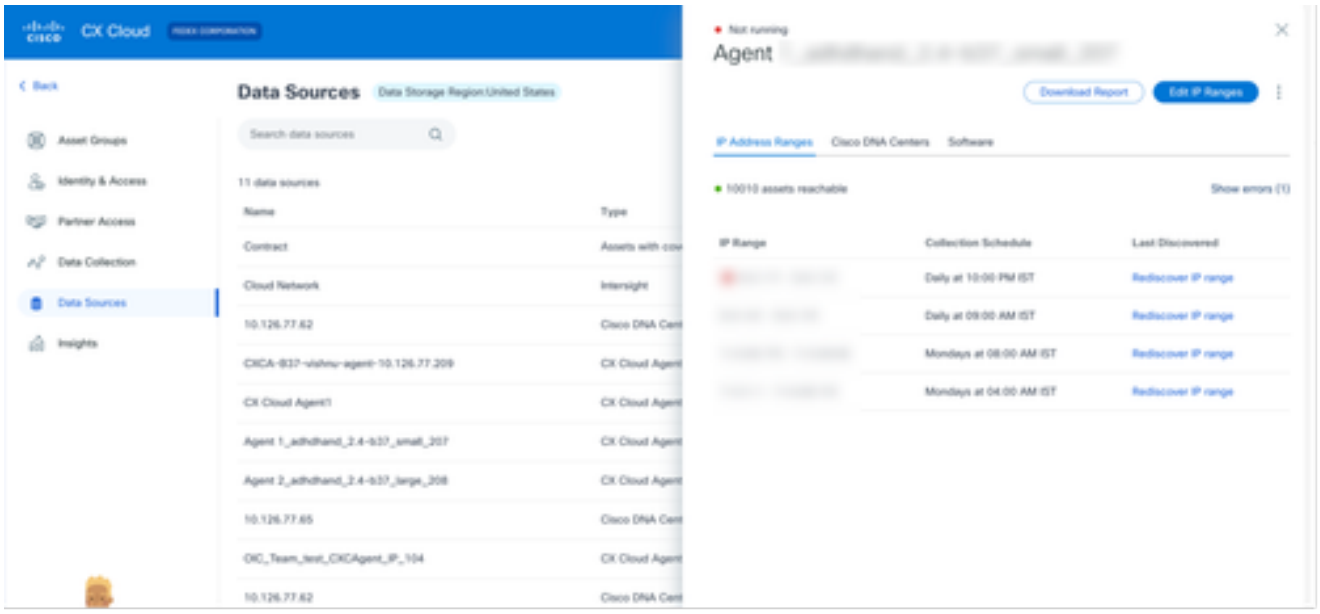


Messaggio di conferma

Modifica degli intervalli IP

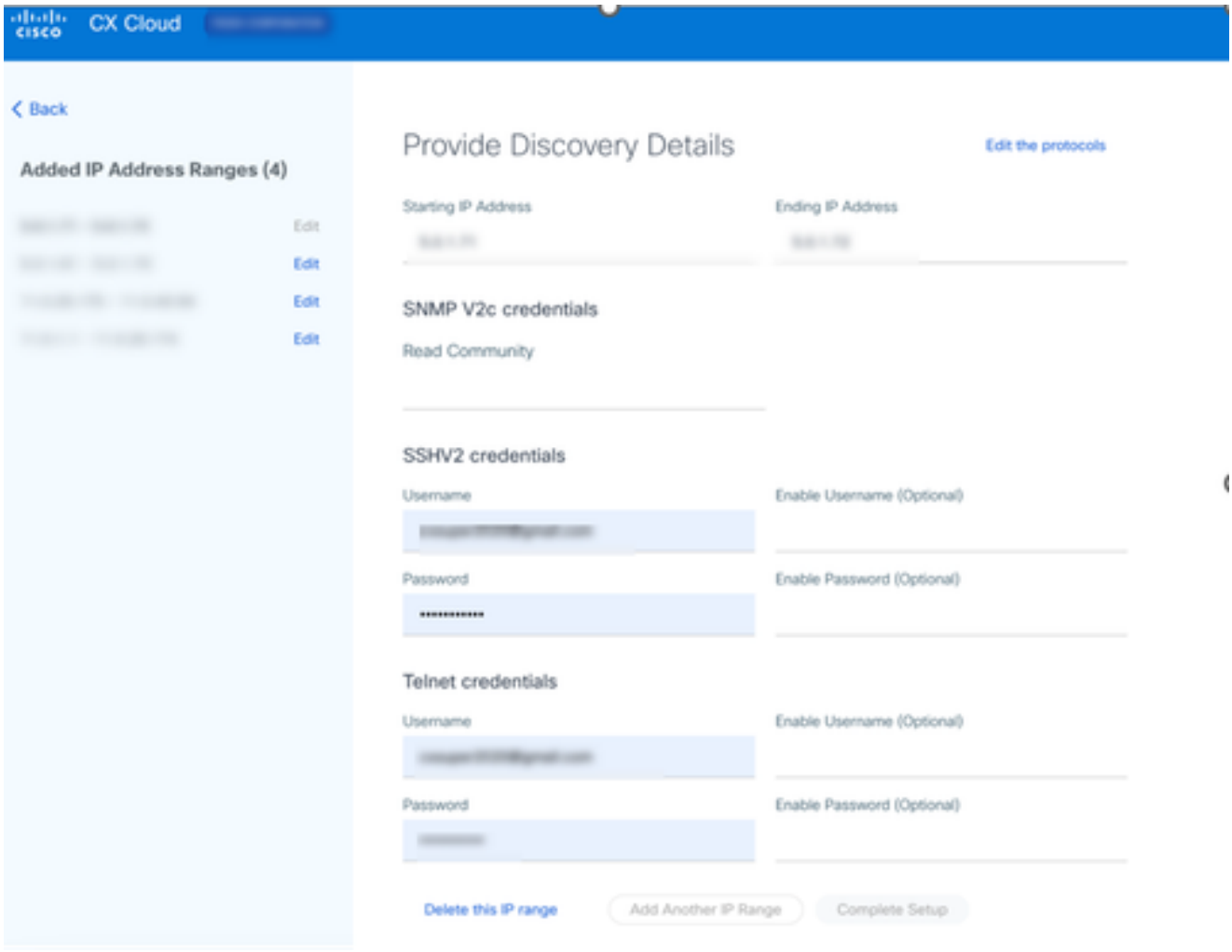
Per modificare un intervallo IP:

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

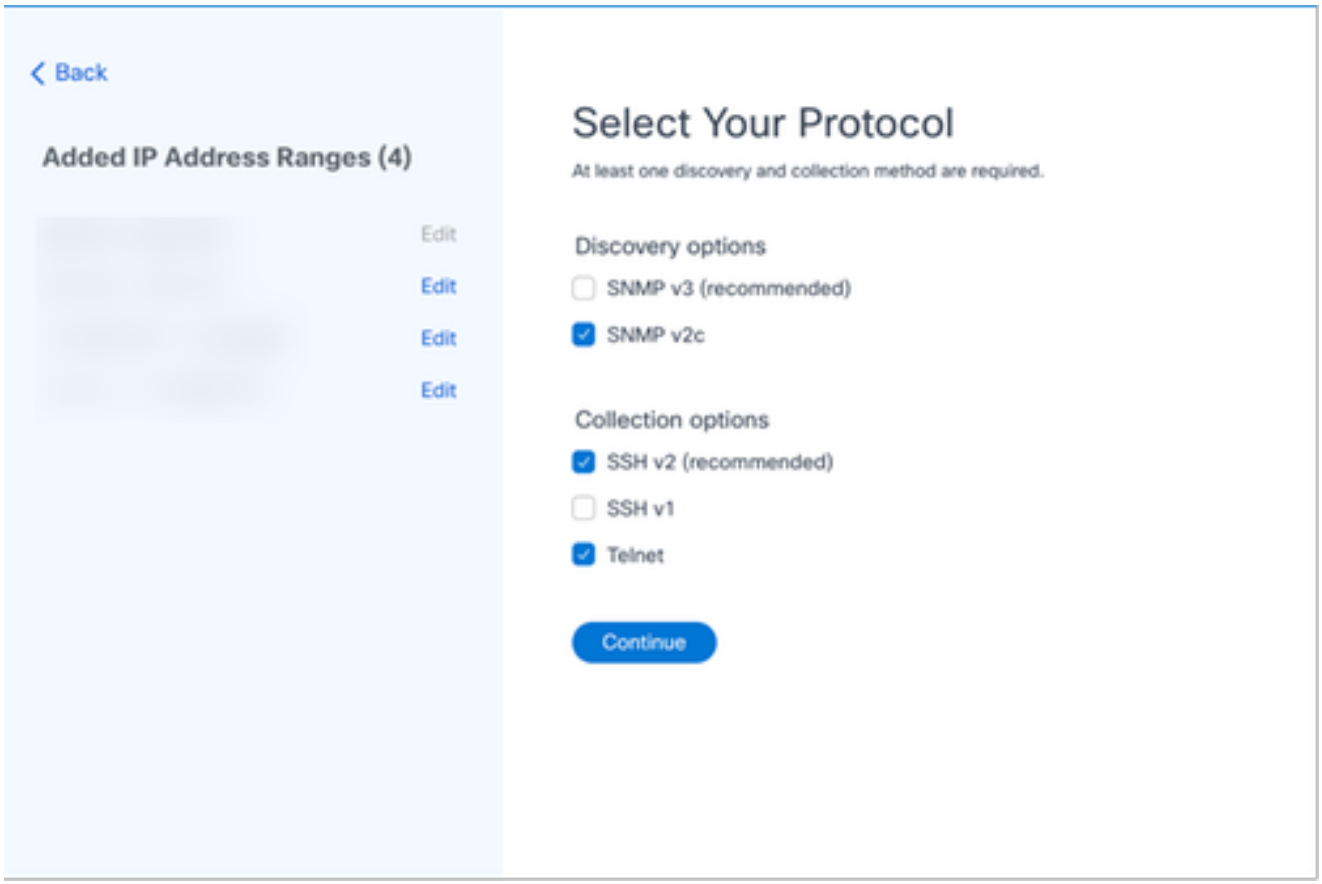


Origini dei dati

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

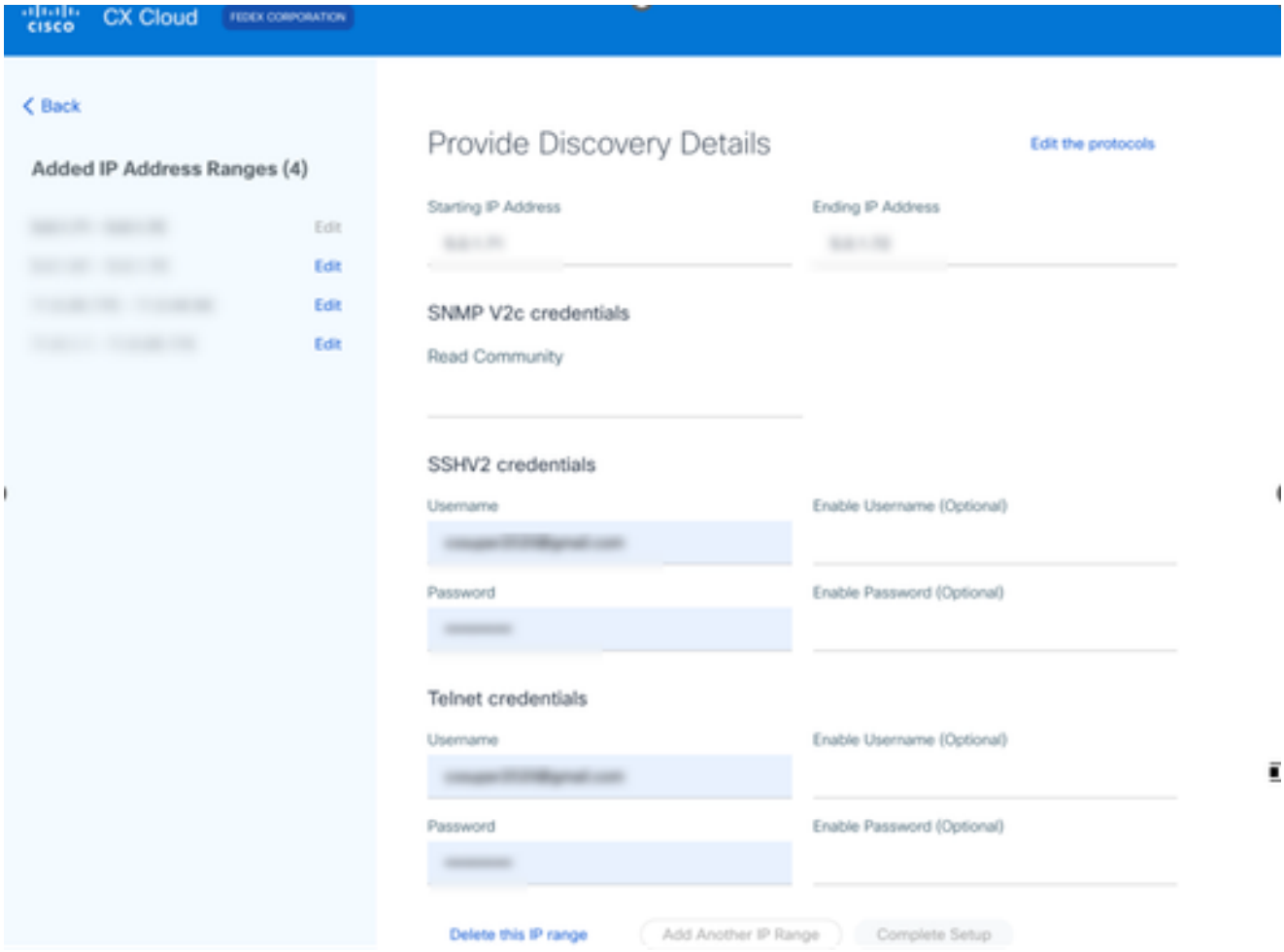


4. Fare clic su Modifica i protocolli. Viene visualizzata la finestra Select Your Protocol.



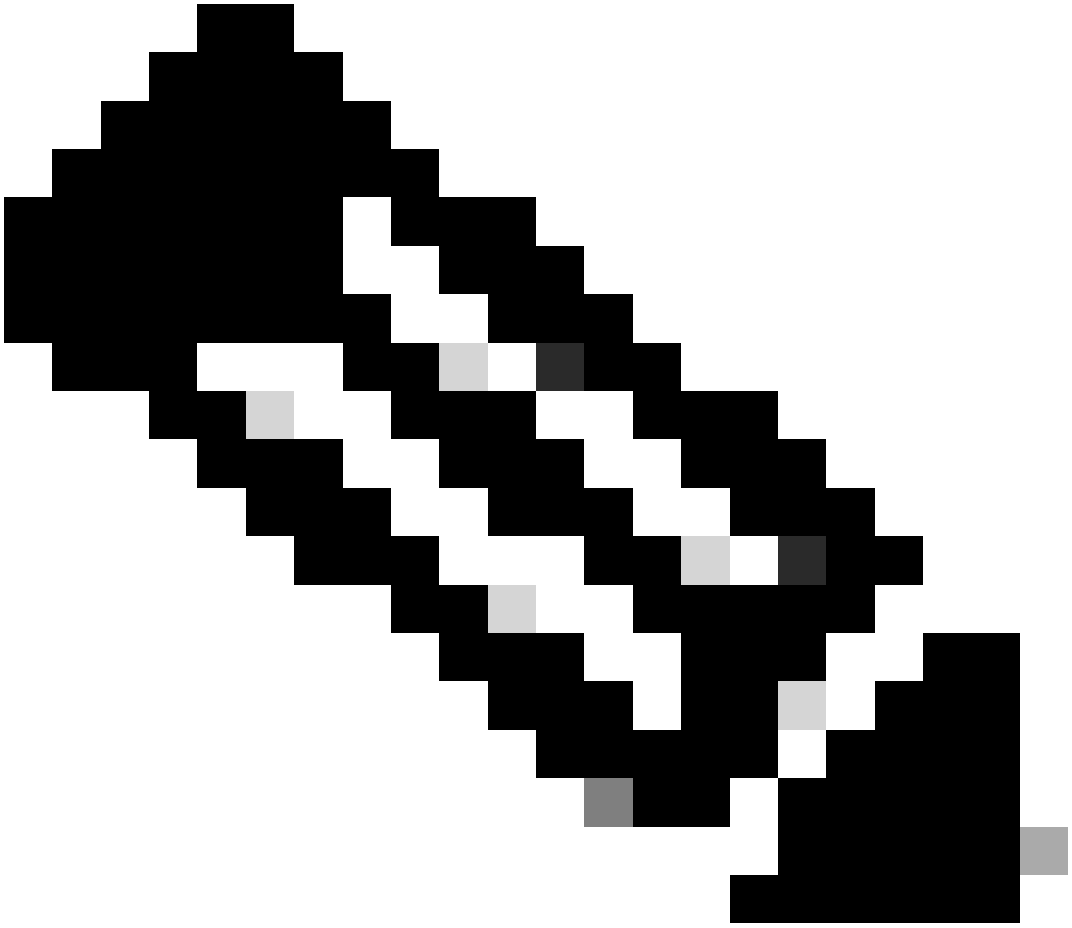
Selezionare il protocollo

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

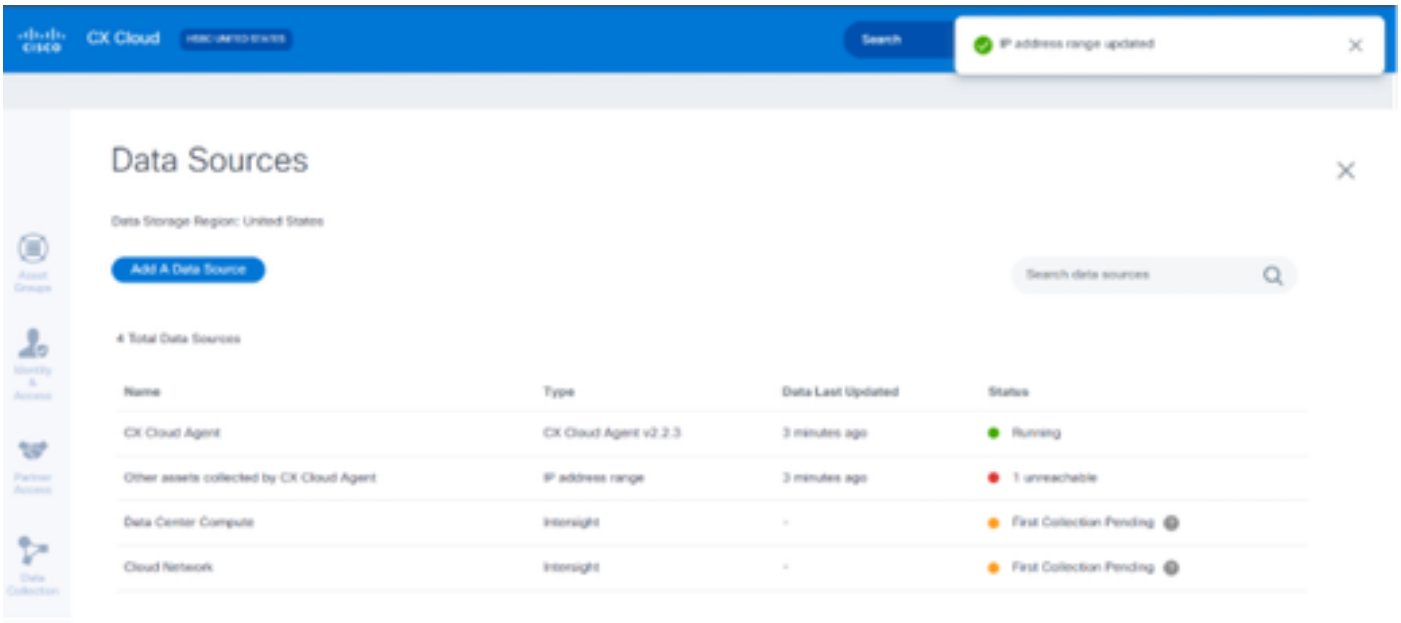


Fornire i dettagli di individuazione

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.



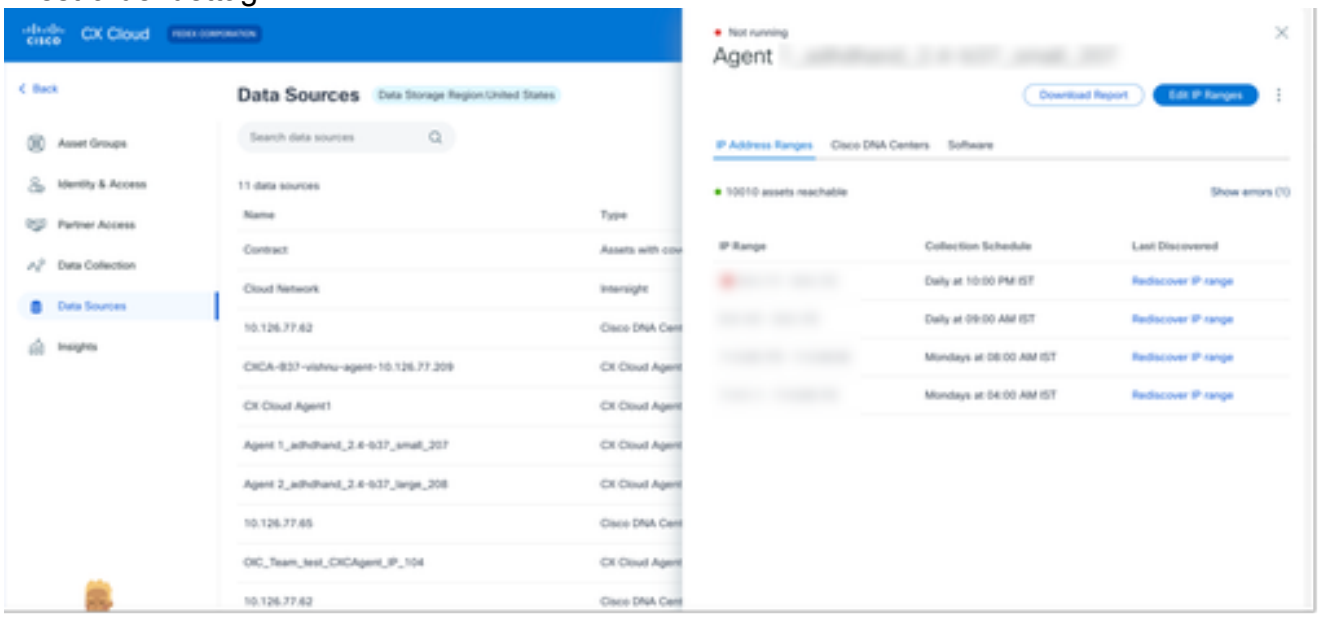
Nota: Questo messaggio di conferma non verifica se i dispositivi compresi nell'intervallo modificato sono raggiungibili o se le loro credenziali vengono accettate. Questa conferma viene eseguita quando il cliente avvia il processo di rilevamento.



Eliminazione intervallo IP

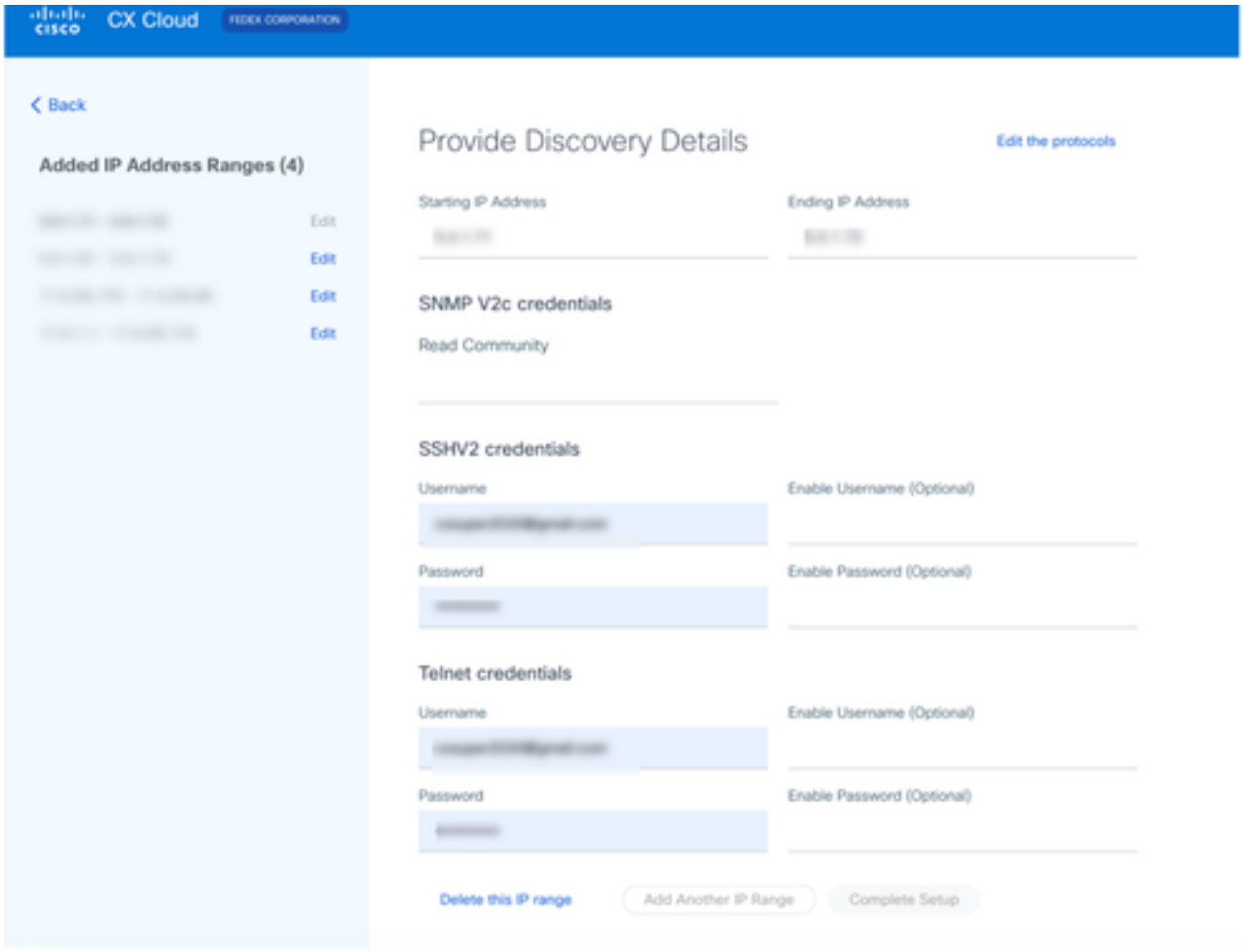
Per eliminare un intervallo IP:

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



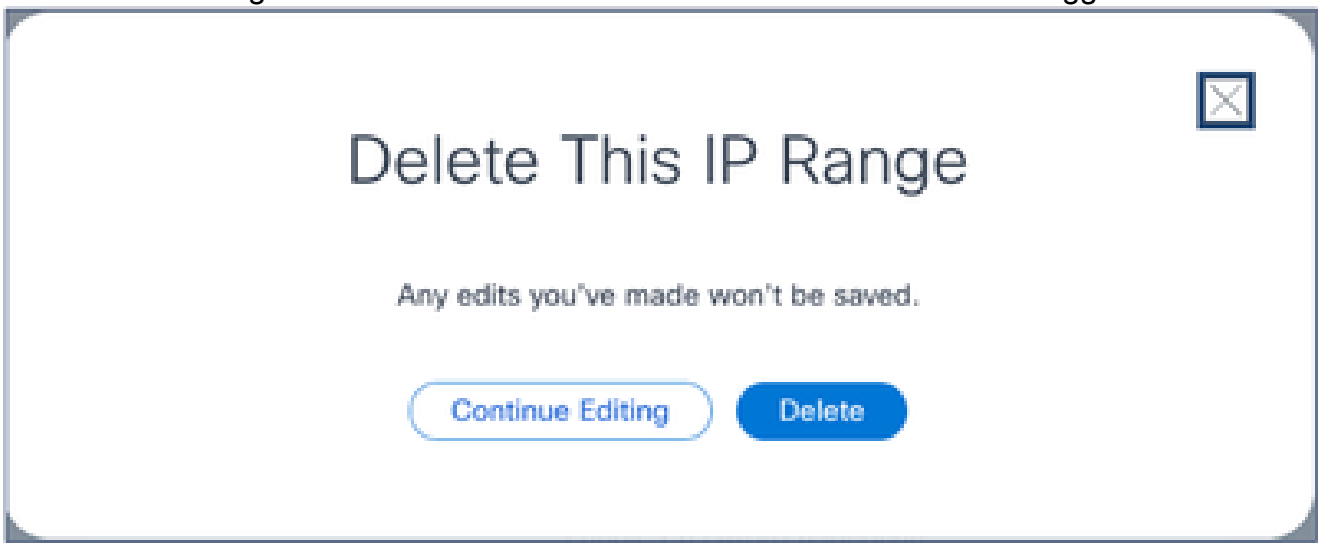
Origini dei dati

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



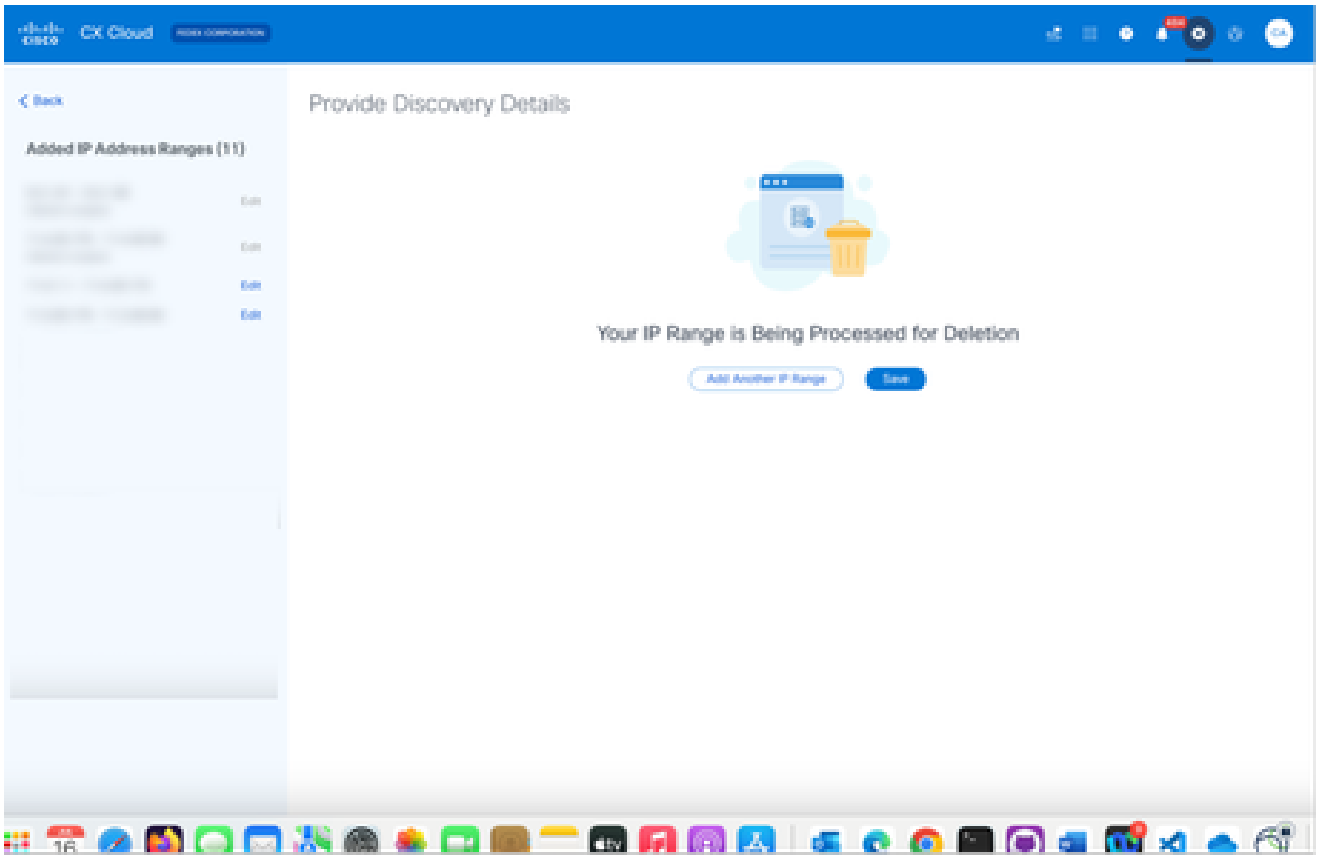
Fornire i dettagli di individuazione

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



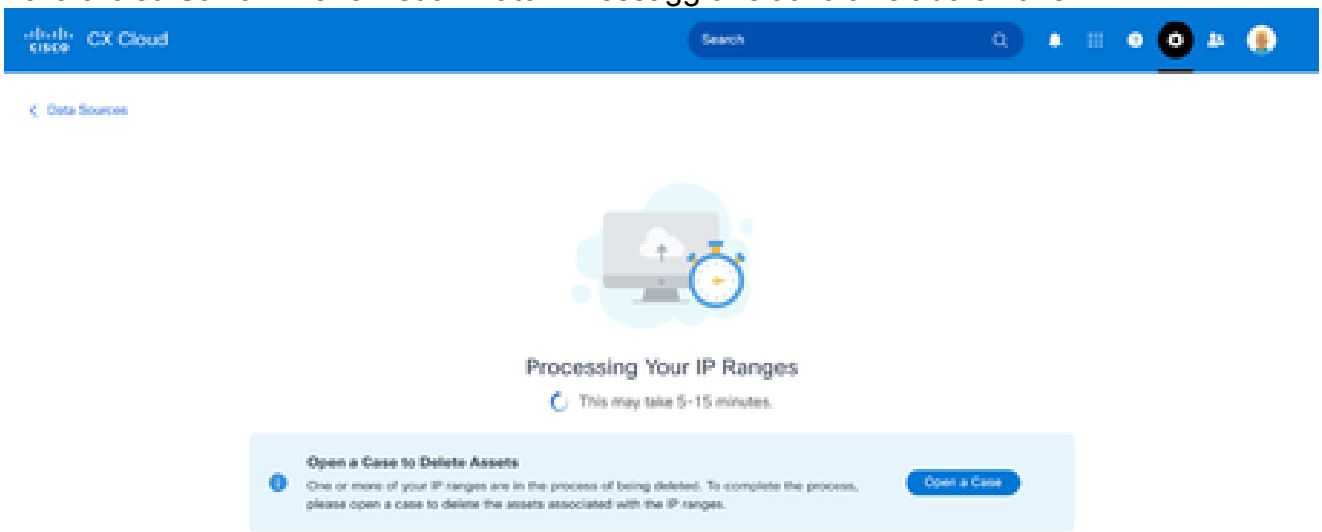
Messaggio eliminazione conferma

5. Fare clic su Elimina.



Eliminazione intervallo IP

6. Fare clic su 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.

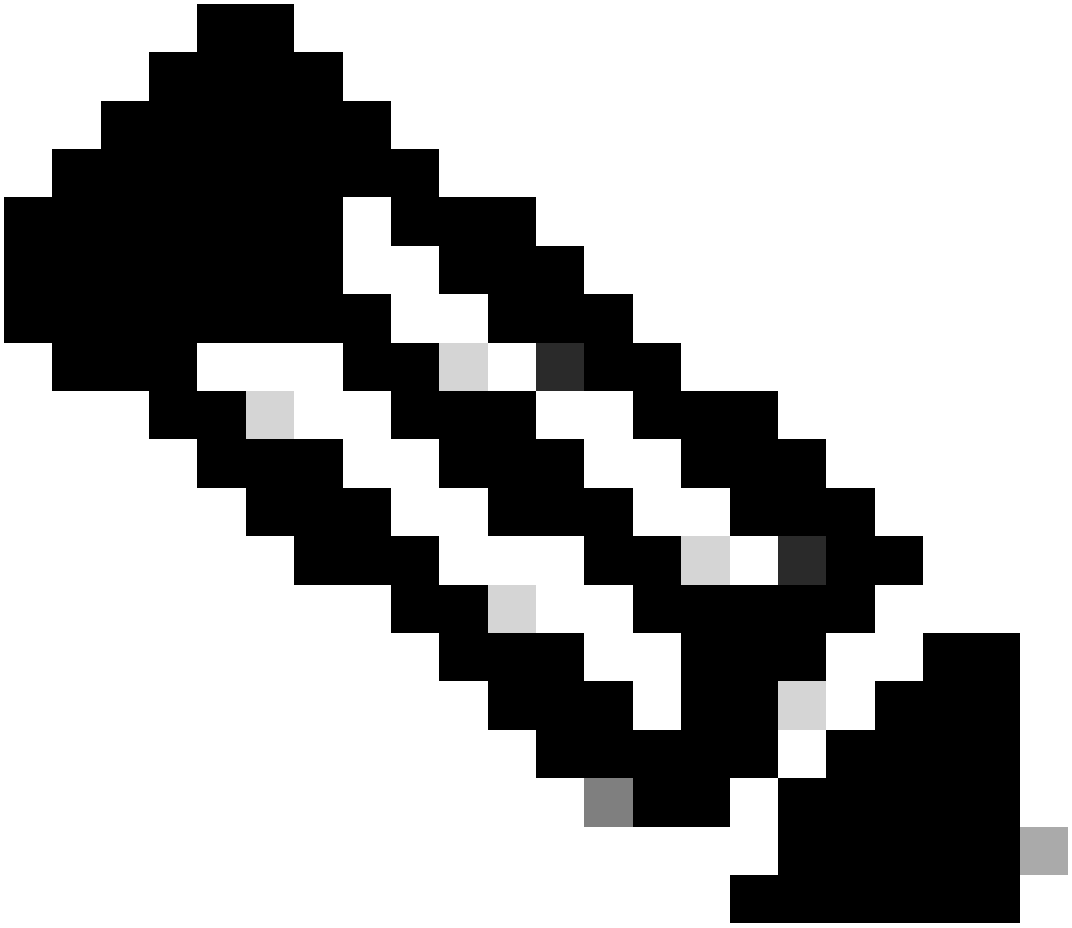
Informazioni sui dispositivi rilevati da più controller

Se Catalyst Center e le altre risorse raccolte dall'agente CX (connessione periferica diretta) si trovano sullo stesso agente CX, è possibile che alcuni dispositivi vengano individuati sia da Cisco Catalyst Center che dalla connessione periferica diretta all'agente 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 CX.

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

Pianificazione delle analisi diagnostiche

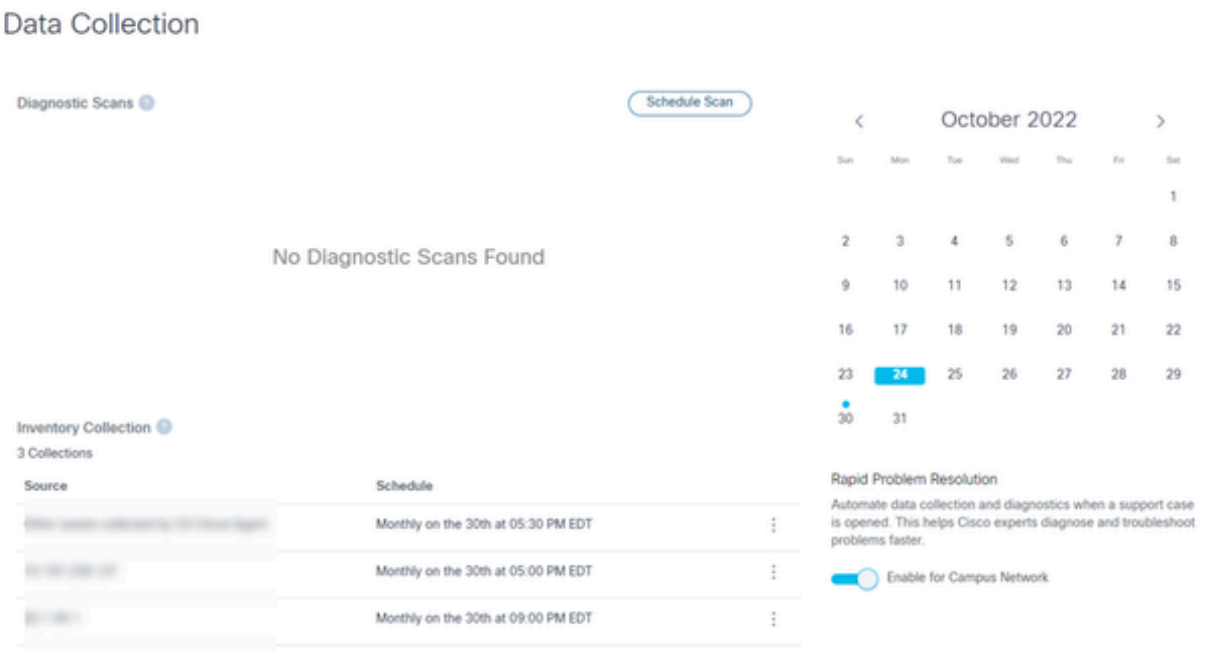
I clienti possono pianificare scansioni diagnostiche su richiesta in CX Cloud per le tracce di successo idonee e i relativi dispositivi coperti per popolare i bug di priorità nelle avvertenze.



Nota: Cisco consiglia di pianificare analisi diagnostiche o di avviare analisi su richiesta ad almeno 6-7 ore di distanza dalle pianificazioni 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.

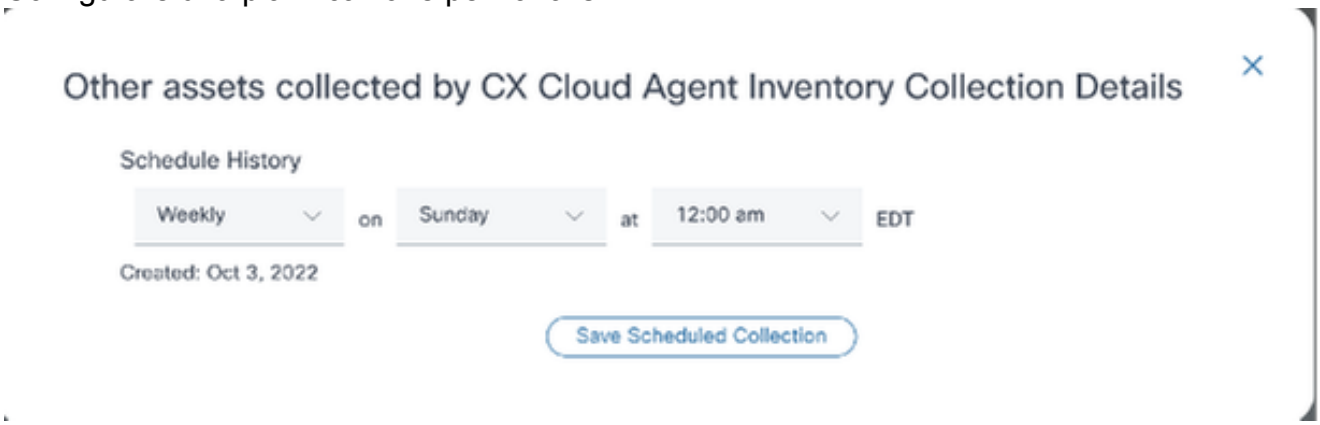
Per pianificare le analisi diagnostiche:

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.



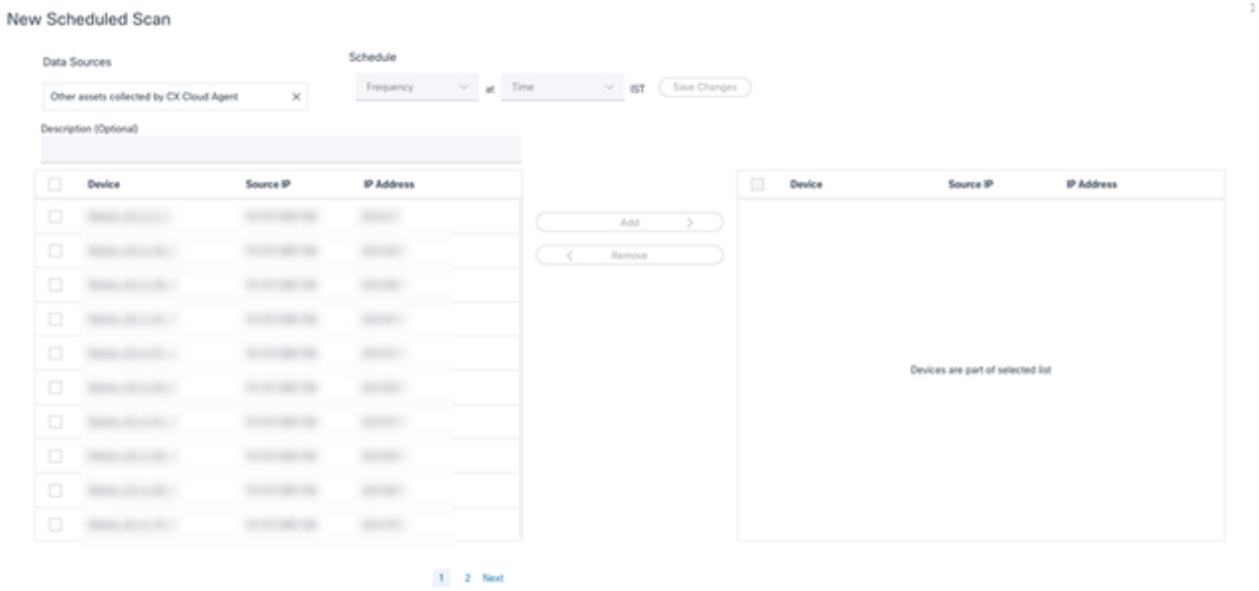
Pianificazione delle analisi

4. Configurare una pianificazione per l'analisi.



Configura pianificazione analisi

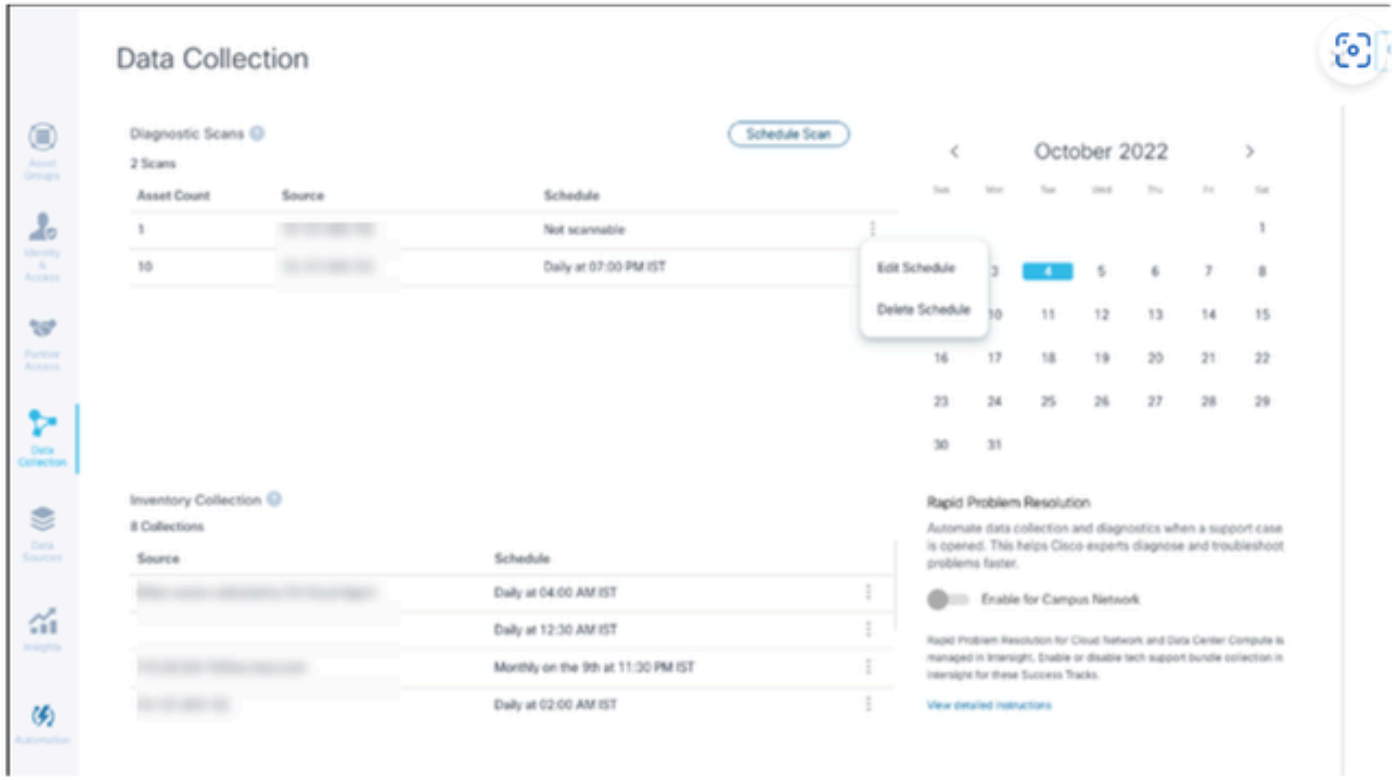
5. Nell'elenco delle periferiche, selezionare tutte le periferiche per la scansione e fare clic su Aggiungi.



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 dati con le opzioni Modifica ed Elimina pianificazione

Aggiornamento delle VM dell'agente CX a configurazioni medie e

grandi

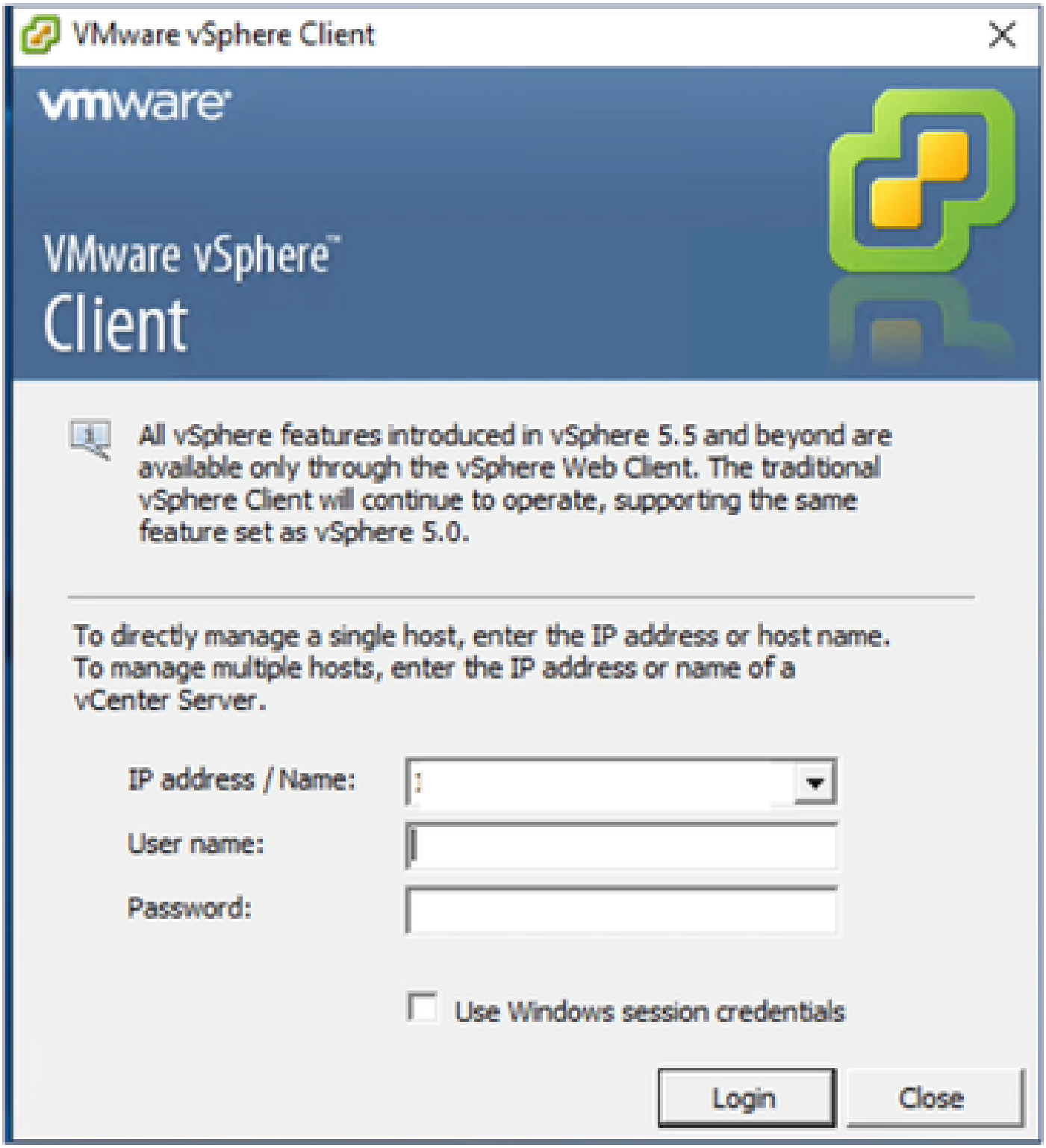
Dopo l'aggiornamento delle VM, non è possibile:

- 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.

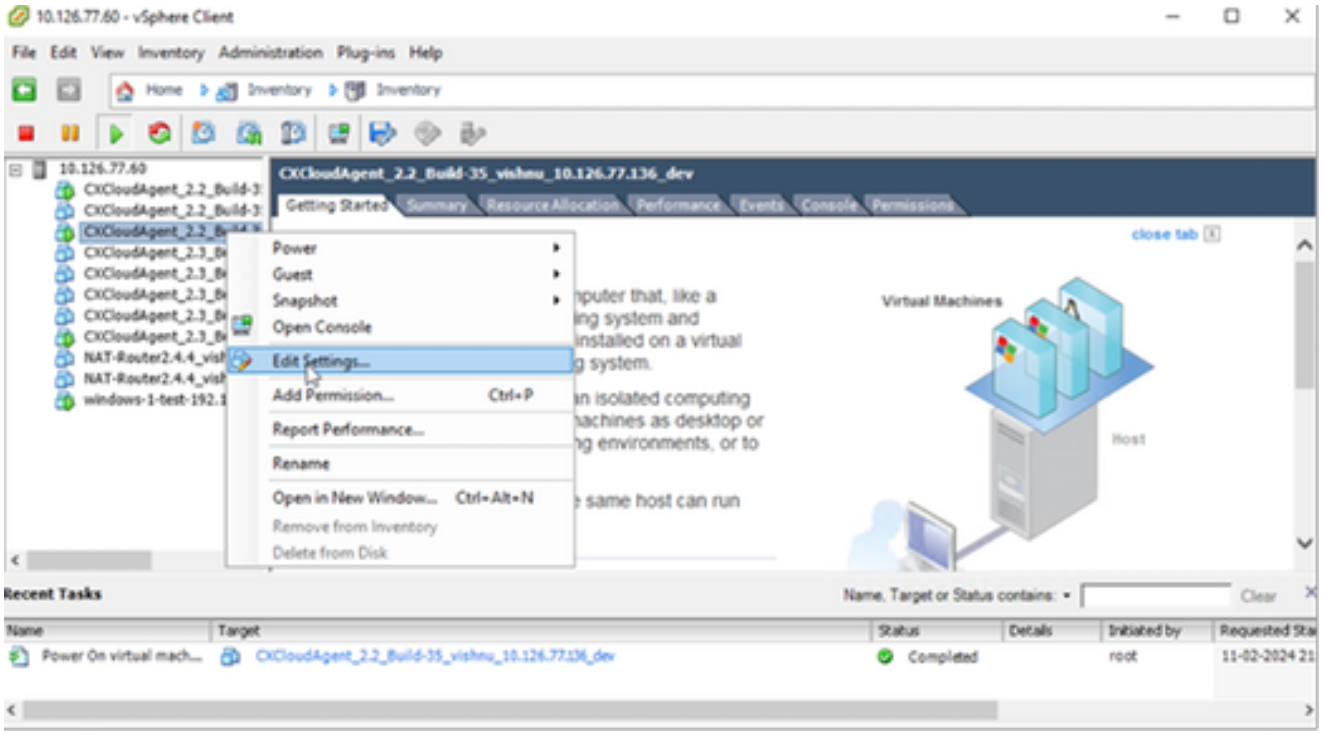
Riconfigurazione con VMware vSphere Thick Client

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



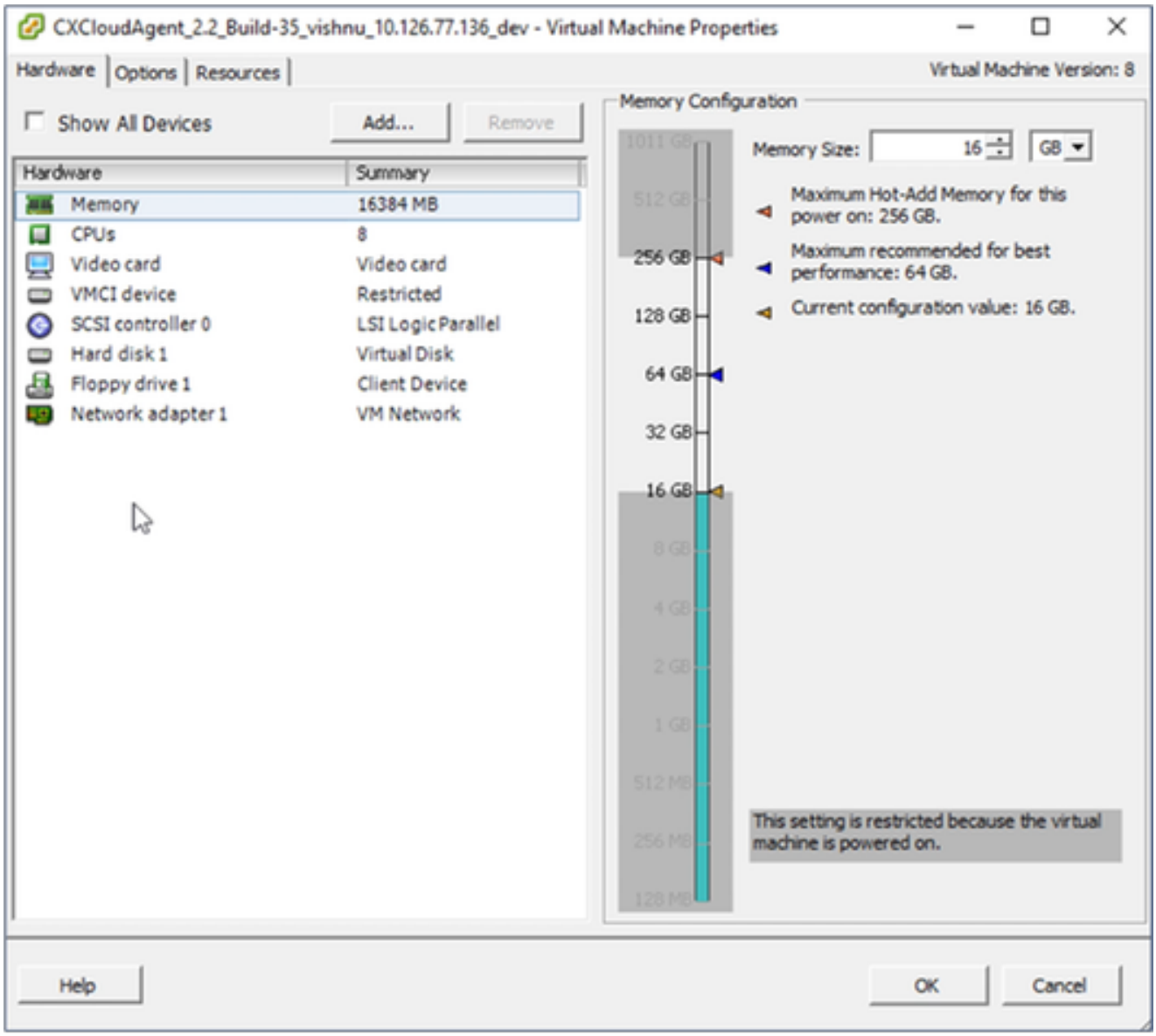
Client vSphere

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



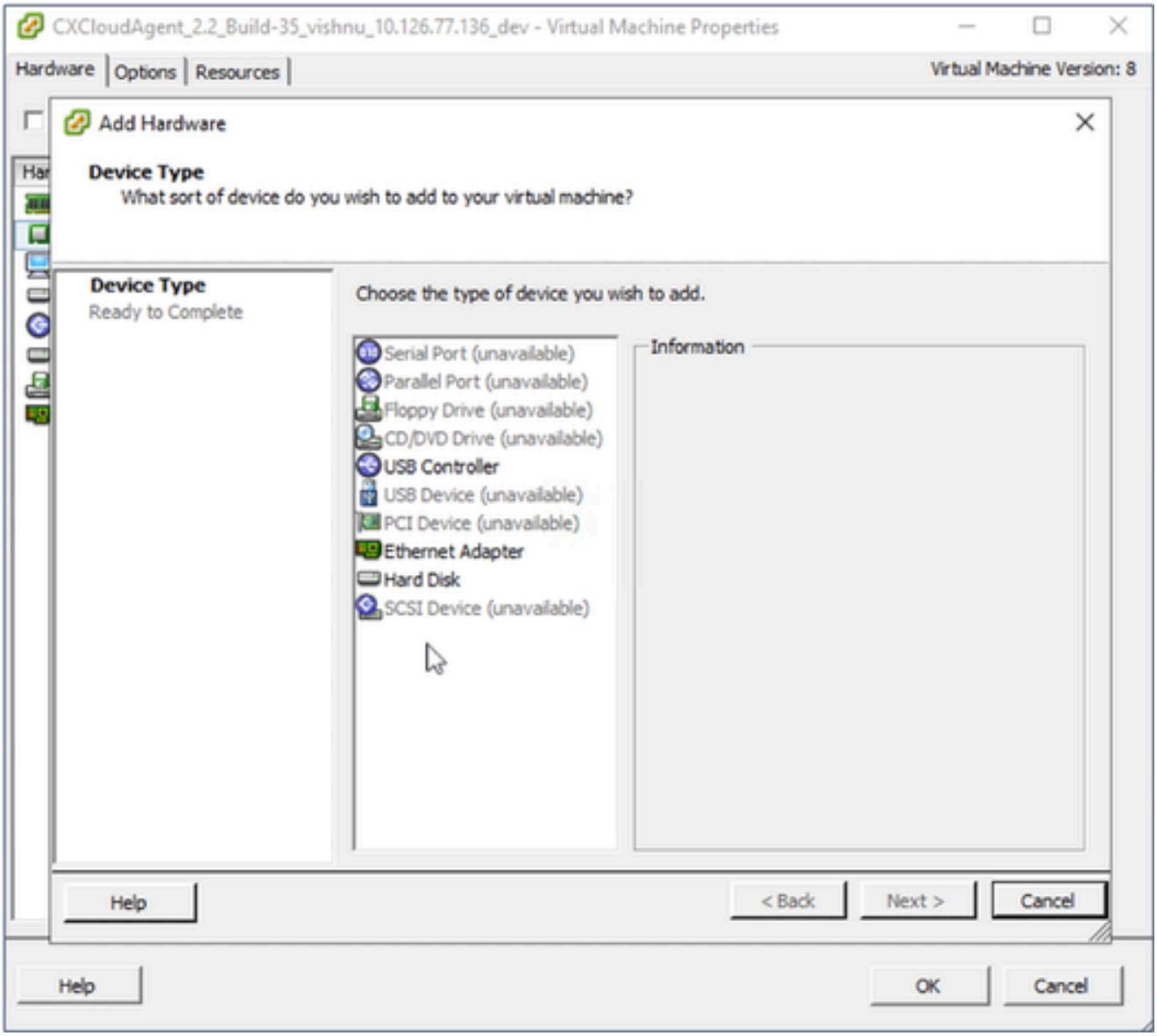
Modifica impostazioni

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.



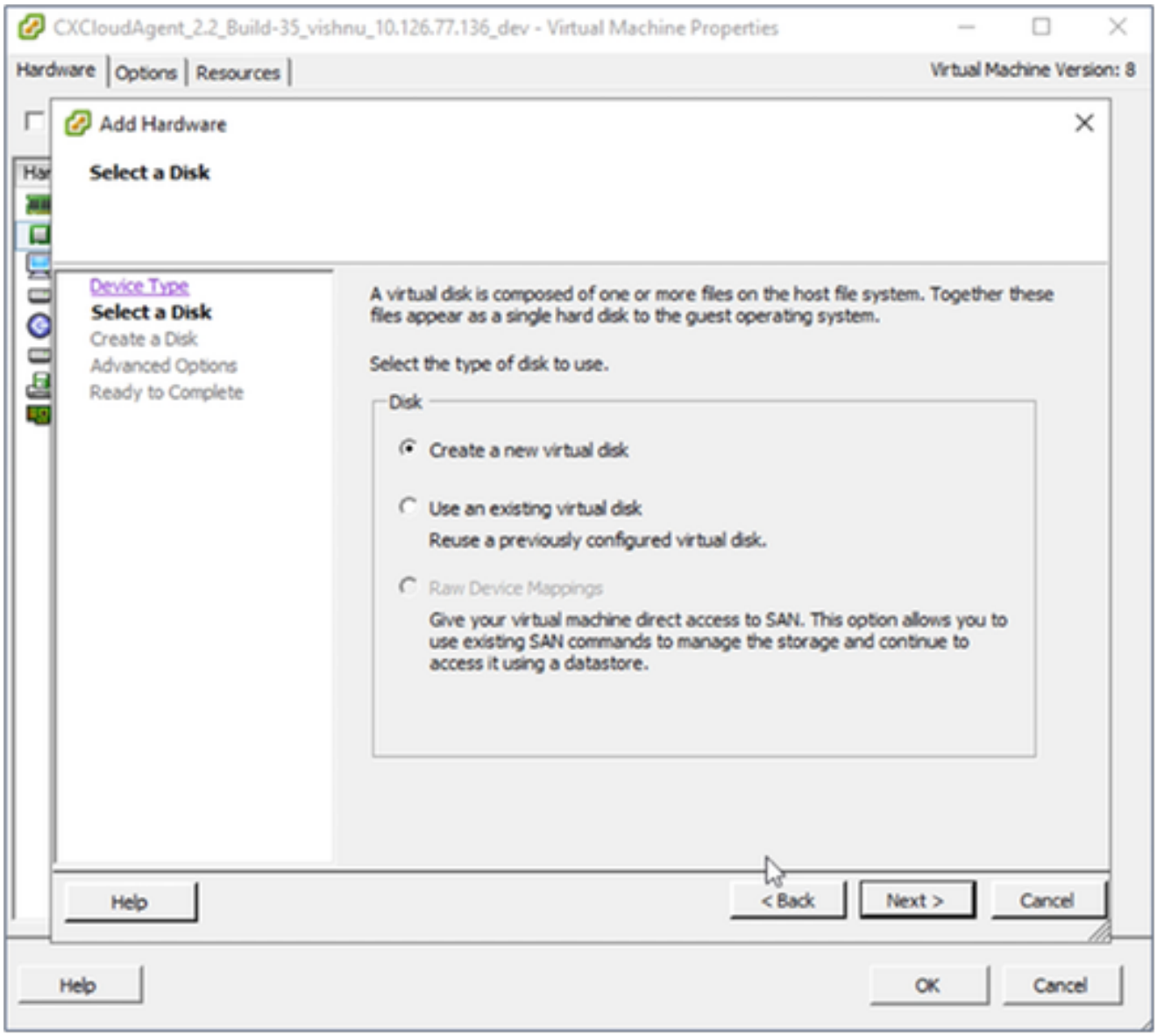
Proprietà macchina virtuale

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.



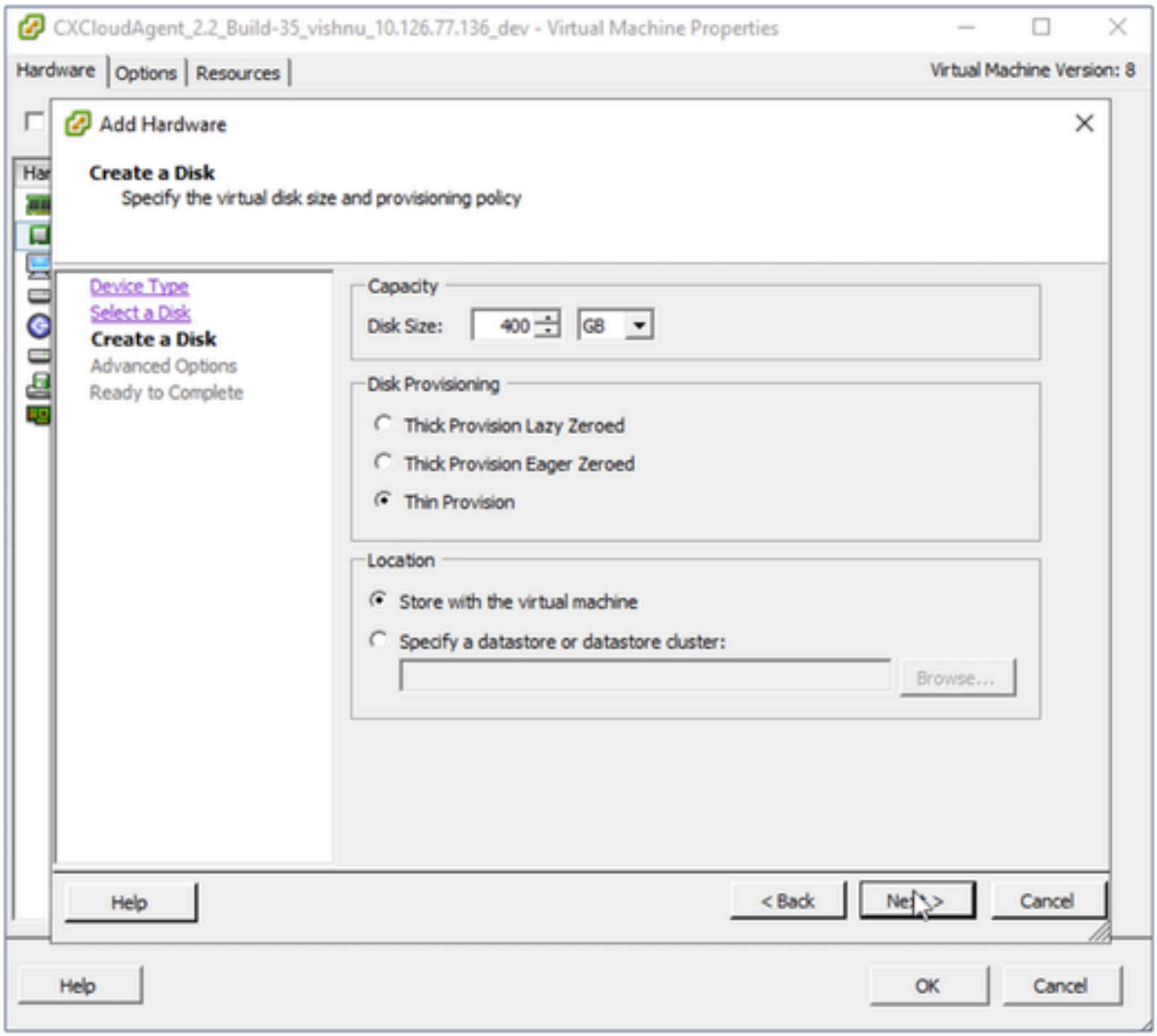
Tipo di dispositivo

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



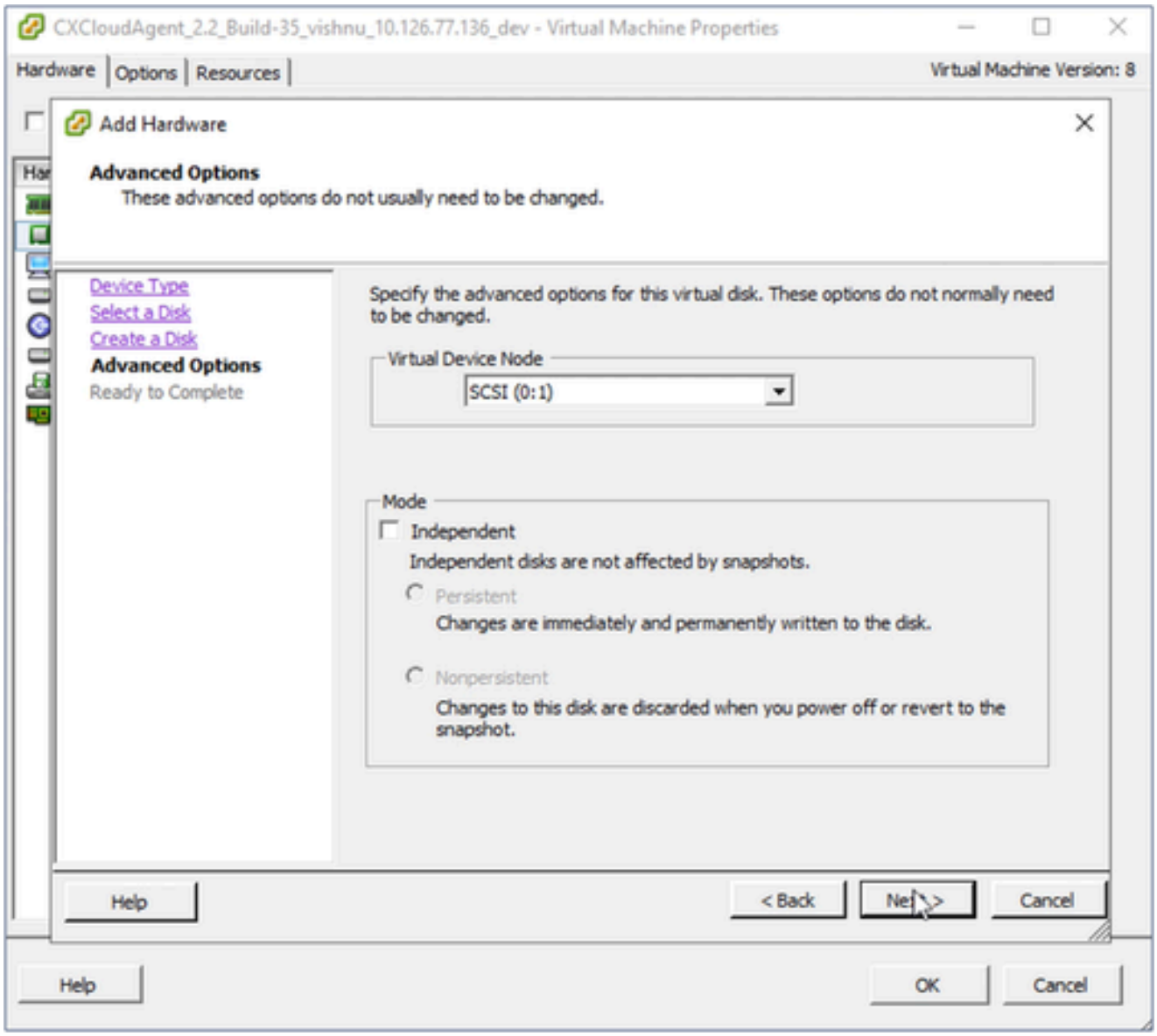
Seleziona disco

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



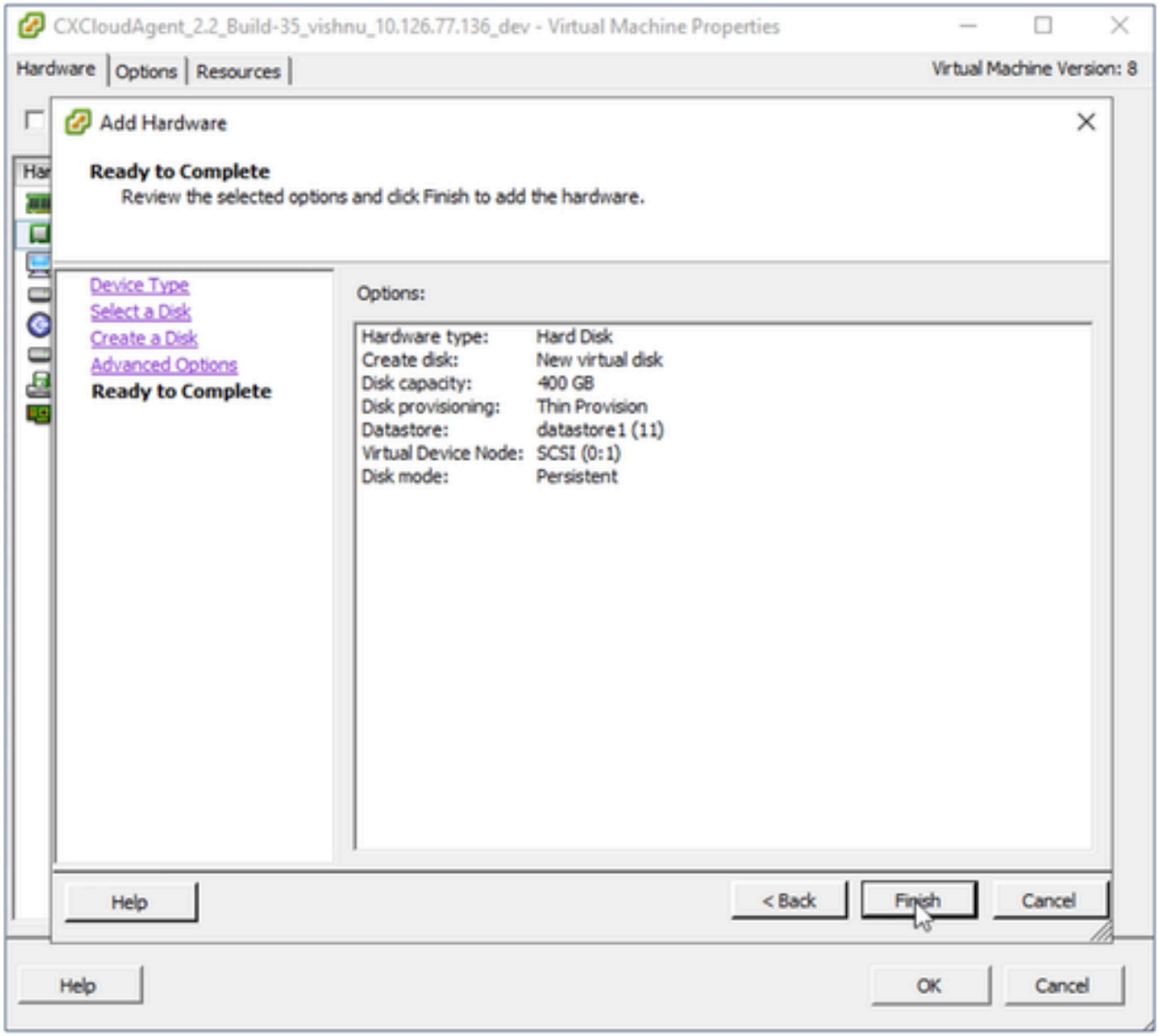
Crea disco

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.



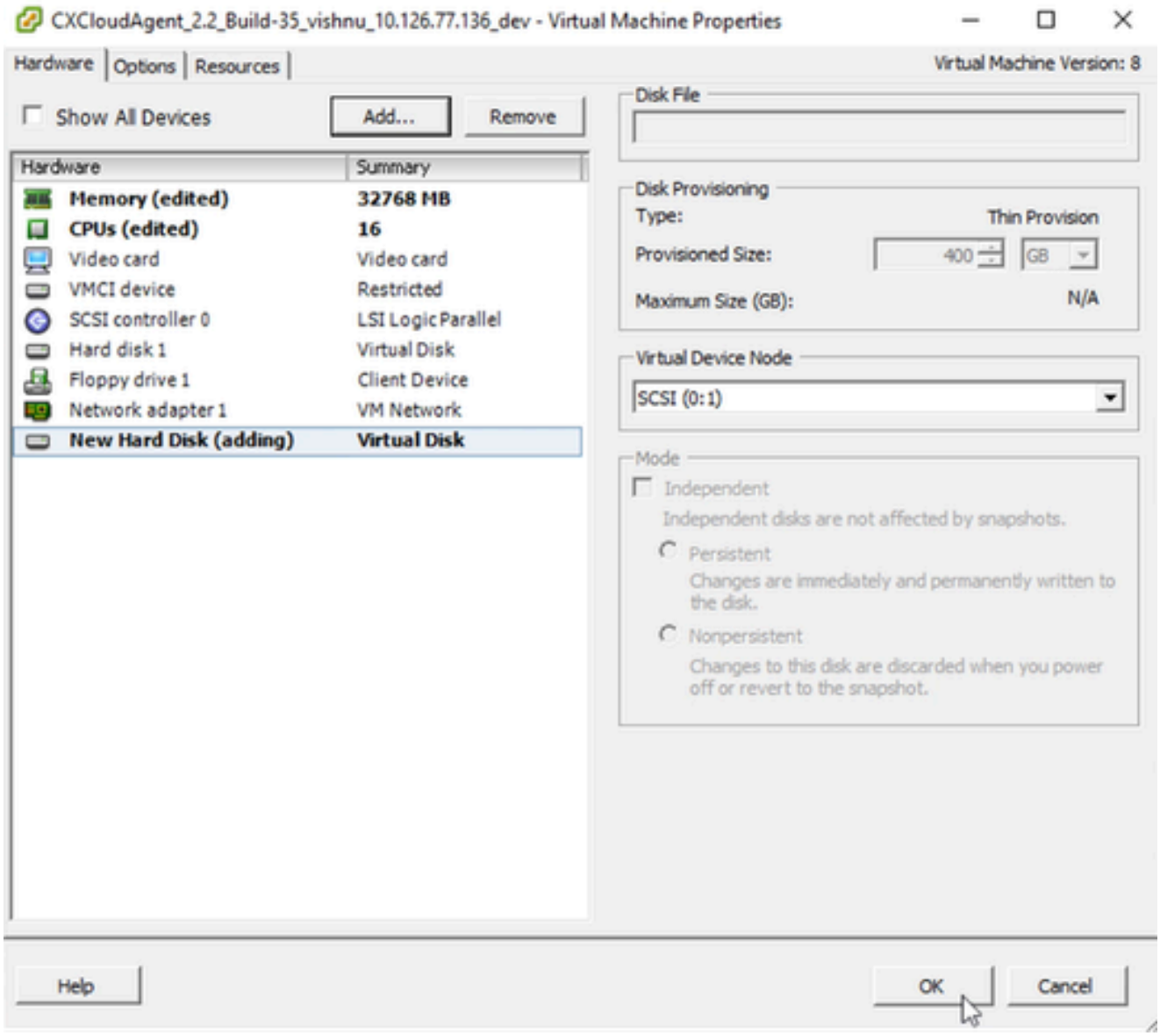
Opzioni avanzate

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



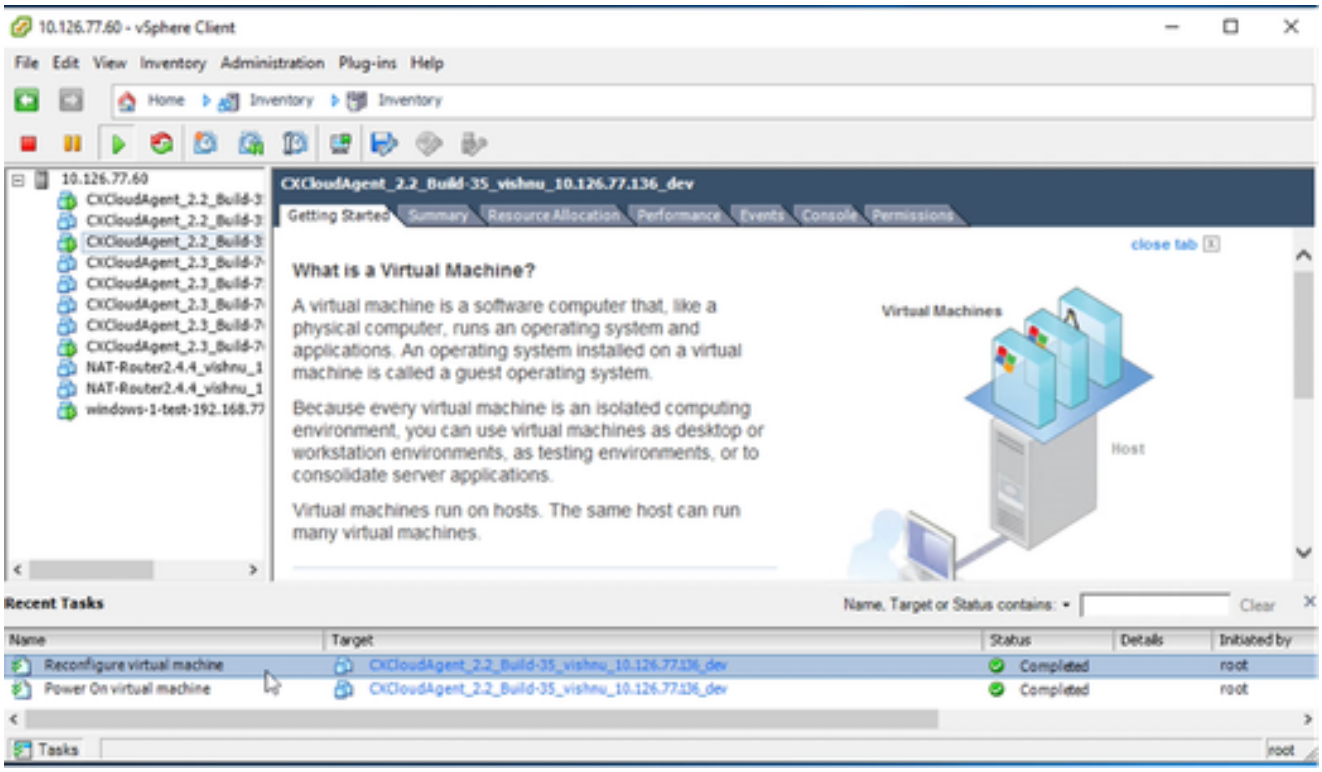
Pronto per il completamento

13. Fare clic su Finish (Fine).

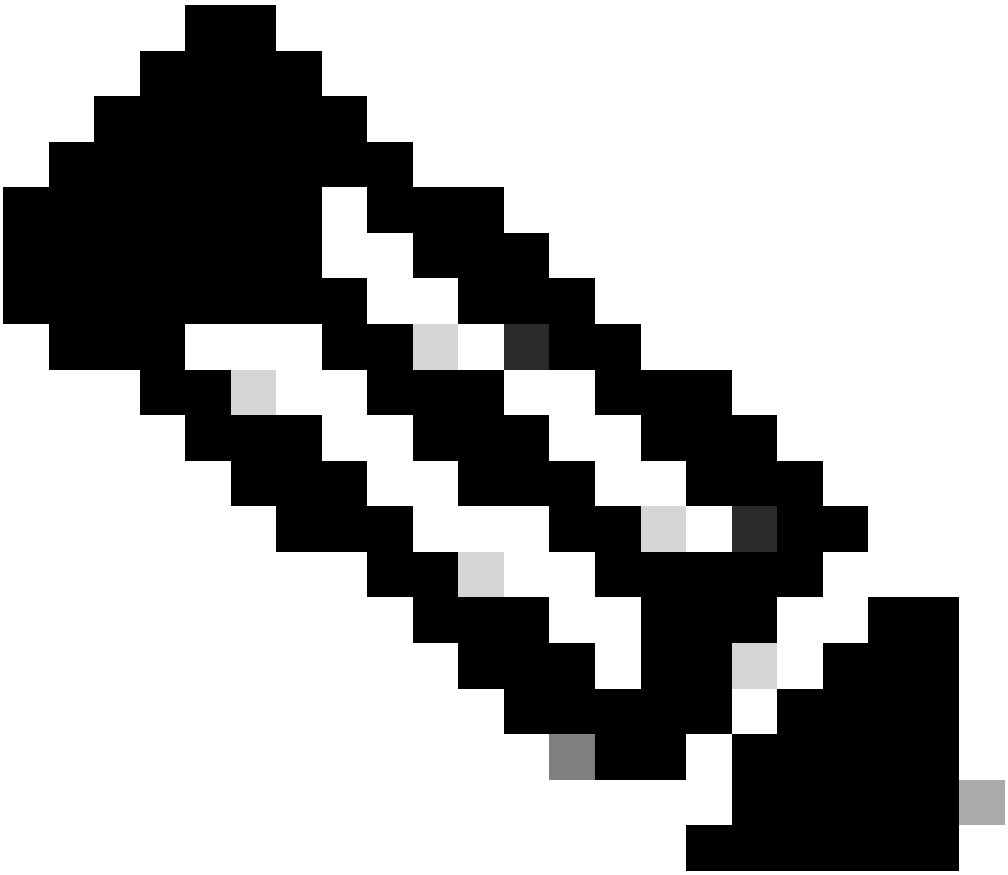


Hardware

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



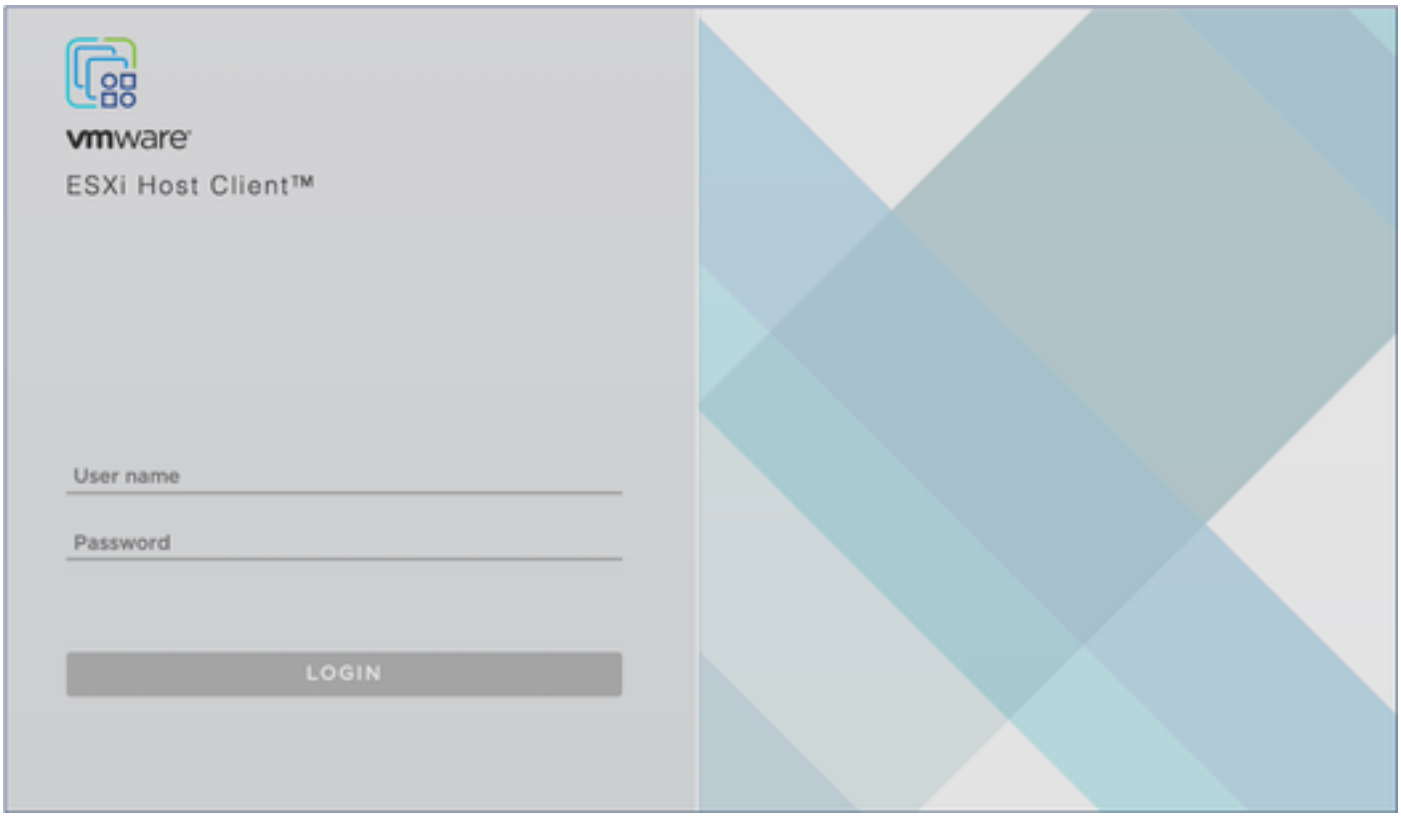
Attività recenti



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

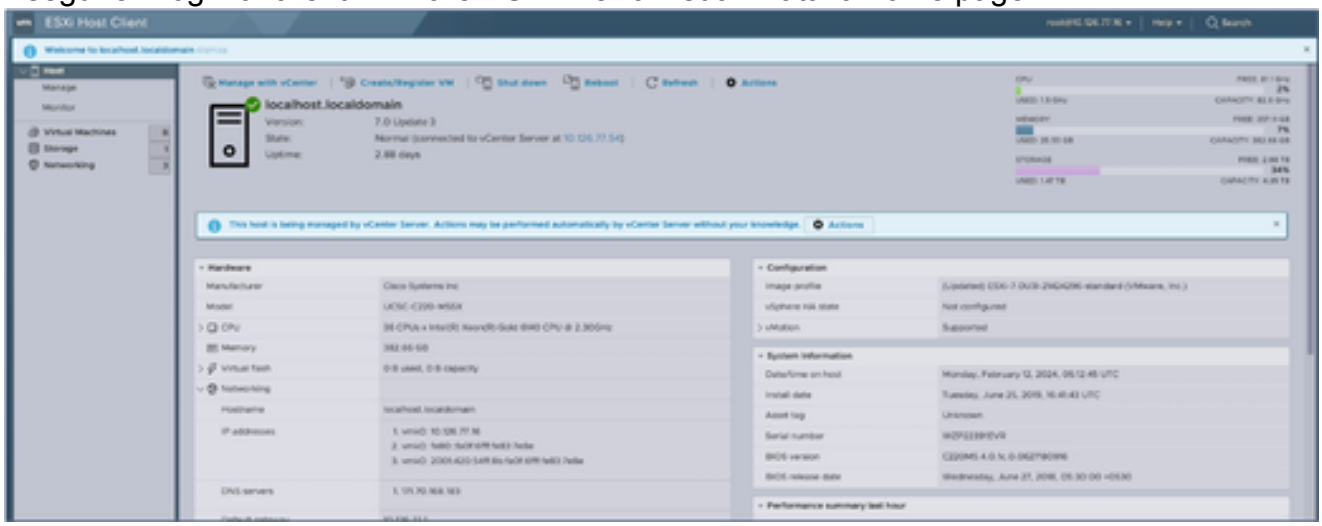
Riconfigurazione con il client Web ESXi v6.0

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



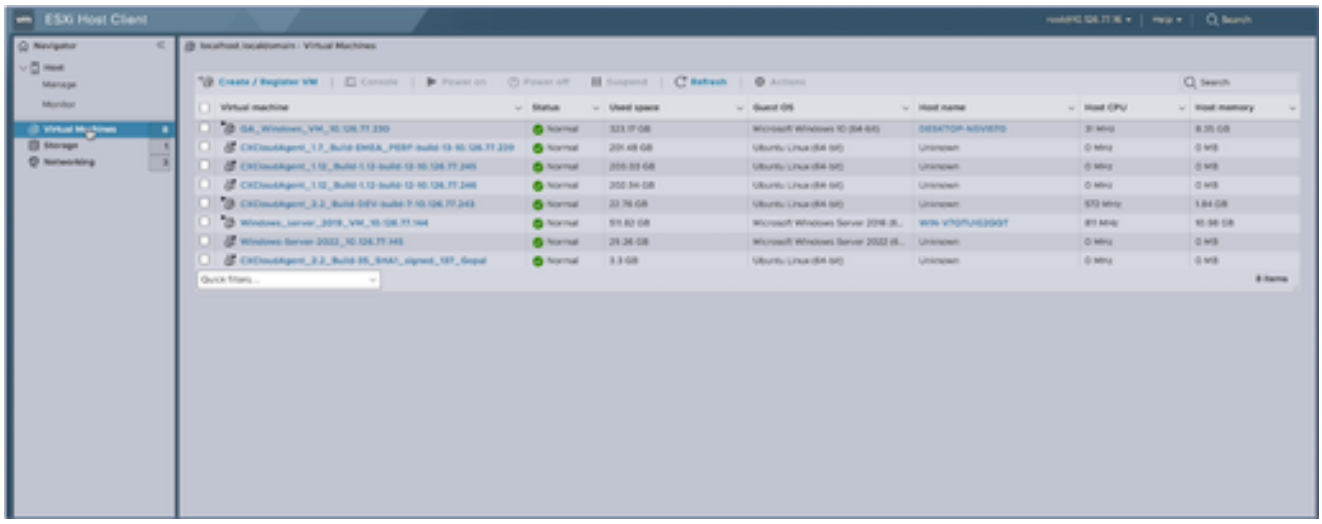
Client ESXi

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



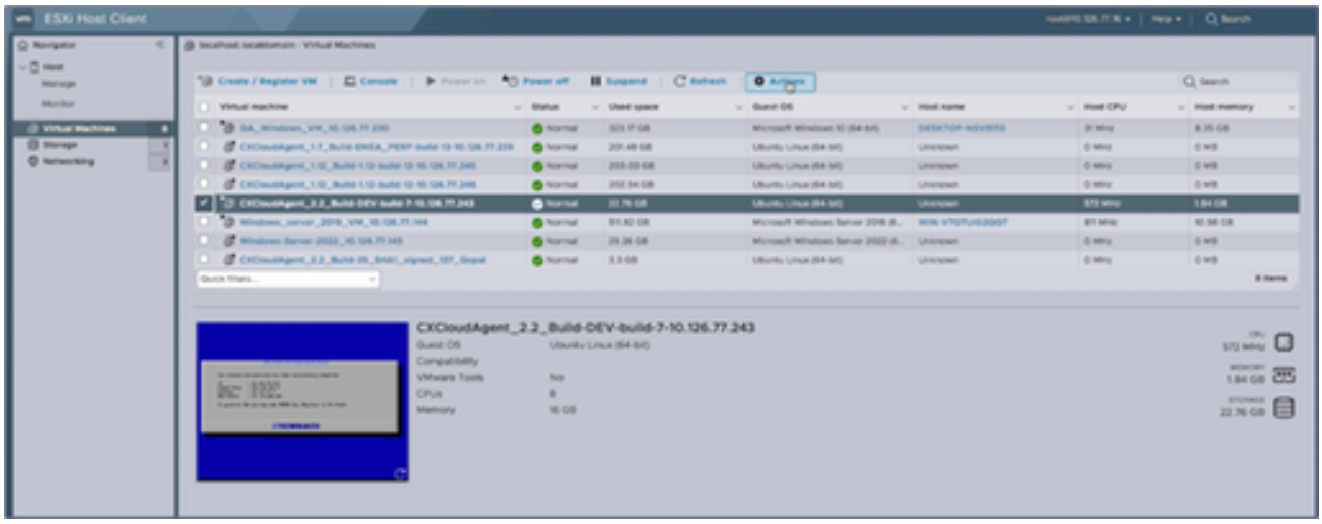
Home page ESXi

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



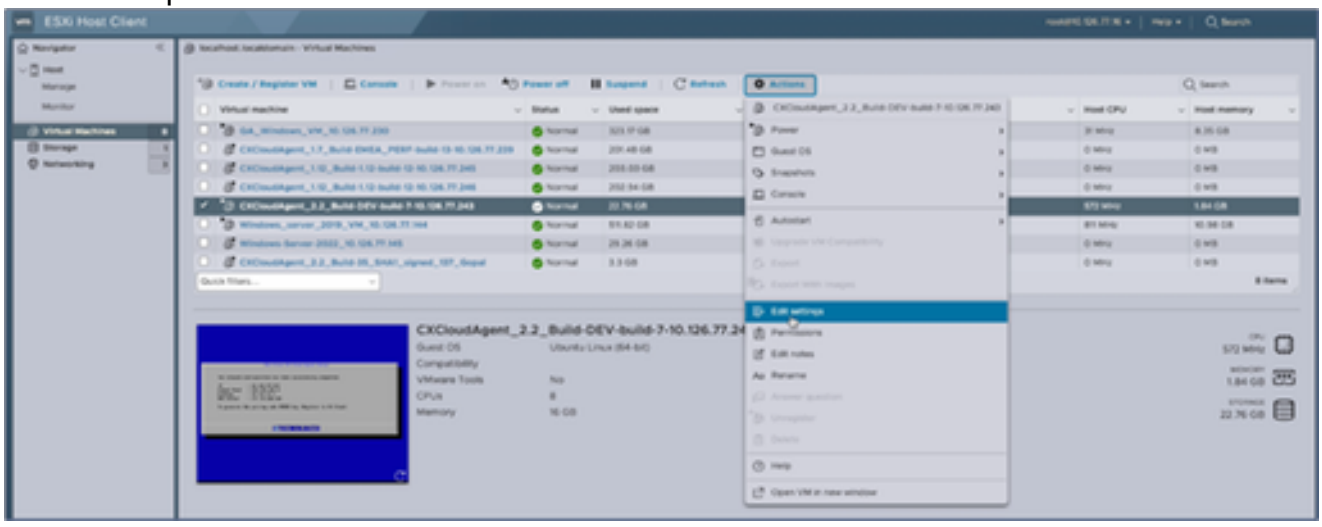
Elenco di macchine virtuali

3. Selezionare la macchina virtuale di destinazione.

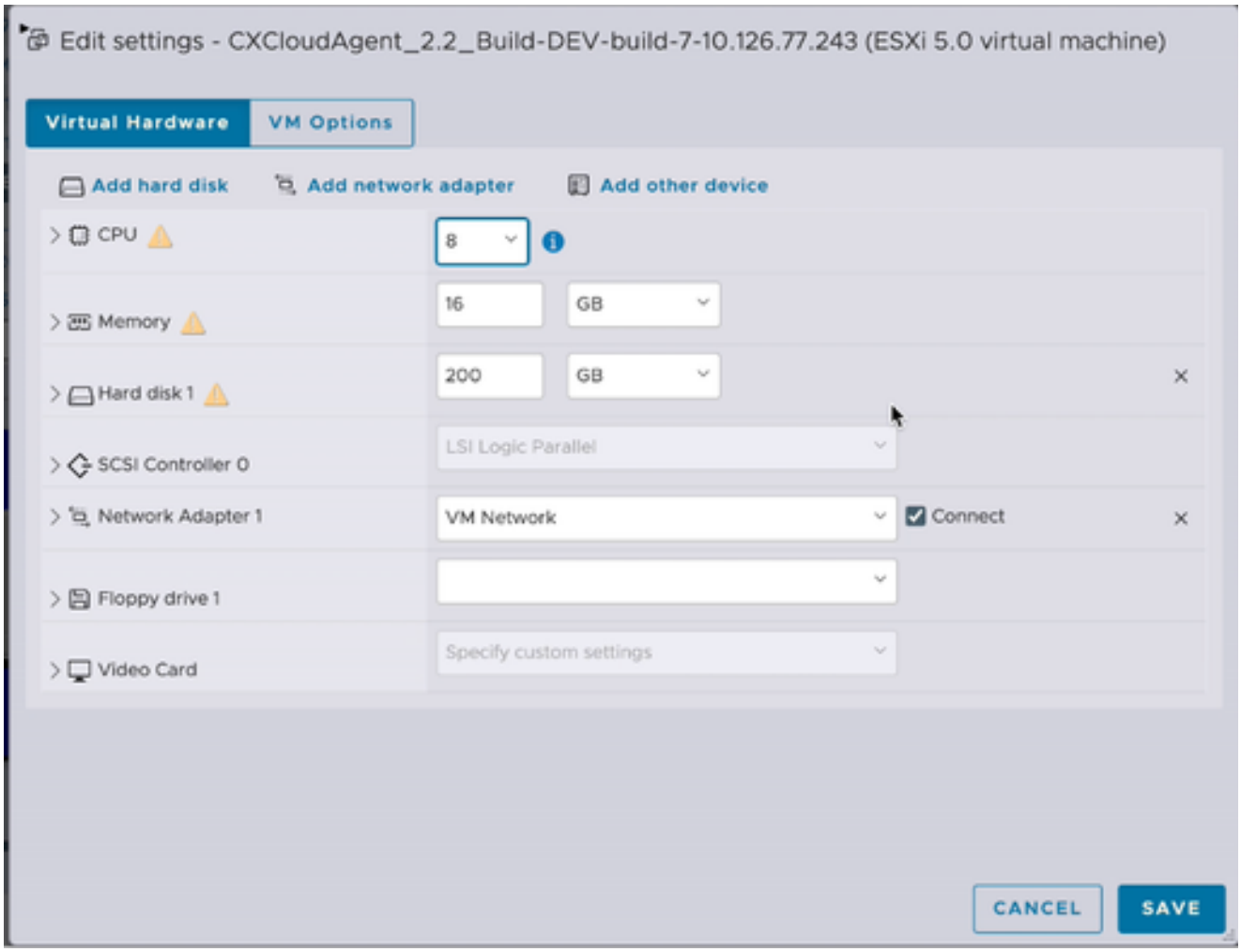


VM di destinazione

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

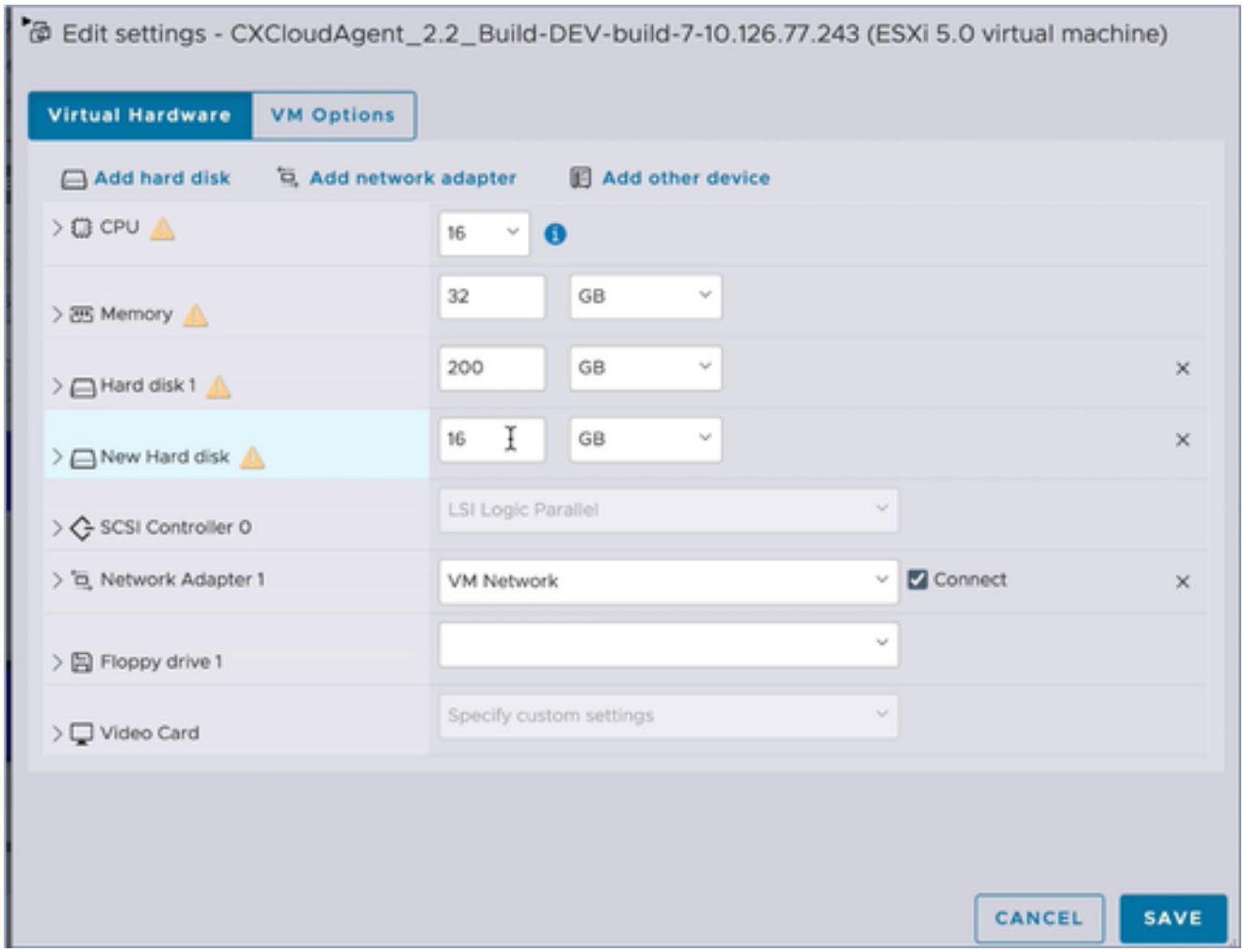


Azioni



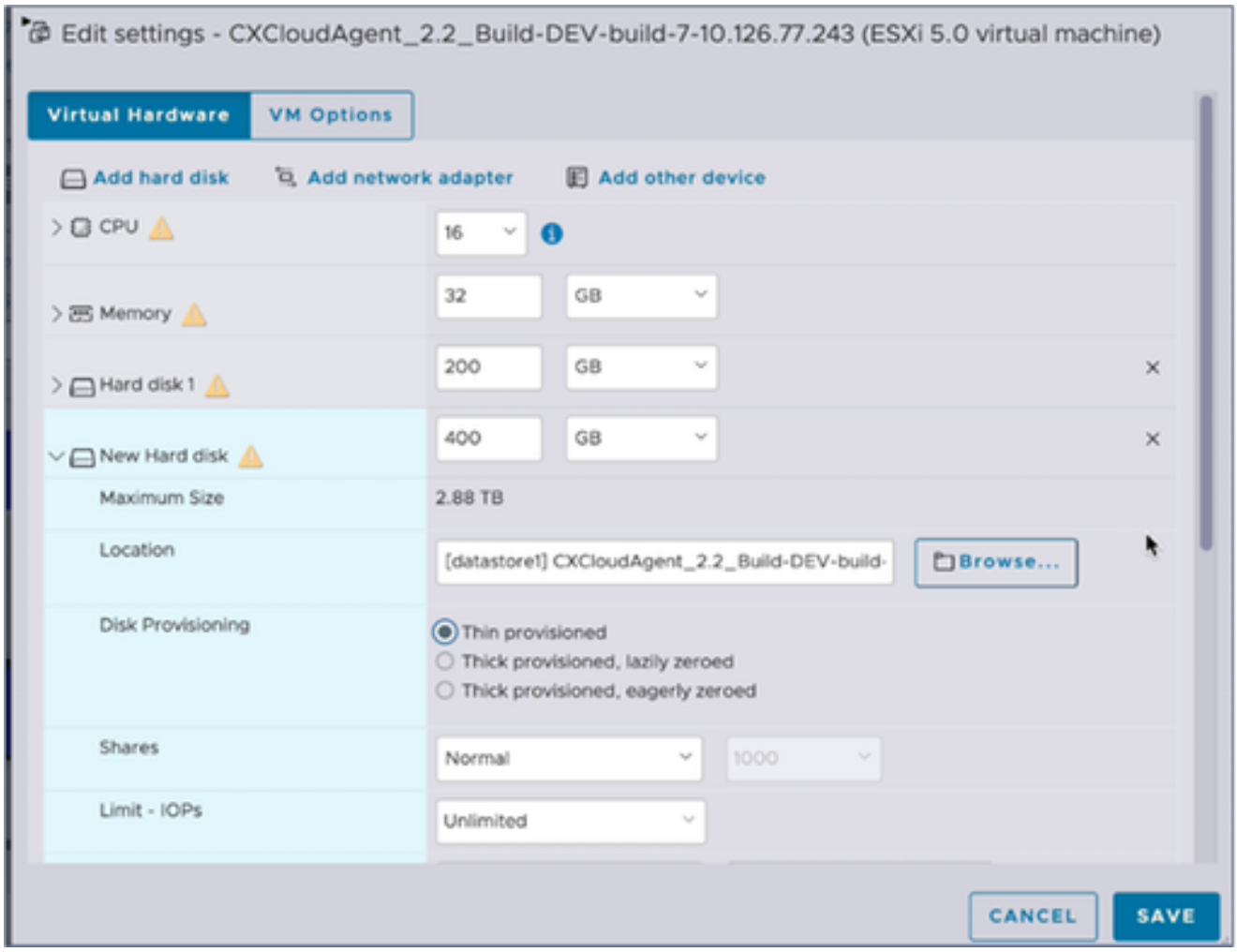
Modifica impostazioni

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
   Grande: 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.



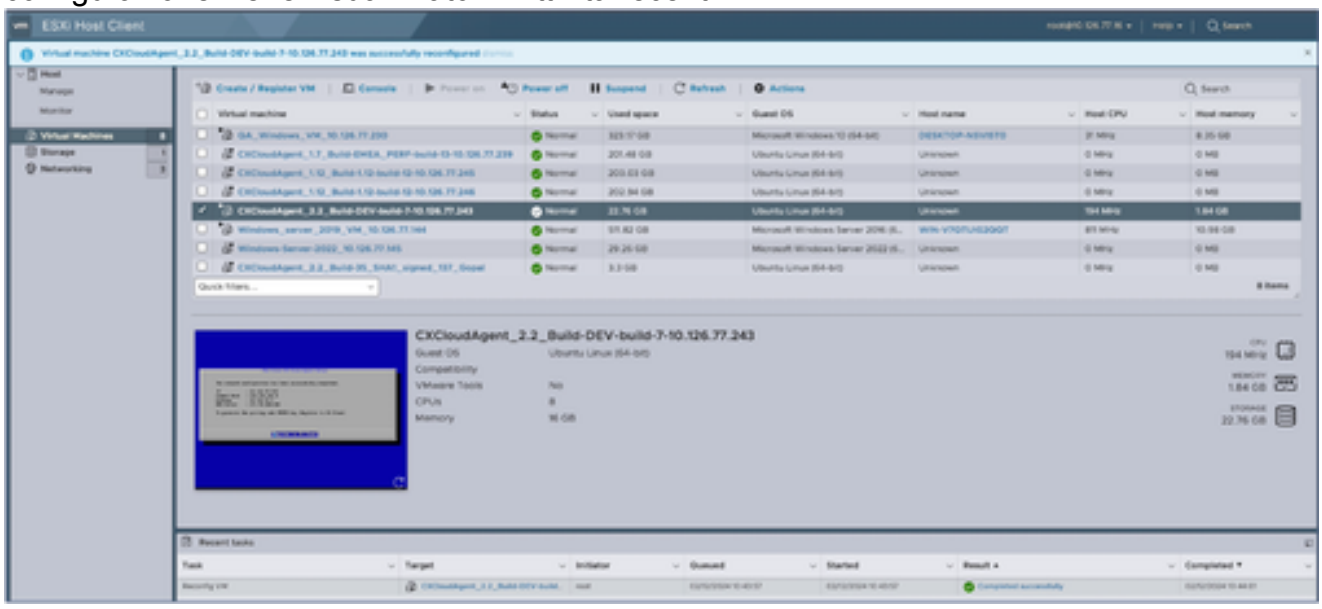
Modifica impostazioni

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.



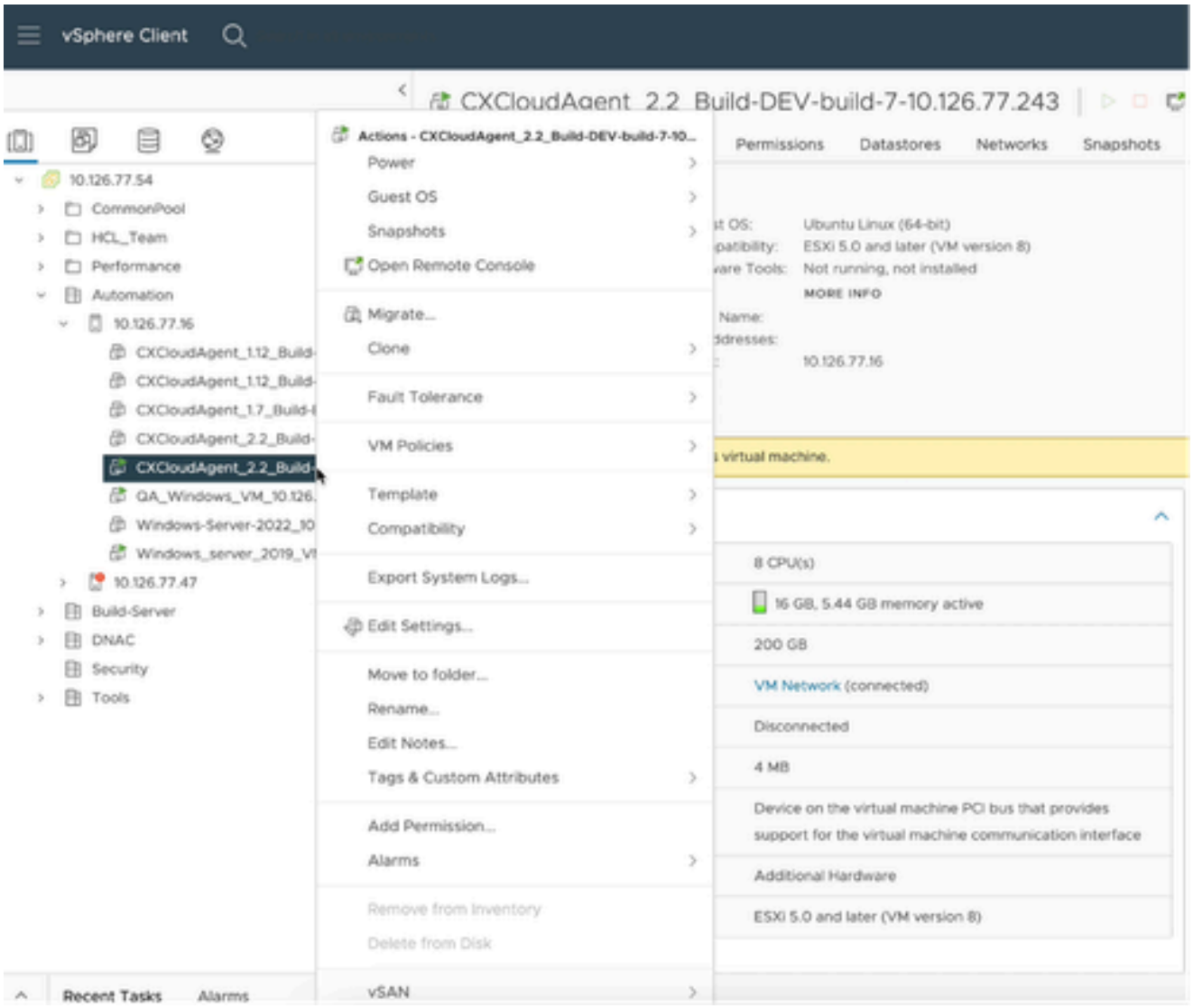
Attività recenti

Riconfigurazione mediante Web Client vCenter

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

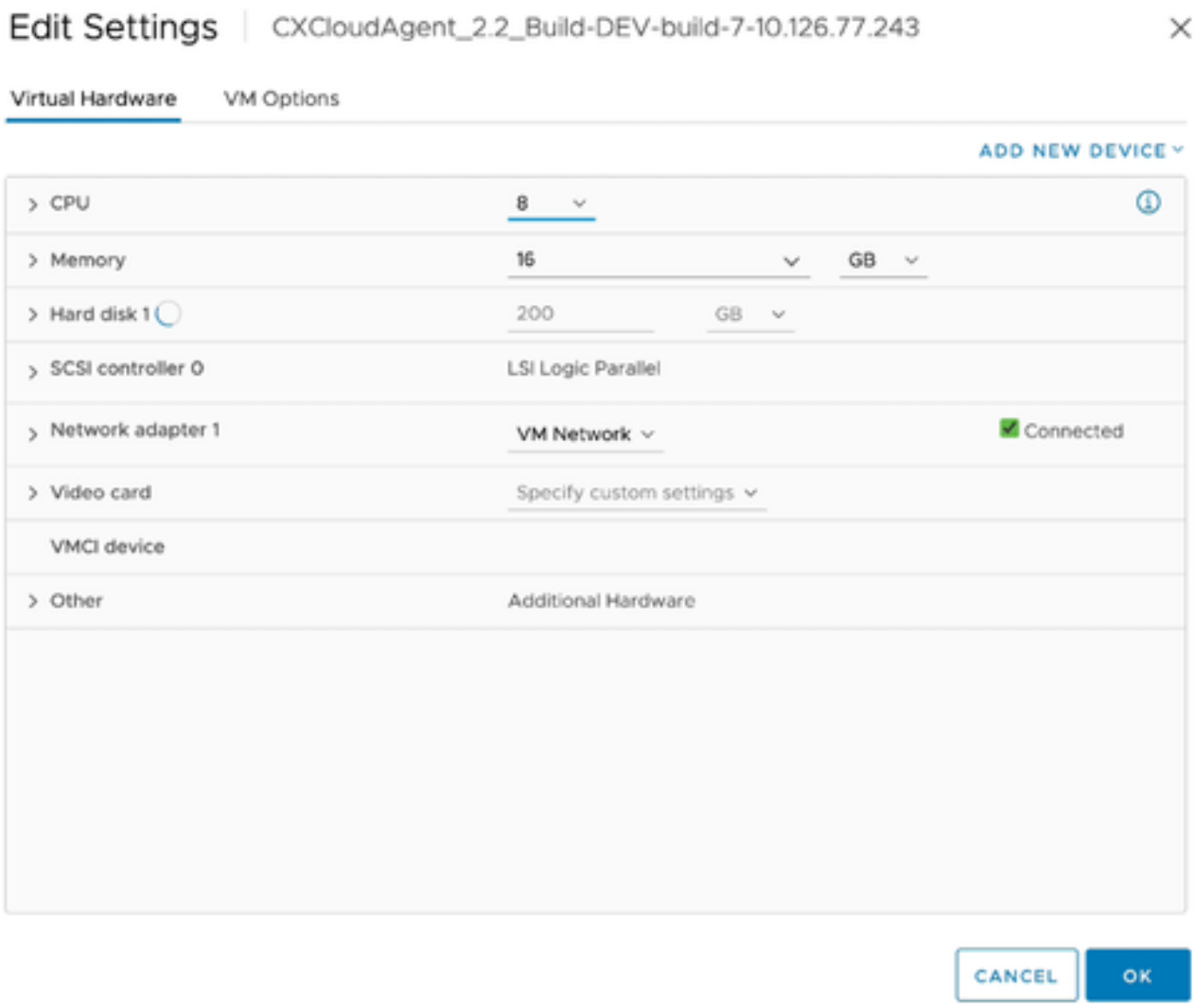
vCenter

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



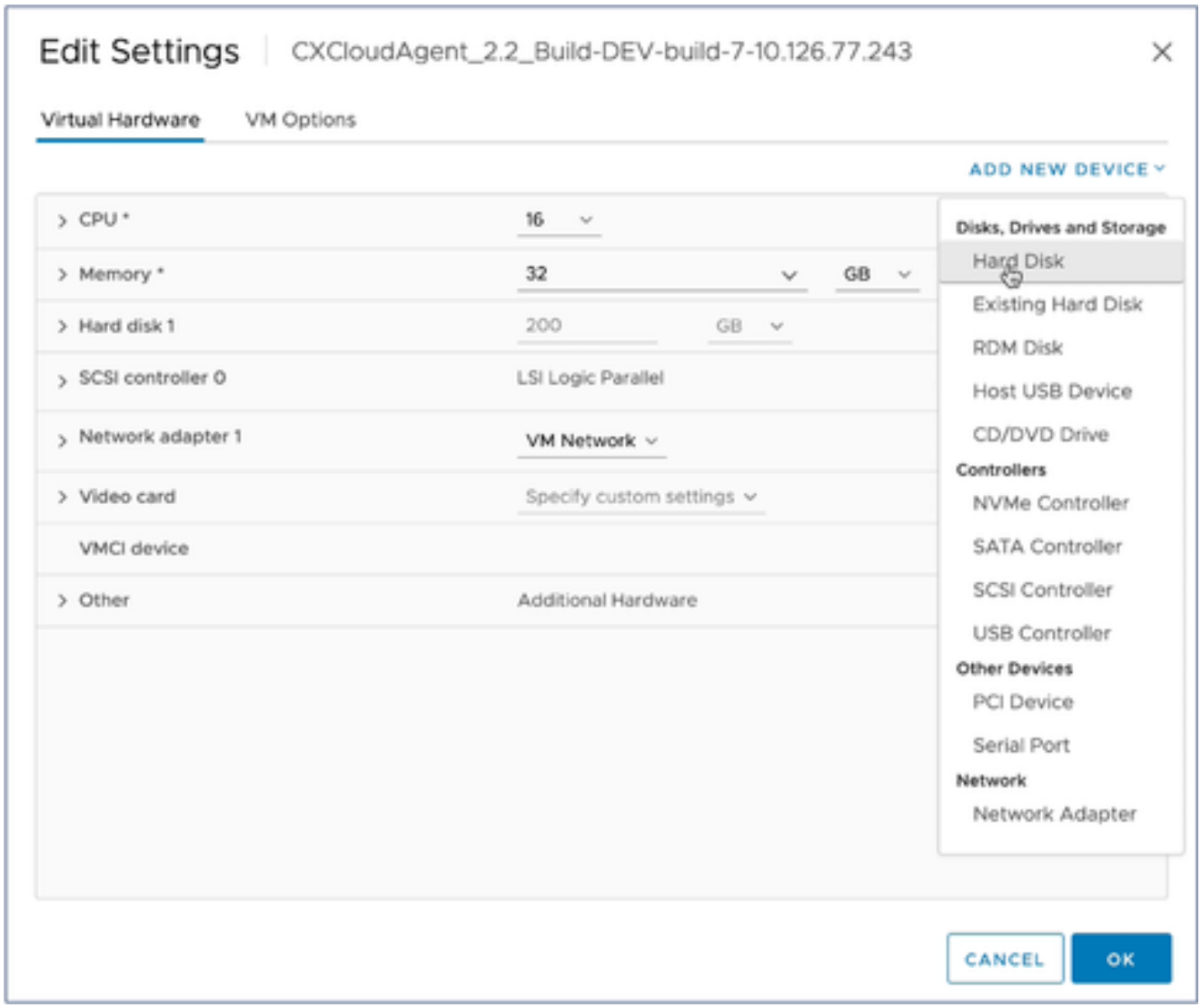
Elenco di macchine virtuali

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.



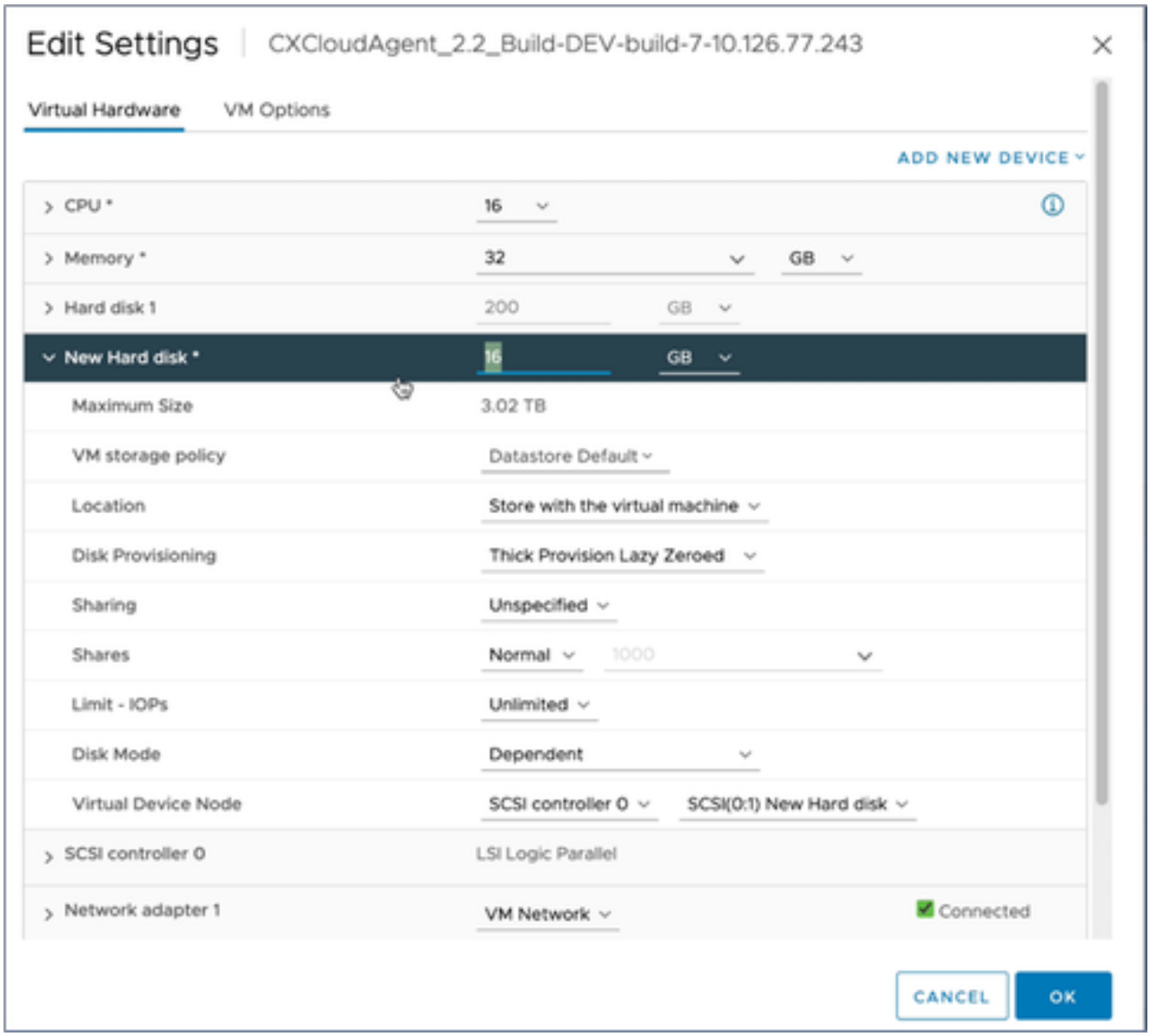
Modifica impostazioni

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
   Grande: 64 GB



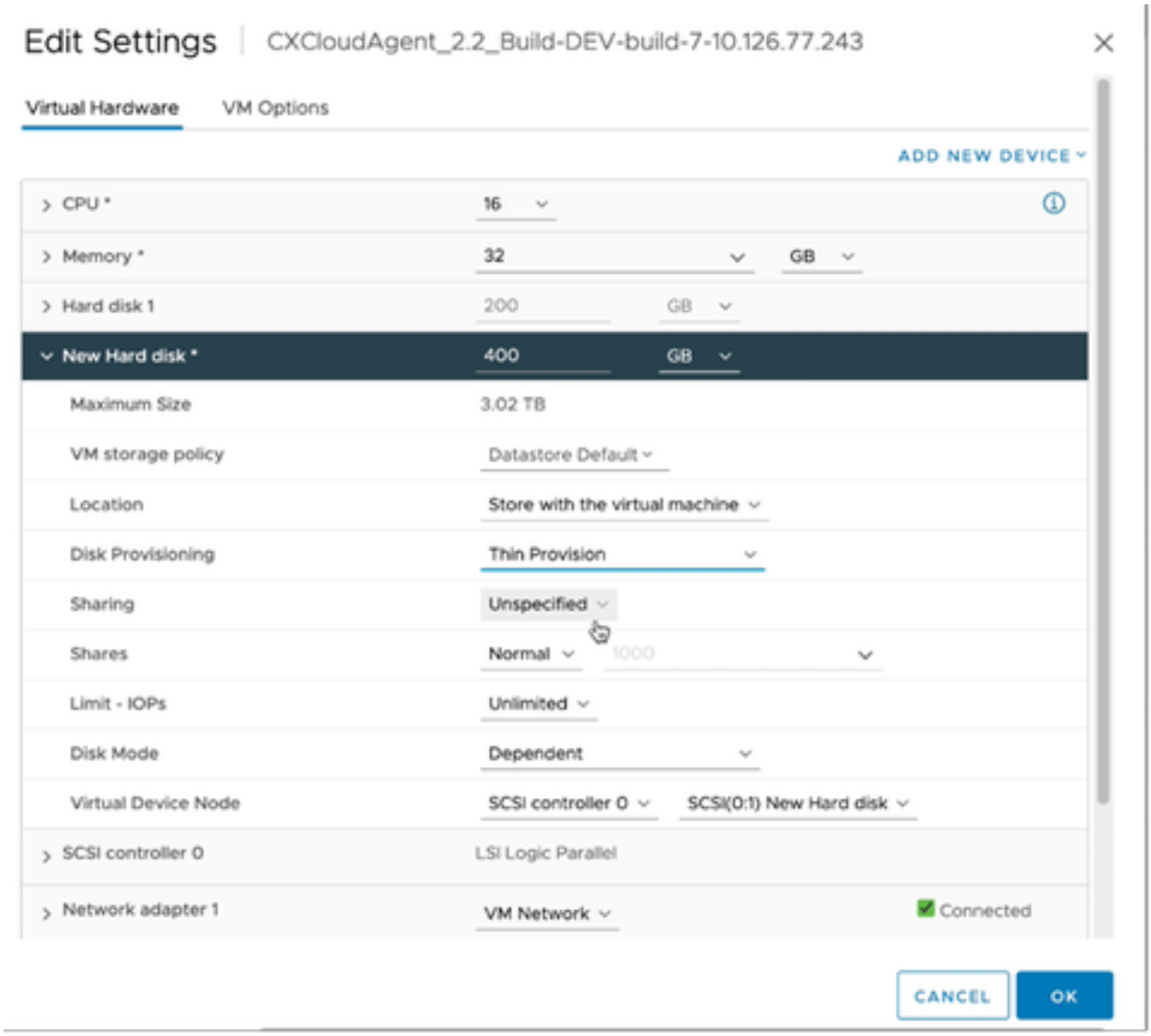
Modifica impostazioni

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 CX:

- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0
- Installazione di VMware vSphere/vCenter Web Client ESXi 6.0 o Web Client vCenter
- Oracle Virtual Box 7.0.12
- Installazione di Microsoft Hyper-V

Implementazione dell'OVA

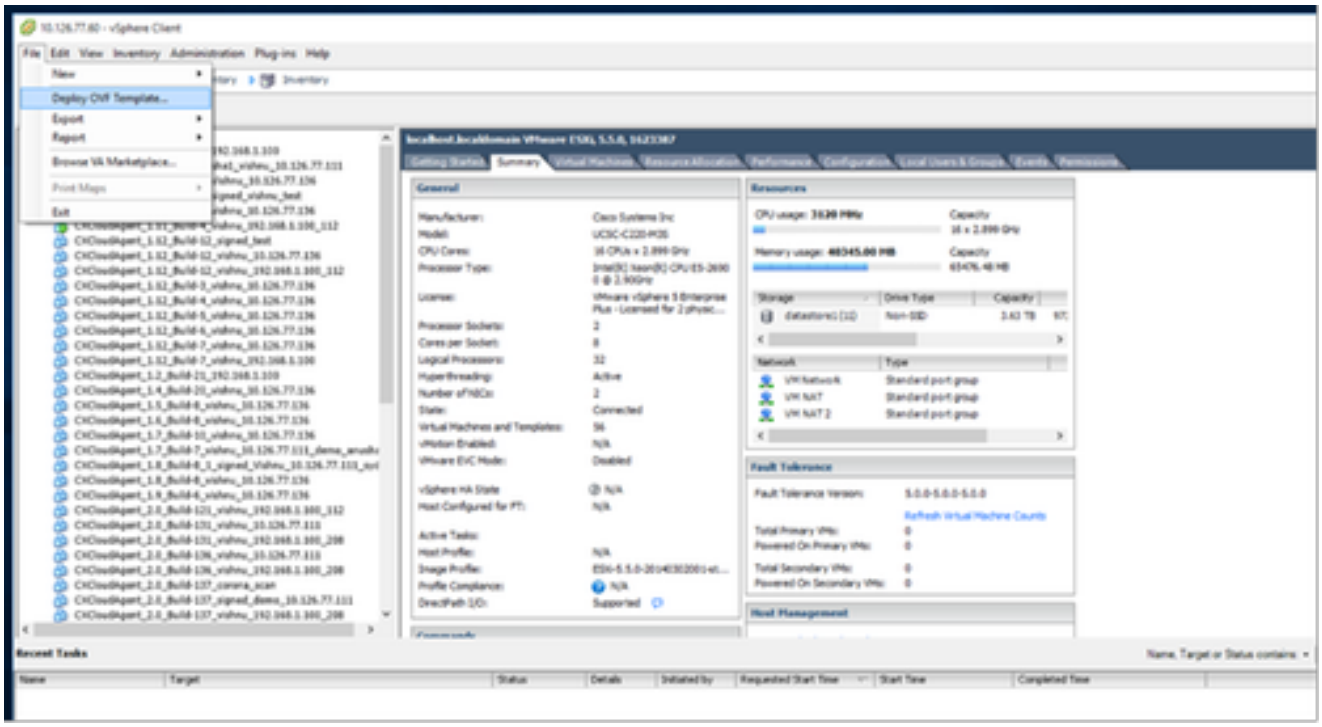
Installazione del thick client ESXi 5.5/6.0

Questo client consente la distribuzione degli OVA dell'agente CX mediante il client thick vSphere.

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

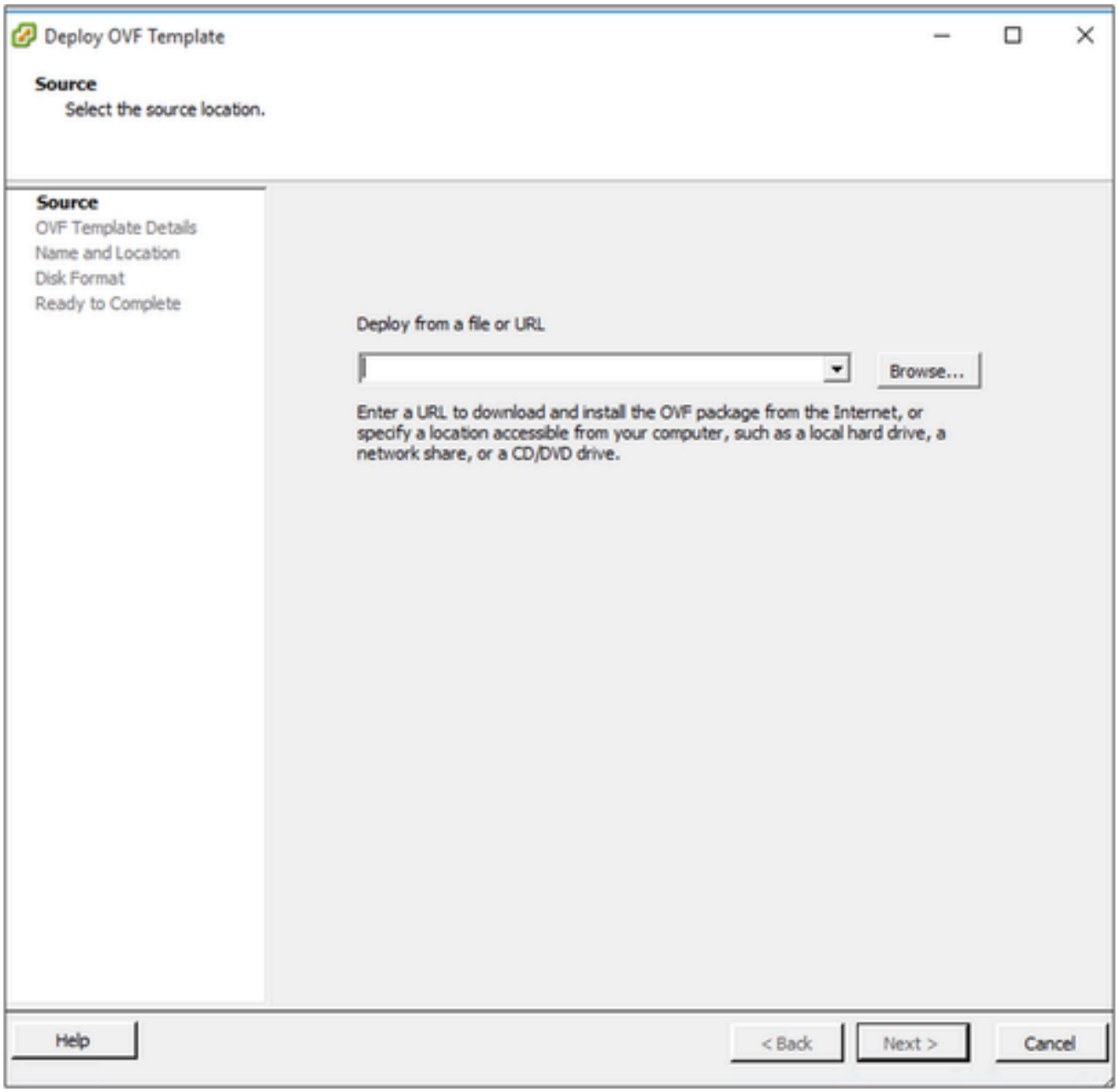
Accesso

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



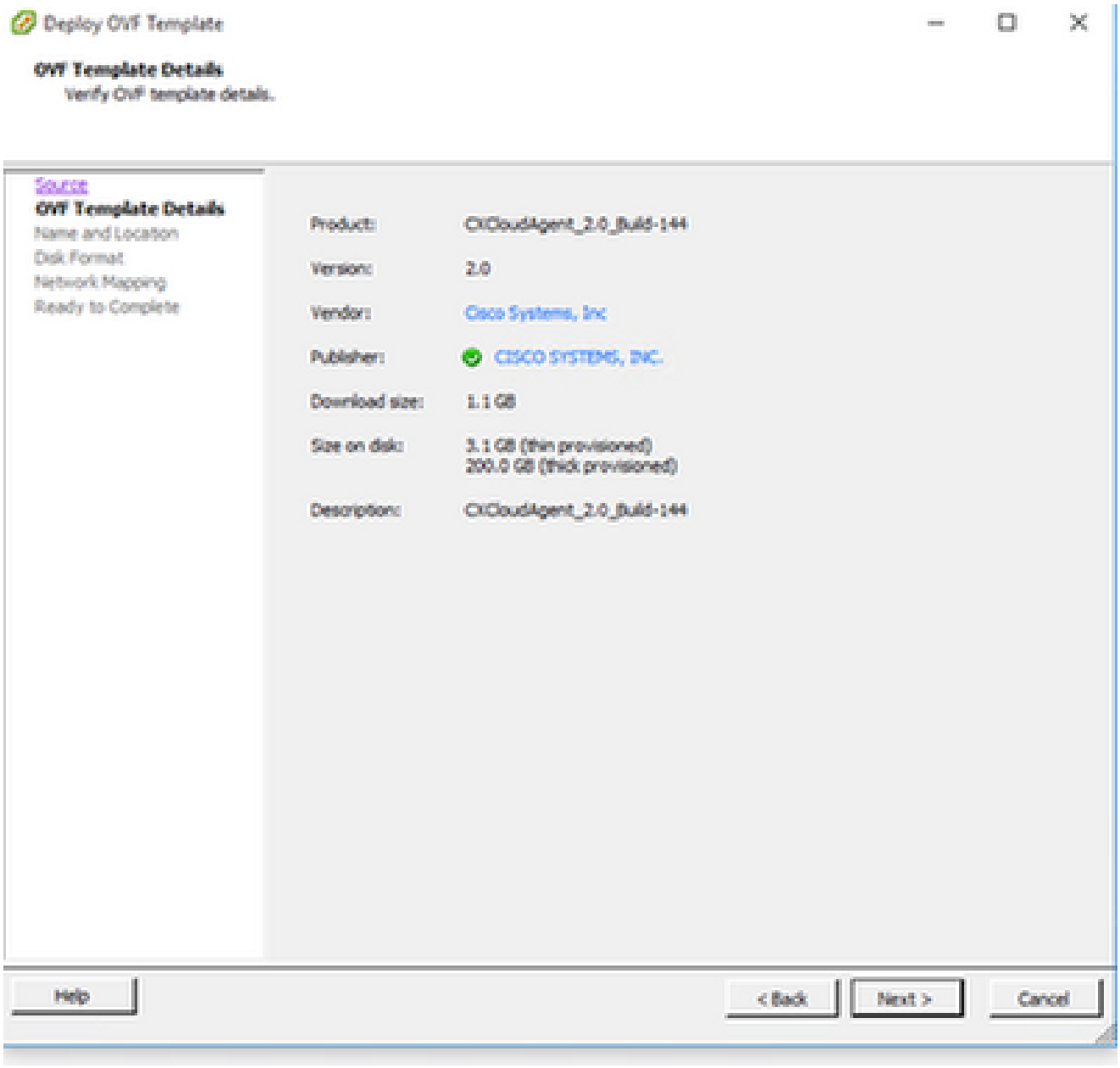
Client vSphere

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



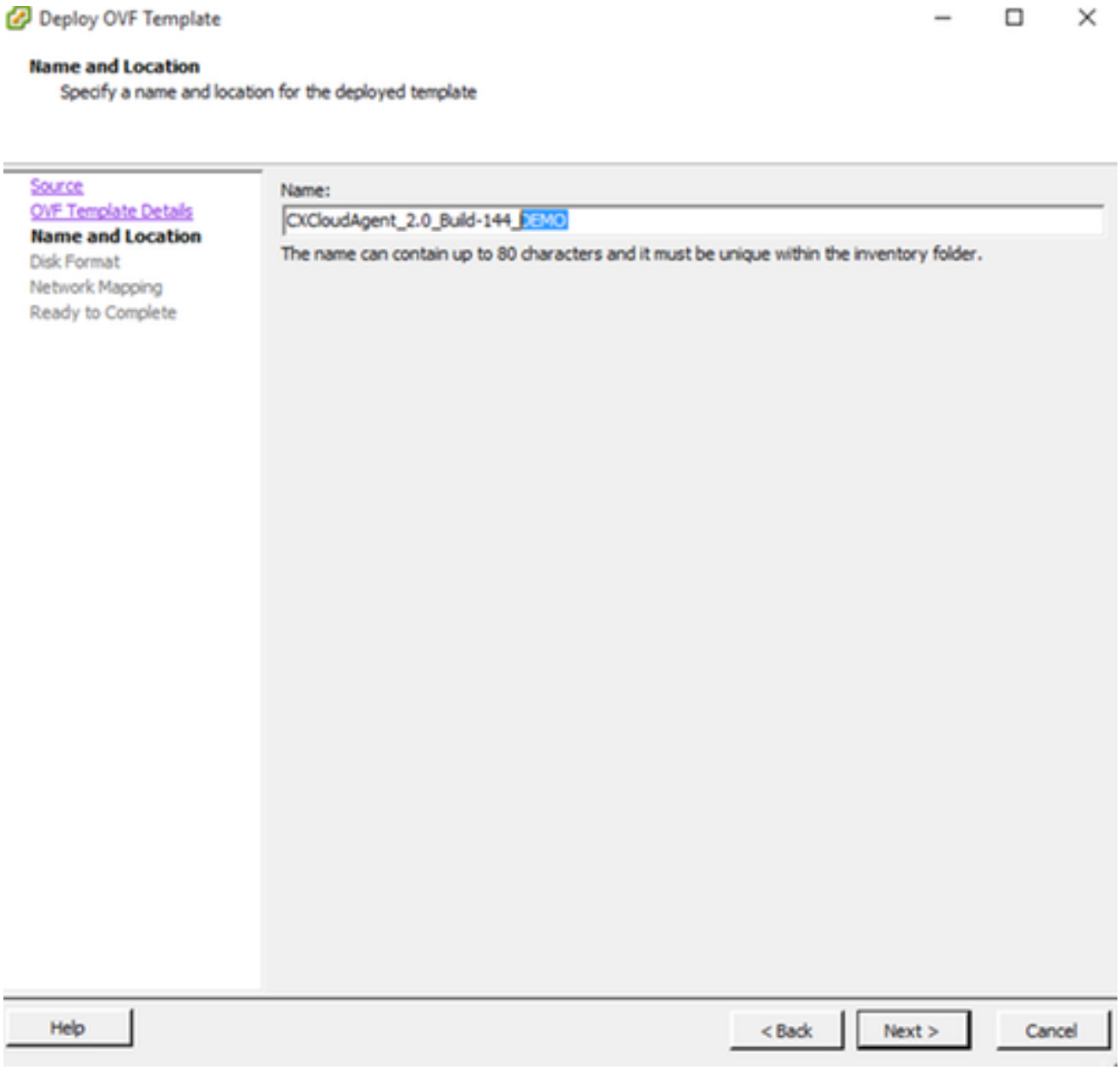
Percorso OVA

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



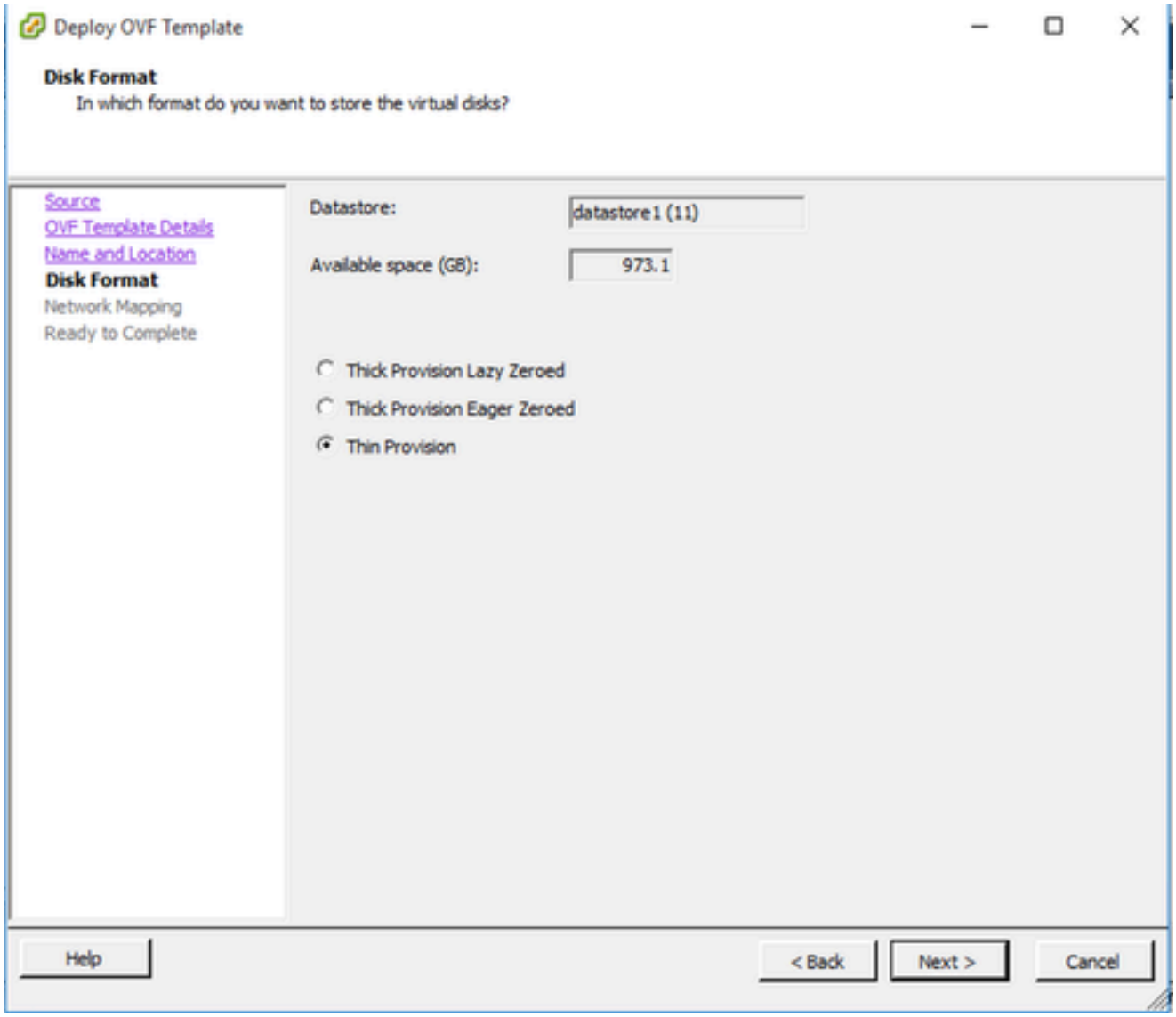
Dettagli del modello

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



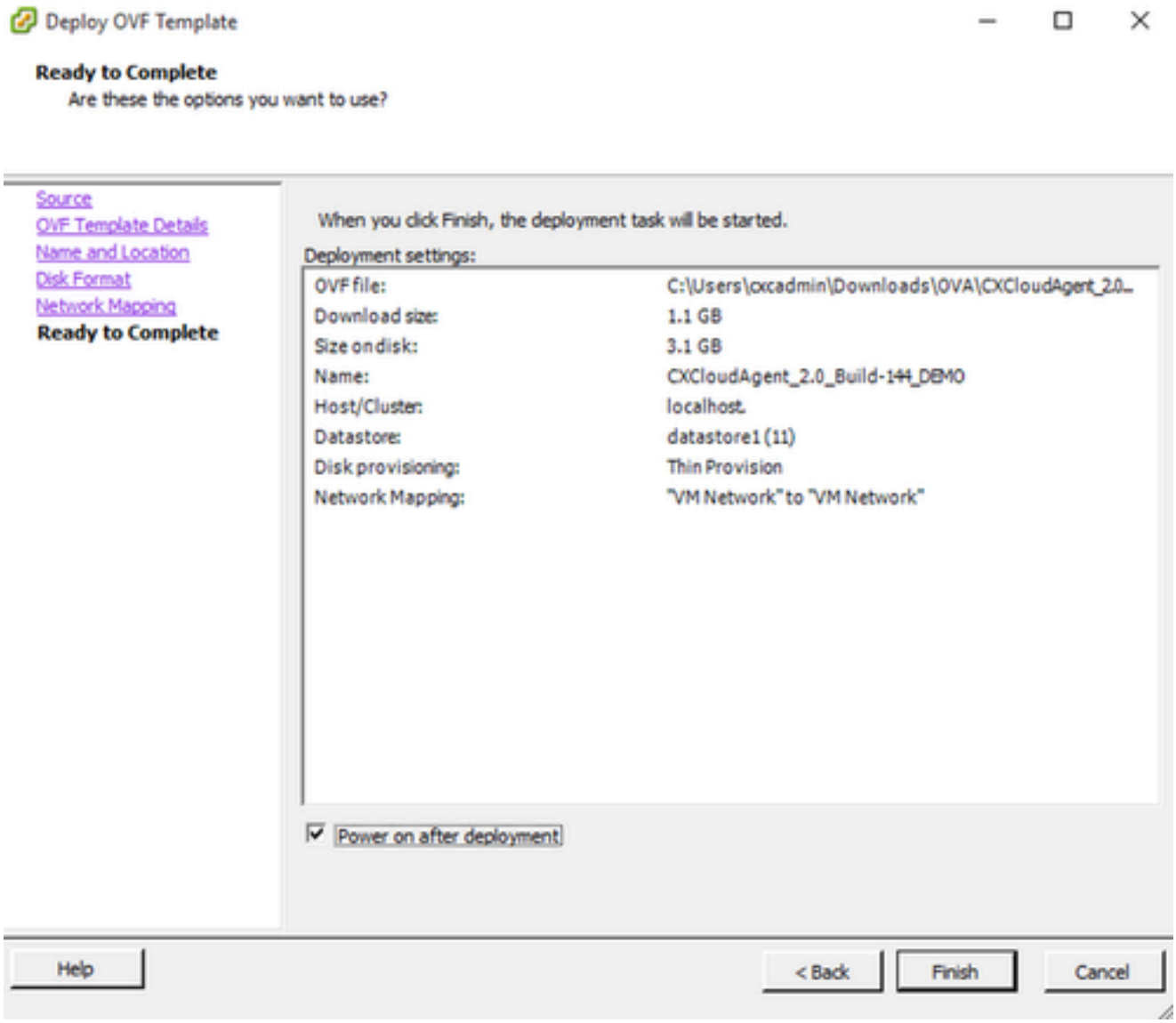
Nome e posizione

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



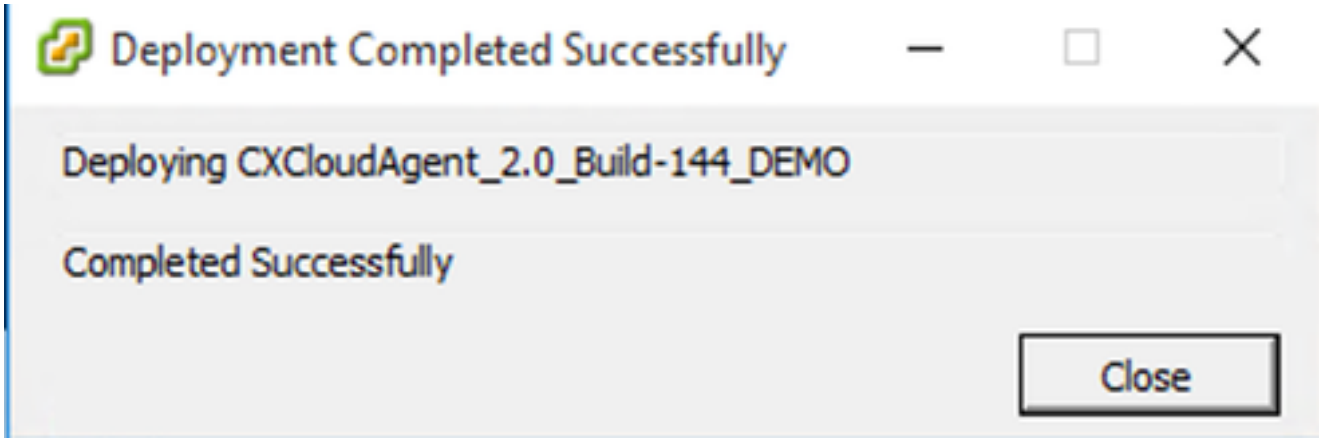
Formato del disco

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.



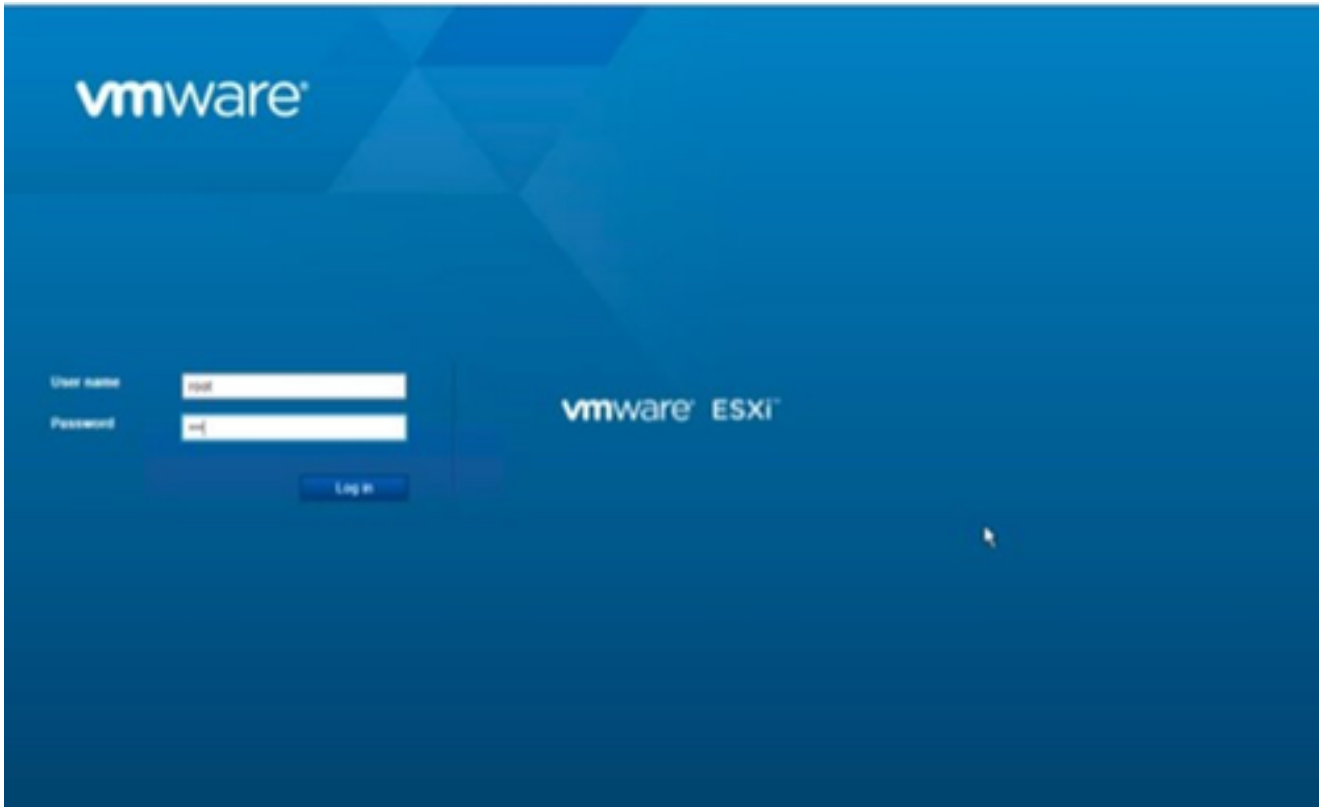
Distribuzione completata

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

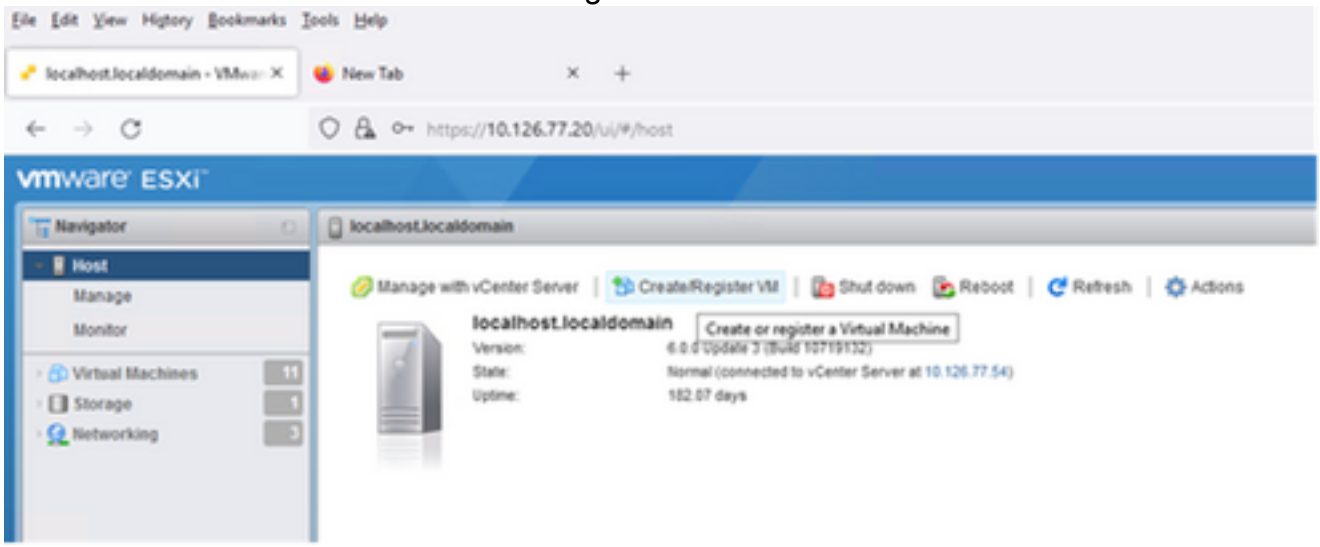
Questo client distribuisce gli OVA di CX Cloud utilizzando il Web vSphere.

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



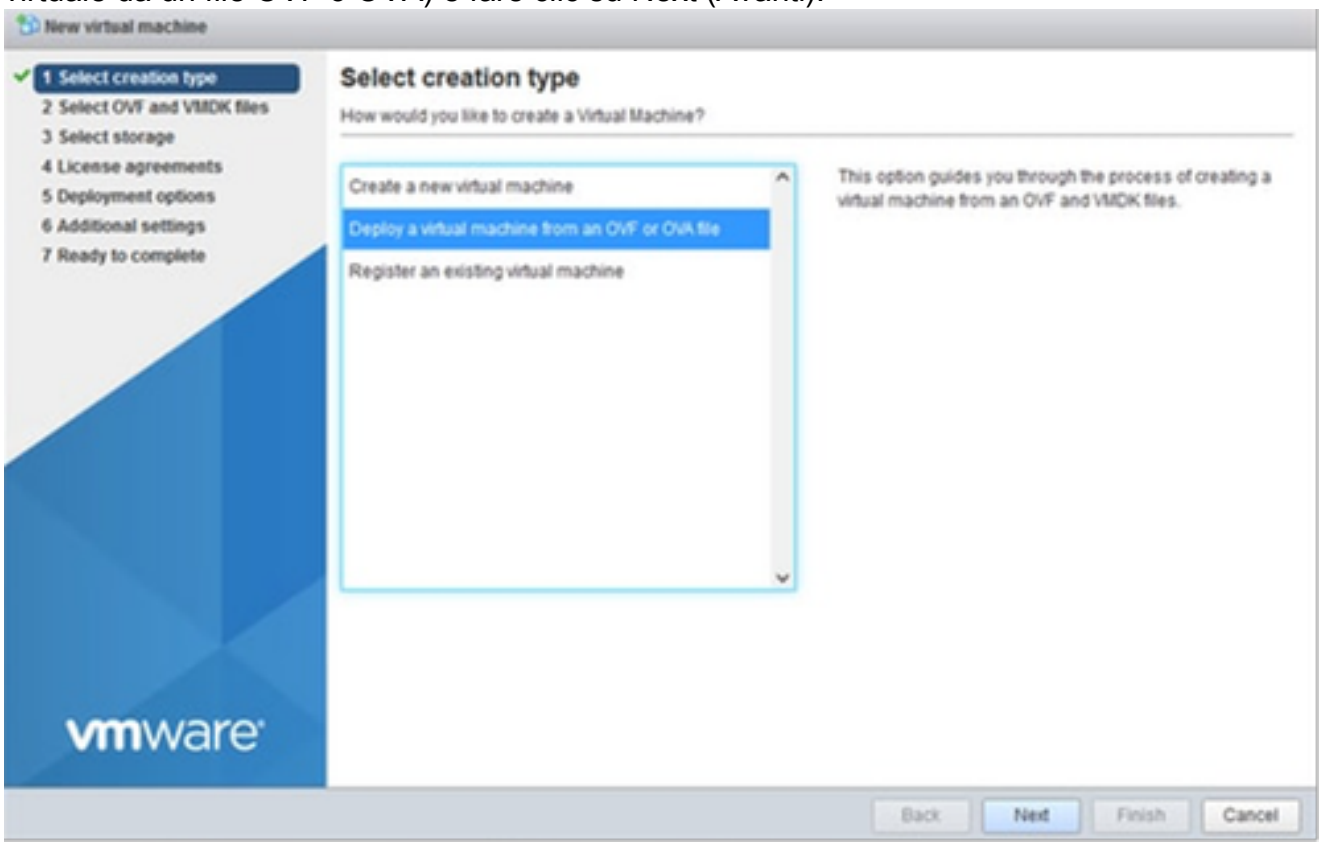
Accesso a VMware ESXi

2. Selezionare Virtual Machine > Create/Register VM.



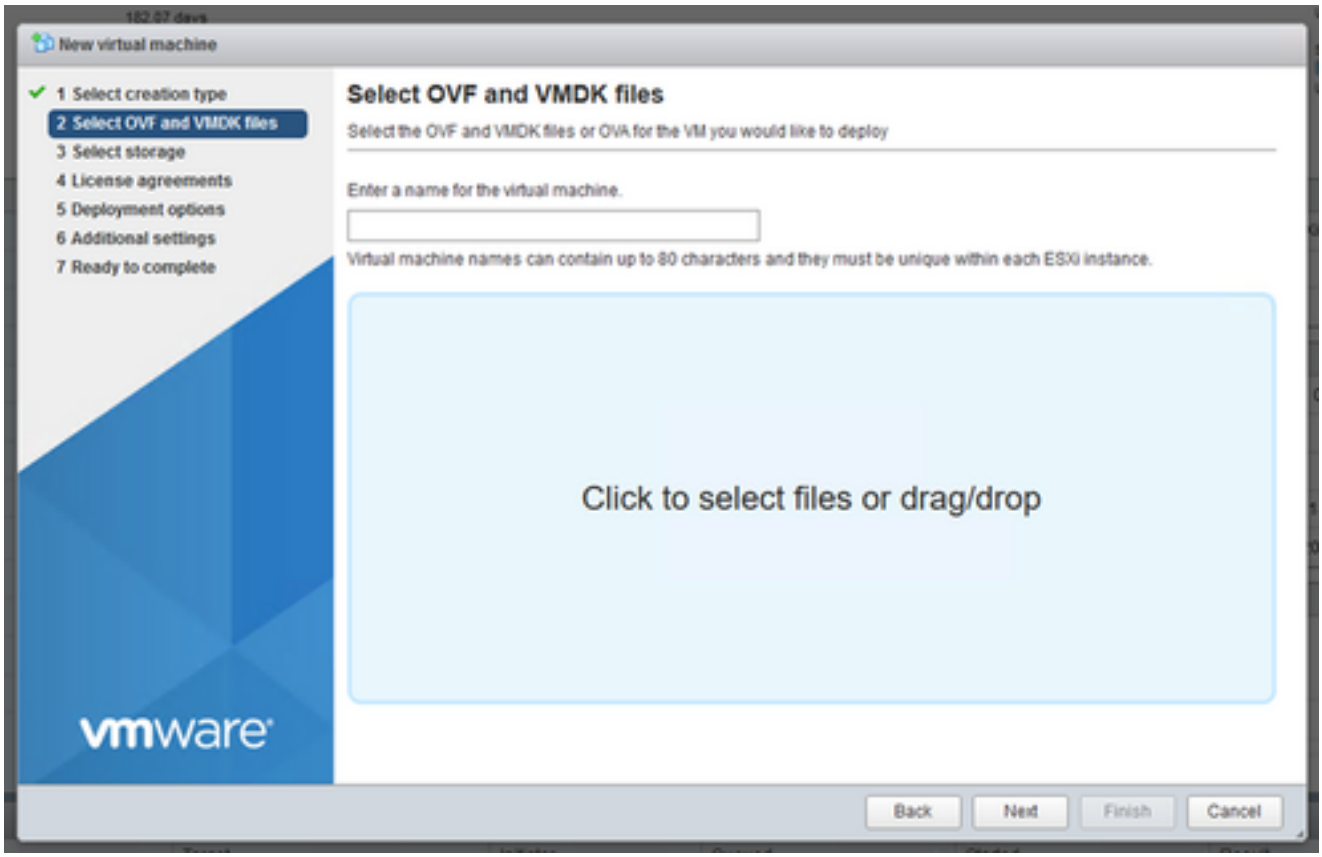
Creazione della VM

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).



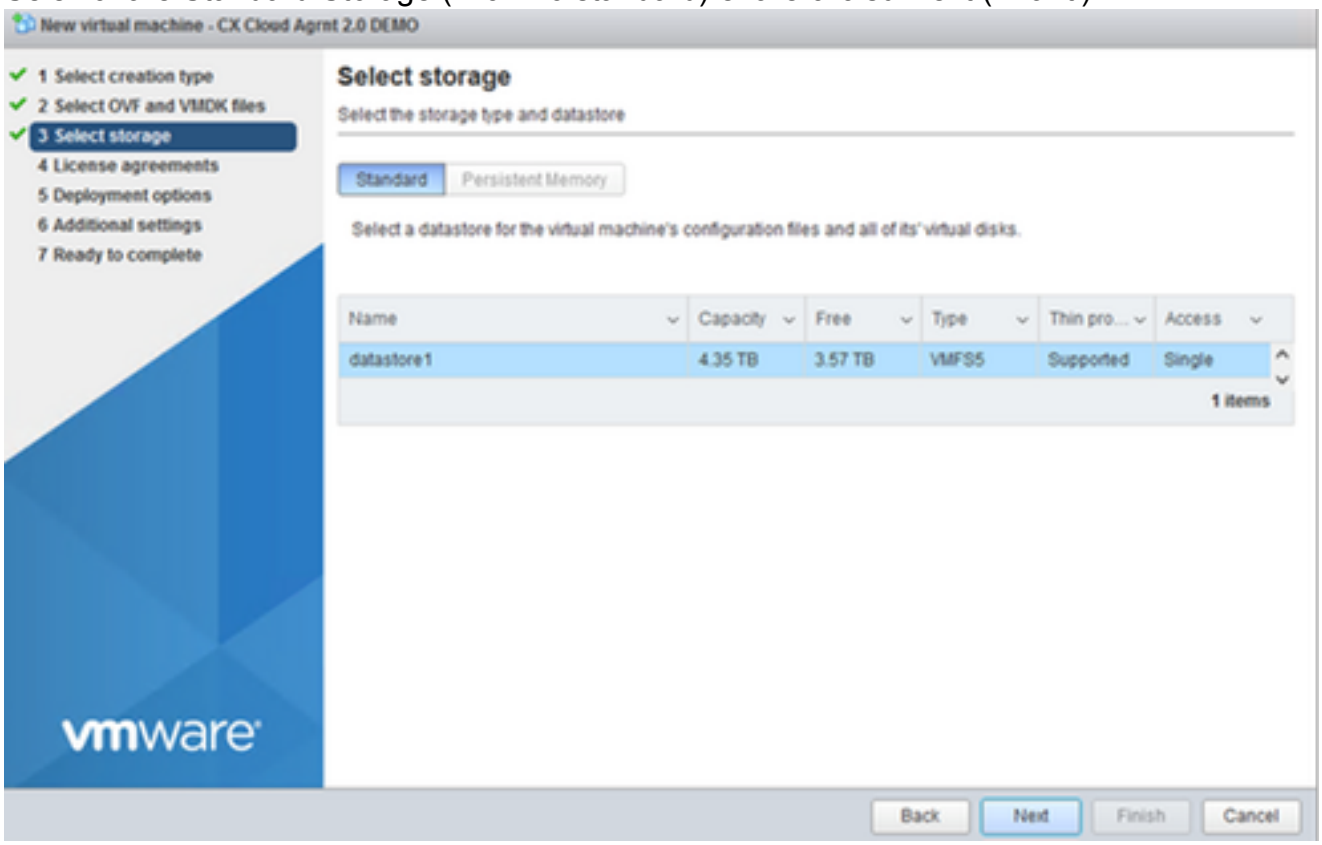
Seleziona tipo di creazione

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



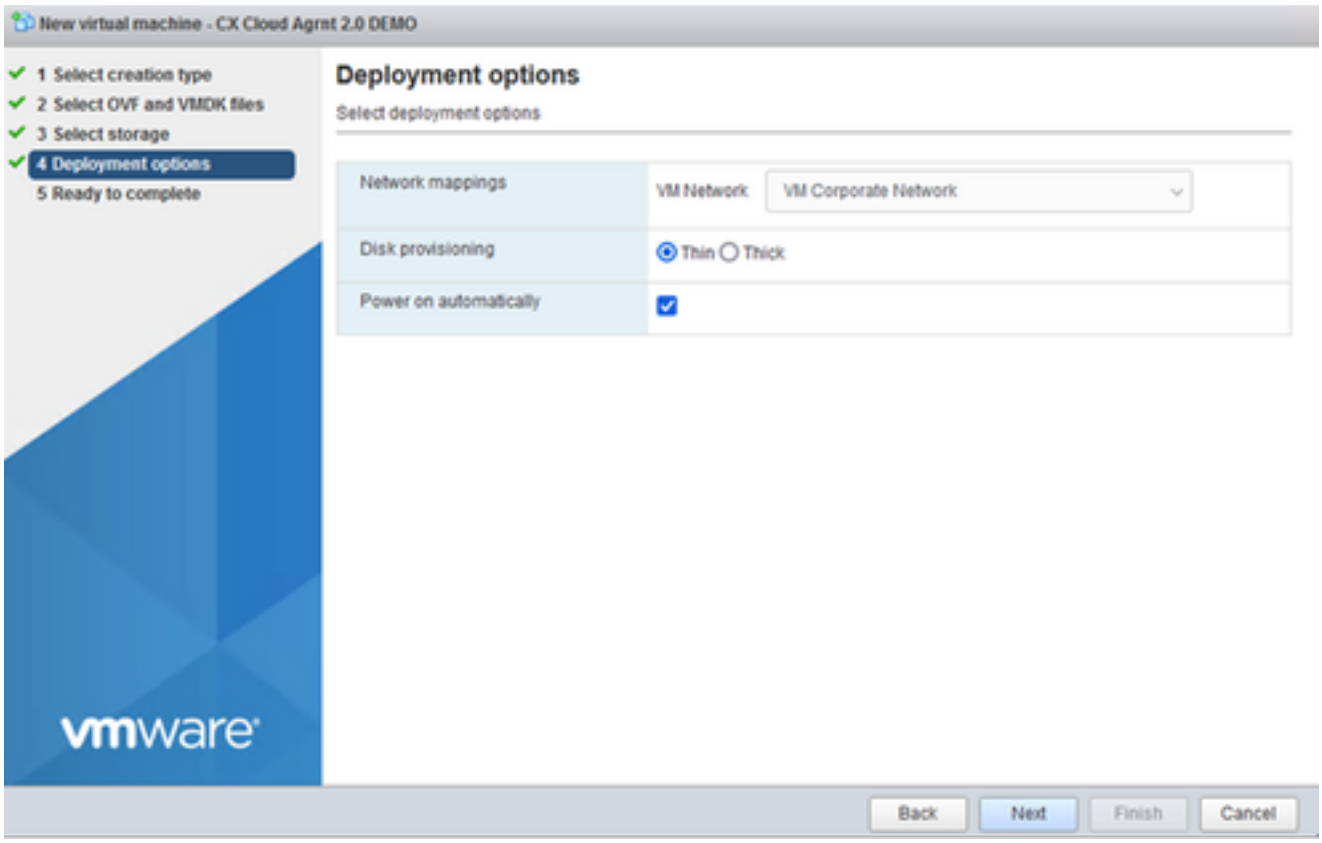
Selezione dell'OVA

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



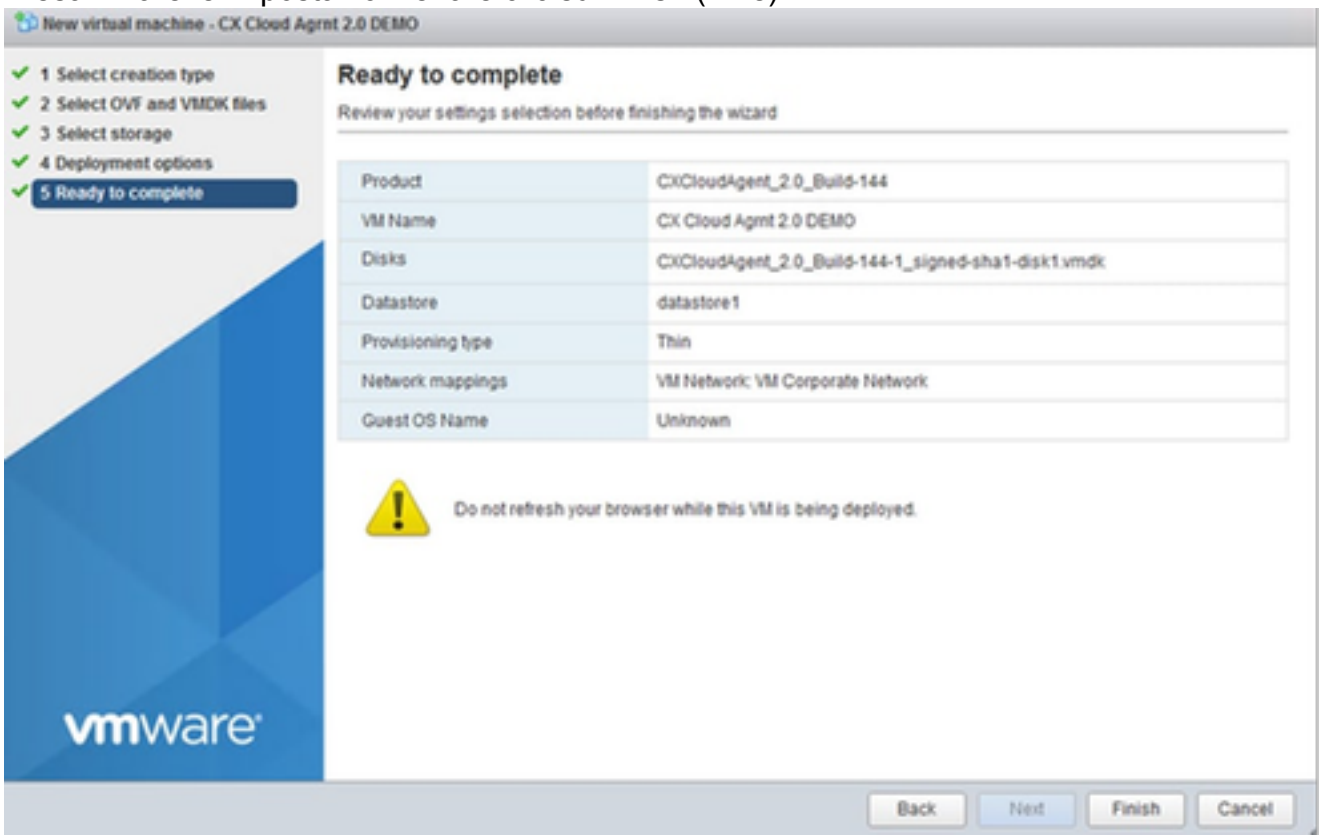
Selezione dell'archivio

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

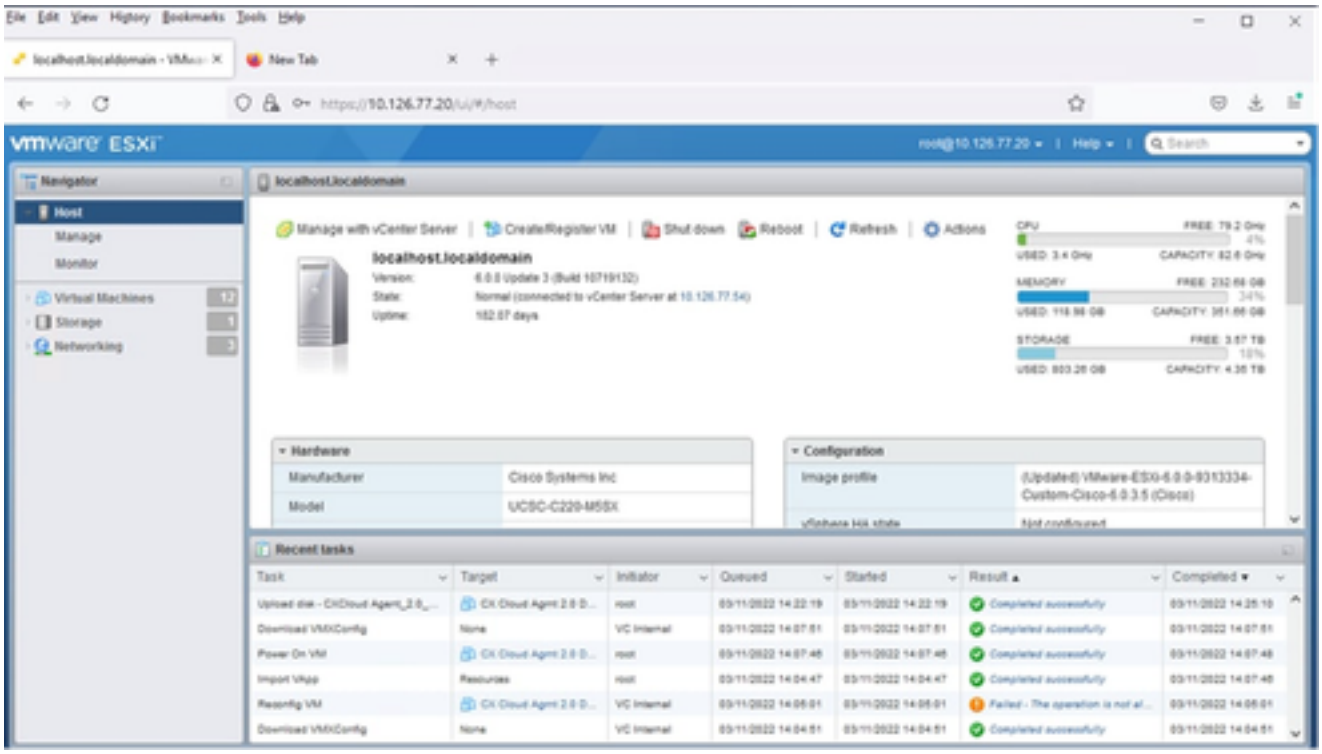


Opzioni di implementazione

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

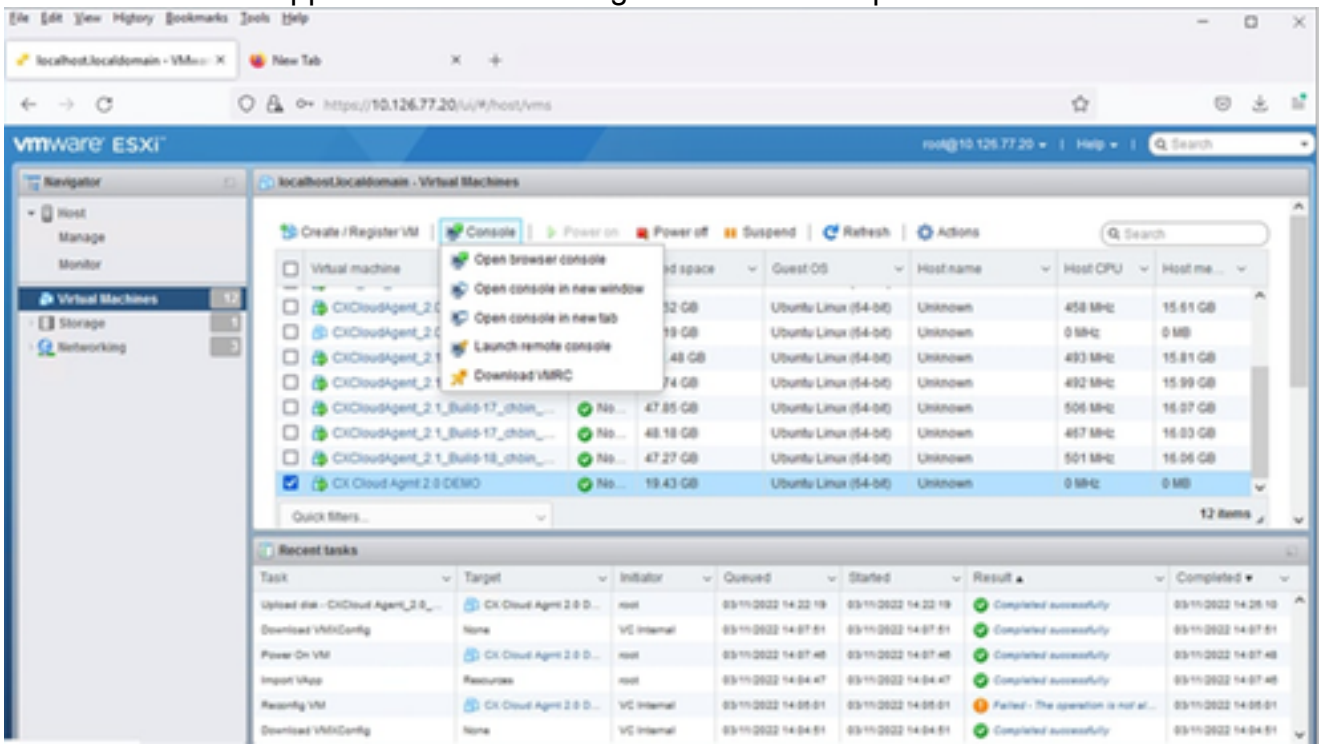


Pronto per il completamento



Procedura completata

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



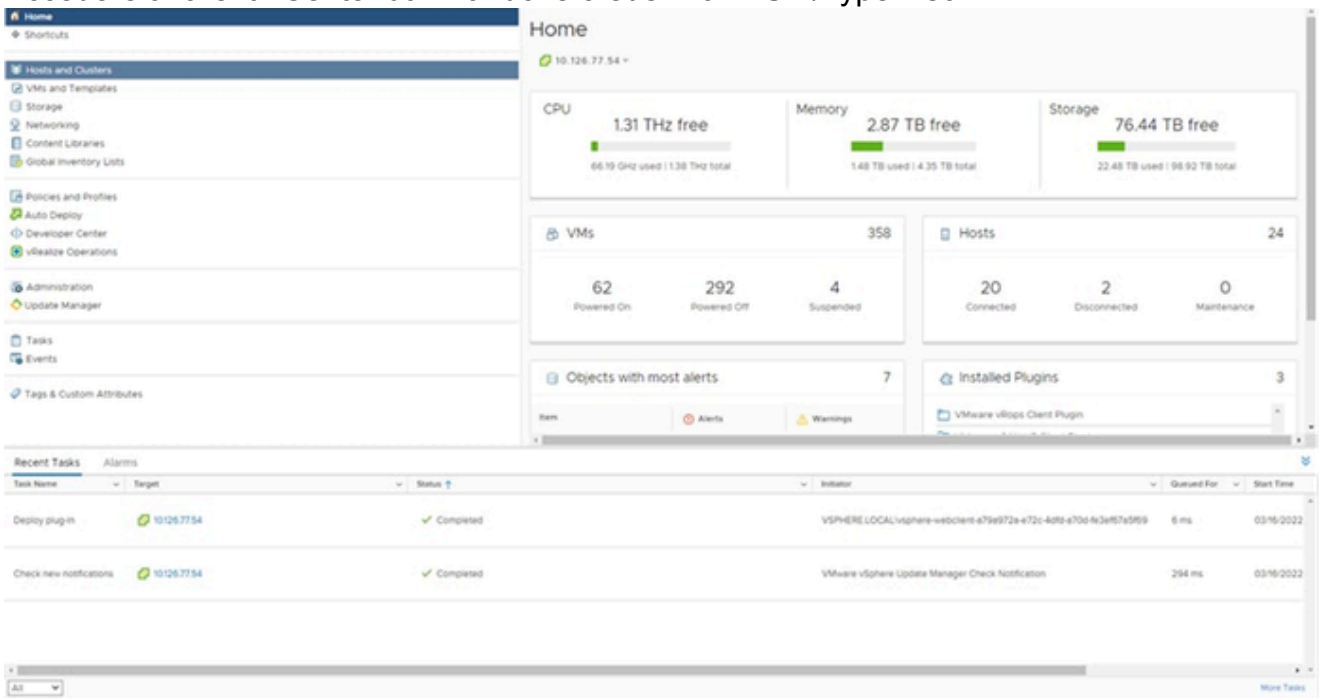
Console

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

Installazione del client Web vCenter

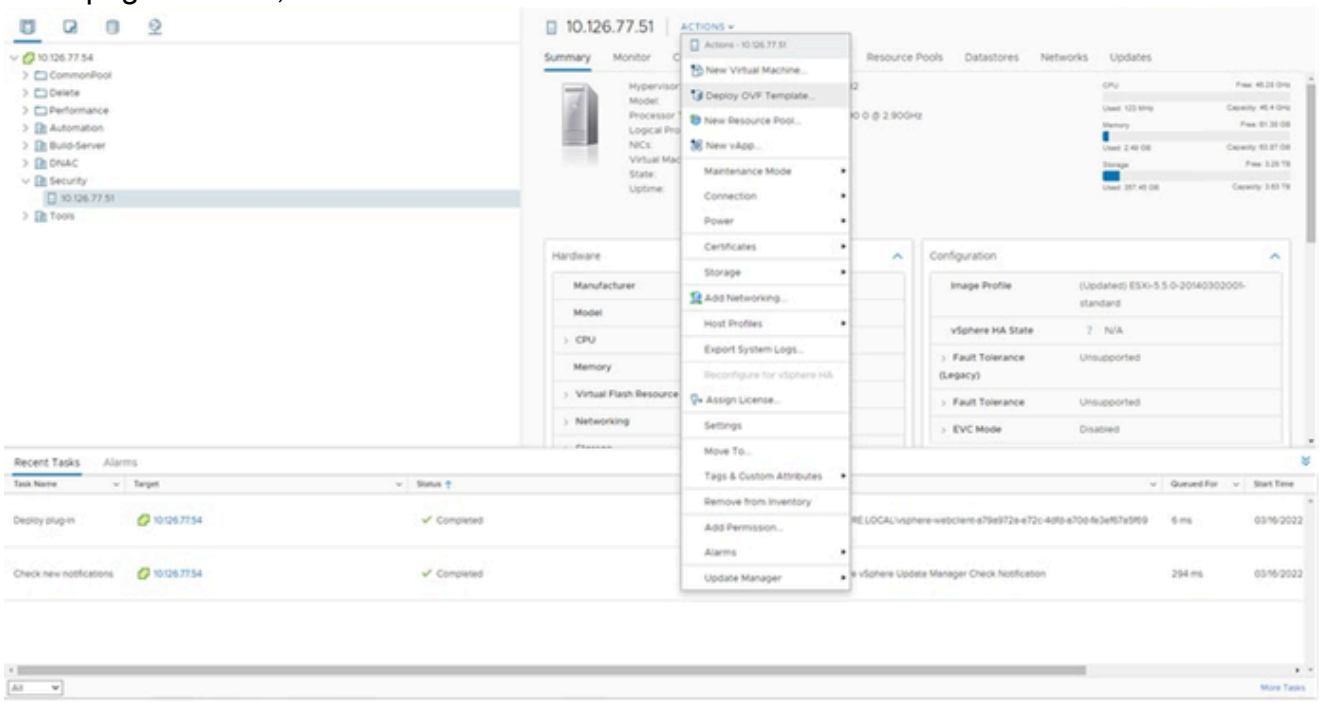
Questo client consente la distribuzione degli OVA dell'agente CX mediante il vCenter del client Web.

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



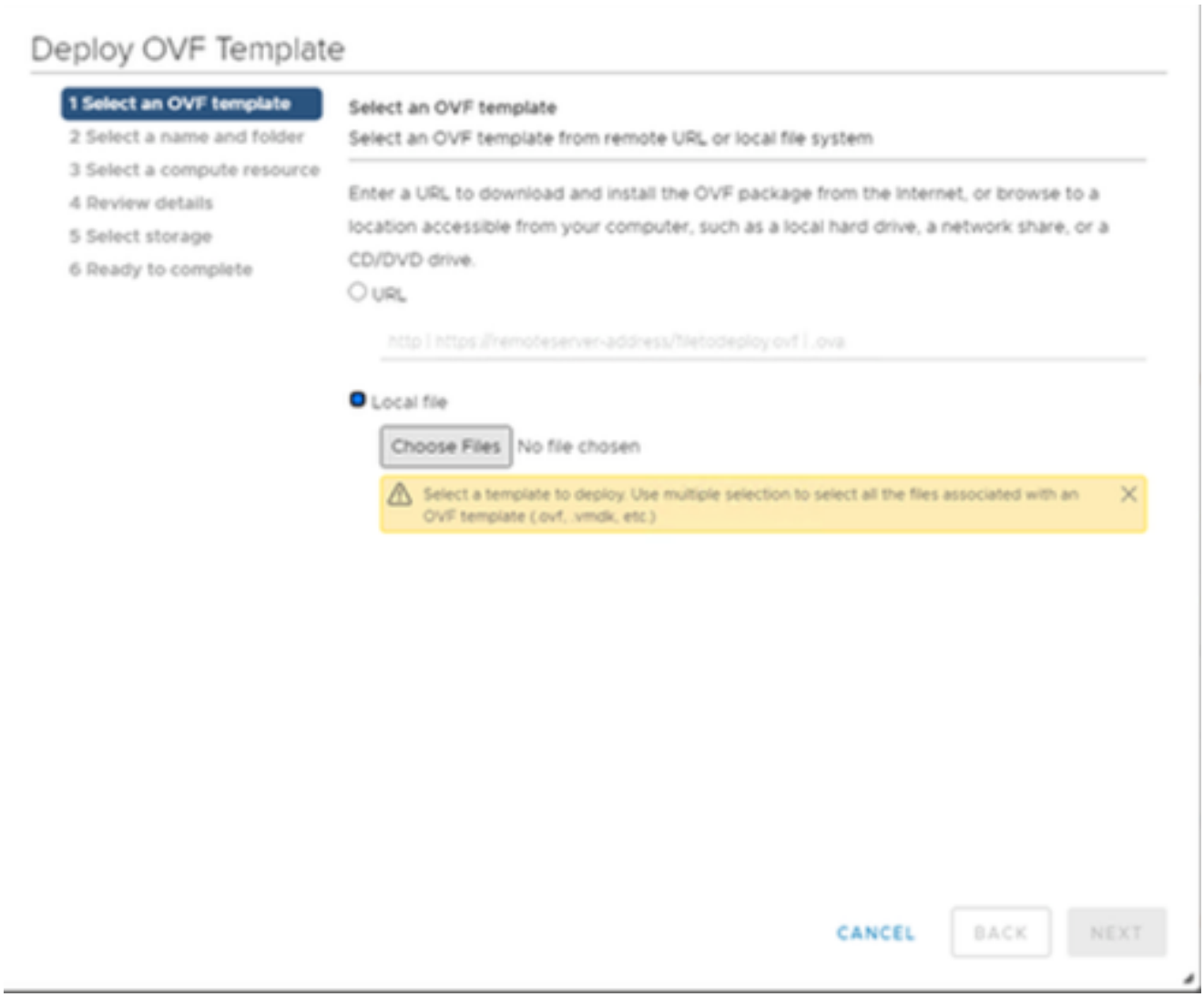
Home page

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



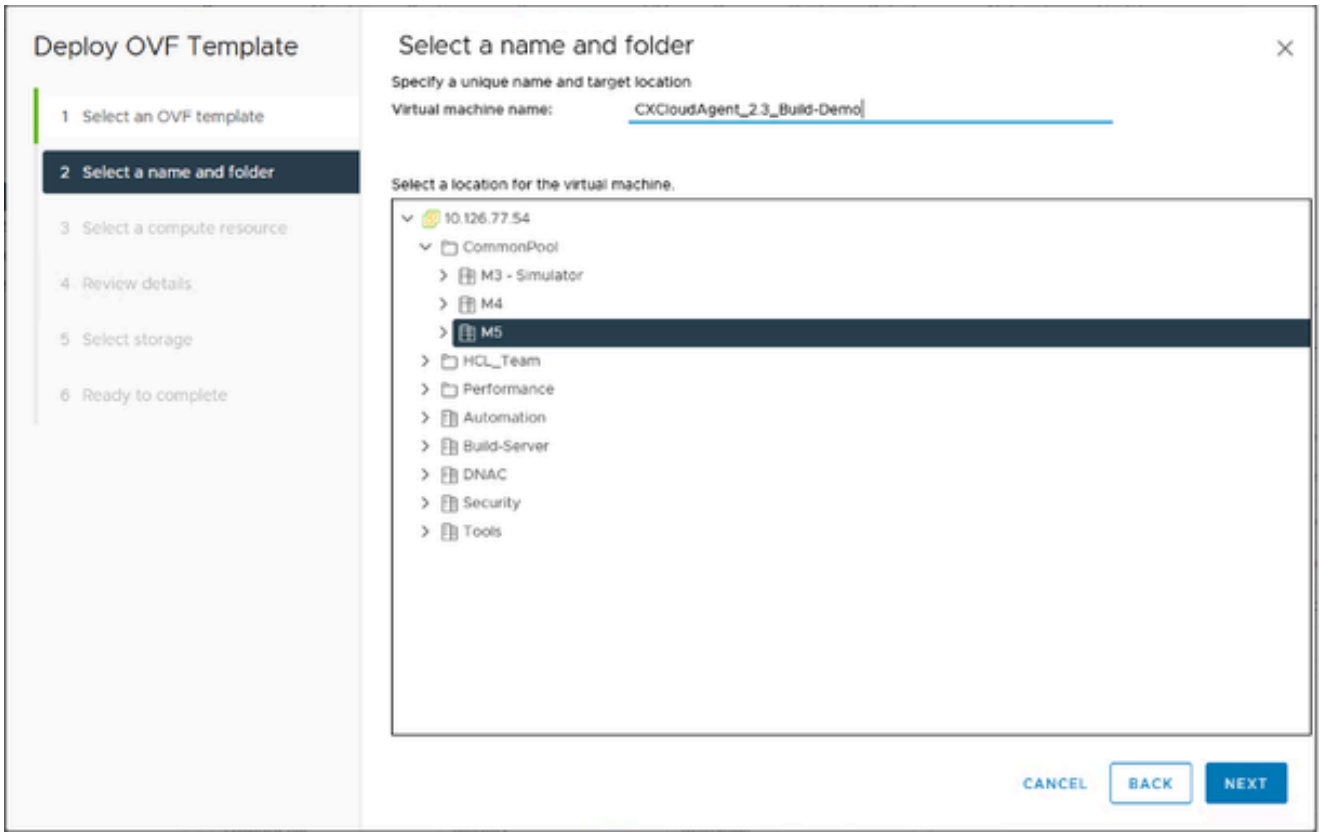
Host e cluster

3. Selezionare VM.com e fare clic su Azione > Distribuisci modello OVF.



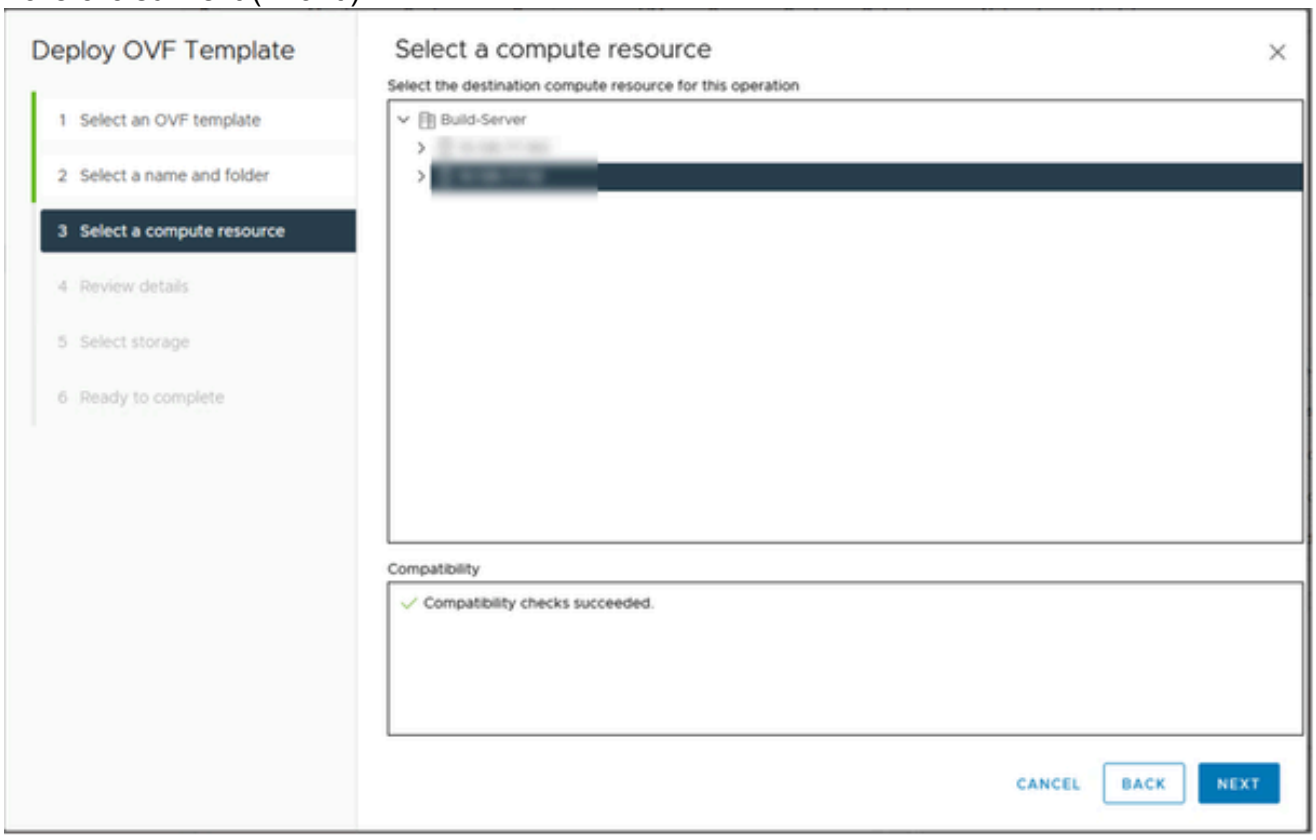
Distribuisci OVF

4. Aggiungere l'URL direttamente o sfogliare per selezionare il file OVA.
5. Fare clic su Next (Avanti).



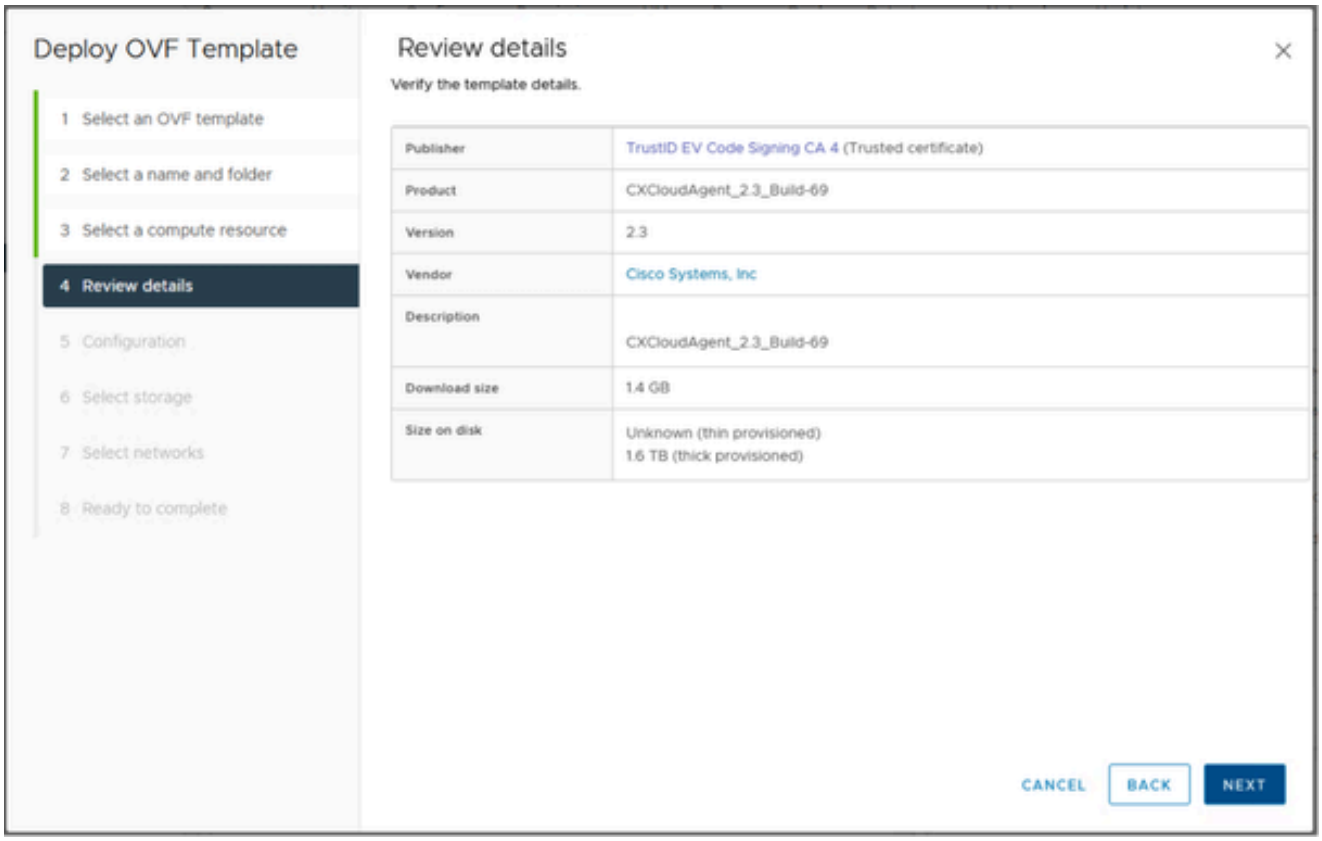
Nome e cartella

6. Se necessario, immettere un nome univoco e selezionare la posizione.
7. Fare clic su Next (Avanti).



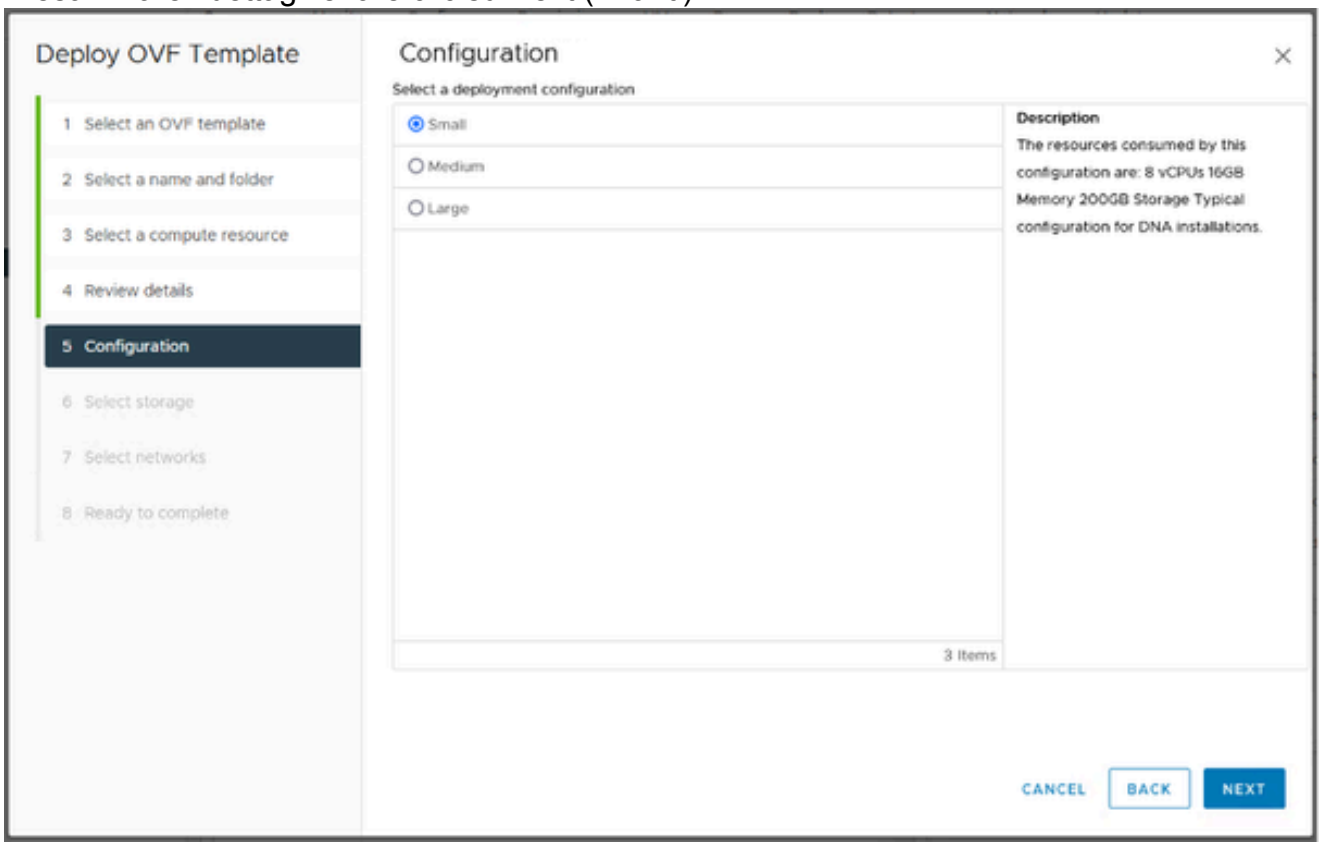
Seleziona risorsa di calcolo

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



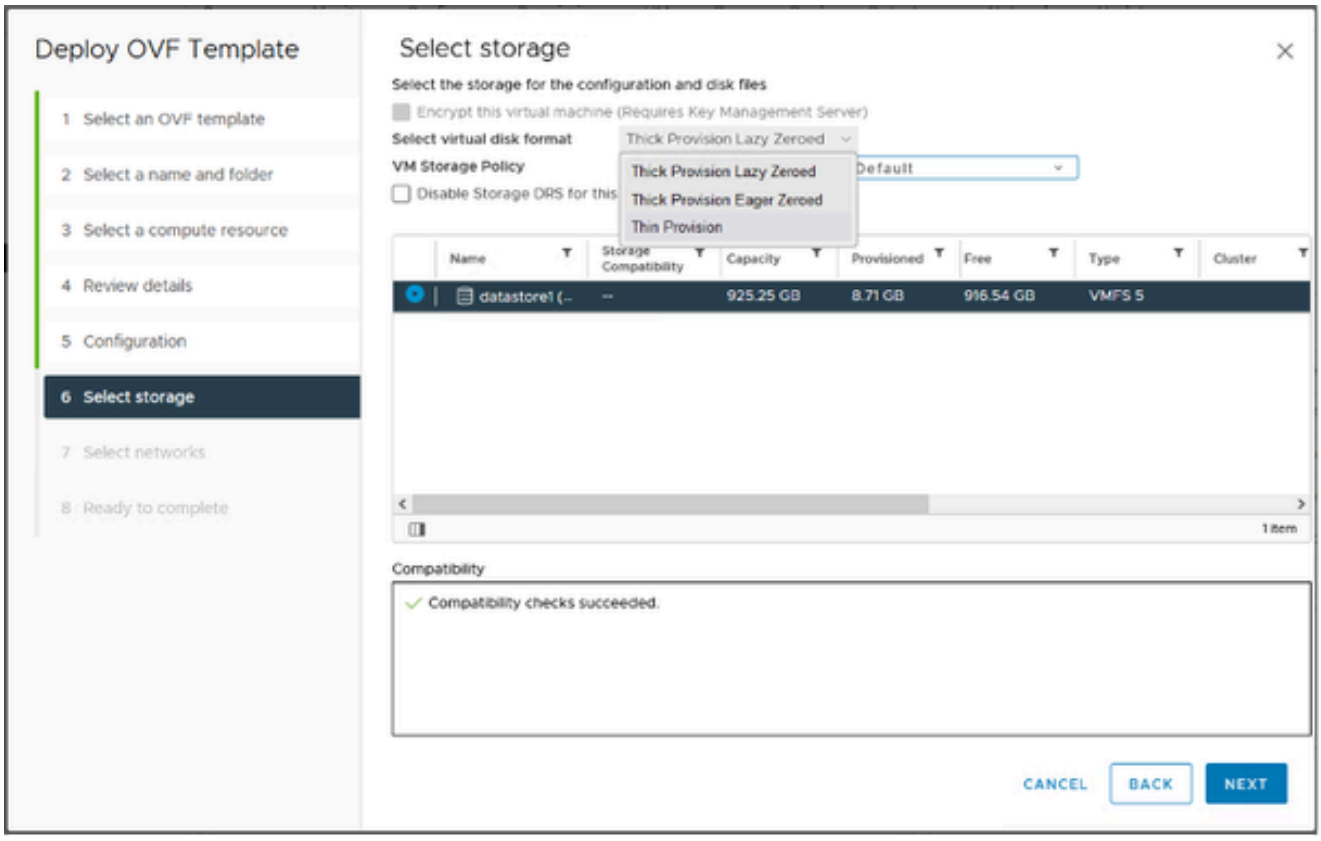
Riesame dei dettagli

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



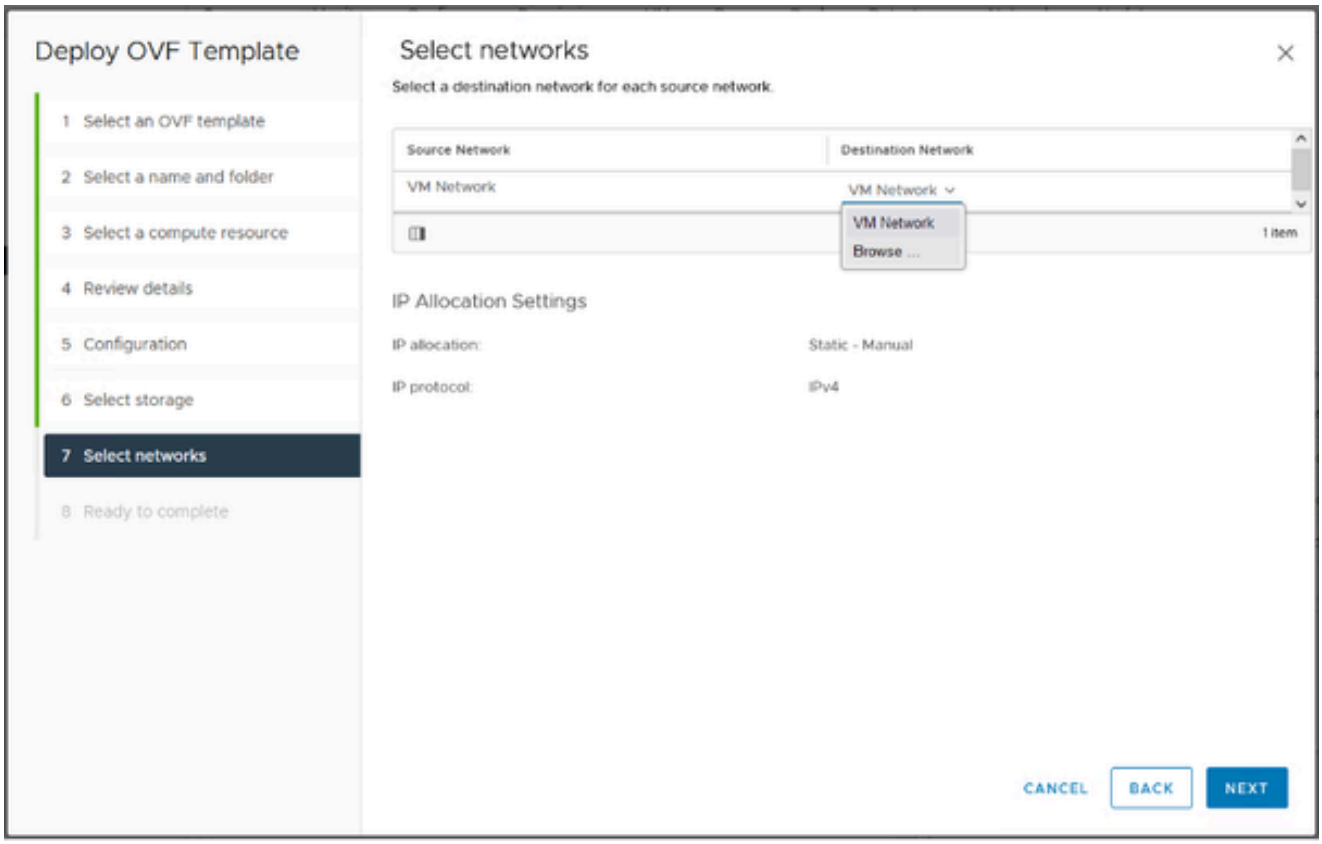
Configurazione

10. Selezionare la configurazione della distribuzione e fare clic su Avanti.



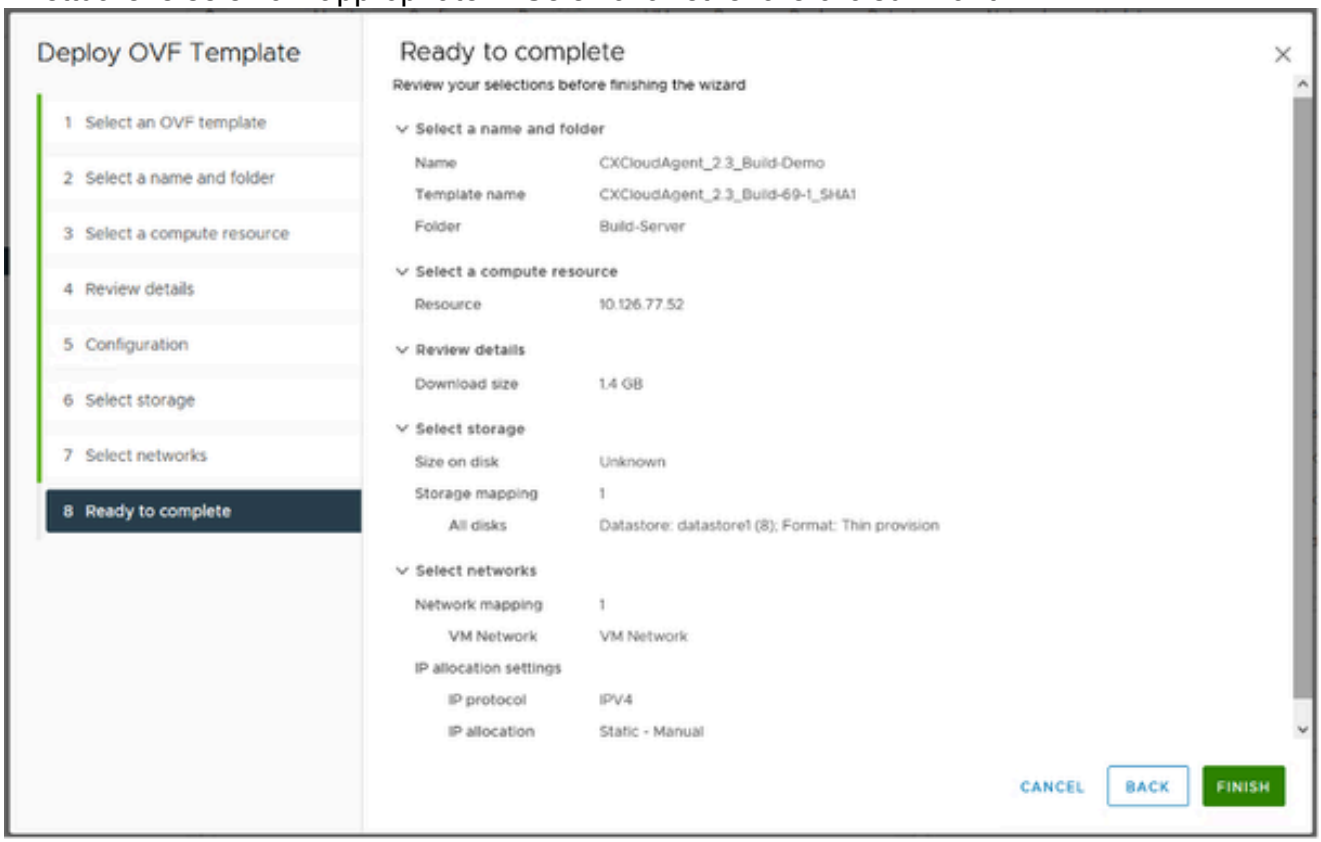
Configurazione

11. Selezionare Archiviazione > Selezionare il formato del disco virtuale dall'elenco a discesa e fare clic su Avanti.



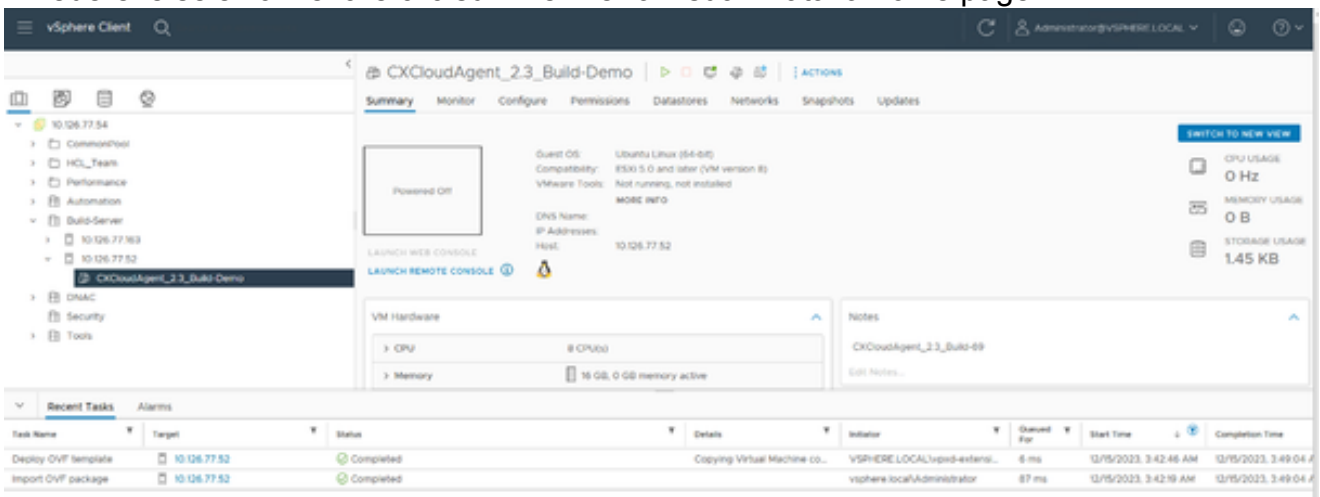
Selezione delle reti

12. Effettuare le selezioni appropriate in Seleziona reti e fare clic su Avanti.



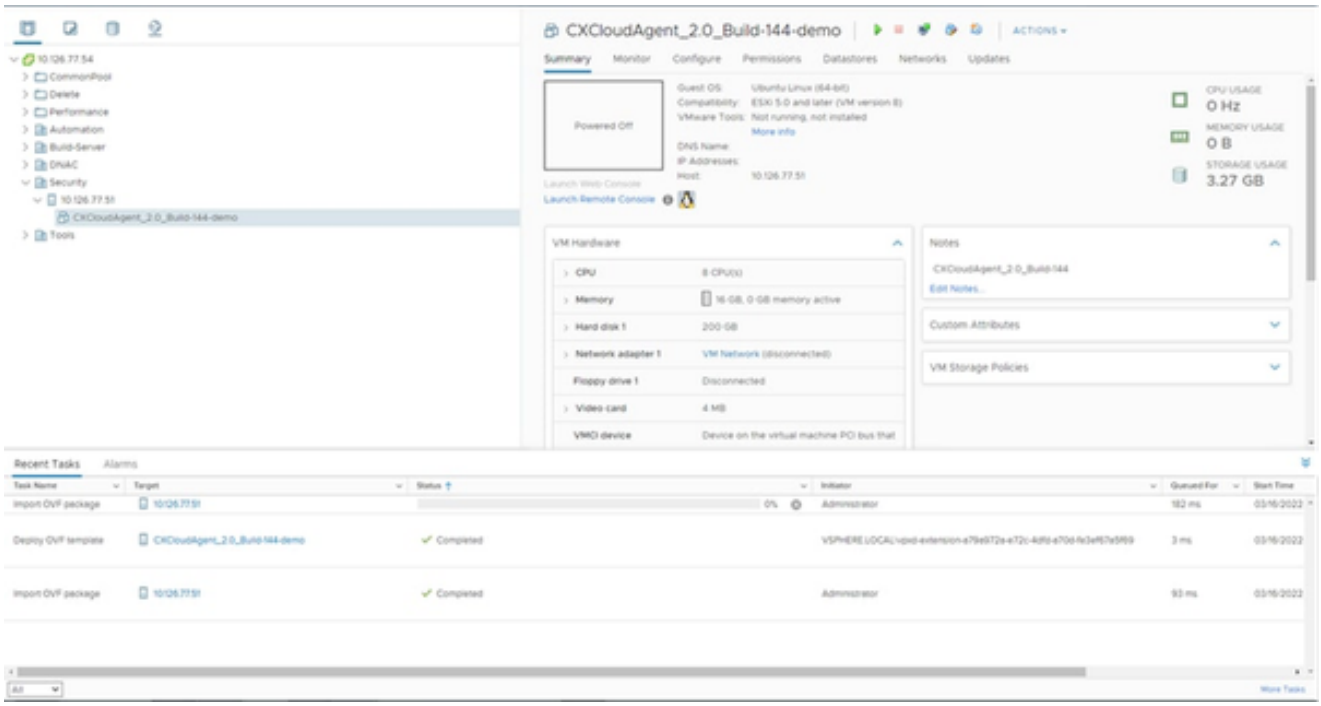
Pronto per il completamento

13. Rivedere le selezioni e fare clic su Fine. Verrà visualizzata la home page.



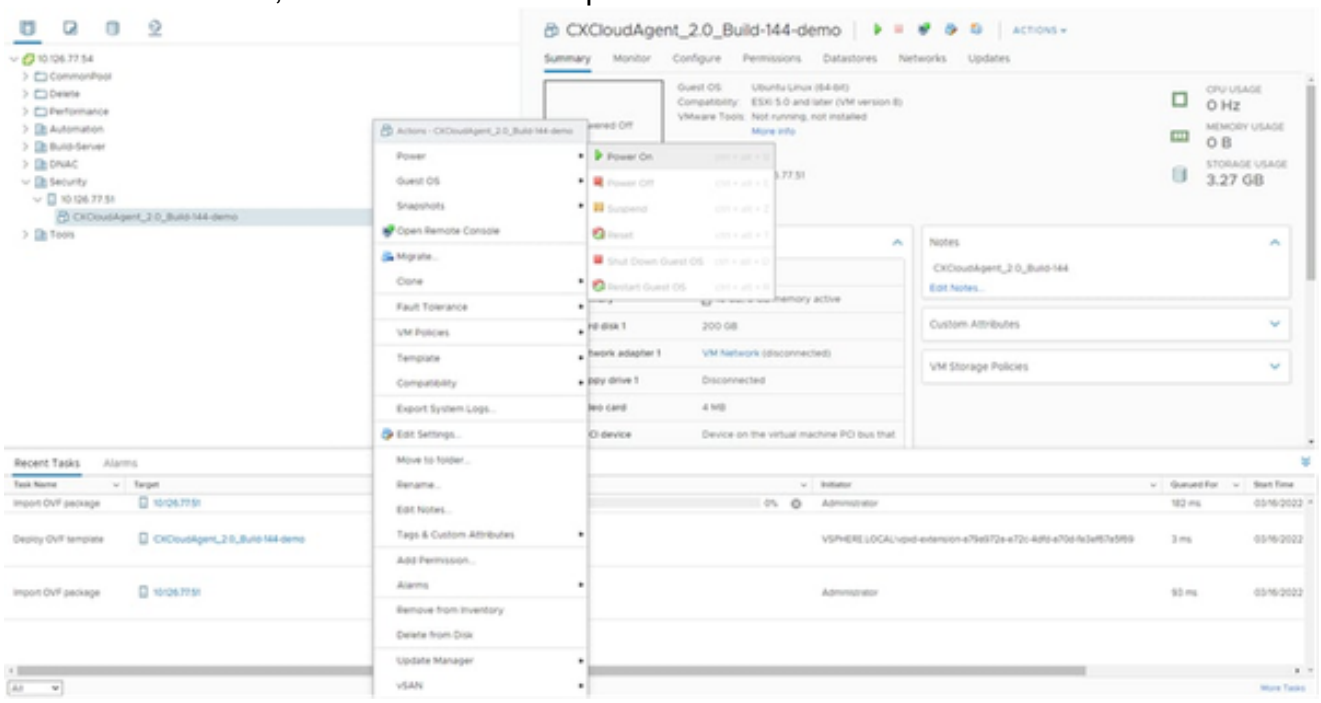
VM aggiunta

14. Fare clic sulla VM appena aggiunta per visualizzare lo stato.



VM aggiunta

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



Apertura della console

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

Installazione di Oracle Virtual Box 7.0.12

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

1. Scaricare l'OAV CXCloudAgent_3.1 nella casella di Windows in una cartella qualsiasi.
2. Individuare la cartella utilizzando l'interfaccia della riga di comando.

3. Decomprimere il file OVA utilizzando il comando tar -xvf D:\CXCloudAgent_3.1_Build-xx.ova.

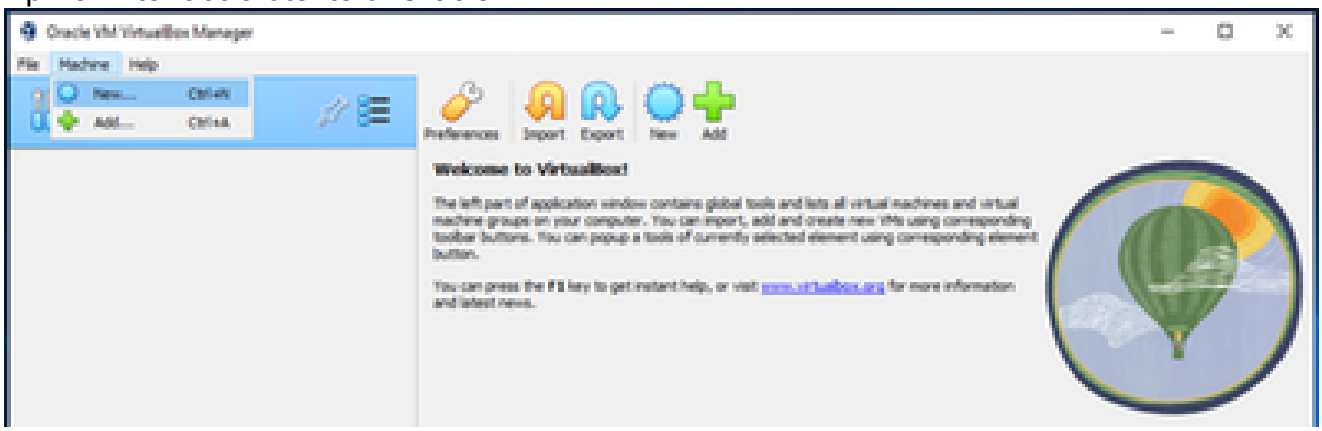
```
D:\>cd CXCAGENT

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

D:\CXCAGENT>_
```

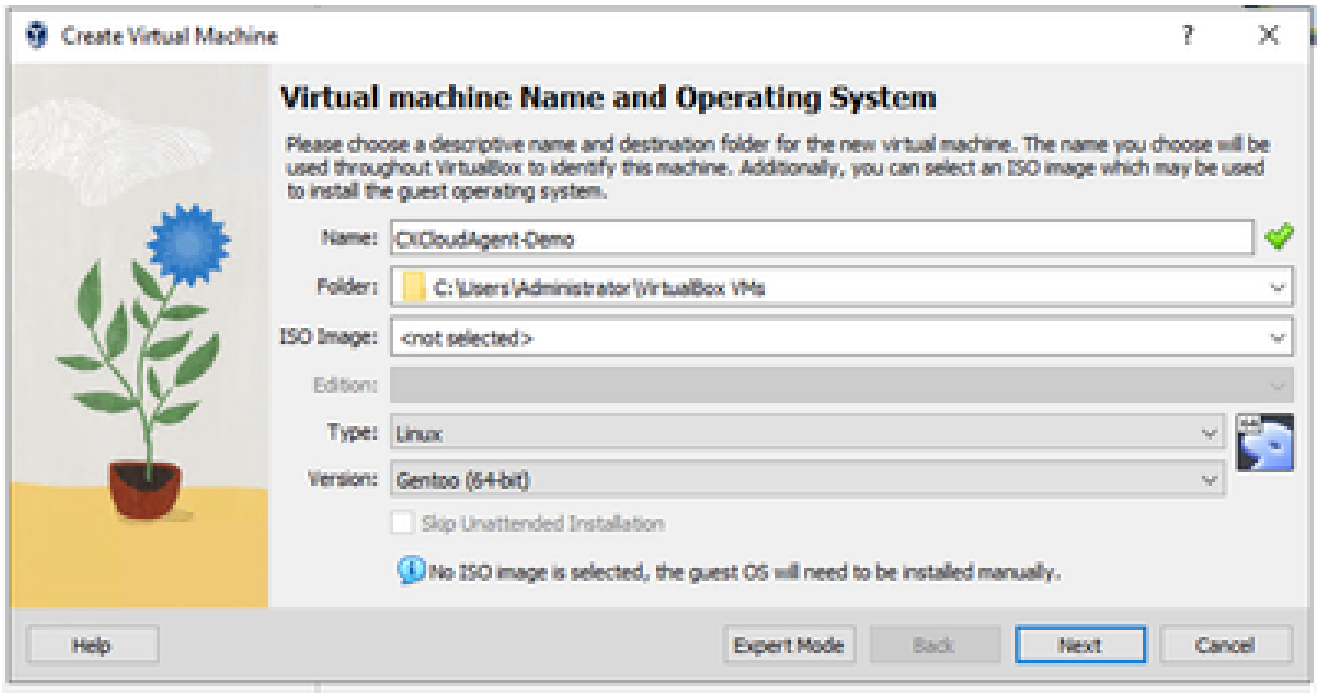
Decomprimi file OVA

4. Aprire l'interfaccia utente di Oracle VM.



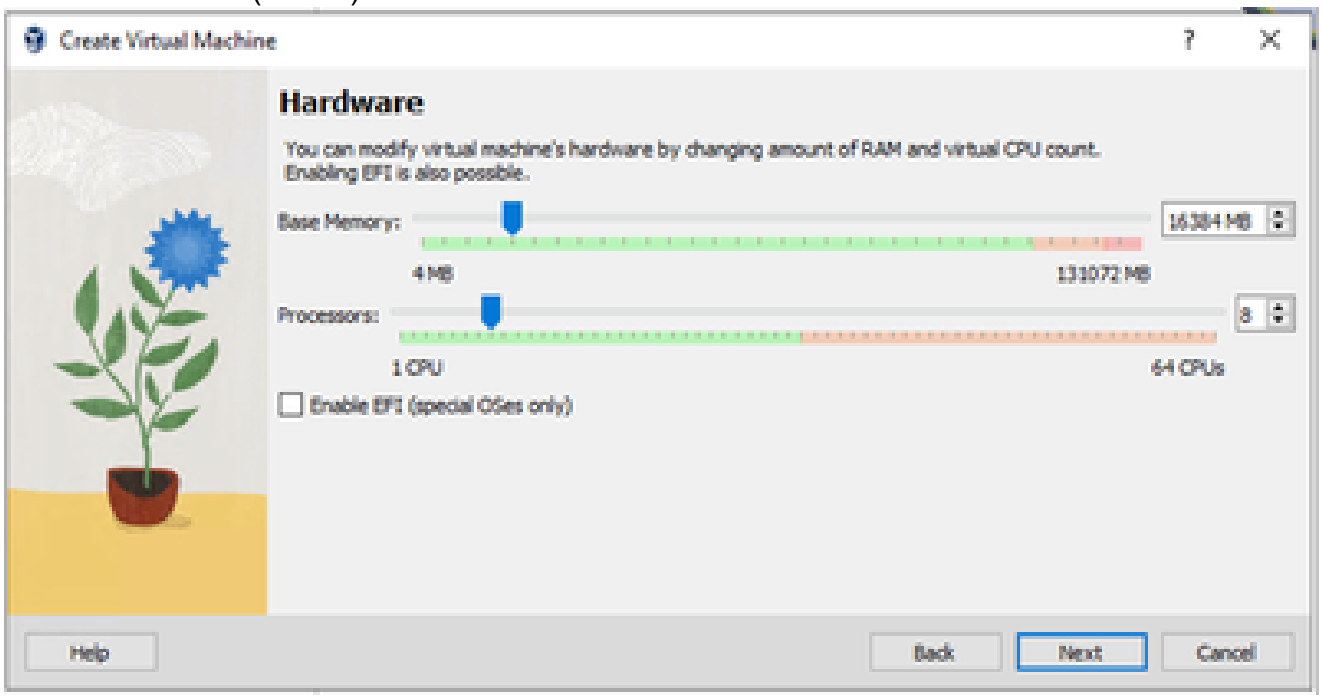
Oracle VM

5. Dal menu, selezionare Lavorazione>Nuova. Verrà visualizzata la finestra Crea macchina virtuale.



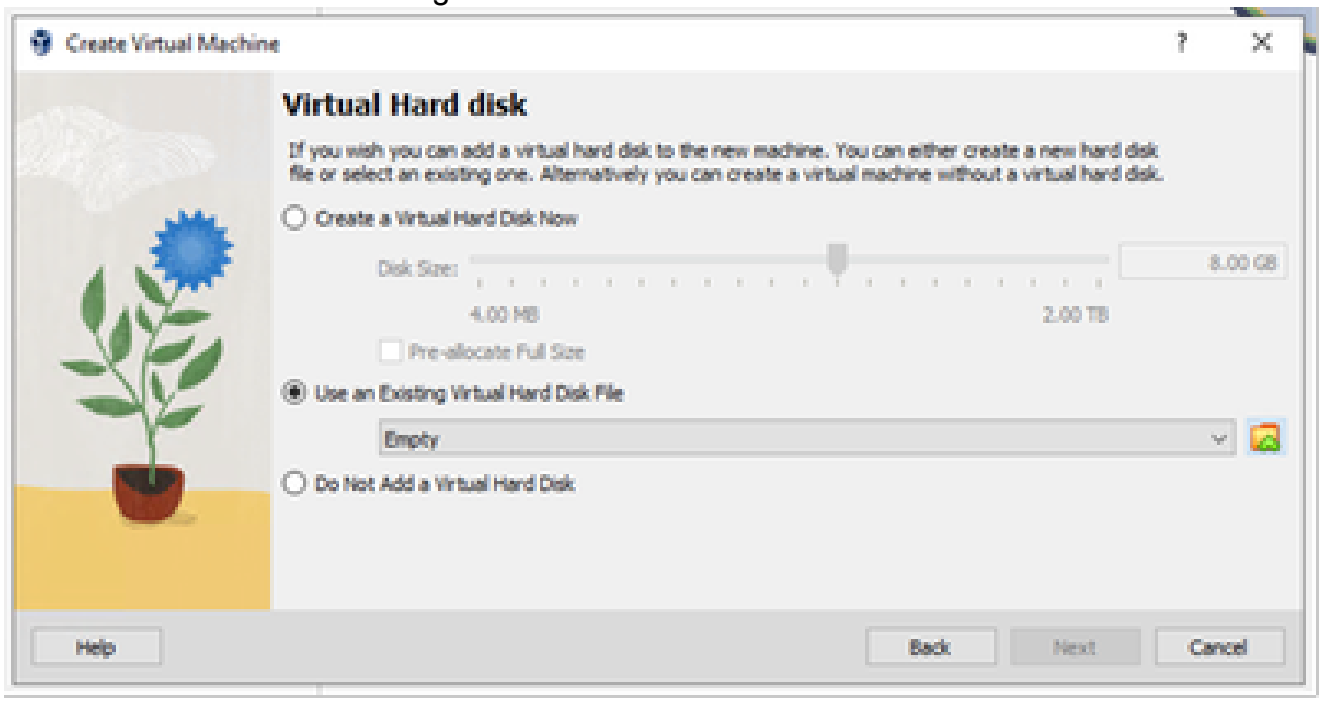
Crea macchina virtuale

6. Immettere i seguenti dettagli nella finestra Nome macchina virtuale e sistema operativo.
   Nome: Nome macchina virtuale
   Cartella: Posizione in cui archiviare i dati della macchina virtuale
   Immagine ISO: nessuna
   Tipo: Linux
   Version: Gentoo (64 bit)
7. Fare clic su Next (Avanti). Viene visualizzata la finestra Hardware.



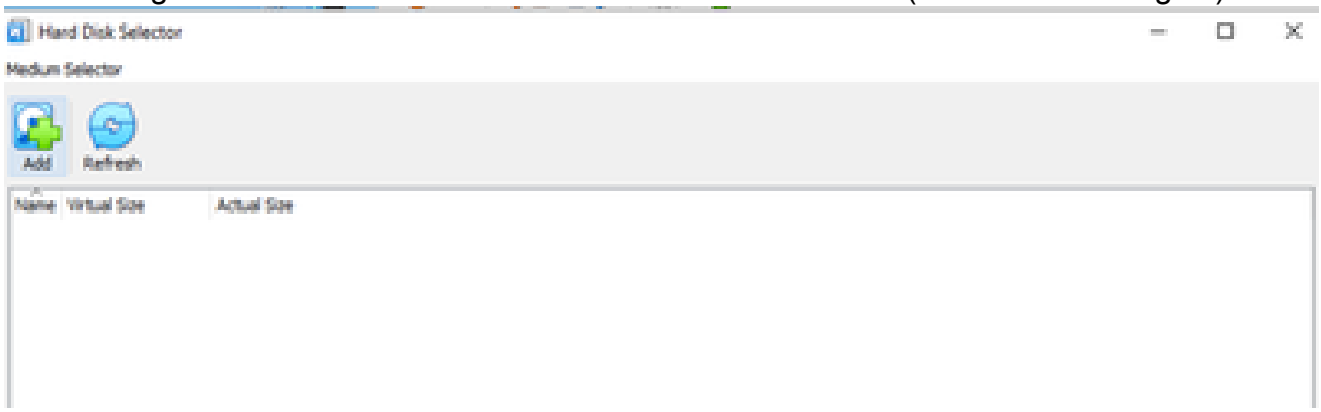
Hardware

8. Immettere Memoria base (16384 MB) e Processori (8 CPU) e fare clic su Avanti. Viene visualizzata la finestra Disco rigido virtuale.



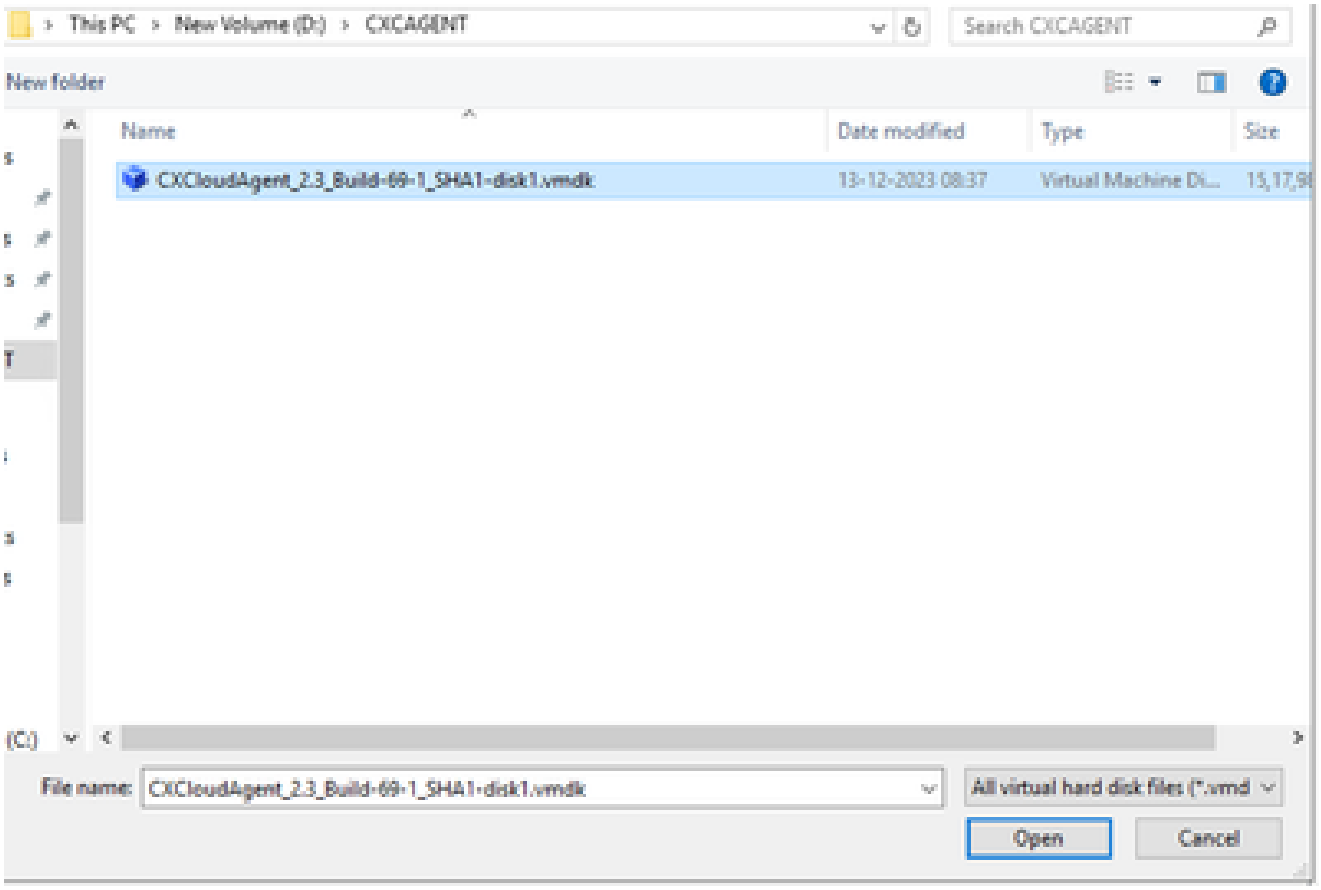
Disco rigido virtuale

9. Selezionare il pulsante di scelta Utilizza un file di disco rigido virtuale esistente e selezionare l'icona Sfoglia. Viene visualizzata la finestra Hard Disk Selector (Selettore disco rigido).



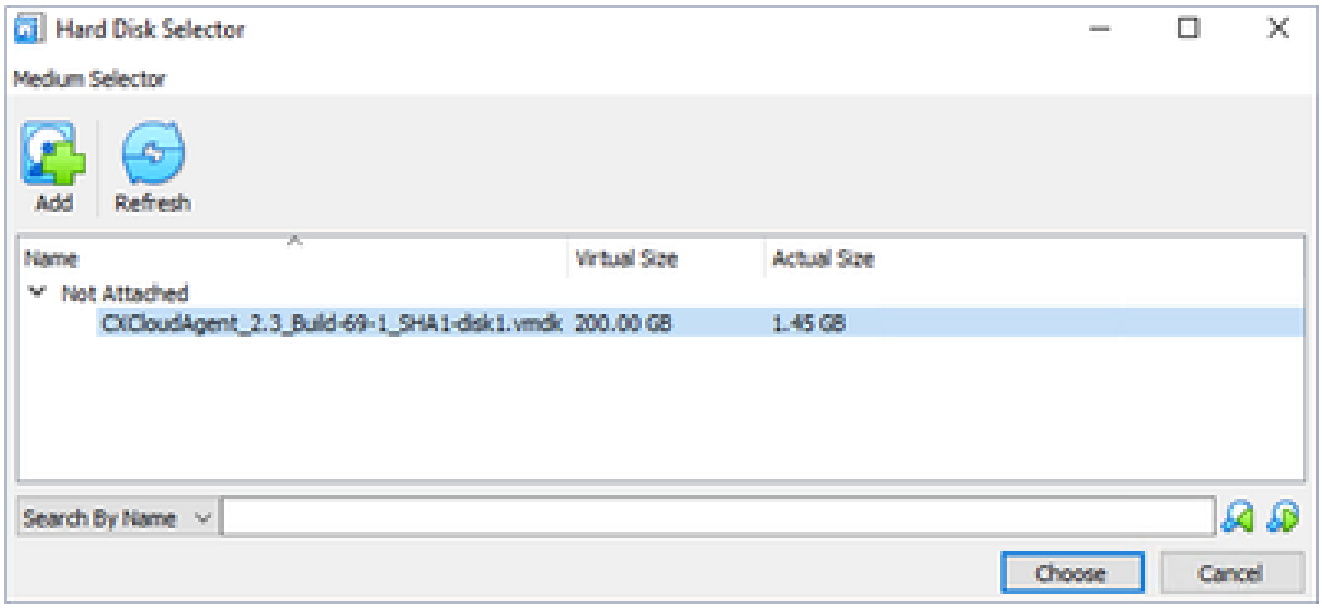
Selettore del disco rigido

10. Selezionare la cartella OVA e il file VMDK.



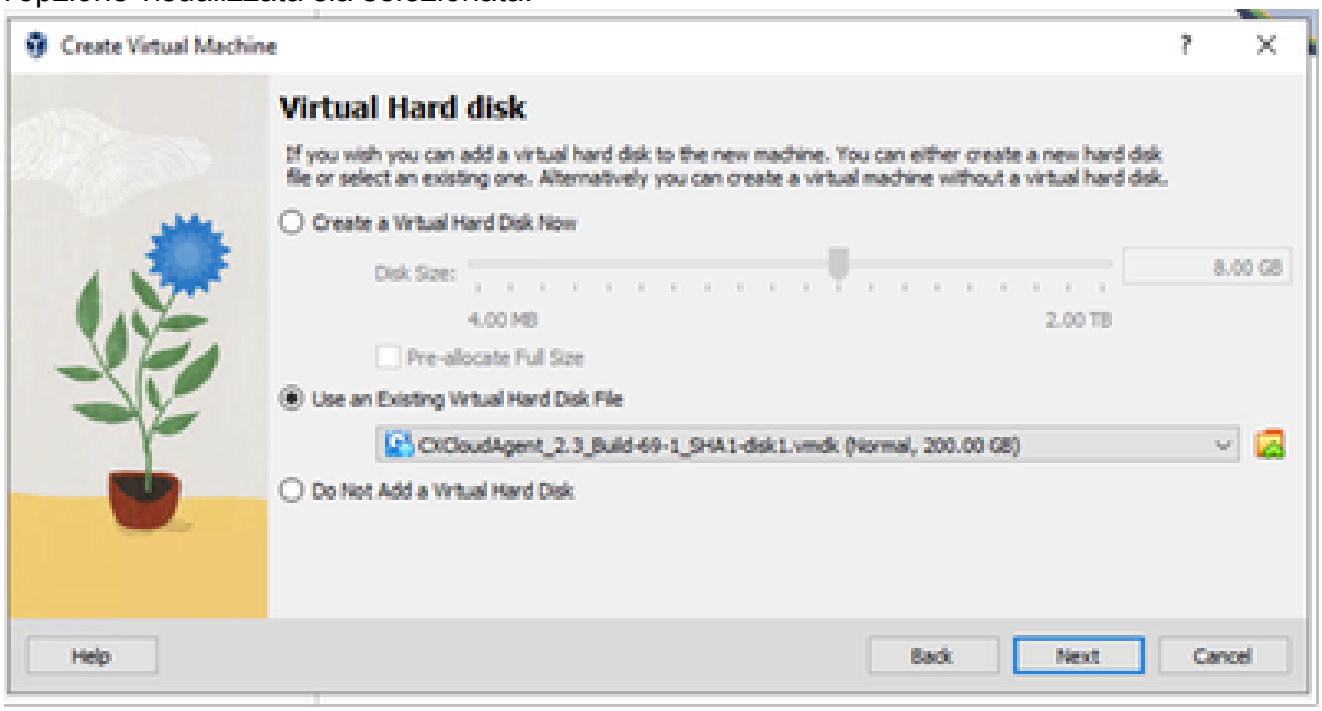
Cartella OVA

11. Fare clic su Apri. Il file viene visualizzato nella finestra Selettore disco hardware.



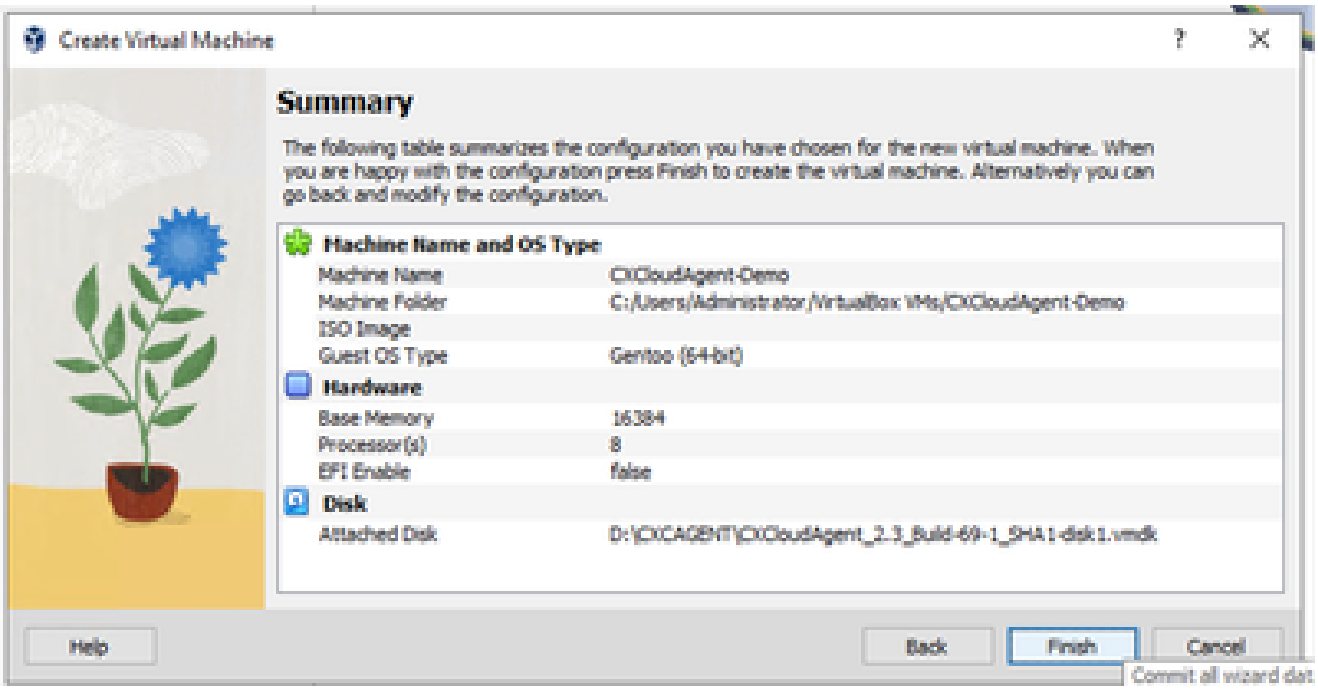
Selettore del disco rigido

12. Fare clic su Scegli. Viene visualizzata la finestra Disco rigido virtuale. Verificare che l'opzione visualizzata sia selezionata.



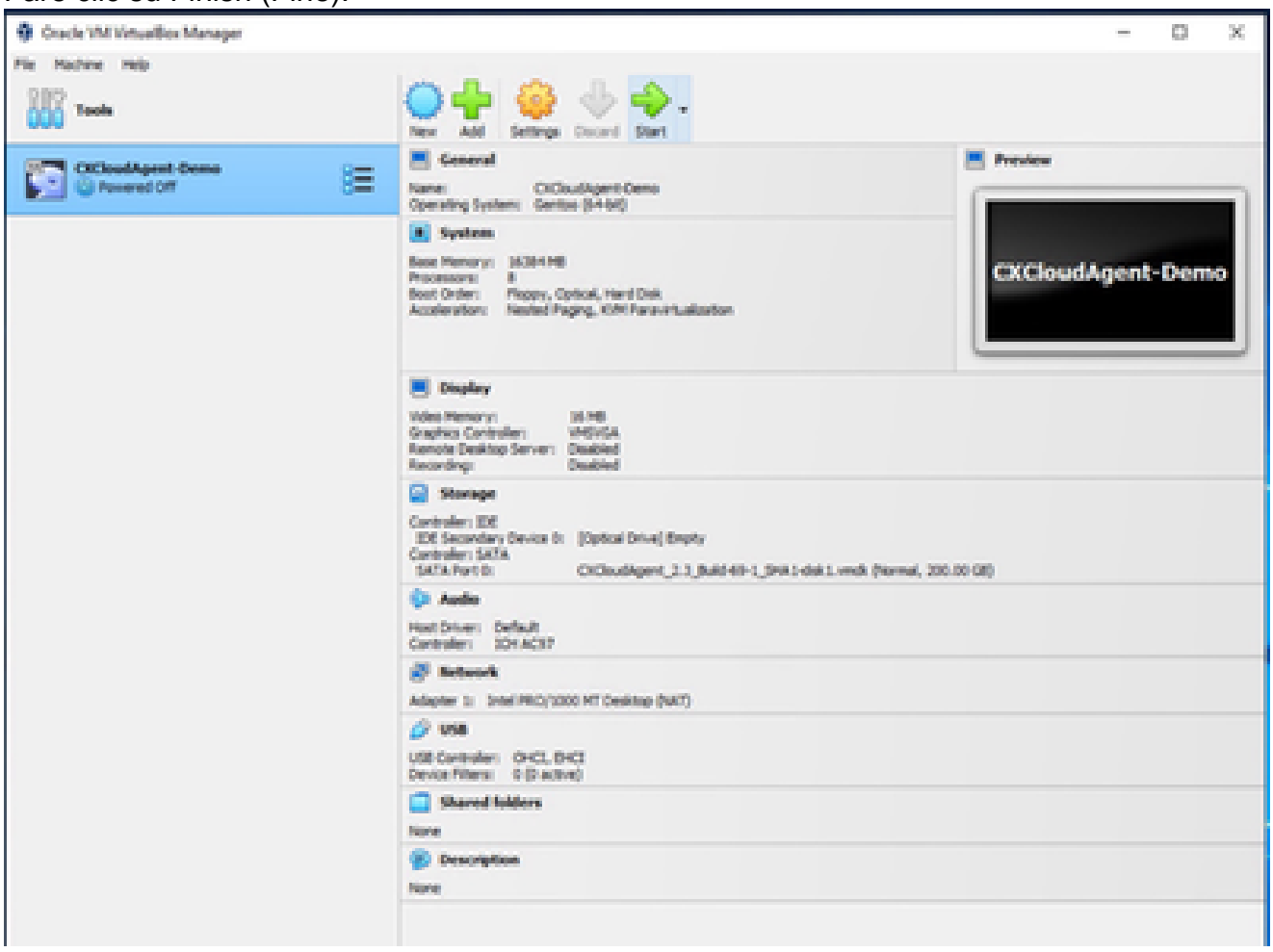
Selezione del file

13. Fare clic su Next (Avanti). Viene visualizzata la finestra Summary.



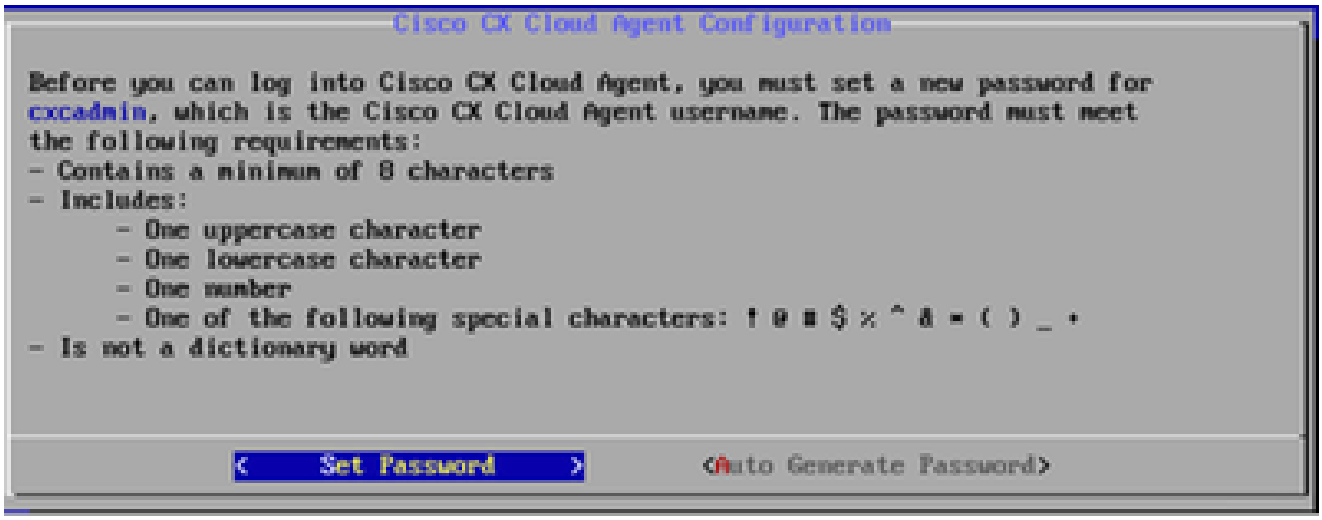
Riepilogo

14. Fare clic su Finish (Fine).



Avvio della console VM

15. Selezionare la macchina virtuale distribuita e fare clic su Avvia. La VM si accende e viene visualizzata la schermata della console per la configurazione.



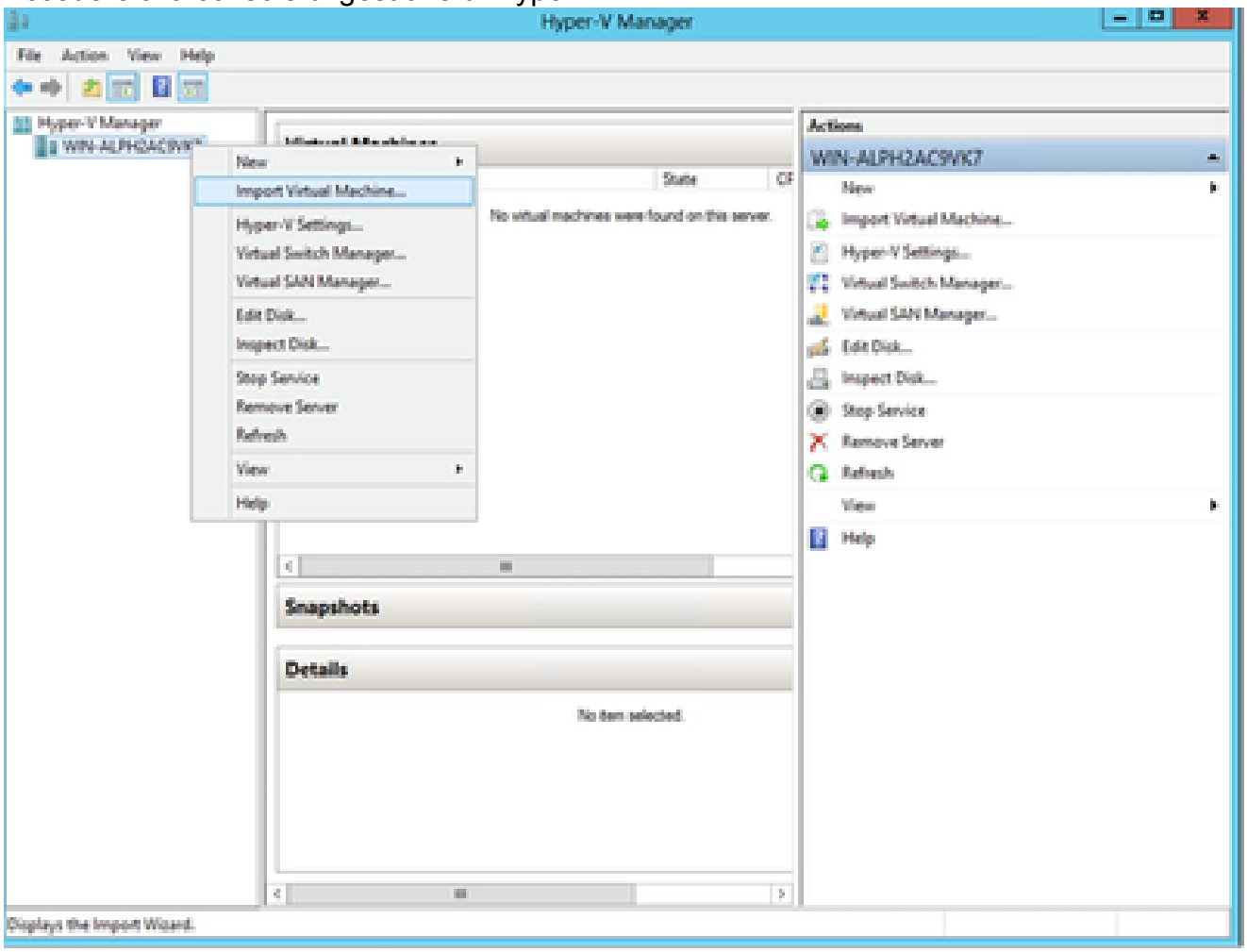
Apertura della console

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

Installazione di Microsoft Hyper-V

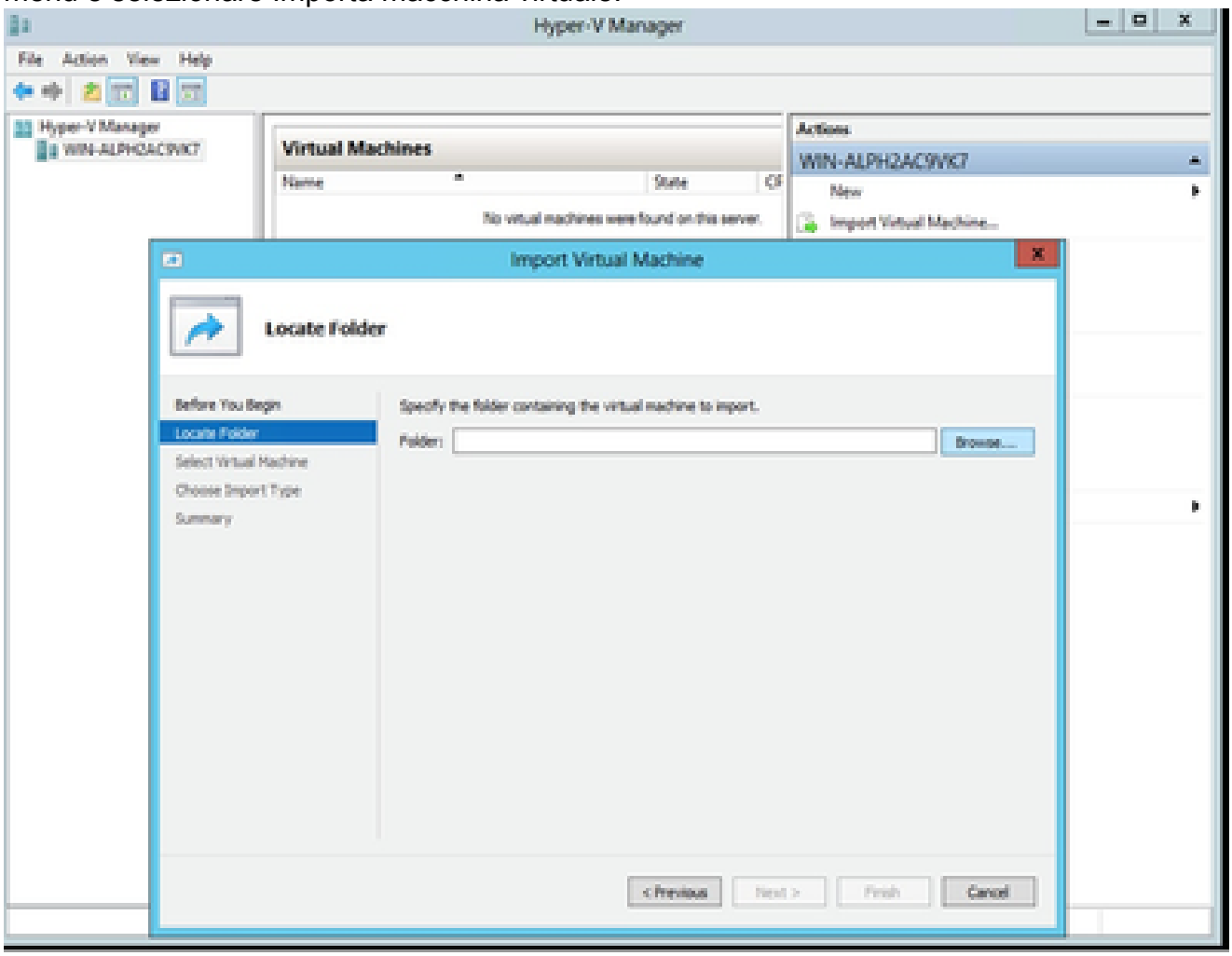
Questo client distribuisce l'agente CX tramite l'installazione di Microsoft Hyper-V.

1. Accedere alla console di gestione di Hyper-V.



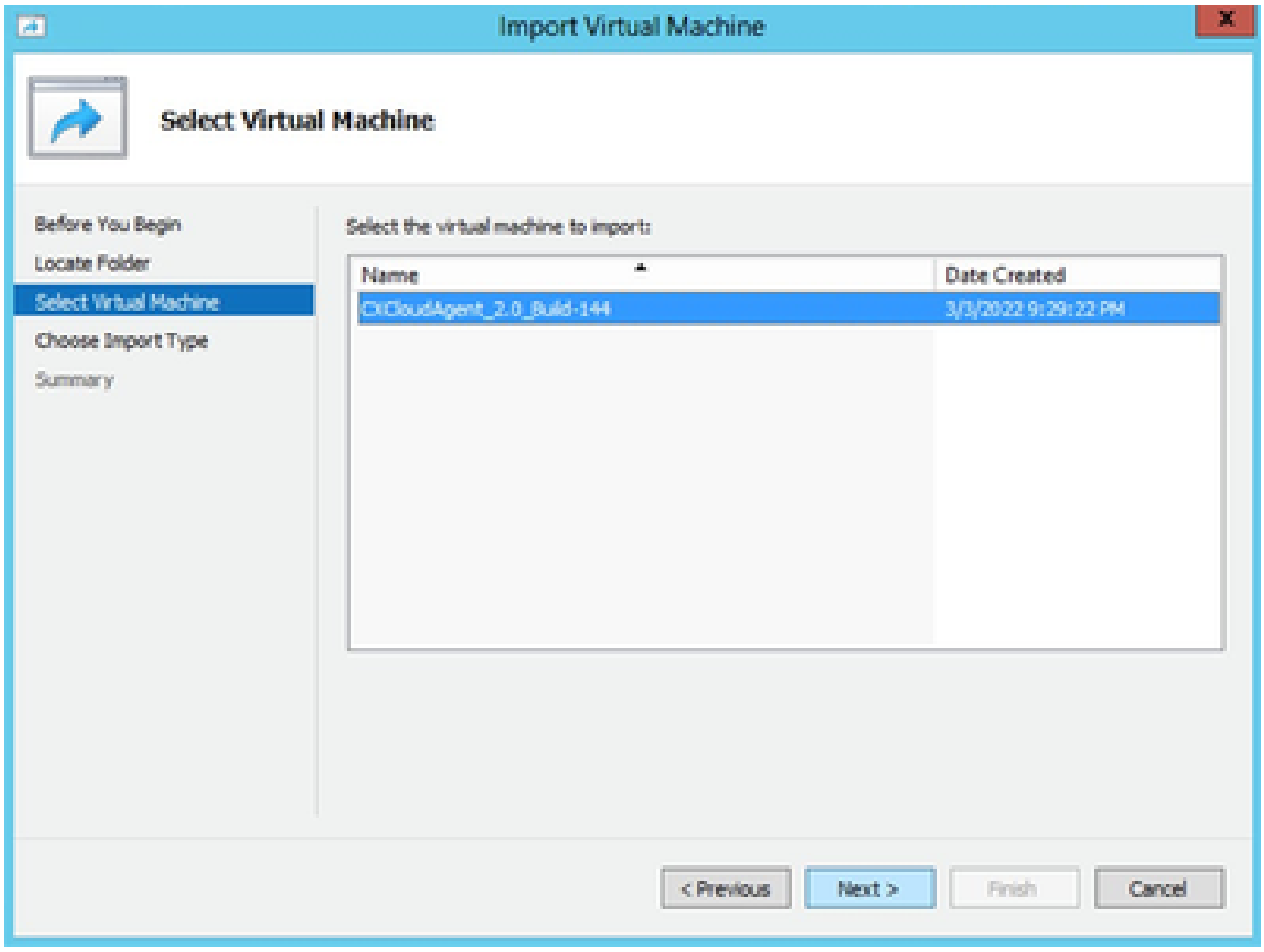
Gestione Hyper-V

2. Selezionare la VM di destinazione, fare clic con il pulsante destro del mouse per aprire il menu e selezionare Importa macchina virtuale.



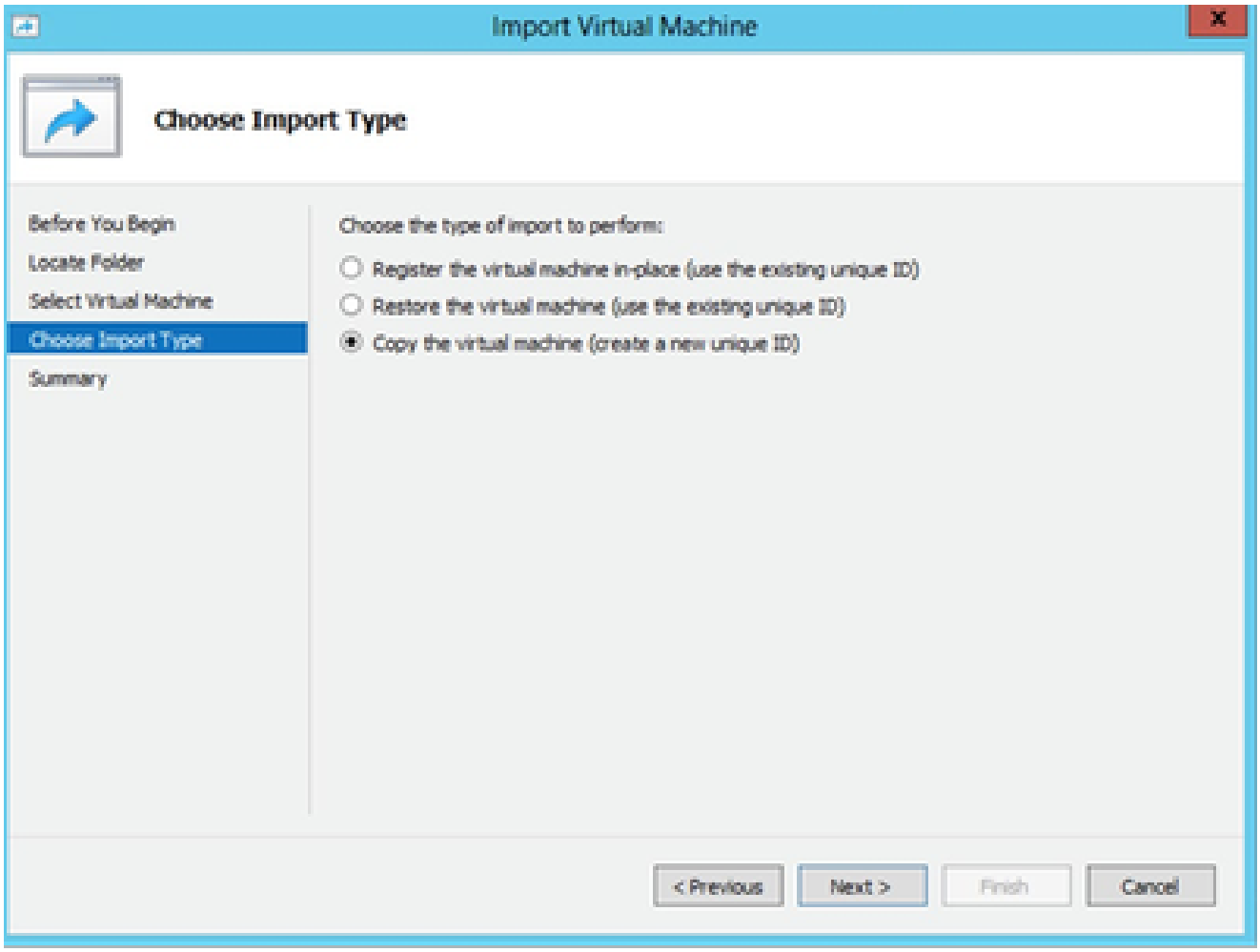
Cartella per l'importazione

3. Selezionare la cartella di download e fare clic su Avanti.



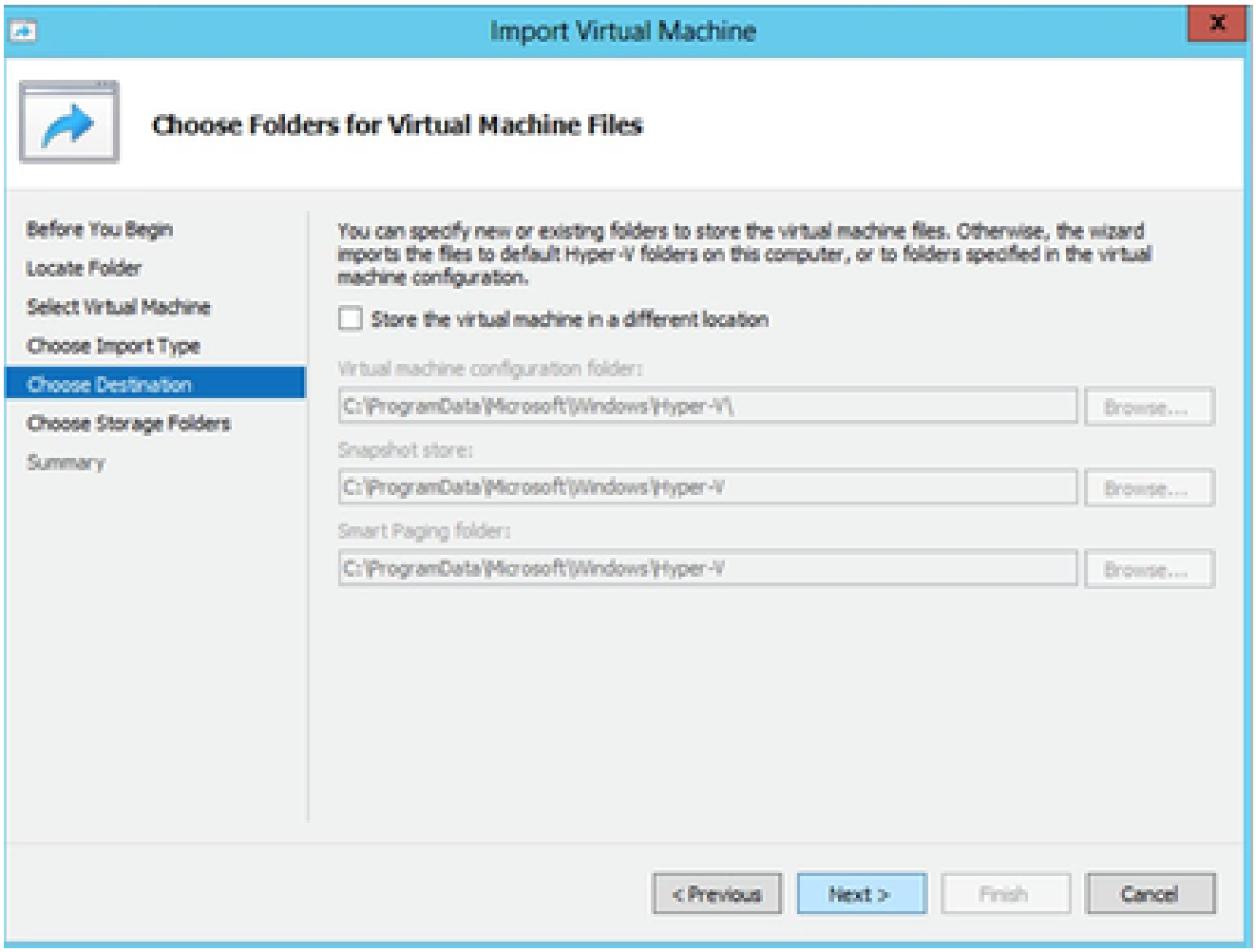
Selezione della VM

4. Selezionare la VM e fare clic su Avanti.



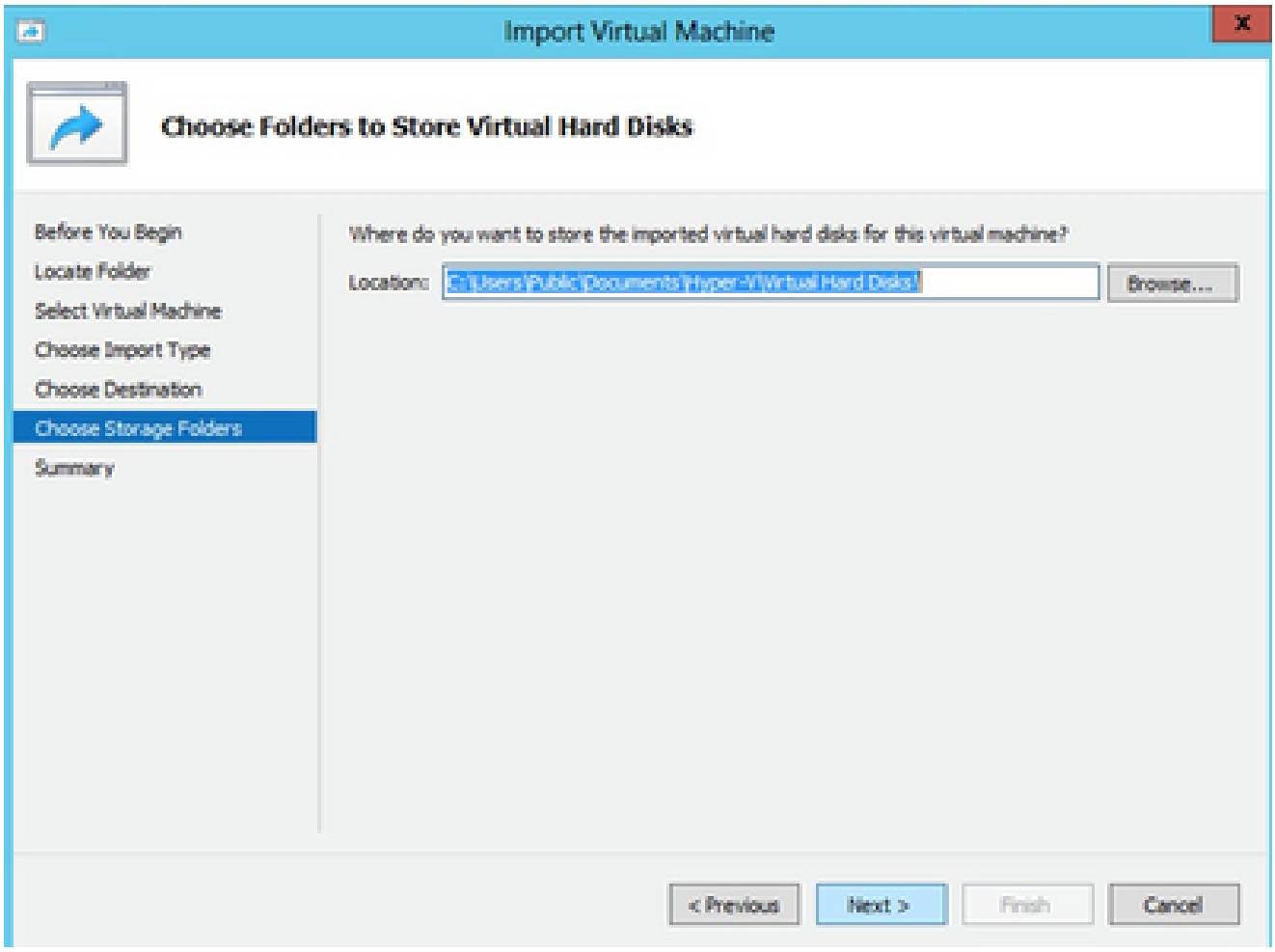
Tipo di importazione

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



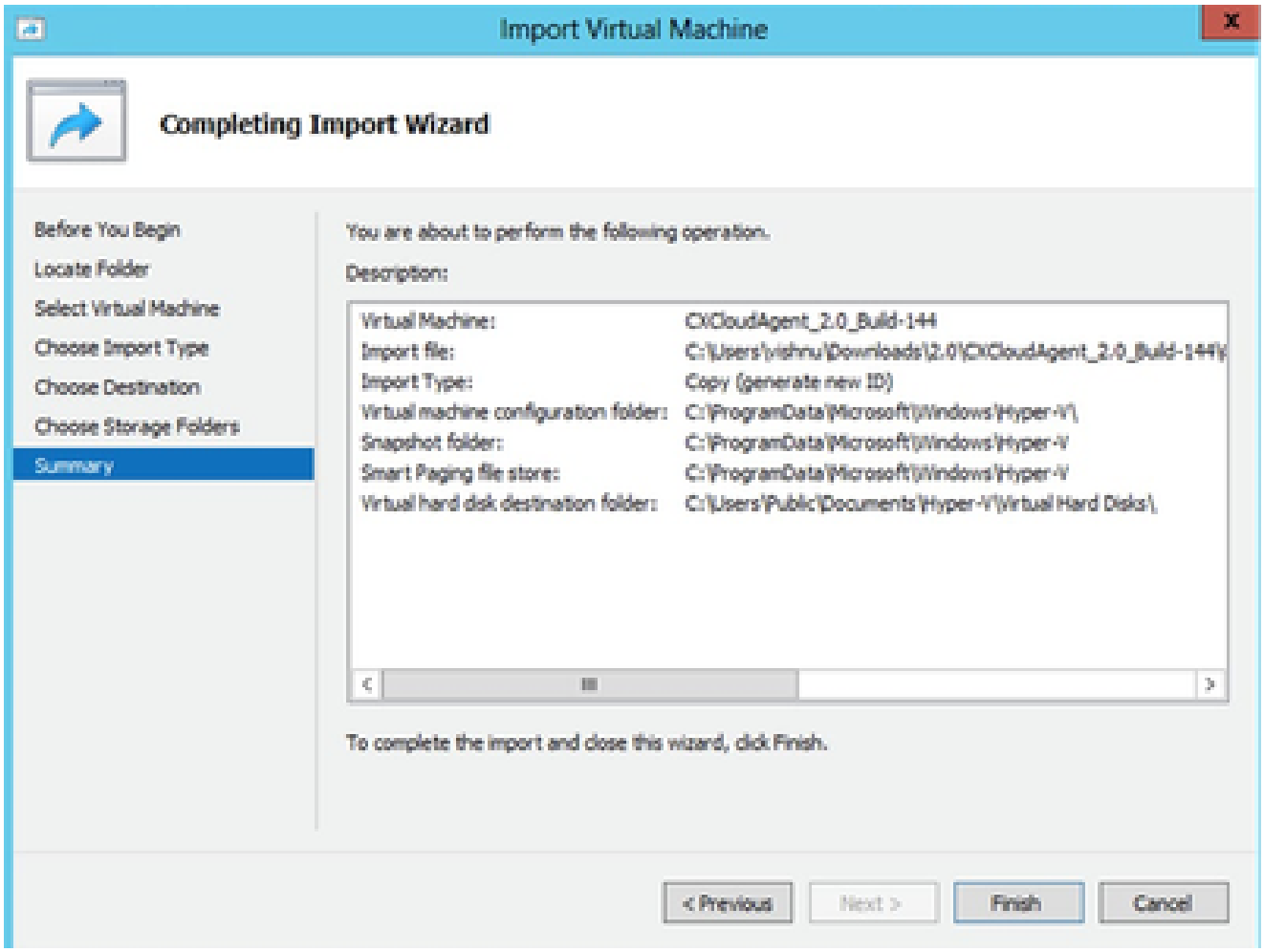
Scegliere le cartelle per i file delle macchine virtuali

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



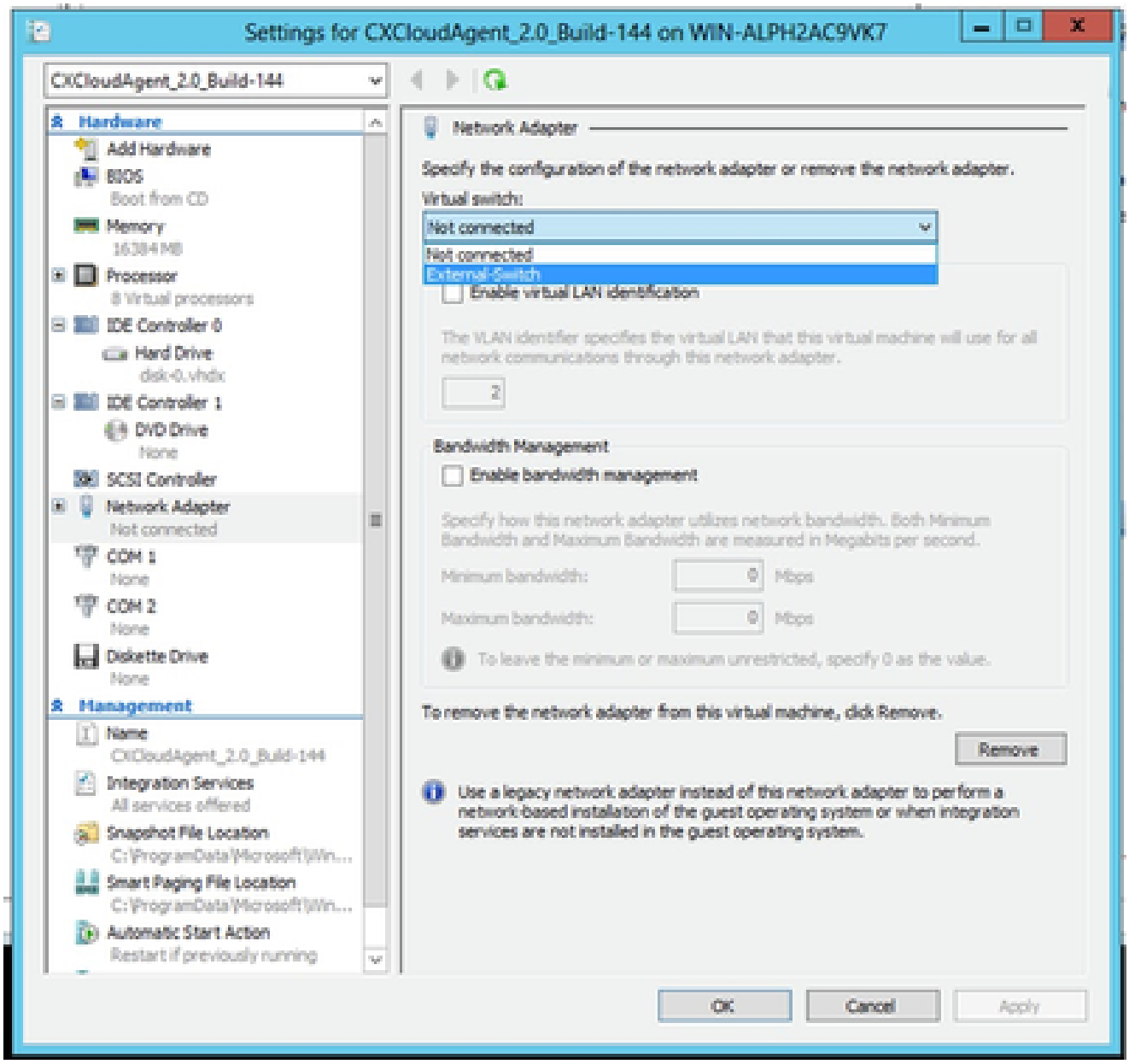
Cartella per l'archiviazione dei dischi rigidi virtuali

8. Individuare e selezionare la cartella in cui archiviare i dischi rigidi della macchina virtuale. Cisco consiglia di utilizzare i percorsi predefiniti.
9. Fare clic su Next (Avanti). Viene visualizzato il riepilogo della VM.



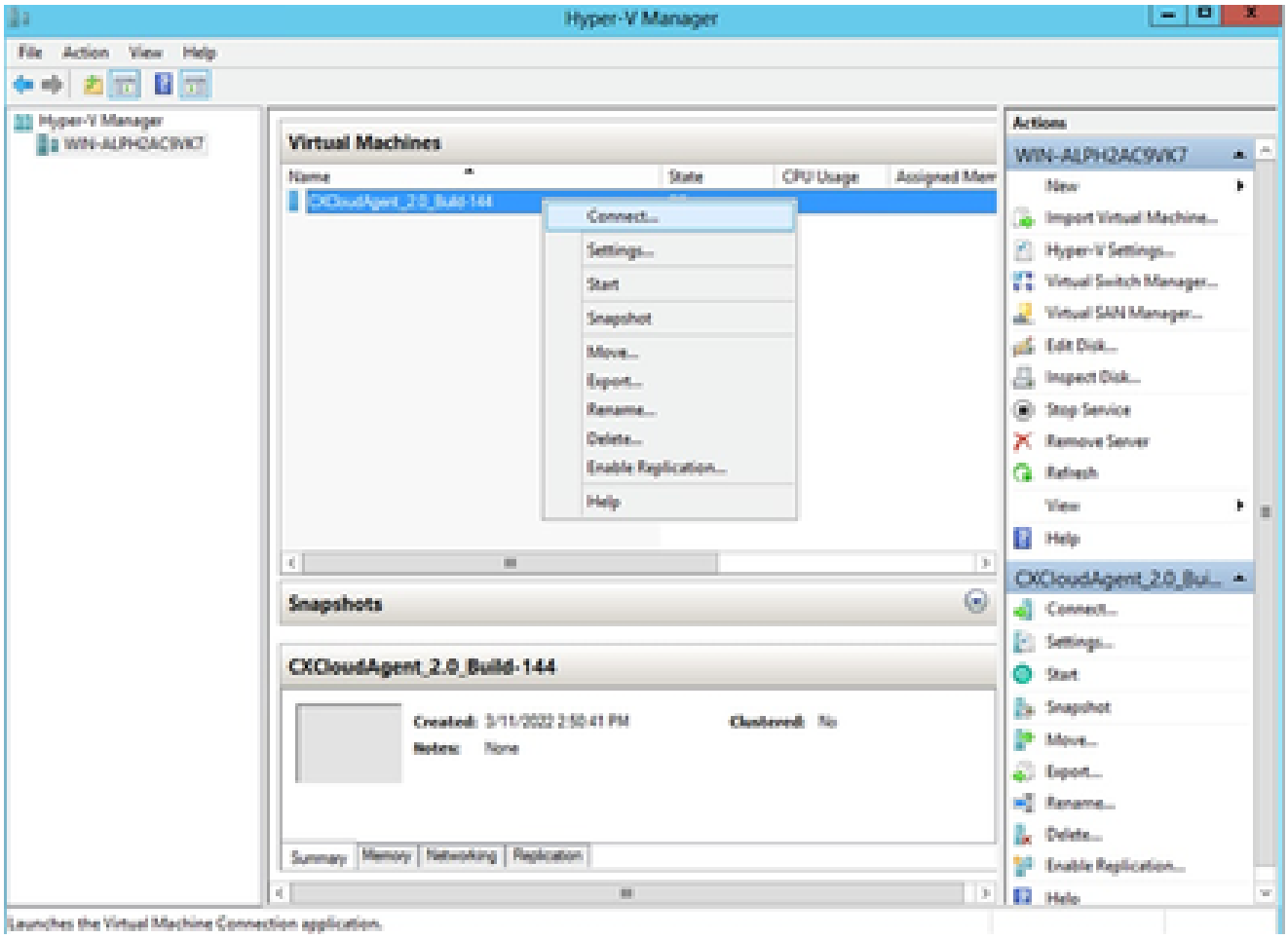
Riepilogo

10. Verificare tutti gli input e fare clic su Fine.
11. Al termine dell'importazione, viene creata una nuova VM in Hyper-V. Aprire le impostazioni della VM.



Switch virtuale

12. Selezionare l'adattatore di rete dal pannello a sinistra e selezionare lo switch virtuale disponibile dall'elenco a discesa.

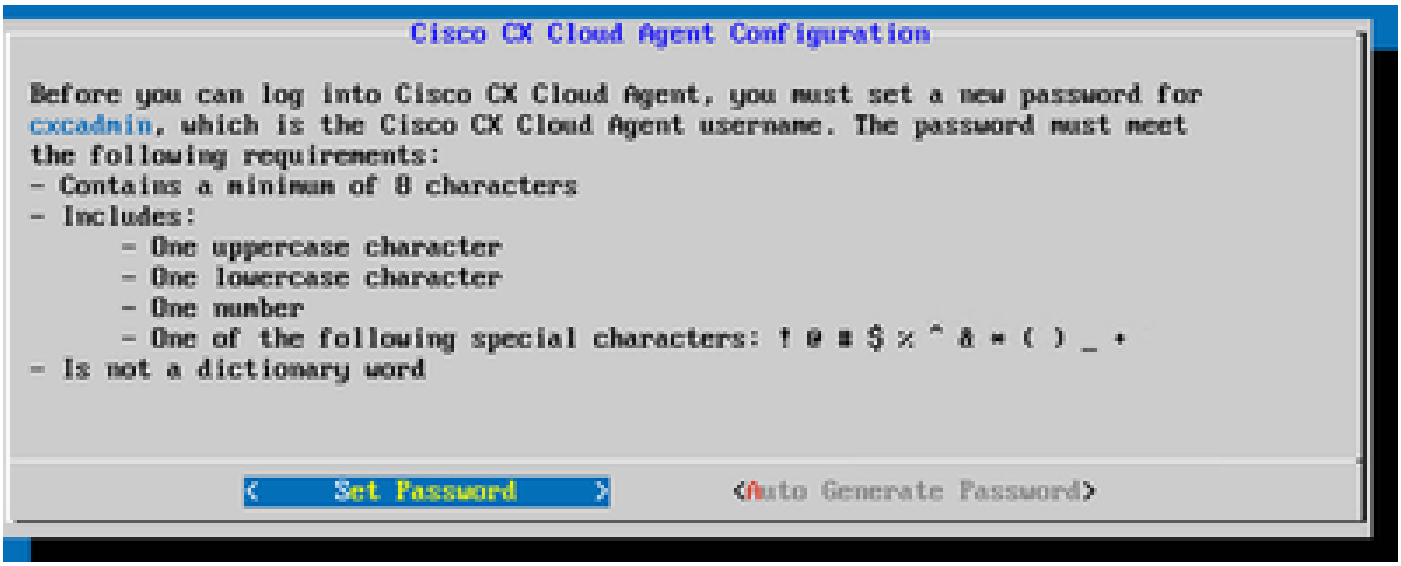


Avvio della VM

13. Selezionare Connect (Connetti) per avviare la VM.
14. Passare a Configurazione di rete per continuare con i passaggi successivi.

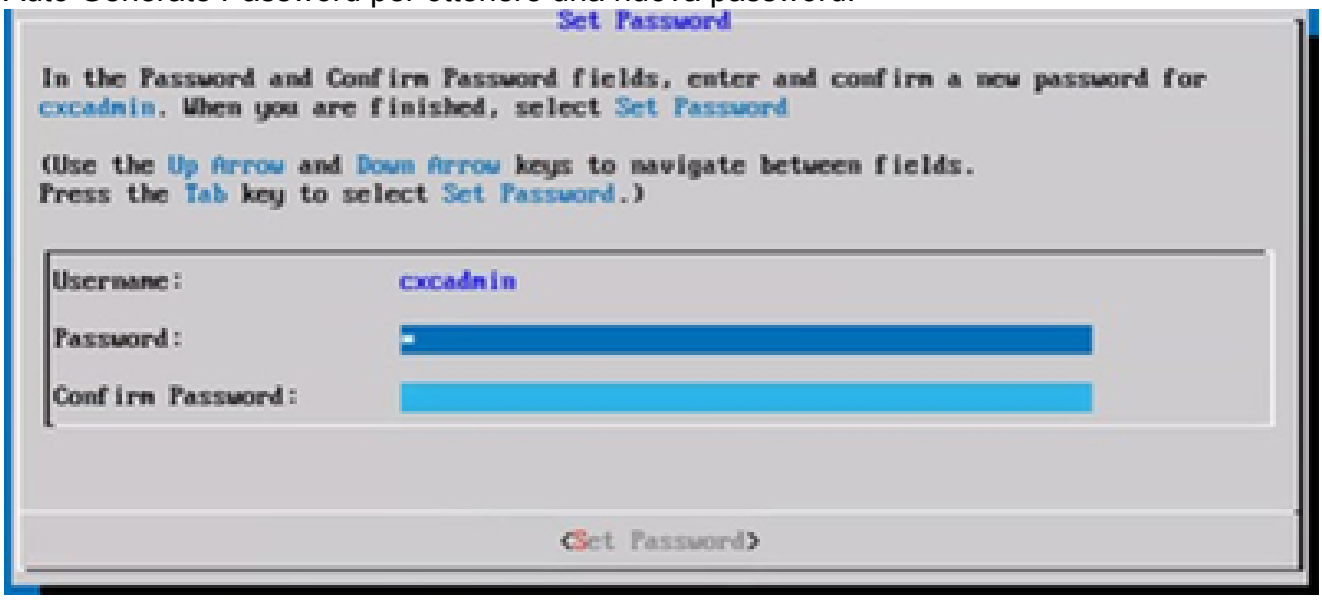
Configurazione della rete

Per impostare la password dell'agente cloud CX per il nome utente cxcadmin:



Imposta password

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



Nuova password

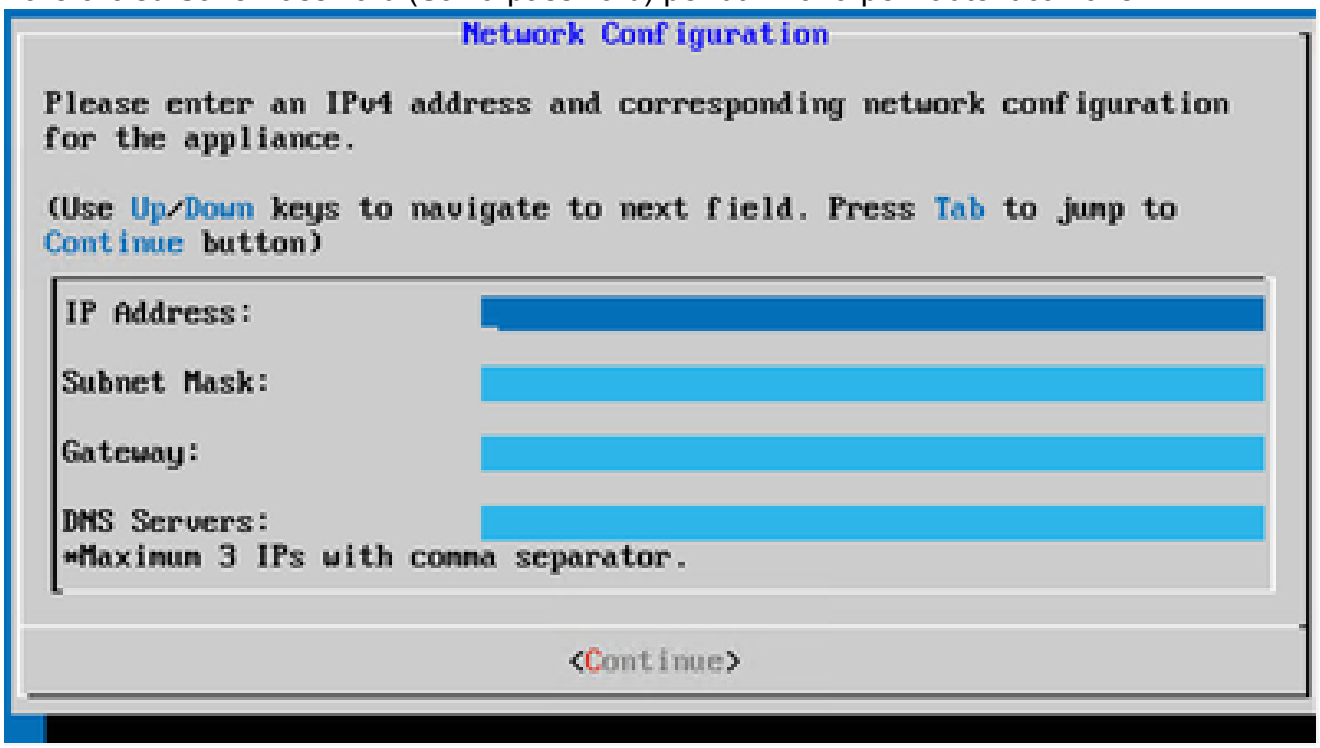
2. Se si seleziona Set Password (Imposta password), immettere la password per cxcadmin e confermarla. Fare clic su Set Password (Imposta password) e andare al passaggio 3.
O

   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

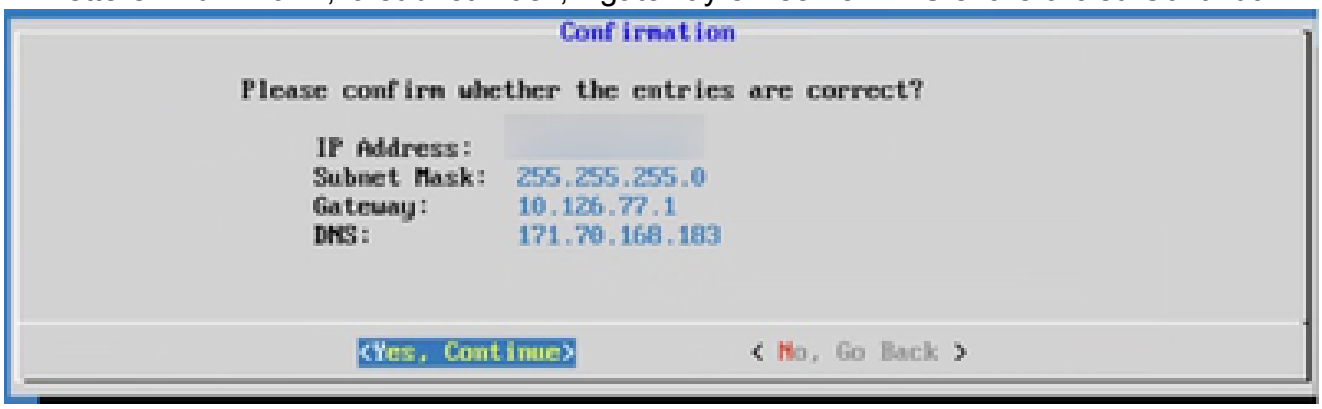
Salva password

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



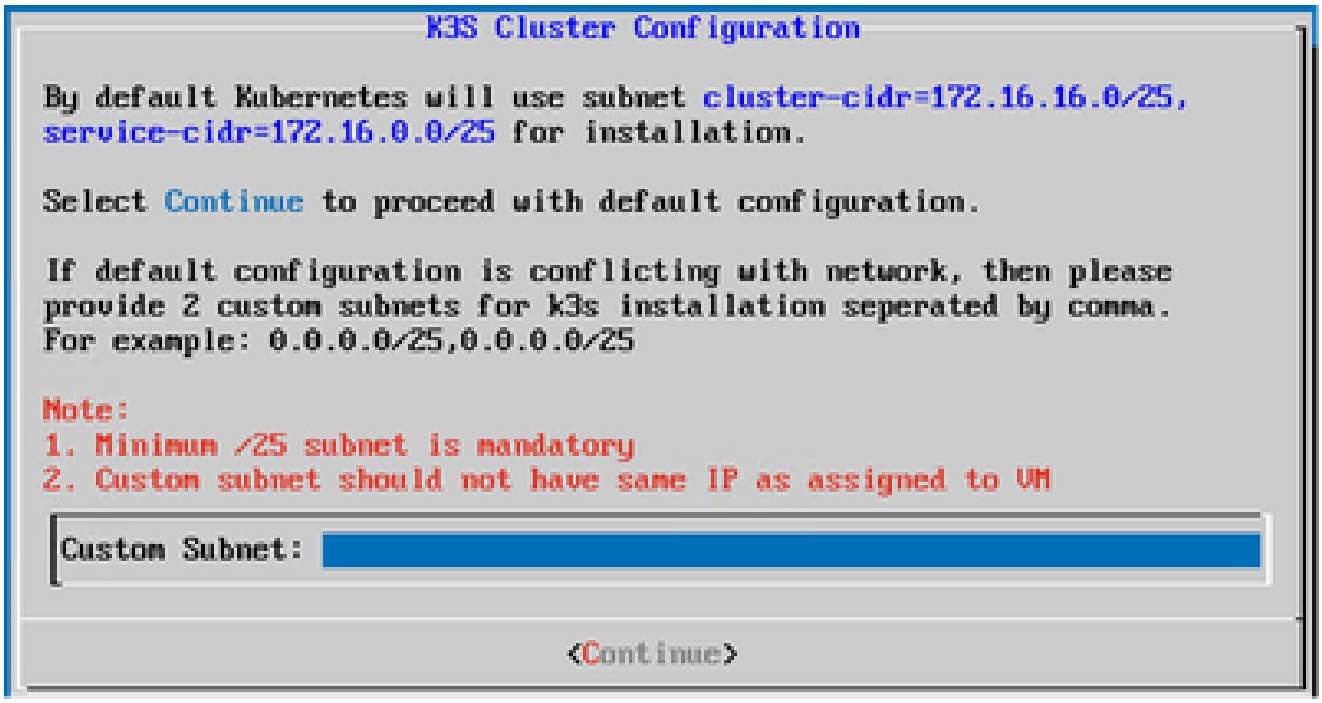
Configurazione della rete

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



Conferma

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

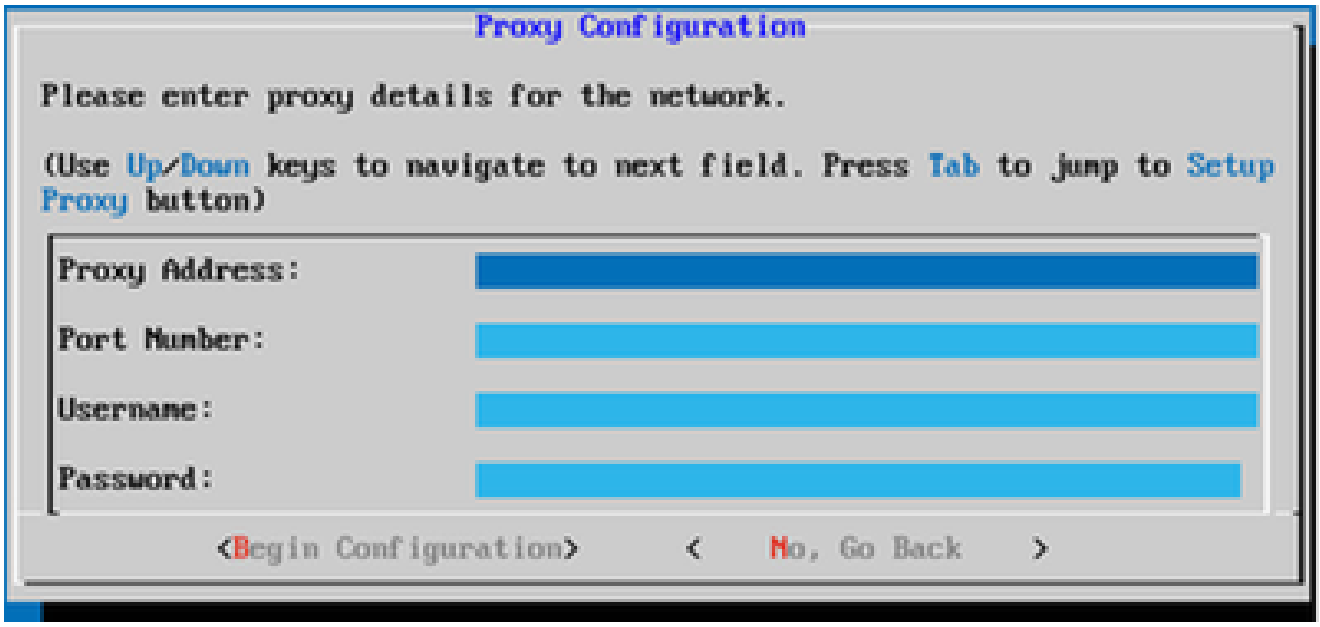


Subnet personalizzata

6. Immettere l'indirizzo IP della subnet personalizzata per la configurazione del cluster K3S (se la subnet predefinita di un cliente è in conflitto con la rete dei dispositivi, selezionare un'altra subnet personalizzata).
7. Fare clic su Continue (Continua).

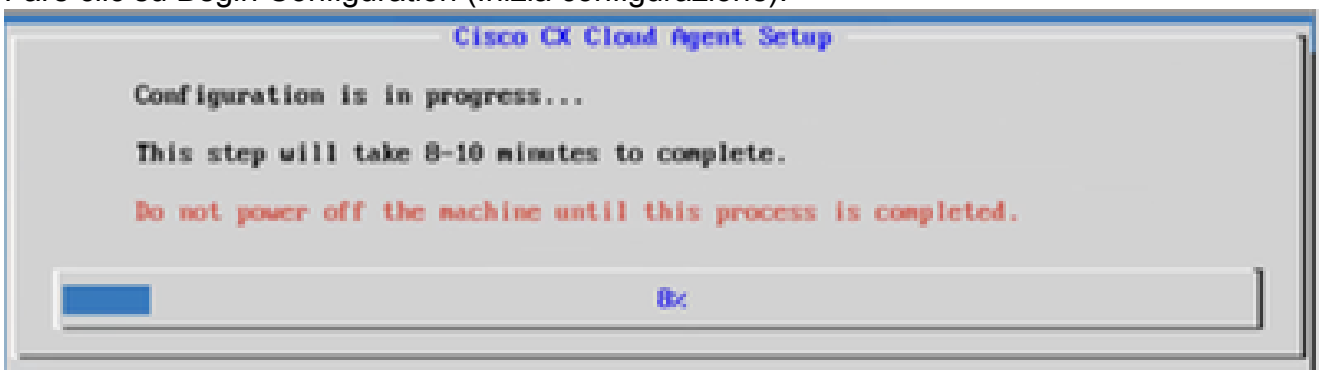
Configurazione proxy

8. Fare clic su Sì, Configura proxy per impostare i dettagli del proxy o su No, Continua alla configurazione per andare direttamente al passo 11.

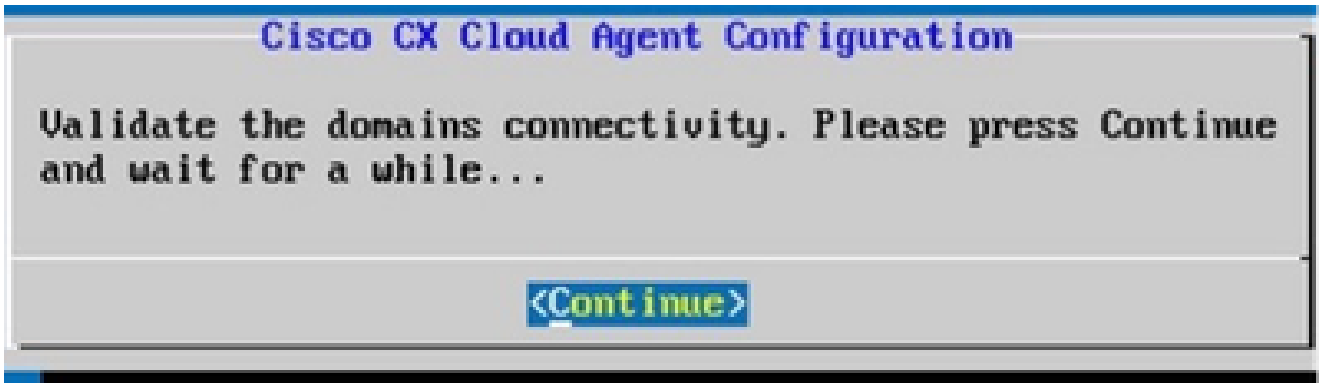


Configurazione del proxy

9. Immettere l'indirizzo proxy, il numero di porta, il nome utente e la password.
10. Fare clic su Begin Configuration (Inizia configurazione).

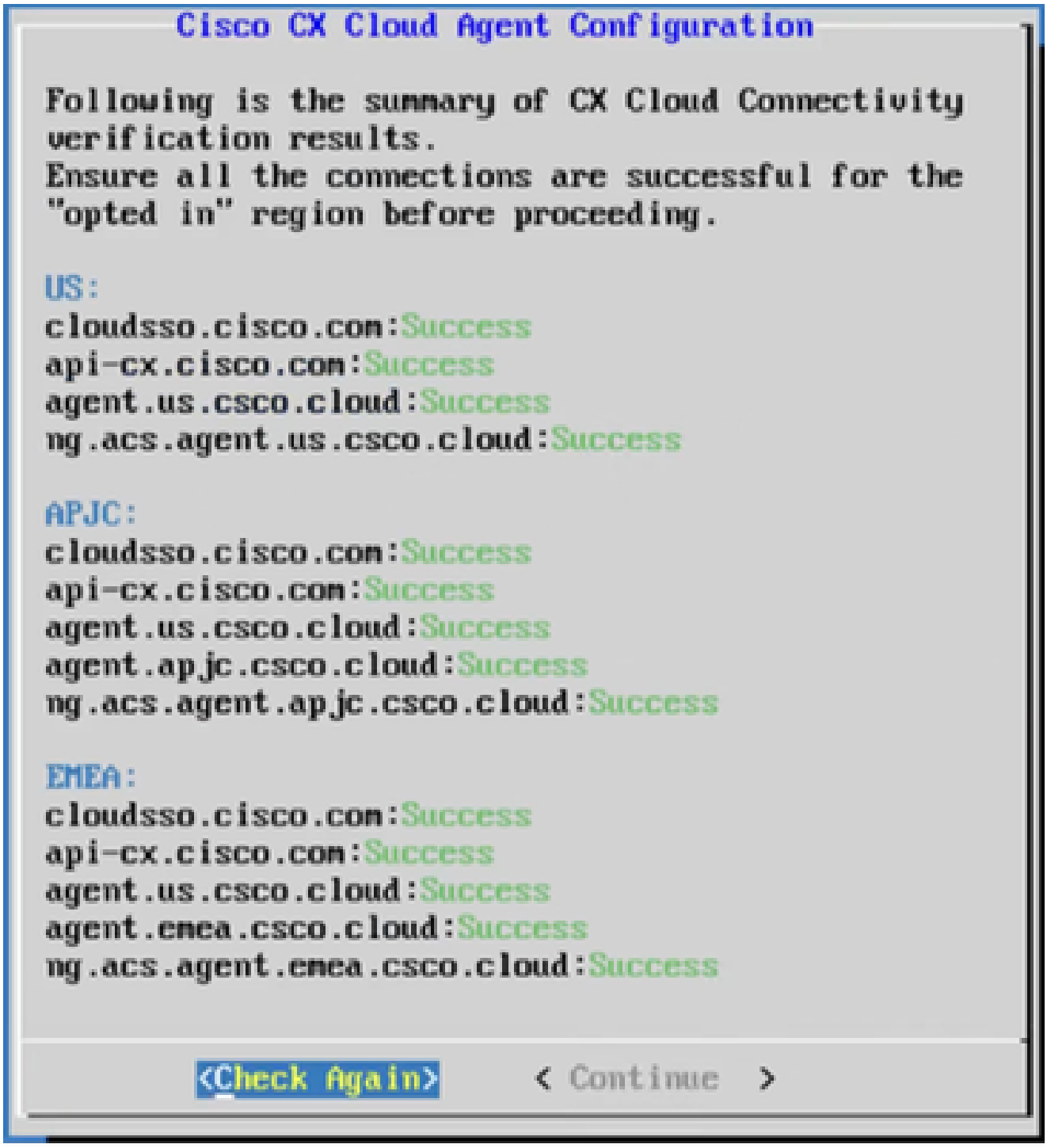


Configurazione di CX Cloud Agent



Configurazione agente cloud CX

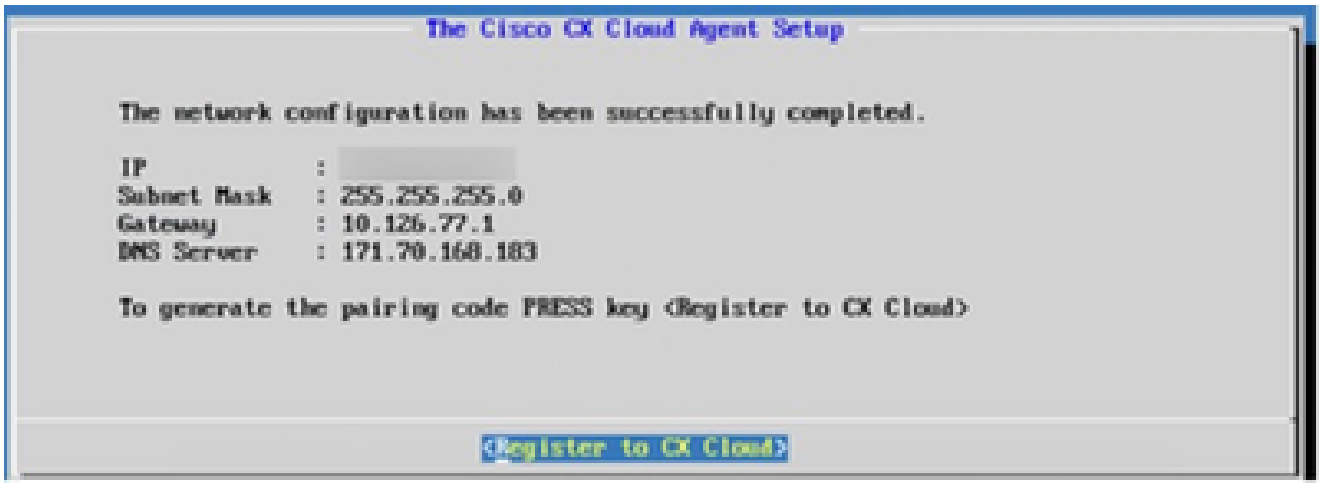
11. Fare clic su Continue (Continua).



Configurazione continua

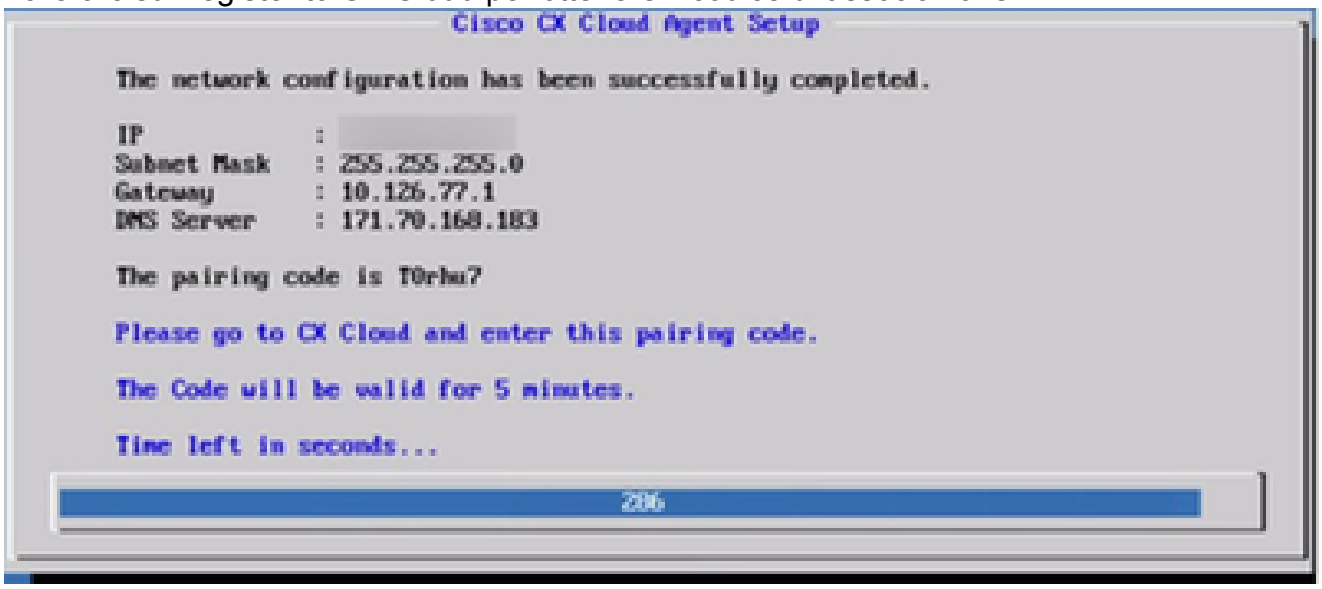
12. Fare clic su Continue (Continua) per procedere con la configurazione in modo che il dominio raggiunga correttamente il dominio. Il completamento della configurazione può richiedere alcuni minuti.

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



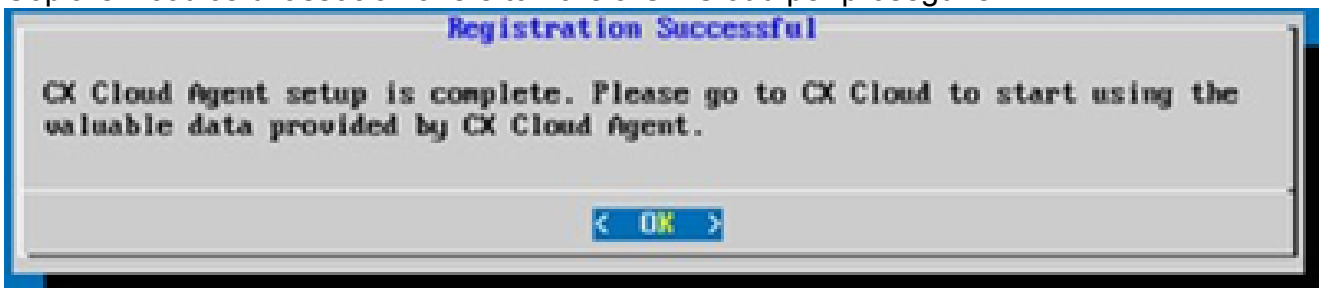
Registrazione in CX Cloud

13. Fare clic su Register to CX Cloud per ottenere il codice di associazione.



Codice di associazione

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



Registrazione completata

Nota: Se il codice di associazione scade, fare clic su Register to CX Cloud per generare un nuovo codice di associazione (passo 13).

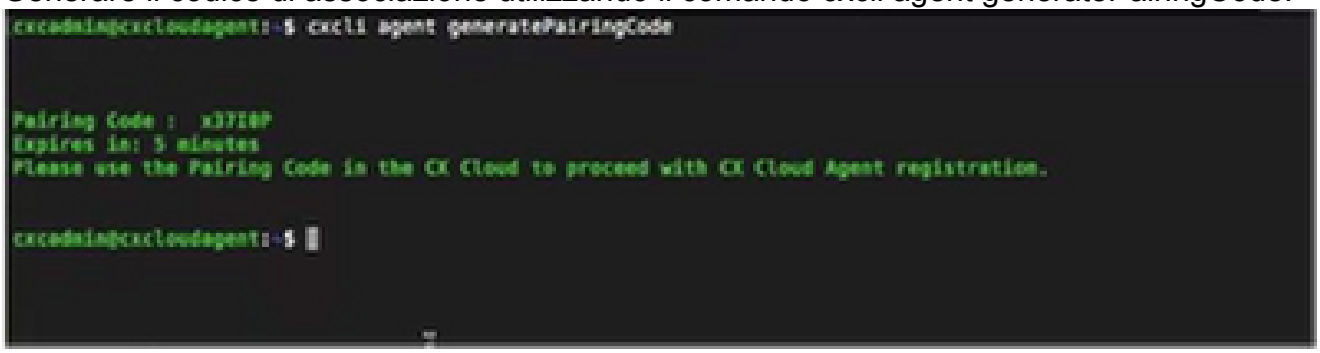
15. Fare clic su OK.

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 utilizzando 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 dei dispositivi per l'inoltro di Syslog all'agente cloud CX

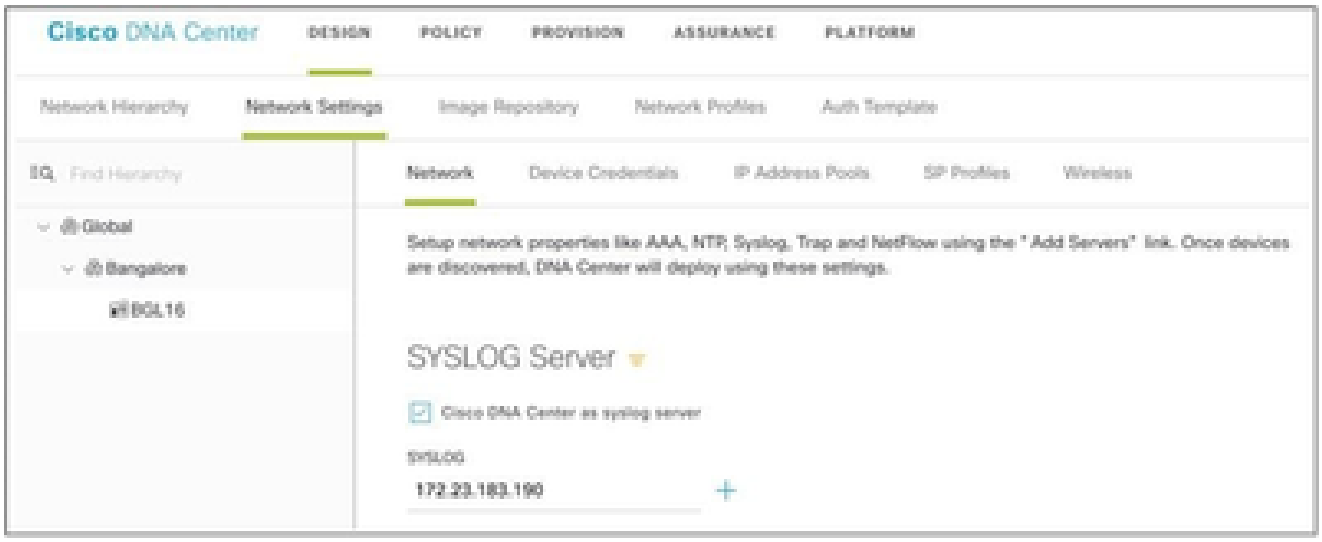
Prerequisiti

Le versioni supportate di Cisco Catalyst Center sono da 2.1.2.0 a 2.2.3.5, da 2.3.3.4 a 2.3.3.6, 2.3.5.0 e Cisco Catalyst Center Virtual Appliance

Configura impostazione inoltro syslog

Per configurare l'inoltro syslog all'agente CX nel Cisco Catalyst Center, attenersi alla seguente procedura:

1. Avviare Cisco Catalyst Center.
2. Andare a Design > Network Settings > Network (Progetto > Impostazioni di rete > Rete).
3. Per ogni sito, aggiungere l'indirizzo IP dell'agente CX come server Syslog.



Server Syslog

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

Configurazione di altre risorse (raccolta di dispositivi diretta) per inoltrare il syslog all'agente CX

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

Nota: L'agente CX riporta solo le informazioni di syslog dalle risorse Campus Success Track Level 2 a CX Cloud. Per gli altri asset non è possibile configurare il syslog per l'agente CX e i relativi dati syslog non vengono riportati in CX Cloud.

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 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 CX. Per i passaggi di configurazione specifici, consultare la documentazione.

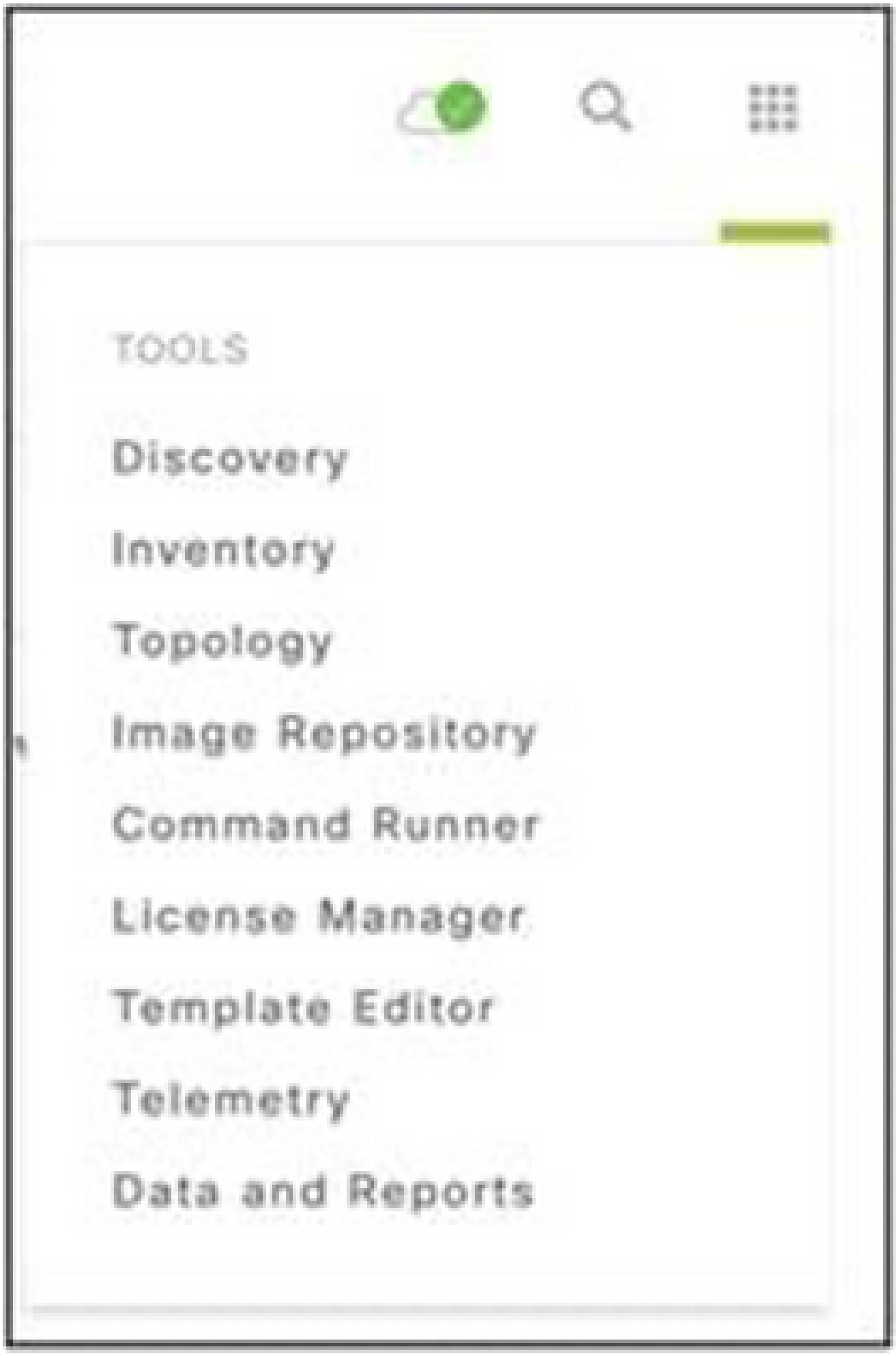
Guida alla configurazione di Cisco IOS® XE

Guida alla configurazione di AireOS Wireless Controller

Abilitazione delle impostazioni syslog a livello di informazioni per Cisco Catalyst Center

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

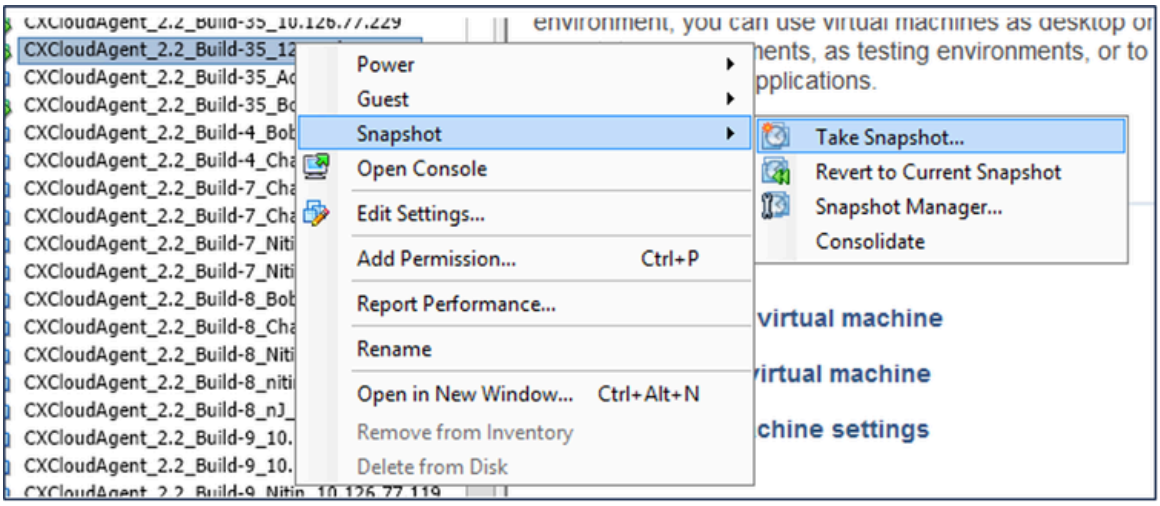
Backup e ripristino della VM del cloud CX

Si consiglia di conservare lo stato e i dati di una VM dell'agente 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.

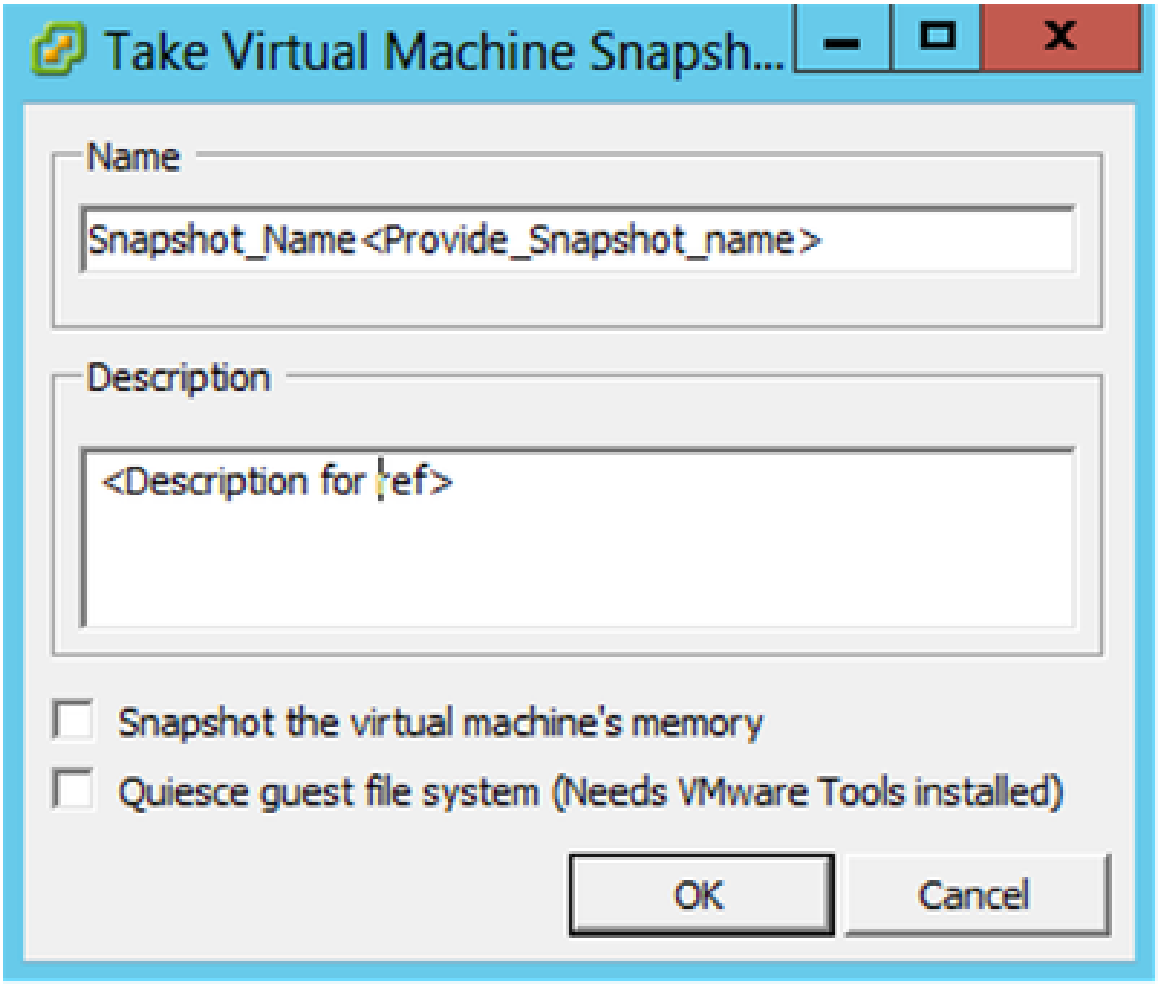
Backup della VM cloud CX

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

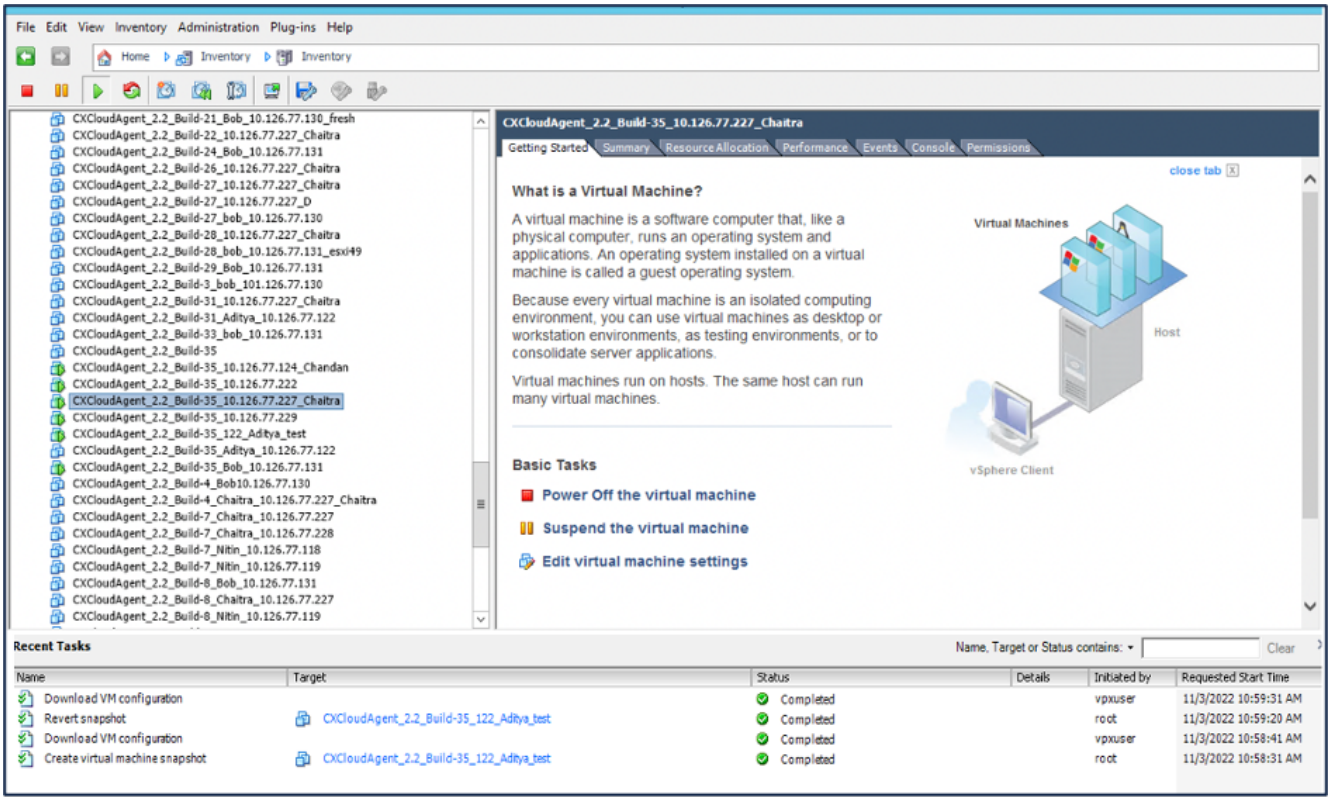


Crea snapshot macchina virtuale

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.

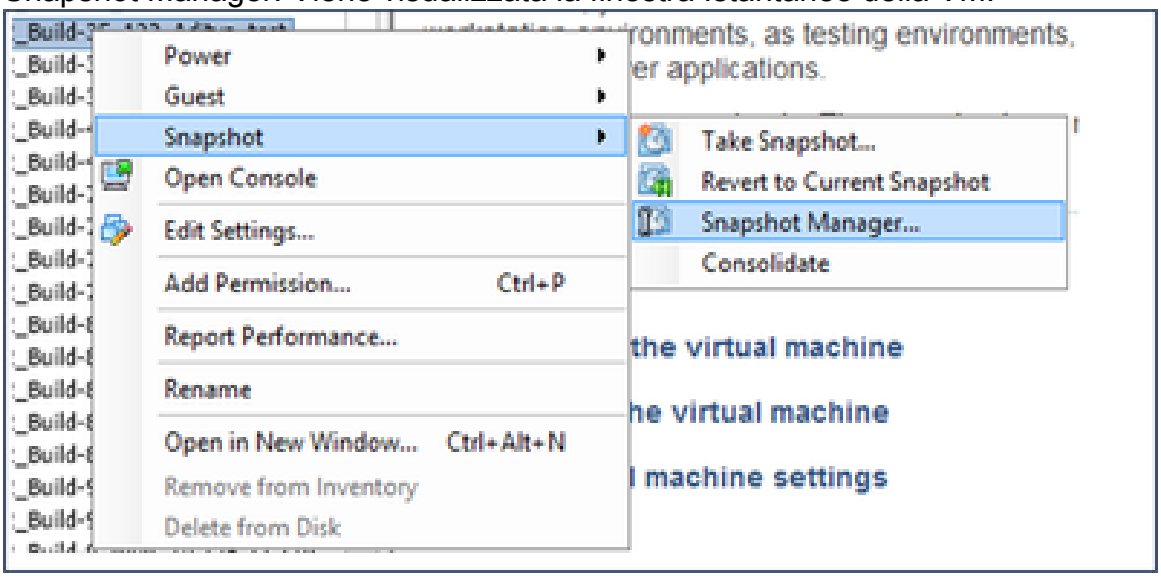


Attività recenti

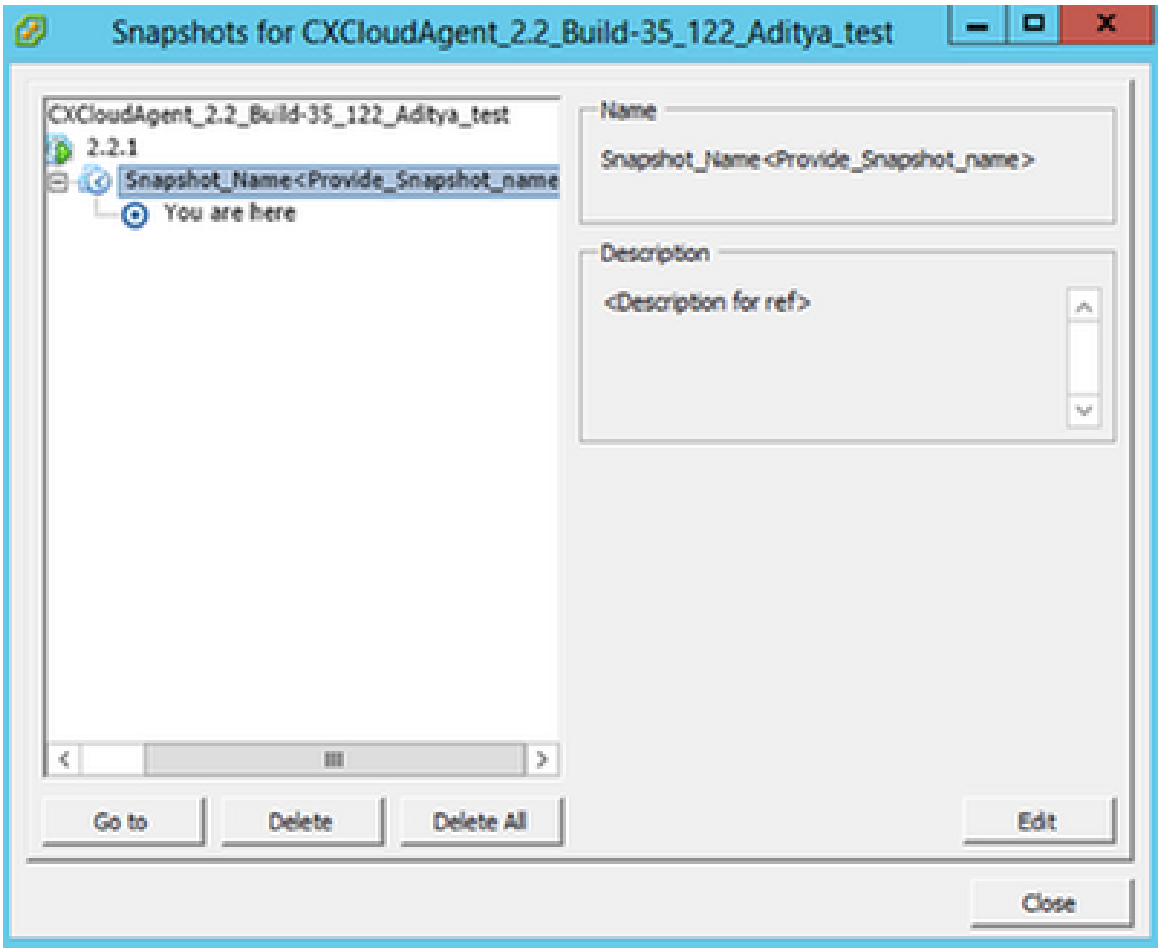
Ripristino della VM del cloud CX

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.

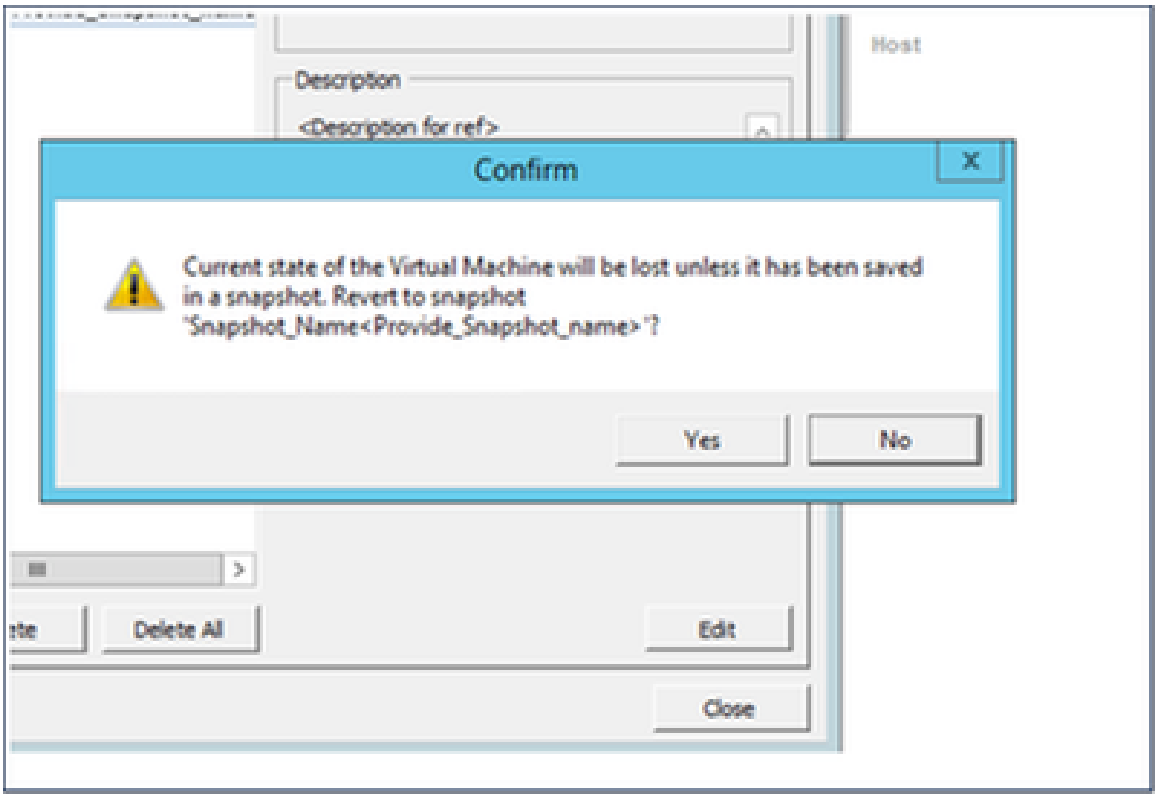


Finestra Seleziona VM



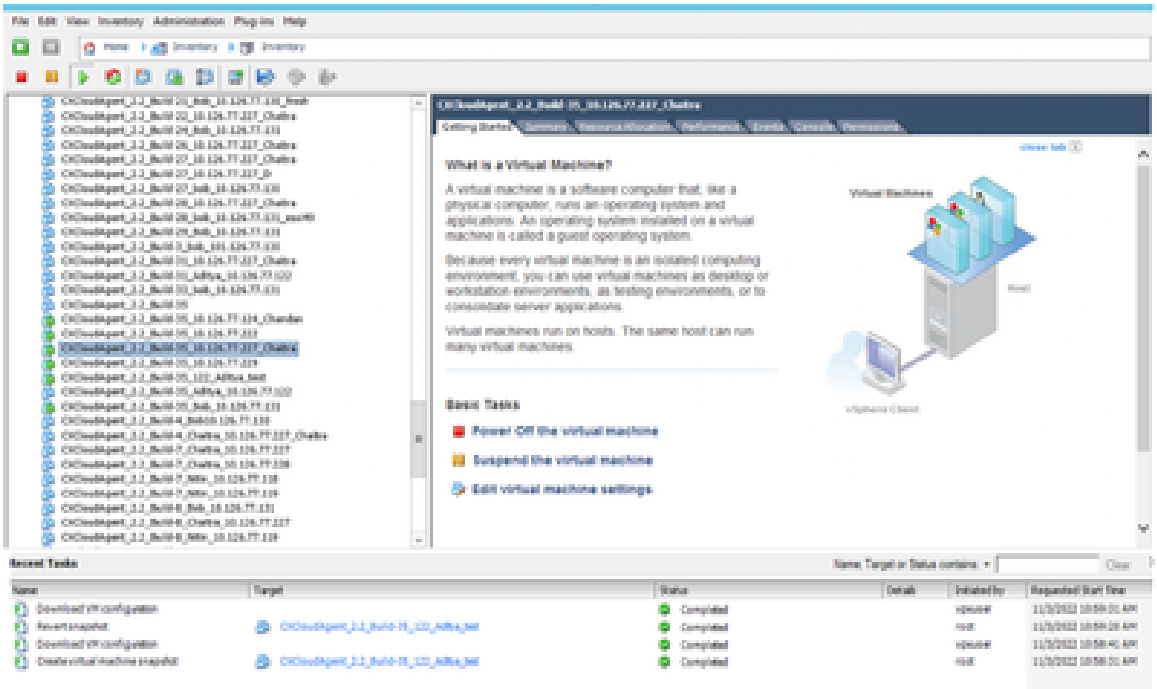
Finestra Snapshot

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



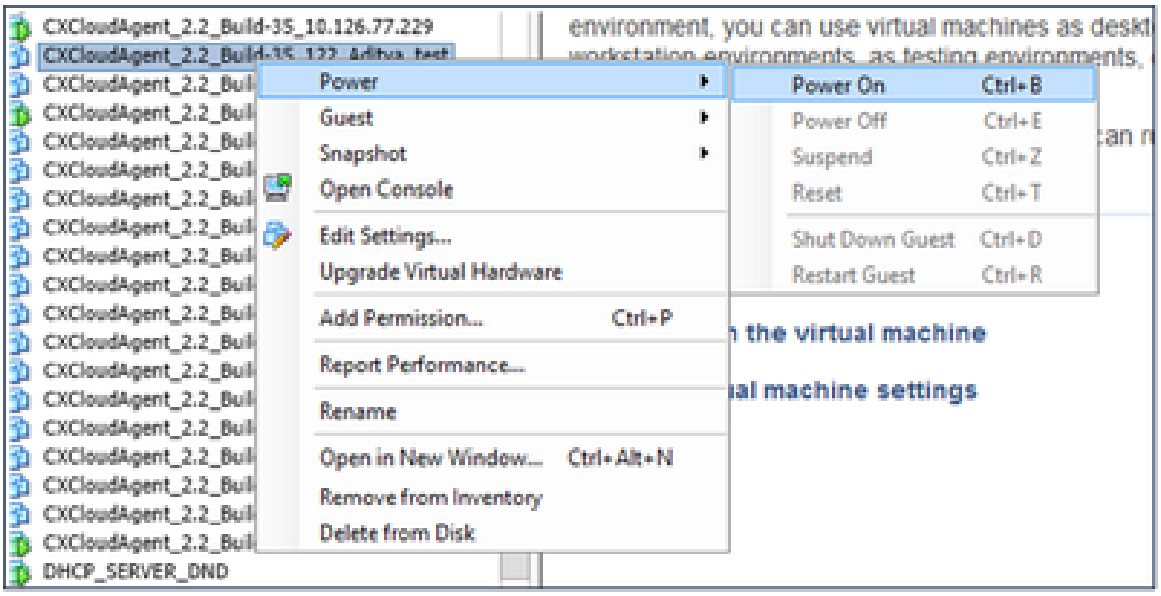
Finestra Conferma

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 Agent garantisce al cliente la sicurezza end-to-end. La connessione tra CX Cloud e CX 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 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 utente/utente cxcadmin vengono utilizzate per accedere alle API dell'agente 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 cxcroot possono ottenere i privilegi root.

Sicurezza della rete

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

Autenticazione

Autenticazione basata sulla password: L'accessorio mantiene un singolo utente (cxcadmin) che consente all'utente di autenticarsi e comunicare con l'agente 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 al portale. gli utenti cxcroot possono ottenere i privilegi root utilizzando questa password decrittografata. La passphrase è valida solo 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 Agent è conforme agli standard di protezione avanzata di Center of Internet Security.

Sicurezza dei dati

L'accessorio dell'agente CX non memorizza le informazioni personali dei clienti. L'applicazione delle credenziali del dispositivo (in esecuzione come uno dei pod) memorizza 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. In questo documento i comandi vengono classificati in base alla loro applicabilità all'inventario del Cisco Catalyst Center, al Diagnostic Bridge, a Intersight, a Compliance Insights, a

Faults e a tutte le altre fonti di telemetria raccolte dall'agente CX.

Le informazioni sensibili all'interno della telemetria degli asset vengono nascoste prima di essere trasmesse al cloud. L'agente CX maschera i dati sensibili di tutte le risorse raccolte che inviano la telemetria direttamente all'agente 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 CX. In alcuni casi, la telemetria delle risorse gestite dai controller può essere ulteriormente anonimizzata. Per ulteriori informazioni sull'anonimizzazione della telemetria, consultare la documentazione di supporto del prodotto corrispondente (ad esempio la sezione Anonimizza dati della Guida dell'amministratore di Cisco Catalyst Center).

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 descritto 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 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 dell'agente CX utilizzando cxcli e dispone dei privilegi minimi sull'accessorio; cxcroot user e la relativa password crittografata vengono generati utilizzando cxcadmin user. ·cxcroot: cxcadmin può creare questo utente utilizzando l'account remoto dell'utilità; Con questo account, l'utente può ottenere privilegi root.
Policy della	·La password ha un hash unidirezionale che utilizza SHA-256 e viene

password di cxcadmin	memorizzata in modo sicuro. · Minimo 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 contiene tre di queste categorie: maiuscole, minuscole, numeri e caratteri speciali. · Cinque tentativi di accesso 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 Catalyst Center vengono crittografate e archiviate 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).