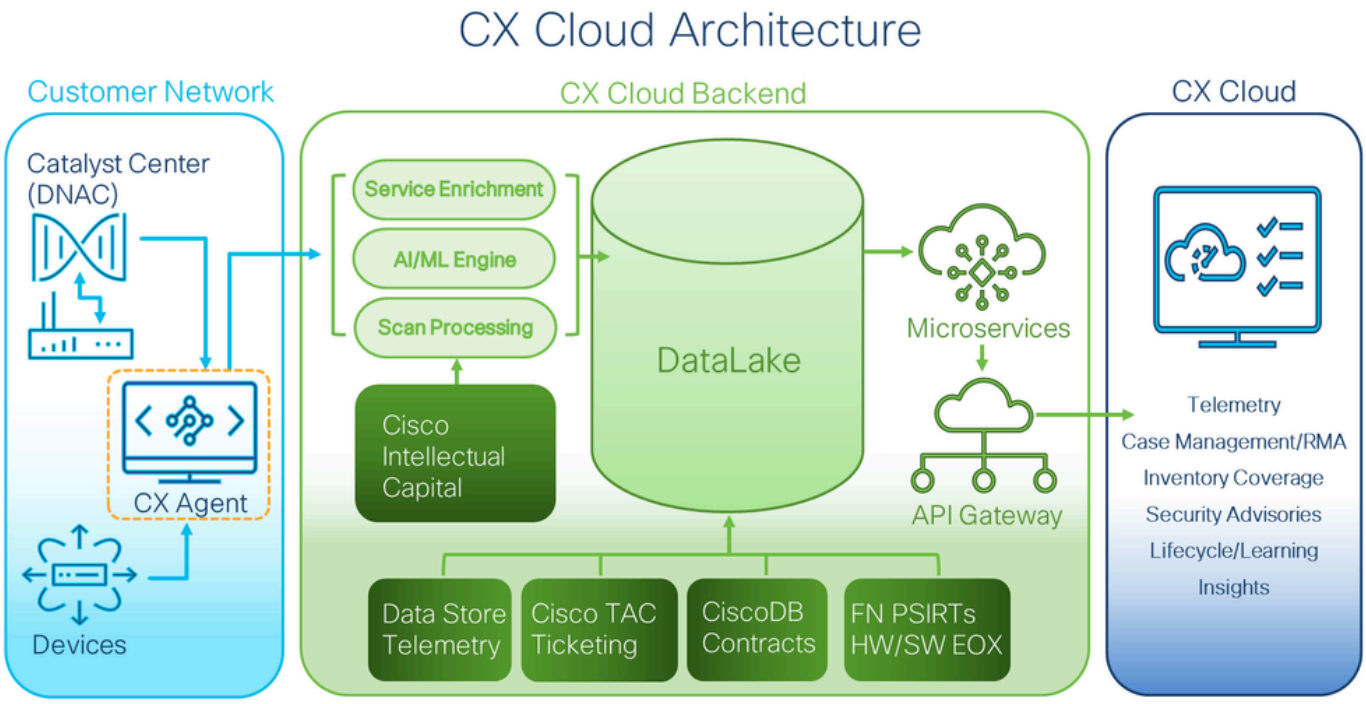
CX Cloud Agent - Übersicht v2.4

Inhalt

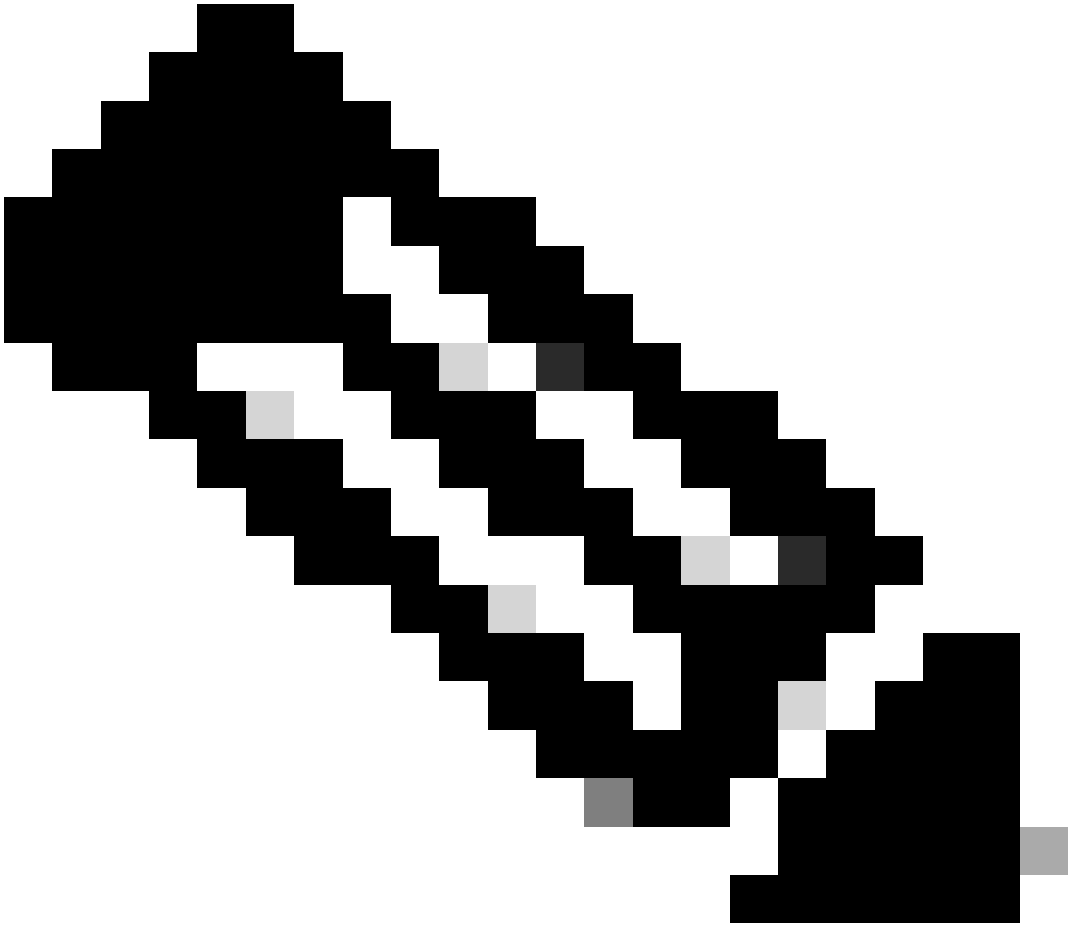
Einleitung

In diesem Dokument wird der Cisco Customer Experience (CX) Cloud Agent beschrieben. Der CX Cloud Agent von Cisco ist eine hochskalierbare Plattform, die Telemetriedaten von Kundennetzwerkgeräten erfasst, um Kunden aussagekräftige Informationen zu liefern. CX Cloud Agent ermöglicht die Umwandlung von aktiven laufenden Konfigurationsdaten in proaktive und prädiktive Einblicke, die in der CX Cloud angezeigt werden, durch künstliche Intelligenz (KI)/maschinelles Lernen (ML).



CX Cloud-Architektur

Dieses Handbuch bezieht sich speziell auf CX Cloud Agent v2.4. Auf der Seite Cisco CX Cloud Agent können Sie auf frühere Versionen zugreifen.



Hinweis: Die Bilder in dieser Anleitung dienen nur zu Referenzzwecken. Die tatsächlichen Inhalte können variieren.

Voraussetzungen

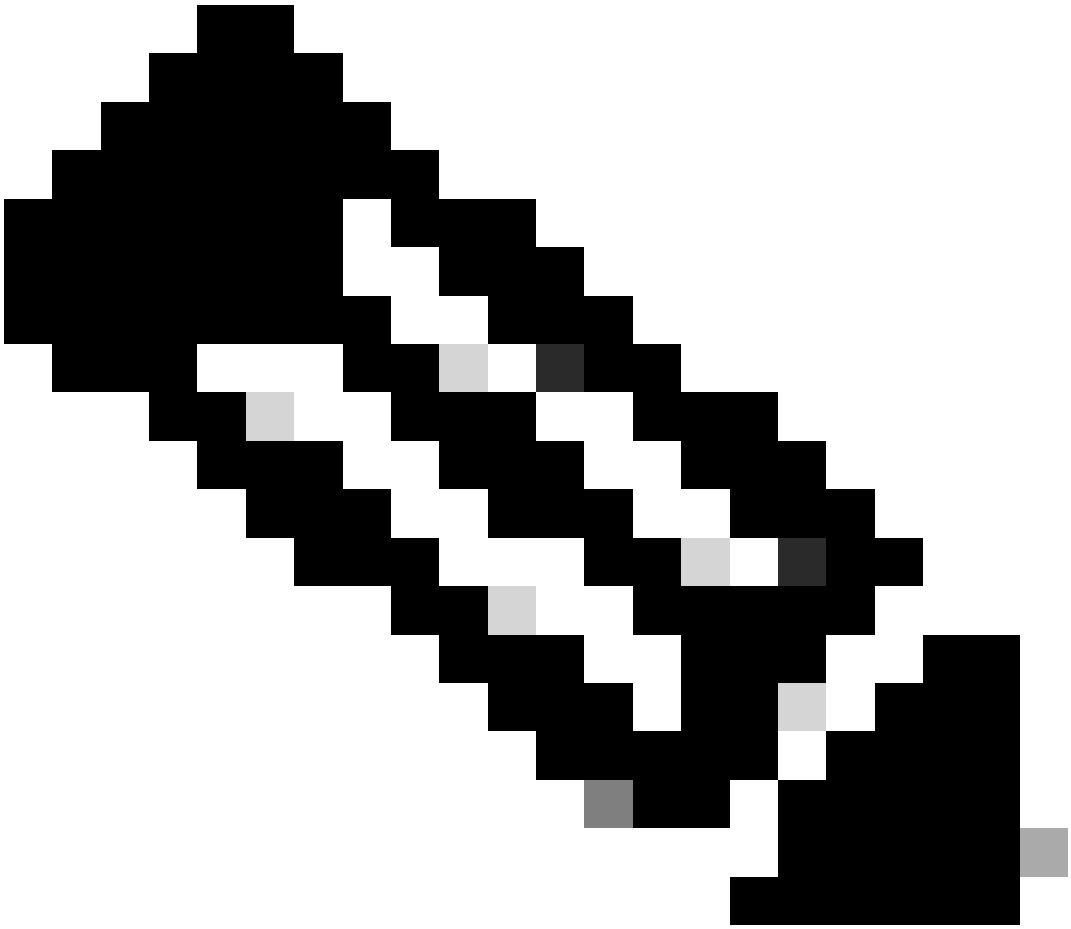
CX Cloud Agent wird als virtuelles System ausgeführt und kann als Open Virtual Appliance (OVA) oder als Virtual Hard Disk (VHD) heruntergeladen werden.

Bereitstellungsanforderungen

- Für eine Neuinstallation ist einer der folgenden Hypervisoren erforderlich:
  - VMware ESXi Version 5.5 oder höher
  - Oracle Virtual Box 5.2.30 oder höher
  - Windows-Hypervisor Version 2012 bis 2022
- Die Konfigurationen in der folgenden Tabelle sind für die Bereitstellung von VM erforderlich:

Bereitstellungstyp des CX Cloud Agent	Anzahl der CPU-Kerne	RAM	Festplatte	* Maximale Anzahl der Ressourcen, die direkt mit CX Cloud Agent verbunden sind
Kleine OVA	8 C	16 GB	200 GB	10,000
Mittlere OVA	16 C	32 GB	600 GB	20,000
Große OVA	32 C	64 GB	1200 GB	50,000:

* Zusätzlich zur Verbindung von 20 Cisco DNA Center-Nicht-Clustern oder 10 Cisco DNA Center-Clustern für jede CX Cloud Agent-Instanz.



Hinweis: Flexible OVA/Patch 2.4 für mittlere und große Konfigurationen ist nur für VMware

---

ESXi VMs verfügbar. Oracle VirtualBox und Windows Hyper-V können nicht für mittlere und große Konfigurationen verwendet werden.

- Für Kunden, die ausgewiesene US-Rechenzentren als primäre Datenregion zur Speicherung von CX Cloud-Daten verwenden, muss der CX Cloud Agent in der Lage sein, eine Verbindung zu den hier gezeigten Servern herzustellen. Hierzu muss der FQDN (Fully Qualified Domain Name) verwendet werden und HTTPS auf TCP-Port 443:
  - FQDN: agent.us.csco.cloud
  - FQDN: ng.acs.agent.us.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Für Kunden, die bestimmte europäische Rechenzentren als primäre Datenregion für die Speicherung von CX Cloud-Daten verwenden: Der CX Cloud Agent muss in der Lage sein, über FQDN und HTTPS auf TCP-Port 443 eine Verbindung zu beiden hier gezeigten Servern herzustellen:
  - FQDN: agent.us.csco.cloud
  - FQDN: agent.emea.cisco.cloud
  - FQDN: ng.acs.agent.emea.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Für Kunden, die ausgewiesene Rechenzentren im Asien-Pazifik-Raum als primäre Datenregion für die Speicherung von CX Cloud-Daten verwenden: Der CX Cloud Agent muss in der Lage sein, über FQDN und HTTPS auf TCP-Port 443 eine Verbindung zu beiden hier gezeigten Servern herzustellen:
  - FQDN: agent.us.csco.cloud
  - FQDN: agent.apjc.csco.cloud
  - FQDN: ng.acs.agent.apjc.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Für Kunden, die bestimmte Rechenzentren in Europa und im Asien-Pazifik-Raum als primäre Datenregion nutzen, ist eine Verbindung zu FQDN: agent.us.csco.cloud nur für die Registrierung des CX Cloud Agent bei CX Cloud während der Ersteinrichtung erforderlich. Nachdem der CX Cloud Agent erfolgreich bei CX Cloud registriert wurde, ist diese Verbindung nicht mehr erforderlich.
- Für die lokale Verwaltung des CX Cloud Agent muss Port 22 zugänglich sein.
- Die folgende Tabelle enthält eine Zusammenfassung der Ports und Protokolle, die geöffnet und aktiviert werden müssen, damit CX Cloud Agent ordnungsgemäß funktioniert:

CX Cloud Agent Traffic

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

- Eine IP wird automatisch erkannt, wenn das Dynamic Host Configuration Protocol (DHCP) in der VM-Umgebung aktiviert ist. Andernfalls müssen eine kostenlose IPv4-Adresse, eine Subnetzmaske, eine Standard-Gateway-IP-Adresse und eine IP-Adresse des Domain Name Service (DNS)-Servers verfügbar sein.
- Nur IPv4 wird unterstützt.
- Die zertifizierten Einzelknoten- und Hochverfügbarkeits-Cluster-Versionen von Cisco DNA Center sind 2.1.2.x bis 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x sowie die Cisco Catalyst Center Virtual Appliance und die Cisco DNA Center Virtual Appliance.
- Wenn das Netzwerk über eine SSL-Überwachung verfügt, geben Sie die IP-Adresse des CX Cloud Agent an.
- Für alle direkt verbundenen Ressourcen ist die SSH-Privilegstufe 15 erforderlich.
- Verwenden Sie nur die angegebenen Hostnamen. Statische IP-Adressen können nicht verwendet werden.

Zugriff auf kritische Domänen

Um mit der CX Cloud zu beginnen, benötigen Benutzer Zugriff auf diese Domänen. Verwenden Sie nur die angegebenen Hostnamen und keine statischen IP-Adressen.

Spezifische Domänen des CX Cloud Agent-Portals

Hauptdomänen	Andere Domänen
csco.cloud	cloudfront.net
	eum-appdynamics.com

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

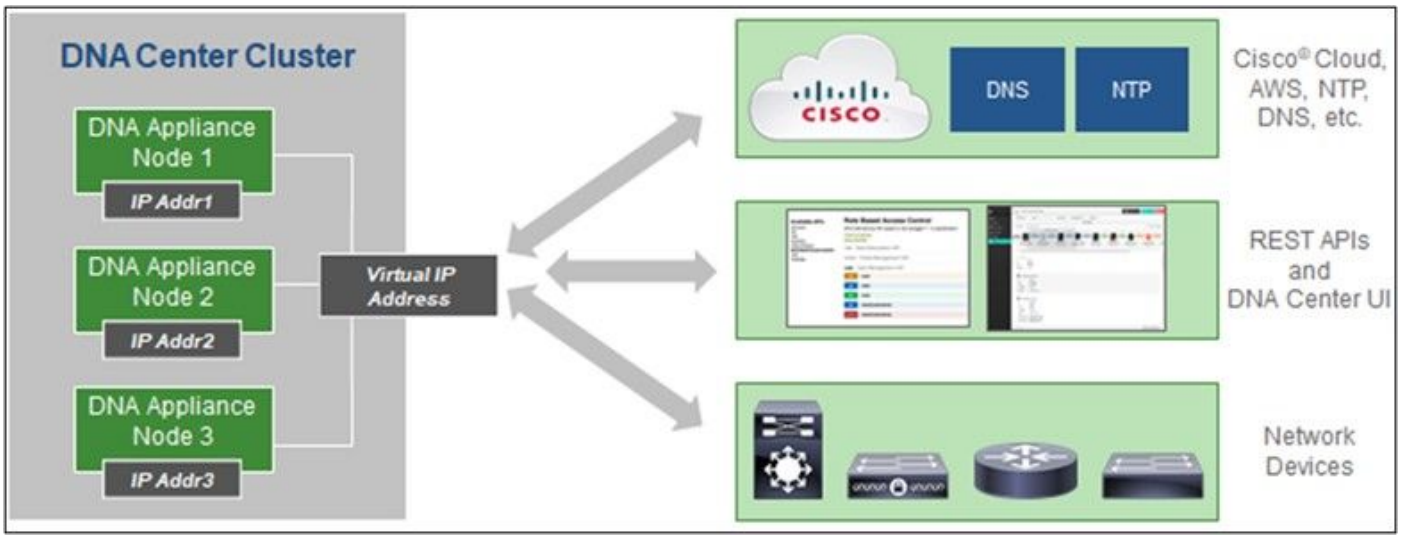
Für CX Cloud Agent OVA spezifische Domänen

NORD- UND SÜDAMERIKA	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	agent.emea.csco.cloud	agent.apjc.csco.cloud
	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Hinweis: Der ausgehende Zugang muss mit aktivierter Umleitung auf Port 443 für die angegebenen FQDNs zugelassen werden.

Von Cisco DNA Center unterstützte Version

Unterstützte Einzelknoten- und HA-Cluster-Versionen von Cisco DNA Center sind 2.1.2.x bis 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x sowie Cisco Catalyst Center Virtual Appliance und Cisco DNA Center Virtual Appliance.



Cisco DNA Center mit HA-Cluster mit mehreren Knoten

Unterstützte Browser

Für eine optimale Nutzung auf Cisco.com wird die neueste offizielle Version dieser Browser empfohlen:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Liste der unterstützten Produkte

Eine Liste der von CX Cloud Agent unterstützten Produkte finden Sie in der Liste der unterstützten Produkte.

Upgrade/Installation von CX Cloud Agent v2.4

- Bestehende Kunden, die ein Upgrade auf die neue Version durchführen, finden weitere Informationen unter Upgrade CX Cloud Agent v2.4.
- Neue Kunden, die eine neue, flexible OVA v2.4-Installation implementieren, sollten sich auf Hinzufügen von CX Cloud Agent als Datenquelle beziehen.

Aktualisieren vorhandener VMs auf große und mittlere Konfigurationen

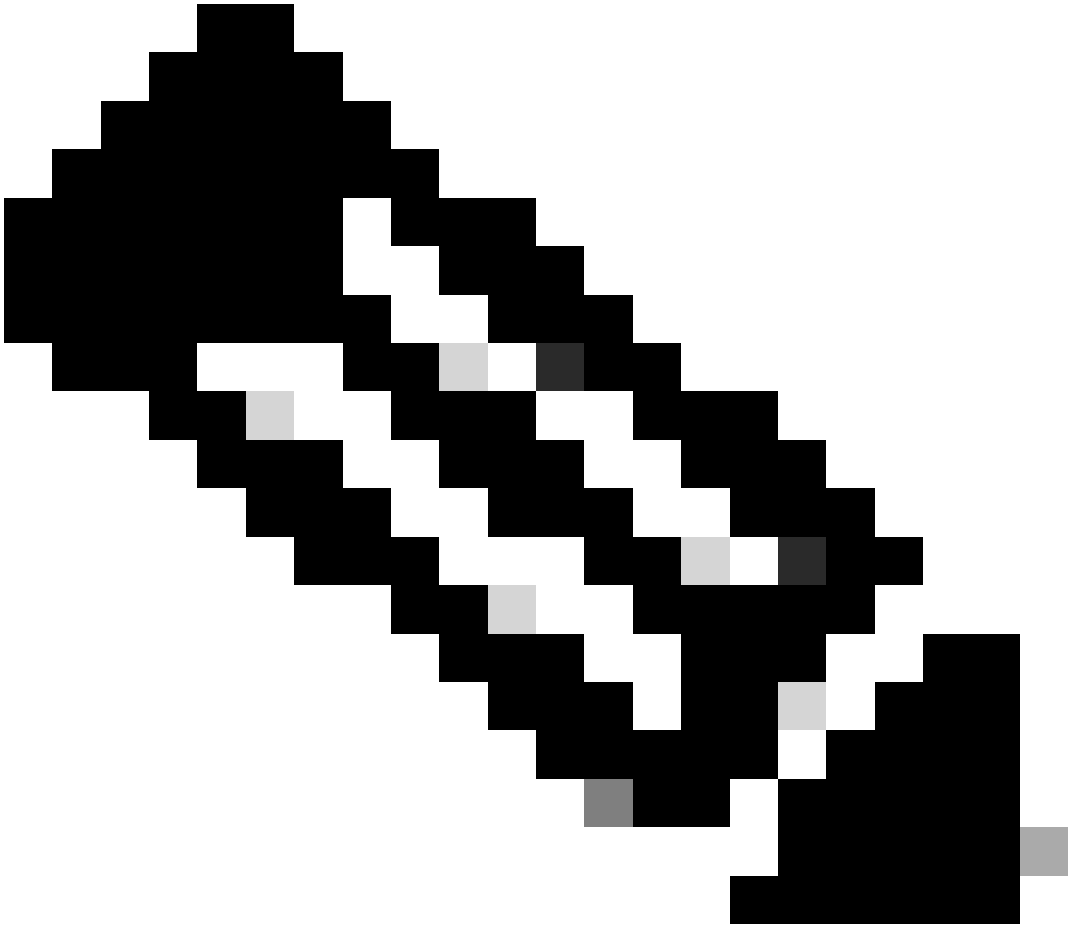
Kunden können ihre vorhandene VM-Konfiguration mithilfe flexibler OVA-Optionen je nach Netzwerkgröße und -komplexität auf mittlere oder große Systeme aktualisieren.

Informationen zum Upgrade der vorhandenen VM-Konfiguration von klein auf mittel oder groß finden Sie im Abschnitt Upgrade von CX Cloud Agent-VMs auf mittel- und große Konfiguration.

Upgrade von CX Cloud Agent v2.4

Kunden mit CX Cloud Agent v2.3.x oder höher können die in diesem Abschnitt beschriebenen

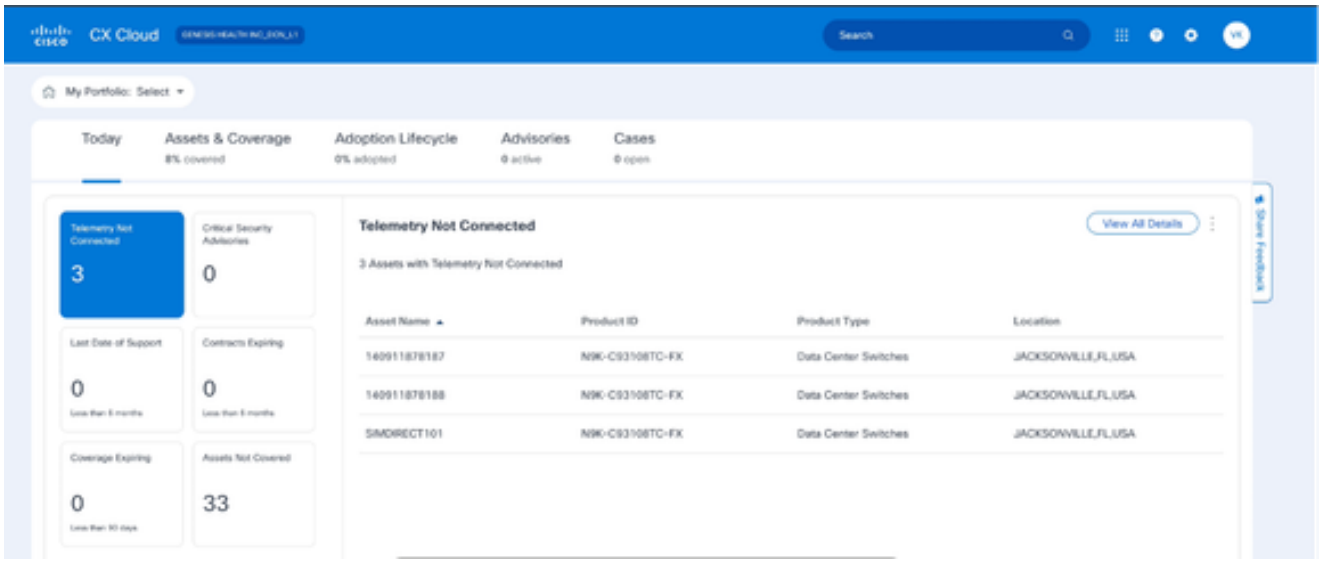
Schritte für ein direktes Upgrade auf v2.4 ausführen.



> Hinweis: Kunden mit CX Cloud Agent v2.2.x sollten ein Upgrade auf v2.3.x durchführen, bevor sie ein Upgrade auf v2.4 durchführen, oder v2.4 als neue OVA-Installation installieren.

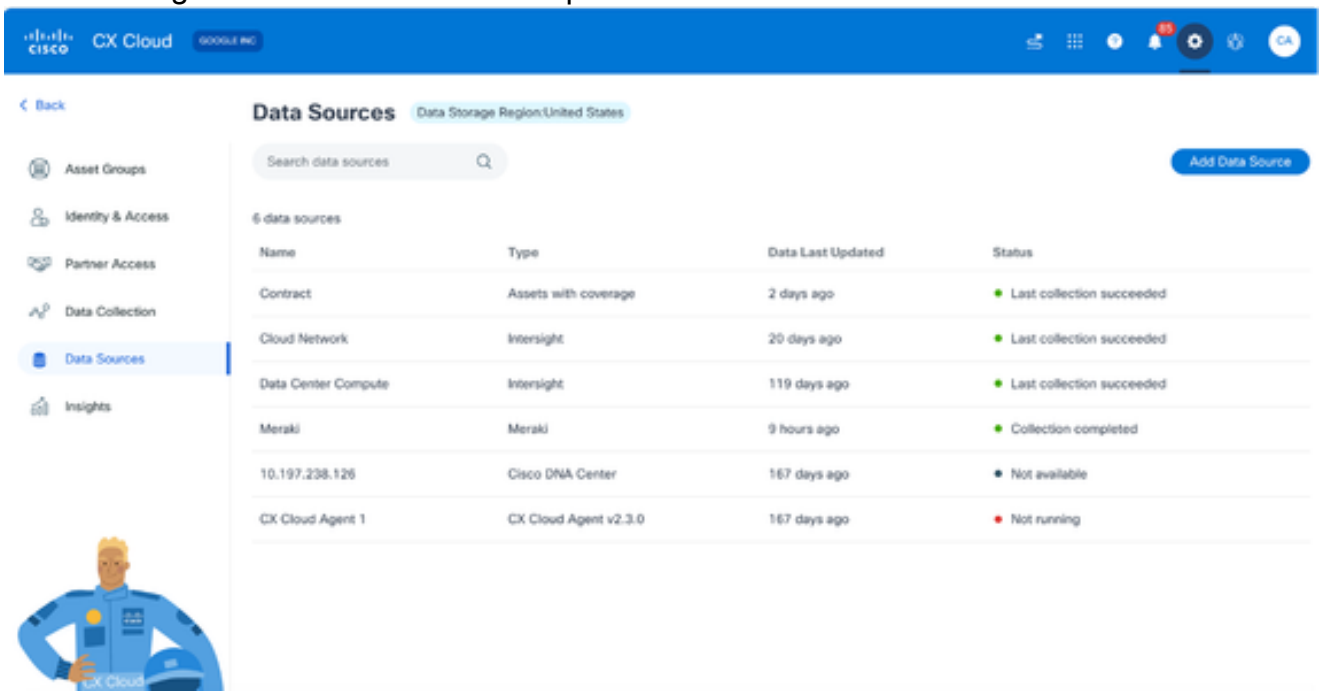
So installieren Sie CX Cloud Agent Upgrade v2.4 von CX Cloud:

1. Melden Sie sich bei CX Cloud an. Die Startseite wird angezeigt.



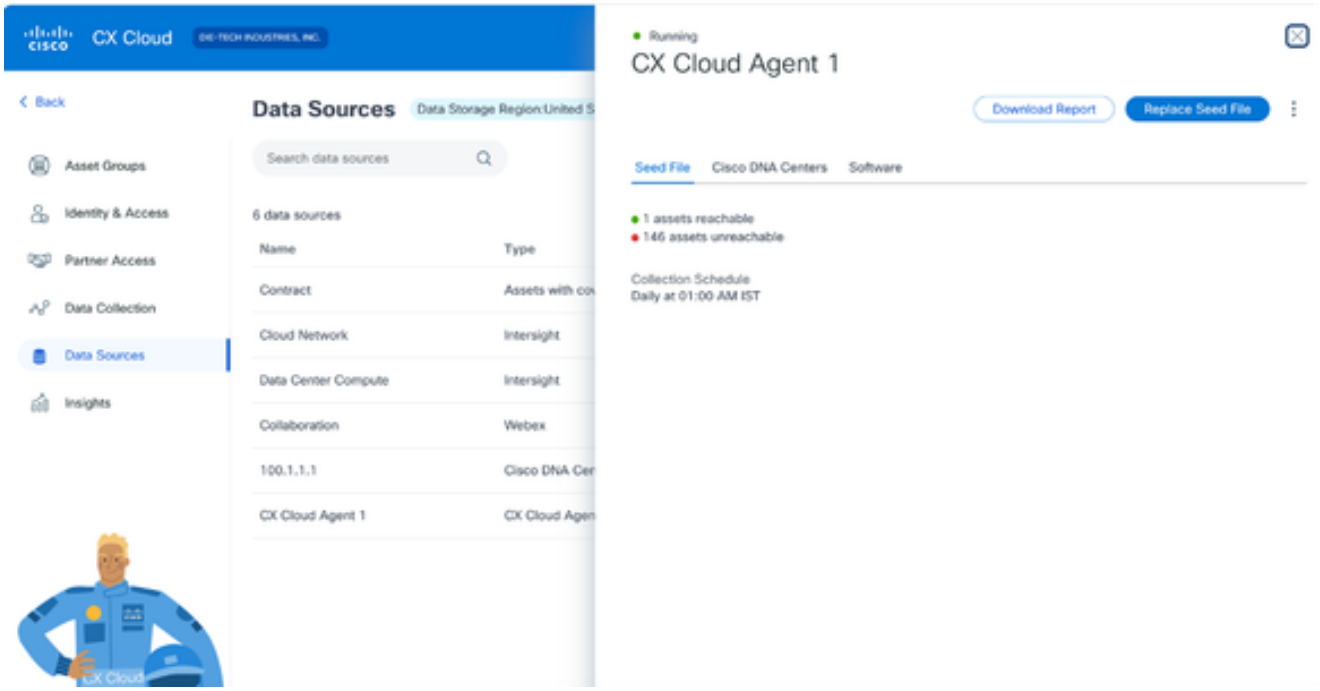
CX Cloud-Startseite

2. Klicken Sie auf das Symbol Admin Center. Das Fenster Datenquellen wird geöffnet und zeigt CX Cloud Agent als vorhandene Datenquelle an.



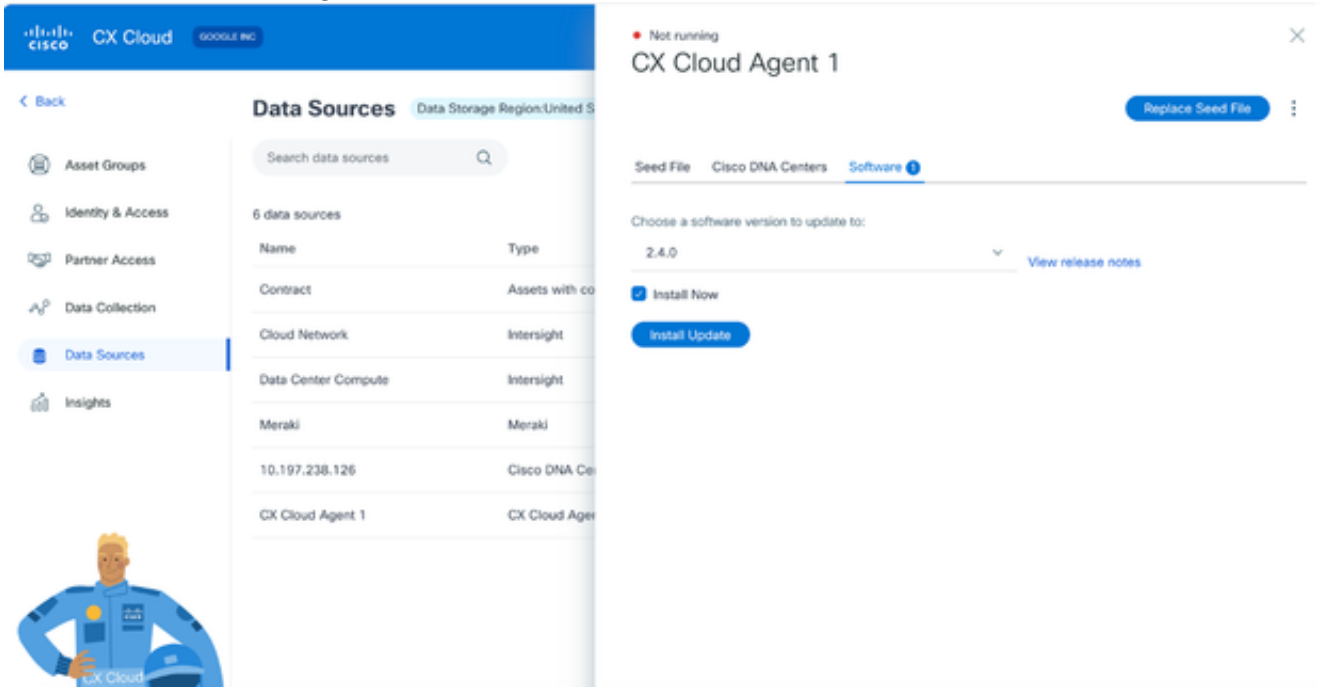
Datenquellen

3. Klicken Sie auf die Datenquelle CX Cloud Agent. Das Detailfenster CX Cloud Agent wird geöffnet.



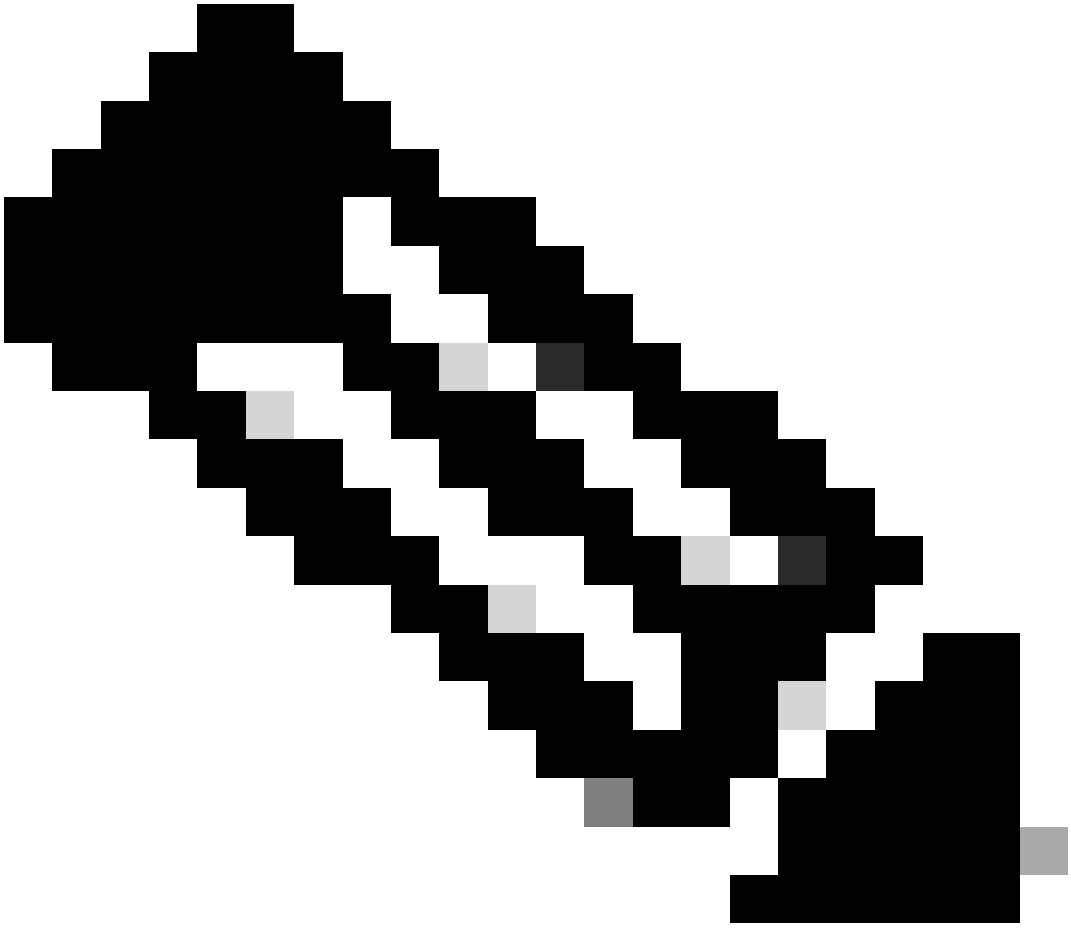
Datenquellen-Detailansicht

4. Klicken Sie auf die Registerkarte Software.



CX Cloud Agent - Detailansicht

5. Wählen Sie die Softwareversion 2.4.0 aus dem Dropdown-Menü Wählen Sie eine Softwareversion aus, die aktualisiert werden soll.
6. Klicken Sie auf Update installieren, um CX Cloud Agent v2.4.0 zu installieren.



Hinweis: Kunden können die Aktualisierung für einen späteren Zeitpunkt planen, indem sie das Kontrollkästchen Jetzt installieren deaktivieren, das Planungsoptionen anzeigt.

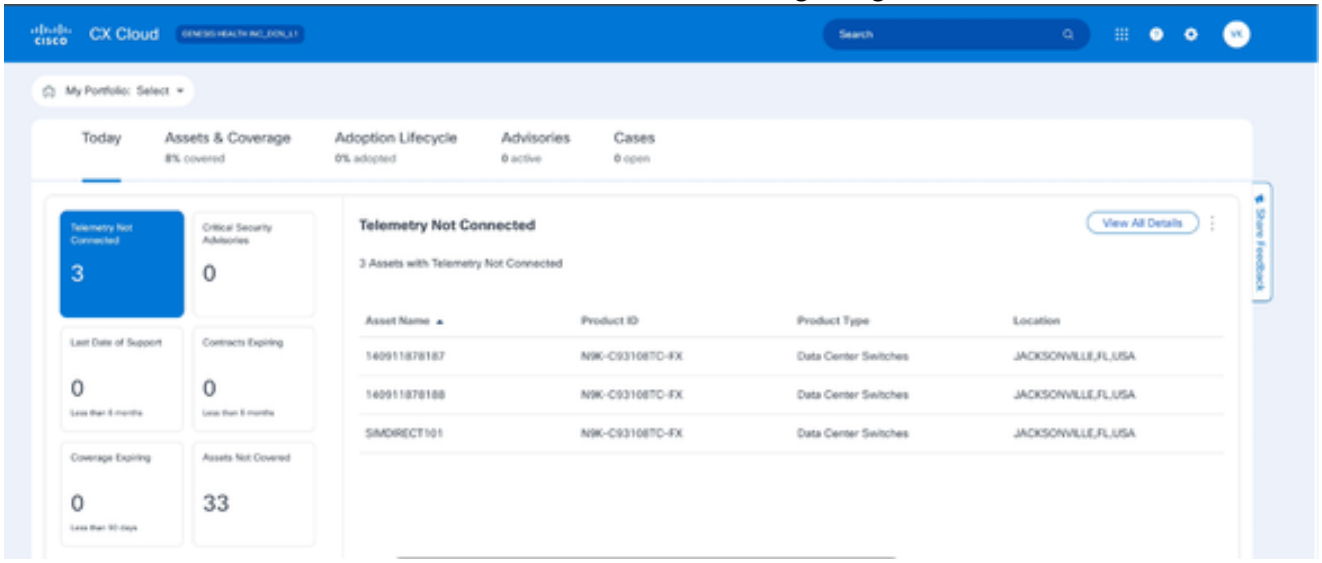
Hinzufügen von CX Cloud Agent

Kunden können bis zu zwanzig (20) CX Cloud Agent-Instanzen in CX Cloud hinzufügen.

So fügen Sie einen CX Cloud Agent hinzu:

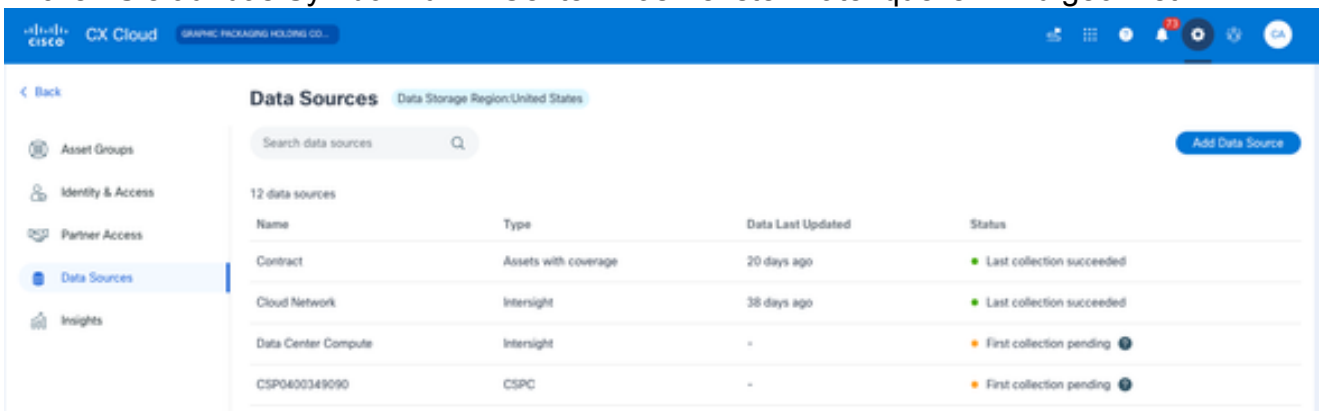
Hinweis: Wiederholen Sie die folgenden Schritte, um weitere CX Cloud Agent-Instanzen als Datenquelle hinzuzufügen.

1. Melden Sie sich bei CX Cloud an. Die Startseite wird angezeigt.



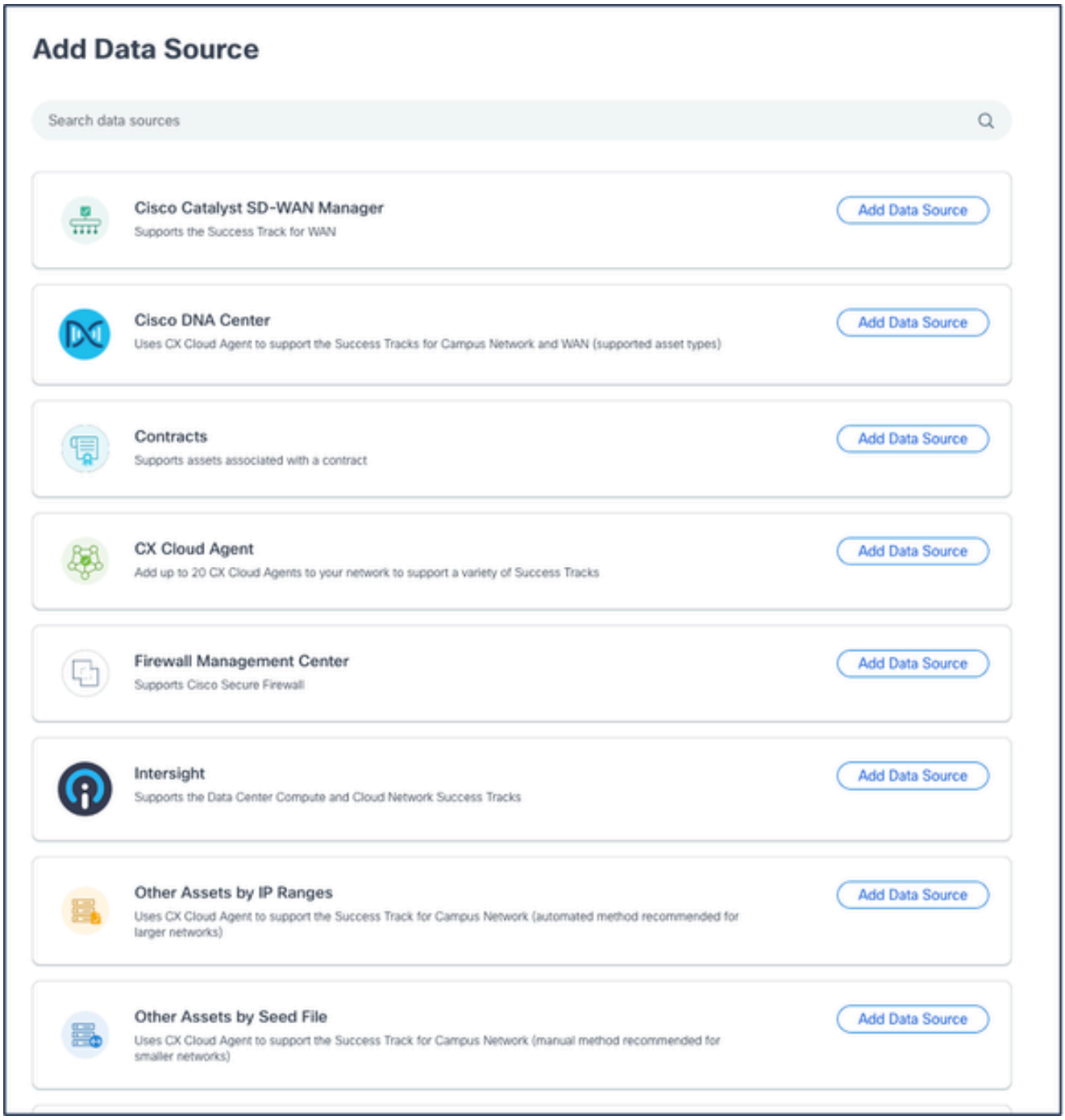
CX Cloud-Startseite

2. Klicken Sie auf das Symbol Admin Center. Das Fenster Datenquellen wird geöffnet.



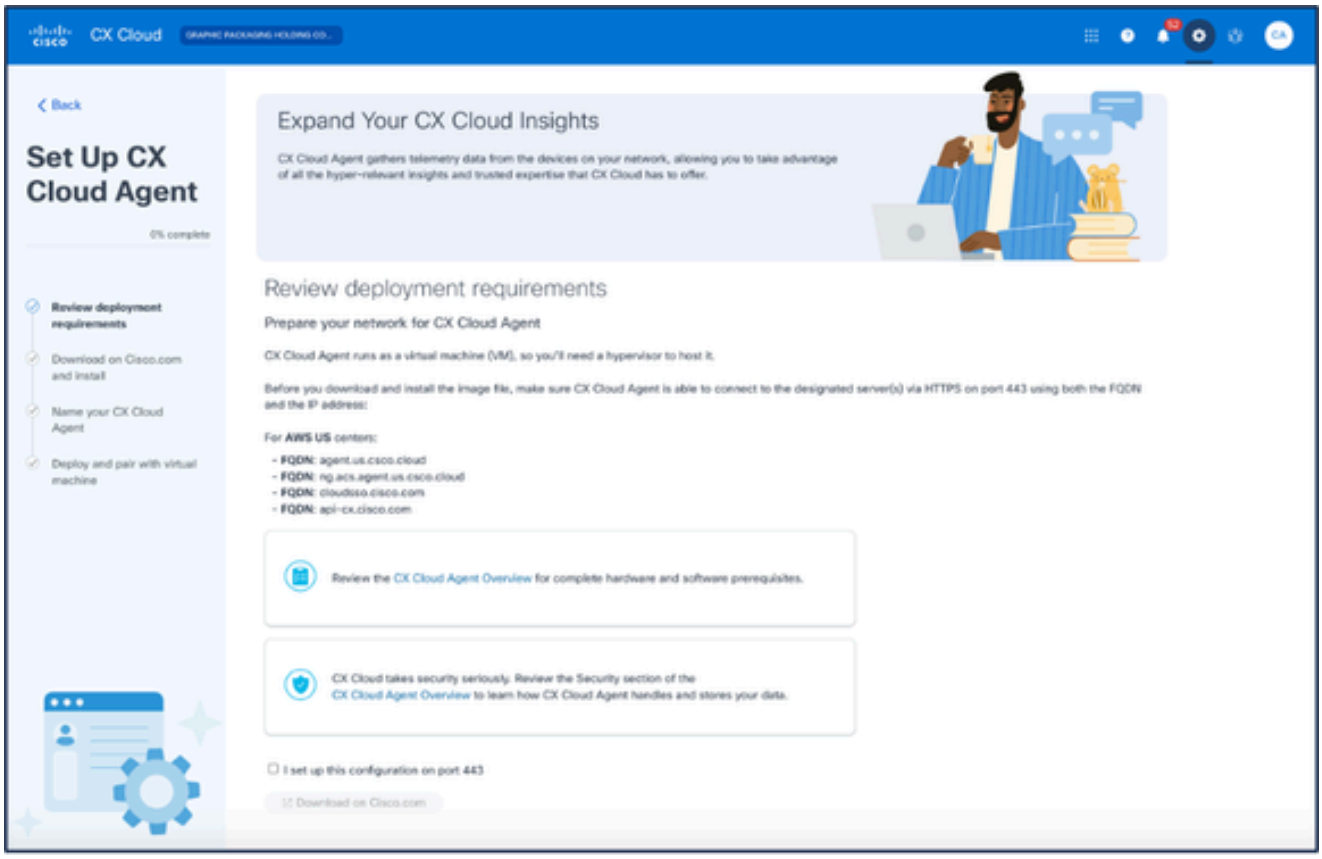
Datenquellen

3. Klicken Sie auf Datenquelle hinzufügen. Das Fenster Datenquelle hinzufügen wird geöffnet. Die angezeigten Optionen variieren je nach Kundenabonnements.



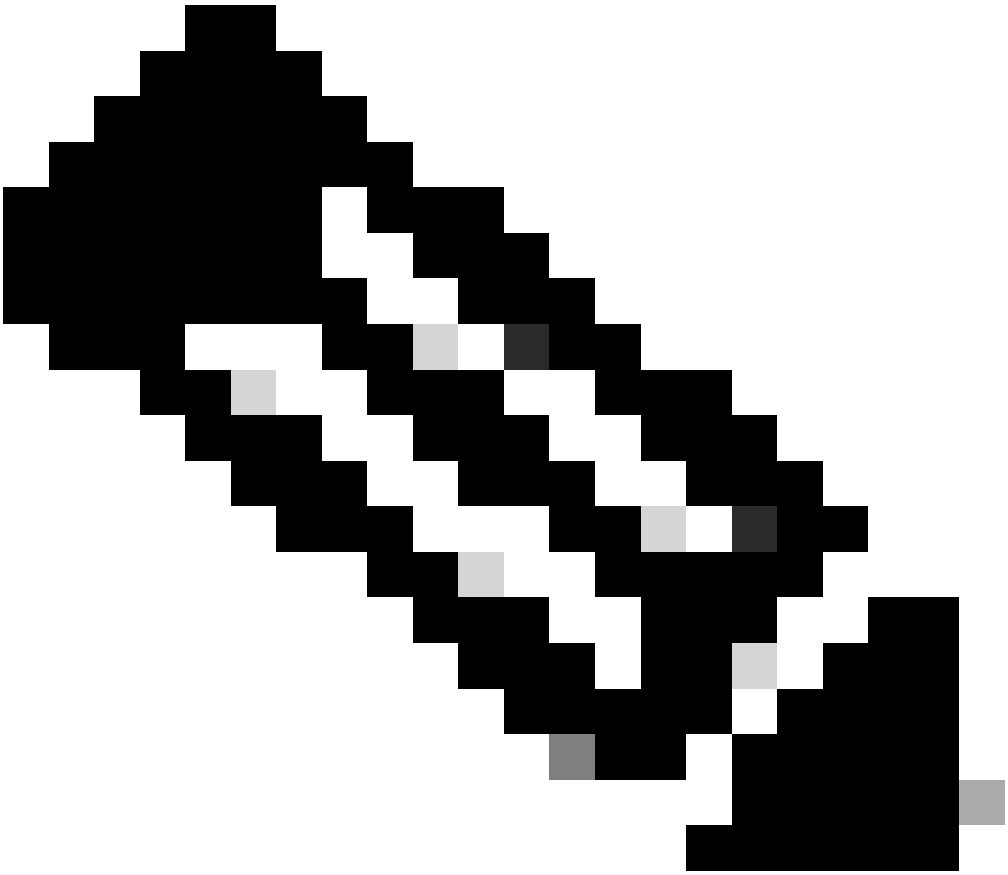
Datenquelle hinzufügen

4. Klicken Sie auf Datenquelle hinzufügen aus der Option CX Cloud Agent. Das Fenster CX Cloud Agent einrichten wird geöffnet.



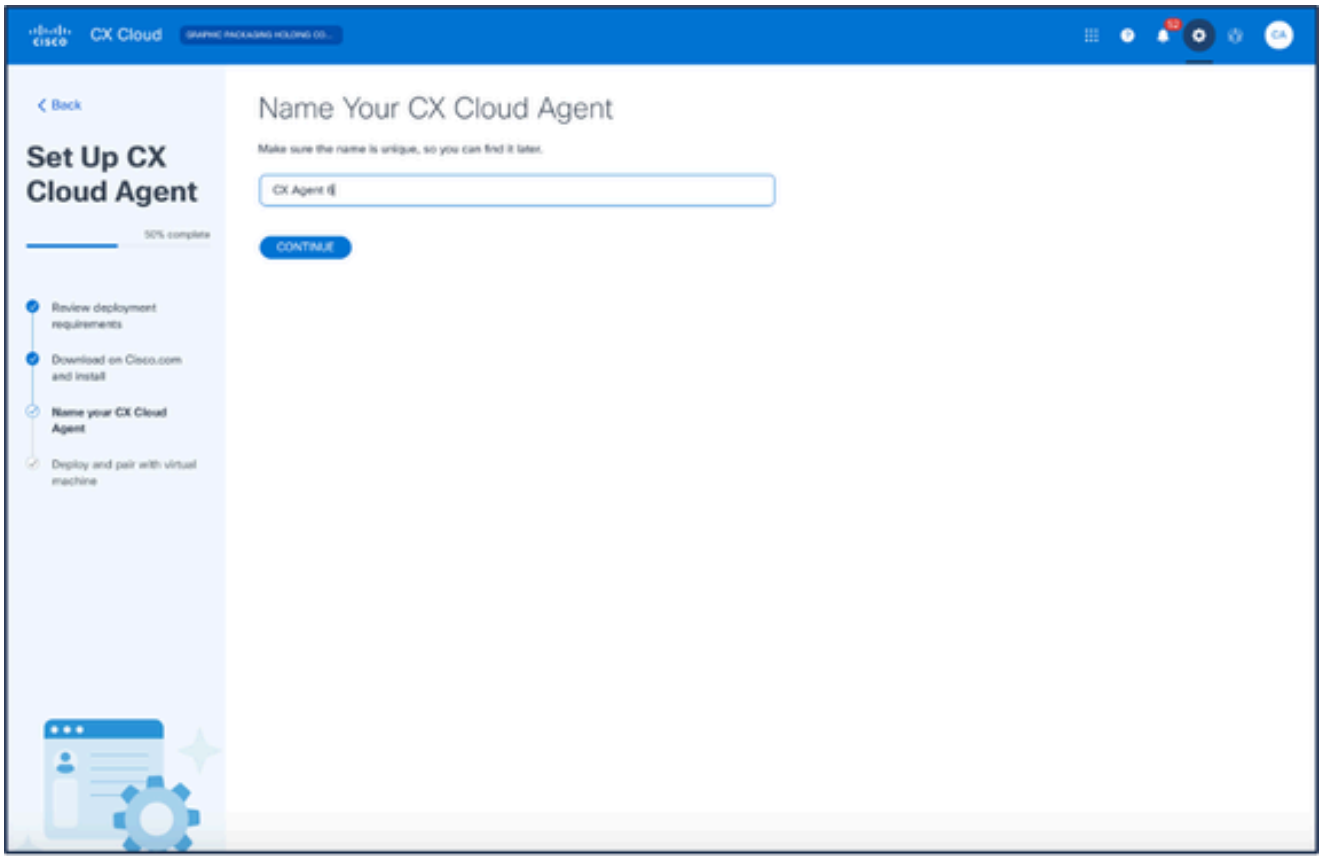
CX Cloud Agent einrichten

5. Lesen Sie den Abschnitt Bereitstellungsanforderungen überprüfen, und aktivieren Sie das Kontrollkästchen Ich richte diese Konfiguration auf Port 443 ein.
6. Klicken Sie auf Cisco.com auf Herunterladen. Die Seite Software Download (Software-Download) wird geöffnet.
7. Laden Sie die OVA-Datei für CX Cloud Agent v2.4 herunter.



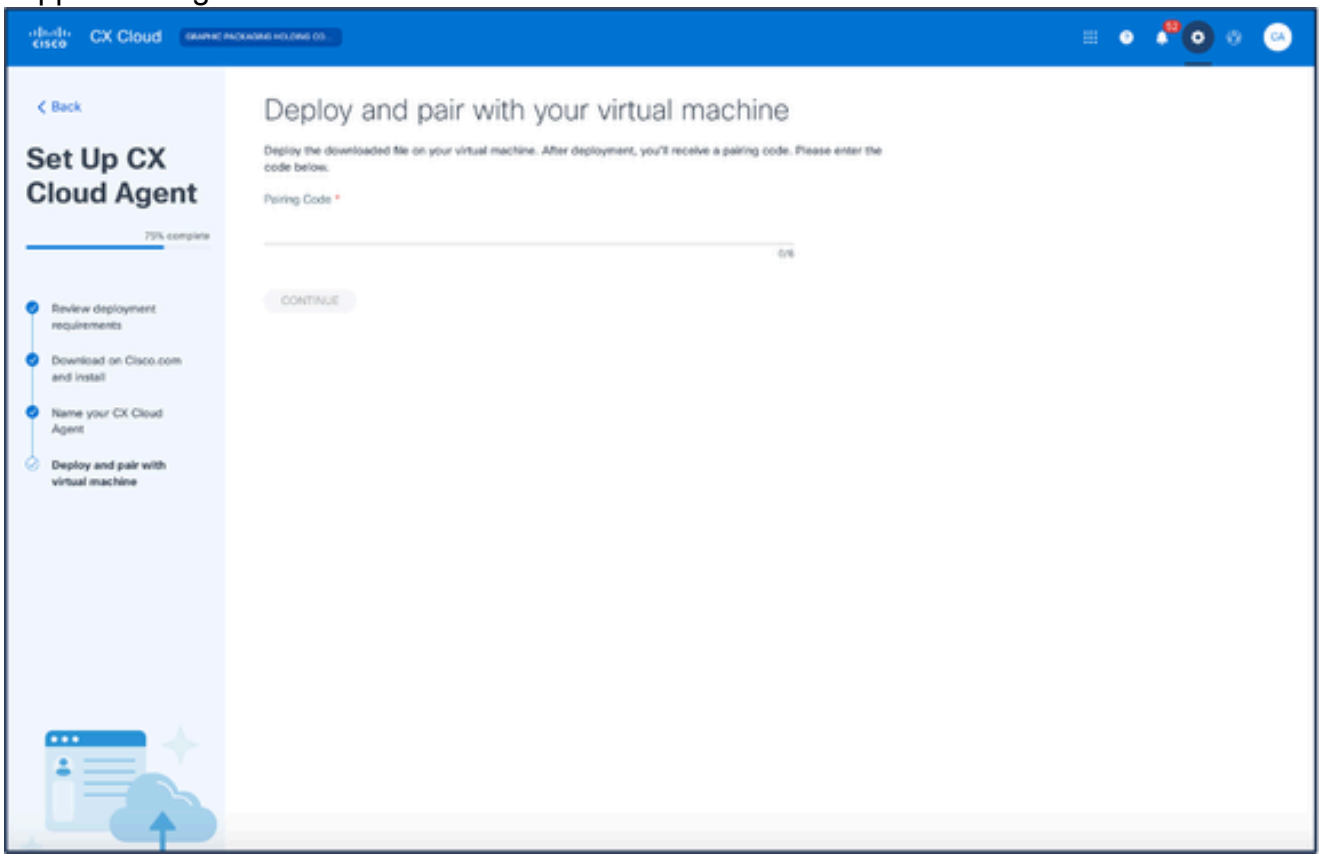
Hinweis: Nach der Bereitstellung der OVA-Datei wird ein Kopplungscode generiert, der erforderlich ist, um die Einrichtung des CX Cloud Agent abzuschließen.

8. Geben Sie den Namen des CX Cloud-Agenten in das Feld Name Ihr CX Cloud-Agenten ein.



Benennen Sie Ihren CX Cloud-Agenten

9. Klicken Sie auf Continue (Weiter). Das Fenster Bereitstellen und mit dem virtuellen System koppeln wird geöffnet.



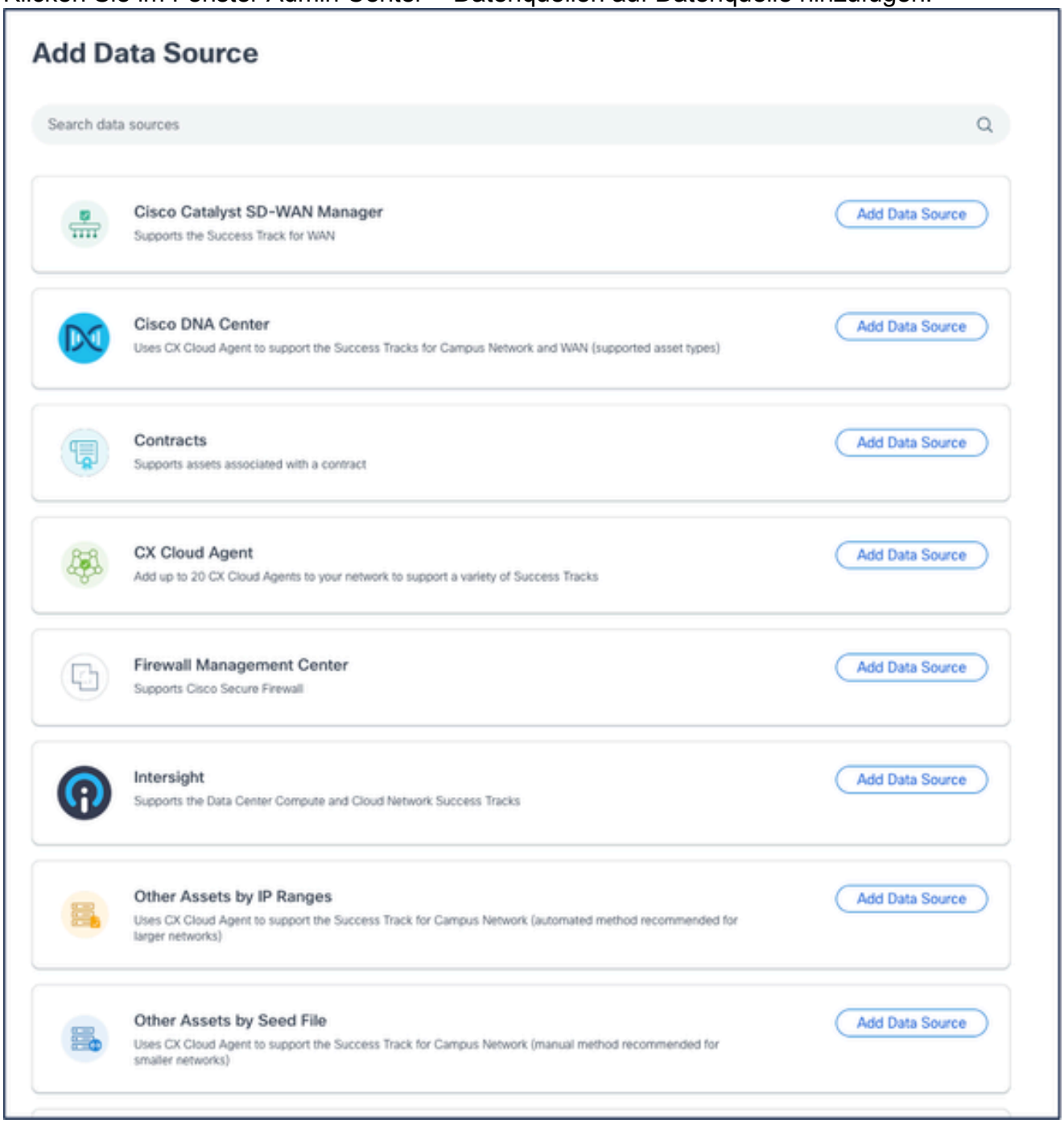
Bereitstellung und Verbindung mit virtuellem System

10. Geben Sie den Kopplungscode ein, der nach der Bereitstellung der heruntergeladenen OVA-Datei empfangen wurde.
11. Klicken Sie auf Continue (Weiter). Der Registrierungsstatus wird angezeigt, gefolgt von einer Bestätigung.

Hinzufügen von Cisco DNA Center als Datenquelle

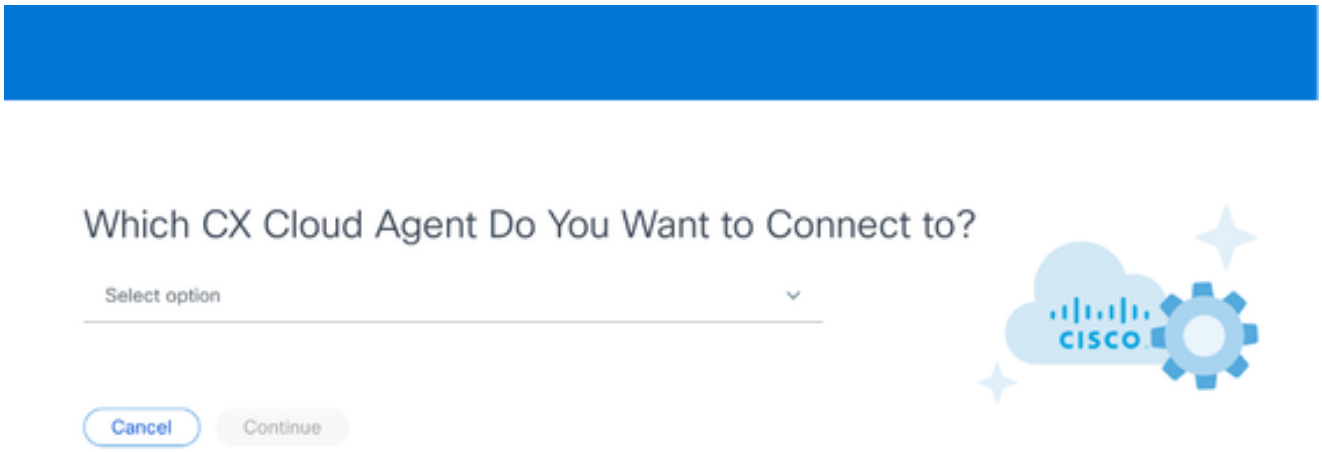
So fügen Sie Cisco DNA Center als Datenquelle hinzu:

1. Klicken Sie im Fenster Admin Center > Datenquellen auf Datenquelle hinzufügen.



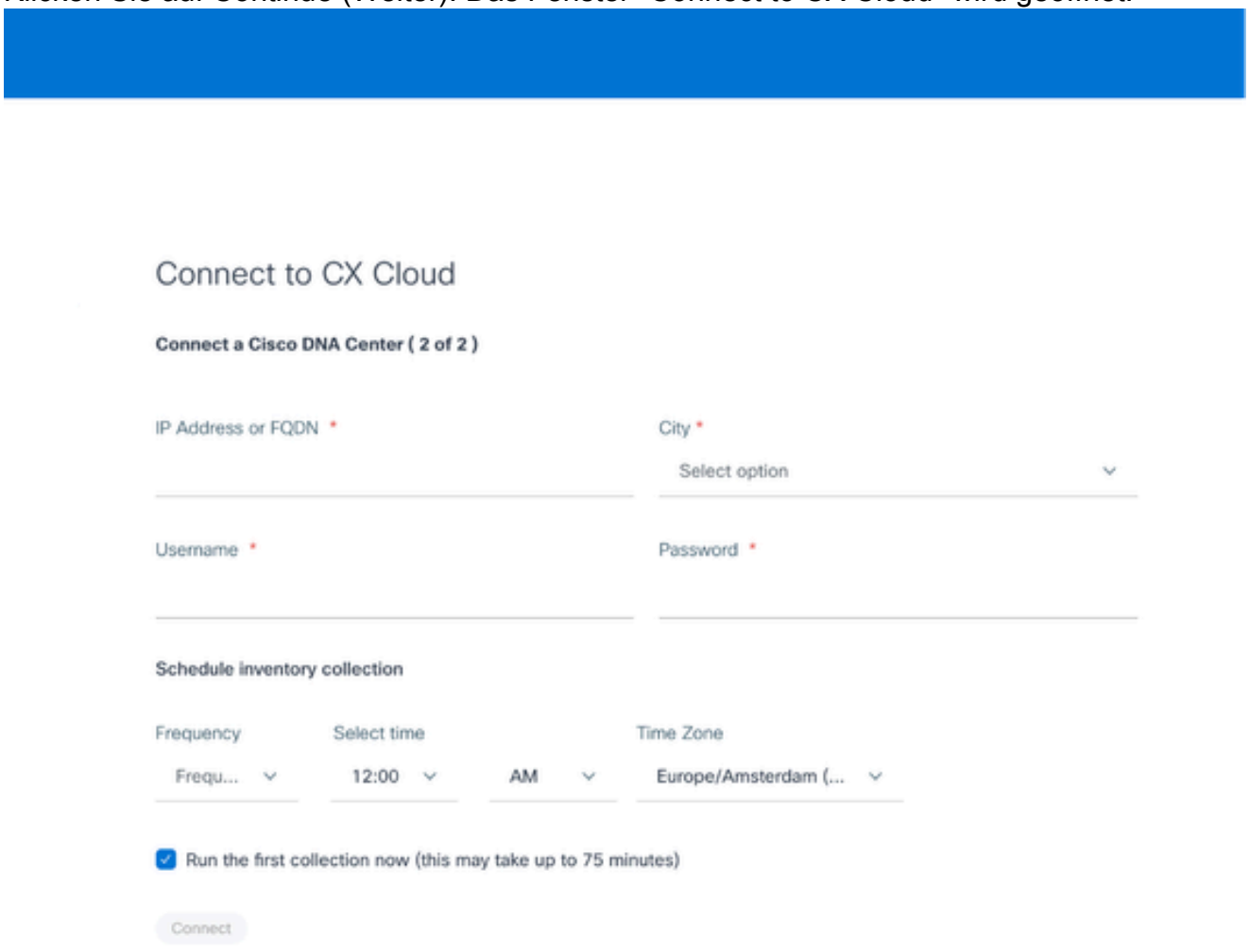
Datenquelle hinzufügen

2. Klicken Sie bei der Option Cisco DNA Center auf Datenquelle hinzufügen.



CX Cloud Agent auswählen

3. Wählen Sie den CX Cloud Agent aus der Dropdown-Liste Welchen CX Cloud Agent möchten Sie verbinden mit aus.
4. Klicken Sie auf Continue (Weiter). Das Fenster "Connect to CX Cloud" wird geöffnet.



Verbindung zur CX Cloud herstellen

5. Geben Sie in das Feld Cisco DNA Center verbinden Folgendes ein:
    - Virtuelle IP-Adresse oder FQDN (d. h. Cisco DNA Center IP-Adresse),
    - Stadt (d. h. der Standort des Cisco DNA Center),
    - Benutzername
    - Kennwort
    - Häufigkeit, Zeit und Zeitzone, um anzugeben, wie oft der CX Cloud Agent Netzwerkscans durchführen soll, in den Abschnitten Schedule Inventory Collection (Inventarerfassung planen)
      Hinweis: Aktivieren Sie das Kontrollkästchen Erste Sammlung jetzt ausführen, um die Sammlung jetzt auszuführen.

6. Klicken Sie auf Verbinden. Daraufhin wird eine Bestätigung mit der Cisco DNA Center-IP-Adresse angezeigt.

Andere Ressourcen als Datenquellen hinzufügen

Die Telemetriesammlung wurde auf Geräte ausgedehnt, die nicht vom Cisco DNA Center verwaltet werden. Kunden können so aus Telemetriedaten gewonnene Erkenntnisse und Analysen abrufen und mit diesen interagieren, um eine breitere Palette an Geräten zu ermöglichen. Nach der Ersteinrichtung von CX Cloud Agent können Benutzer CX Cloud Agent für die Verbindung mit 20 weiteren Cisco DNA Centern innerhalb der von CX Cloud überwachten Infrastruktur konfigurieren.

Benutzer können Geräte identifizieren, die in die CX Cloud integriert werden sollen, indem sie diese Geräte anhand einer Seed-Datei eindeutig identifizieren oder einen IP-Bereich angeben, der von CX Cloud Agent gescannt werden kann. Bei beiden Ansätzen wird SNMP (Simple Network Management Protocol) zur Erkennung und SSH (Secure Shell) für die Verbindung verwendet. Diese müssen ordnungsgemäß konfiguriert werden, damit die Telemetriesammlung erfolgreich durchgeführt werden kann.

So fügen Sie andere Ressourcen als Datenquellen hinzu:

- Hochladen einer Seed-Datei mithilfe einer Seed-Dateivorlage.
- Geben Sie einen IP-Adressbereich an.

Discovery-Protokolle

Sowohl die direkte Geräteerkennung auf Basis der Seed-Datei als auch die IP-Bereich-basierte Erkennung stützen sich auf SNMP als Erkennungsprotokoll. Es gibt verschiedene Versionen von SNMP, aber CX Cloud Agent unterstützt SNMPV2c und SNMP V3, und es können entweder eine oder beide Versionen konfiguriert werden. Dieselben Informationen, die nachfolgend ausführlich beschrieben werden, müssen vom Benutzer bereitgestellt werden, um die Konfiguration abzuschließen und die Verbindung zwischen dem von SNMP verwalteten Gerät und dem SNMP-Servicemanager zu aktivieren.

SNMPV2c und SNMPV3 unterscheiden sich hinsichtlich der Sicherheit und des Remote-

Konfigurationsmodells. SNMPV3 verwendet ein erweitertes kryptographisches Sicherheitssystem, das die SHA-Verschlüsselung unterstützt, um Nachrichten zu authentifizieren und ihre Privatsphäre zu gewährleisten. Es wird empfohlen, SNMPv3 in allen öffentlichen und mit dem Internet verbundenen Netzwerken zu verwenden, um den Schutz vor Sicherheitsrisiken und -bedrohungen zu gewährleisten. Auf der CX Cloud sollte SNMPv3 vorzugsweise konfiguriert werden und nicht SNMPv2c, mit Ausnahme älterer Legacy-Geräte, die keine integrierte Unterstützung für SNMPv3 bieten. Wenn beide Versionen von SNMP vom Benutzer konfiguriert wurden, kann der CX Cloud Agent standardmäßig versuchen, mit den jeweiligen Geräten über SNMPv3 zu kommunizieren und auf SNMPv2c zurückzugreifen, wenn die Kommunikation nicht erfolgreich ausgehandelt werden kann.

Verbindungsprotokolle

Im Rahmen der Einrichtung der direkten Geräteanbindung müssen Benutzer Details zum Geräteanbindungsprotokoll angeben: SSH (oder Telnet). SSHv2 kann verwendet werden, außer in Fällen von einzelnen Legacy-Ressourcen, die nicht über die entsprechende integrierte Unterstützung verfügen. Beachten Sie, dass das SSHv1-Protokoll grundlegende Schwachstellen enthält. Ohne zusätzliche Sicherheit können Telemetriedaten und die zugrunde liegenden Ressourcen aufgrund dieser Schwachstellen bei Verwendung von SSHv1 gefährdet werden. Auch Telnet ist unsicher. Die über Telnet übermittelten Anmeldeinformationen (Benutzernamen und Kennwörter) sind nicht verschlüsselt und daher kompromittierbar, da keine zusätzliche Sicherheit gegeben ist.

Einschränkung der Telemetrieverarbeitung für Geräte

Die folgenden Einschränkungen gelten für die Verarbeitung von Telemetriedaten für Geräte:

- Einige Geräte werden in der Sammlungsübersicht als erreichbar angezeigt, sind jedoch auf der Seite CX Cloud-Ressourcen nicht sichtbar. Einschränkungen bei der Geräteausstattung verhindern die Verarbeitung solcher Geräte und Telemetriedaten.
- Wenn ein Gerät aus der Seed-Datei oder den Sammlungen des IP-Bereichs ebenfalls Teil des Cisco DNA Center-Inventars ist, wird das Gerät nur einmal für den Cisco DNA Center-Eintrag gemeldet. Die entsprechenden Geräte innerhalb des Eintrags für die Seed-Datei/den IP-Bereich werden übersprungen, um eine Duplizierung zu vermeiden.

Hinzufügen weiterer Ressourcen mit einer Seed-Datei

Eine Seed-Datei ist eine CSV-Datei, bei der jede Zeile einen Systemdatensatz darstellt. In einer Seed-Datei entspricht jeder Seed-Datei-Datensatz einem eindeutigen Gerät, von dem aus Telemetriedaten von CX Cloud Agent erfasst werden können. Alle Fehler- oder Informationsmeldungen zu jedem Geräteeintrag aus der importierten Seed-Datei werden als Teil der Jobprotokolldetails erfasst. Alle Geräte in einer Seed-Datei werden als verwaltete Geräte angesehen, auch wenn die Geräte zum Zeitpunkt der Erstkonfiguration nicht erreichbar sind. Wenn eine neue Seed-Datei hochgeladen wird, um eine vorherige Datei zu ersetzen, wird das Datum des letzten Uploads in CX Cloud angezeigt.

Der CX Cloud Agent kann versuchen, eine Verbindung mit den Geräten herzustellen, kann jedoch nicht jede dieser Verbindungen verarbeiten, um sie auf den Seiten "Assets" (Ressourcen) anzuzeigen, wenn die PIDs oder Seriennummern nicht ermittelt werden können. Jede Zeile in der Seed-Datei, die mit einem Semikolon beginnt, wird ignoriert. Die Headerzeile in der Seed-Datei beginnt mit einem Semikolon und kann unverändert beibehalten (empfohlene Option) oder beim Erstellen der Seed-Datei des Kunden gelöscht werden.

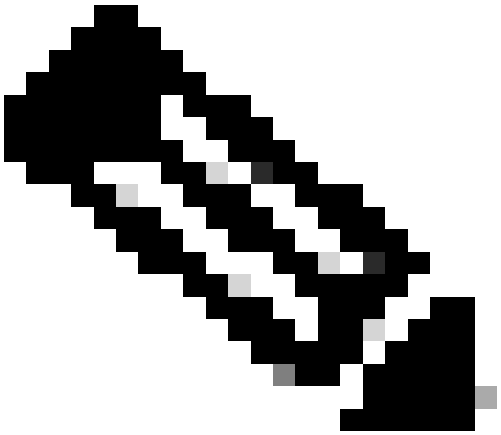
Es ist wichtig, dass das Format der Beispiel-Seed-Datei, einschließlich der Spaltenüberschriften, in keiner Weise geändert wird. Klicken Sie auf den angegebenen Link, um eine Seed-Datei im PDF-Format anzuzeigen. Diese PDF-Datei dient nur zu Referenzzwecken und kann zum Erstellen einer Seed-Datei verwendet werden, die im CSV-Format gespeichert werden muss.

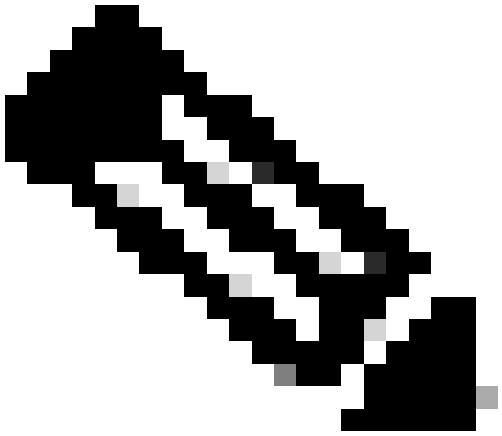
Klicken Sie auf diesen Link, um eine Seed-Datei anzuzeigen, mit der eine Seed-Datei im CSV-Format erstellt werden kann.

Hinweis: Diese PDF-Datei dient nur zu Referenzzwecken und kann zum Erstellen einer Seed-Datei verwendet werden, die im CSV-Format gespeichert werden muss.

Diese Tabelle enthält alle erforderlichen Seed-Dateispalten und die Daten, die in jeder Spalte enthalten sein müssen.

Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
A	IP-Adresse oder Hostname	Geben Sie eine gültige, eindeutige IP-Adresse oder einen Hostnamen des Geräts an.
B	SNMP-Protokollversion	Das SNMP-Protokoll wird von CX Cloud Agent benötigt und zur Geräteerkennung im Kundennetzwerk verwendet. Werte können snmpv2c oder snmpv3 sein, aber aus Sicherheitsgründen wird snmpv3 empfohlen.
C	snmpRo : Erforderlich, wenn col#=3 als 'snmpv2c' ausgewählt ist	Wenn die ältere Variante von SNMPv2 für ein bestimmtes Gerät ausgewählt ist, müssen snmpRO-Anmeldeinformationen (schreibgeschützt) für die SNMP-Sammlung des Geräts angegeben werden. Andernfalls kann der Eintrag leer sein.
G	snmpv3UserName : Erforderlich, wenn col#=3 als 'snmpv3' ausgewählt ist	Wenn SNMPv3 für die Kommunikation mit einem bestimmten Gerät ausgewählt ist, muss der entsprechende Benutzername für die Anmeldung angegeben werden.

Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
O	snmpv3AuthAlgorithm: Werte können MD5 oder SHA sein.	Das SNMPv3-Protokoll ermöglicht die Authentifizierung entweder über den MD5- oder den SHA-Algorithmus. Wenn das Gerät mit sicherer Authentifizierung konfiguriert ist, muss der entsprechende Auth-Algorithmus angegeben werden.  Hinweis: MD5 gilt als unsicher, und SHA kann auf allen Geräten verwendet werden, die es unterstützen.
F	snmpv3AuthKennwort: Kennwort	Wenn auf dem Gerät entweder ein MD5- oder ein SHA-Verschlüsselungsalgorithmus konfiguriert ist, muss das entsprechende Authentifizierungskennwort für den Gerätezugriff angegeben werden.
G	snmpv3PrivAlgorithm: Werte können DES, 3DES sein.	Wenn das Gerät mit dem SNMPv3-Datenschutzalgorithmus konfiguriert ist (dieser Algorithmus wird zur Verschlüsselung der Antwort verwendet), muss der entsprechende Algorithmus angegeben werden.

Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
		 Hinweis: Die von DES verwendeten 56-Bit-Schlüssel werden als zu kurz angesehen, um kryptografische Sicherheit zu bieten, und 3DES kann auf allen Geräten verwendet werden, die es unterstützen.
H	snmpv3PrivKennwort: Kennwort	Wenn der SNMPv3-Datenschutzalgorithmus auf dem Gerät konfiguriert ist, muss das entsprechende Datenschutzkennwort für die Geräteverbindung angegeben werden.
I	snmpv3EngineId : Engine-ID, eindeutige, das Gerät repräsentierende ID; Engine-ID angeben, wenn manuell auf dem Gerät konfiguriert	Die SNMPv3-Engine-ID ist eine eindeutige ID für jedes Gerät. Diese Engine-ID wird während der Erfassung der SNMP-Datensätze durch den CX Cloud Agent als Referenz gesendet. Wenn der Kunde die EngineID manuell konfiguriert, muss die entsprechende EngineID angegeben werden.
J	cliProtocol: Werte können 'telnet', 'sshv1', 'sshv2' sein. Wenn leer, kann standardmäßig 'sshv2' eingestellt werden	Die CLI ist für die direkte Interaktion mit dem Gerät vorgesehen. CX Cloud Agent verwendet dieses Protokoll für die CLI-Erfassung für ein bestimmtes Gerät. Diese CLI-Erfassungsdaten werden für Ressourcen- und andere Insights-Berichte in der CX Cloud verwendet. SSHv2 wird empfohlen; da keine anderen Netzwerksicherheitsmaßnahmen ergriffen

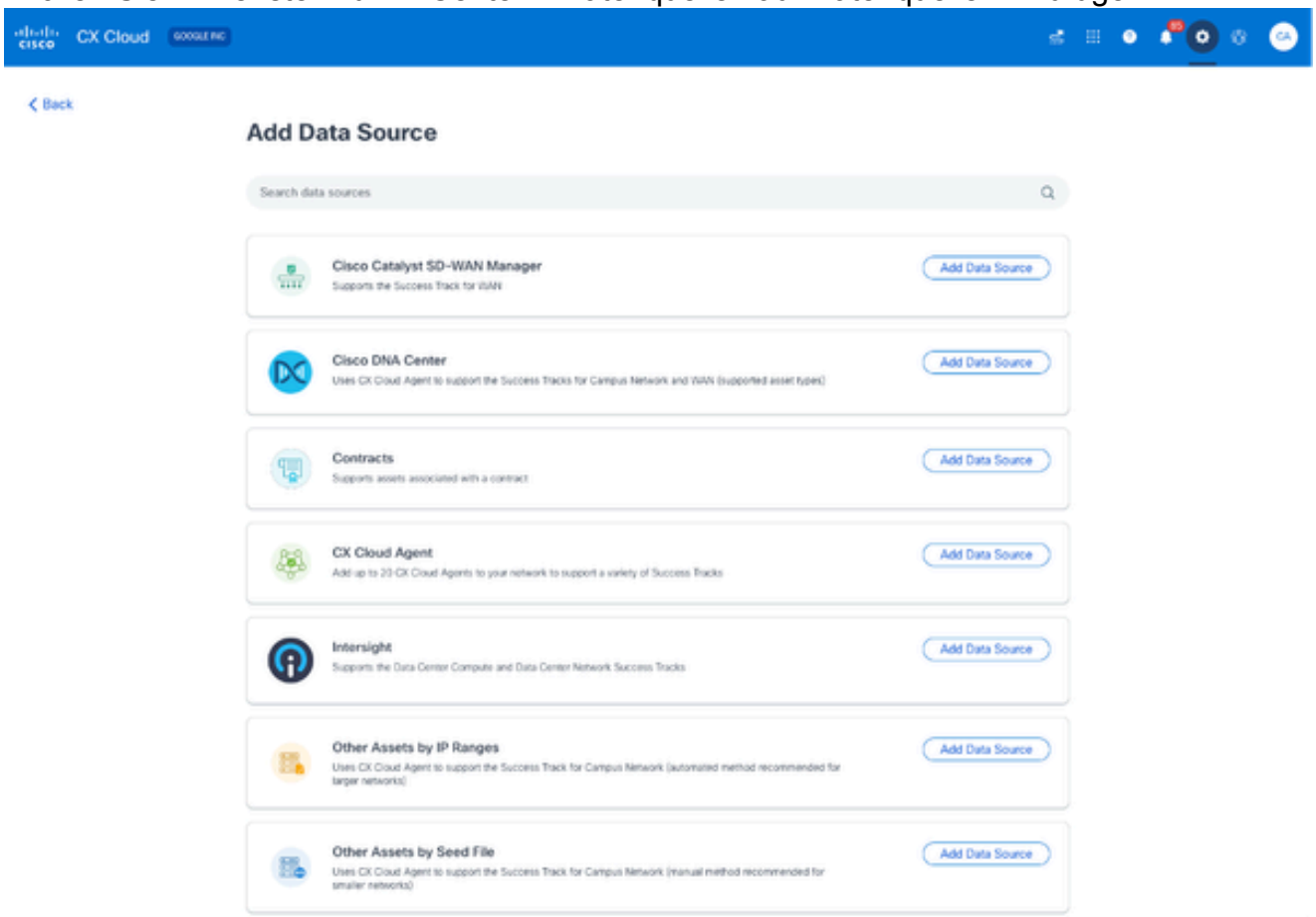
Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
		werden, bieten SSHv1- und Telnet-Protokolle keine ausreichende Transportsicherheit.
K	cliPort : CLI-Protokoll-Portnummer	Wenn ein CLI-Protokoll ausgewählt wird, muss die entsprechende Portnummer angegeben werden. Beispiel: 22 für SSH und 23 für Telnet.
L	cliUser : CLI Benutzername (entweder CLI Benutzername/Passwort oder BEIDE können angegeben werden, ABER beide Spalten (col#=12 und col#=13) dürfen nicht leer sein.)	Der entsprechende CLI-Benutzername des Geräts muss angegeben werden. Dies wird von CX Cloud Agent zum Zeitpunkt der Verbindung mit dem Gerät während der CLI-Erfassung verwendet.
M	cliPassword : CLI-Benutzerkennwort (entweder CLI-Benutzername/Kennwort oder BEIDE können angegeben werden, ABER beide Spalten (col#=12 und col#=13) dürfen nicht leer sein.)	Das entsprechende CLI-Kennwort des Geräts muss angegeben werden. Dies wird von CX Cloud Agent zum Zeitpunkt der Verbindung mit dem Gerät während der CLI-Erfassung verwendet.
N	CLIEnableUser	Wenn enable auf dem Gerät konfiguriert ist, muss der enableUsername-Wert des Geräts angegeben werden.
O	CLIEnablePassword	Wenn enable auf dem Gerät konfiguriert ist, muss der enablePassword-Wert des Geräts angegeben werden.
F	Künftiger Support (keine Eingaben erforderlich)	Reserviert für zukünftige Verwendung
F	Künftiger Support (keine	Reserviert für zukünftige Verwendung

Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
	Eingaben erforderlich)	
R	Künftiger Support (keine Eingaben erforderlich)	Reserviert für zukünftige Verwendung
S	Künftiger Support (keine Eingaben erforderlich)	Reserviert für zukünftige Verwendung

Andere Ressourcen mit einer neuen Seed-Datei hinzufügen

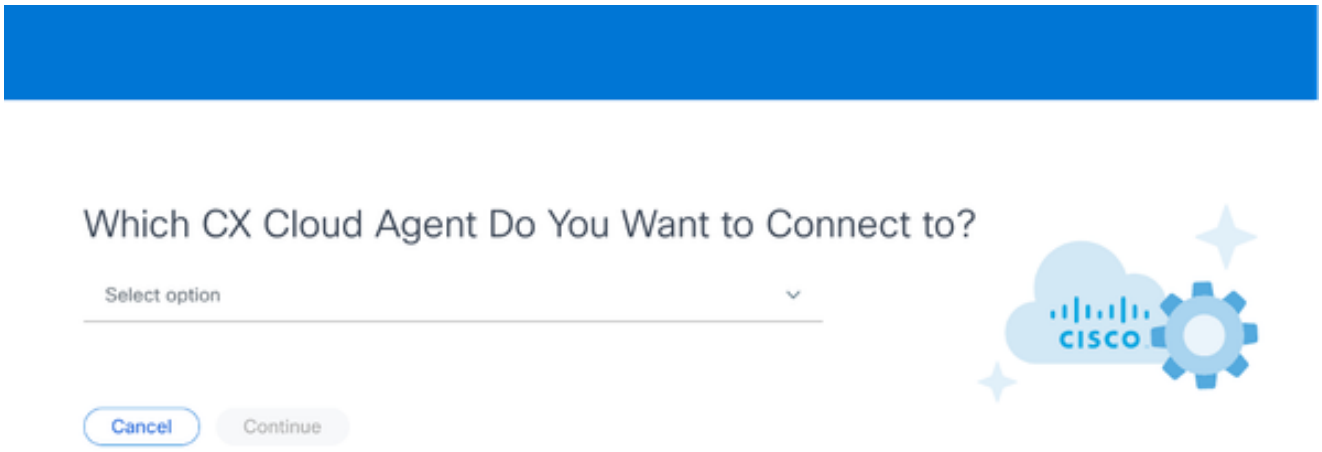
So fügen Sie andere Ressourcen mithilfe einer neuen Seed-Datei hinzu:

1. Klicken Sie im Fenster Admin Center > Datenquellen auf Datenquelle hinzufügen.



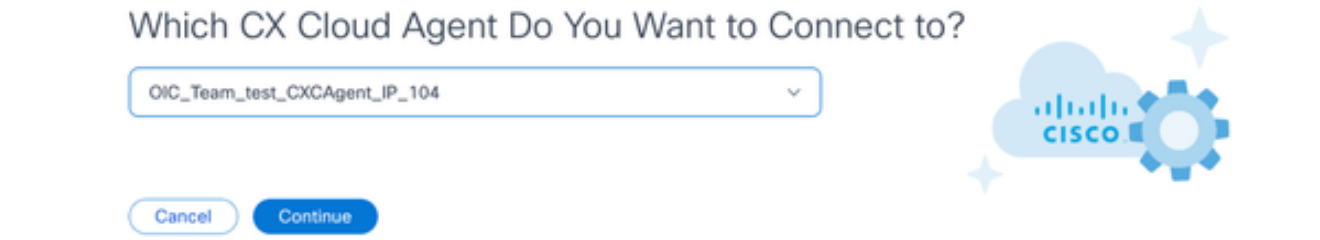
Datenquelle hinzufügen

2. Klicken Sie auf Datenquelle hinzufügen in der Option Andere Ressourcen nach Seed-Datei.



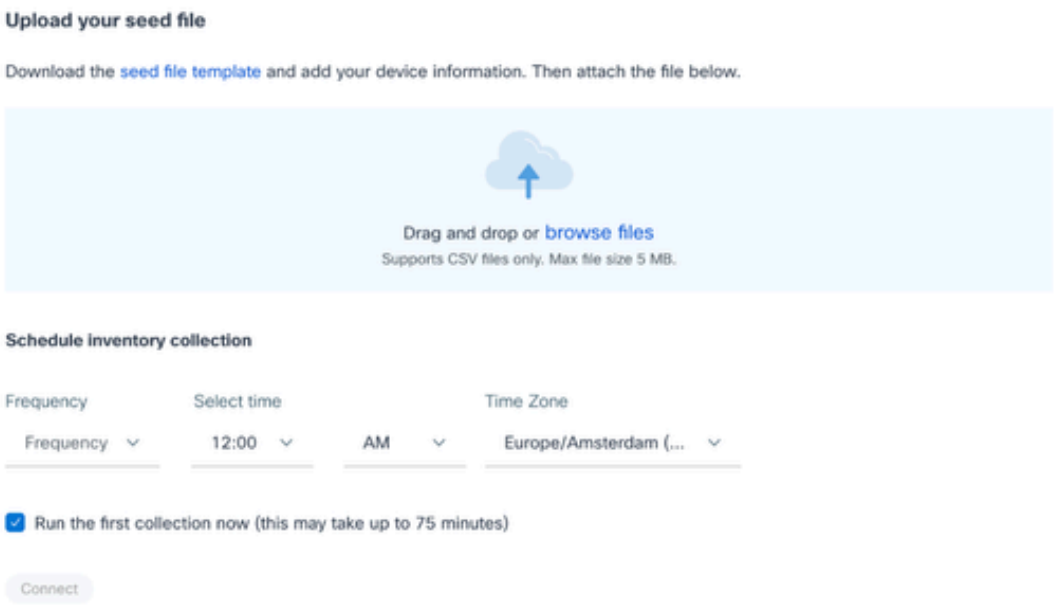
CX Cloud Agent auswählen

3. Wählen Sie den CX Cloud Agent aus der Dropdown-Liste Welchen CX Cloud Agent möchten Sie verbinden mit aus.



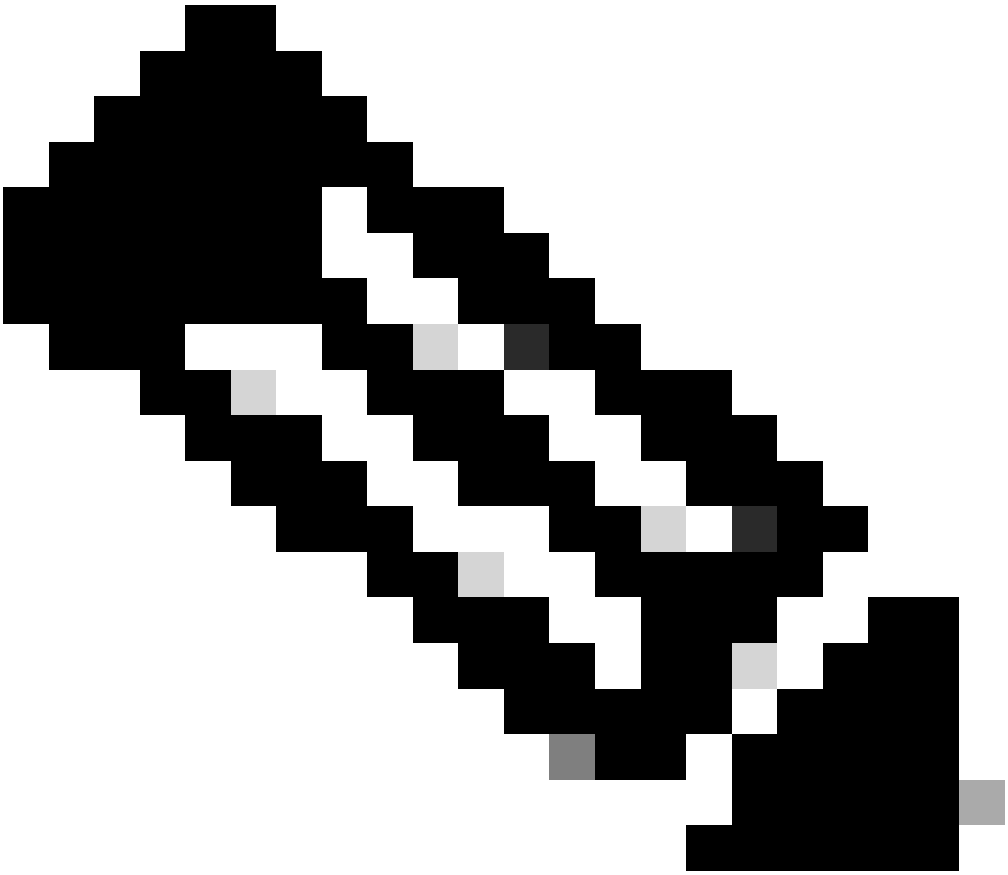
Fortfahren

4. Klicken Sie auf Continue (Weiter). Die Seite Upload Your Seed File (Seed-Datei hochladen) wird angezeigt.



Seed-Datei hochladen

5. Klicken Sie auf die Vorlage für die verlinkte Seed-Datei, um die Vorlage herunterzuladen.
6. Manuelles Eingeben oder Importieren von Daten in die Datei Speichern Sie die Vorlage abschließend als CSV-Datei, um die Datei in CX Cloud Agent zu importieren.
7. Drag & Drop oder klicken Sie auf Dateien durchsuchen, um die CSV-Datei hochzuladen.
8. Füllen Sie den Abschnitt "Inventarerfassung planen" aus.



Hinweis: Bevor die Erstkonfiguration von CX Cloud abgeschlossen ist, muss CX Cloud Agent die erste Telemetriesammlung durchführen, indem die Seed-Datei verarbeitet und die Verbindung mit allen identifizierten Geräten hergestellt wird. Die Erfassung kann je nach Bedarf gestartet oder gemäß einem hier definierten Zeitplan ausgeführt werden. Benutzer können die erste Telemetrieverbindung durchführen, indem sie das Kontrollkästchen Erste Sammlung jetzt ausführen aktivieren. Je nach Anzahl der in der Seed-Datei angegebenen Einträge und anderen Faktoren kann dieser Vorgang sehr lange dauern.

9. Klicken Sie auf Verbinden. Das Fenster Datenquellen wird geöffnet und zeigt eine Bestätigungsmeldung an.

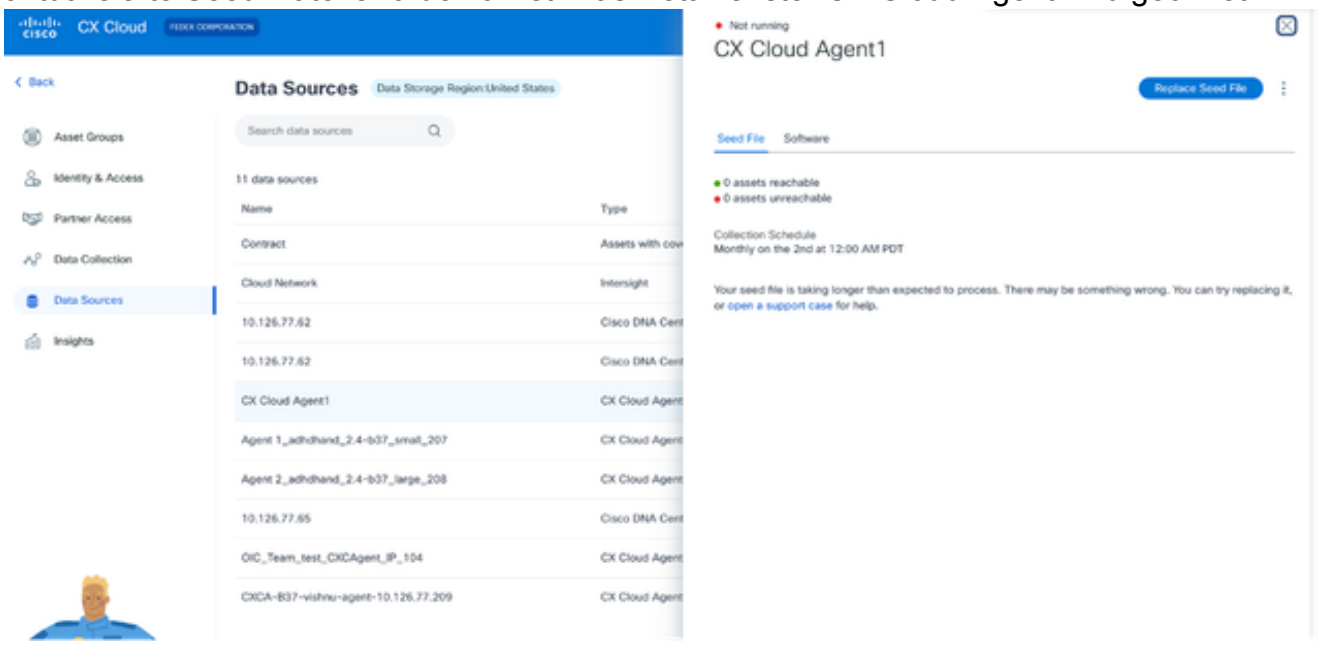
Andere Ressourcen mit einer geänderten Seed-Datei hinzufügen

So fügen Sie Geräte mithilfe der aktuellen Seed-Datei hinzu, ändern oder löschen sie:

1. Öffnen Sie die zuvor erstellte Seed-Datei, nehmen Sie die erforderlichen Änderungen vor, und speichern Sie die Datei.

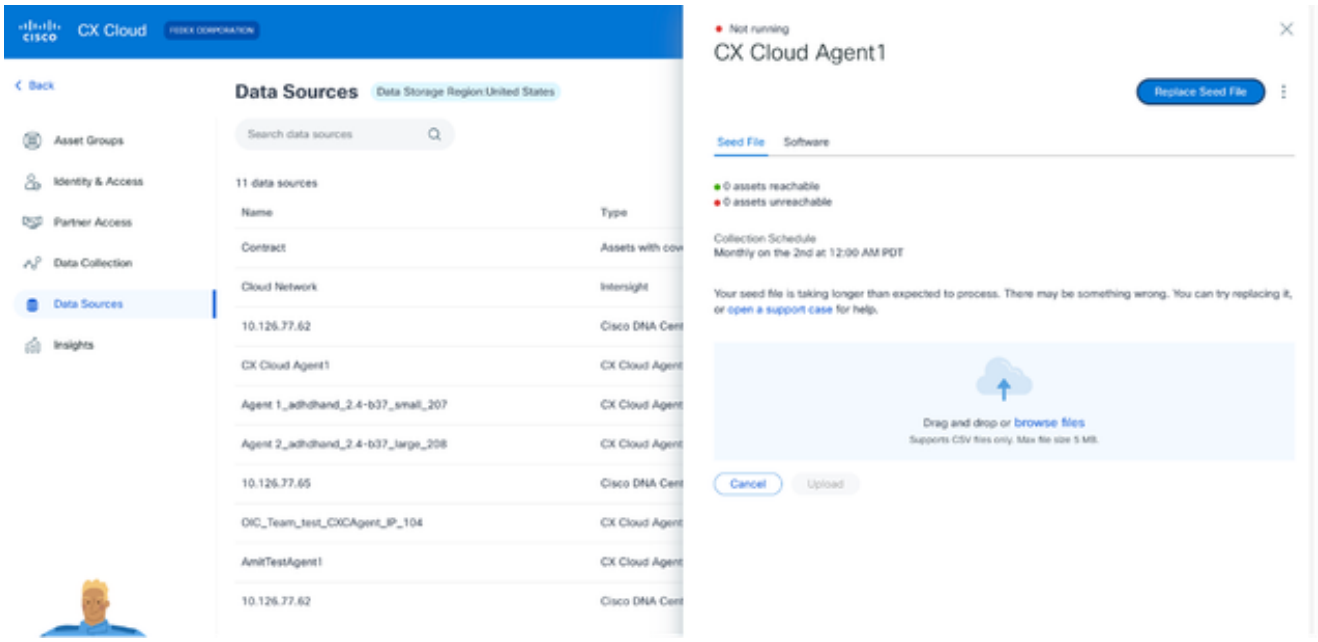
Hinweis: Um der Seed-Datei Assets hinzuzufügen, fügen Sie diese Assets an die zuvor erstellte Seed-Datei an, und laden Sie die Datei neu. Dies ist notwendig, da das Hochladen einer neuen Seed-Datei die aktuelle Seed-Datei ersetzt. Nur die zuletzt hochgeladene Seed-Datei wird für die Erkennung und Sammlung verwendet.

2. Klicken Sie auf der Seite Datenquellen auf die Datenquelle des CX Cloud Agent, für die eine aktualisierte Seed-Datei erforderlich ist. Das Detailfenster CX Cloud Agent wird geöffnet.



CX Cloud Agent - Detailfenster

3. Klicken Sie auf Seed-Datei ersetzen.



Fenster "CX Cloud Agent"

4. Ziehen Sie die geänderte Seed-Datei, oder klicken Sie auf Dateien durchsuchen, um sie hochzuladen.
5. Klicken Sie auf Hochladen.

Hinzufügen weiterer Ressourcen mithilfe von IP-Bereichen

IP-Bereiche ermöglichen es Benutzern, Hardware-Ressourcen zu identifizieren und anschließend Telemetriedaten von diesen Geräten basierend auf IP-Adressen zu sammeln. Die Geräte für die Telemetriesammlung können eindeutig identifiziert werden, indem ein einzelner IP-Bereich auf Netzwerkebene angegeben wird, der vom CX Cloud Agent mithilfe des SNMP-Protokolls gescannt werden kann. Wenn der IP-Bereich zum Identifizieren eines direkt verbundenen Geräts ausgewählt wird, können die IP-Adressen, auf die verwiesen wird, so restriktiv wie möglich sein, während gleichzeitig alle erforderlichen Ressourcen abgedeckt werden.

- Es können bestimmte IPs bereitgestellt werden, oder es können Platzhalter verwendet werden, um die Achtbitzeichen einer IP zu ersetzen und einen Bereich zu erstellen.
- Wenn eine bestimmte IP-Adresse nicht in dem IP-Bereich enthalten ist, der während der Einrichtung identifiziert wurde, versucht CX Cloud Agent nicht, mit einem Gerät zu kommunizieren, das über eine solche IP-Adresse verfügt, und sammelt auch keine Telemetrie von einem solchen Gerät.
- Bei Eingabe von *.*.*.* kann CX Cloud Agent die vom Benutzer bereitgestellten Anmeldeinformationen mit jeder IP verwenden. Beispiel: 172.16.*.* ermöglicht die Verwendung der Anmeldeinformationen für alle Geräte im Subnetz 172.16.0.0/16.
- Wenn Änderungen am Netzwerk oder an vorhandenen Installationen (Installed Base, IB) vorgenommen werden, kann der IP-Bereich geändert werden. Siehe Abschnitt Bearbeiten von IP-Bereichen

Der CX Cloud Agent versucht, eine Verbindung mit den Geräten herzustellen, kann diese jedoch möglicherweise nicht verarbeiten, um sie in der Assets-Ansicht anzuzeigen, falls er nicht in der Lage ist, die PIDs oder Seriennummern zu ermitteln.

Hinweise:
Durch Klicken auf IP-Adressbereich bearbeiten wird die Geräteerkennung bei Bedarf initiiert. Wenn einem angegebenen IP-Bereich ein neues Gerät hinzugefügt oder (innerhalb oder außerhalb) daraus gelöscht wird, muss der Kunde immer auf IP-Adressbereich bearbeiten klicken (siehe Abschnitt Bearbeiten von IP-Bereichen) und die erforderlichen Schritte ausführen, um die Geräteerkennung auf Anforderung zu initiieren und neu hinzugefügte Geräte in den CX Cloud Agent-Erfassungsbestand aufzunehmen.

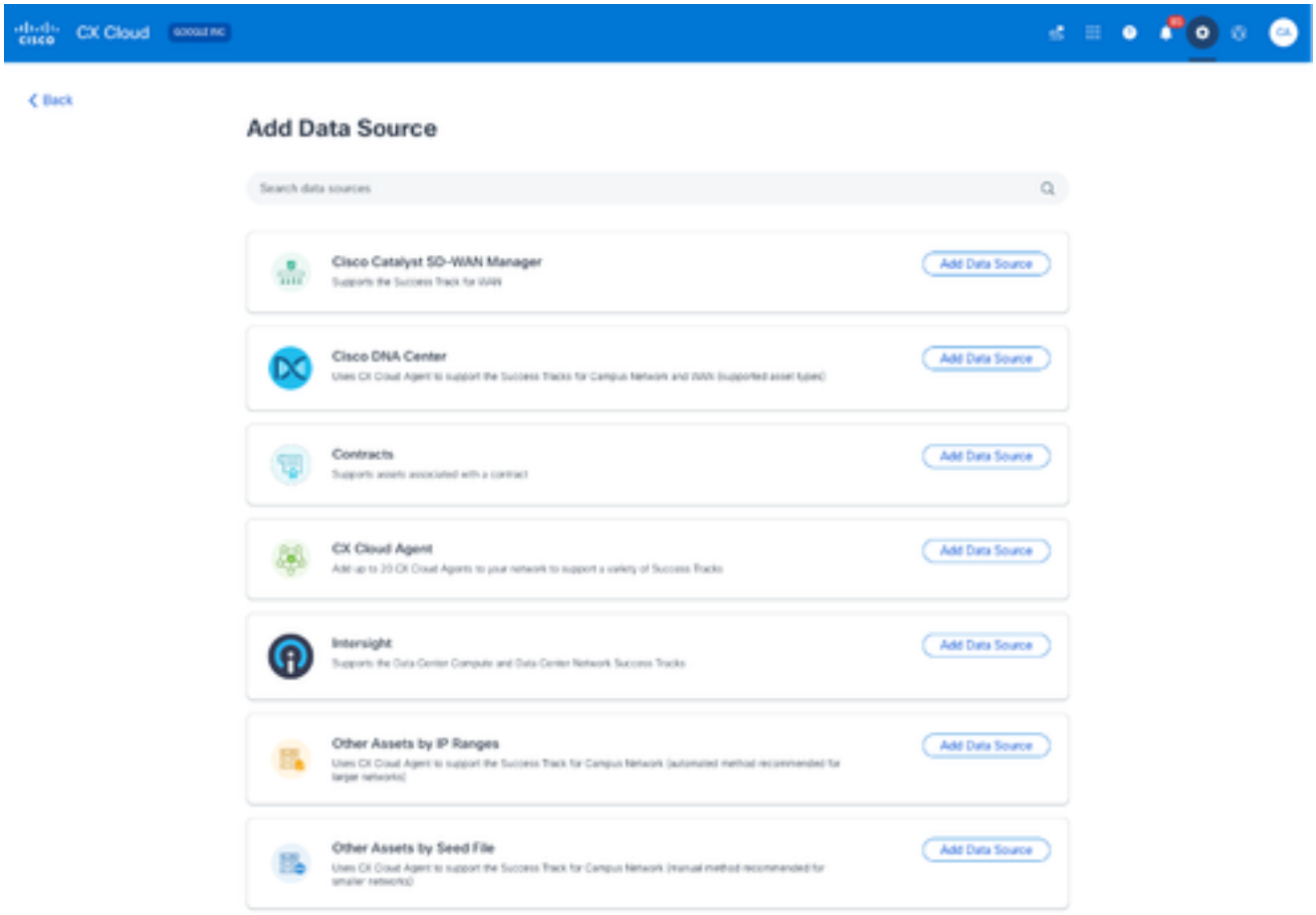
Um Geräte über einen IP-Bereich hinzuzufügen, müssen Benutzer alle anwendbaren Anmeldeinformationen über die Konfigurations-Benutzeroberfläche angeben. Die sichtbaren Felder variieren je nach den Protokollen, die in den vorherigen Fenstern ausgewählt wurden. Wenn mehrere Optionen für dasselbe Protokoll ausgewählt werden, z. B. sowohl SNMPv2c als auch SNMPv3 oder SSHv2 und SSHv1, wird die Protokollauswahl vom CX Cloud Agent basierend auf den einzelnen Gerätefunktionen automatisch ausgehandelt.

Wenn Geräte über IP-Adressen verbunden werden, muss der Kunde sicherstellen, dass alle relevanten Protokolle im IP-Bereich sowie die SSH-Versionen und Telnet-Anmeldeinformationen gültig sind oder die Verbindungen fehlschlagen.

Hinzufügen weiterer Ressourcen nach IP-Bereichen

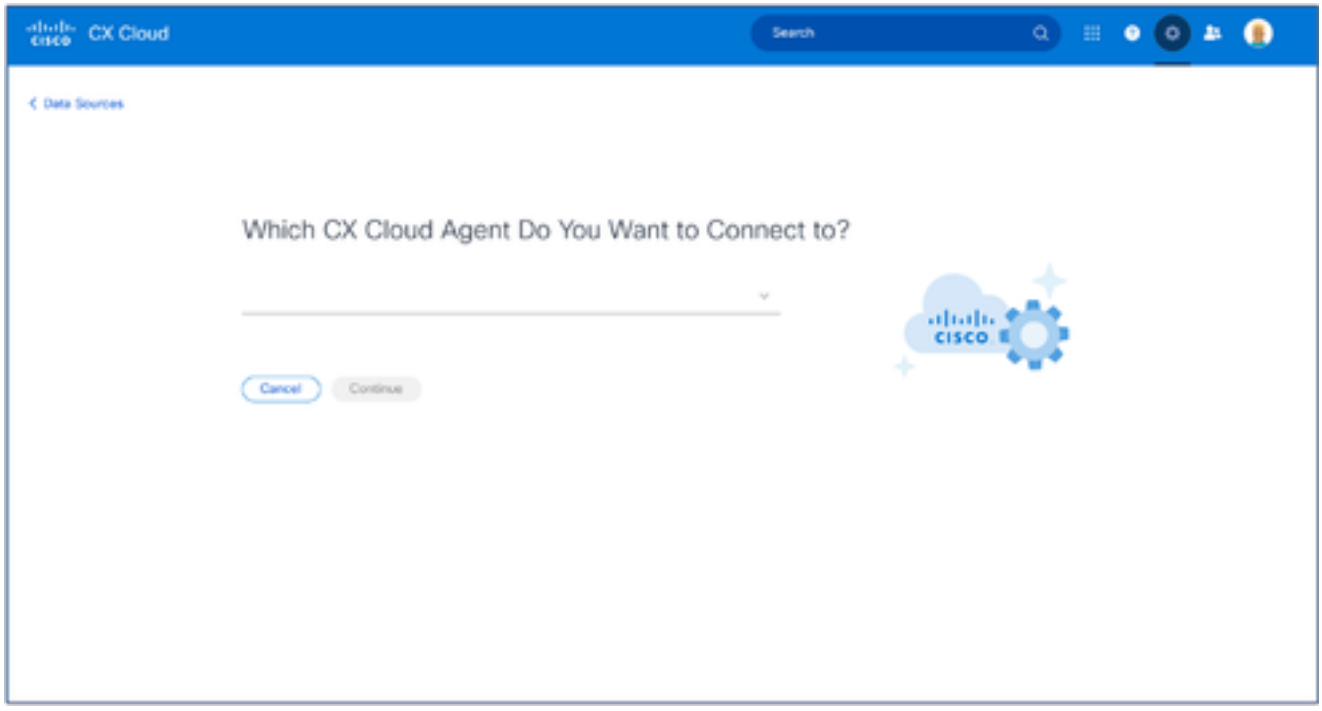
So fügen Sie Geräte über den IP-Bereich hinzu:

1. Klicken Sie im Fenster Admin Center > Datenquellen auf Datenquelle hinzufügen.



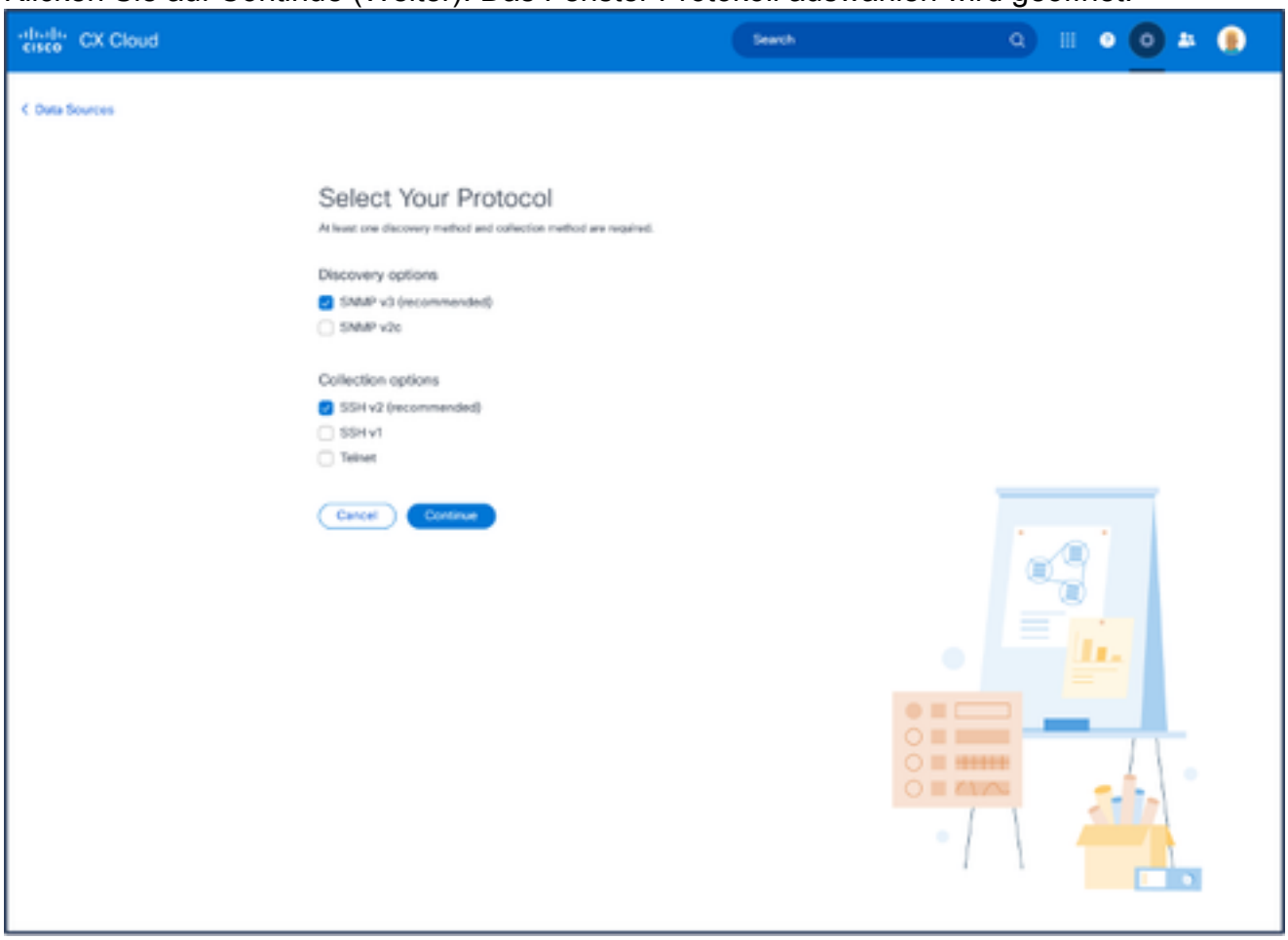
Datenquellen hinzufügen

2. Klicken Sie in der Option Andere Assets nach IP-Bereichen auf Datenquelle hinzufügen.



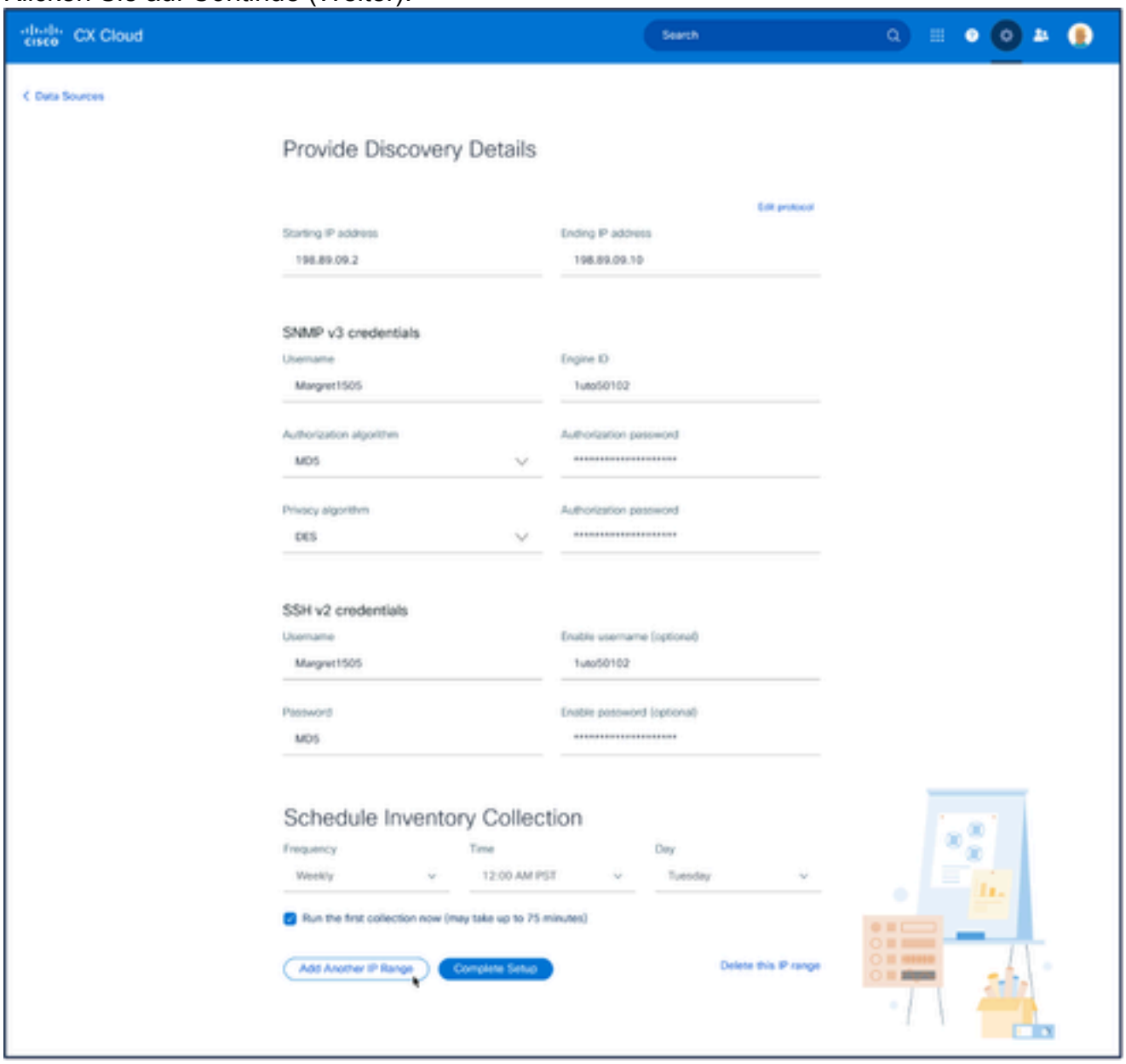
CX Cloud Agent auswählen

3. Wählen Sie den CX Cloud Agent aus der Dropdown-Liste Welchen CX Cloud Agent möchten Sie verbinden mit aus.
4. Klicken Sie auf Continue (Weiter). Das Fenster Protokoll auswählen wird geöffnet.



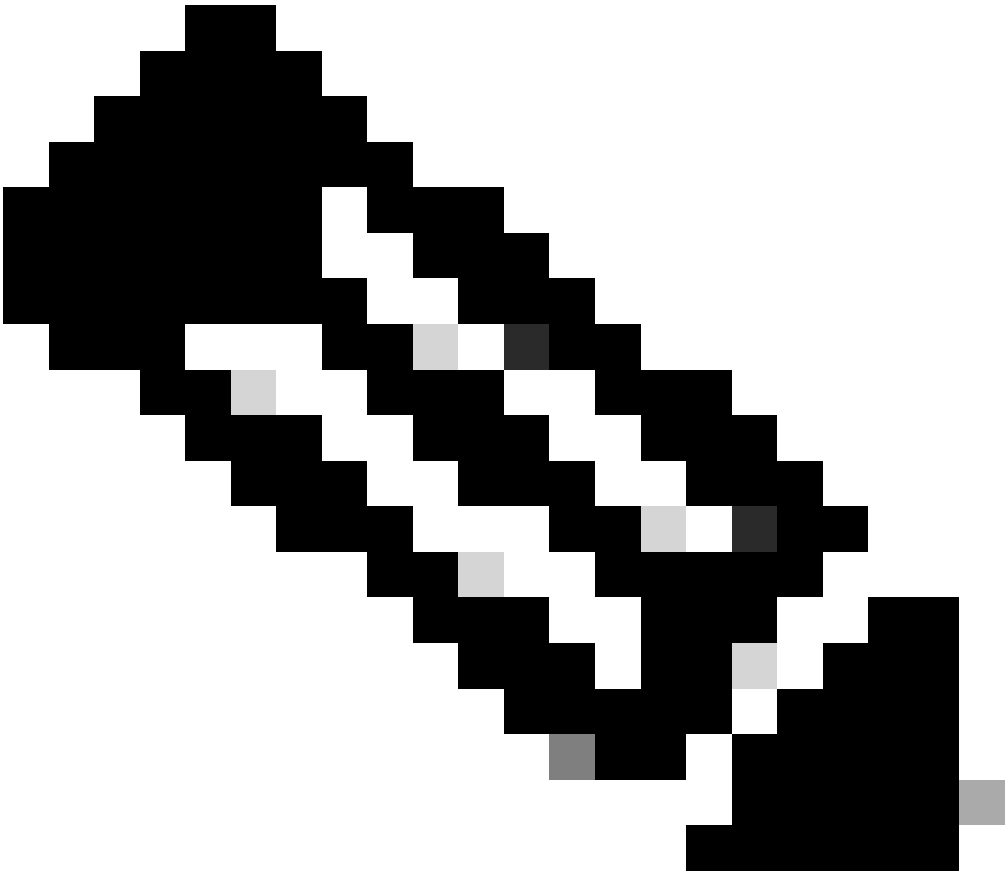
Protokoll auswählen

5. Aktivieren Sie die entsprechenden Kontrollkästchen für die Erkennungsoptionen und die Erfassungsoptionen.
6. Klicken Sie auf Continue (Weiter).



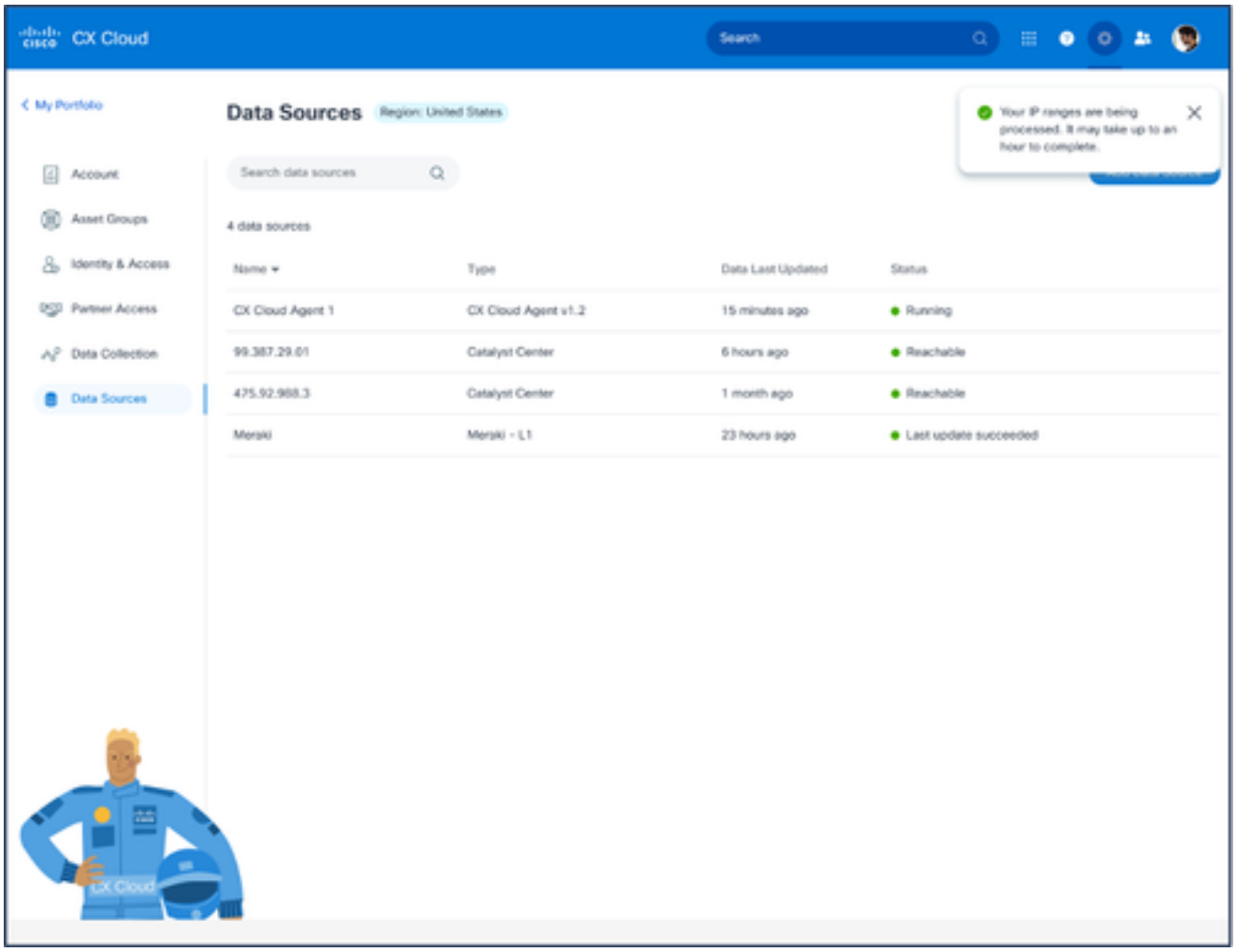
Bereitstellung von Erkennungsdetails und Planung der Bestandserfassung

7. Geben Sie die erforderlichen Details in den Abschnitten Discovery-Details bereitstellen und Inventory Collection planen ein.



Hinweis: Um einen weiteren IP-Bereich für den ausgewählten CX Cloud Agent hinzuzufügen, klicken Sie auf Add Another IP Range (Weiteren IP-Bereich hinzufügen), um zurück zum Fenster "Set Your Protocol" (Protokoll festlegen) zu navigieren und die Schritte in diesem Abschnitt zu wiederholen.

8. Klicken Sie auf Setup abschließen. Bei erfolgreicher Bereitstellung wird eine Bestätigung angezeigt.

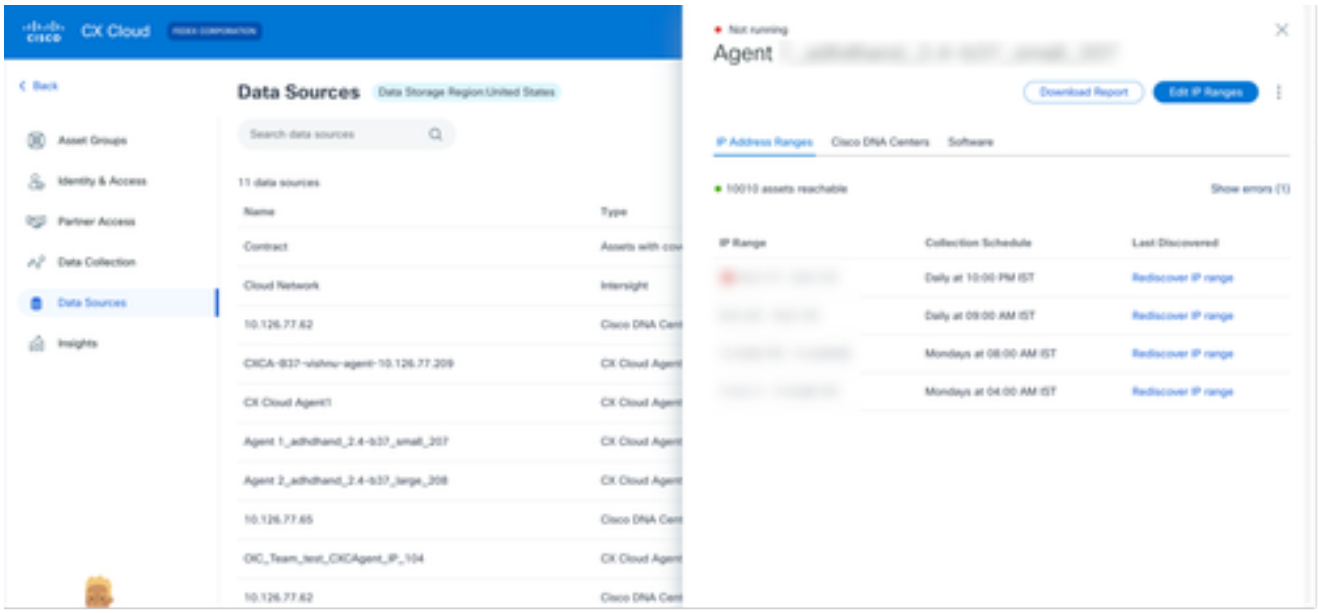


Bestätigungsmeldung

Bearbeiten von IP-Bereichen

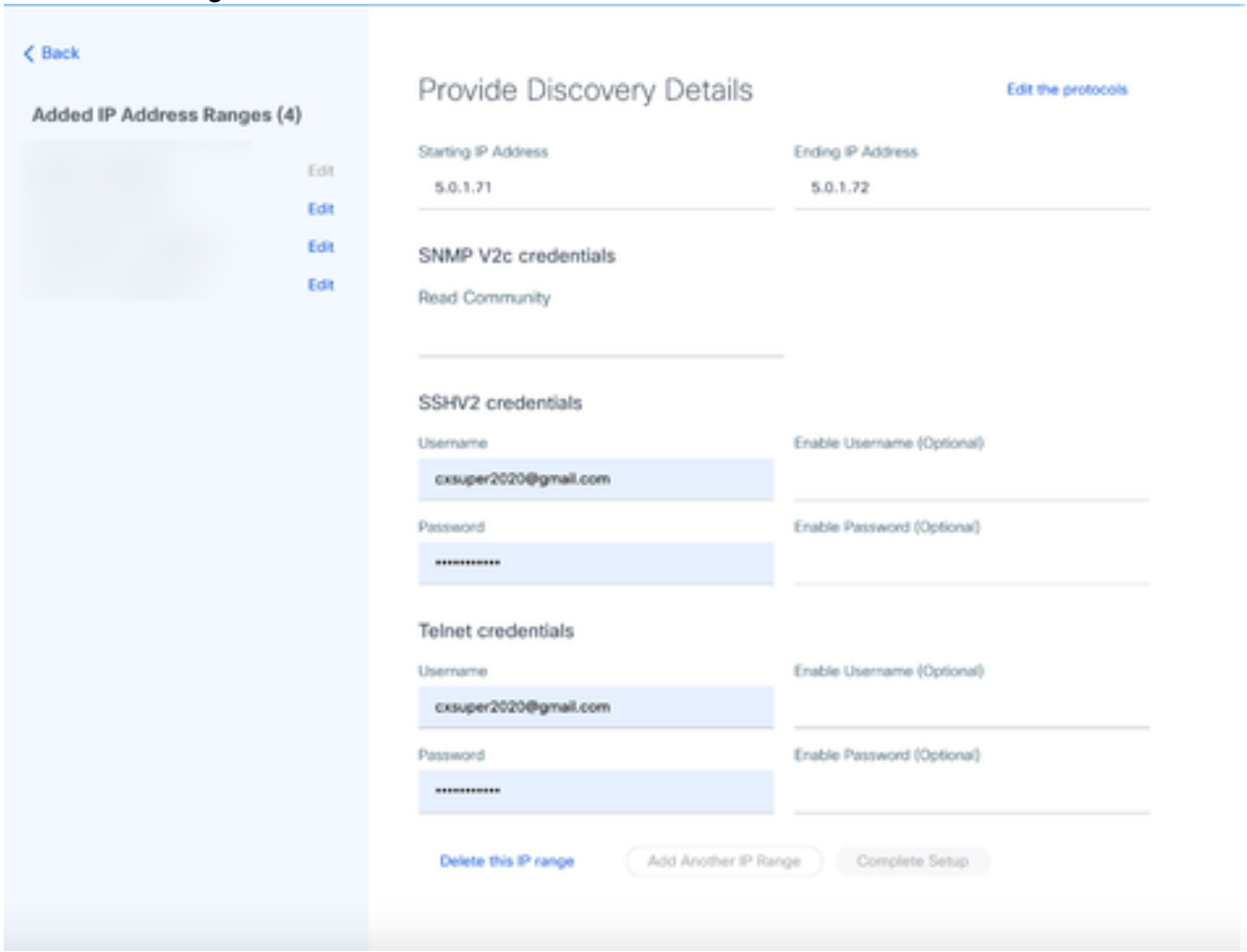
So bearbeiten Sie einen IP-Bereich

1. Navigieren Sie in das Fenster Datenquellen.
2. Klicken Sie auf den CX Cloud Agent, der die Bearbeitung des IP-Bereichs in Datenquellen erfordert. Das Detailfenster wird geöffnet.



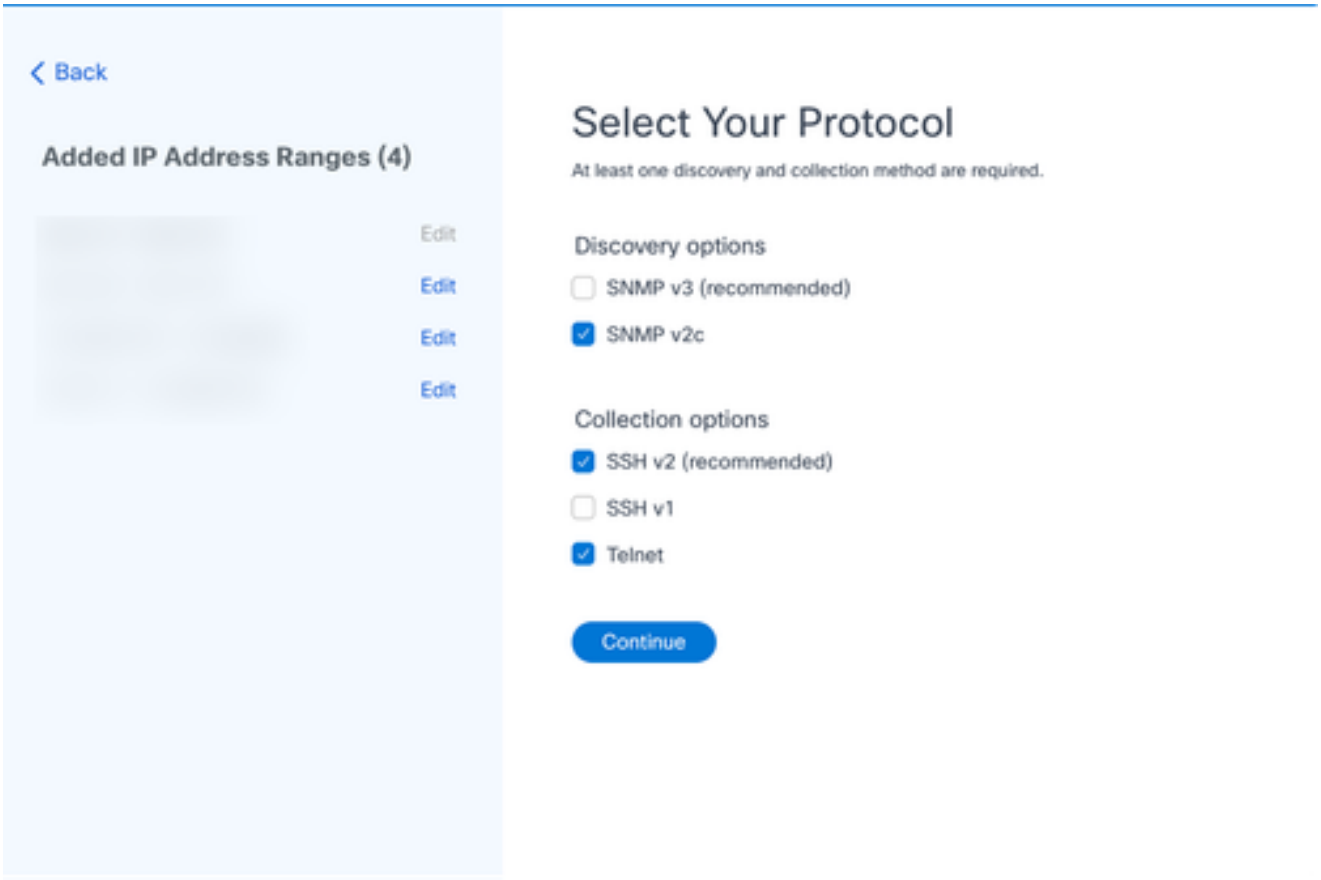
Datenquellen

3. Klicken Sie auf IP-Adressbereich bearbeiten. Das Fenster Verbindung mit CX Cloud herstellen wird geöffnet.



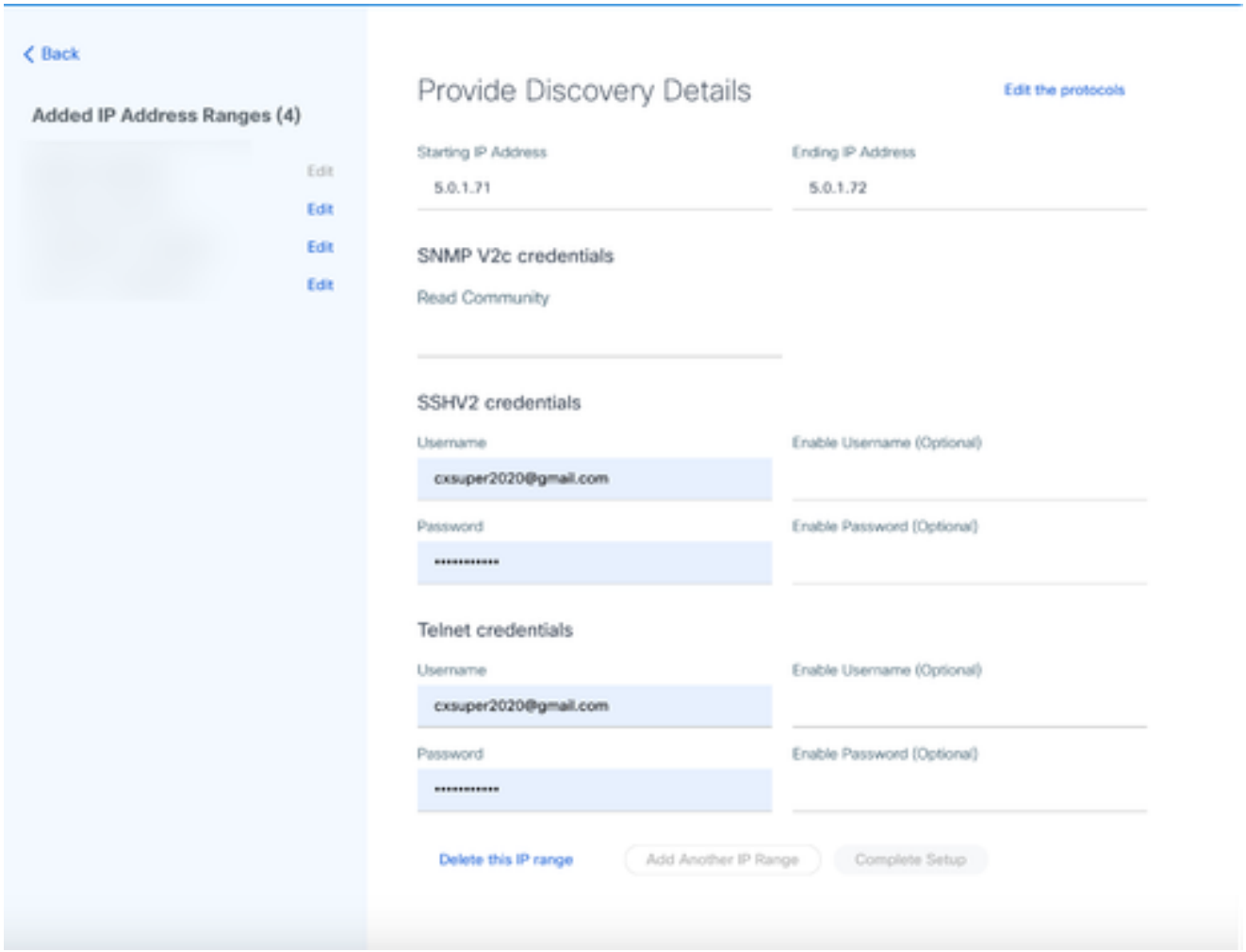
Bereitstellung von Erkennungsdetails

4. Klicken Sie auf Protokolle bearbeiten. Das Fenster Protokoll auswählen wird geöffnet.



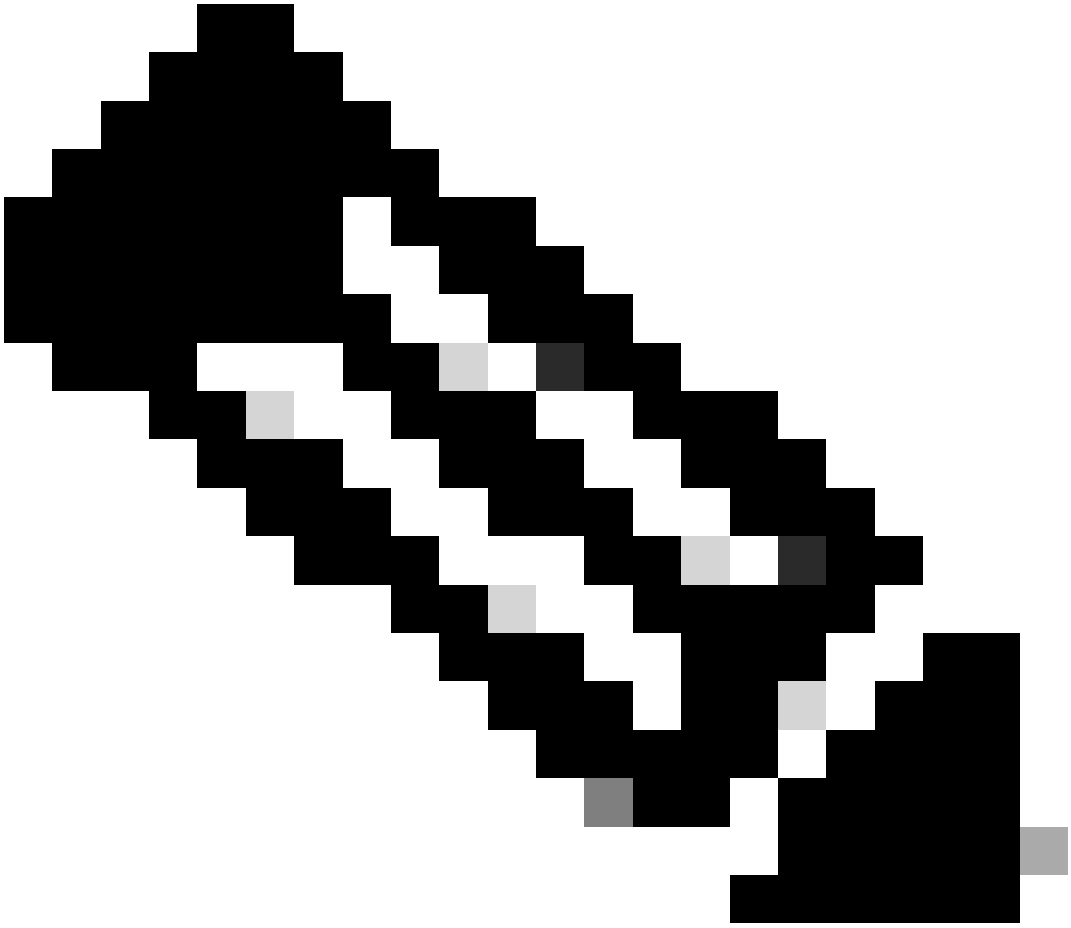
Protokoll auswählen

5. Aktivieren Sie die entsprechenden Kontrollkästchen, um die entsprechenden Protokolle auszuwählen, und klicken Sie auf Weiter, um zurück zum Fenster Discovery-Details angeben zu navigieren.



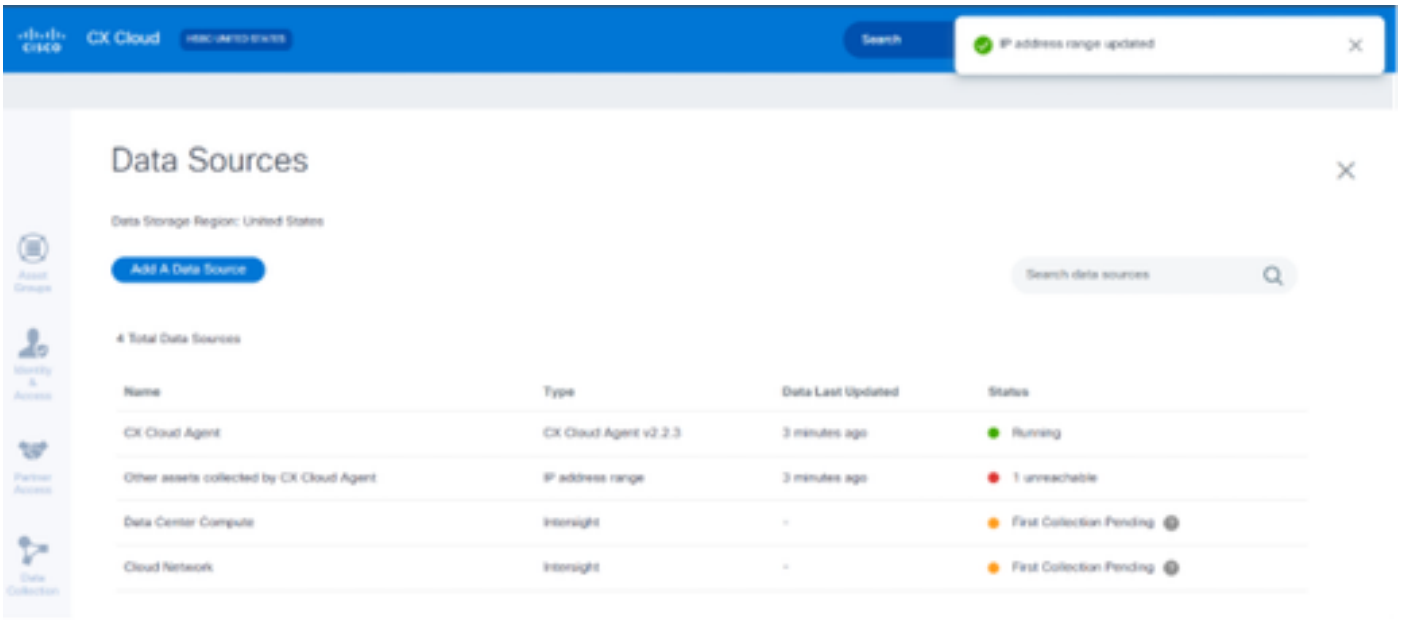
Bereitstellung von Erkennungsdetails

6. Bearbeiten Sie die Details nach Bedarf, und klicken Sie auf Complete Setup (Einrichtung abschließen). Das Fenster Datenquellen wird geöffnet und zeigt eine Meldung an, die das Hinzufügen eines oder mehrerer neu hinzugefügter IP-Adressbereiche bestätigt.



Hinweis: Diese Bestätigungsmeldung überprüft nicht, ob Geräte innerhalb des geänderten Bereichs erreichbar sind oder ob ihre Anmeldeinformationen akzeptiert werden. Diese Bestätigung erfolgt, wenn der Kunde den Erkennungsprozess initiiert.

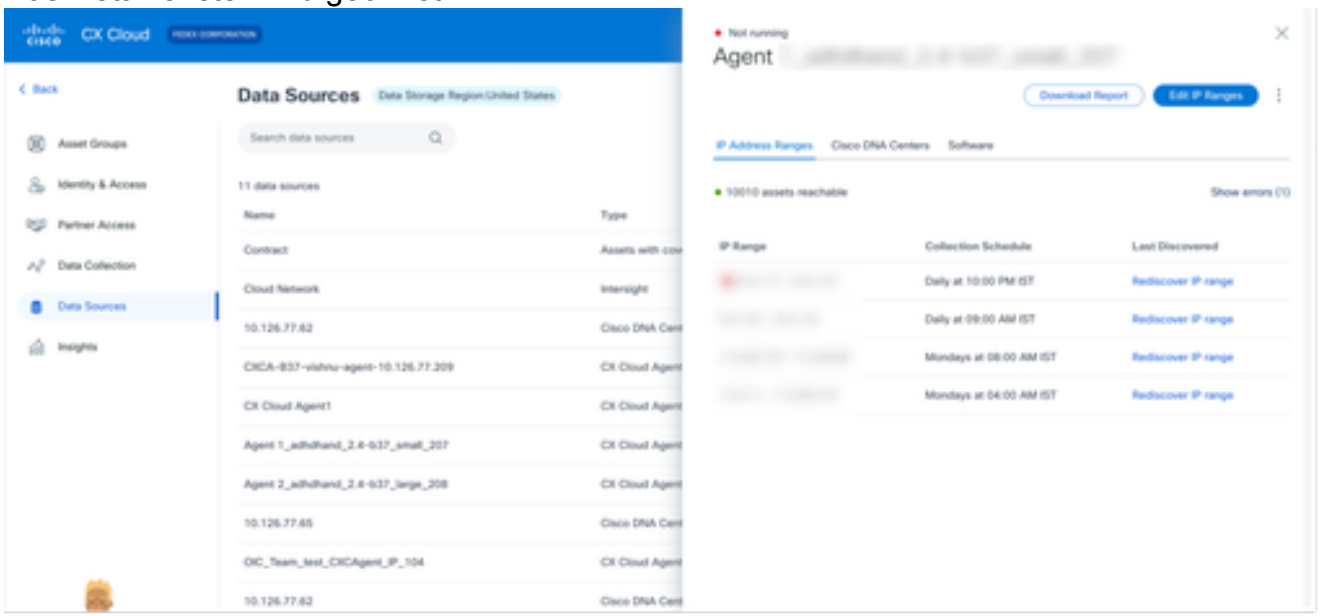
.



IP-Bereich wird gelöscht

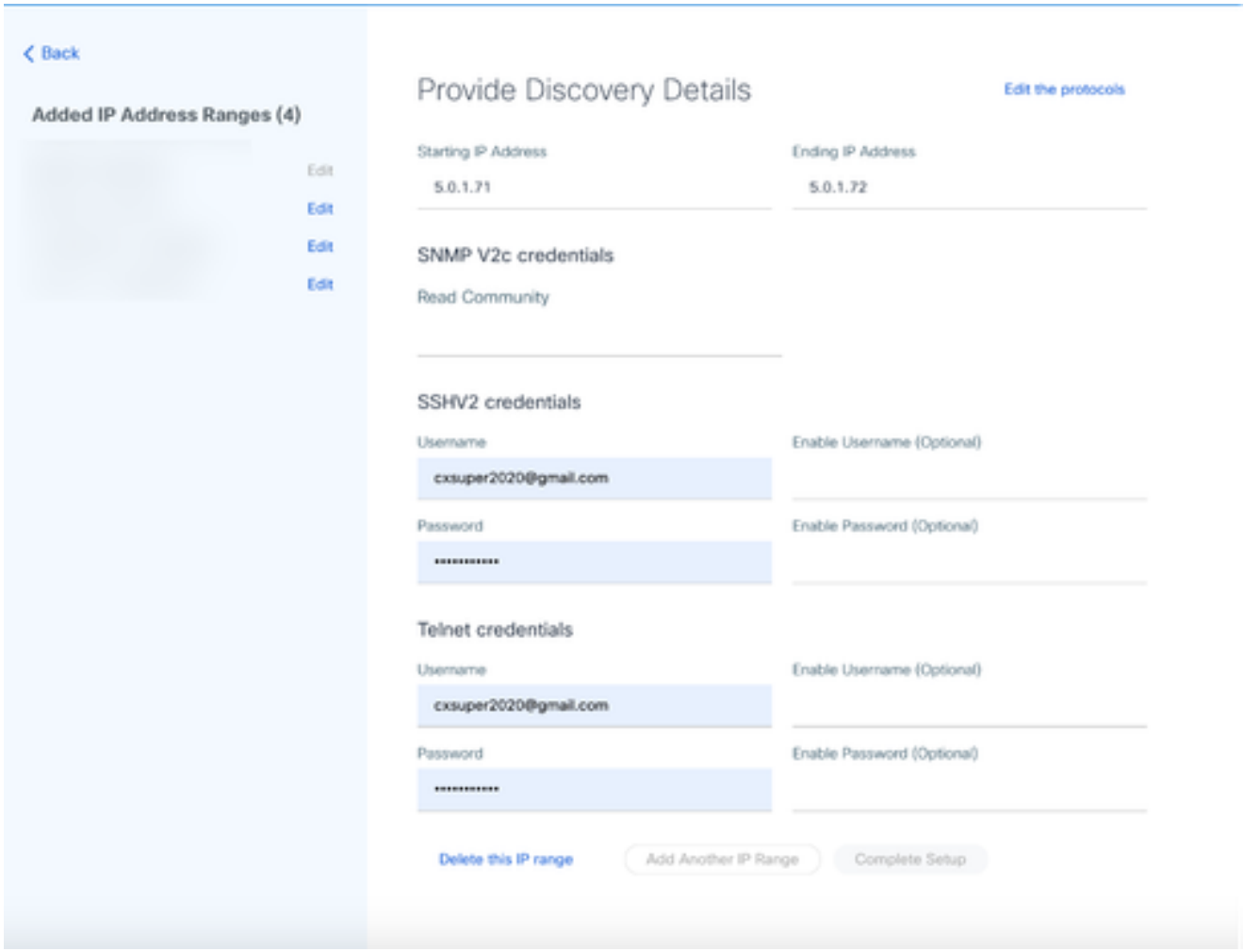
So löschen Sie einen IP-Bereich:

1. Navigieren Sie in das Fenster Datenquellen.
2. Wählen Sie den entsprechenden CX Cloud Agent mit dem zu löschenden IP-Bereich aus. Das Detailfenster wird geöffnet.



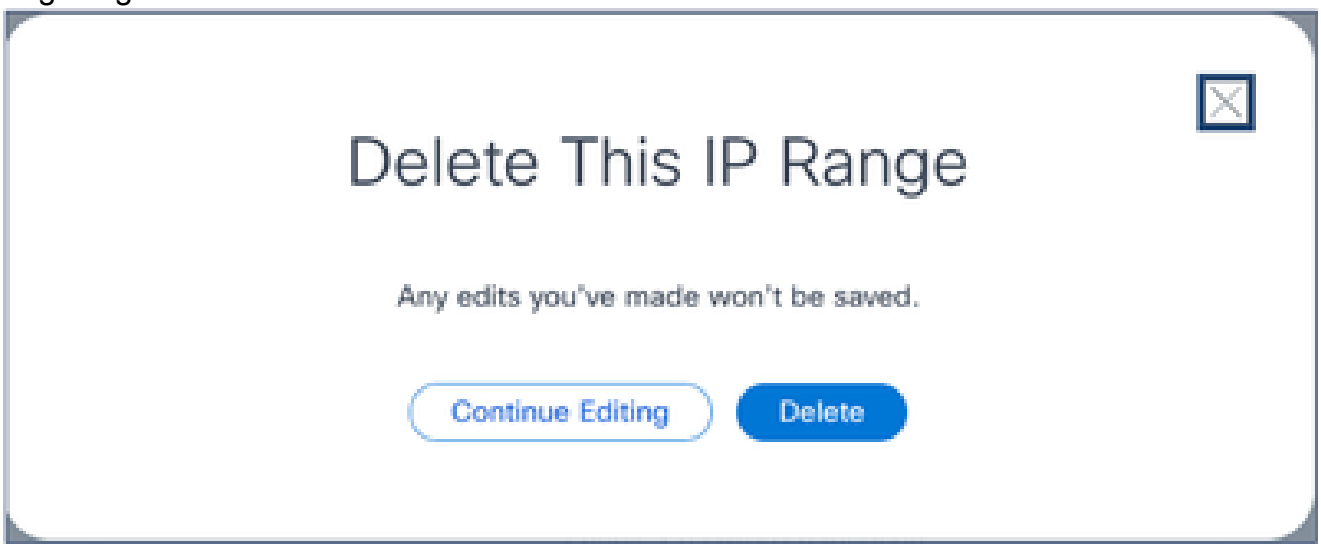
Datenquellen

3. Klicken Sie auf IP-Bereiche bearbeiten. Das Fenster Discovery-Details angeben wird geöffnet.



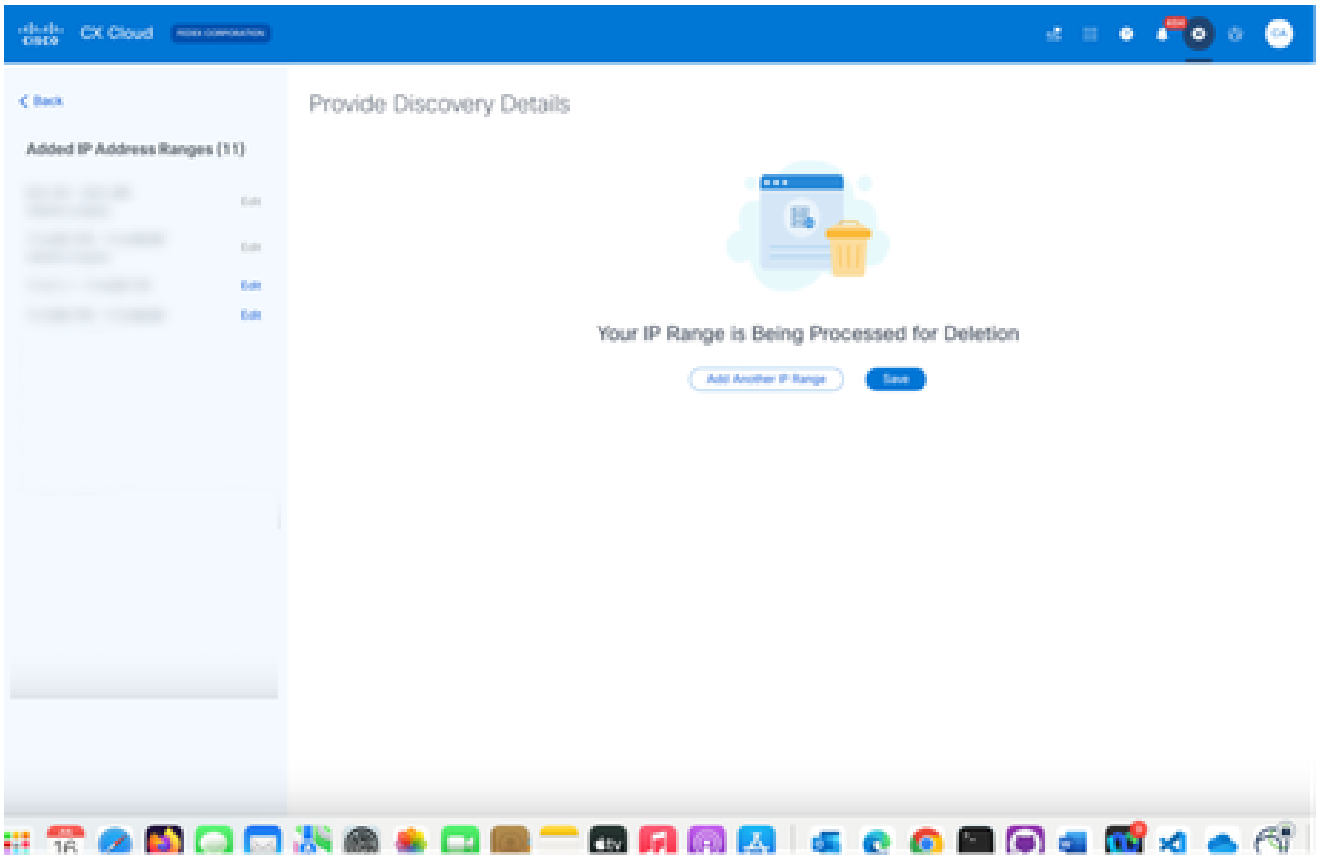
Bereitstellung von Erkennungsdetails

4. Klicken Sie auf den Link Diesen IP-Bereich löschen. Die Bestätigungsmeldung wird angezeigt.



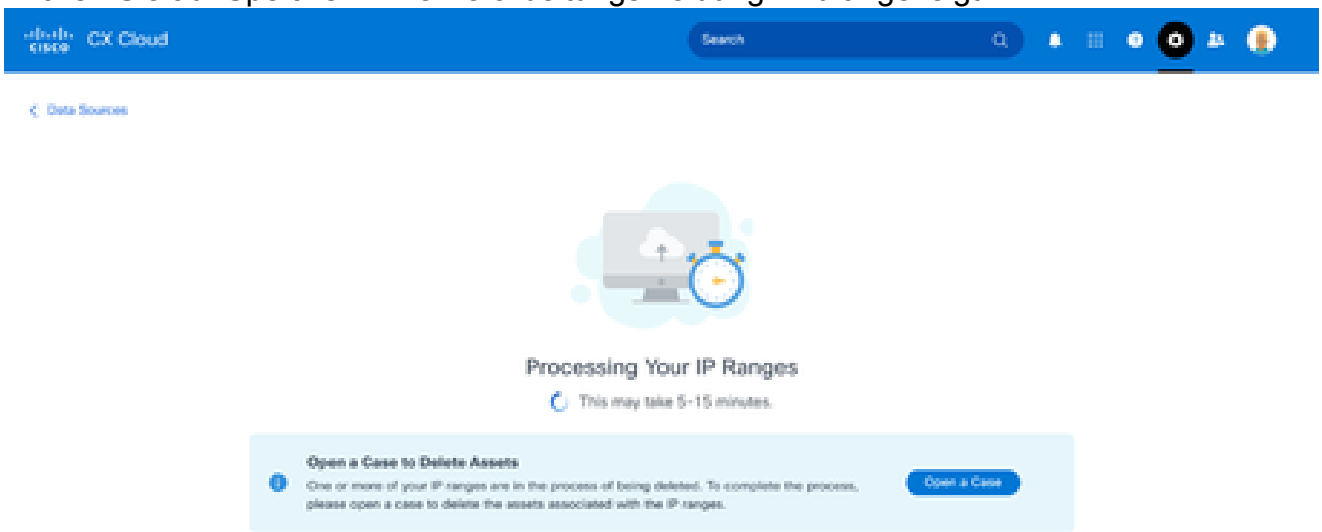
Löschen der Nachricht bestätigen

5. Klicken Sie auf Löschen.



Löschen des IP-Bereichs

6. Klicken Sie auf Speichern. Die Verarbeitungsmeldung wird angezeigt.



7. Klicken Sie auf Ticket öffnen, um ein Ticket zu erstellen und die dem IP-Bereich zugeordneten Ressourcen zu löschen. Das Fenster Datenquellen wird geöffnet und zeigt eine Bestätigungsmeldung an.

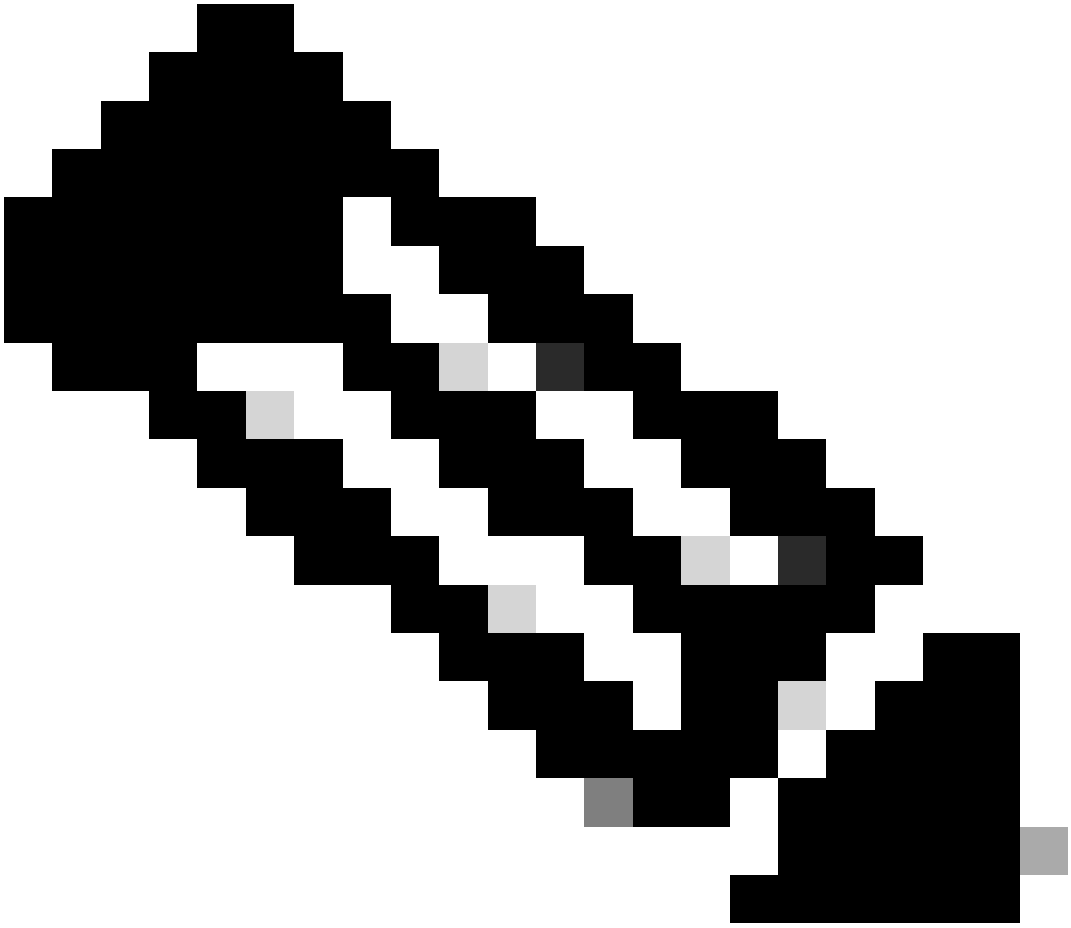
Von mehreren Controllern erkannte Geräte

Es ist möglich, dass einige Geräte sowohl vom Cisco DNA Center als auch von einer direkten Geräteverbindung zu CX Cloud Agent erkannt werden, wodurch doppelte Daten von diesen Geräten gesammelt werden. Um zu vermeiden, dass doppelte Daten gesammelt werden und die Geräte nur von einem Controller verwaltet werden, muss eine Rangfolge festgelegt werden, für die CX Cloud Agent die Geräte verwaltet.

- Wenn ein Gerät zuerst vom Cisco DNA Center entdeckt und dann durch direkte Geräteverbindung (mithilfe einer Seed-Datei oder eines IP-Bereichs) wiederentdeckt wird, hat Cisco DNA Center bei der Steuerung des Geräts Vorrang.
- Wenn ein Gerät zuerst durch eine direkte Geräteverbindung mit dem CX Cloud Agent erkannt und dann vom Cisco DNA Center wiederentdeckt wird, hat Cisco DNA Center bei der Steuerung des Geräts Vorrang.

Planen von Diagnosescans

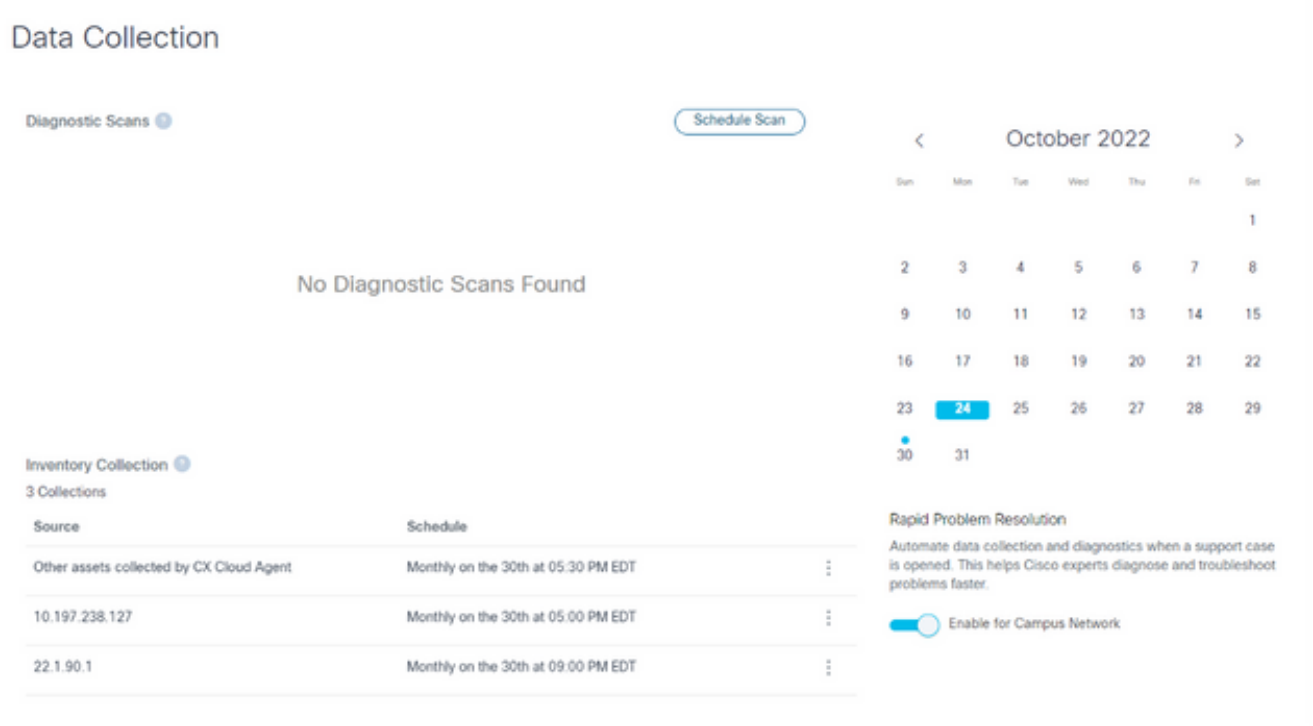
Kunden können On-Demand-Diagnosen in der CX Cloud planen.



Hinweis: Cisco empfiehlt, Diagnosescans zu planen oder bedarfsgesteuerte Scans in einem Abstand von mindestens 6-7 Stunden von den Bestandserfassungsplänen zu initiieren, damit sie sich nicht überschneiden. Die gleichzeitige Ausführung mehrerer Diagnosescans kann den Scanvorgang verlangsamen und möglicherweise zu Scanfehlern führen.

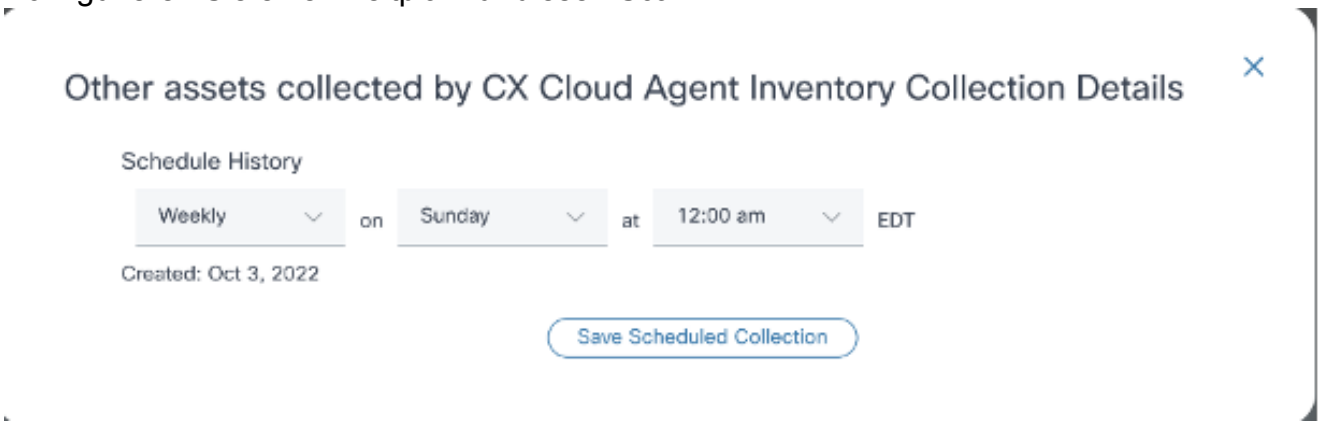
So planen Sie Diagnosescans:

1. Klicken Sie auf der Startseite auf das Symbol Einstellungen (Geräte).
2. Wählen Sie auf der Seite Datenquellen im linken Bereich die Option Datensammlung aus.
3. Klicken Sie auf Scannen planen.



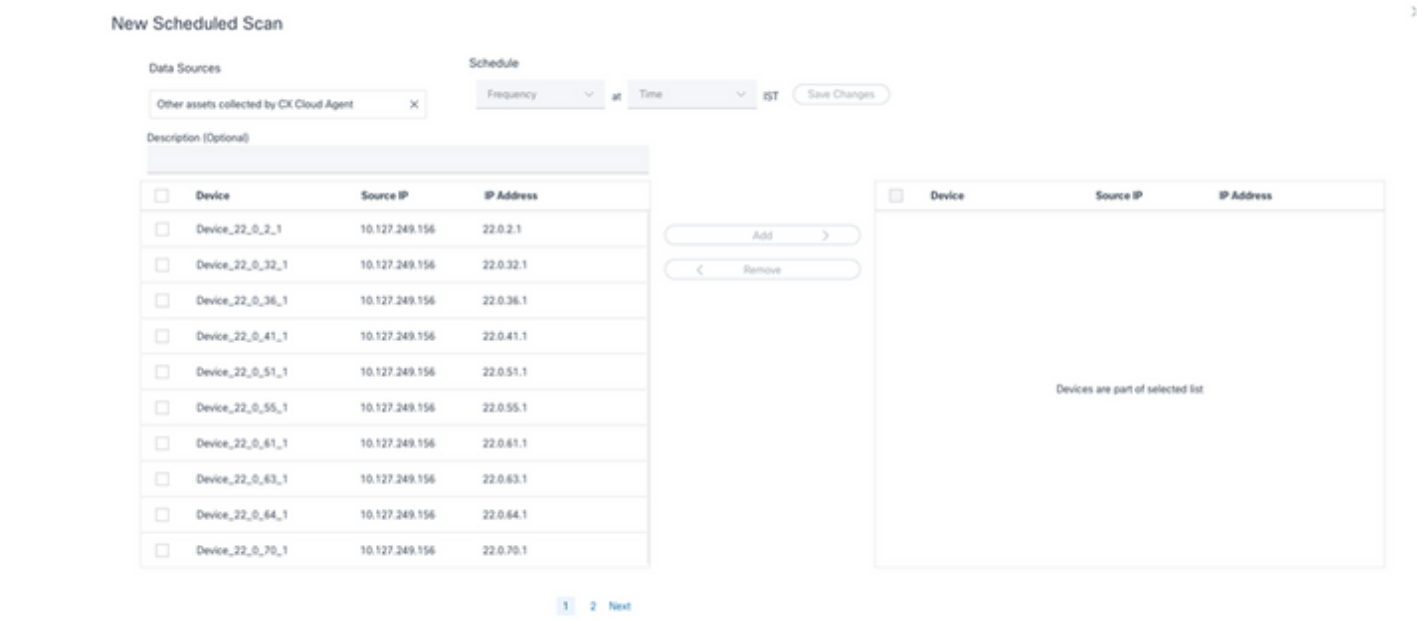
Datensammlung

4. Konfigurieren Sie einen Zeitplan für diesen Scan.



Scan-Zeitplan konfigurieren

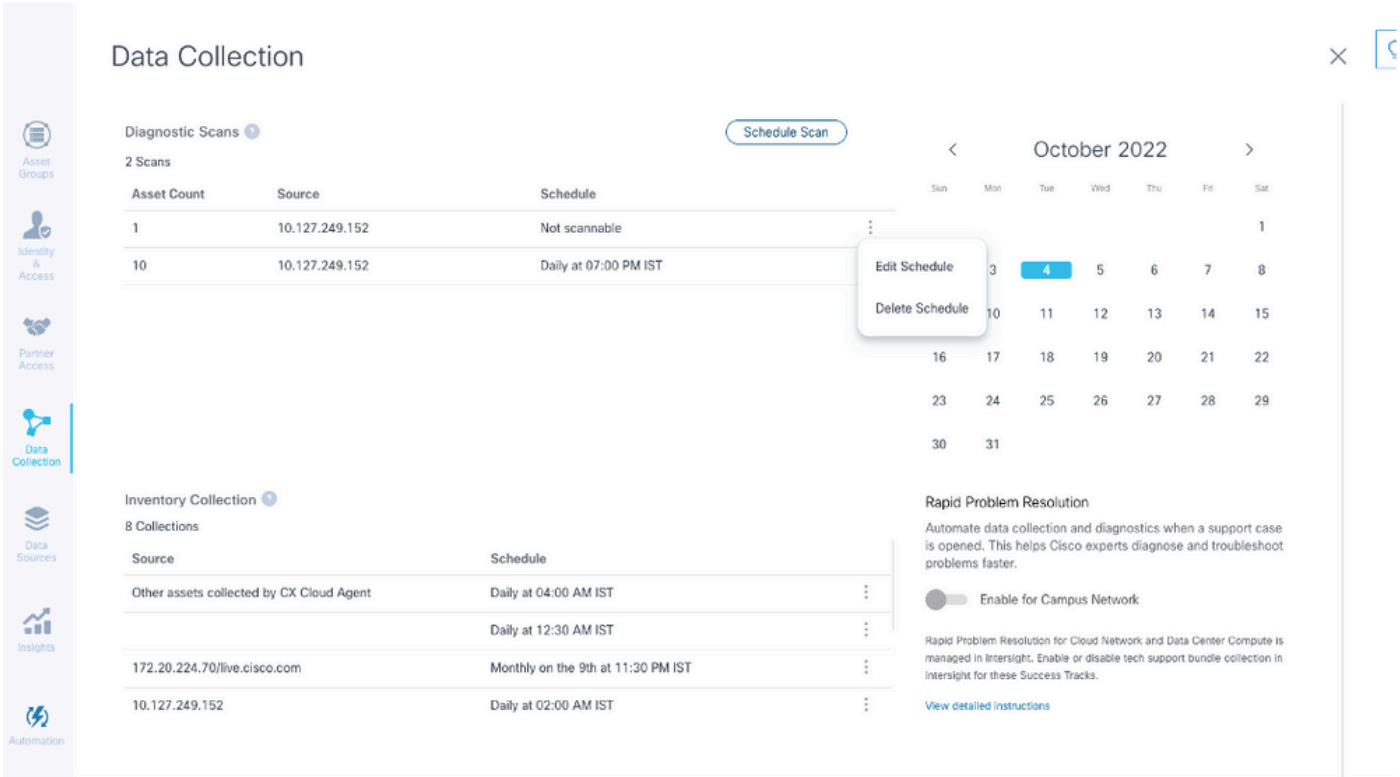
5. Wählen Sie in der Geräteliste alle Geräte für den Scan aus, und klicken Sie auf Hinzufügen.



Einen Scan ansetzen

6. Klicken Sie auf Save Changes (Änderungen speichern), wenn die Planung abgeschlossen ist.

Die Diagnosescans und die Inventarerfassungszeitpläne können auf der Seite Datenerfassung bearbeitet und gelöscht werden.



Datenerfassung mit Optionen zum Bearbeiten und Löschen von Zeitplänen

Upgrade von CX Cloud Agent VMs auf mittlere und große

Konfigurationen

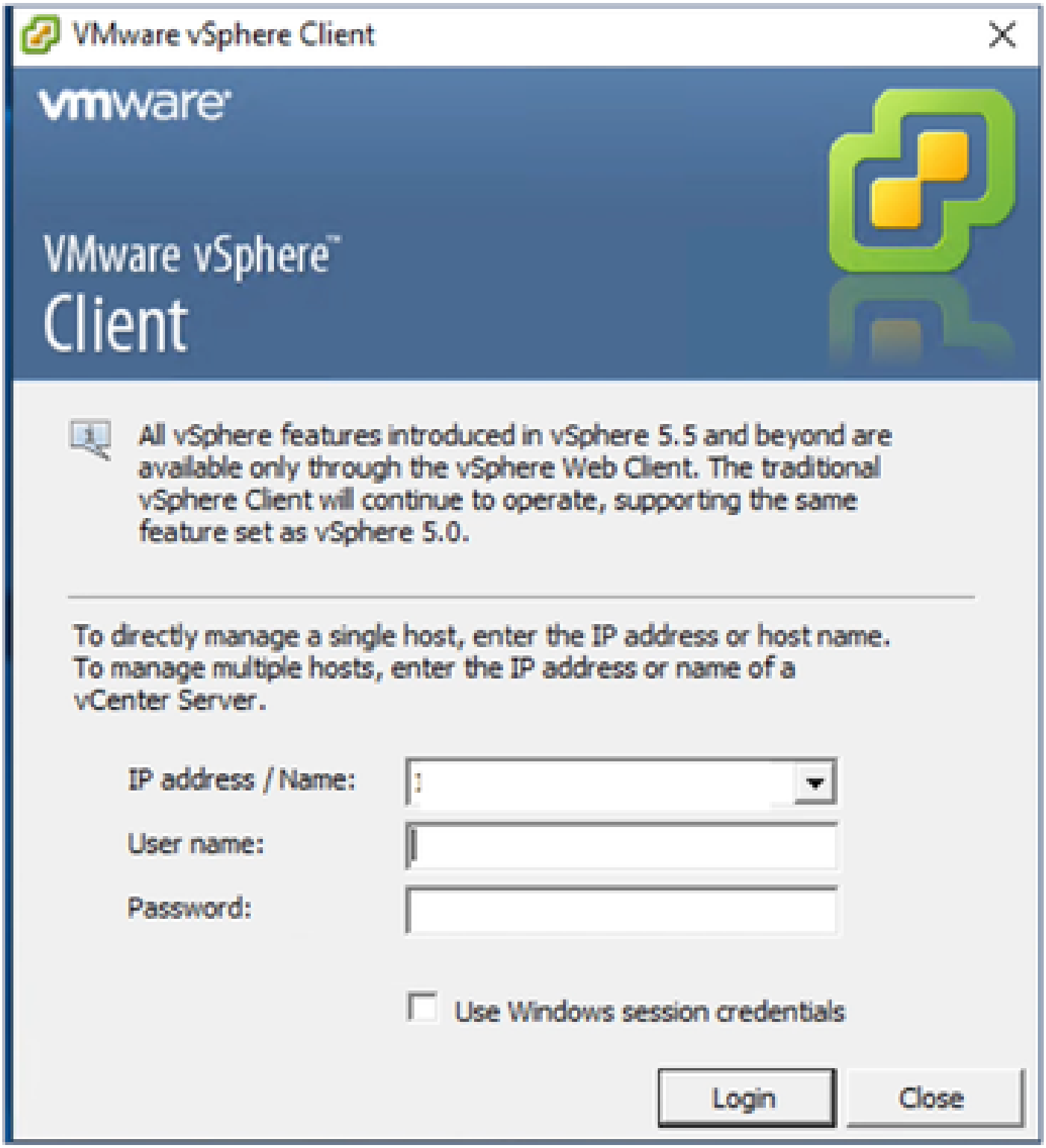
Nach dem Upgrade von VMs ist Folgendes nicht möglich:

- Herabstufung von einer großen oder mittleren bis hin zu einer kleinen Konfiguration
- Herabstufung von einer großen auf eine mittlere Konfiguration
- Upgrade von einer mittleren auf eine große Konfiguration

Vor dem Upgrade des virtuellen Systems empfiehlt Cisco die Erstellung eines Snapshots für die Wiederherstellung bei einem Ausfall. Weitere Informationen finden Sie unter Sichern und Wiederherstellen der CX Cloud VM.

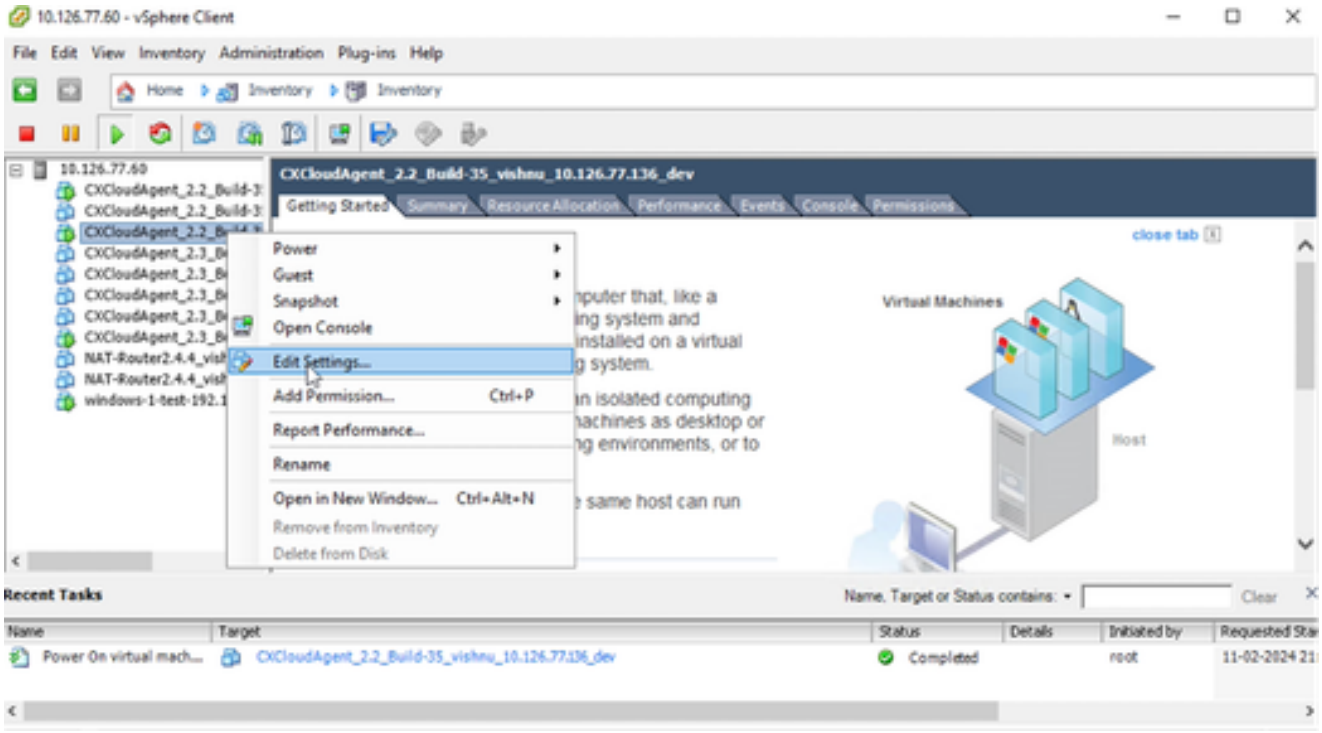
Neukonfiguration mit VMware vSphere Thick Client

So aktualisieren Sie die VM-Konfiguration mit dem vorhandenen VMware vSphere Thick Client:



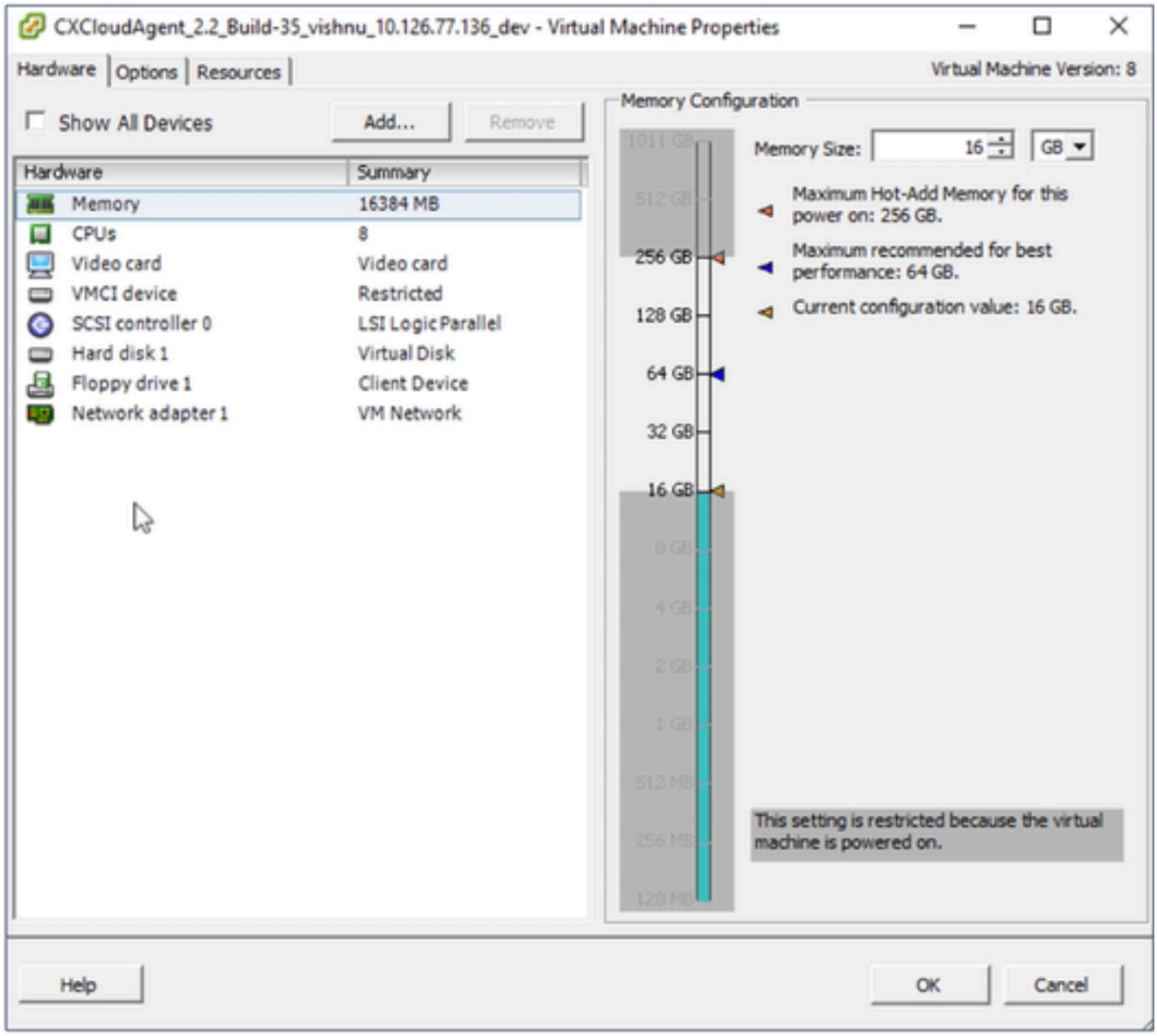
vSphere-Client

1. Melden Sie sich beim VMware vSphere-Client an. Auf der Startseite wird eine Liste der virtuellen Systeme angezeigt.



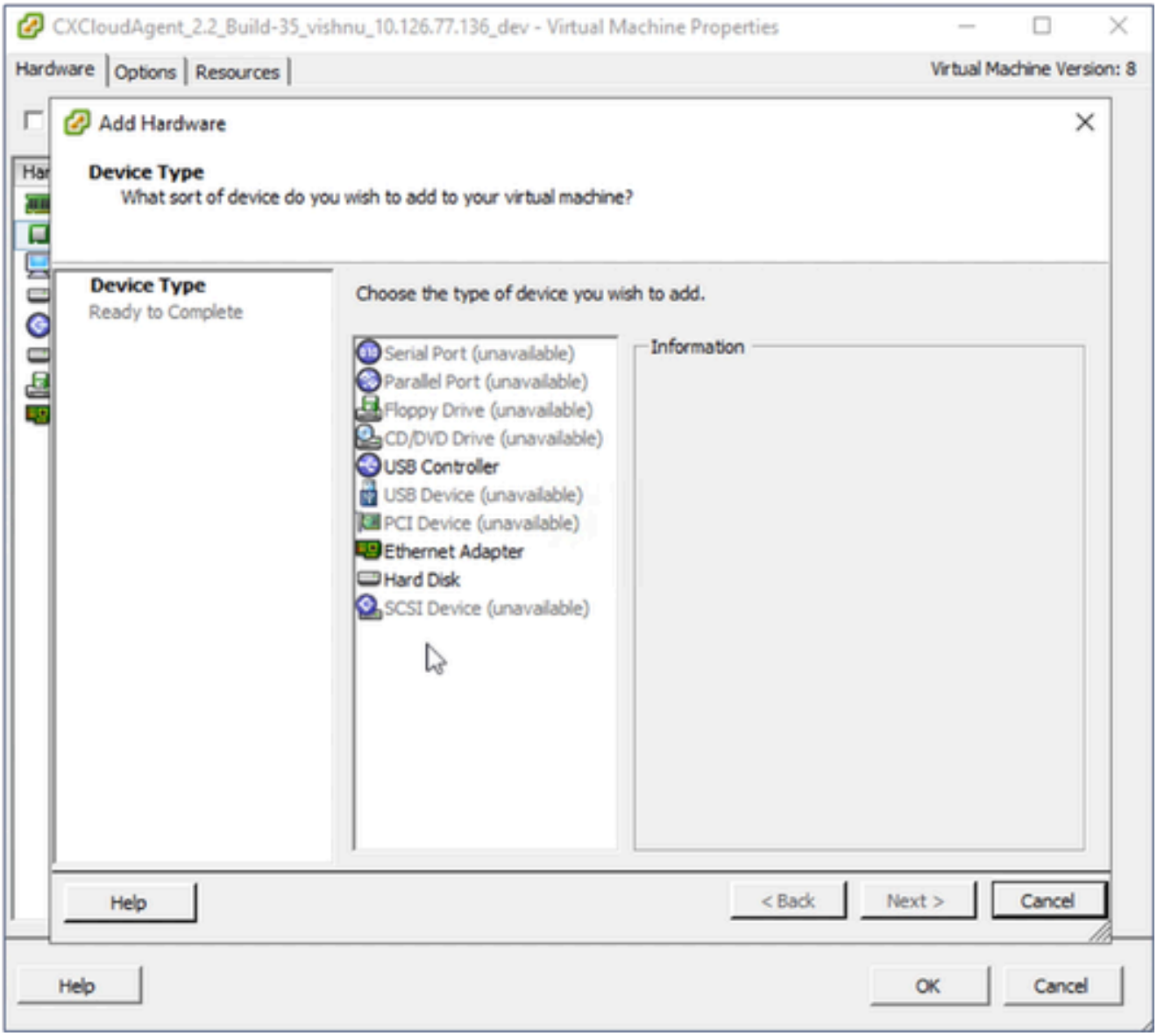
Einstellungen bearbeiten

2. Klicken Sie mit der rechten Maustaste auf die Ziel-VM, und wählen Sie im Menü Edit Settings (Einstellungen bearbeiten). Das Fenster VM-Eigenschaften wird geöffnet.



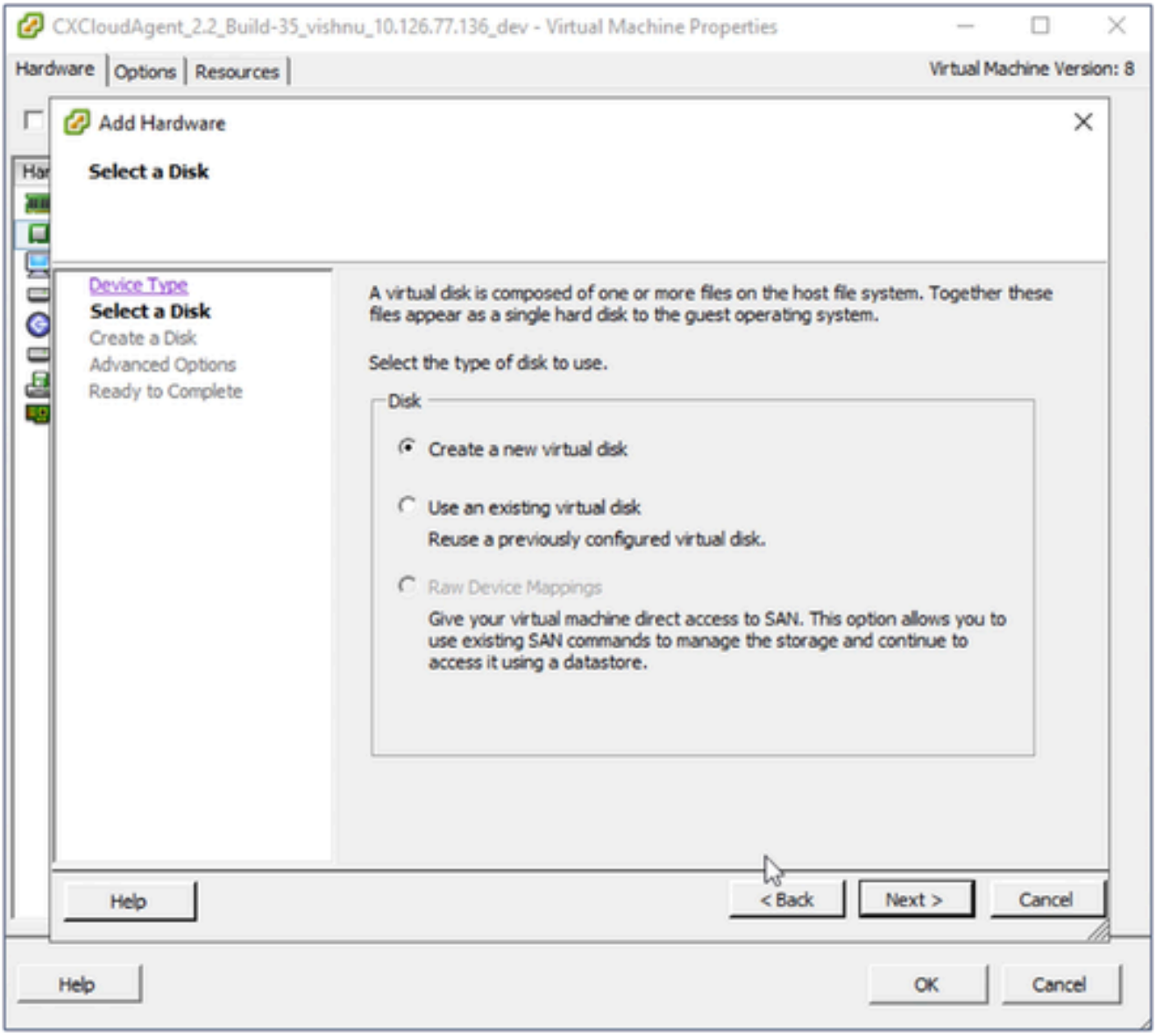
VM-Eigenschaften

3. Aktualisieren Sie die Werte für die Speichergröße wie angegeben:
   Mittel: 32 GB (32768 MB)
   Groß: 64 GB (65536 MB)
4. Wählen Sie CPUs aus, und aktualisieren Sie die angegebenen Werte:
   Mittel: 16 Kerne (8 Sockel *2 Kerne/Sockel)
   Groß: 32 Kerne (16 Sockel *2 Kerne/Sockel)
5. Klicken Sie auf Hinzufügen. Das Fenster Hardware hinzufügen wird geöffnet.



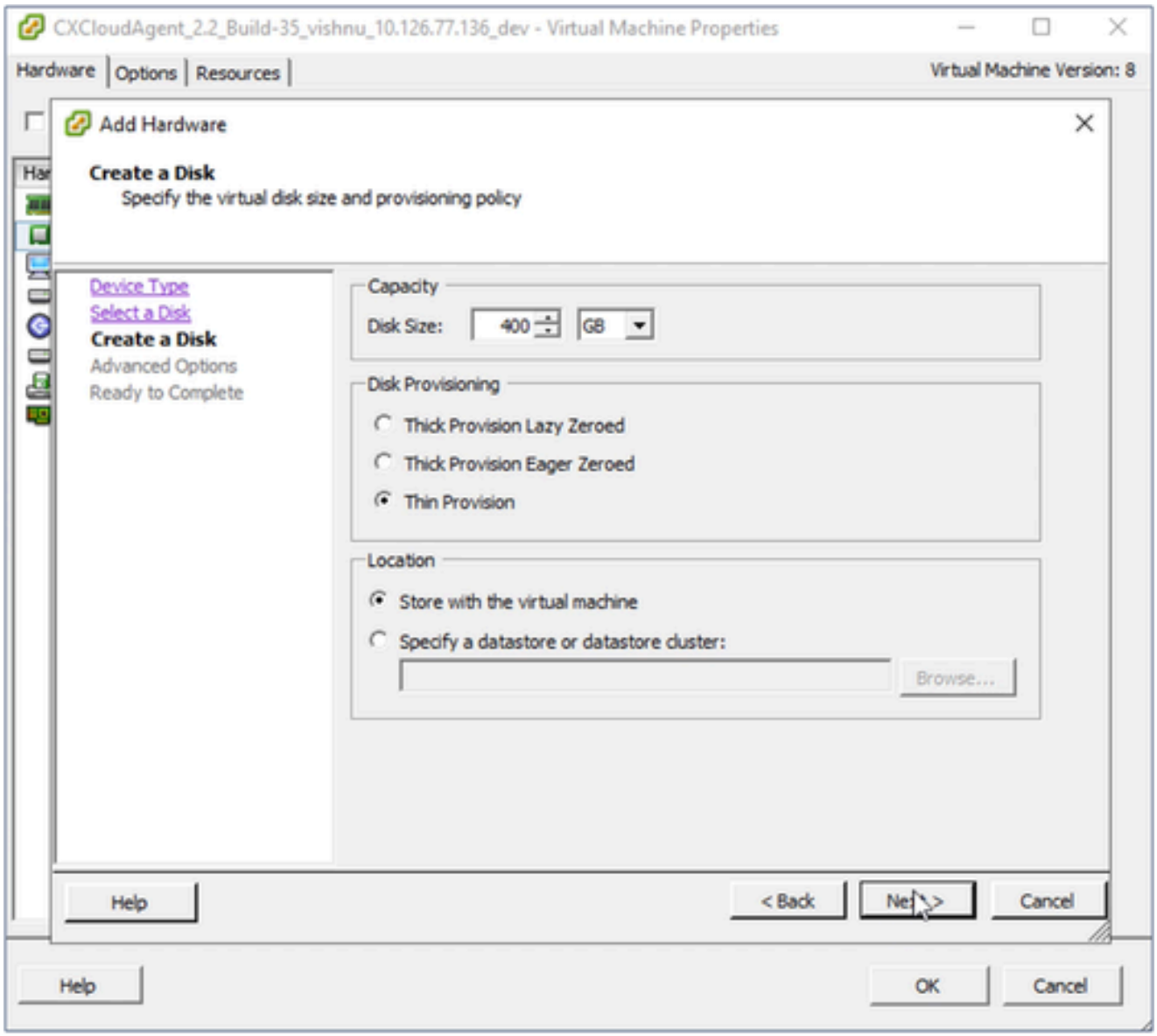
Gerätetyp

6. Wählen Sie als Gerätetyp Hard Disk (Festplatte).
7. Klicken Sie auf Next (Weiter).



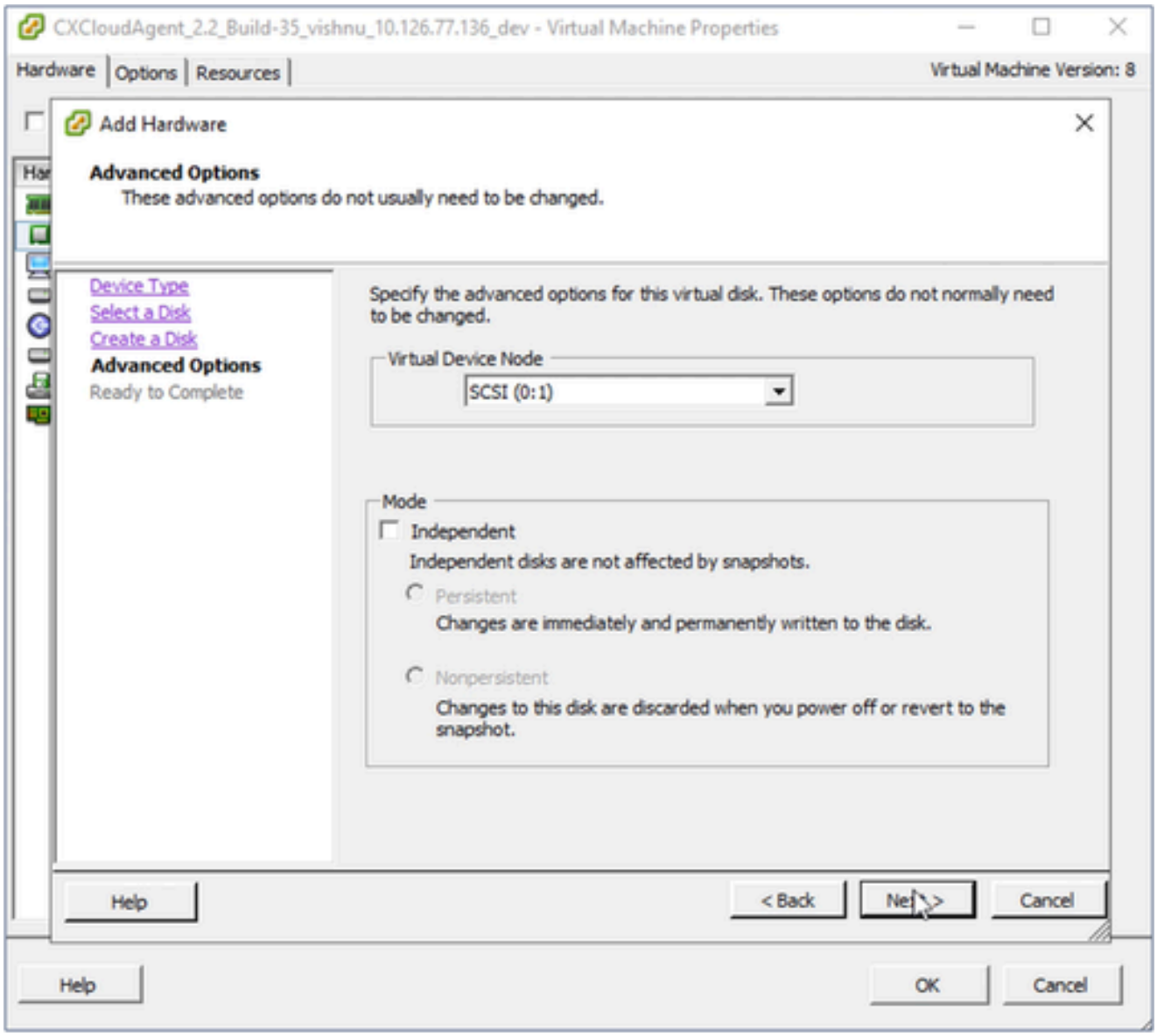
Festplatte auswählen

8. Aktivieren Sie das Optionsfeld Neues virtuelles Laufwerk erstellen, und klicken Sie auf Weiter.



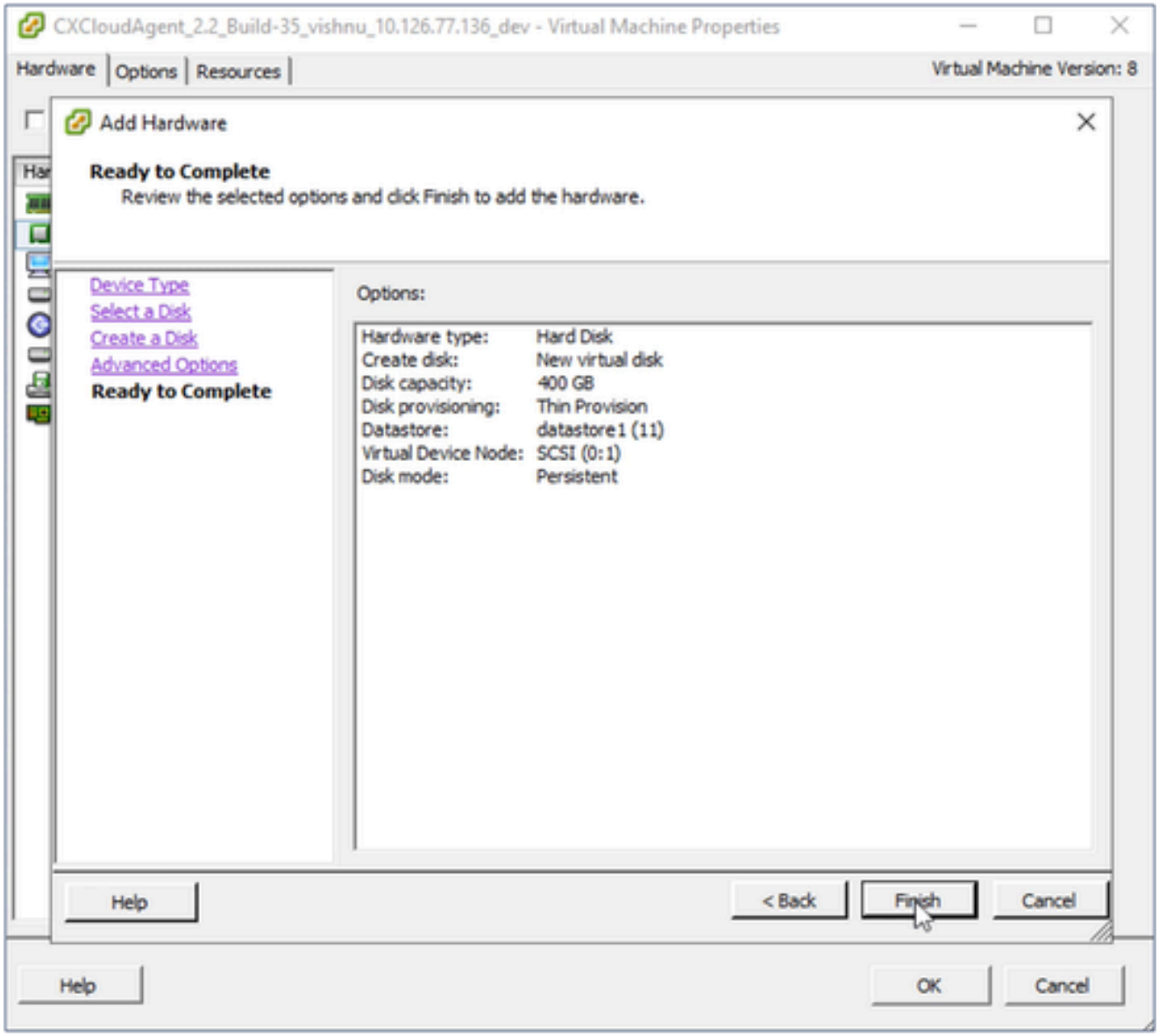
Datenträger erstellen

9. Aktualisieren Sie Kapazität > Festplattengröße wie angegeben:
   Klein bis mittel: 400 GB (Anfangsgröße: 200 GB, Erhöhung der Gesamtkapazität auf 600 GB)
   Klein bis groß: 1.000 GB (Anfangsgröße: 200 GB, Erhöhung der Gesamtkapazität auf 1.200 GB)
10. Wählen Sie das Optionsfeld Thin Provision für die Festplattenbereitstellung aus.
11. Klicken Sie auf Next (Weiter). Das Fenster Erweiterte Optionen wird angezeigt.



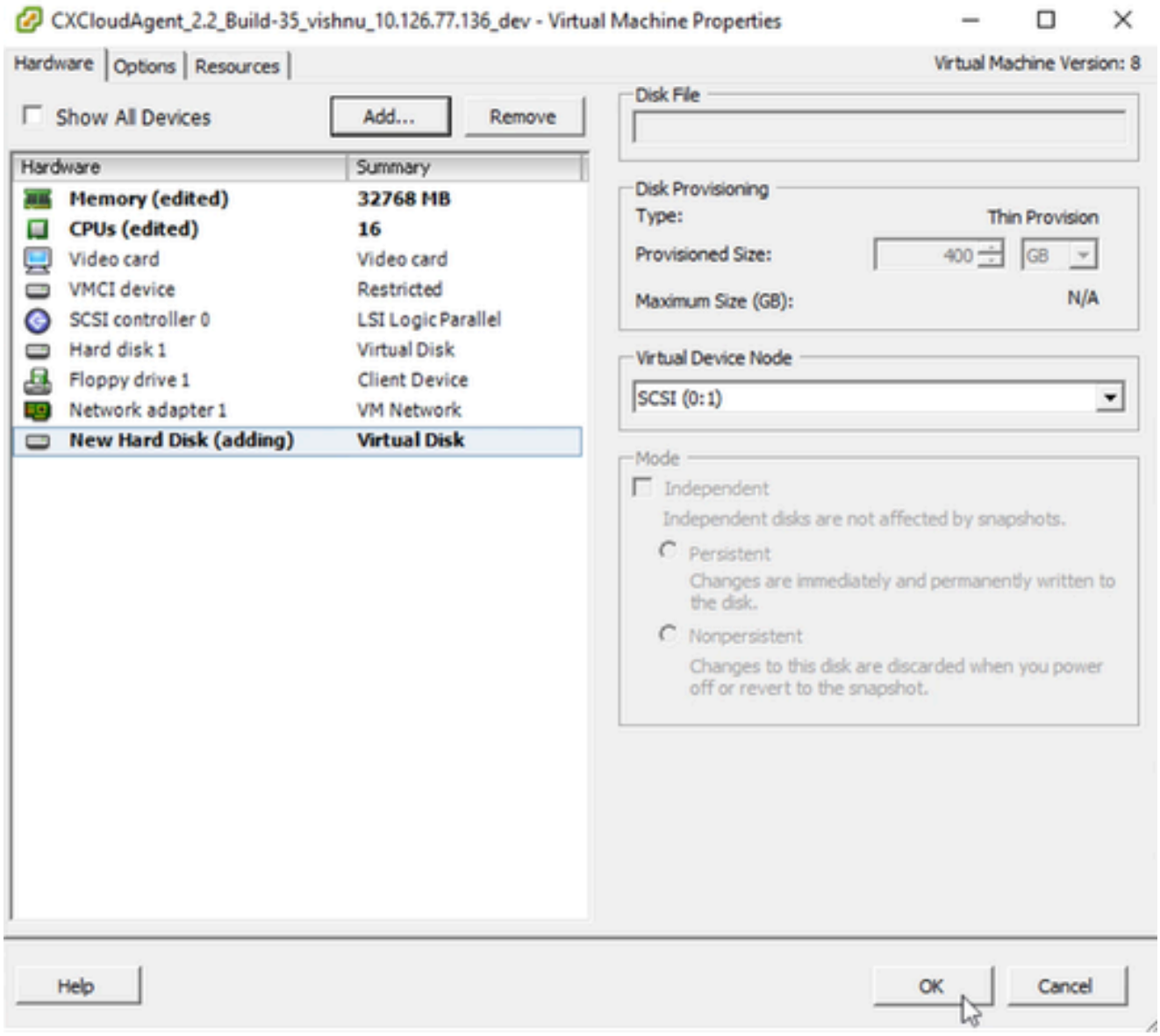
Erweiterte Optionen

12. Nehmen Sie keine Änderungen vor. Klicken Sie auf Weiter, um fortzufahren.



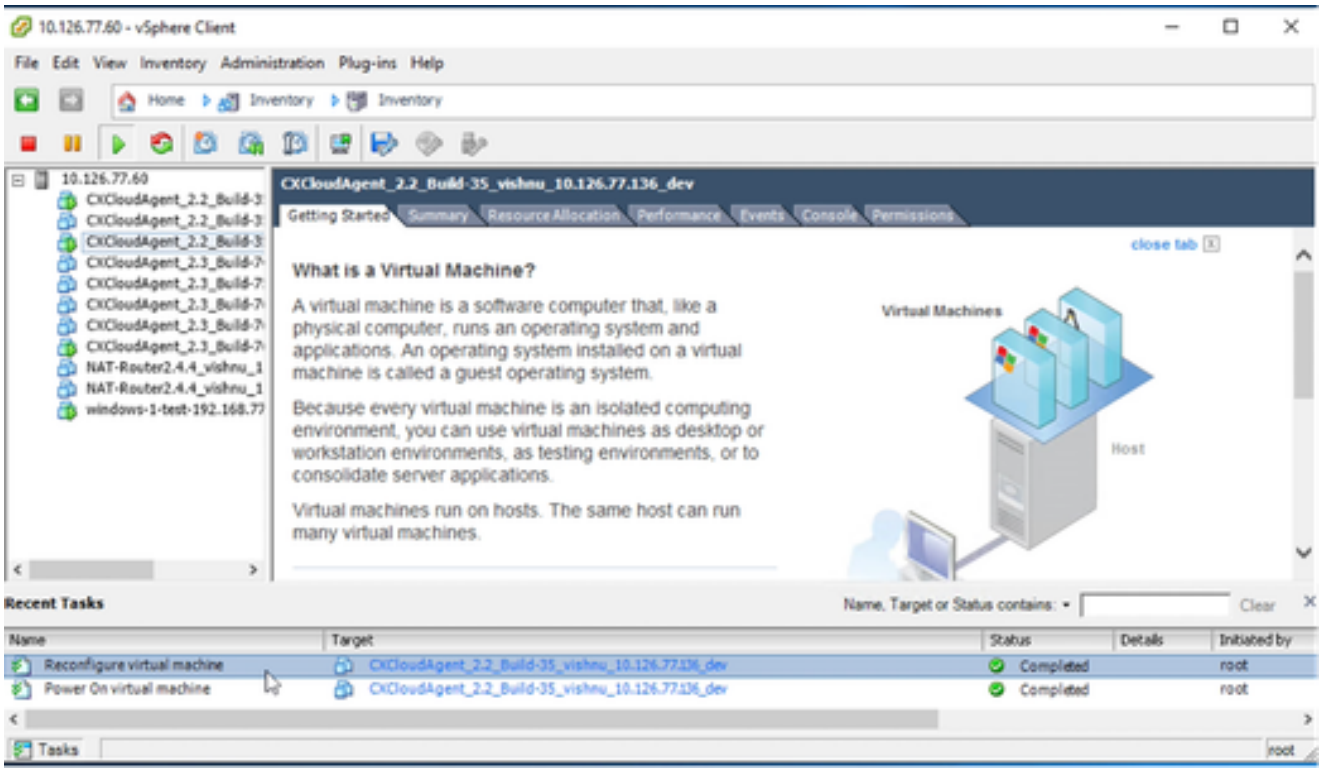
Bereit zur Fertigstellung

13. Klicken Sie auf Beenden.

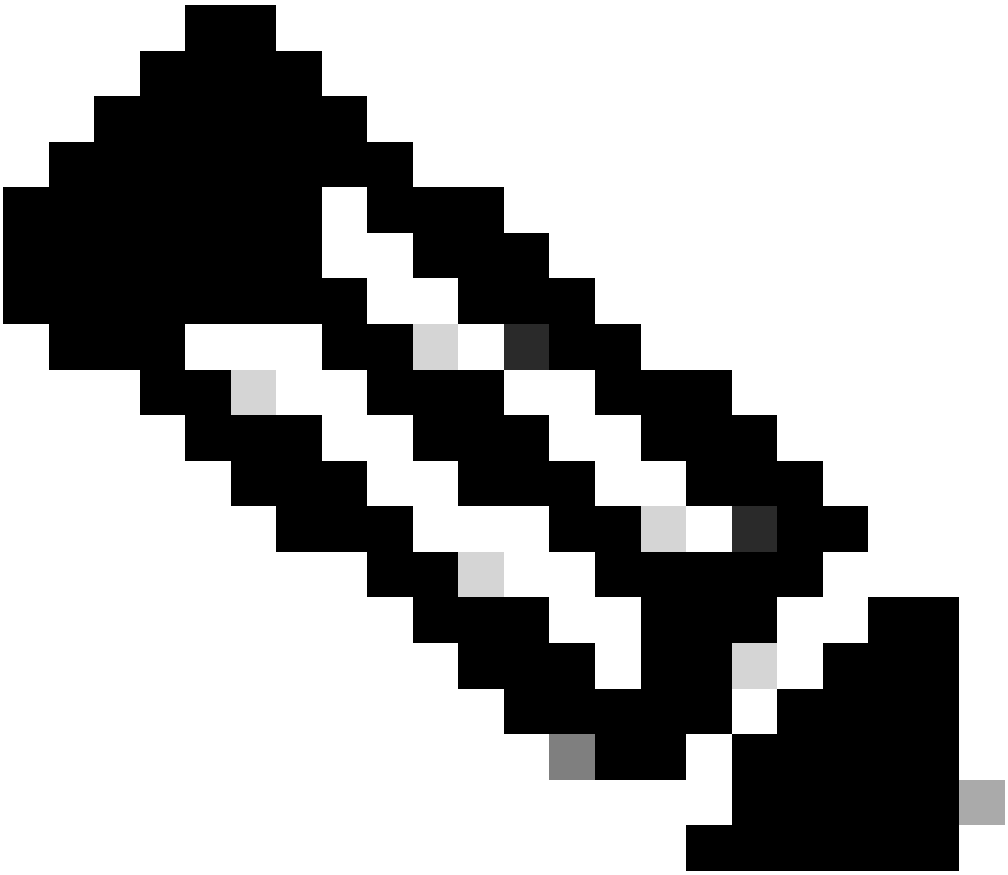


Hardware

14. Klicken Sie auf OK, um die Neukonfiguration abzuschließen. Die abgeschlossene Neukonfiguration wird im Bereich Zuletzt durchgeführte Aufgaben angezeigt.



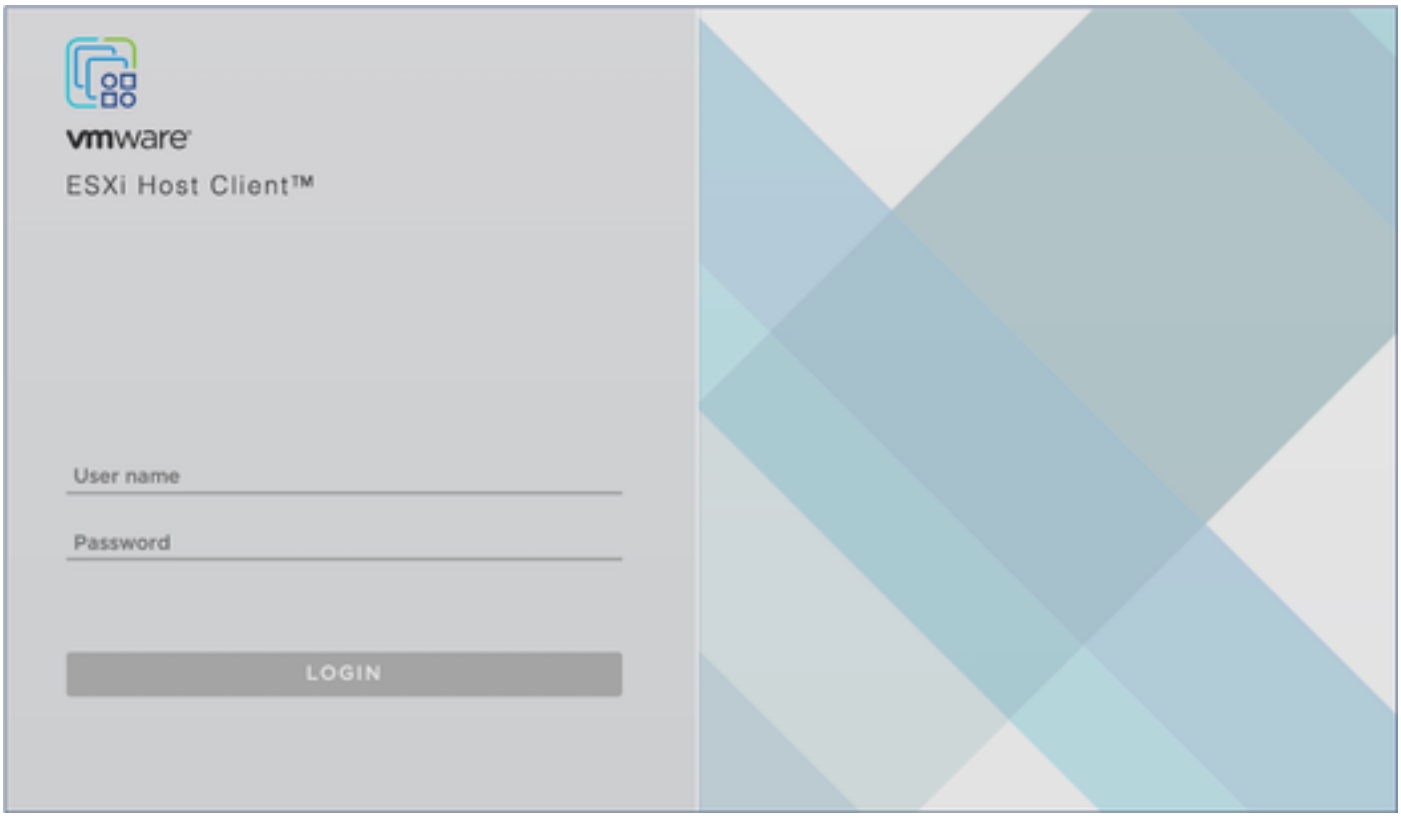
Zuletzt durchgeführte Aufgaben



Hinweis: Konfigurationsänderungen können in etwa fünf Minuten abgeschlossen werden.

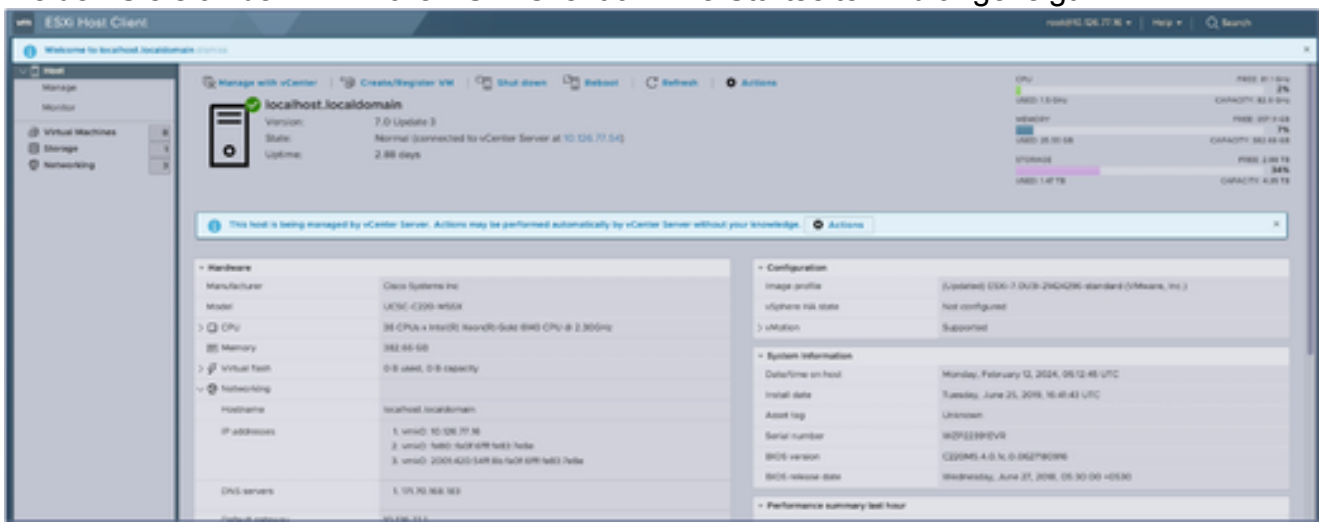
Neukonfiguration mit Web-Client ESXi v6.0

So aktualisieren Sie VM-Konfigurationen mit Web Client ESXi v6.0:



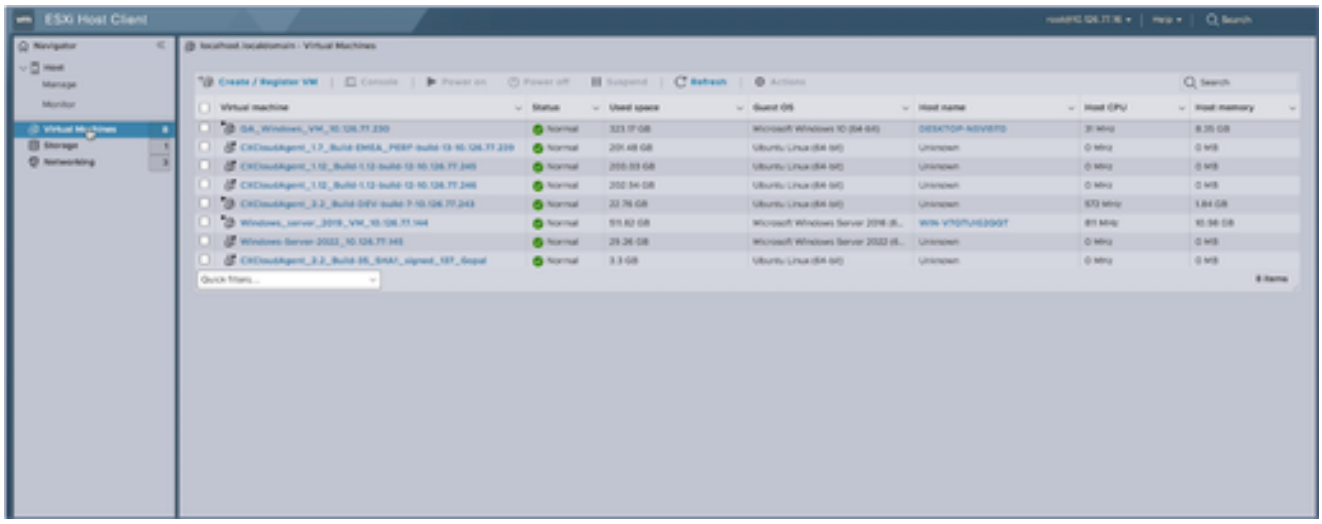
ESXi-Client

1. Melden Sie sich beim VMware ESXi-Client an. Die Startseite wird angezeigt.



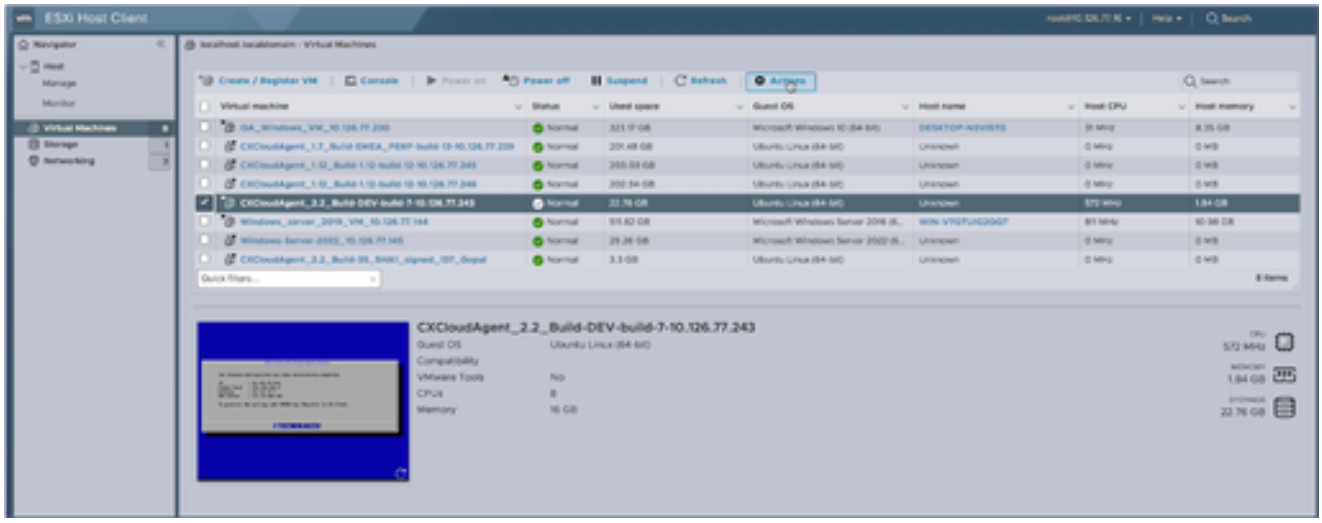
ESXi-Startseite

2. Klicken Sie auf Virtual Machine, um eine Liste der virtuellen Systeme anzuzeigen.



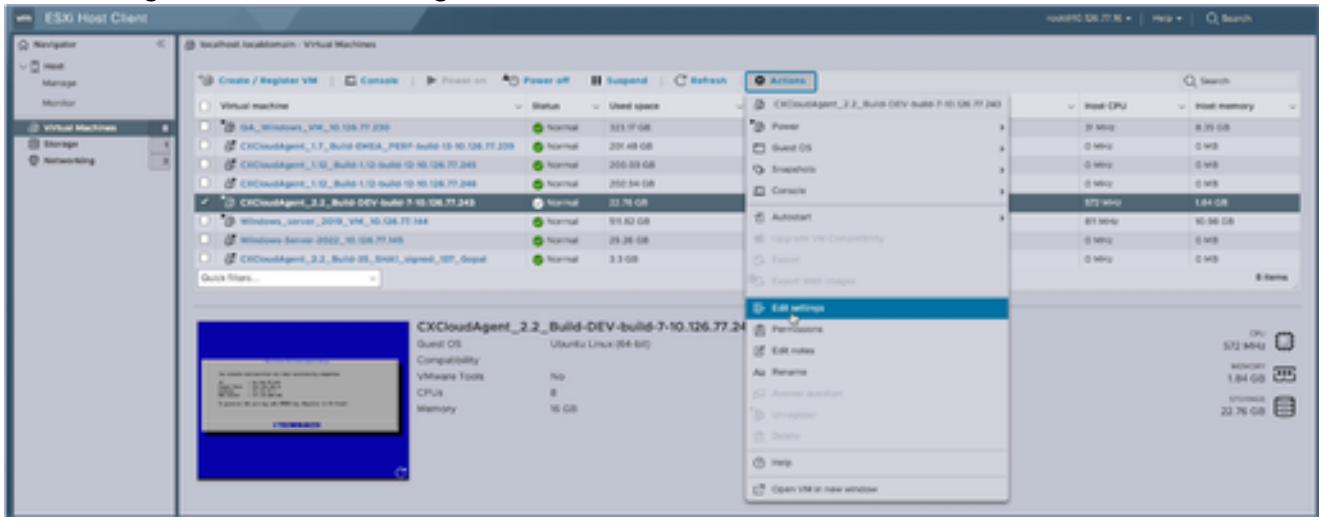
Liste der VMs

3. Wählen Sie die Ziel-VM aus.

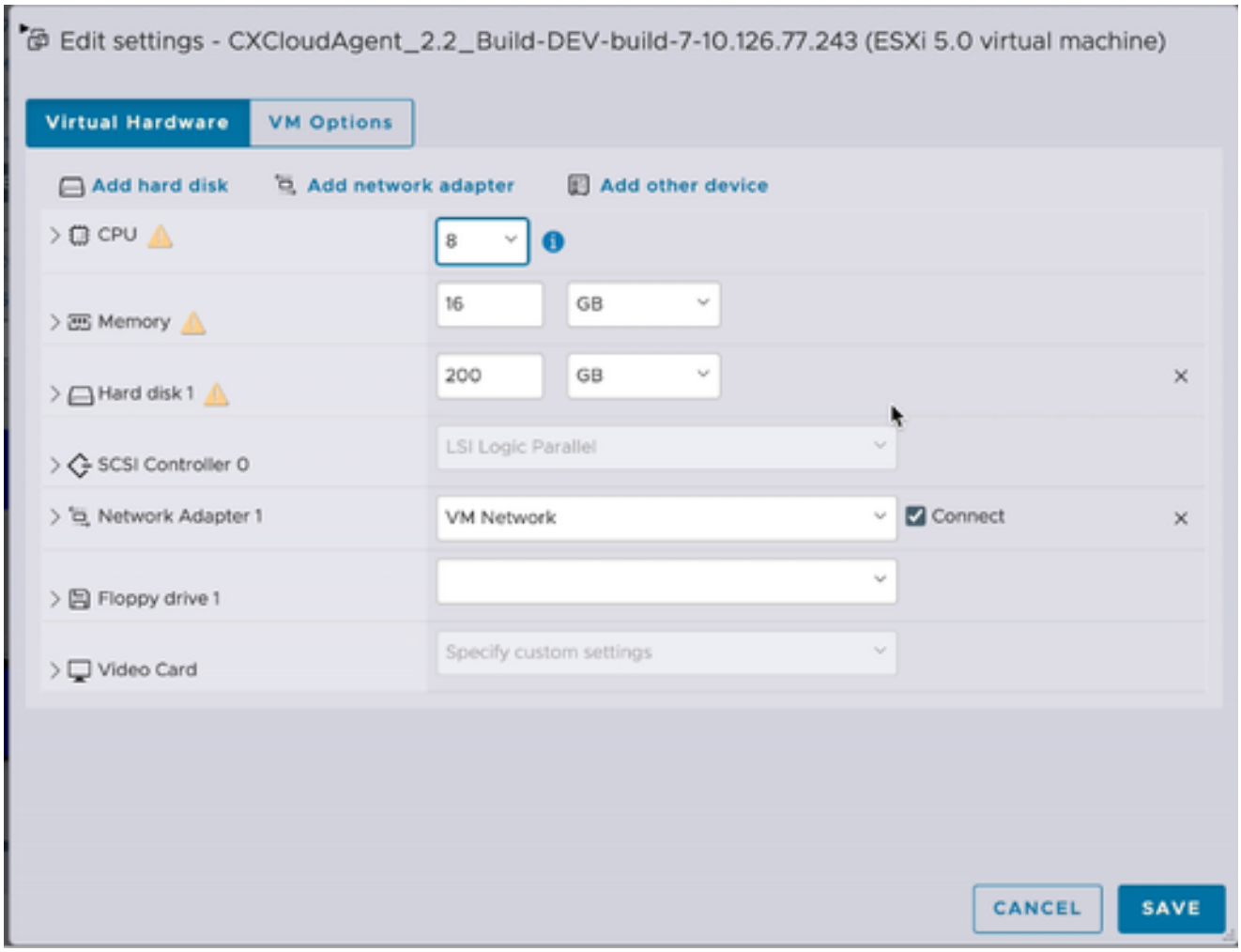


Ziel-VM

4. Klicken Sie auf Aktionen, und wählen Sie Einstellungen bearbeiten aus. Das Fenster Einstellungen bearbeiten wird geöffnet.

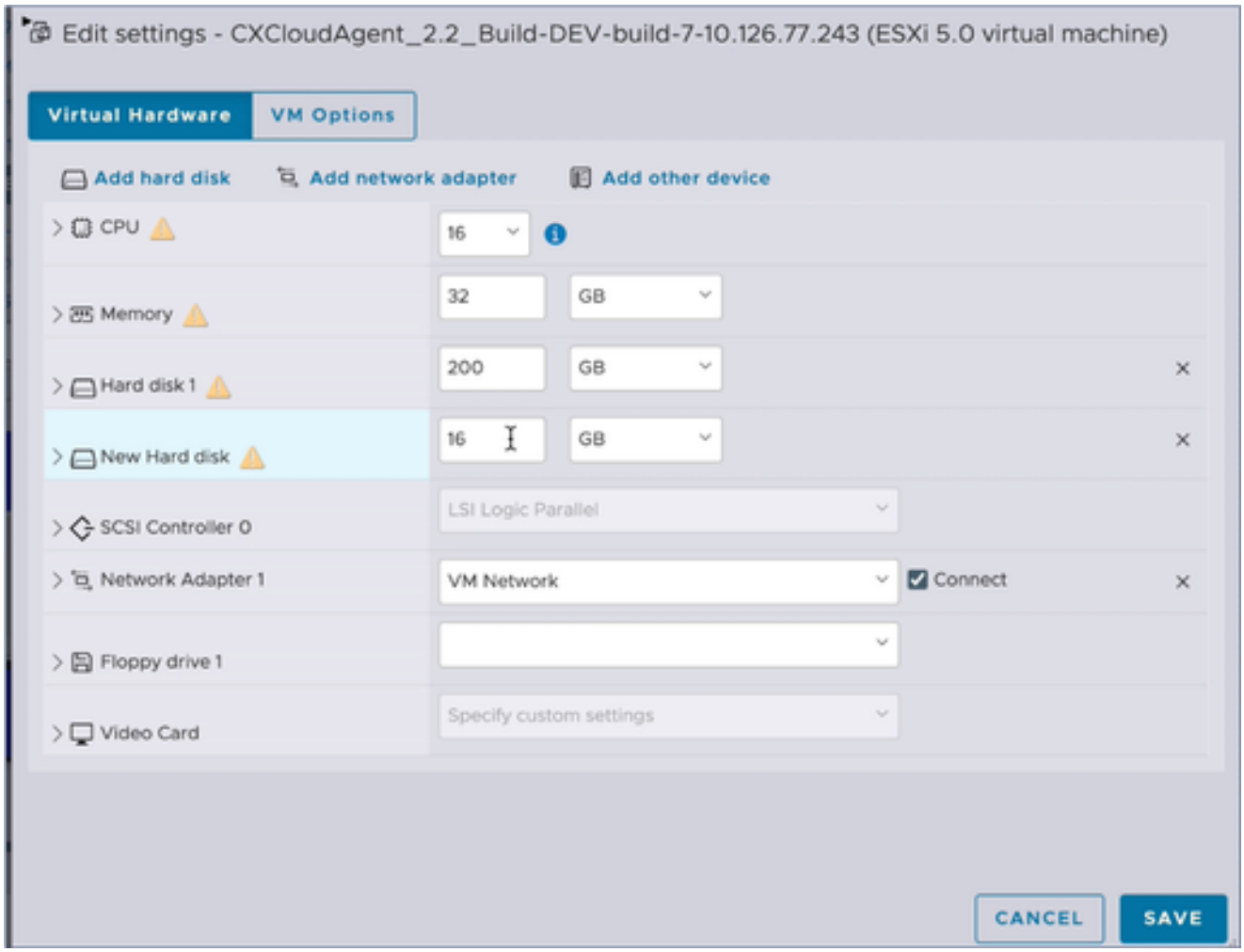


Aktionen



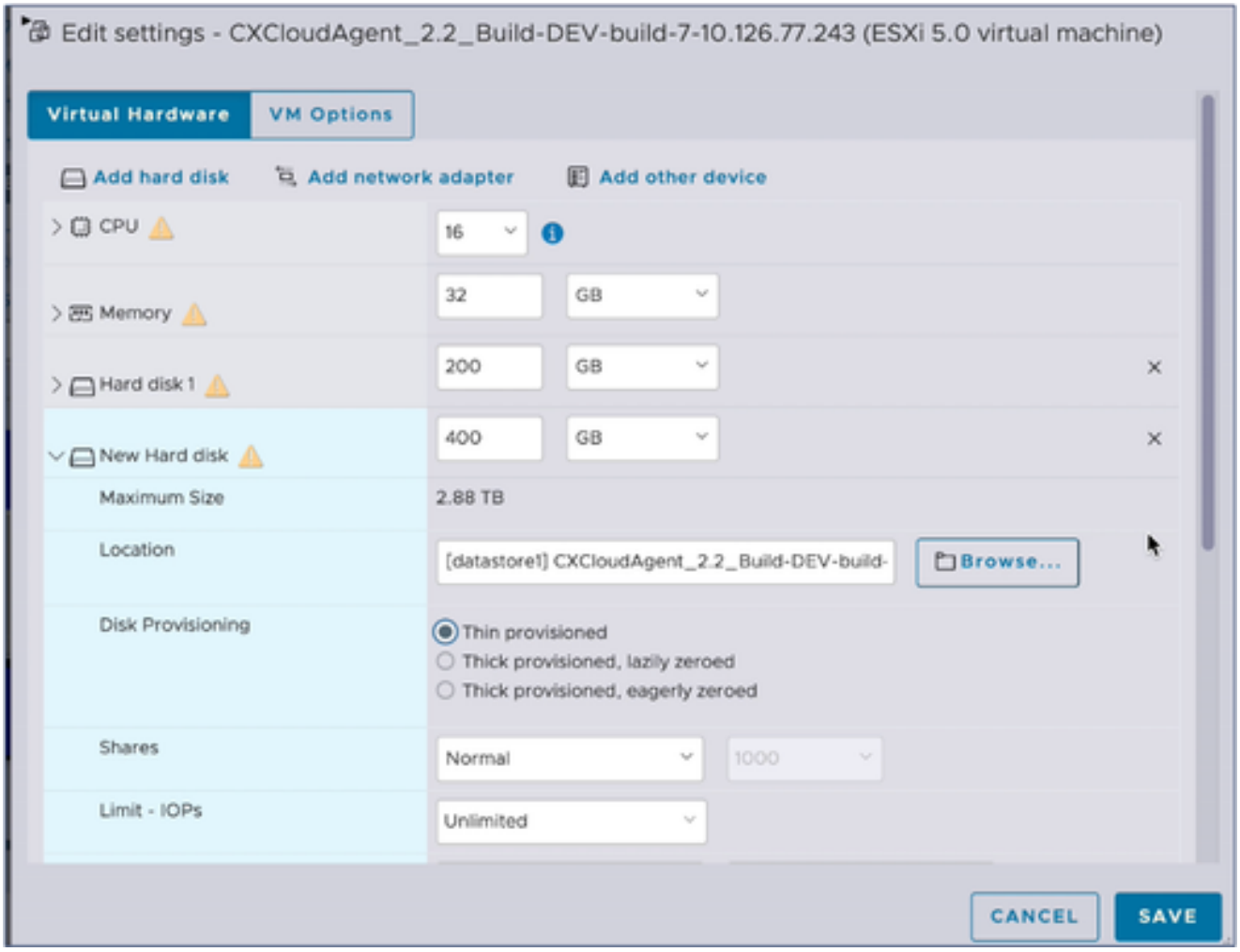
Einstellungen bearbeiten

5. Aktualisieren Sie den CPU-Wert wie angegeben:
   Mittel: 16 Kerne (8 Sockel *2 Kerne/Sockel)
   Groß: 32 Kerne (16 Sockel *2 Kerne/Sockel)
6. Aktualisieren Sie den Wert Arbeitsspeicher wie angegeben:
   Mittel: 32 GB
   Groß: 64 GB
7. Klicken Sie auf Festplatte hinzufügen > Neue Standardfestplatte. Der neue Festplatteneintrag wird im Fenster Einstellungen bearbeiten angezeigt.



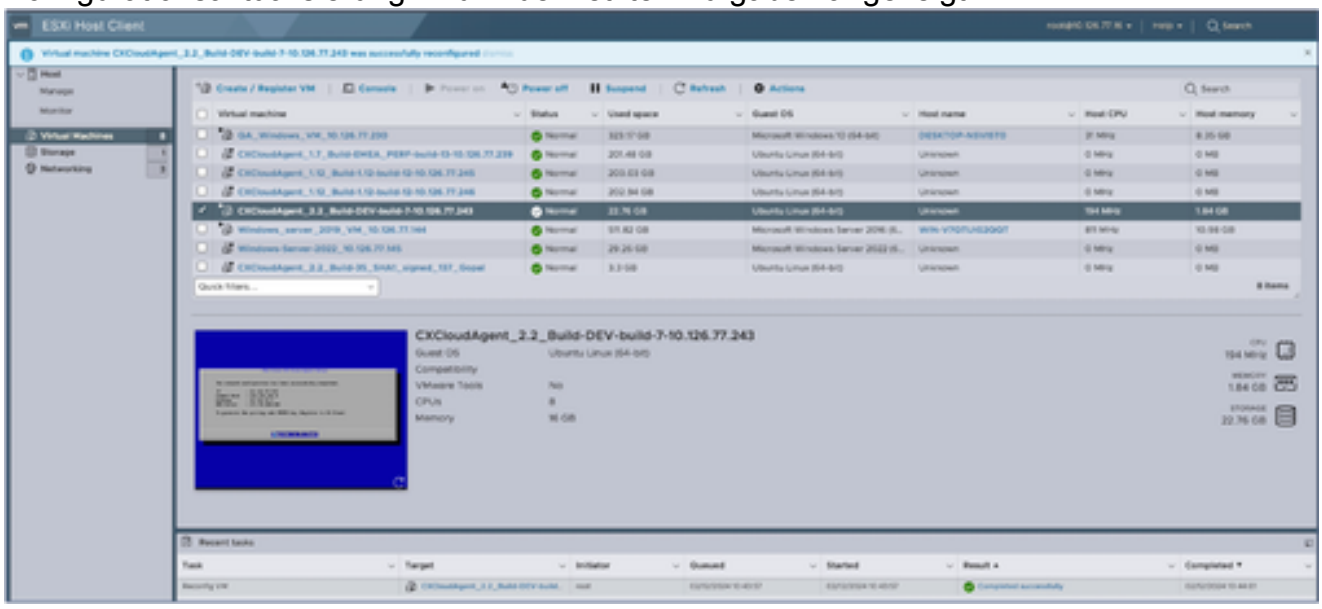
Einstellungen bearbeiten

8. Neue Festplattenwerte wie angegeben aktualisieren:
   Klein bis mittel: 400 GB (Anfangsgröße: 200 GB, Erhöhung der Gesamtkapazität auf 600 GB)
   Klein bis groß: 1.000 GB (Anfangsgröße: 200 GB, Erhöhung der Gesamtkapazität auf 1.200 GB)
9. Klicken Sie auf den Pfeil, um Neue Festplatte zu erweitern. Die Eigenschaften werden angezeigt.



Einstellungen bearbeiten

10. Wählen Sie das Optionsfeld Thin provisioned (Thin bereitgestellt) aus.
11. Klicken Sie auf Speichern, um die Konfiguration abzuschließen. Die Konfigurationsaktualisierung wird in den letzten Aufgaben angezeigt.



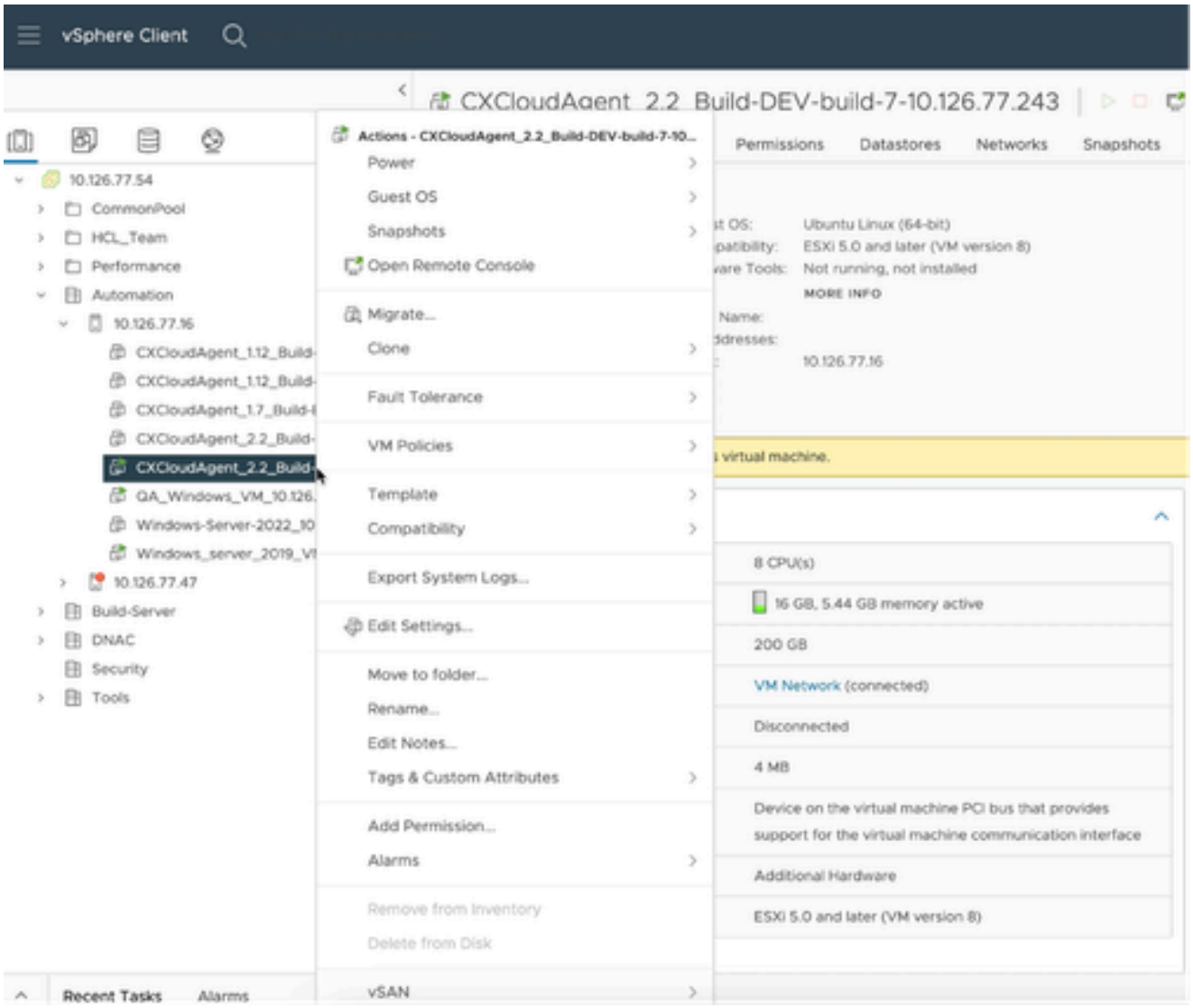
Zuletzt durchgeführte Aufgaben

Neukonfiguration mit Web Client vCenter

So aktualisieren Sie die VM-Konfigurationen mit Web Client vCenter:

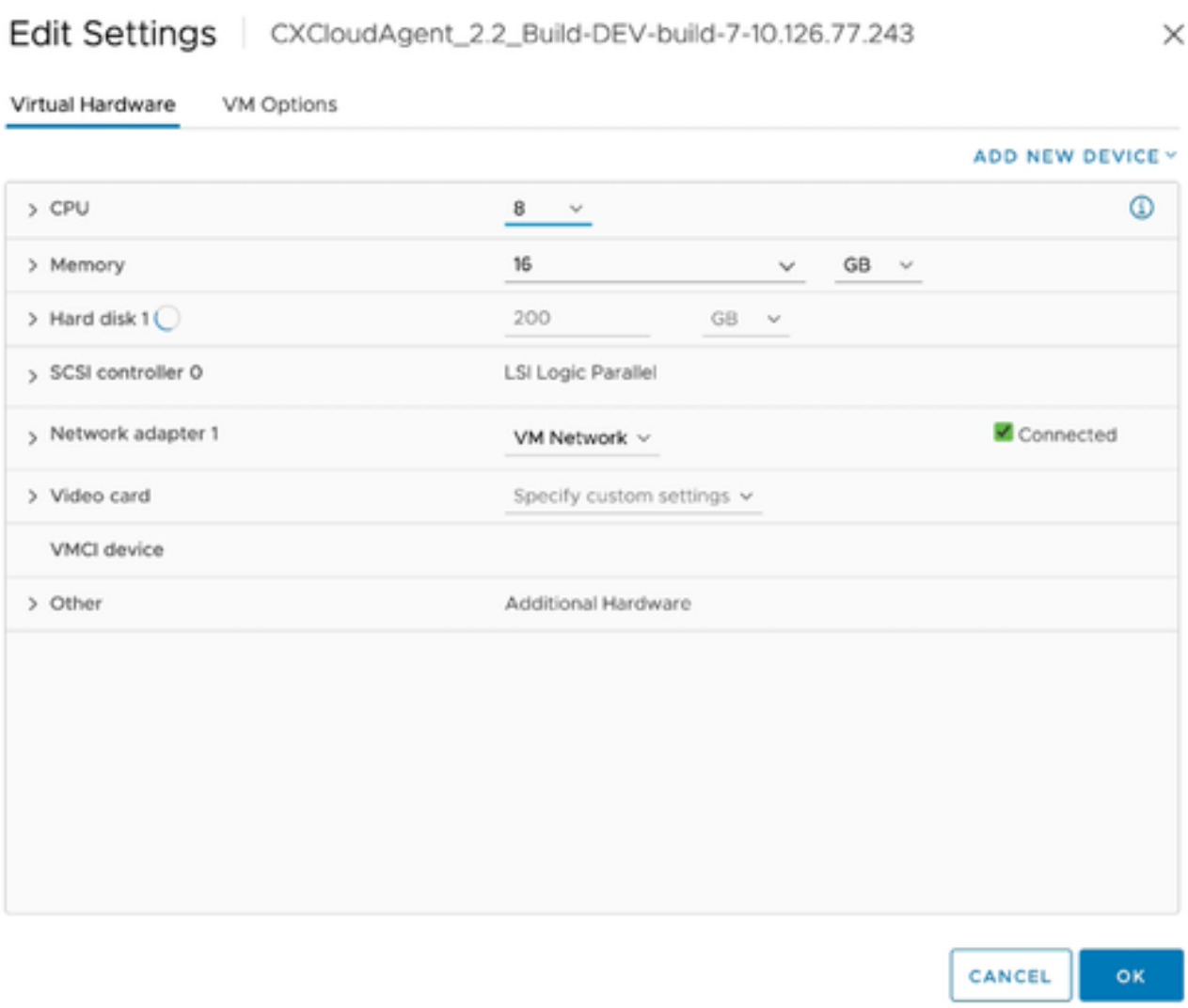
vCenter

1. Melden Sie sich bei vCenter an. Die Startseite wird angezeigt.



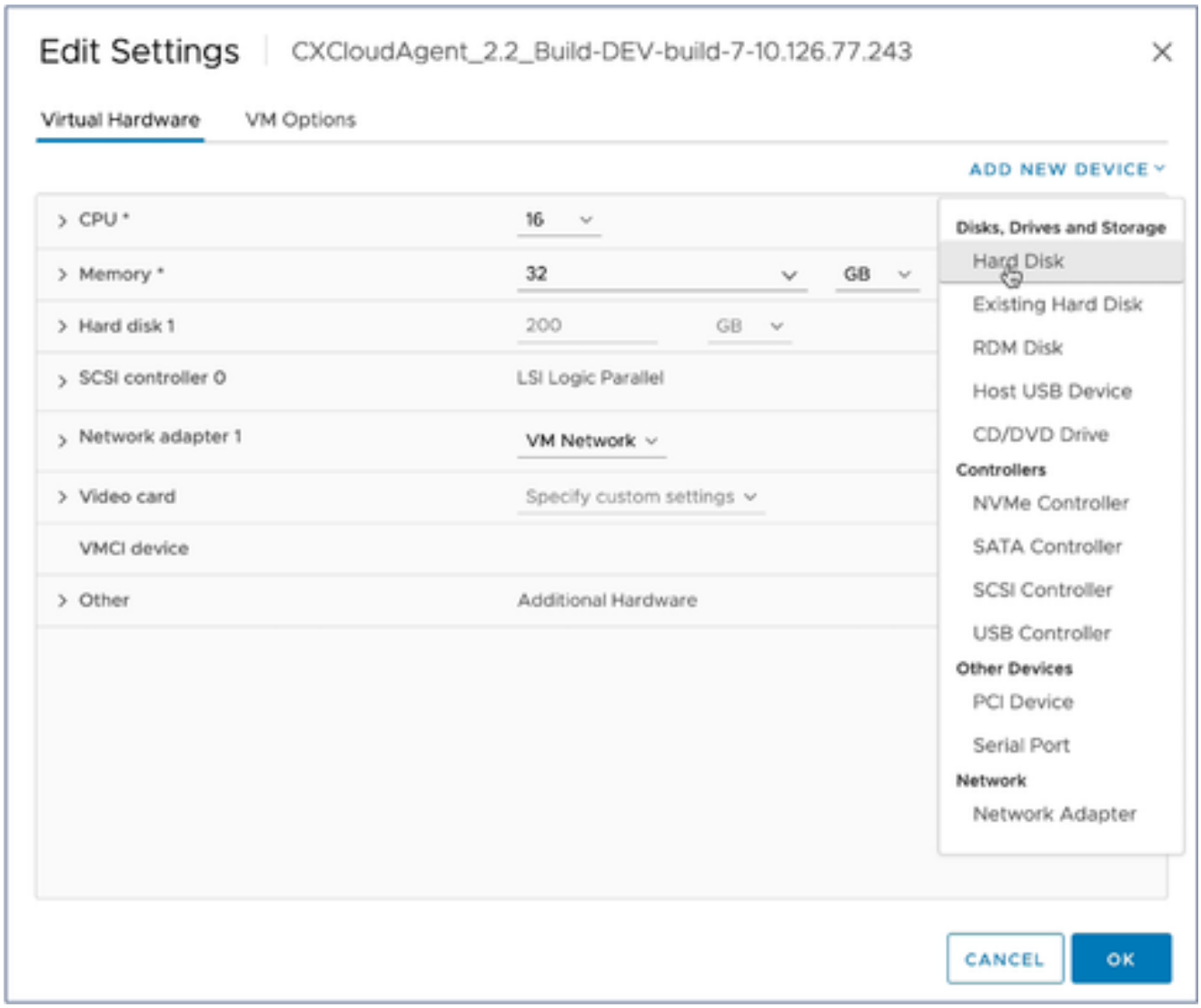
Liste der VMs

2. Klicken Sie mit der rechten Maustaste auf die Ziel-VM, und wählen Sie Edit Settings aus dem Menü aus. Das Fenster Einstellungen bearbeiten wird geöffnet.



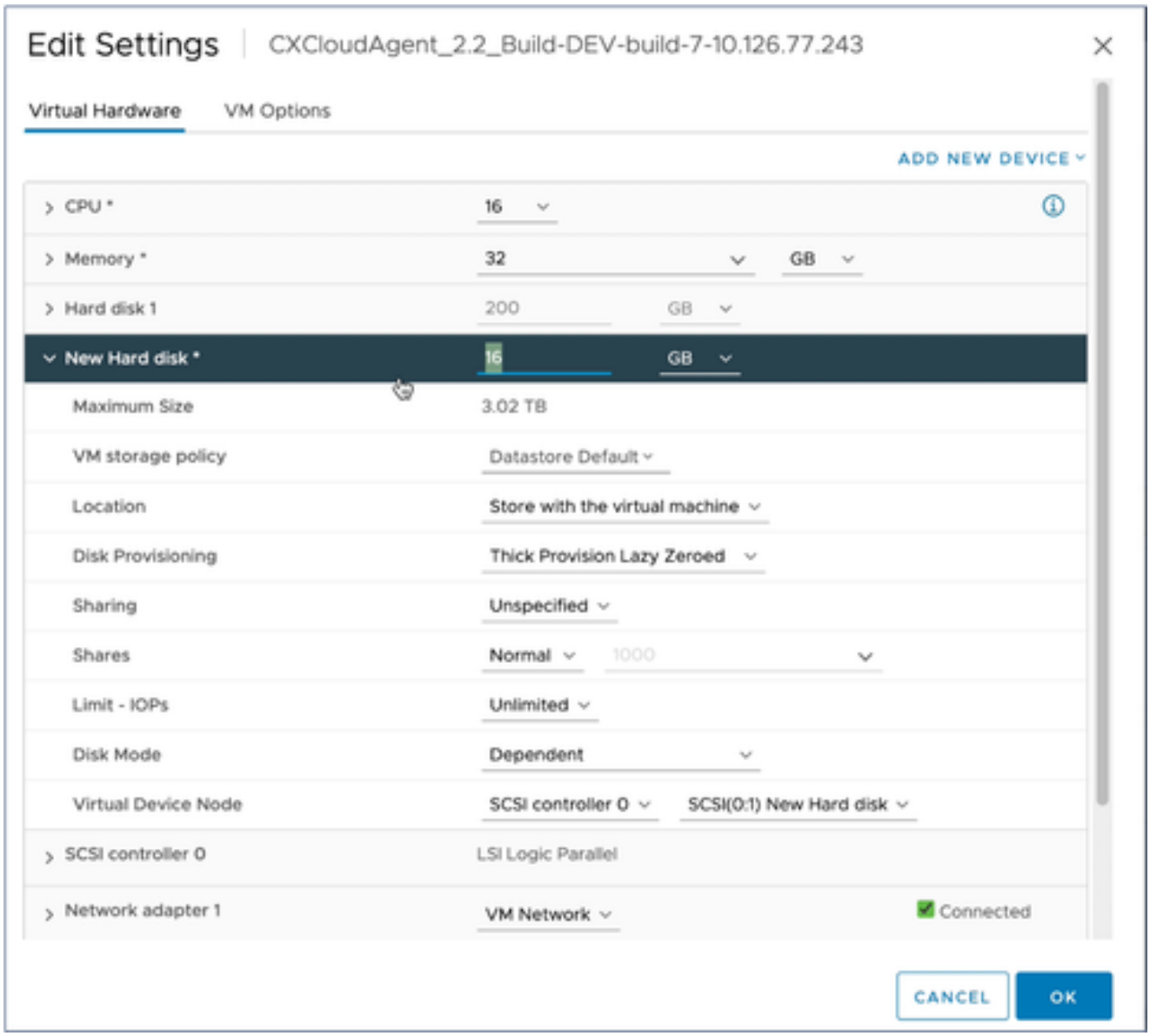
Einstellungen bearbeiten

3. Aktualisieren Sie die CPU-Werte wie angegeben:
   Mittel: 16 Kerne (8 Sockel *2 Kerne/Sockel)
   Groß: 32 Kerne (16 Sockel *2 Kerne/Sockel)
4. Aktualisieren Sie die angegebenen Speicherwerte:
   Mittel: 32 GB
   Groß: 64 GB



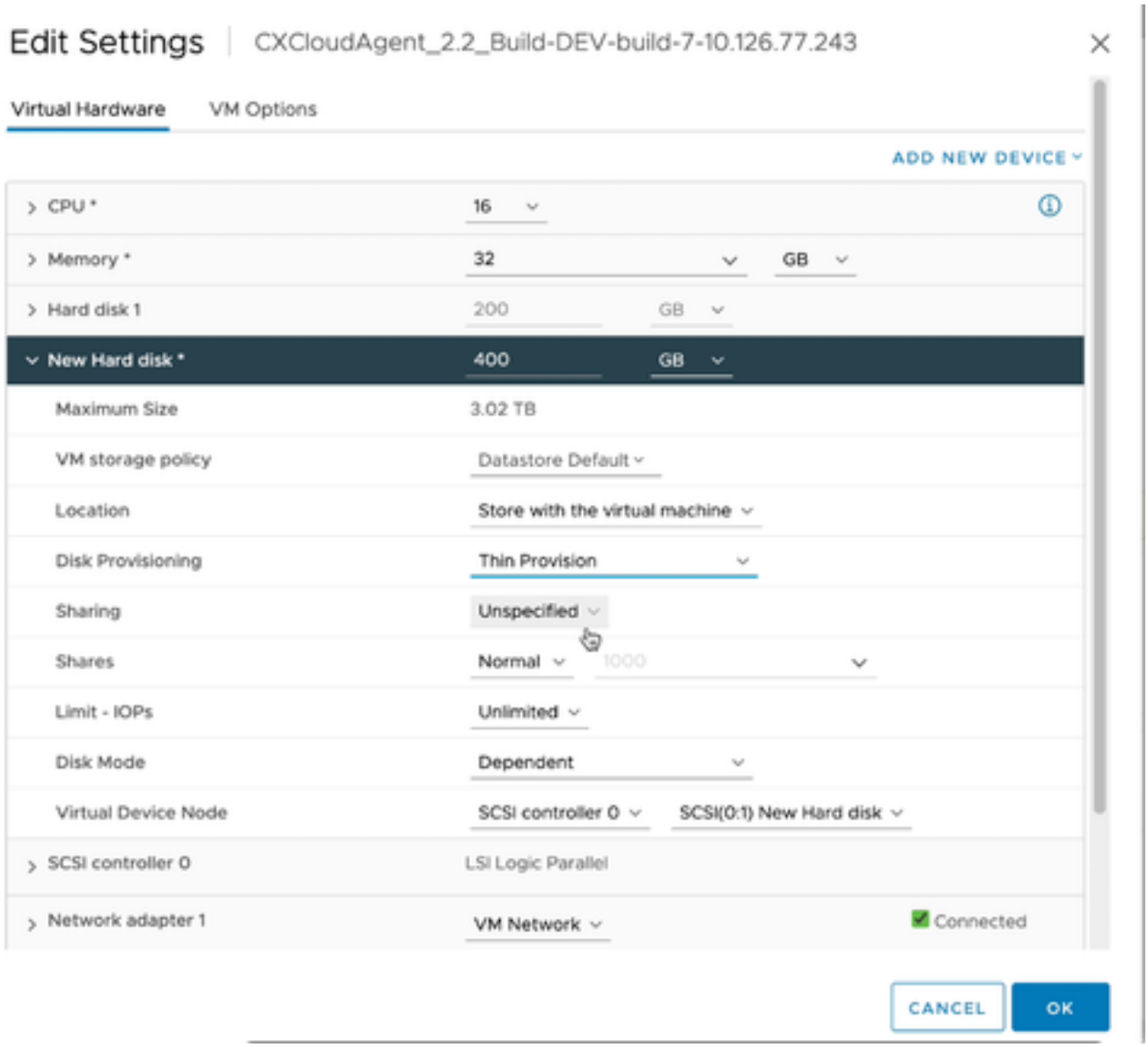
Einstellungen bearbeiten

5. Klicken Sie auf Neues Gerät hinzufügen, und wählen Sie Festplatte aus. Der Eintrag Neue Festplatte wird hinzugefügt.



Einstellungen bearbeiten

6. Neuen Festplattenspeicher aktualisieren wie angegeben:
   Klein bis mittel: 400 GB (Anfangsgröße: 200 GB, Erhöhung der Gesamtkapazität auf 600 GB)
   Klein bis groß: 1.000 GB (Anfangsgröße: 200 GB, Erhöhung der Gesamtkapazität auf 1.200 GB)



Einstellungen bearbeiten

7. Wählen Sie Thin Provision aus der Dropdown-Liste Disk Provisioning aus.
8. Klicken Sie auf OK, um die Aktualisierung abzuschließen.

Bereitstellung und Netzwerkkonfiguration

Wählen Sie eine der folgenden Optionen aus, um den CX Cloud Agent bereitzustellen:

- Zur Auswahl von VMware vSphere/vCenter Thick Client ESXi 5.5/6.0 gehen Sie zu Thick Client
- Zur Auswahl von VMware vSphere/vCenter Web Client ESXi 6.0 wechseln Sie zu Web Client oder vSphere Center
- Um Oracle Virtual Box 5.2.30 auszuwählen, gehen Sie zu Oracle VM
- Um Microsoft Hyper-V auszuwählen, gehen Sie zu Hyper-V.

OVA-Bereitstellung

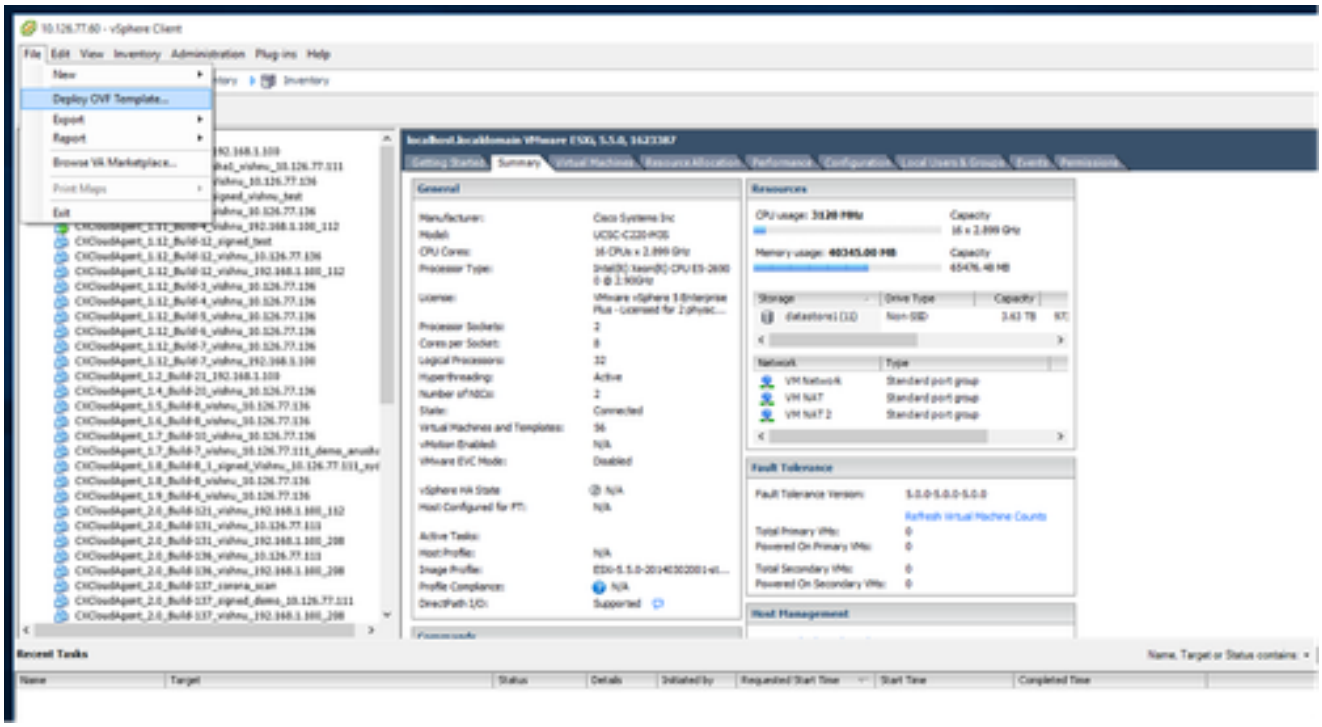
Installation von Thick Client ESXi 5.5/6.0

Dieser Client ermöglicht die Bereitstellung von CX Cloud Agent OVA mithilfe des vSphere-Thick-Clients.

1. Starten Sie nach dem Herunterladen des Images den VMware vSphere Client, und melden Sie sich an.

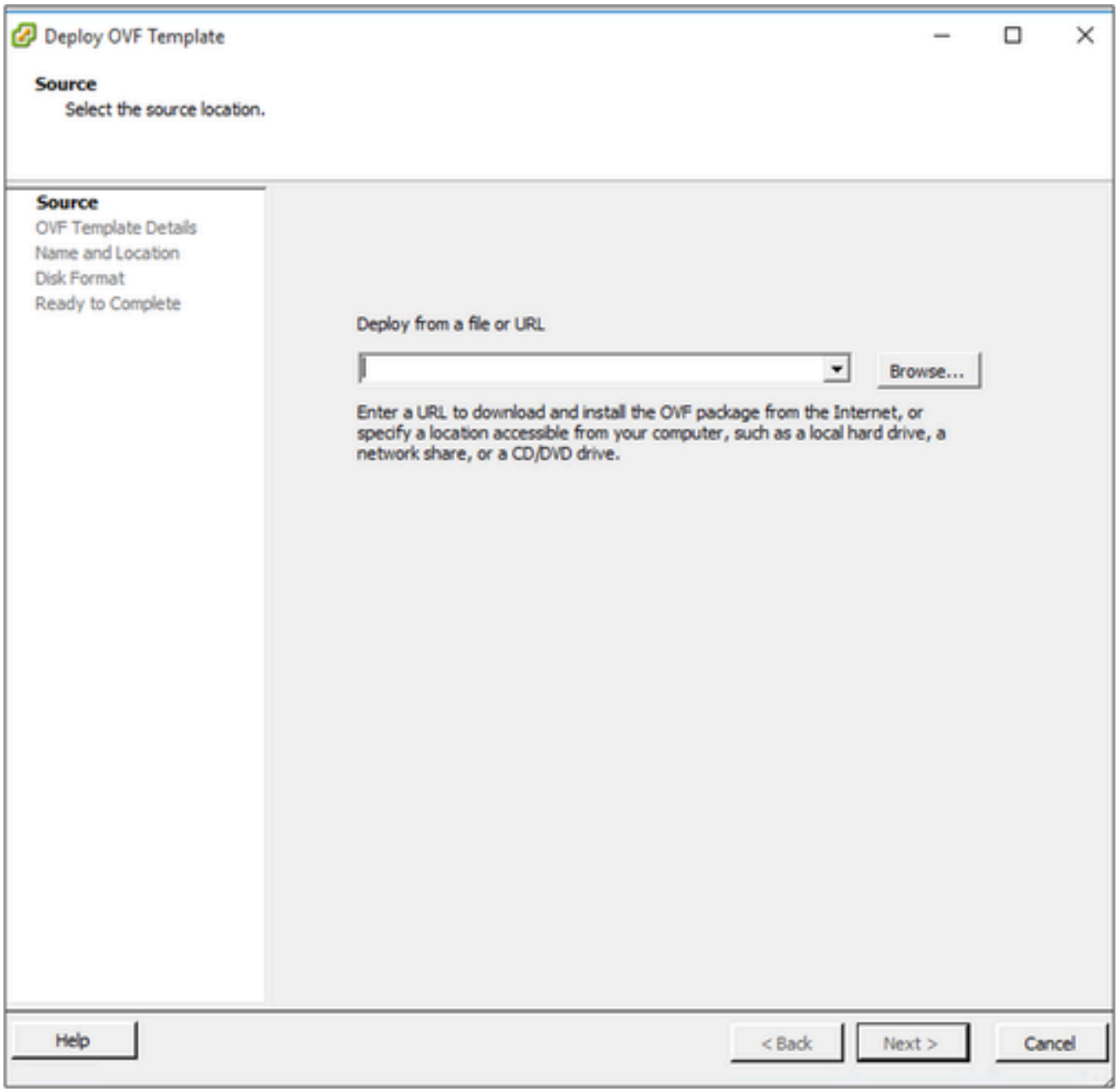
Anmelden

2. Wählen Sie im Menü Datei > OVF-Vorlage bereitstellen aus.



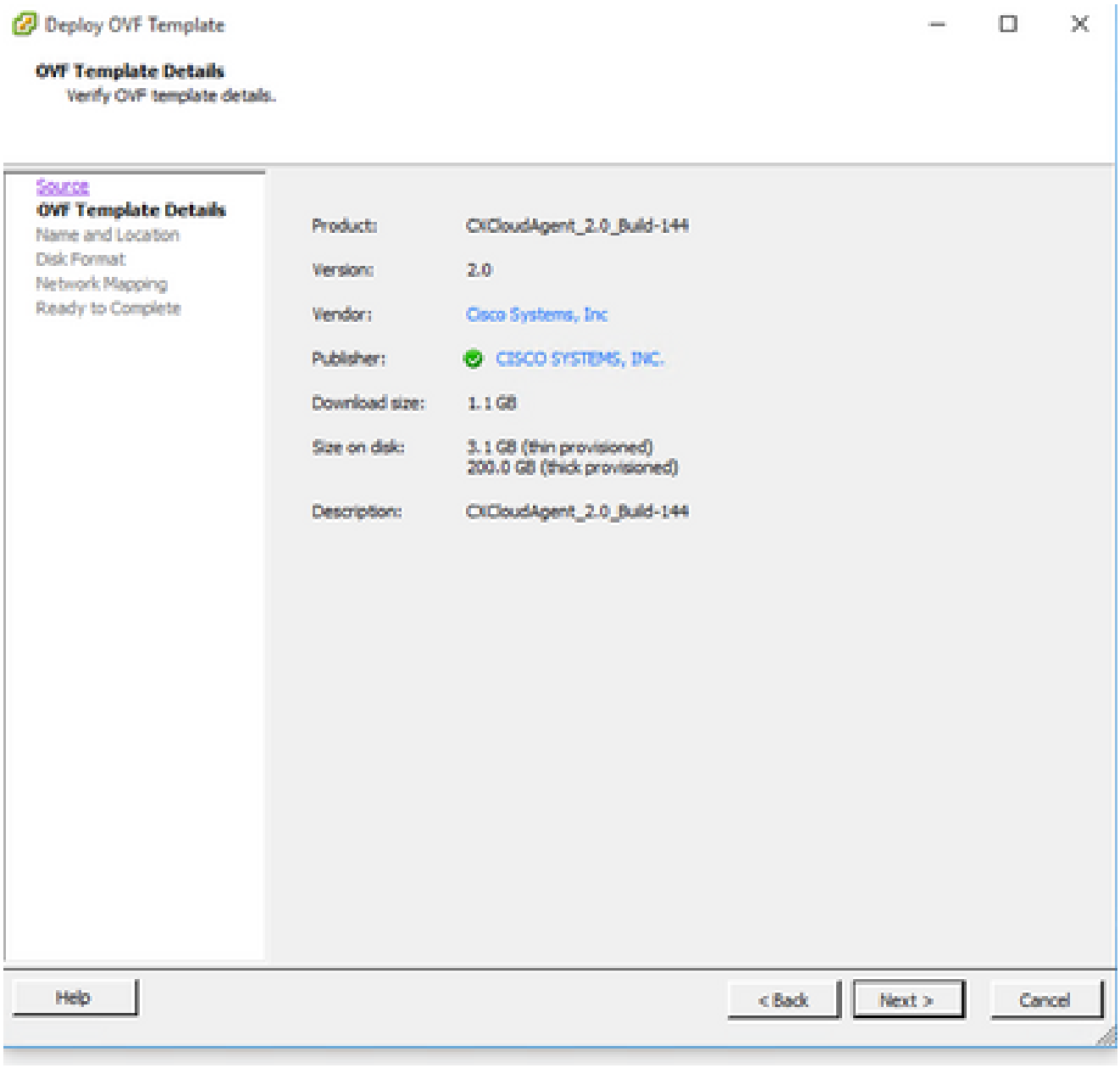
vSphere-Client

3. Wählen Sie die OVA-Datei aus, und klicken Sie auf Weiter.



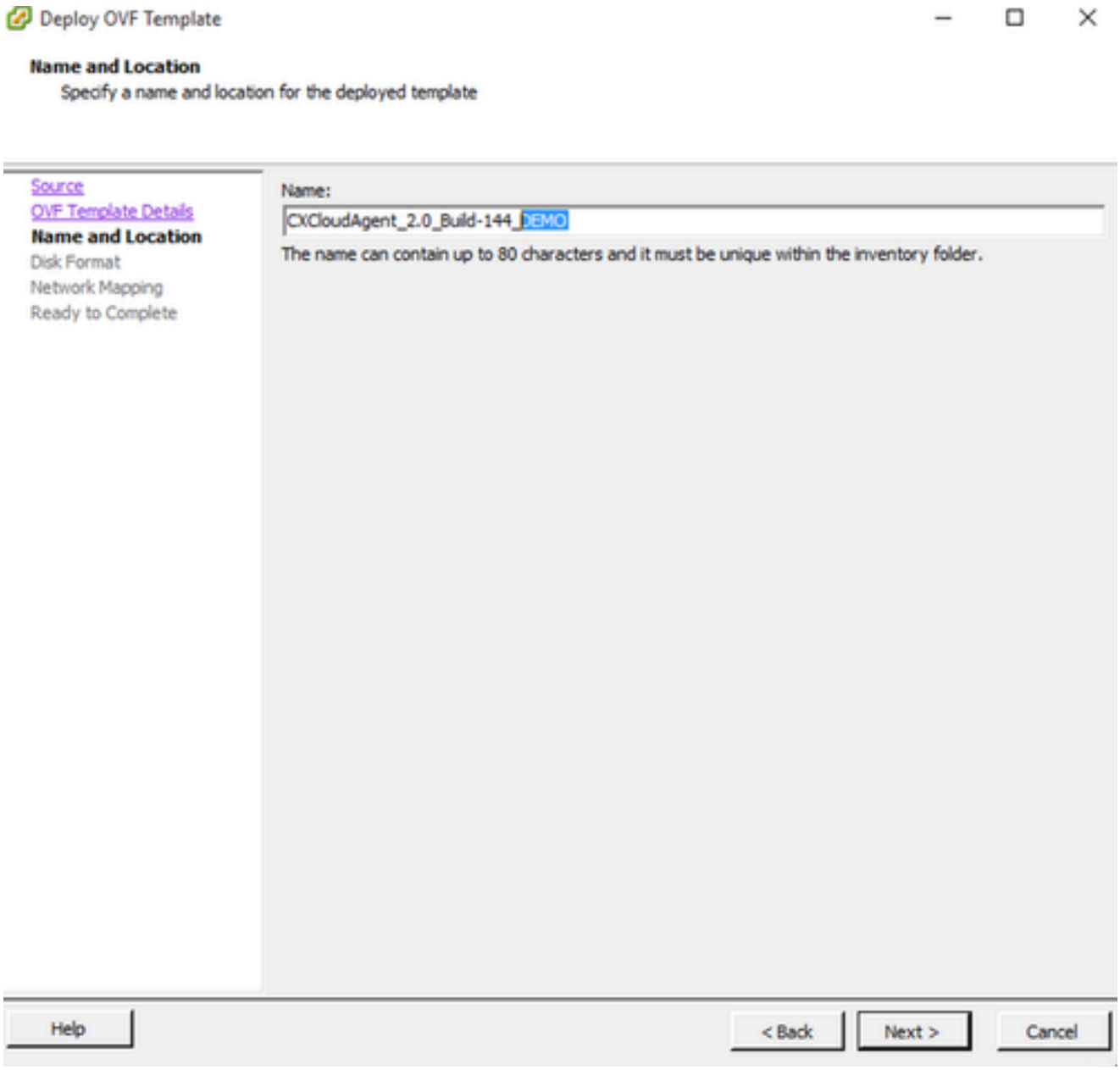
OVA-Pfad

4. Überprüfen Sie die OVF-Details, und klicken Sie auf Weiter.



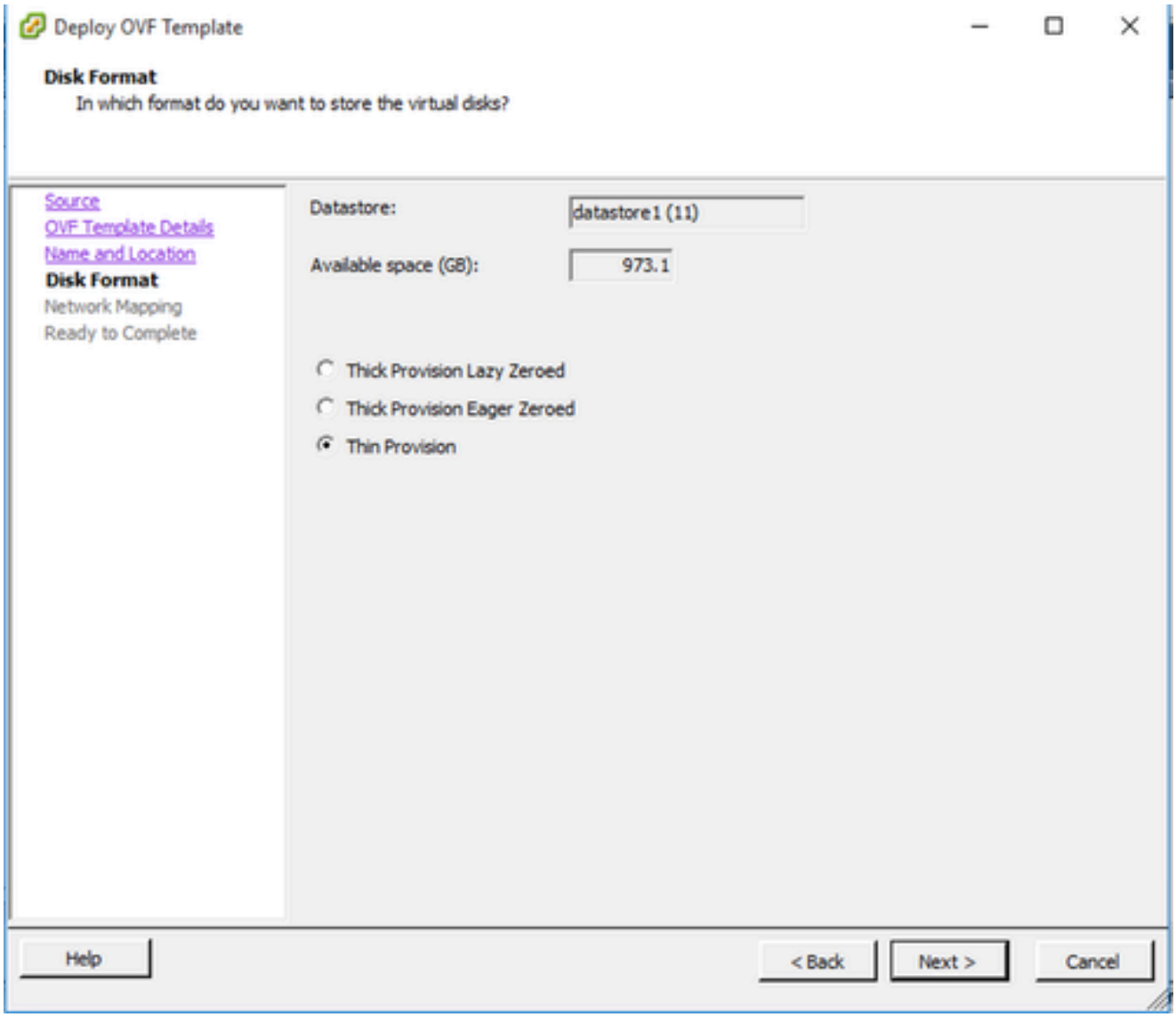
Vorlagendetails

5. Geben Sie einen eindeutigen Namen ein, und klicken Sie auf Weiter.



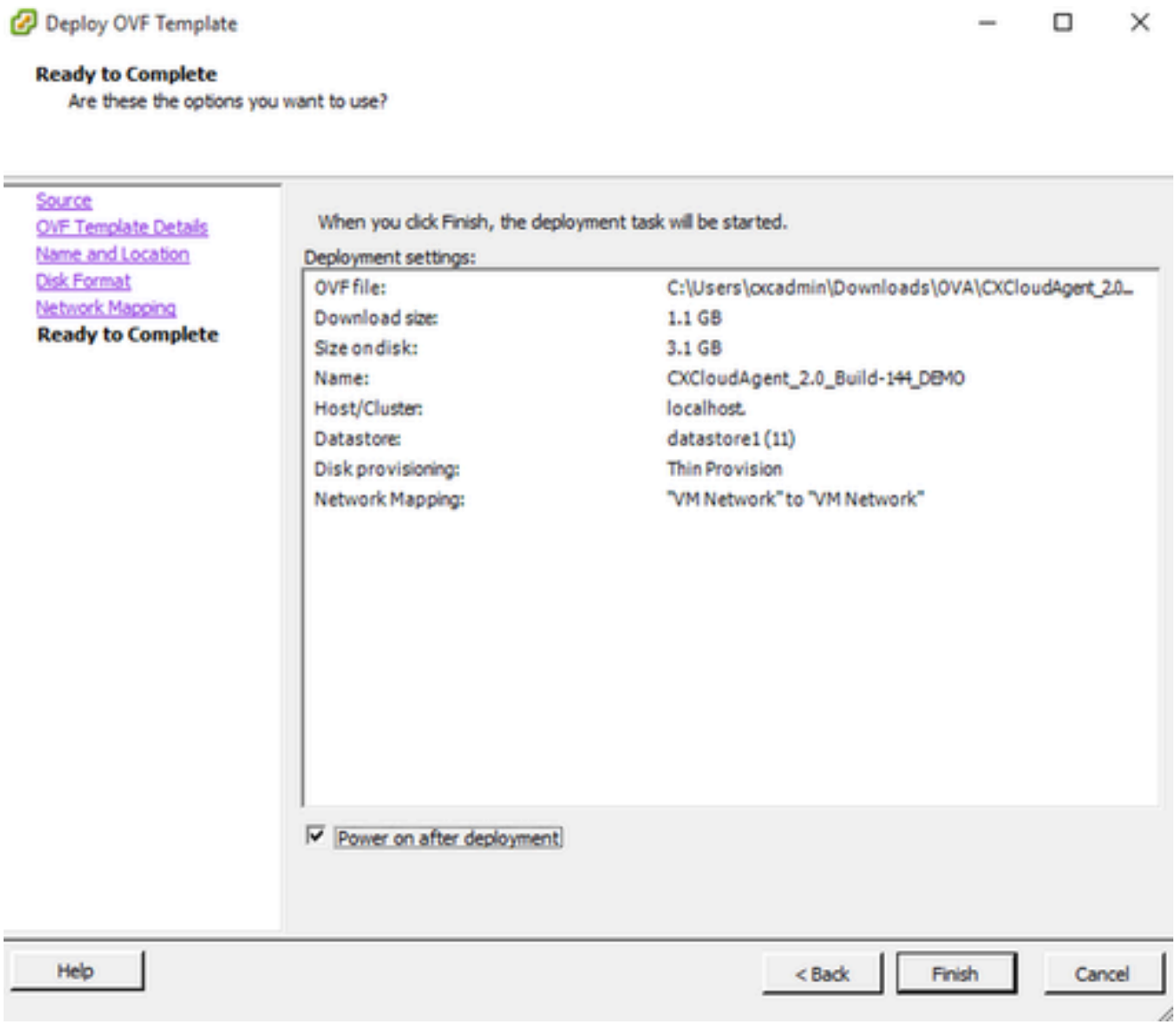
Name und Standort

6. Wählen Sie ein Festplattenformat aus, und klicken Sie auf Weiter (Thin Provision wird empfohlen).



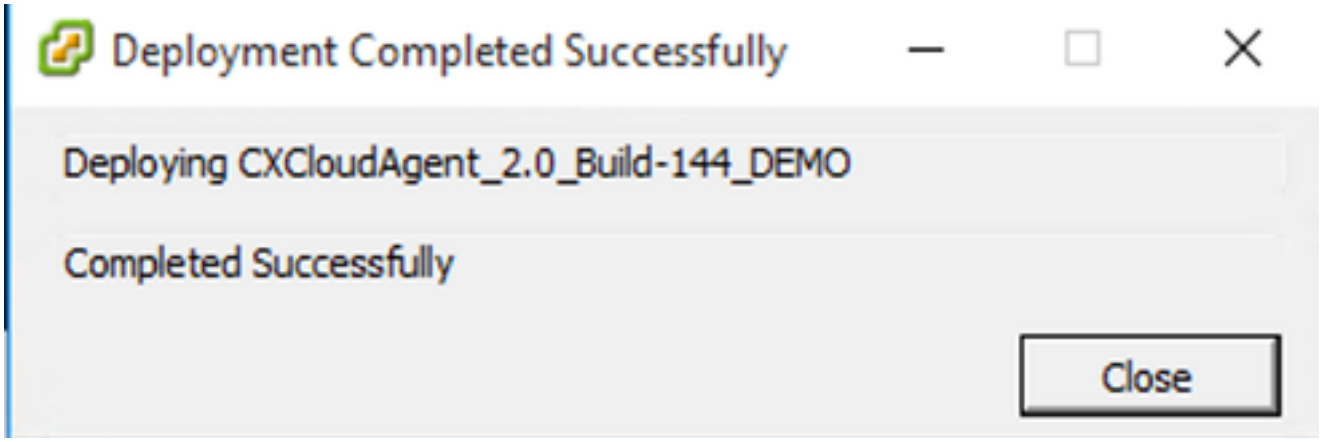
Datenträgerformatierung

7. Aktivieren Sie das Kontrollkästchen Nach Bereitstellung einschalten, und klicken Sie auf Schließen.



Bereit zur Fertigstellung

Die Bereitstellung kann einige Minuten dauern. Nach erfolgreicher Bereitstellung wird eine Bestätigung angezeigt.



Bereitstellung abgeschlossen

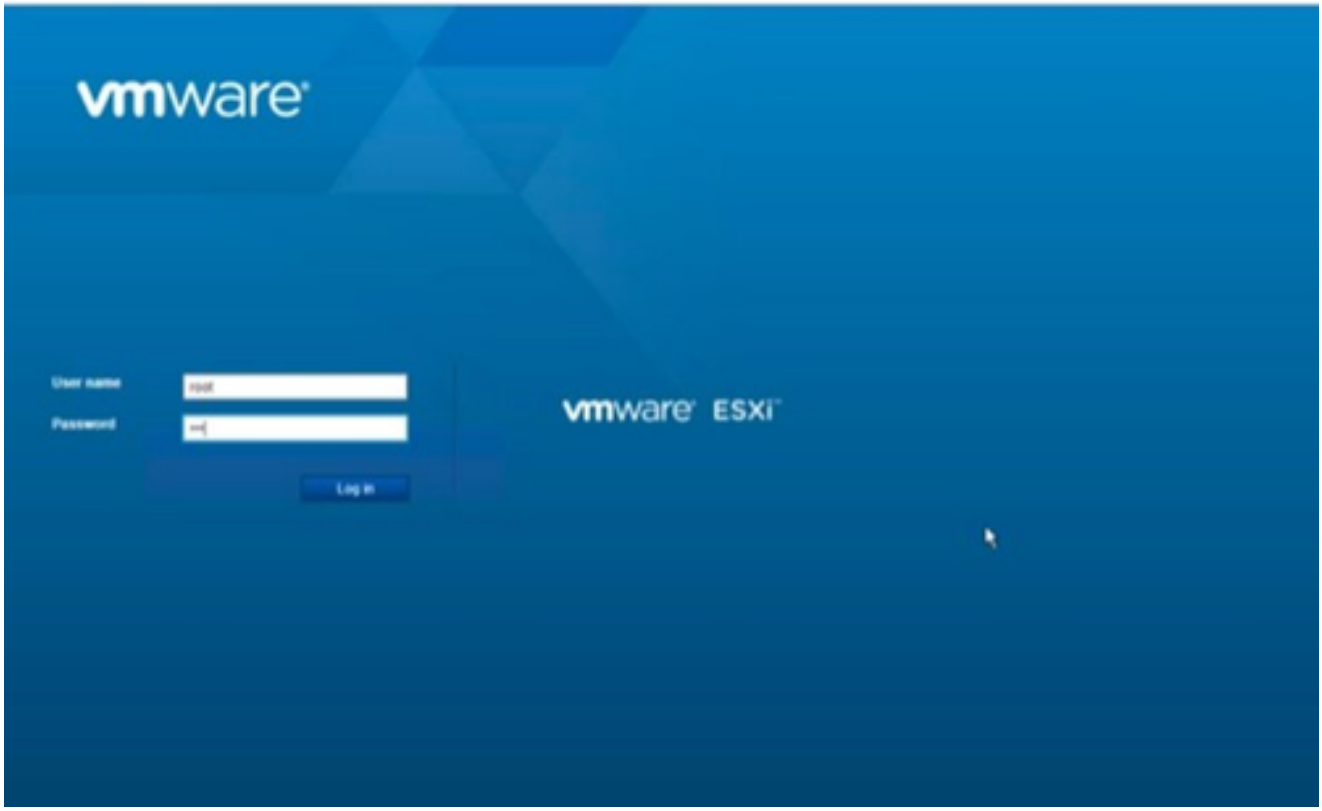
8. Wählen Sie das bereitgestellte virtuelle System aus, öffnen Sie die Konsole, und gehen Sie

zu Network Configuration, um mit den nächsten Schritten fortzufahren.

Installation von Web Client ESXi 6.0

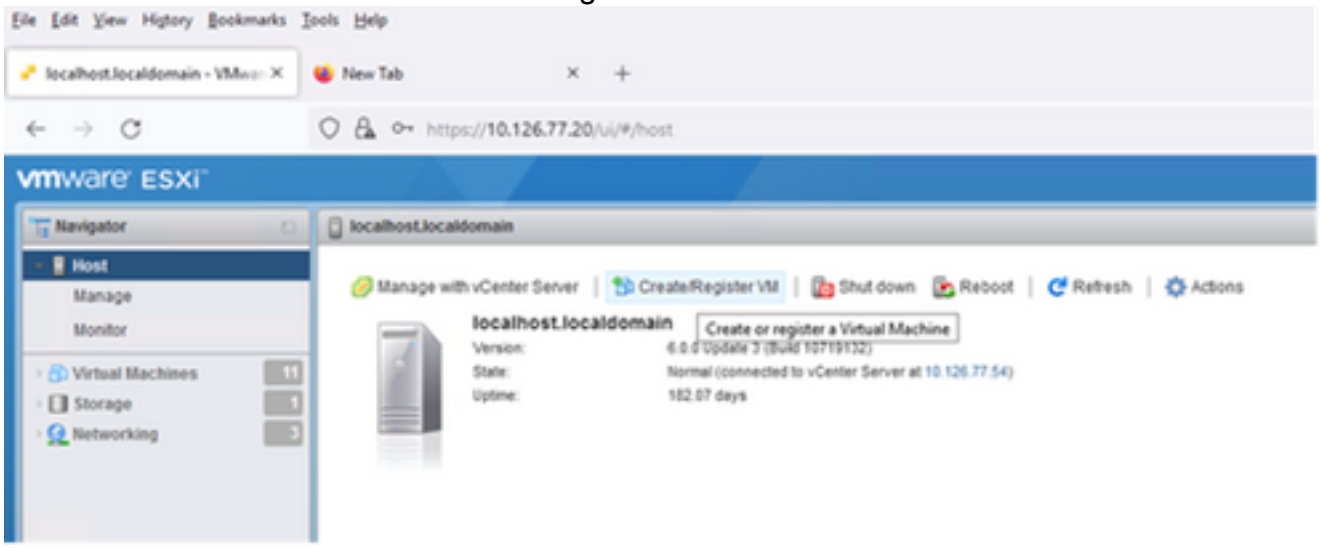
Dieser Client stellt CX Cloud Agent OVA mithilfe von vSphere Web bereit.

1. Melden Sie sich mit den ESXi/Hypervisor-Anmeldeinformationen für die Bereitstellung von VM in der VMWare-Benutzeroberfläche an.



VMware ESXi-Anmeldung

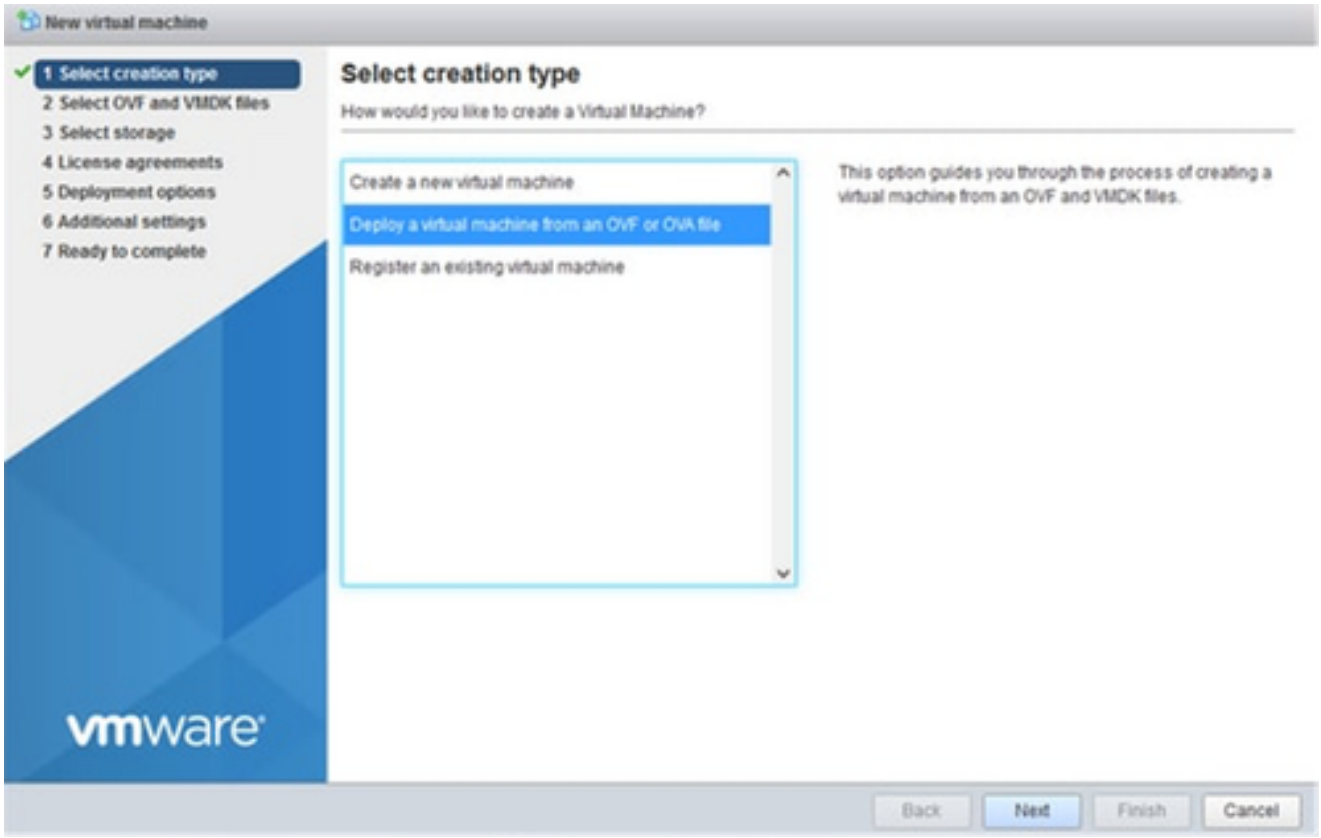
2. Wählen Sie Virtual Machine > Create/Register VM aus.



VM erstellen

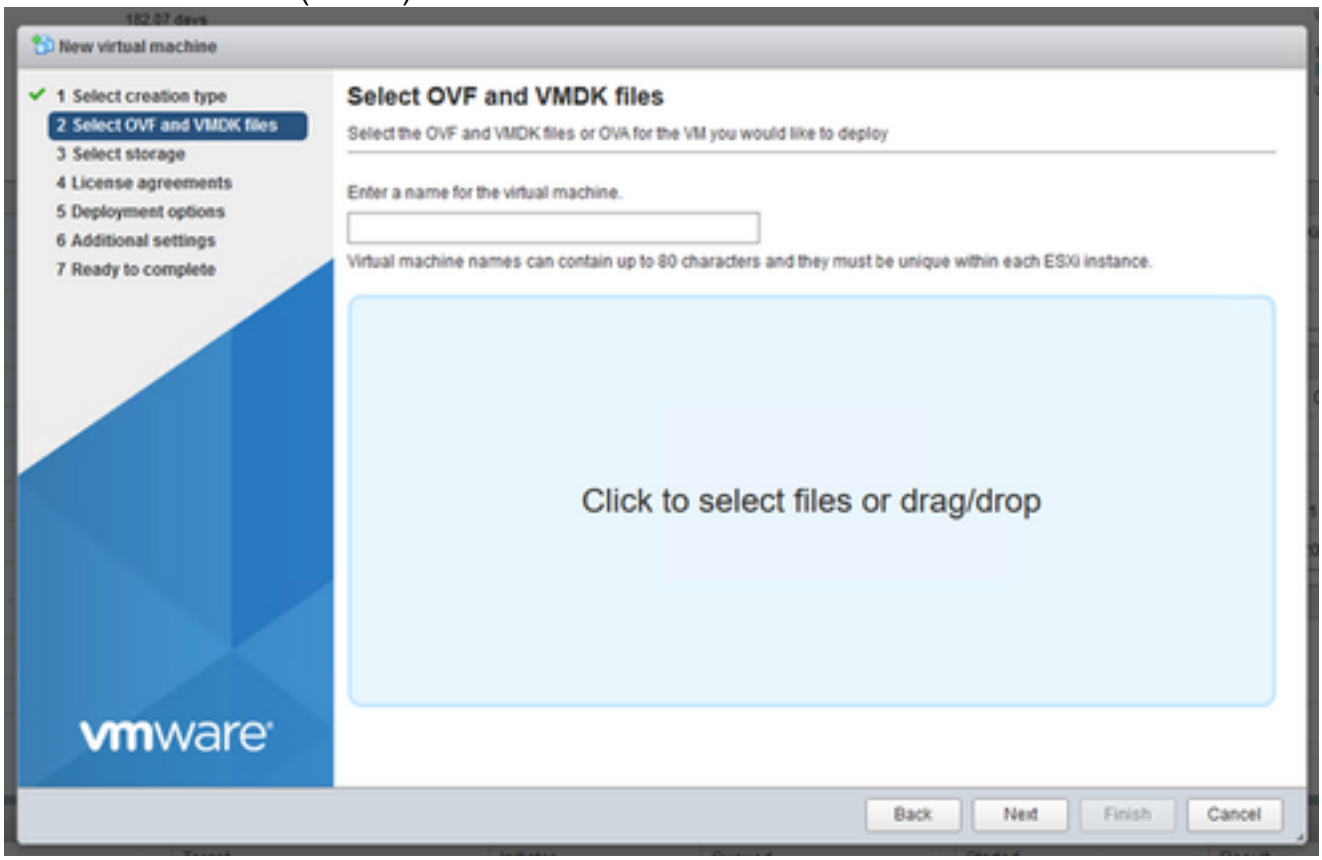
3. Wählen Sie Virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen aus und klicken

Sie auf Weiter.



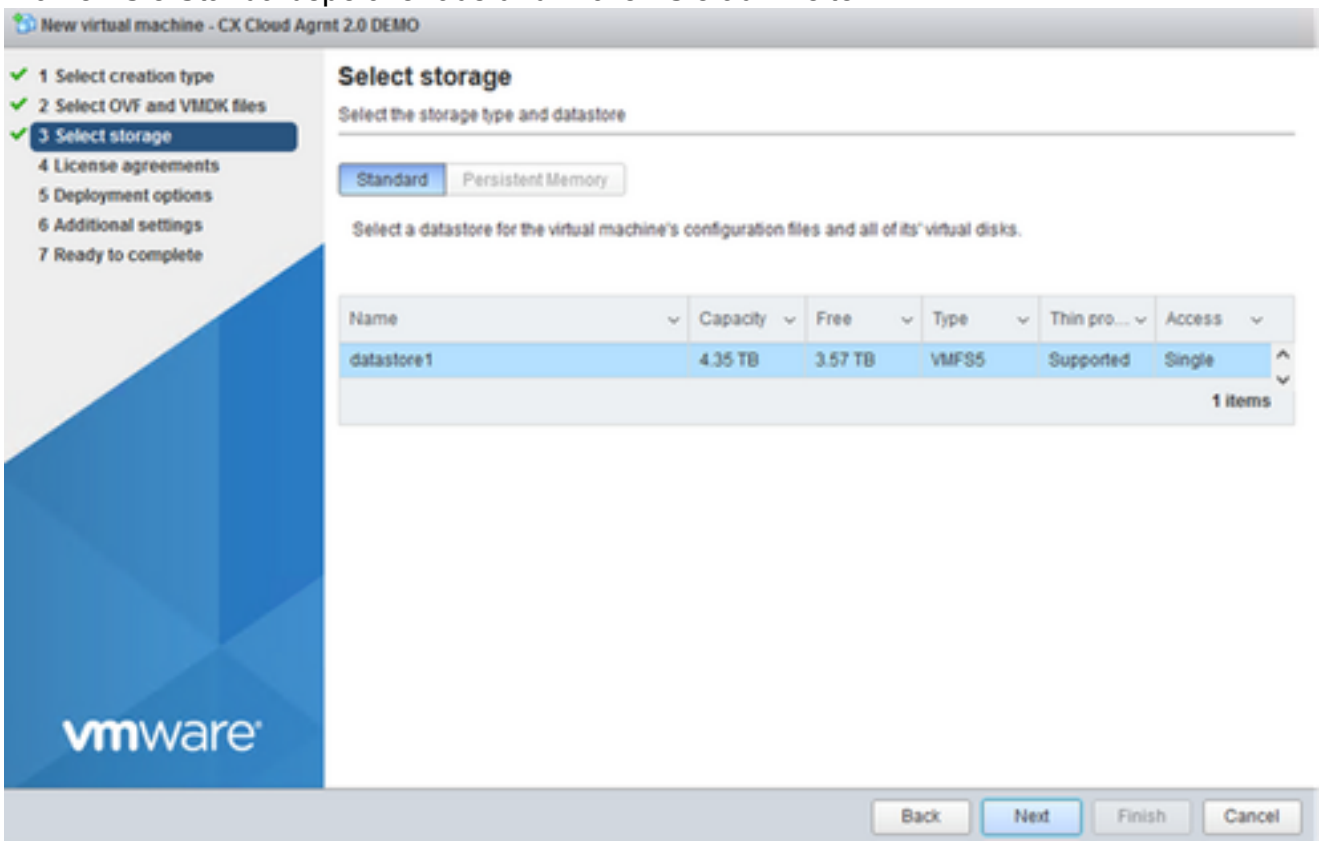
Erstellungstyp auswählen

4. Geben Sie den Namen des virtuellen Systems ein, wählen Sie die Datei aus, oder ziehen Sie die heruntergeladene OVA-Datei per Drag-and-Drop.
5. Klicken Sie auf Next (Weiter).



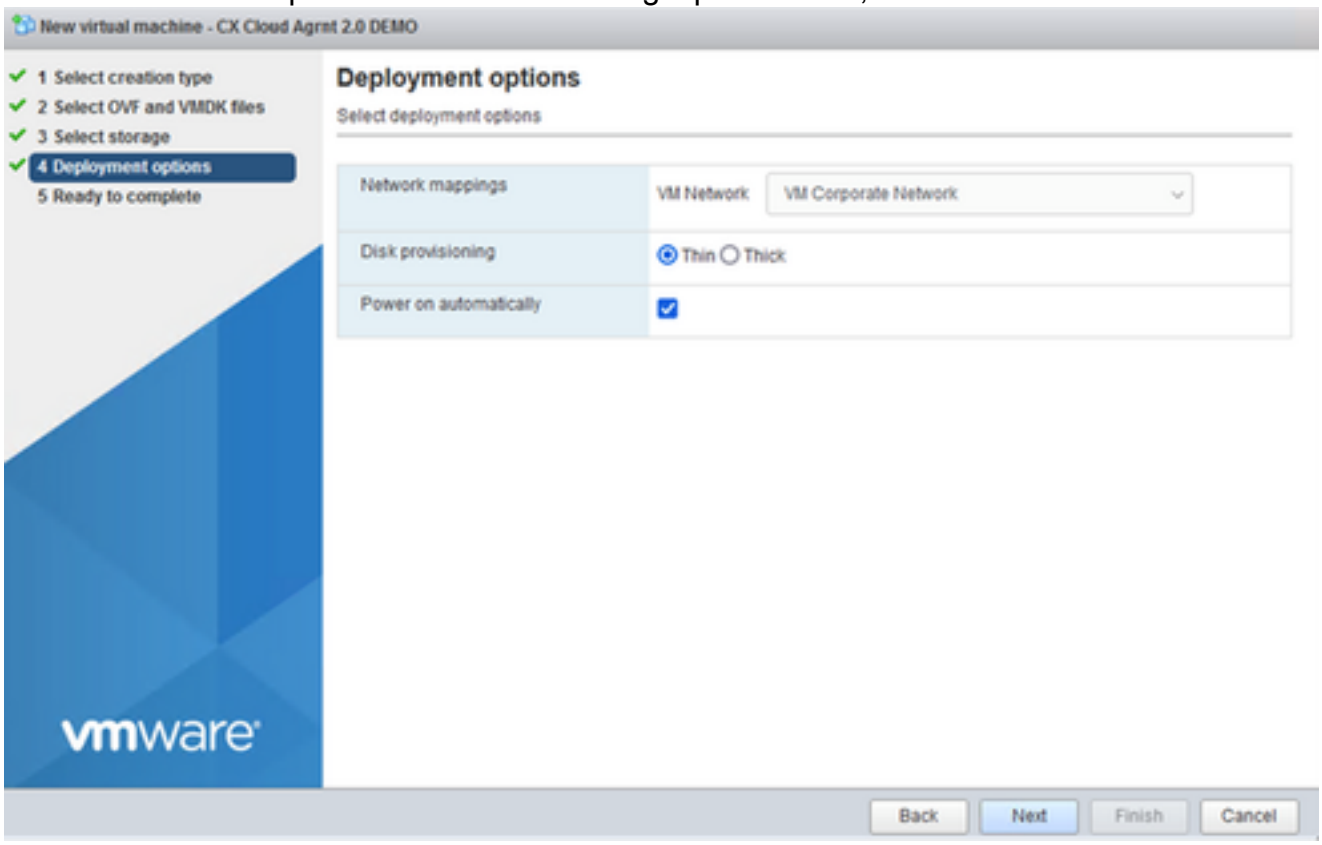
OVA-Auswahl

6. Wählen Sie Standardspeicher aus und klicken Sie auf Weiter.



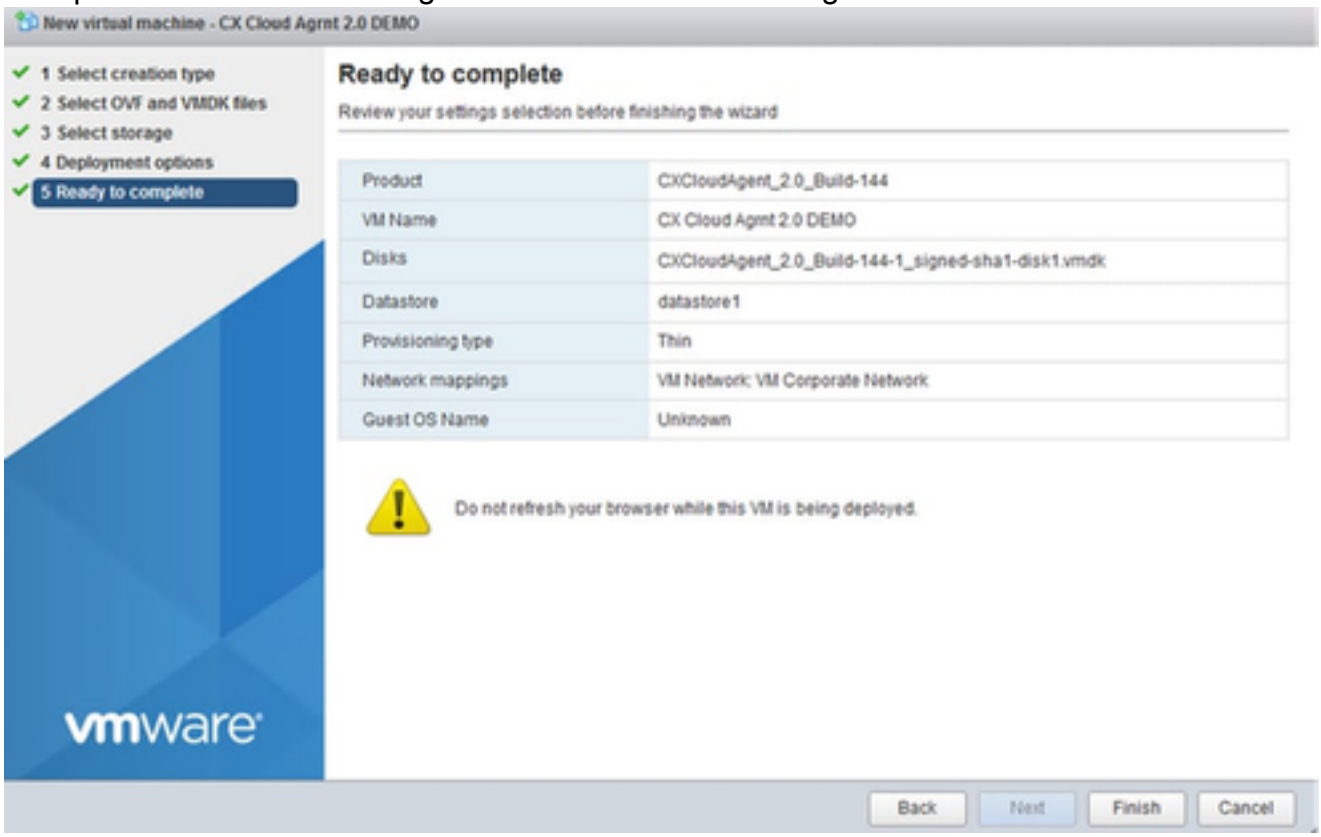
Auswahl von externem Speicher

7. Wählen Sie die entsprechenden Bereitstellungsoptionen aus, und klicken Sie auf Weiter.

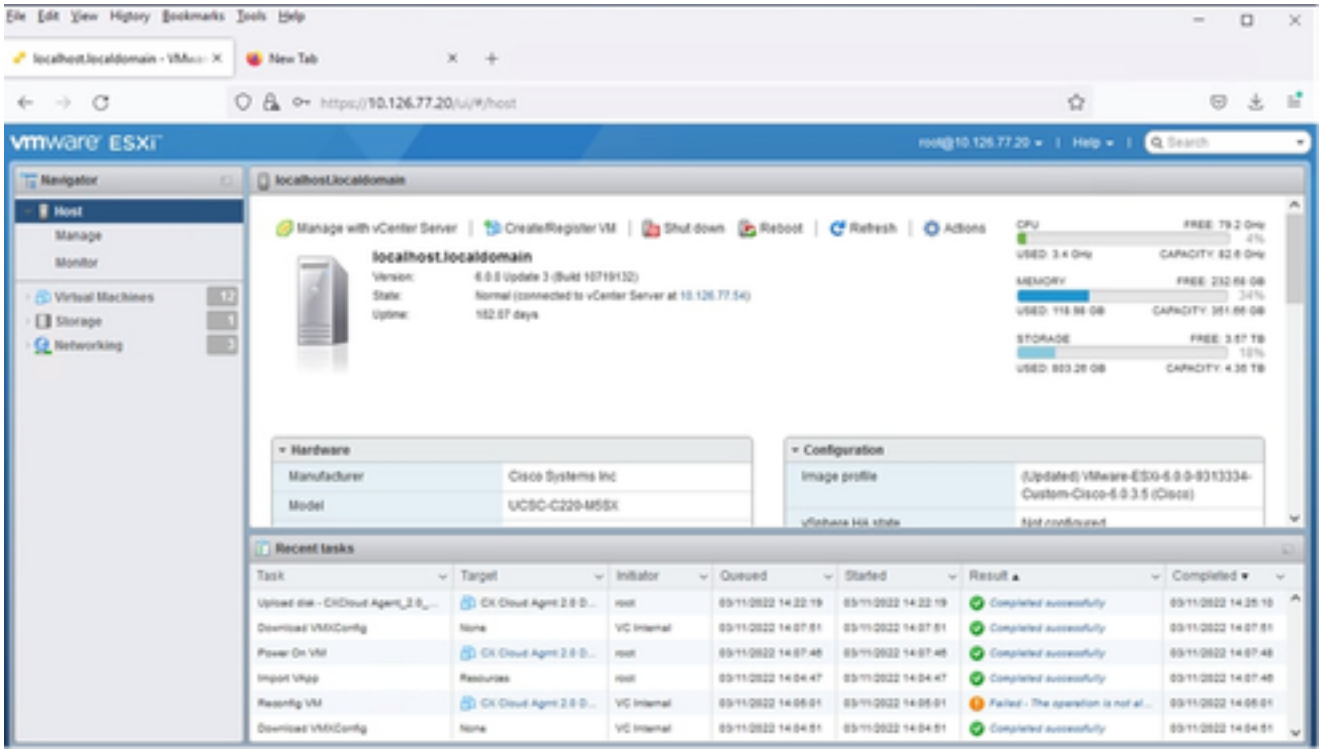


Bereitstellungsoptionen

8. Überprüfen Sie die Einstellungen und klicken Sie auf Fertig stellen.

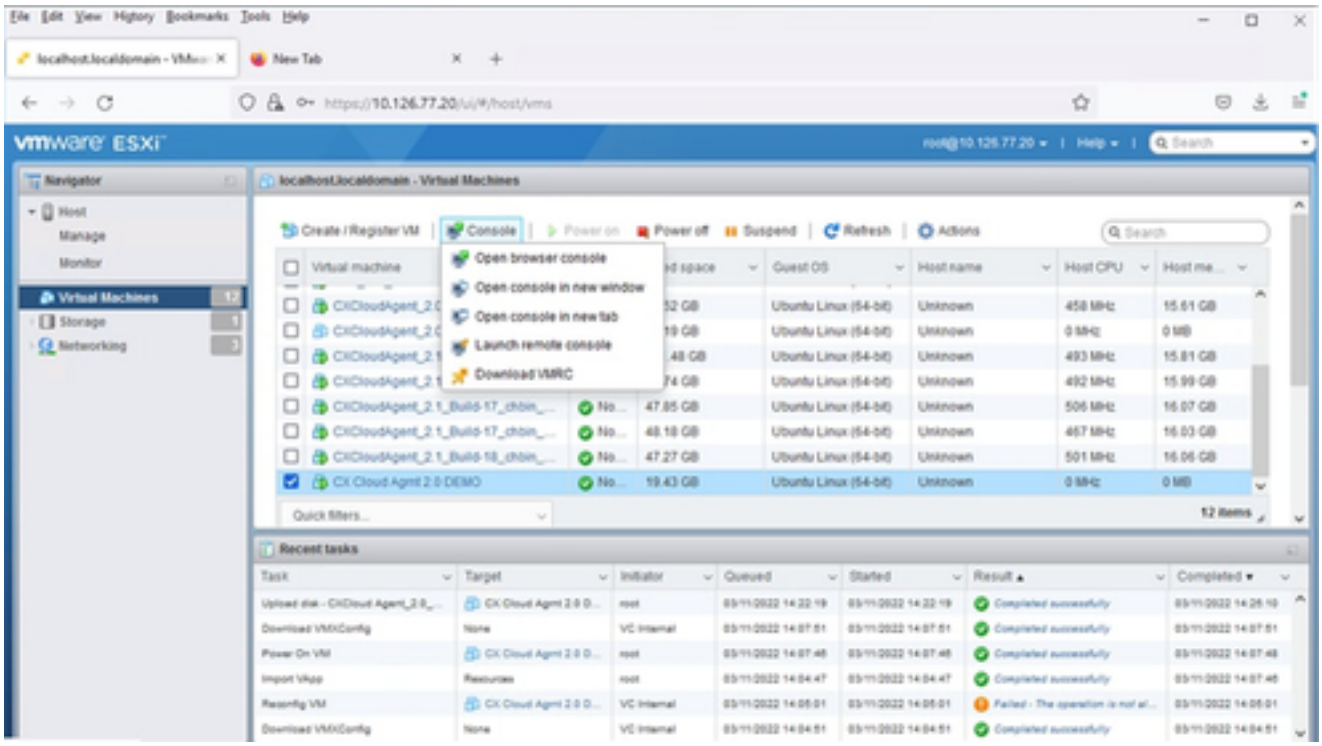


Bereit zur Fertigstellung



Abschluss erfolgreich

9. Wählen Sie das gerade bereitgestellte virtuelle System aus, und wählen Sie Console > Open browser console aus.



Konsole

10. Navigieren Sie zu Network Configuration, um mit den nächsten Schritten fortzufahren.

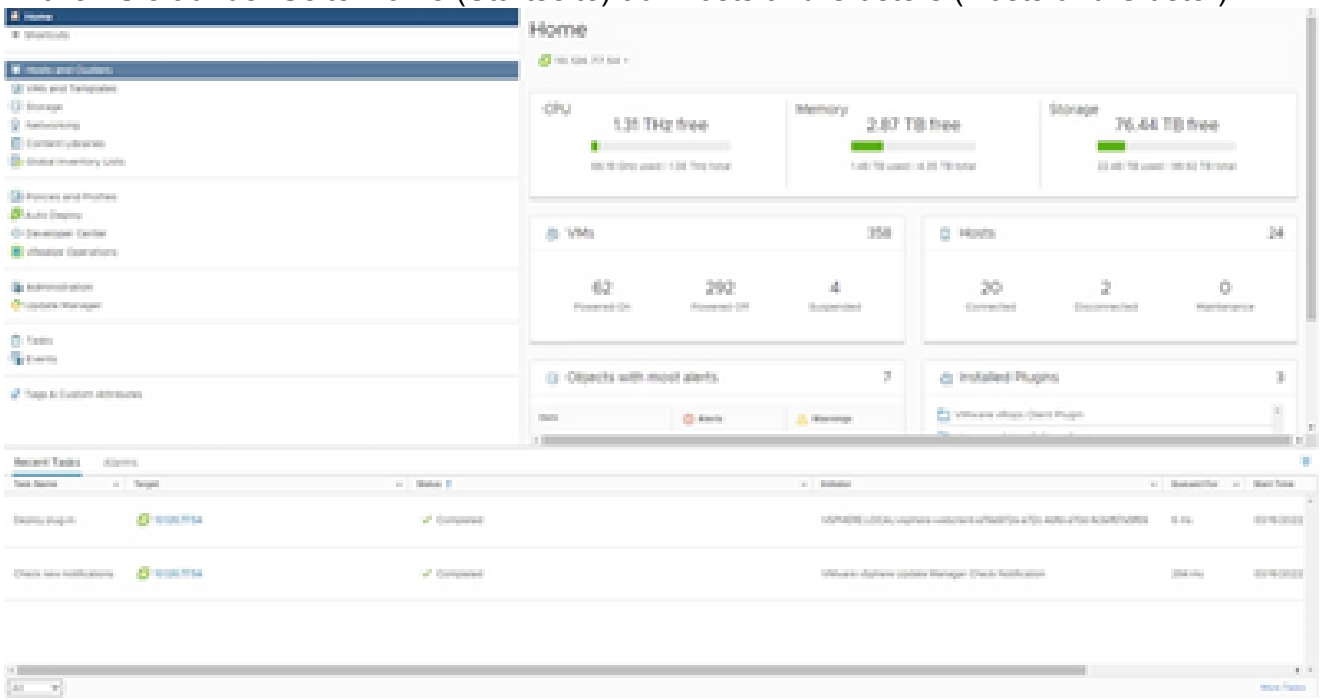
Installation von Web Client vCenter

Führen Sie die folgenden Schritte aus:

1. Melden Sie sich mit ESXi/Hypervisor-Anmeldeinformationen beim vCenter-Client an.

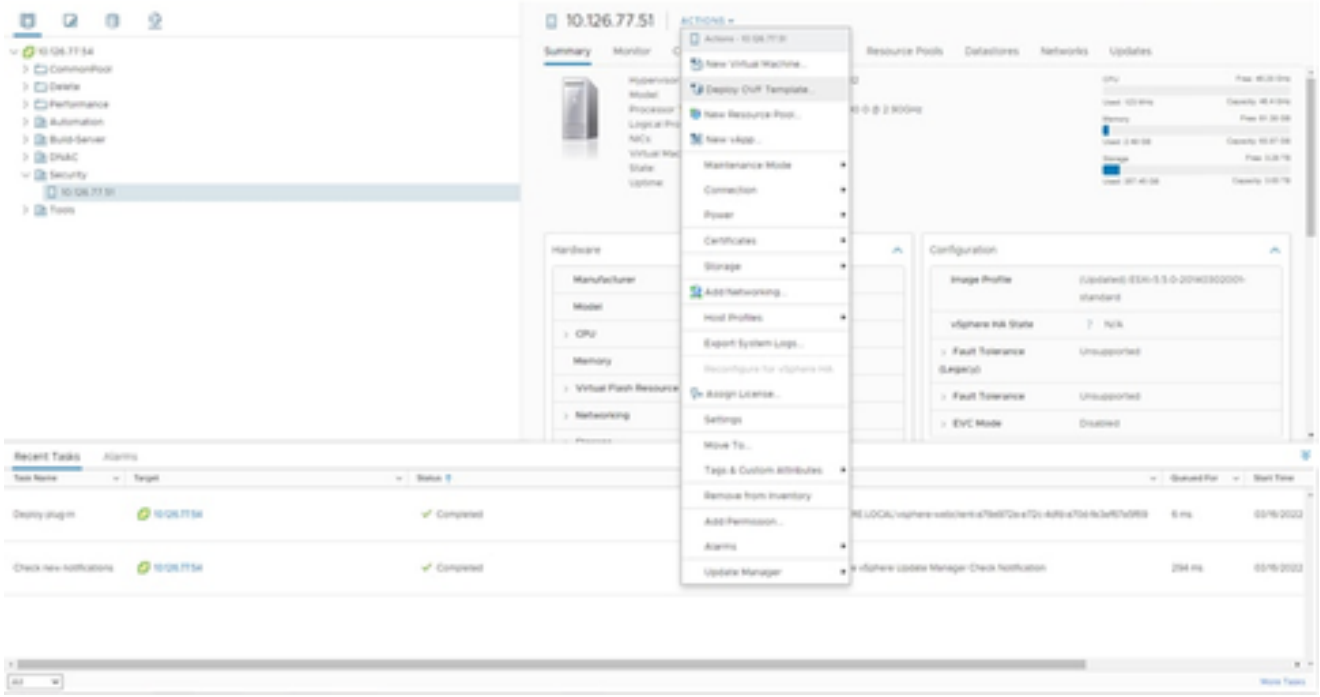
Anmelden

2. Klicken Sie auf der Seite Home (Startseite) auf Hosts and Clusters (Hosts und Cluster).

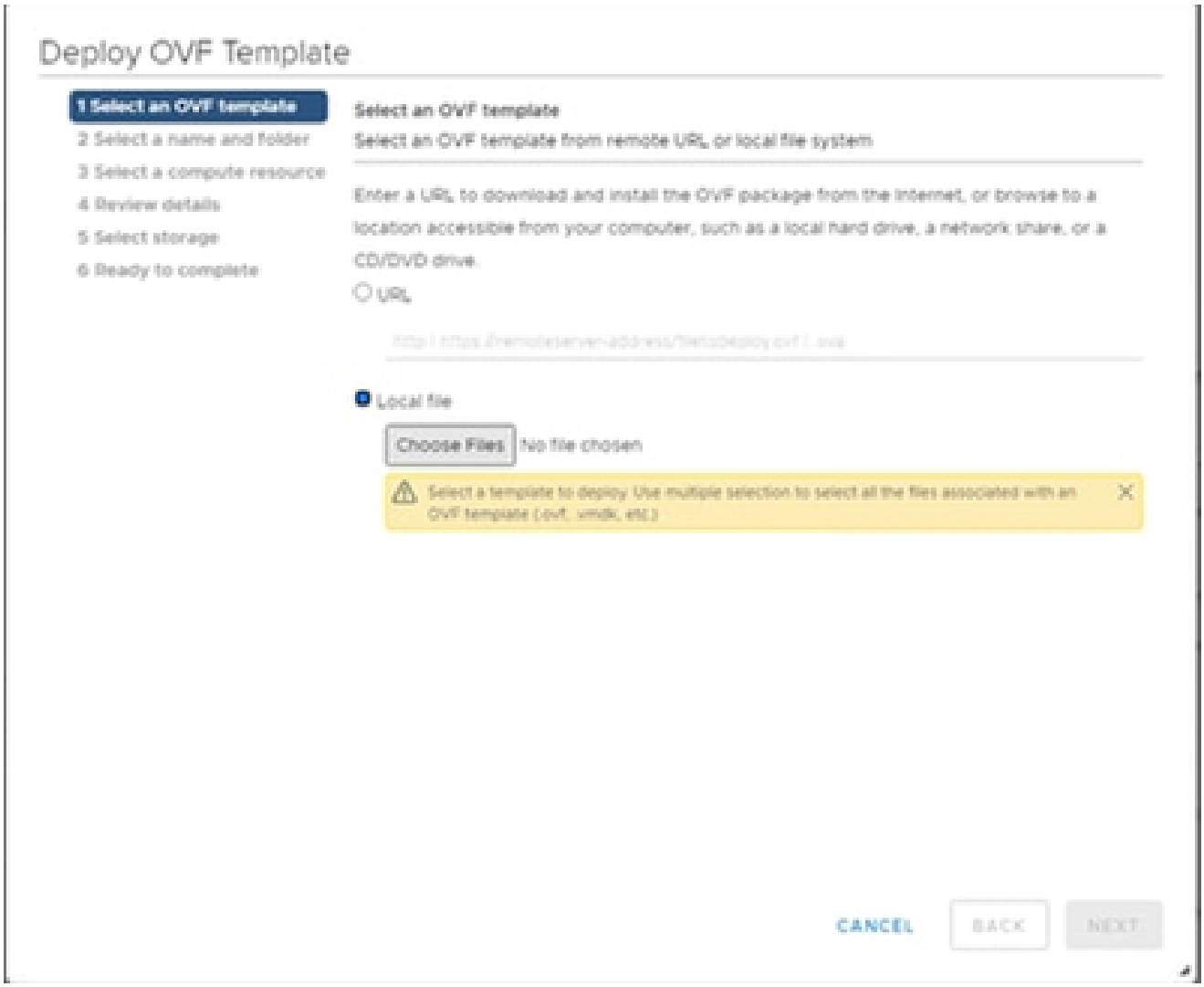


Startseite

3. Wählen Sie die VM aus und klicken Sie auf "Aktion" > "OVF-Vorlage bereitstellen".

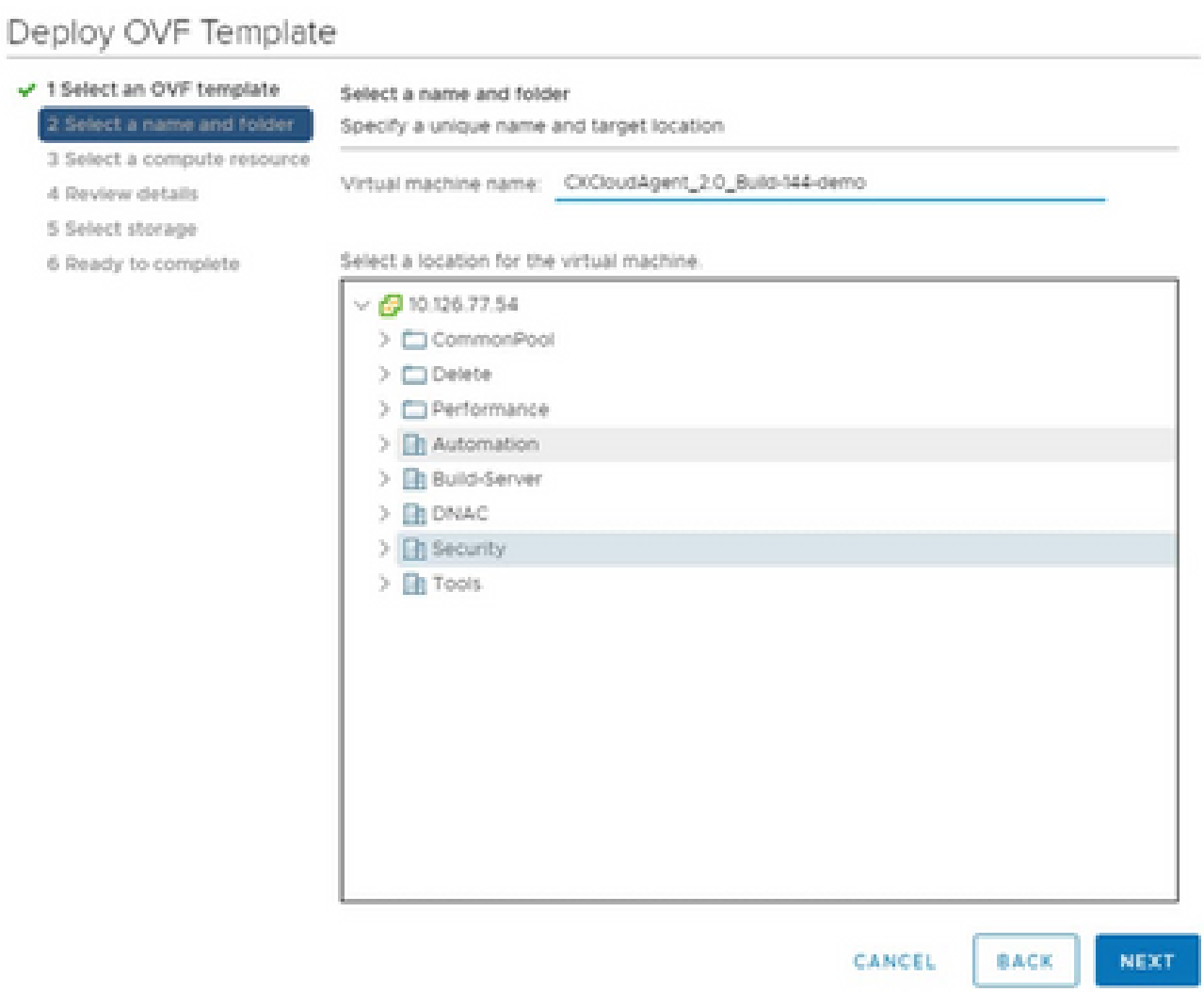


Aktionen



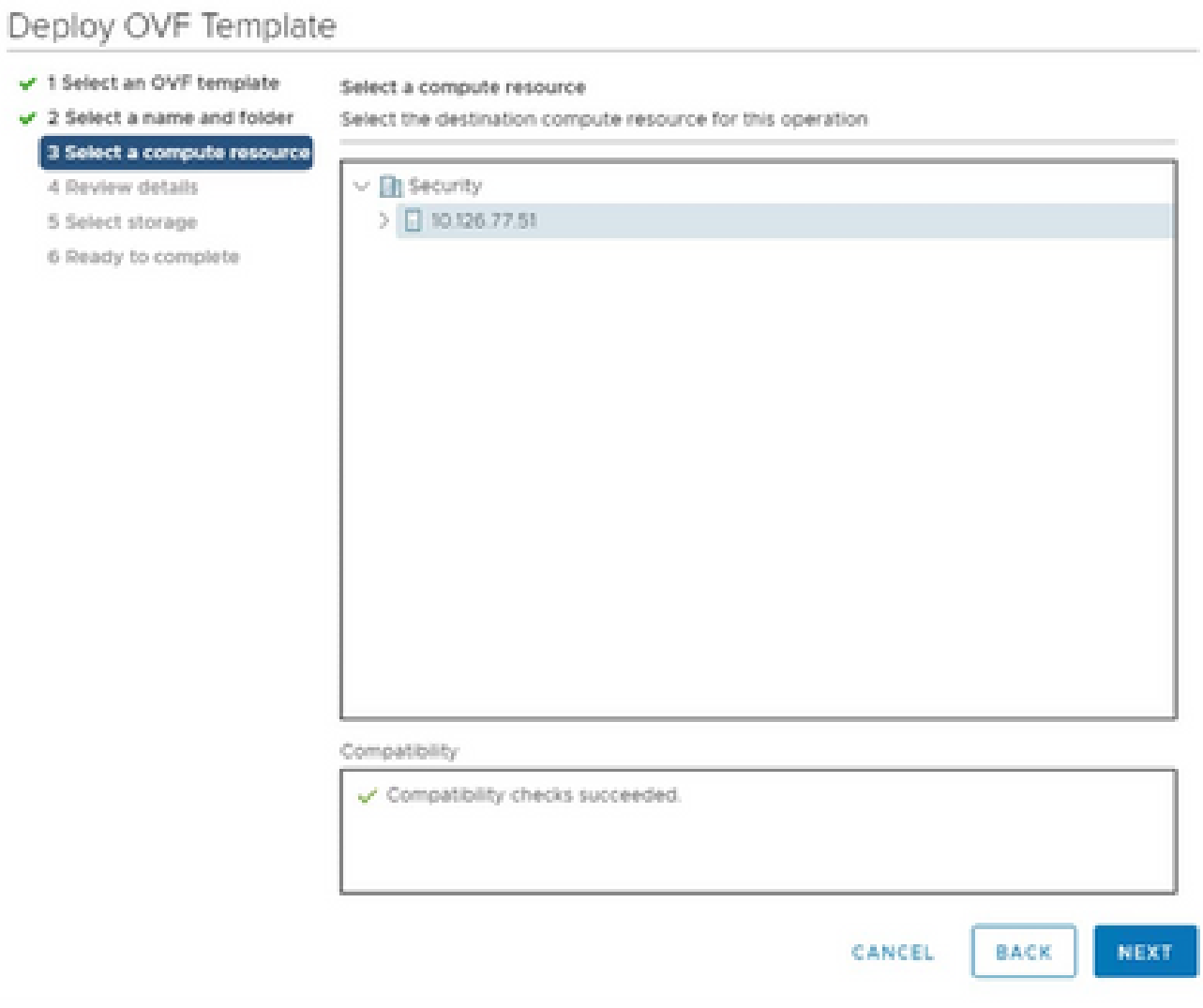
Vorlage auswählen

4. Fügen Sie die URL direkt hinzu, oder wählen Sie die OVA-Datei aus, und klicken Sie auf Weiter.
5. Geben Sie einen eindeutigen Namen ein, und navigieren Sie ggf. zum gewünschten Speicherort.
6. Klicken Sie auf Next (Weiter).



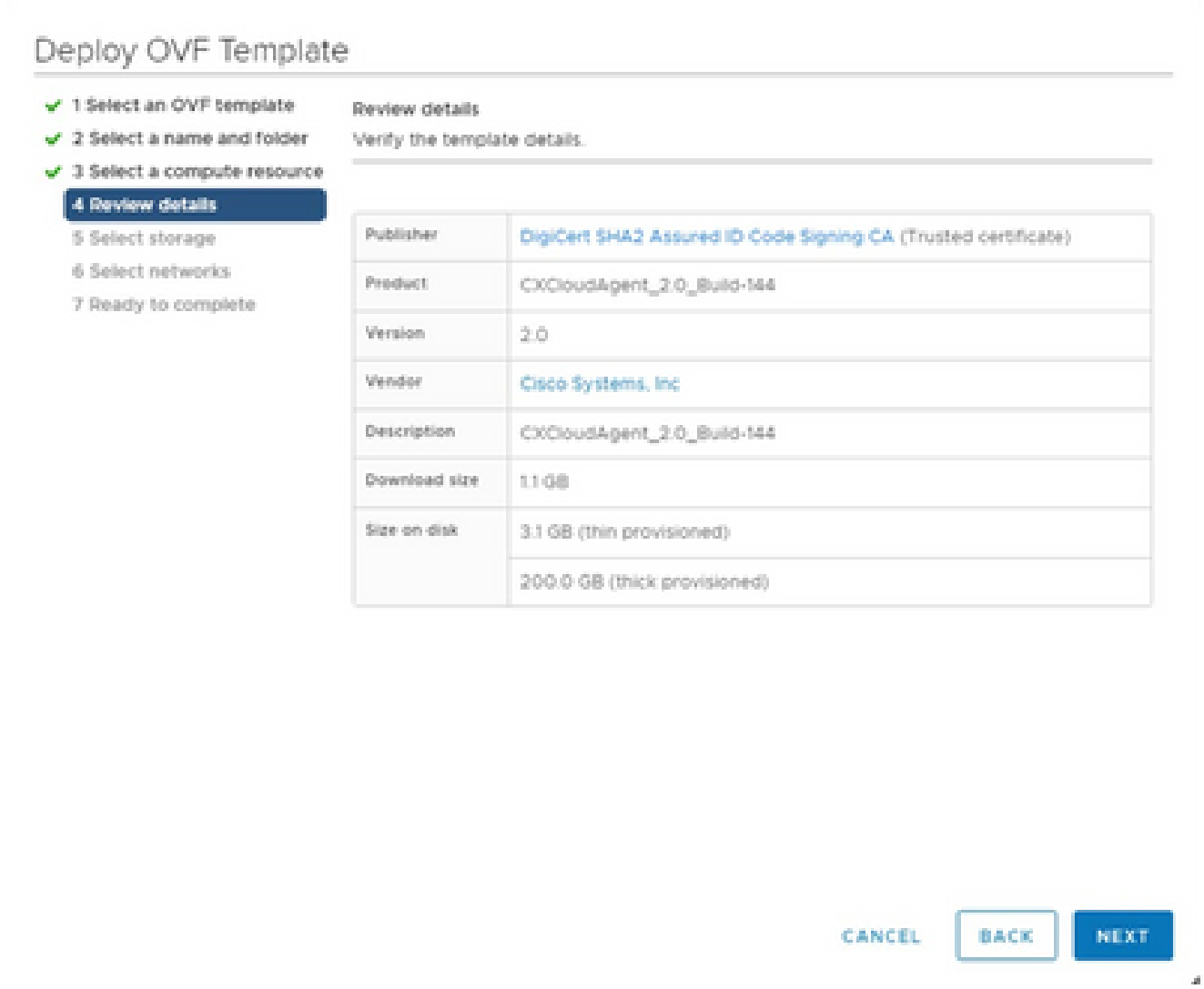
Name und Ordner

7. Wählen Sie eine Rechenressource aus, und klicken Sie auf Weiter.



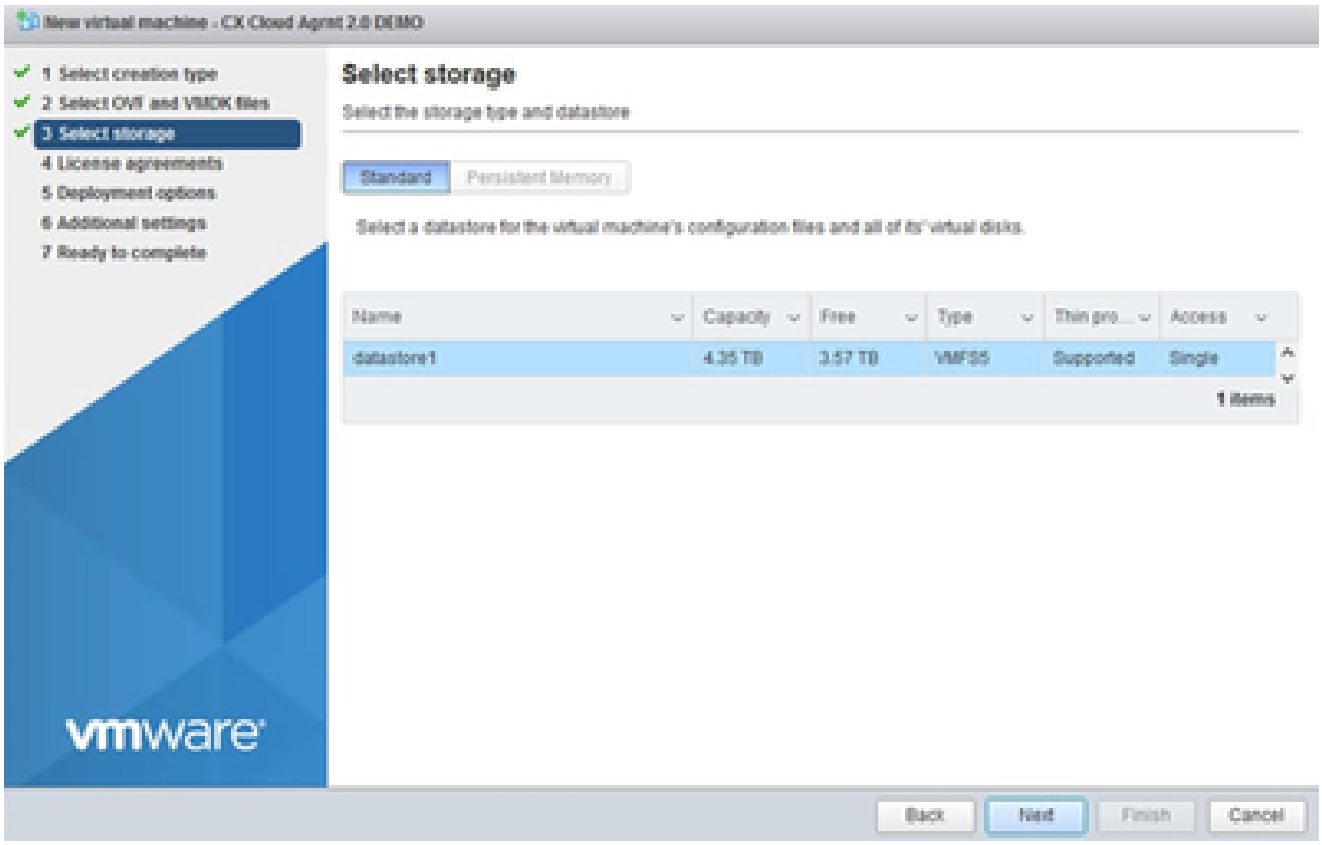
Computerressource auswählen

8. Überprüfen Sie die Details und klicken Sie auf Weiter.



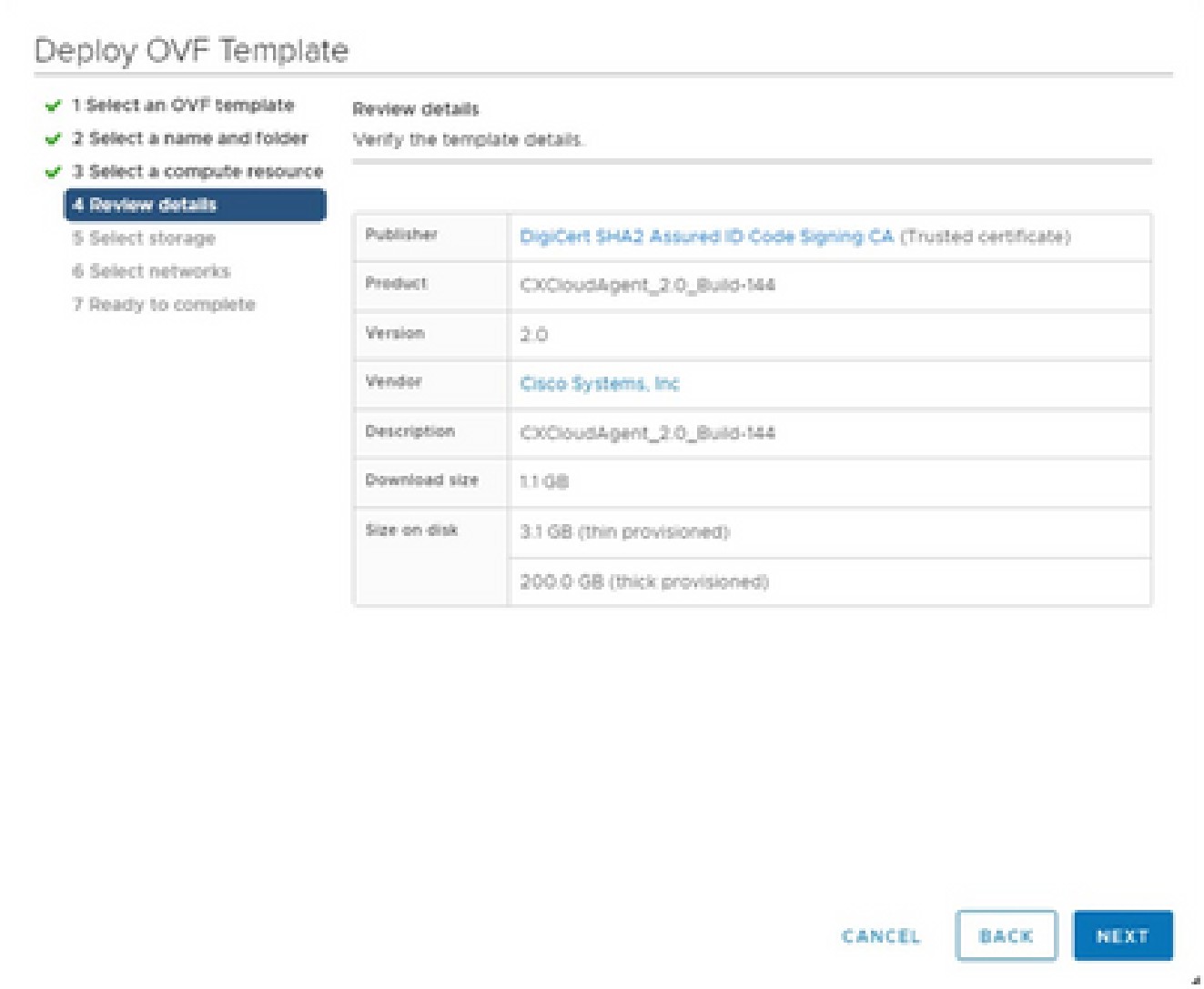
Details überprüfen

9. Wählen Sie das Format des virtuellen Datenträgers aus und klicken Sie auf Weiter.



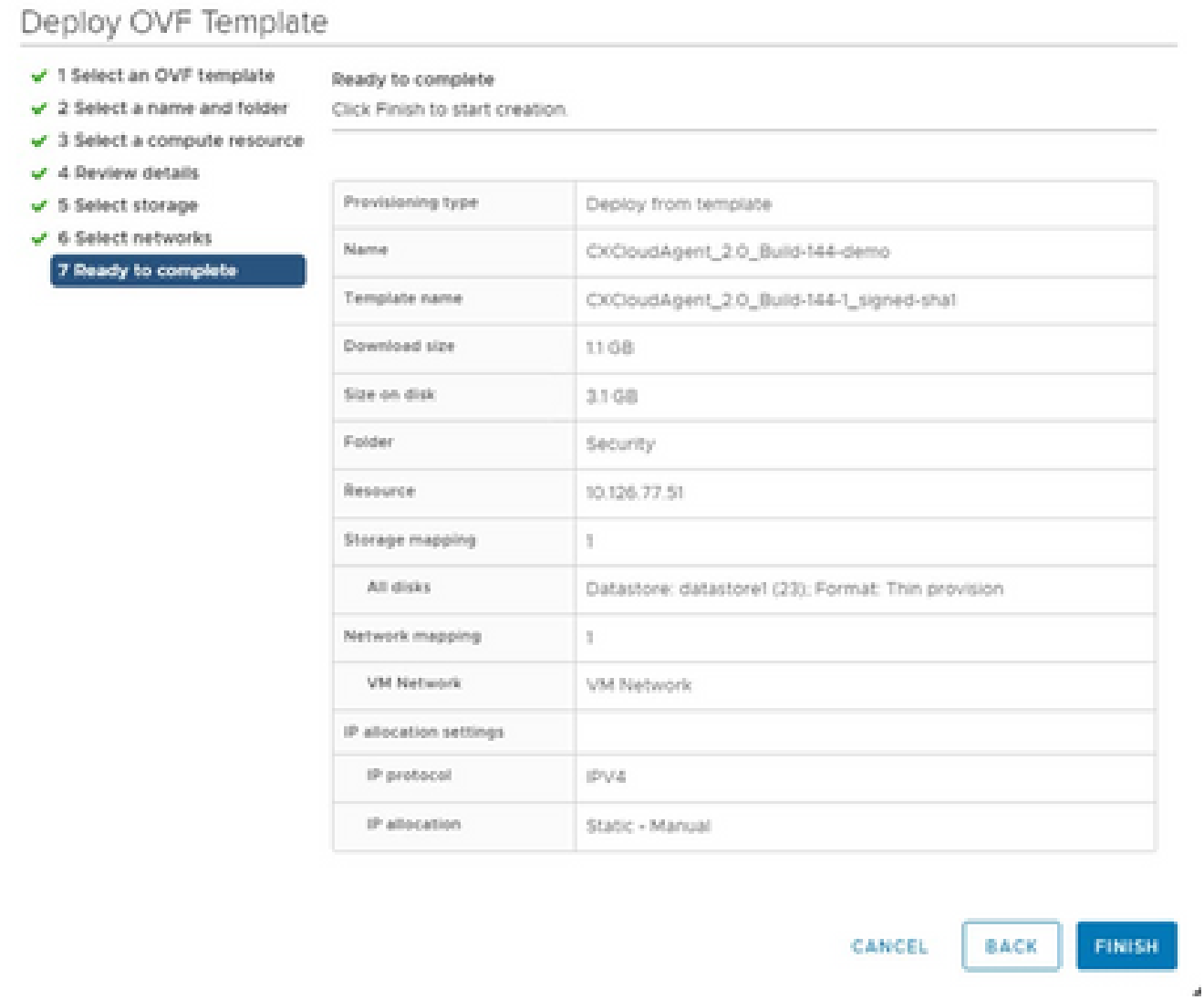
Auswahl von externem Speicher

10. Klicken Sie auf Next (Weiter).



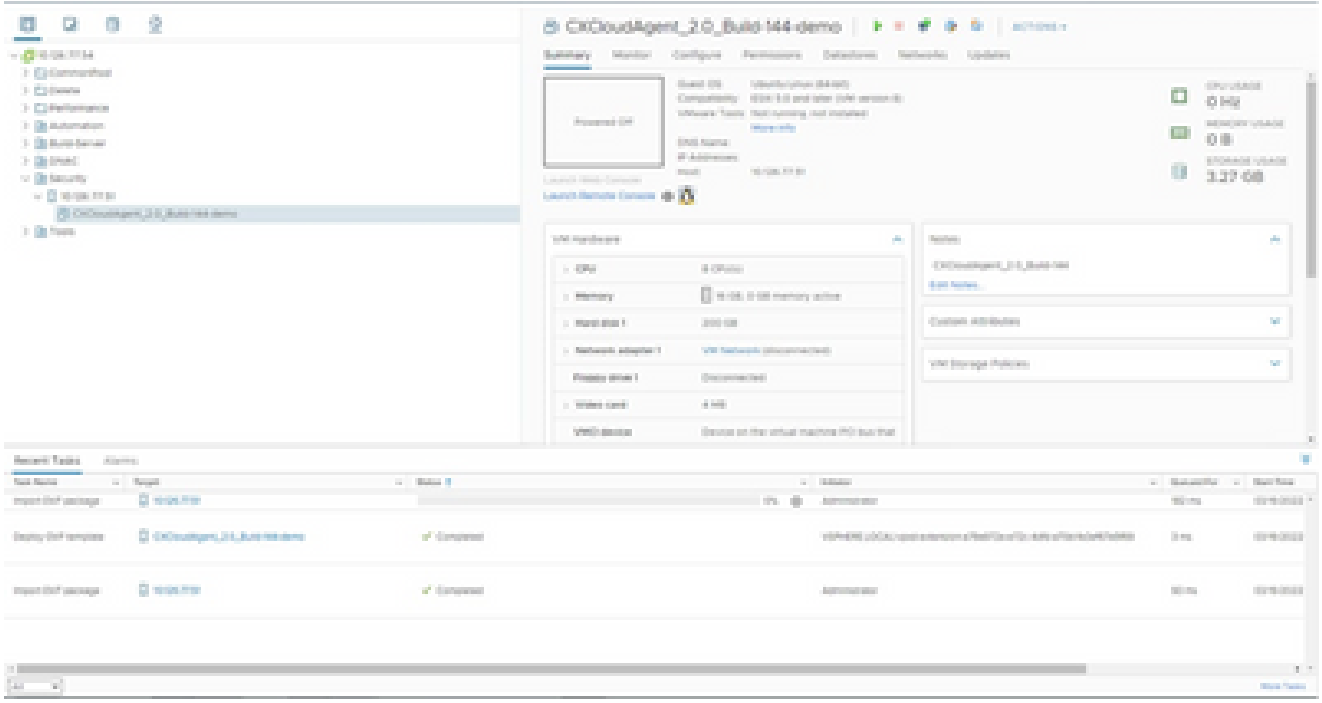
Netzwerk auswählen

11. Klicken Sie auf Beenden.



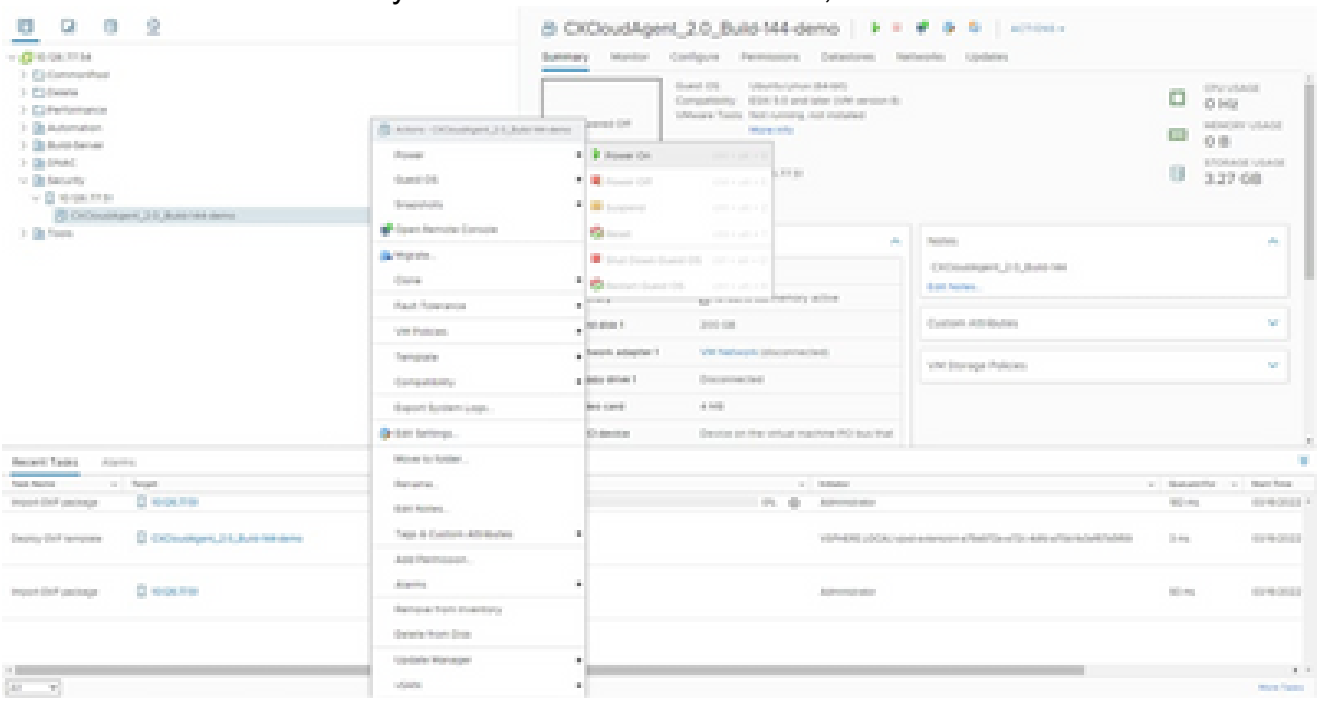
Bereit zur Fertigstellung

12. Klicken Sie auf den Namen der neu hinzugefügten VM, um den Status anzuzeigen.



VM hinzugefügt

13. Schalten Sie das virtuelle System nach der Installation ein, und öffnen Sie die Konsole.



Konsole öffnen

14. Navigieren Sie zu Network Configuration, um die nächsten Schritte auszuführen.

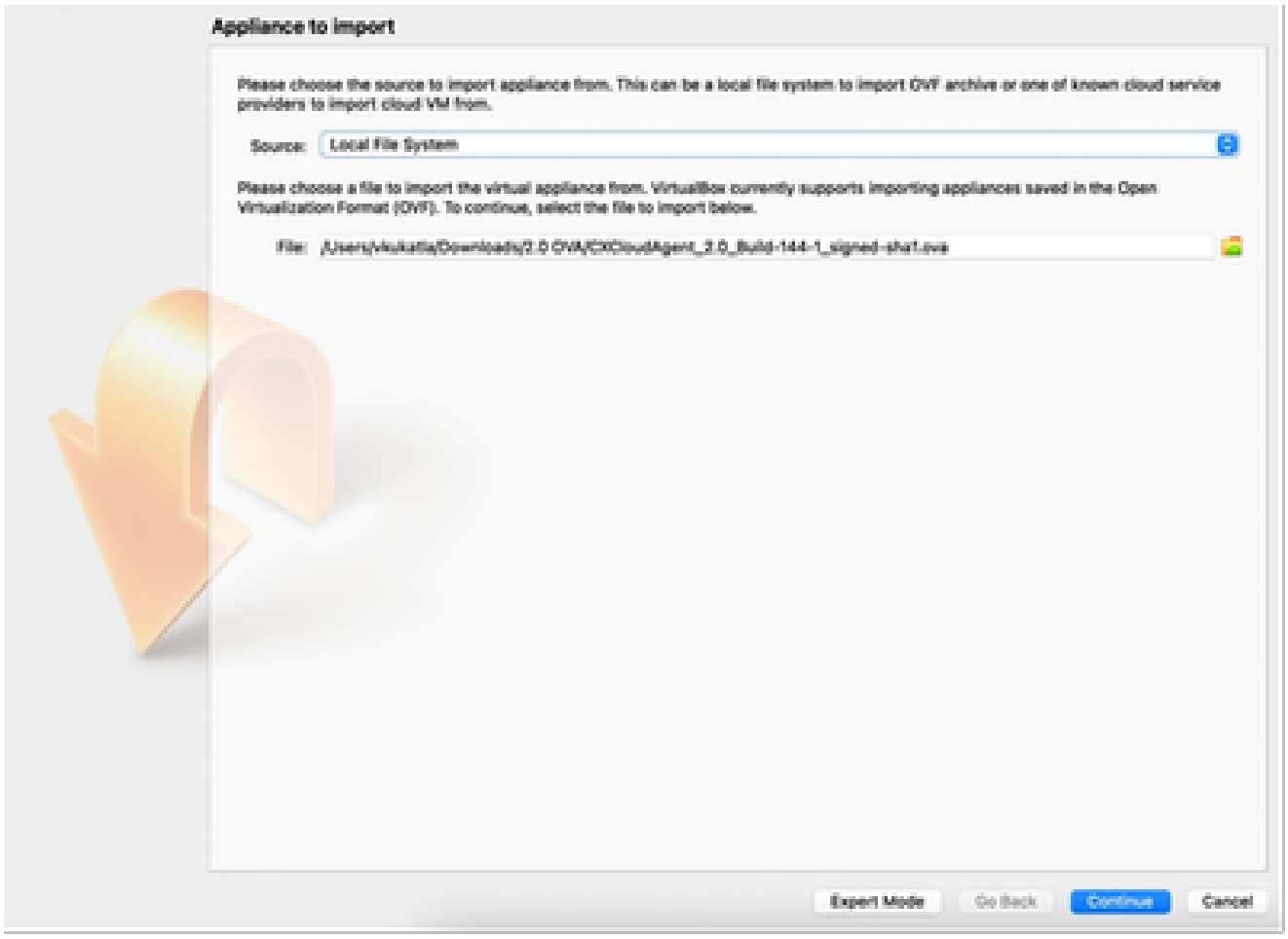
Installation von Oracle VirtualBox 5.2.30

Dieser Client stellt CX Cloud Agent OVA über die Oracle Virtual Box bereit.

1. Öffnen Sie die Oracle VM-Benutzeroberfläche, und wählen Sie Datei > Appliance importieren aus.

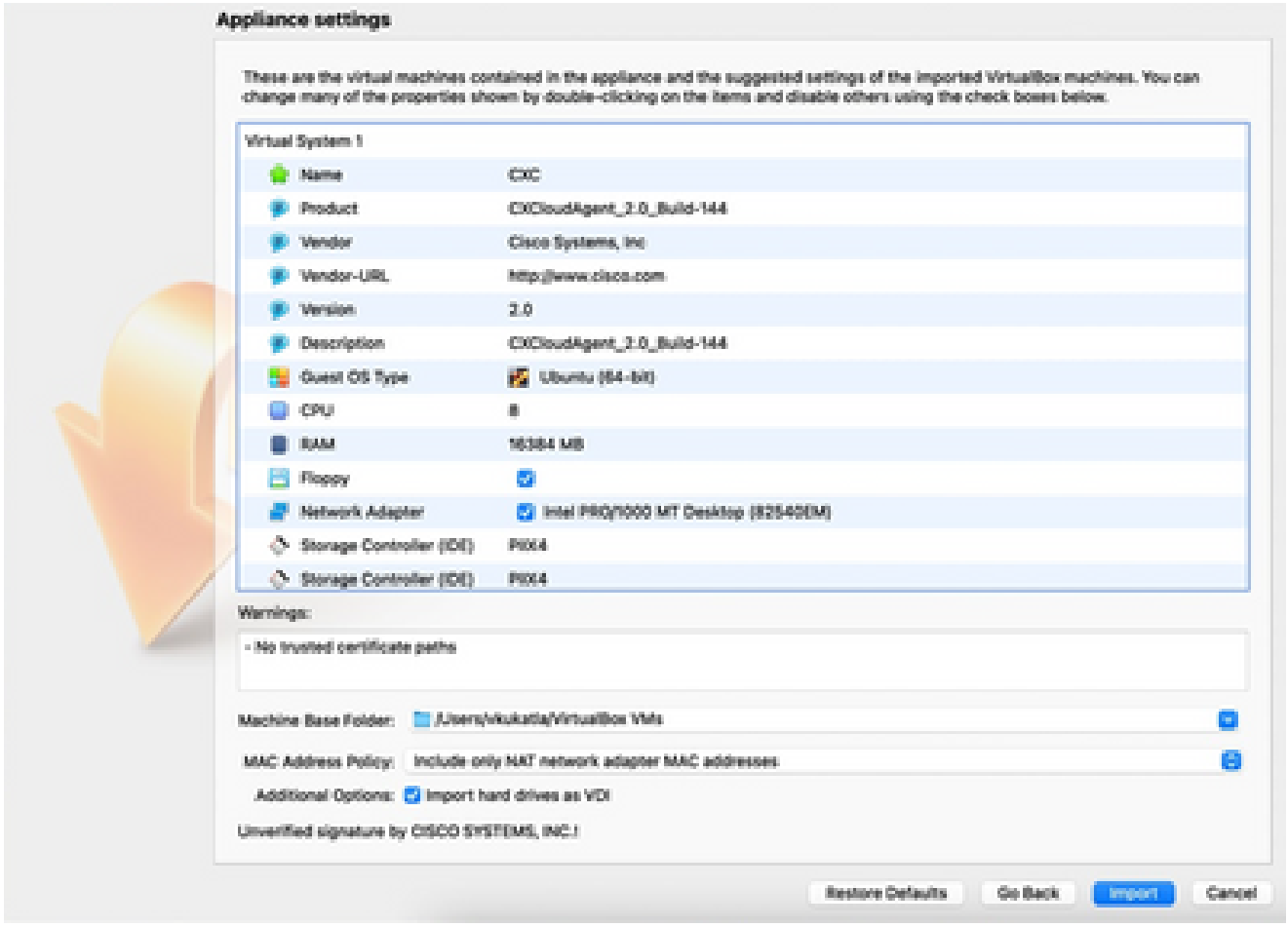
Oracle VM

2. Klicken Sie auf "Durchsuchen", um die OVA-Datei zu importieren.



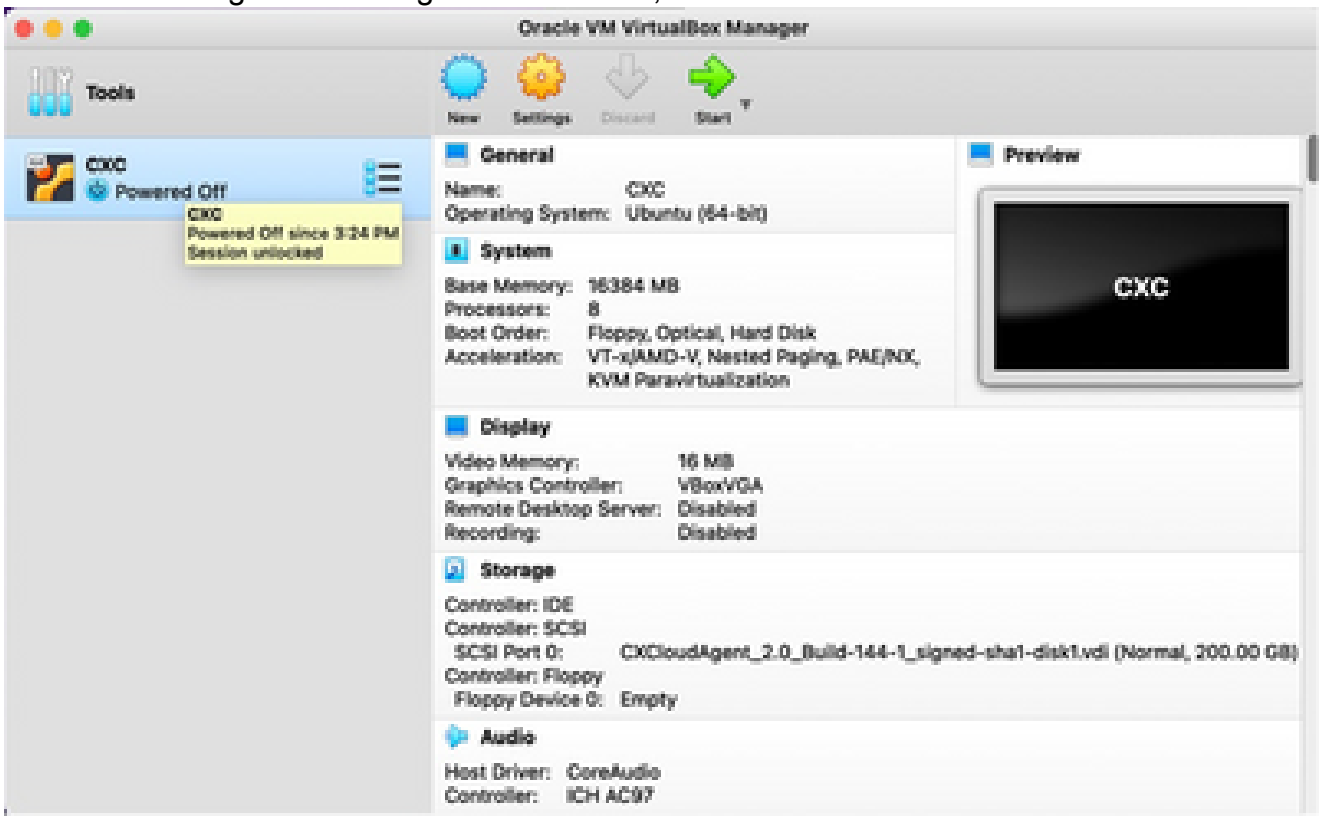
Datei auswählen

3. Klicken Sie auf Importieren.

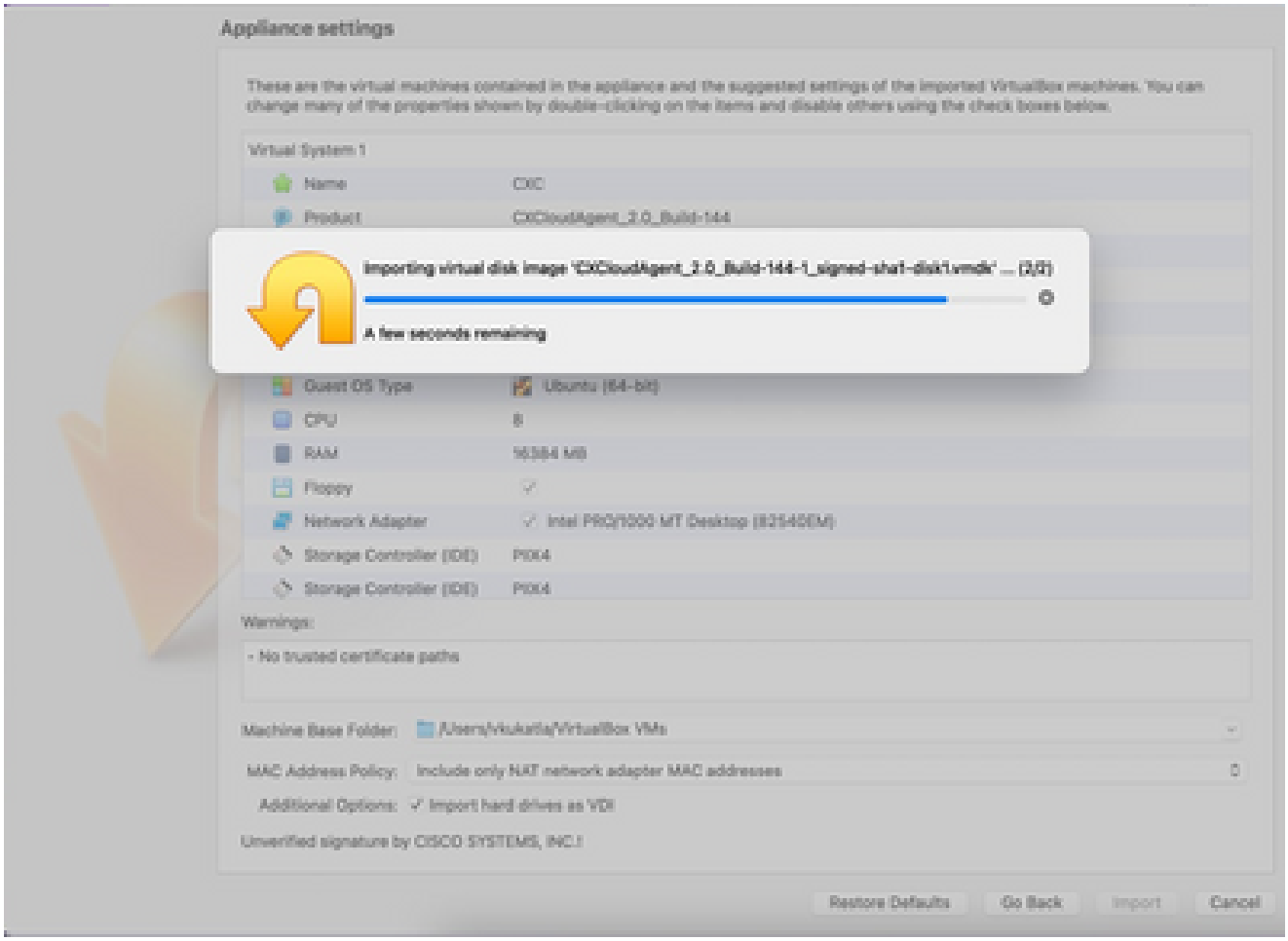


Datei importieren

4. Wählen Sie die gerade bereitgestellte VM aus, und klicken Sie auf Start.

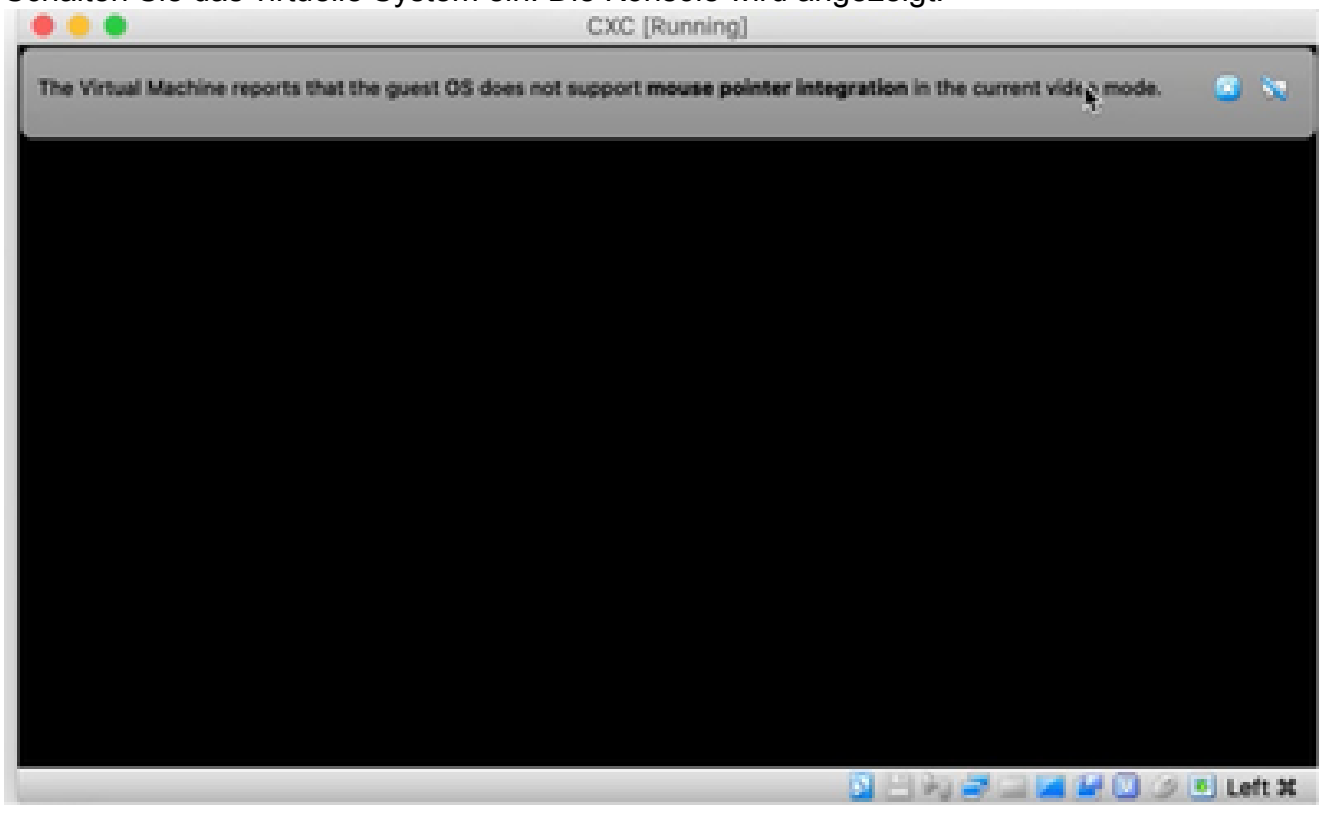


Start der VM-Konsole



Import in Bearbeitung

5. Schalten Sie das virtuelle System ein. Die Konsole wird angezeigt.



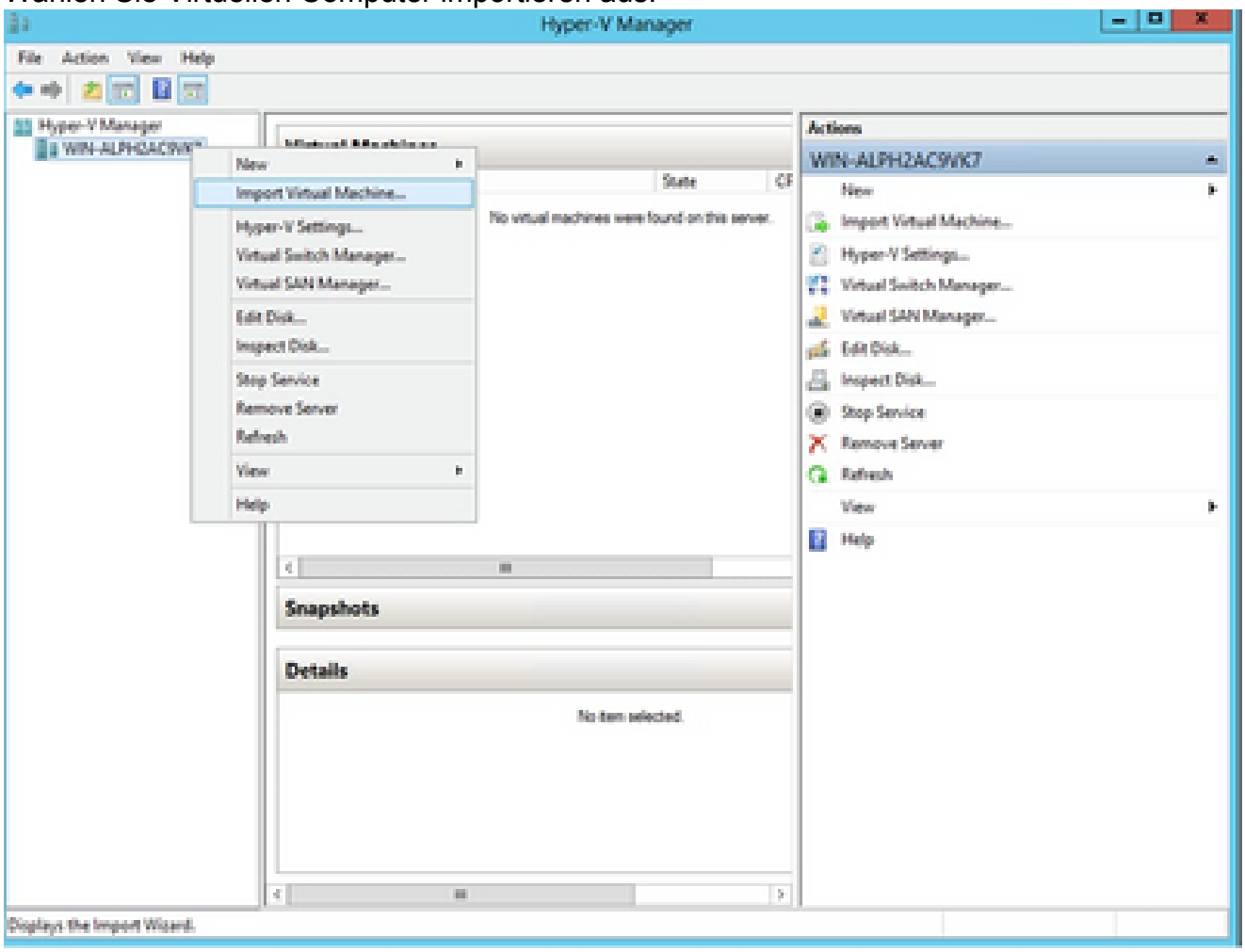
Konsole öffnen

6. Navigieren Sie zu Network Configuration, um mit den nächsten Schritten fortzufahren.

Installation von Microsoft Hyper-V

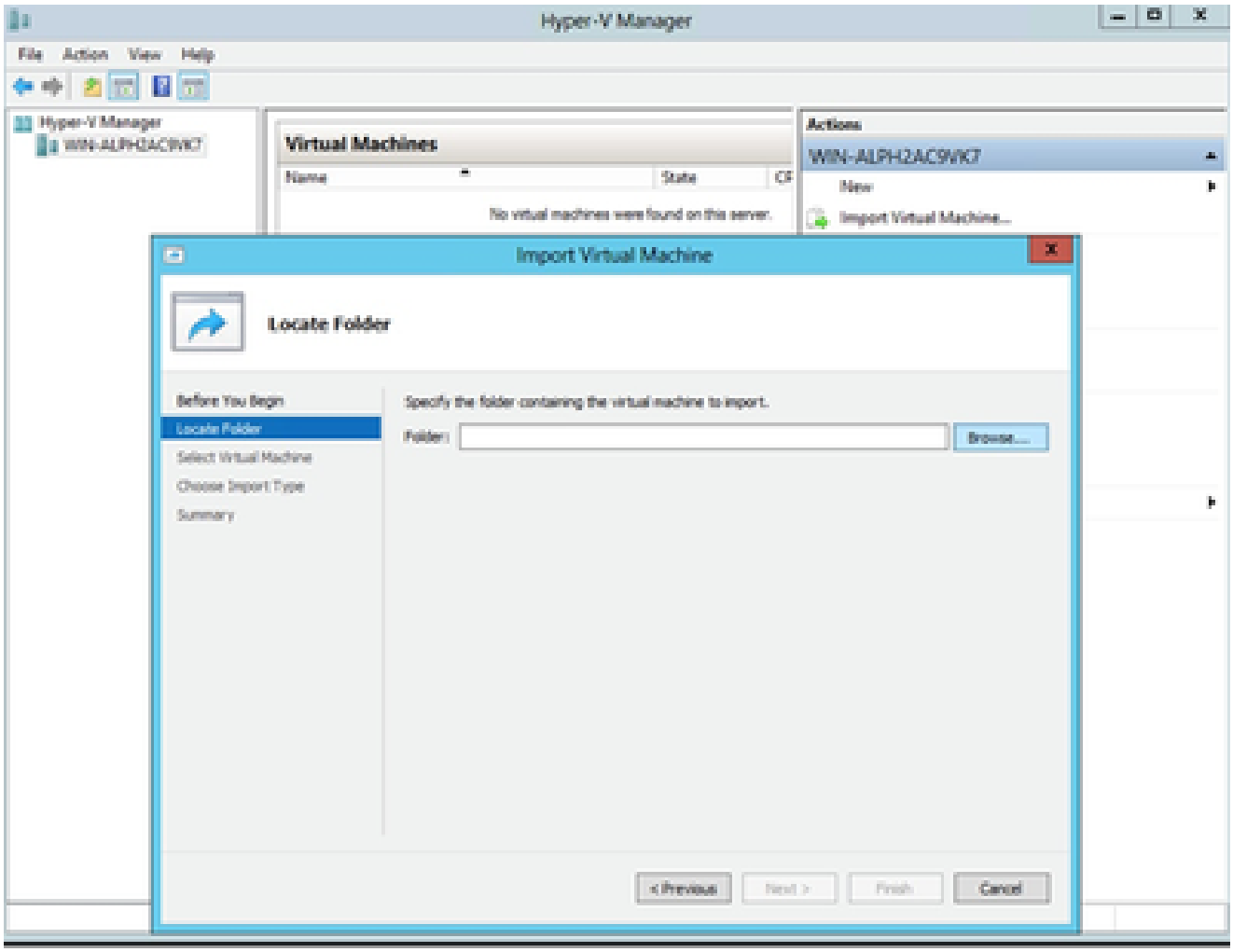
Führen Sie die folgenden Schritte aus:

1. Wählen Sie Virtuellen Computer importieren aus.



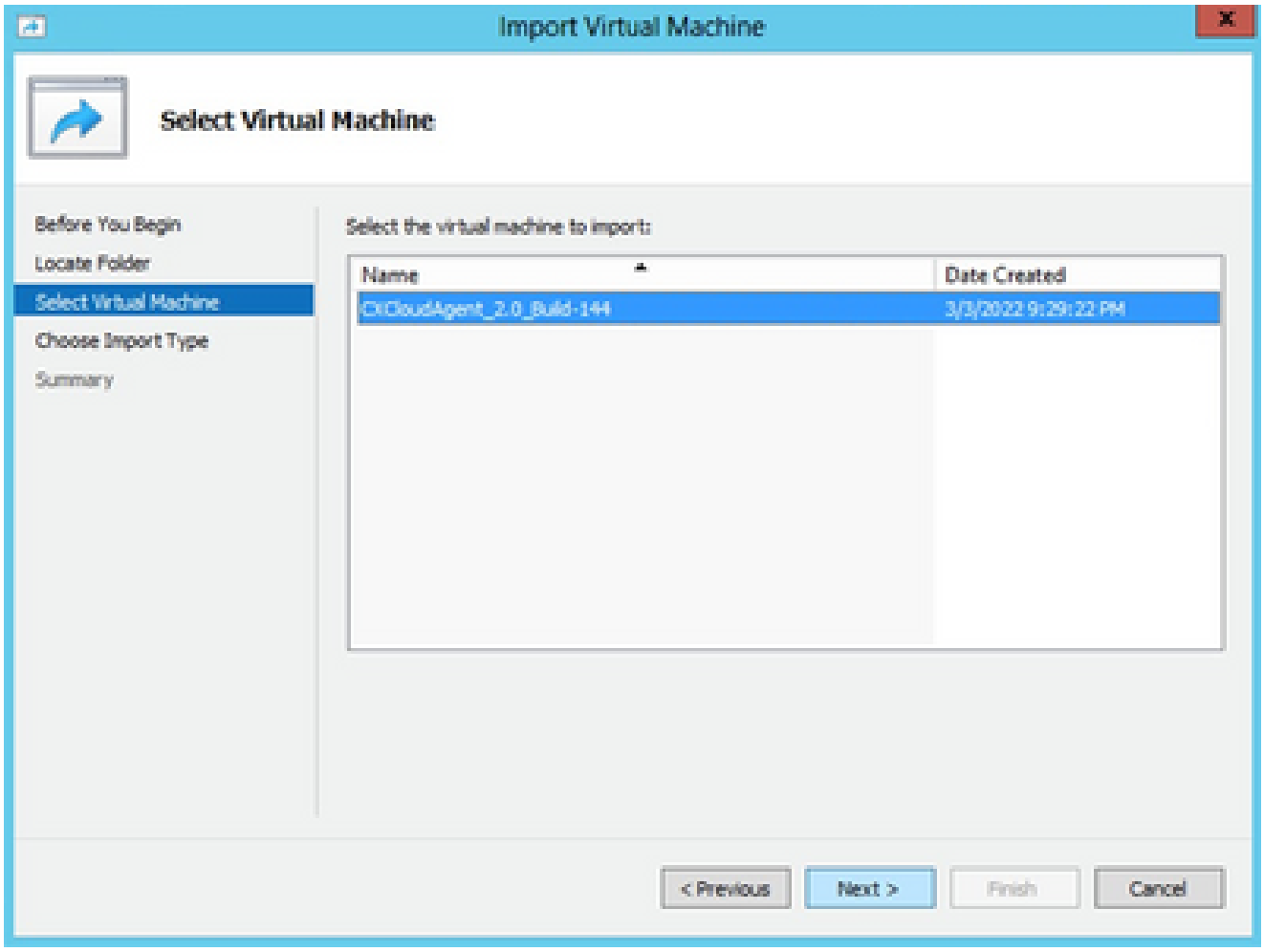
Hyper-V-Manager

2. Suchen Sie den Ordner "Downloads" und wählen Sie ihn aus.
3. Klicken Sie auf Next (Weiter).



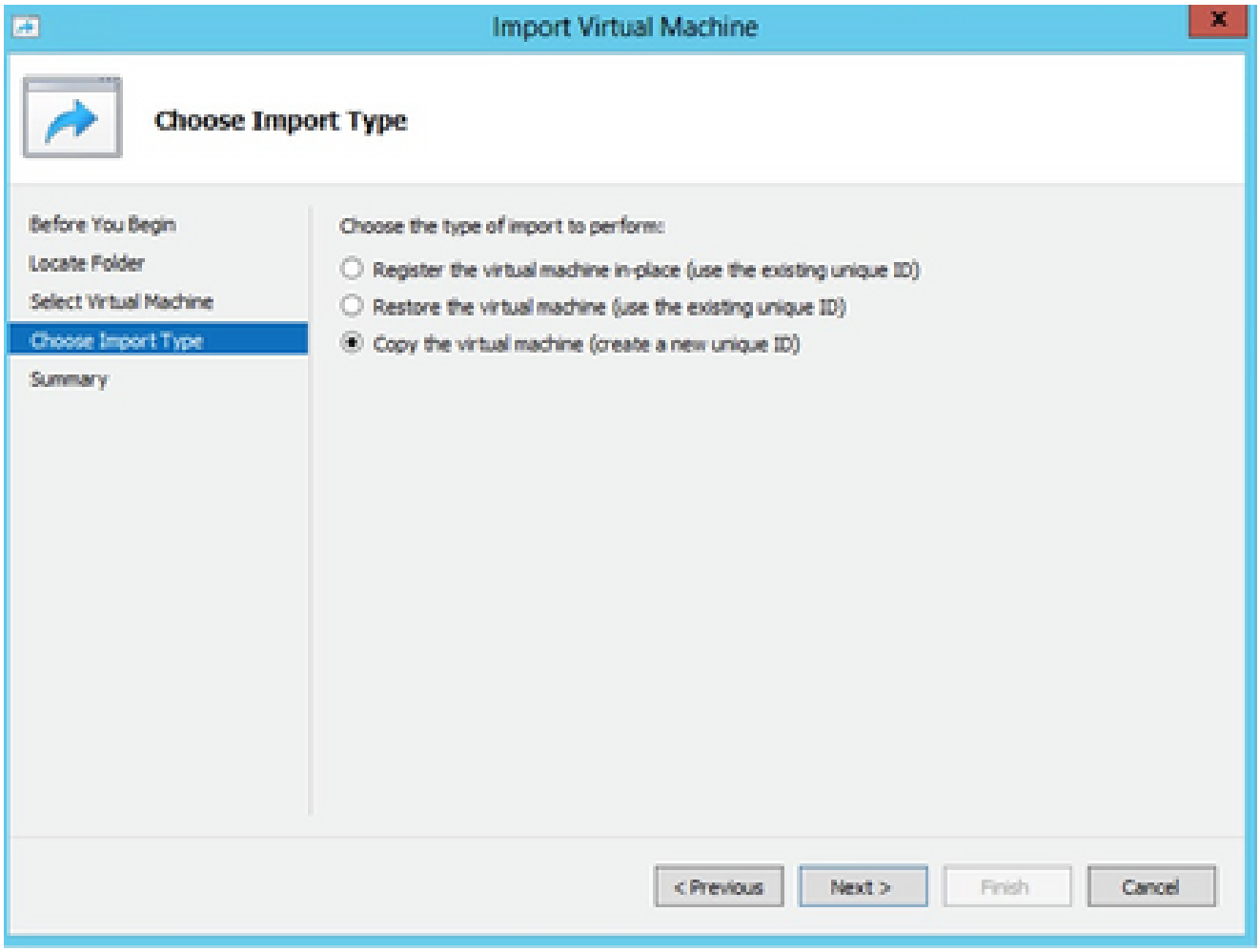
Zu importierender Ordner

4. Wählen Sie die VM aus, und klicken Sie auf Weiter.



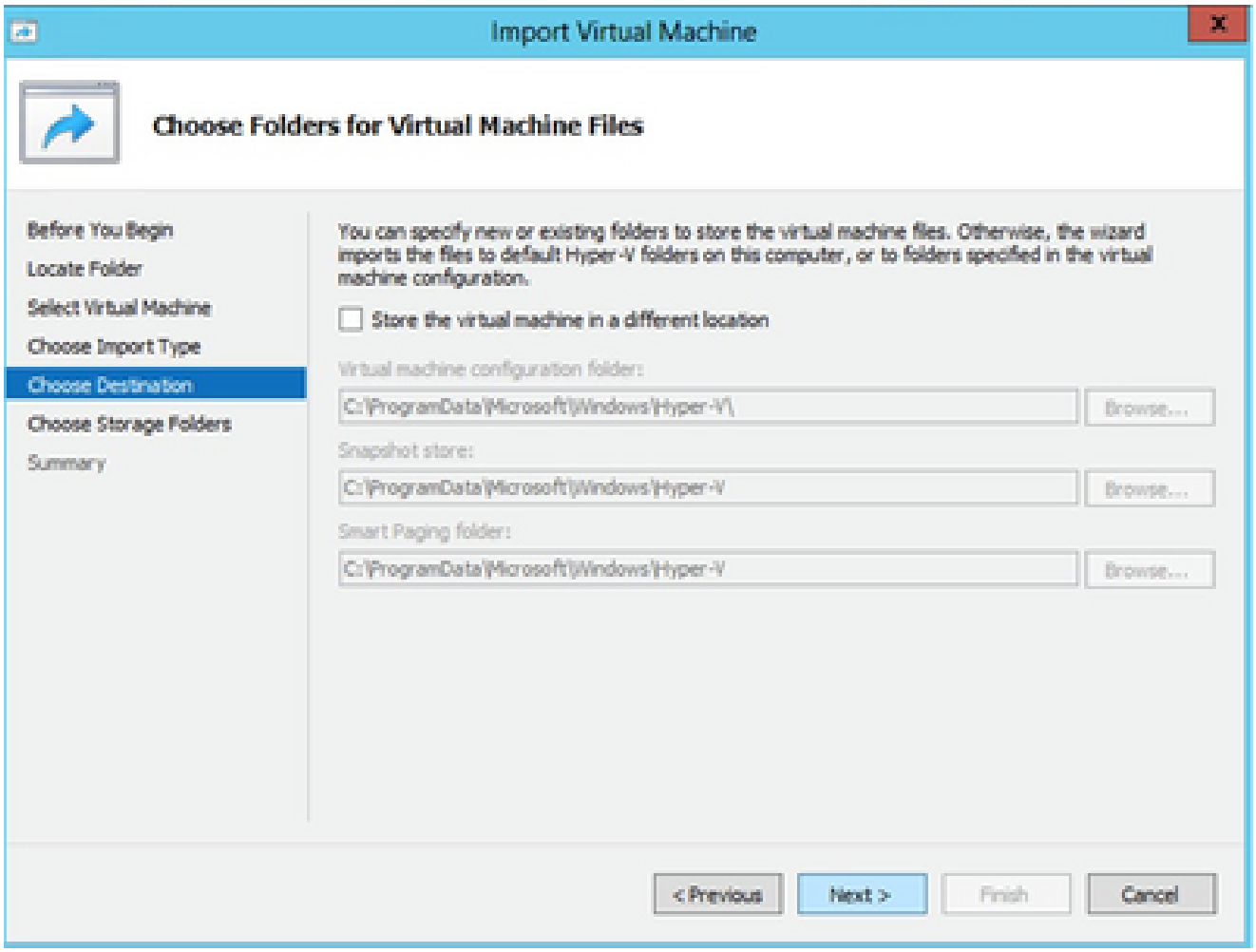
VM auswählen

5. Aktivieren Sie das Optionsfeld Virtuellen Computer kopieren (neue eindeutige ID erstellen), und klicken Sie auf Weiter.



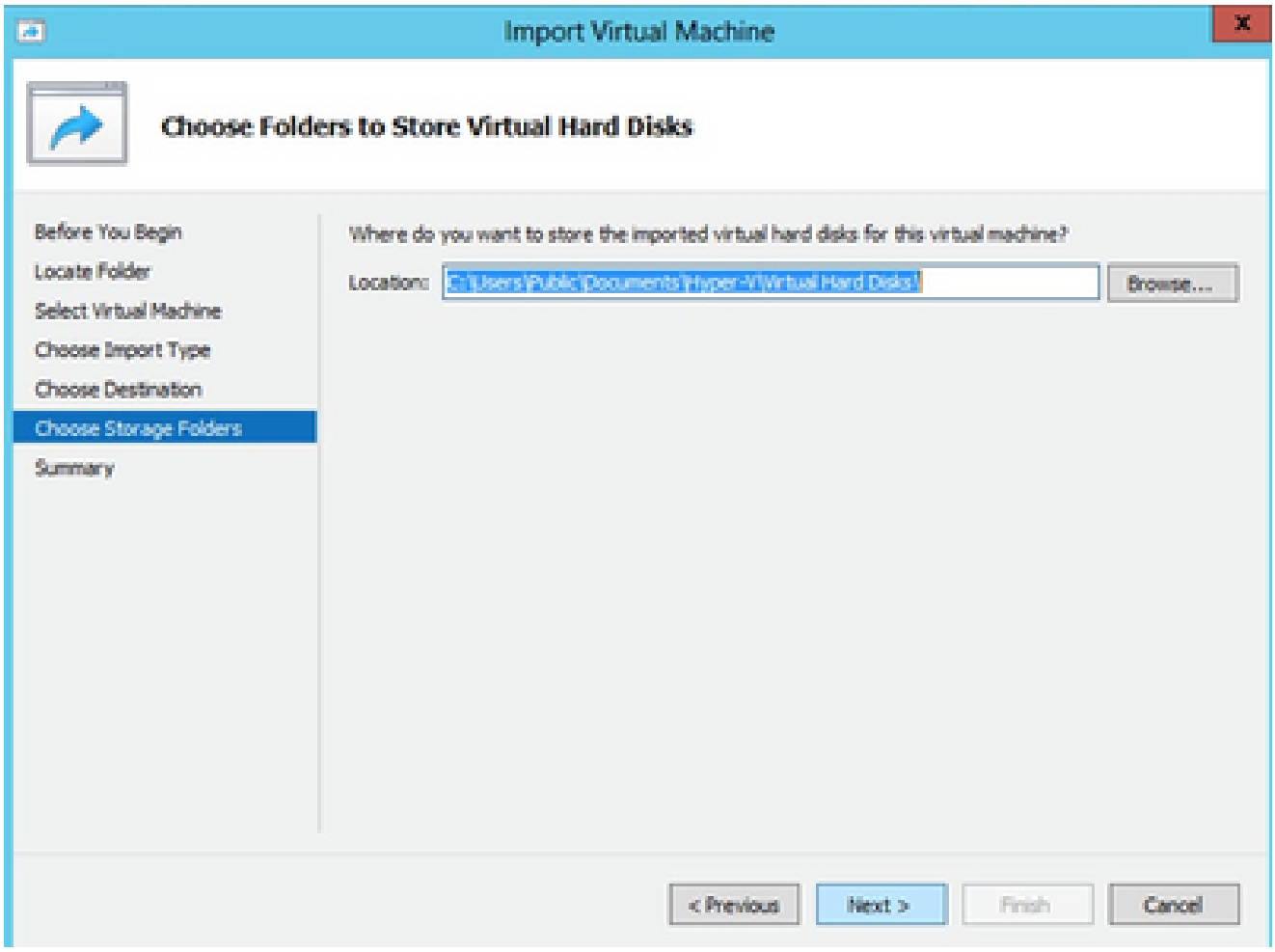
Importtyp

6. Klicken Sie auf "Durchsuchen", um den Ordner für VM-Dateien auszuwählen. Es wird empfohlen, die Standardpfade zu verwenden.
7. Klicken Sie auf Next (Weiter).



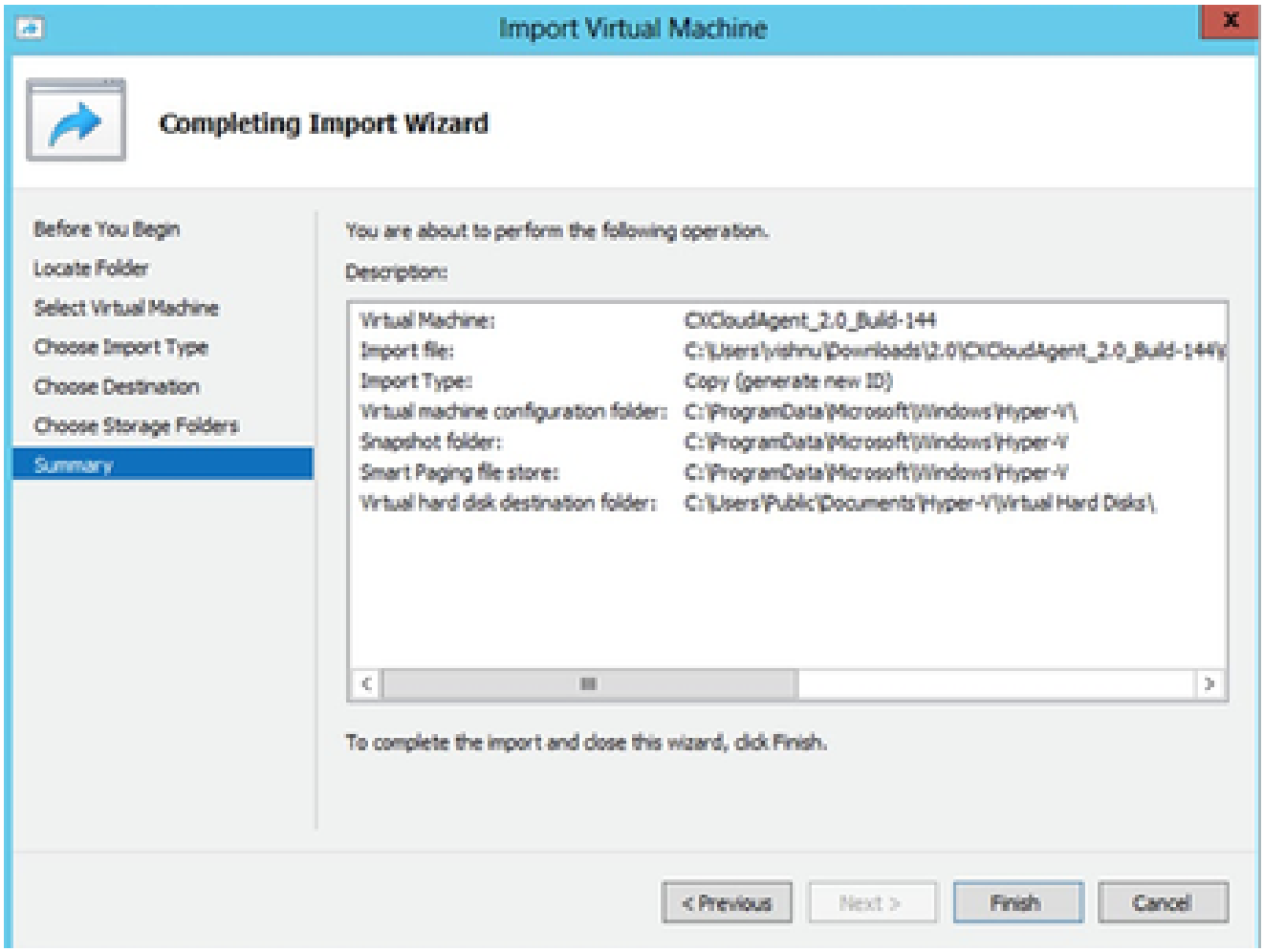
Ordner für Dateien virtueller Systeme auswählen

8. Suchen Sie nach dem Ordner zum Speichern der VM-Festplatte und wählen Sie ihn aus. Es wird empfohlen, Standardpfade zu verwenden.
9. Klicken Sie auf Next (Weiter).



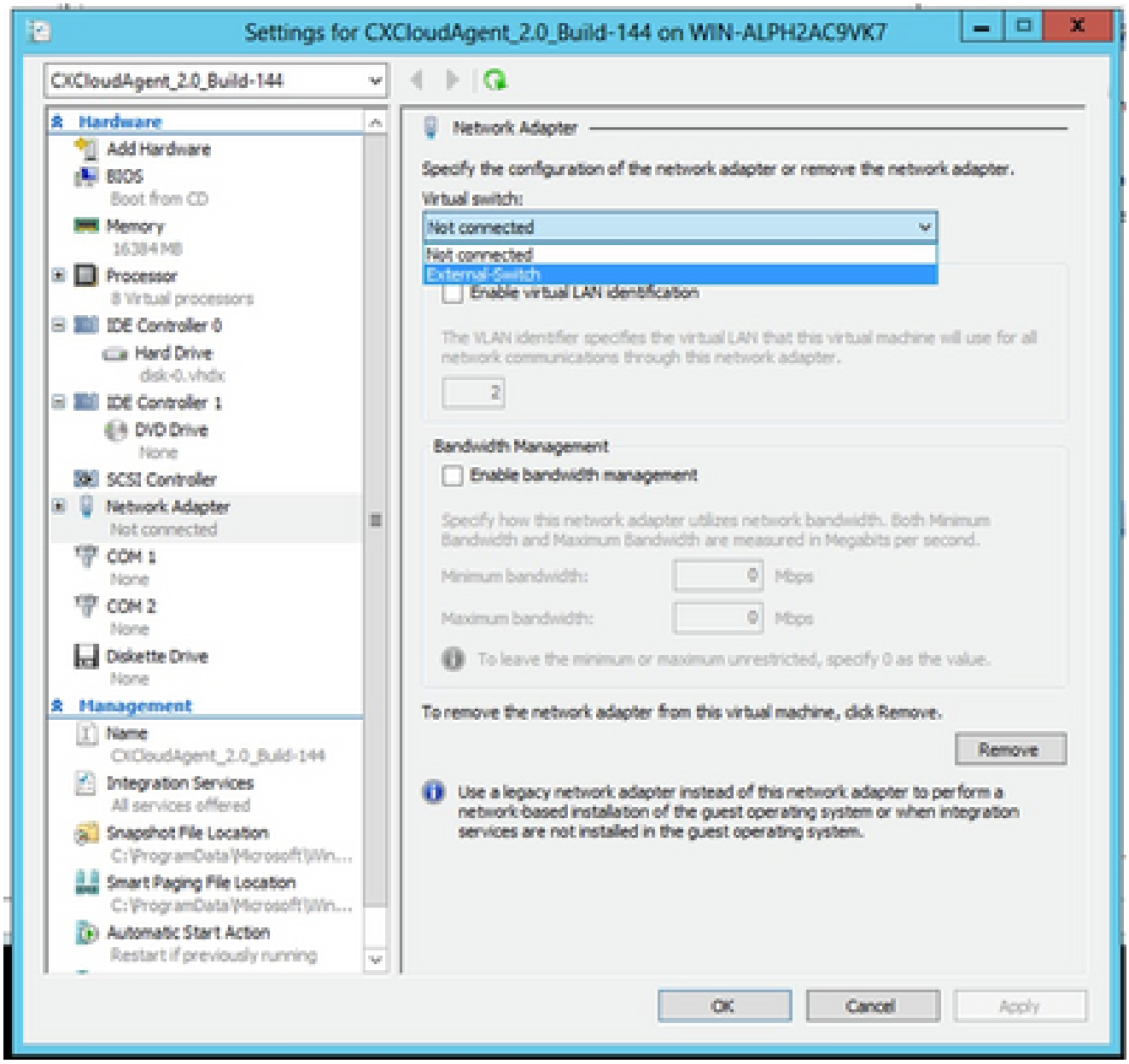
Ordner zum Speichern der virtuellen Festplatten

10. Die VM-Übersicht wird angezeigt. Überprüfen Sie alle Eingaben, und klicken Sie auf Fertig stellen.



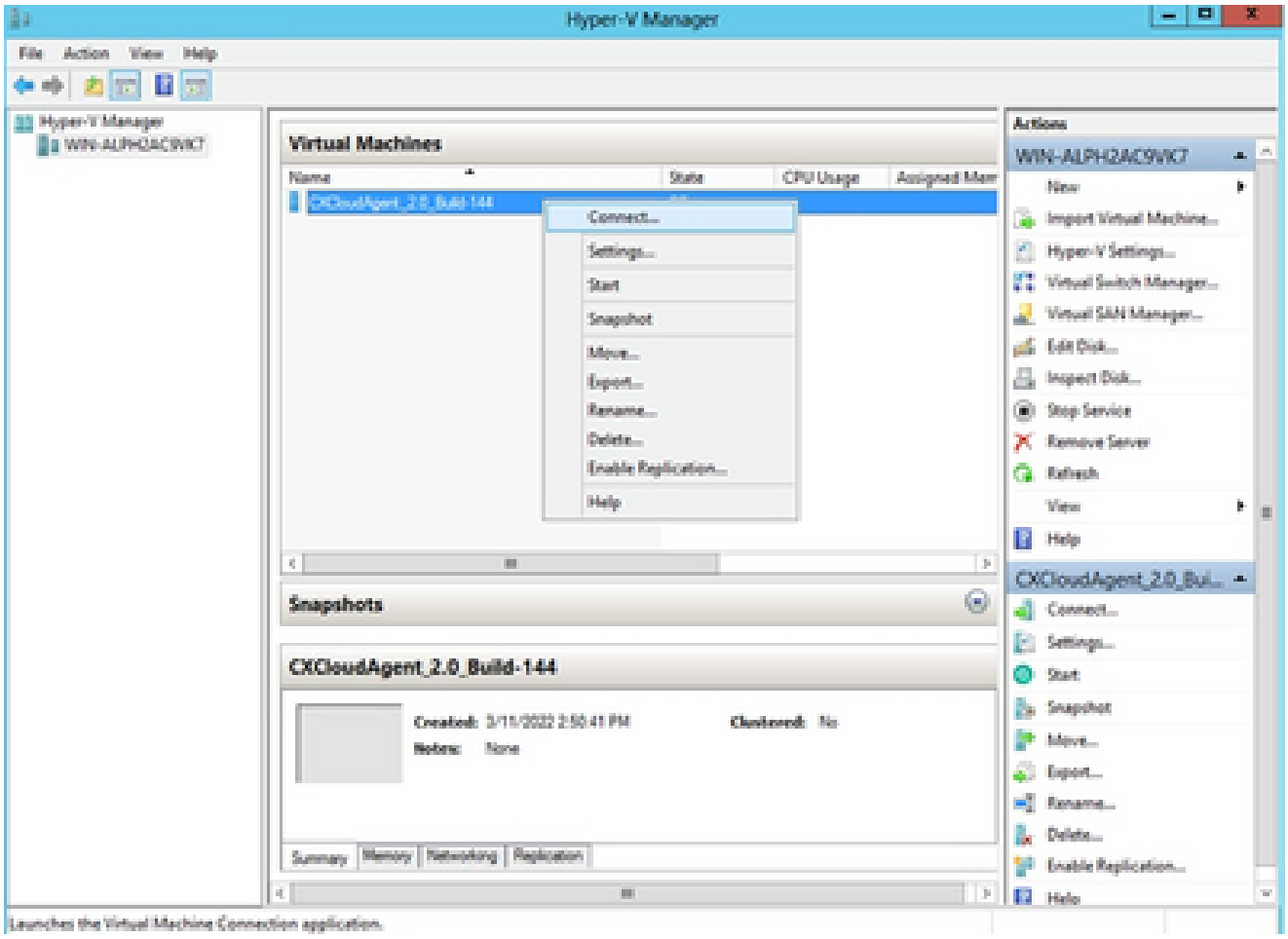
Zusammenfassung

11. Nachdem der Import erfolgreich abgeschlossen wurde, wird eine neue VM auf Hyper-V erstellt. Öffnen Sie die VM-Einstellung.
12. Wählen Sie im linken Bereich den Netzwerkadapter und anschließend aus dem Dropdown-Menü den verfügbaren virtuellen Switch aus.



Virtueller Switch

13. Wählen Sie Verbinden, um das virtuelle System zu starten.

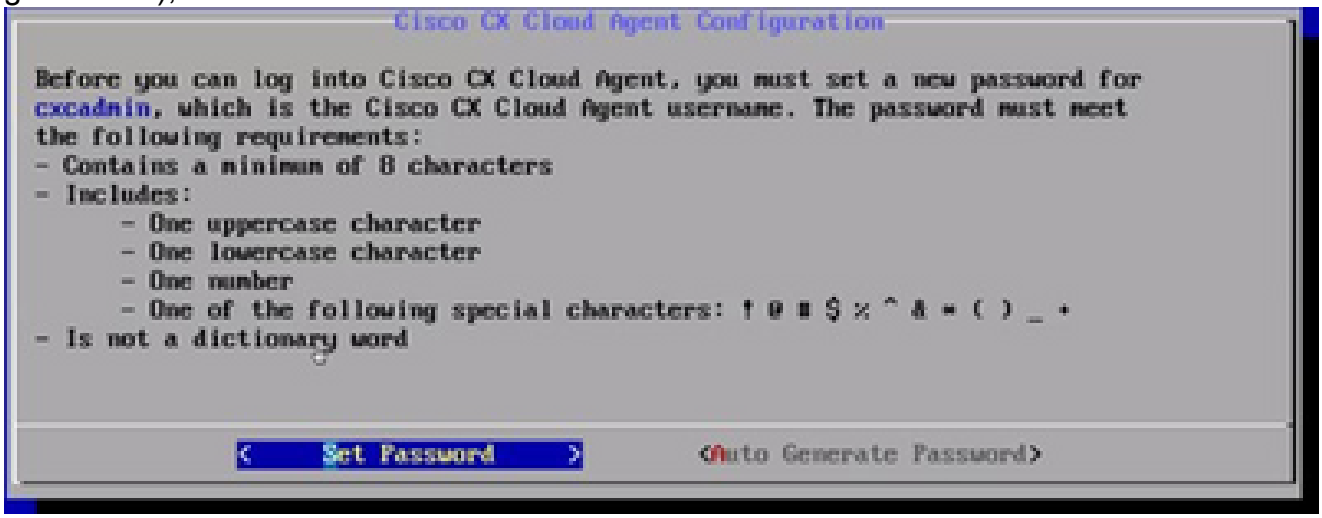


VM wird gestartet

14. Navigieren Sie zu Network Configuration, um mit den nächsten Schritten fortzufahren.

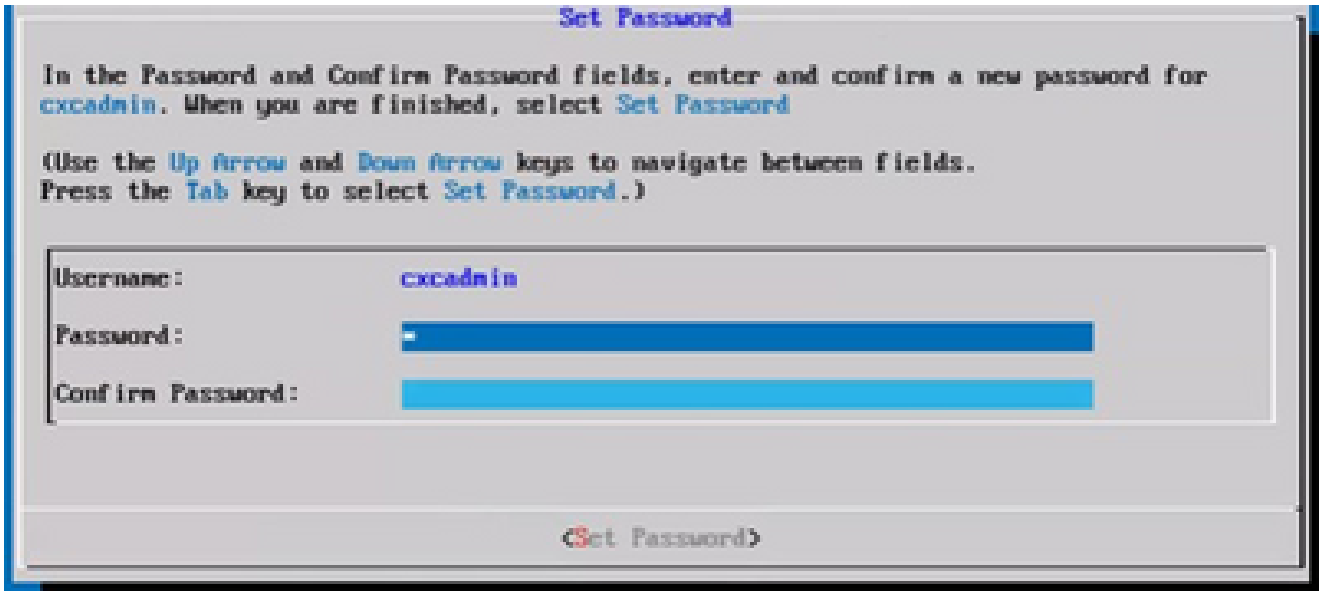
Netzwerkkonfiguration

1. Klicken Sie auf Set Password (Kennwort festlegen), um ein neues Kennwort für cxcadmin hinzuzufügen, ODER klicken Sie auf Auto Generate Password (Kennwort automatisch generieren), um ein neues Kennwort zu erhalten.



Passwort festlegen

2. Wenn Sie sich für Kennwort festlegen entscheiden, geben Sie das Kennwort für cxcadmin ein und bestätigen Sie es. Klicken Sie auf Kennwort festlegen und fahren Sie mit Schritt 3 fort.



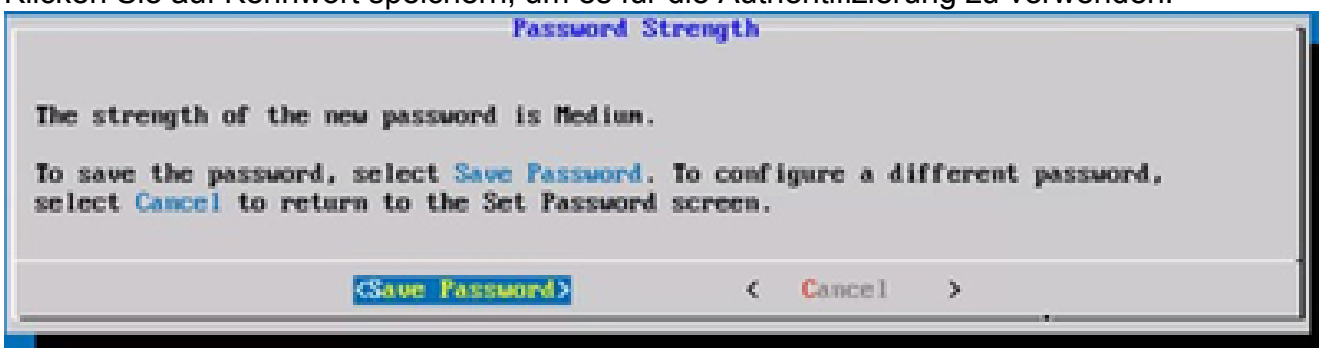
Neues Kennwort

ODER

Wenn Kennwort automatisch generieren ausgewählt ist, kopieren Sie das generierte Kennwort, und speichern Sie es zur späteren Verwendung. Klicken Sie auf Kennwort speichern und fahren Sie mit Schritt 4 fort.

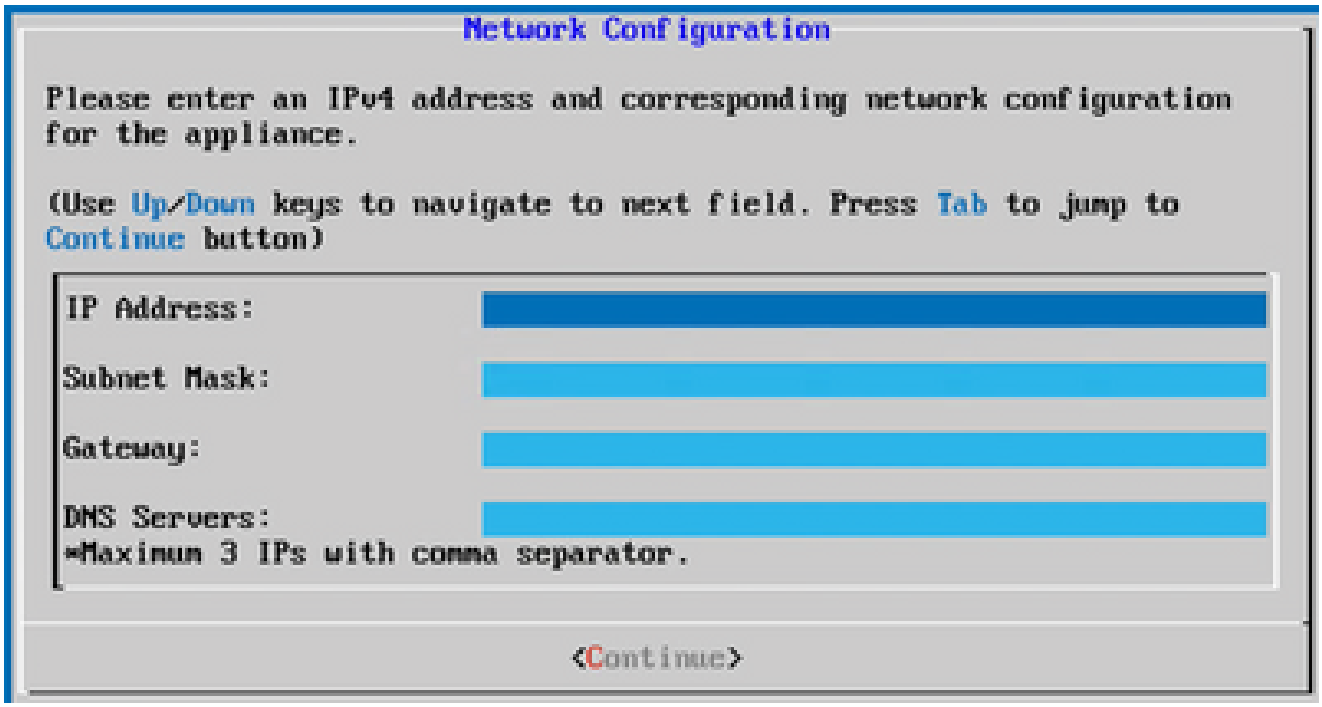
Auto Generated Password (Automatisch generiertes Kennwort)

3. Klicken Sie auf Kennwort speichern, um es für die Authentifizierung zu verwenden.



Passwort speichern

4. Geben Sie die IP-Adresse, die Subnetzmaske, den Gateway und den DNS-Server ein, und klicken Sie auf Weiter.



Netzwerkkonfiguration

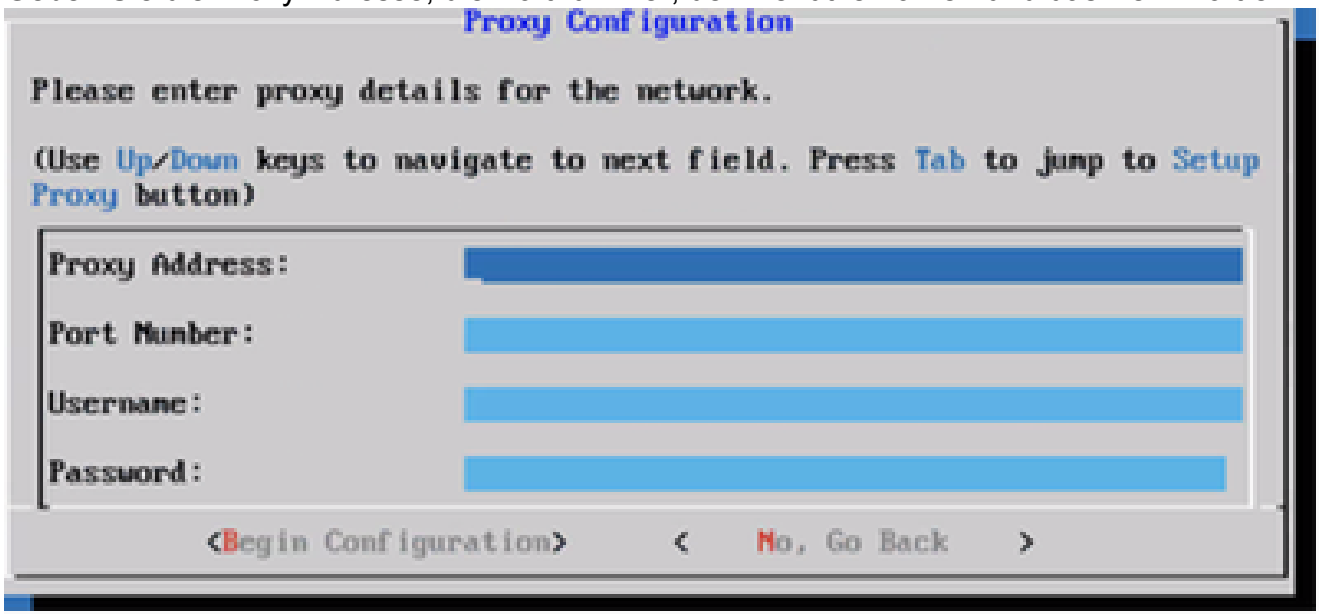
5. Bestätigen Sie die Eingaben, und klicken Sie auf Ja, weiter.

Konfiguration

6. Klicken Sie zum Festlegen der Proxydetails auf Ja, Proxy einrichten oder auf Nein, Konfiguration fortsetzen, um die Konfiguration abzuschließen, und fahren Sie mit Schritt 8 fort.

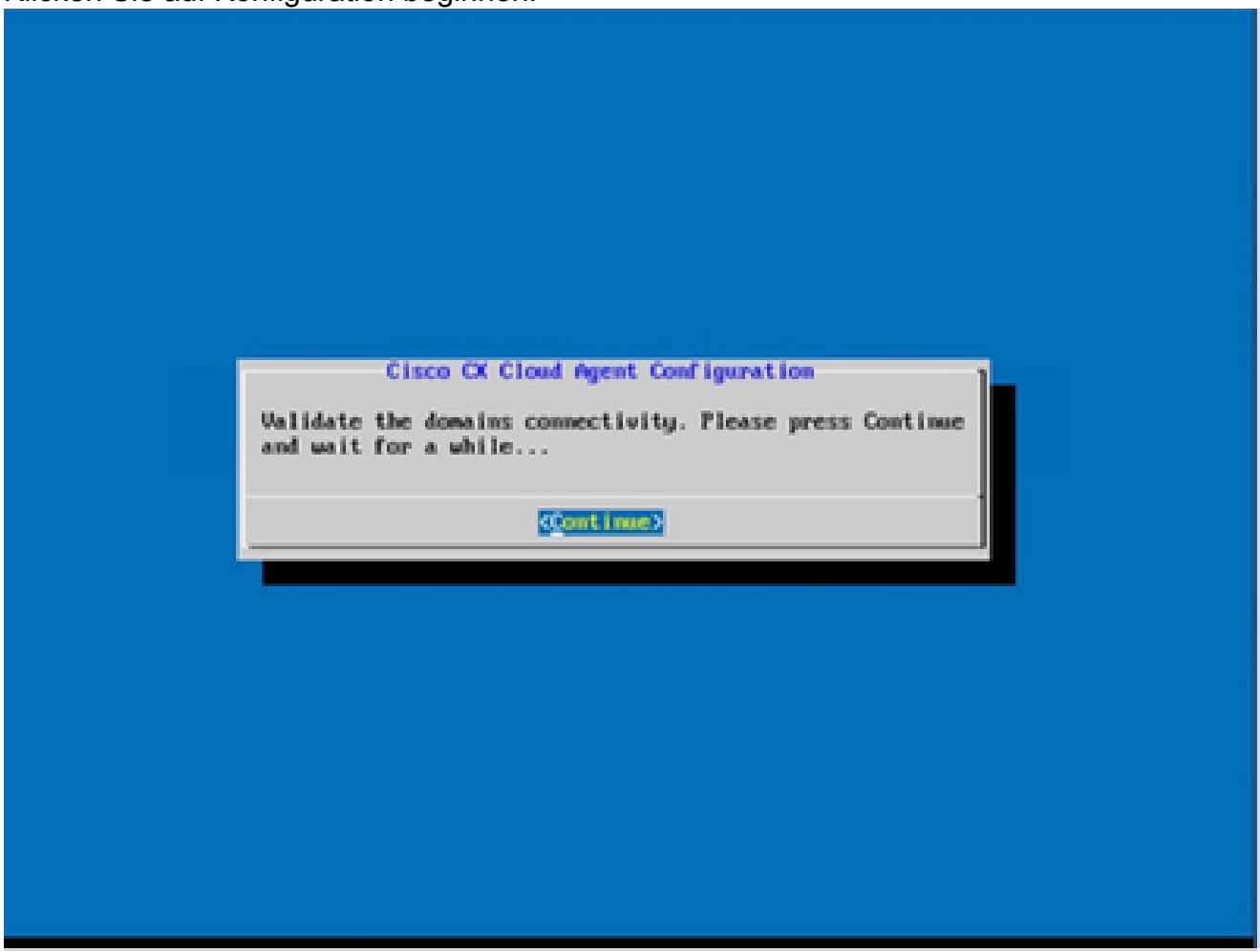
Proxy-Einrichtung

7. Geben Sie die Proxy-Adresse, die Portnummer, den Benutzernamen und das Kennwort ein.



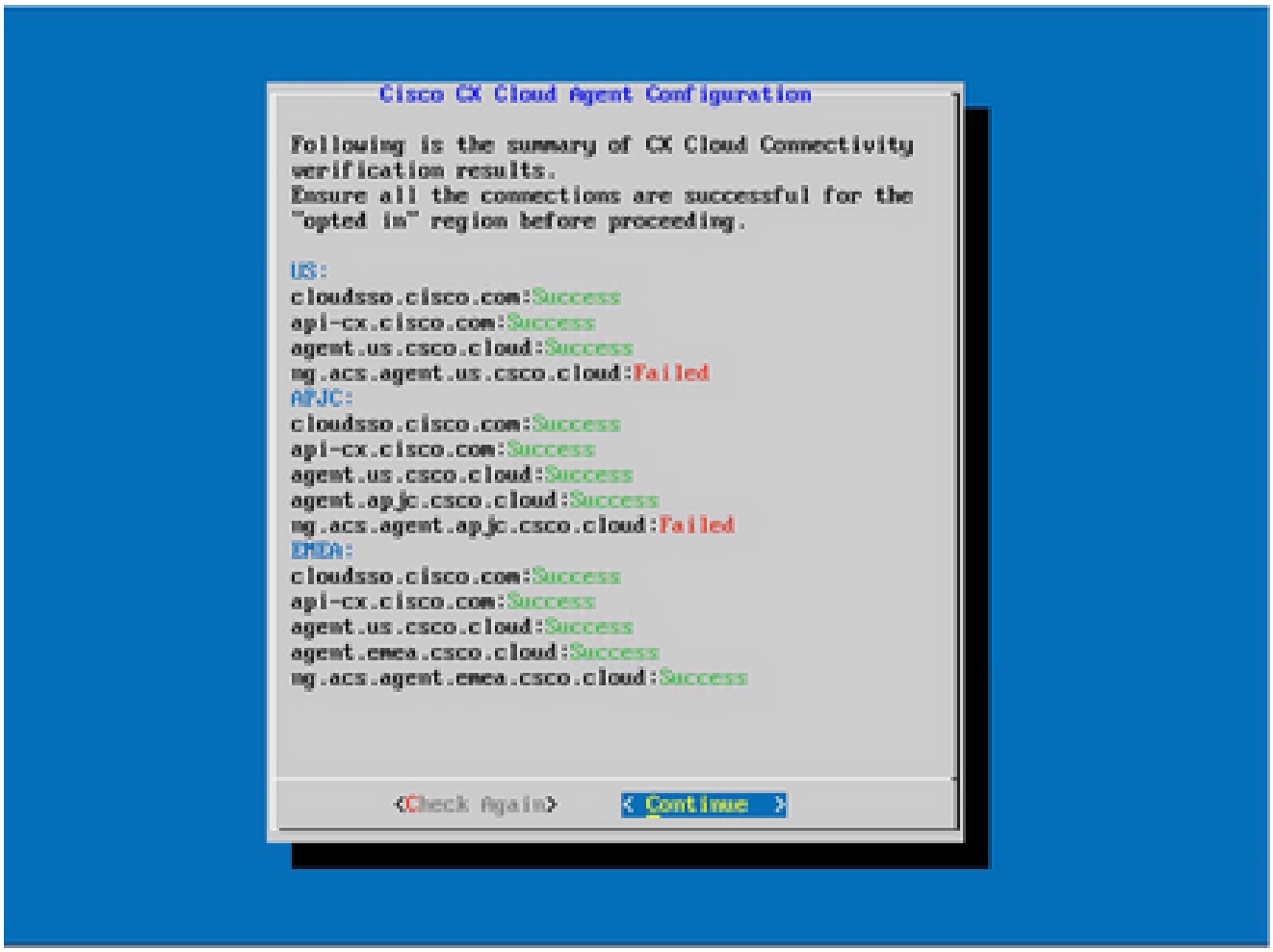
Proxy-Konfiguration

8. Klicken Sie auf Konfiguration beginnen.



Konfiguration beginnen

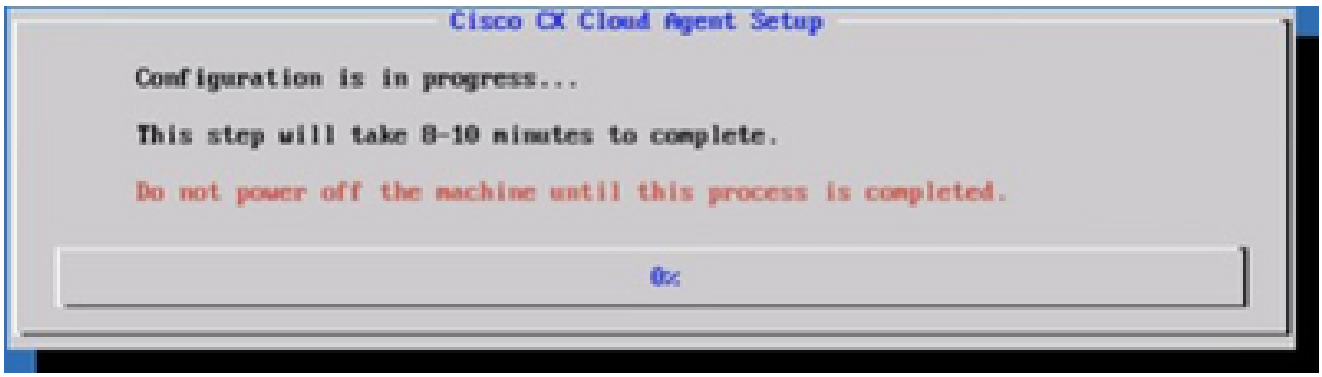
9. Klicken Sie auf Continue (Weiter).



Konfiguration wird fortgesetzt

10. Klicken Sie auf Continue (Weiter), um mit der Konfiguration fortzufahren, damit die Domäne erreicht werden kann. Die Konfiguration kann einige Minuten in Anspruch nehmen.

Hinweis: Wenn die Domänen nicht erfolgreich erreicht werden können, muss der Kunde die Erreichbarkeit der Domäne durch Änderungen an seiner Firewall korrigieren, um sicherzustellen, dass die Domänen erreichbar sind. Klicken Sie auf Erneut prüfen, sobald das Problem mit der Erreichbarkeit der Domänen behoben ist.

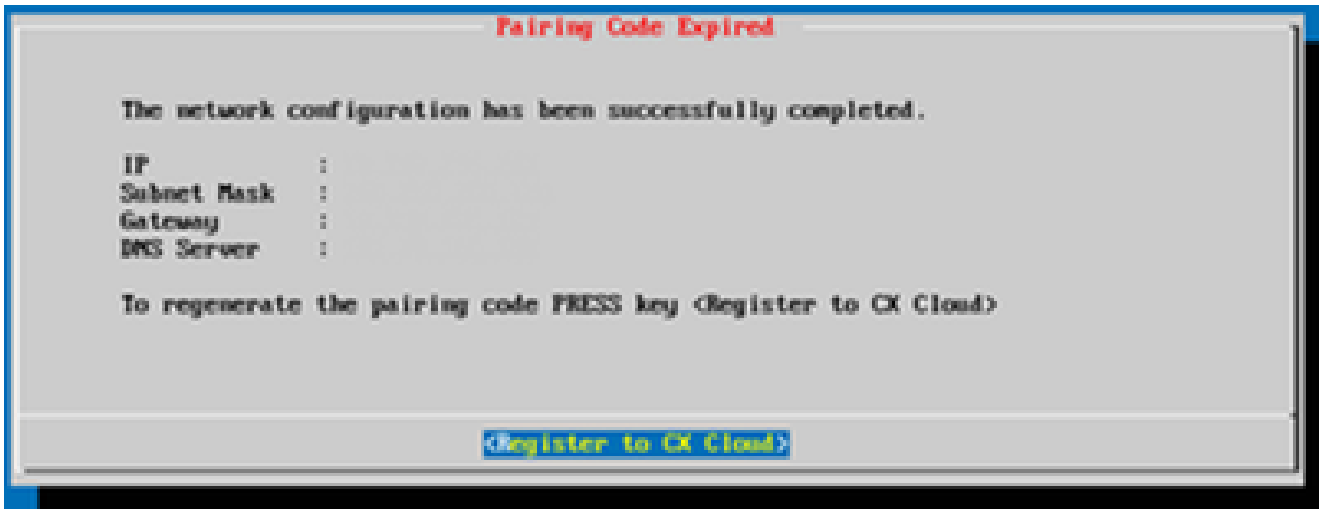


Konfiguration in Bearbeitung

11. Kopieren Sie den Kopplungscode und kehren Sie zu CX Cloud zurück, um mit der Einrichtung fortzufahren.

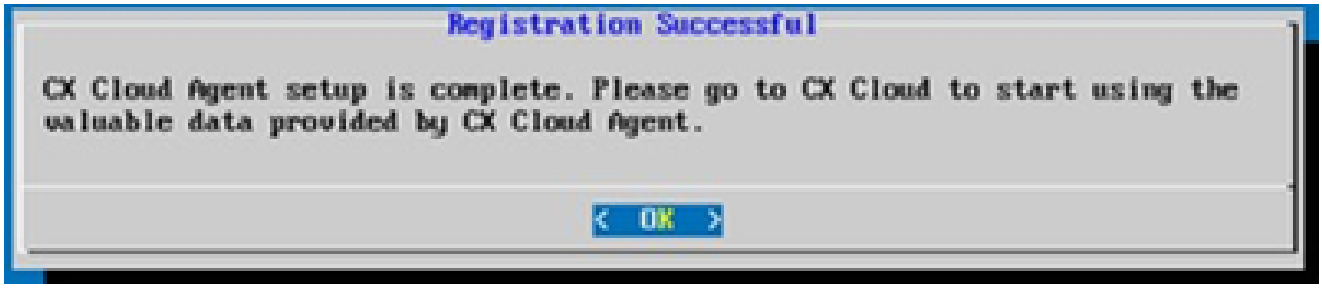
Kopplungscode

12. Wenn der Kopplungscode abläuft, klicken Sie auf Bei CX Cloud registrieren, um den Code erneut abzurufen.



Code abgelaufen

13. Klicken Sie auf OK.



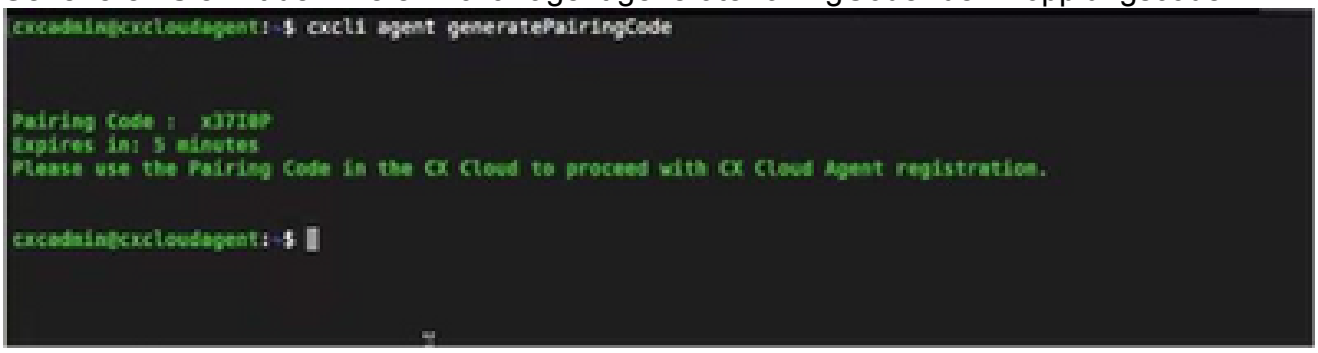
Registrierung erfolgreich

Alternativer Ansatz zum Generieren von Kopplungscode mithilfe der CLI

Benutzer können einen Kopplungscode auch mithilfe von CLI-Optionen generieren.

So generieren Sie einen Kopplungscode über die CLI:

1. Melden Sie sich mit den Anmeldeinformationen für cxcadmin-Benutzer über SSH beim Cloud Agent an.
2. Generieren Sie mit dem Befehl "cxcli agent generatePairingCode" den Kopplungscode.



Kopplungscode-CLI generieren

3. Kopieren Sie den Kopplungscode und kehren Sie zu CX Cloud zurück, um mit der Einrichtung fortzufahren.

Konfigurieren von Cisco DNA Center für die Weiterleitung von Syslog an den CX Cloud Agent

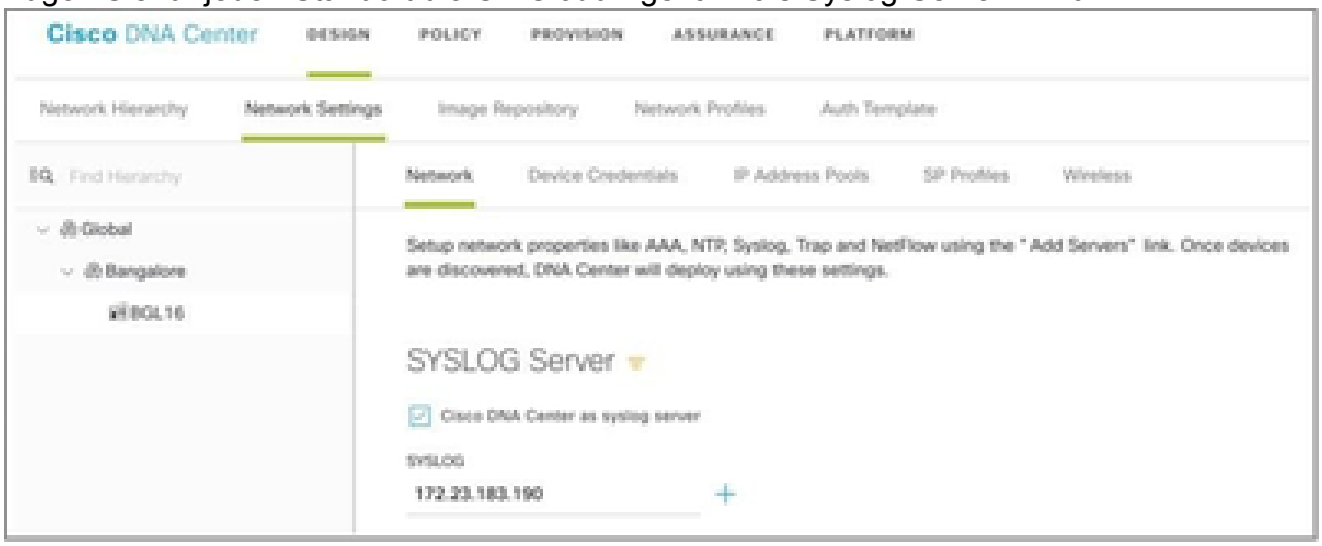
Voraussetzungen

Unterstützte Cisco DNA Center-Versionen: 2.1.2.0 bis 2.2.3.5, 2.3.3.4 bis 2.3.3.6, 2.3.5.0 und Cisco DNA Center Virtual Appliance

Syslog-Weiterleitungseinstellung konfigurieren

So konfigurieren Sie Syslog Forwarding to CX Cloud Agent im Cisco DNA Center:

1. Starten Sie Cisco DNA Center.
2. Gehen Sie zu Design > Netzwerkeinstellungen > Netzwerk.
3. Fügen Sie für jeden Standort die CX Cloud Agent-IP als Syslog-Server hinzu.



Hinweise:
Nach der Konfiguration werden alle Geräte, die diesem Standort zugeordnet sind, so konfiguriert, dass sie Syslog mit der für CX Cloud Agent kritischen Stufe senden. Die Geräte müssen einem Standort zugeordnet werden, um die Syslog-Weiterleitung vom Gerät an den CX Cloud Agent zu aktivieren. Wenn eine Syslog-Servereinstellung aktualisiert wird, werden alle Geräte, die diesem Standort zugeordnet sind, automatisch auf die kritische Standardstufe gesetzt.

Konfigurieren anderer Ressourcen für die Weiterleitung von Syslog an den CX Cloud Agent

Die Geräte müssen so konfiguriert werden, dass sie Syslog-Meldungen an den CX Cloud Agent senden, um die Fehlerverwaltungsfunktion von CX Cloud zu verwenden.

Hinweis: Nur Campus Success Track Level 2-Geräte sind zur Konfiguration anderer Ressourcen für die Weiterleitung von Syslog berechtigt.

Vorhandene Syslog-Server mit Weiterleitungsfunktion

Führen Sie die Konfigurationsanweisungen für die Syslog-Serversoftware aus, und fügen Sie die IP-Adresse des CX Cloud Agent als neues Ziel hinzu.

Hinweis: Stellen Sie beim Weiterleiten von Syslogs sicher, dass die Quell-IP-Adresse der ursprünglichen Syslog-Nachricht beibehalten wird.

Vorhandene Syslog-Server ohne Weiterleitungsfunktion ODER ohne Syslog-Server

Konfigurieren Sie jedes Gerät so, dass Syslogs direkt an die IP-Adresse des CX Cloud-Agenten gesendet werden. Spezifische Konfigurationsschritte finden Sie in dieser Dokumentation.

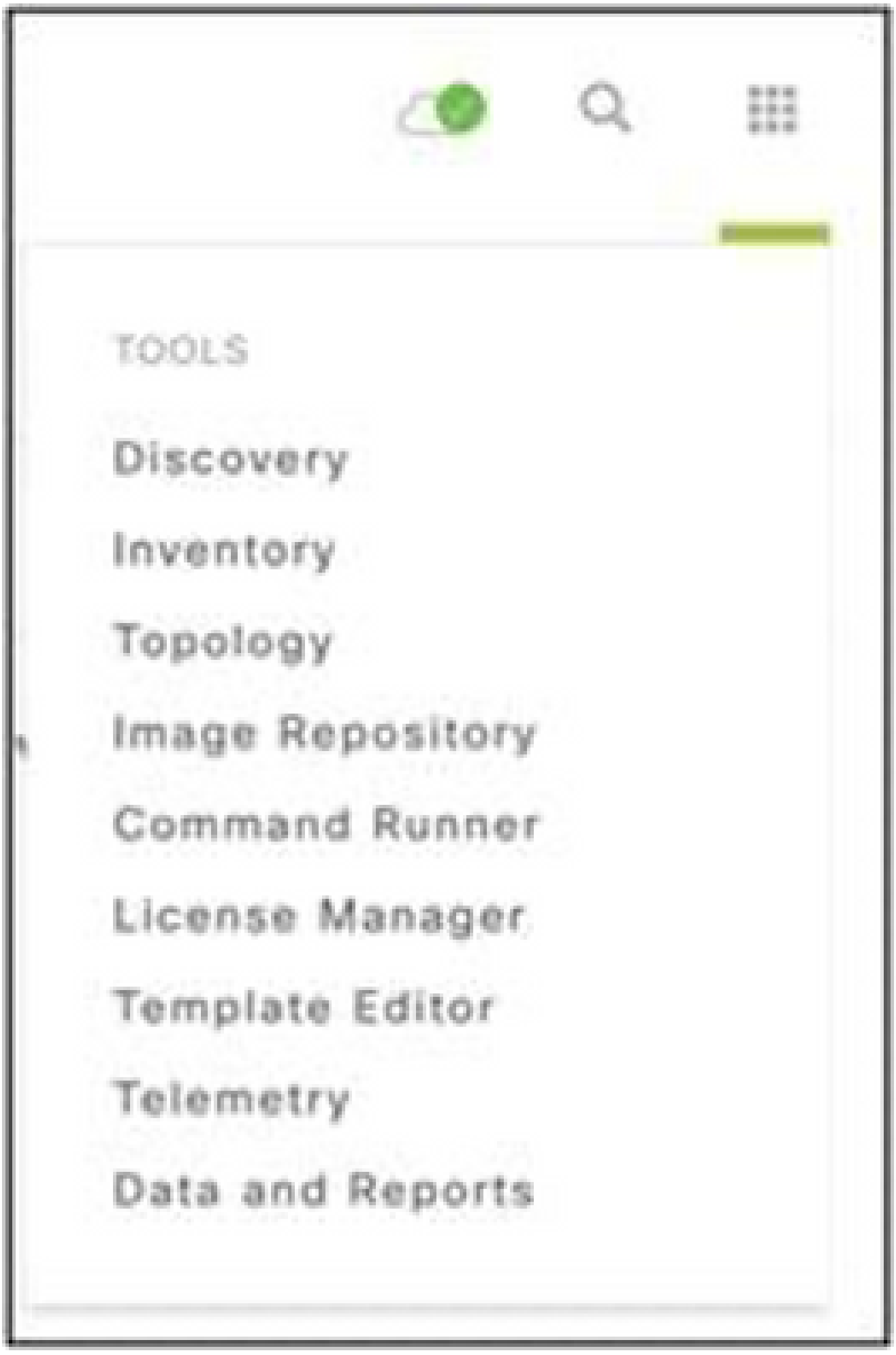
Cisco IOS® XE Konfigurationsleitfaden

Konfigurationsanleitung für den AireOS Wireless Controller

Syslog-Einstellungen auf Informationsebene aktivieren

So machen Sie die Syslog-Informationen sichtbar:

1. Navigieren Sie zu Extras> Telemetrie.


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

Menü Extras

2. Wählen und erweitern Sie die Websiteansicht, und wählen Sie eine Website aus der Websitehierarchie aus.

Standortansicht

3. Wählen Sie den erforderlichen Standort aus, und aktivieren Sie das Kontrollkästchen Gerätename für alle Geräte.

4. Wählen Sie im Dropdown-Menü Aktionen die Option Optimale Transparenz aus.

Aktionen

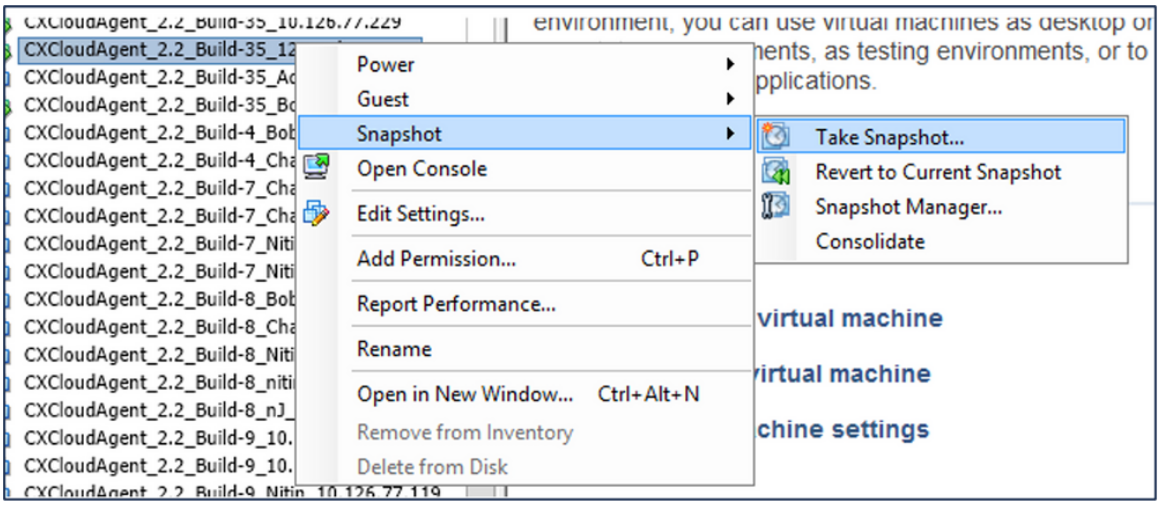
Backup und Wiederherstellung des CX Cloud VM

Es wird empfohlen, den Status und die Daten einer CX Cloud Agent VM zu einem bestimmten Zeitpunkt mithilfe der Snapshot-Funktion beizubehalten. Diese Funktion erleichtert die Wiederherstellung des virtuellen Systems der CX Cloud auf den spezifischen Zeitpunkt, zu dem der Snapshot erstellt wird.

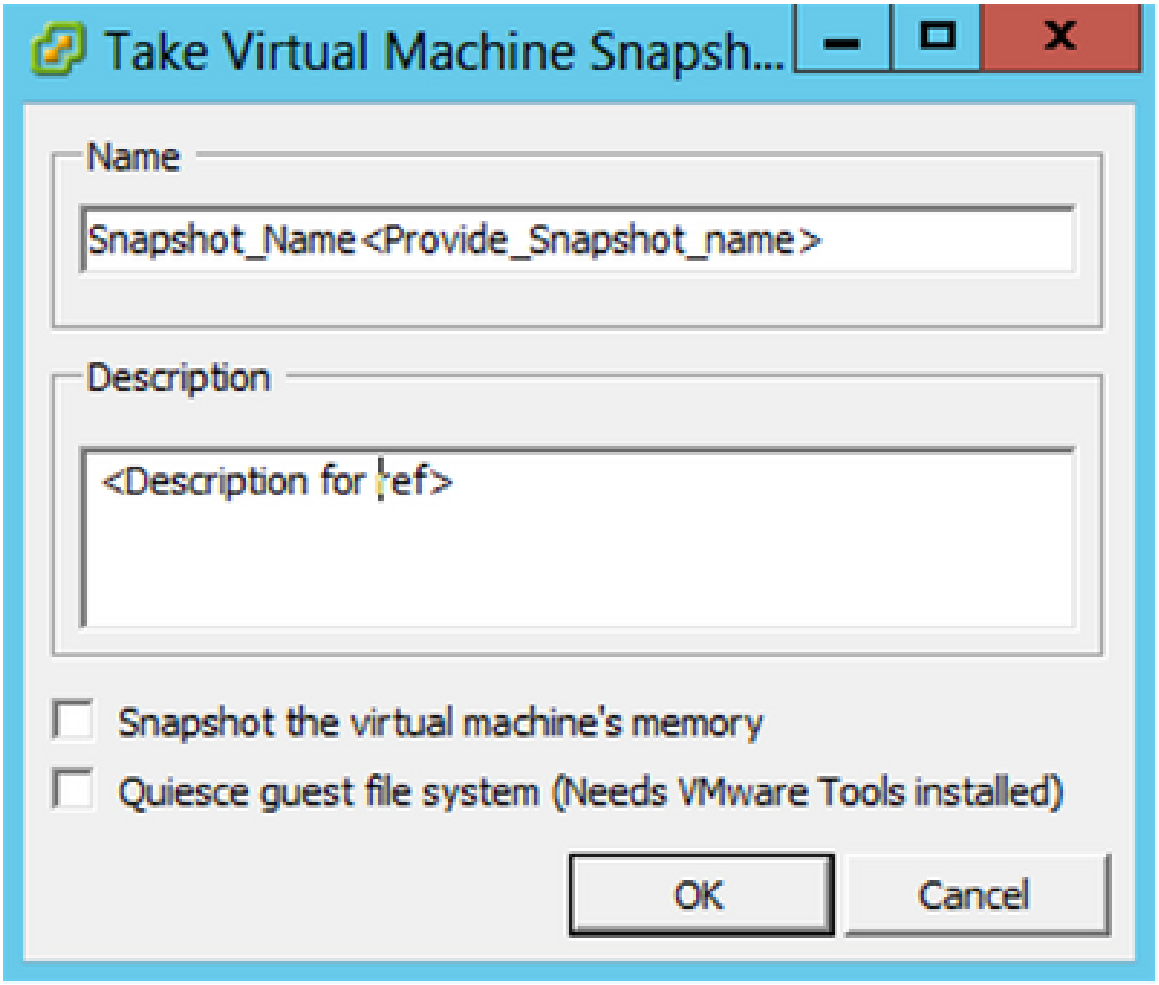
Sichern

So sichern Sie die CX Cloud VM:

1. Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie Snapshot > Snapshot erstellen aus. Das Fenster Snapshot des virtuellen Computers erstellen wird geöffnet.



VM auswählen



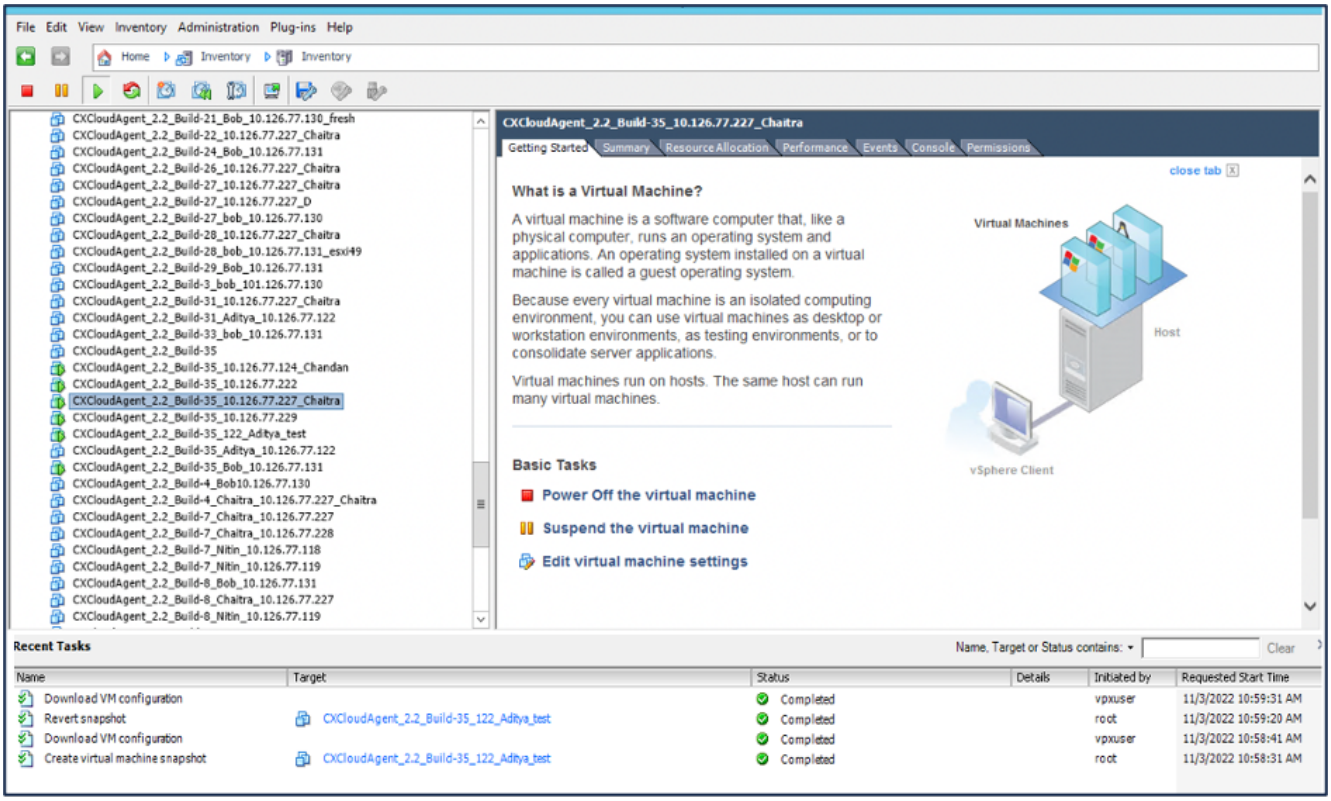
Snapshot des virtuellen Systems erstellen

2. Geben Sie einen Namen und eine Beschreibung ein.

✎ Hinweis: Stellen Sie sicher, dass das Kontrollkästchen Snapshot des Speichers des virtuellen Systems deaktiviert ist.

---

3. Klicken Sie auf OK. Der Status Snapshot des virtuellen Computers erstellen wird in der Liste Zuletzt durchgeführte Aufgaben als Abgeschlossen angezeigt.

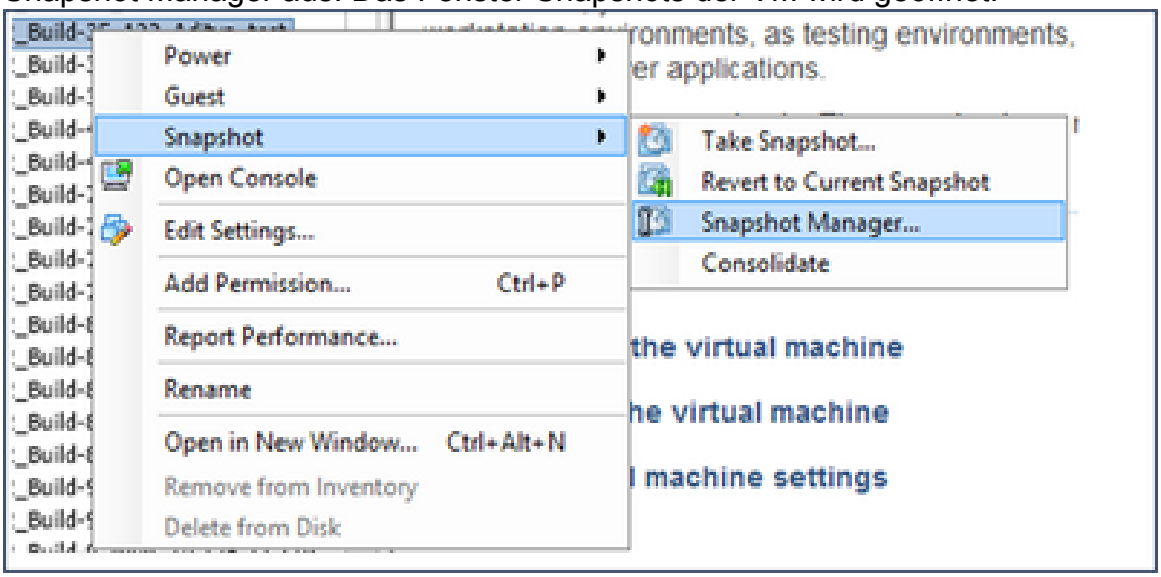


Zuletzt durchgeführte Aufgaben

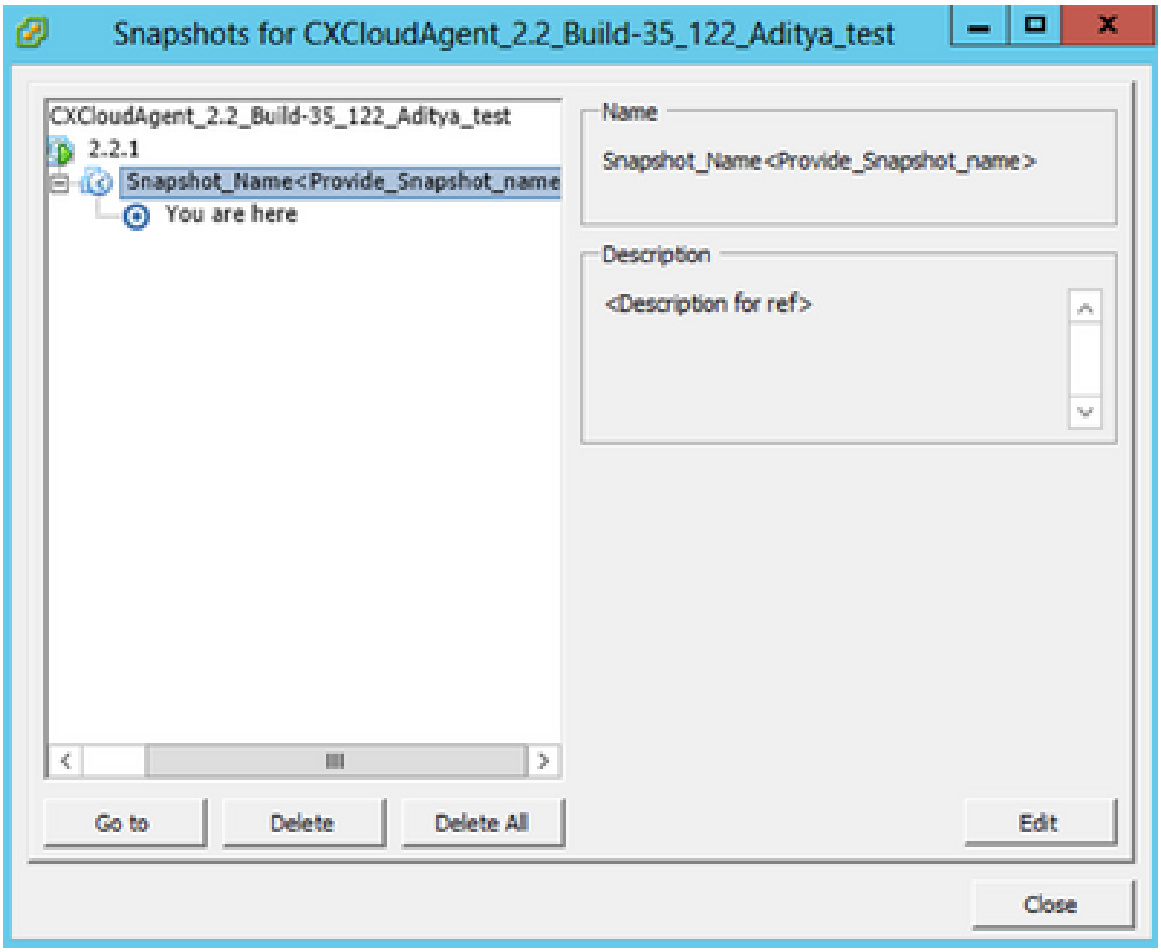
Wiederherstellen

So stellen Sie die CX Cloud VM wieder her:

1. Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie Snapshot > Snapshot Manager aus. Das Fenster Snapshots der VM wird geöffnet.

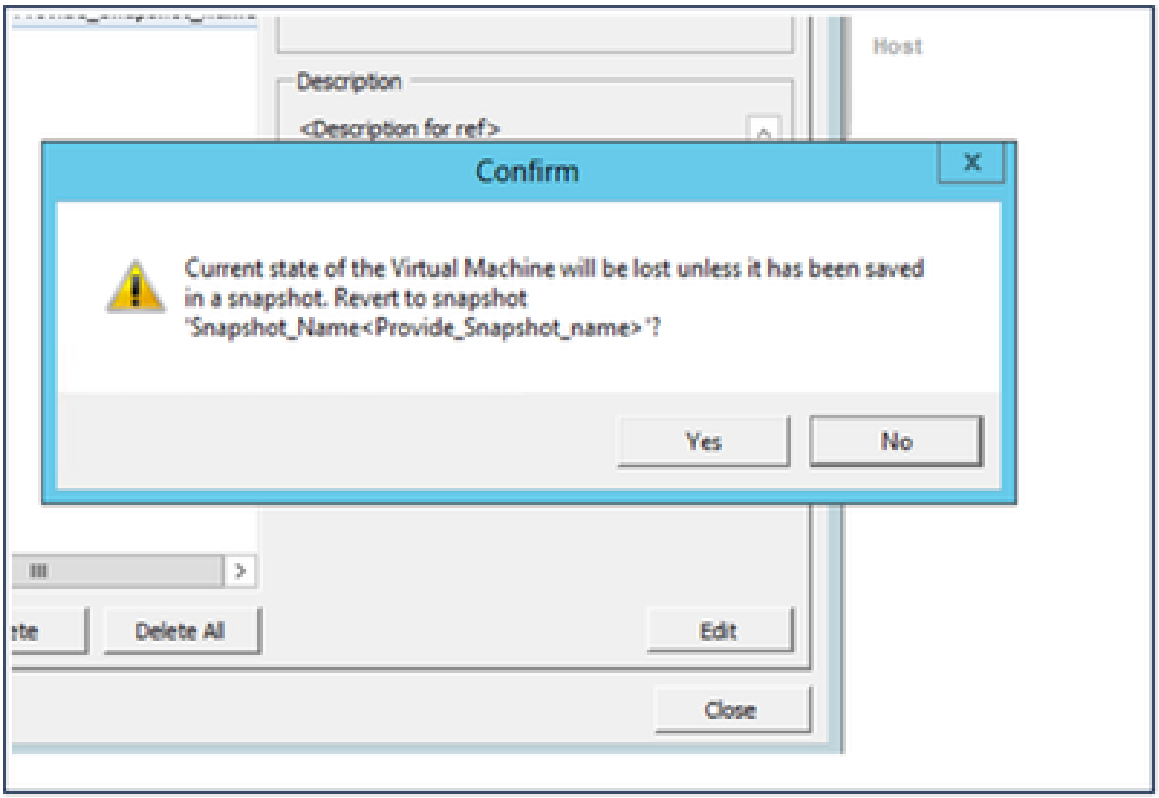


Fenster "VM auswählen"



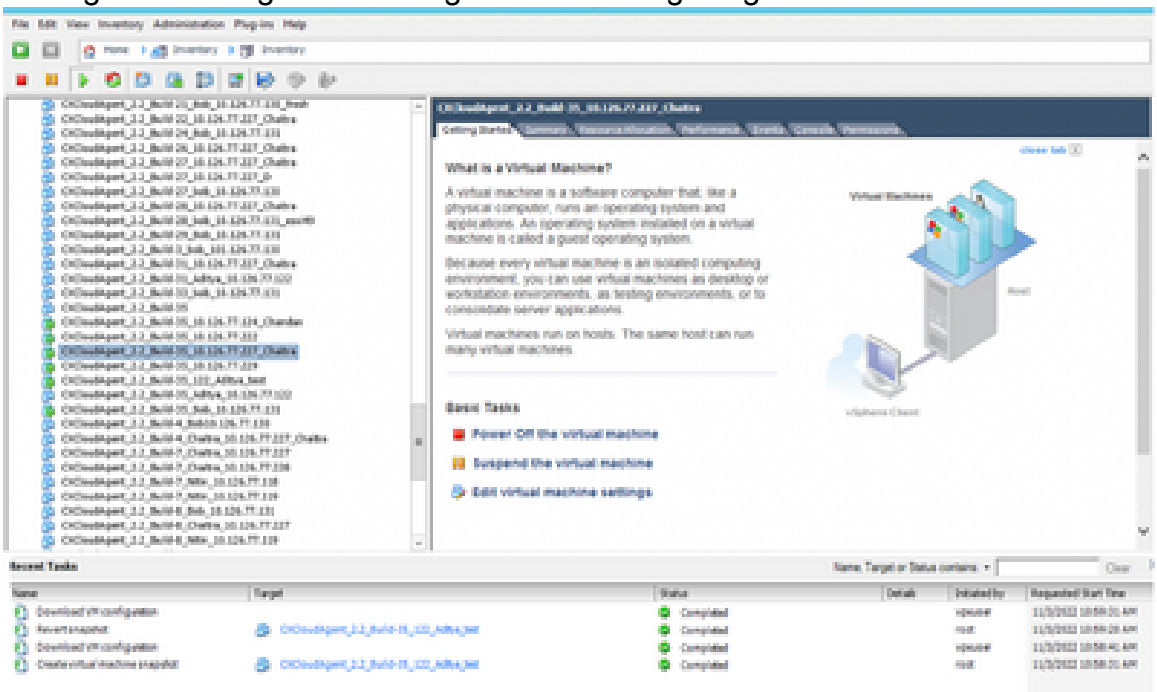
Fenster Snapshots

2. Klicken Sie auf Gehe zu. Das Fenster Bestätigen wird geöffnet.



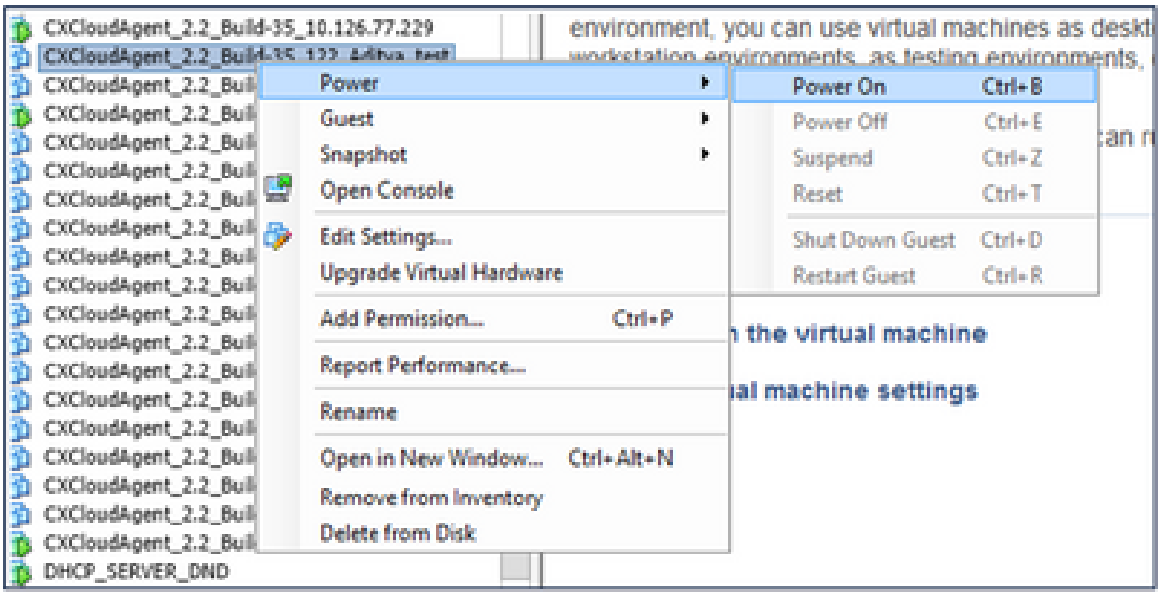
Fenster bestätigen

3. Klicken Sie auf Ja. Der Status Snapshot zurücksetzen wird in der Liste Zuletzt durchgeführte Aufgaben als Abgeschlossen angezeigt.



Zuletzt durchgeführte Aufgaben

4. Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie Power > Power On (Einschalten) aus, um die VM einzuschalten.



Sicherheit

CX Cloud Agent gewährleistet dem Kunden umfassende Sicherheit. Die Verbindung zwischen CX Cloud und CX Cloud Agent ist durch TLS gesichert. Der Standard-SSH-Benutzer des Cloud Agent ist auf die Ausführung nur grundlegender Vorgänge beschränkt.

Personen- und Gebäudeschutz

Bereitstellung eines OVA-Images des CX Cloud Agent in einem sicheren VMware-Serverunternehmen. Die OVA wird über das Cisco Software Download Center sicher freigegeben. Für das Bootloader-Kennwort (Einzelbenutzermodus) wird ein zufälliges, eindeutiges Kennwort festgelegt. Benutzer müssen in dieser FAQ dieses Bootloader-Passwort (Einzelbenutzermodus) festlegen.

Kontosicherheit

Während der Bereitstellung wird das cxcadmin-Benutzerkonto erstellt. Benutzer sind gezwungen, während der Erstkonfiguration ein Kennwort festzulegen. cxcadmin-Benutzer/Anmeldeinformationen werden verwendet, um sowohl auf die CX Cloud Agent-APIs zuzugreifen als auch um sich über SSH mit der Appliance zu verbinden.

cxcadmin-Benutzer haben eingeschränkten Zugriff mit den geringsten Rechten. Das cxcadmin-Kennwort folgt der Sicherheitsrichtlinie und wird einseitig gehasht mit einer Ablaufzeit von 90 Tagen. cxcadmin-Benutzer können einen cxcroot-Benutzer mit dem Dienstprogramm "remoteaccount" erstellen. cxcadmin-Benutzer können Root-Berechtigungen erhalten.

Netzwerksicherheit

Der Zugriff auf die CX Cloud Agent VM erfolgt über SSH mit cxcadmin-Benutzeranmeldeinformationen. Eingehende Ports sind auf 22 (SSH), 514 (Syslog) beschränkt.

Authentifizierung

Passwortbasierte Authentifizierung: Die Appliance unterhält einen einzelnen Benutzer (cxcadmin), über den der Benutzer sich authentifizieren und mit dem CX Cloud Agent kommunizieren kann.

- Privilegierte Aktionen auf der Appliance mit SSH rooten.

cxcadmin-Benutzer können cxcroot-Benutzer mit dem Dienstprogramm remoteAccount erstellen. Dieses Dienstprogramm zeigt ein verschlüsseltes RSA/ECB/PKCS1v1_5-Kennwort an, das nur vom SWIM-Portal entschlüsselt werden kann (DECRYPT-Anforderungsformular). Nur autorisierte Mitarbeiter haben Zugriff auf dieses Portal. cxcroot-Benutzer können mit diesem entschlüsselten Kennwort Root-Berechtigungen erlangen. Die Passphrase ist nur zwei Tage gültig. Benutzer von cxcadmin müssen das Konto neu erstellen und das Kennwort beim Ablauf des Kennworts für den SWIM-Portal-Beitrag abrufen.

Härtung

Die CX Cloud Agent-Appliance folgt den Härtungsstandards von Center of Internet Security.

Datensicherheit

Die CX Cloud Agent-Appliance speichert keine persönlichen Kundeninformationen. Die Anwendung für Geräteanmeldeinformationen (die als einer der PODs ausgeführt wird) speichert verschlüsselte Serveranmeldeinformationen in einer sicheren Datenbank. Die erfassten Daten werden in keiner Form innerhalb der Appliance gespeichert, außer vorübergehend, wenn sie verarbeitet werden. Telemetriedaten werden so bald wie möglich nach Abschluss der Erfassung in die CX Cloud hochgeladen und umgehend aus dem lokalen Speicher gelöscht, nachdem bestätigt wurde, dass der Upload erfolgreich war.

Datenübertragung

Das Registrierungspaket enthält das erforderliche eindeutige X.509-Gerätezertifikat sowie Schlüssel zum Aufbau einer sicheren Verbindung mit Iot Core. Mit diesem Agent wird eine sichere Verbindung mithilfe von Message Queuing Telemetry Transport (MQTT) over Transport Layer Security (TLS) v1.2 hergestellt.

Protokolle und Überwachung

Die Protokolle enthalten keine persönlichen Daten (PII). Überwachungsprotokolle erfassen alle sicherheitsrelevanten Aktionen, die auf der CX Cloud Agent-Appliance ausgeführt werden.

Cisco Telemetrie-Befehle

CX Cloud ruft Asset-Telemetrie mithilfe der APIs und Befehle ab, die in den Cisco Telemetry Commands aufgeführt sind. Dieses Dokument kategorisiert Befehle nach ihrer Anwendbarkeit auf das Cisco DNA Center-Inventar, die Diagnose-Bridge, Intersight, Compliance Insights, Faults und alle anderen vom CX Cloud Agent erfassten Telemetriequellen.

Vertrauliche Informationen aus der Asset-Telemetrie werden vor der Übertragung in die Cloud maskiert. Der CX Cloud Agent maskiert vertrauliche Daten für alle erfassten Ressourcen, die Telemetrie direkt an den CX Cloud Agent senden. Dazu gehören Kennwörter, Schlüssel, Community-Strings, Benutzernamen usw. Controller bieten Datenmaskierung für alle vom Controller verwalteten Ressourcen, bevor diese Informationen an den CX Cloud Agent übertragen werden. In einigen Fällen kann die Telemetrie der vom Controller verwalteten Ressourcen weiter anonymisiert werden. Weitere Informationen zur Anonymisierung der Telemetrie finden Sie in der entsprechenden Produktsupport-Dokumentation (z. B. im Abschnitt Anonymisierungsdaten im Cisco DNA Center Administrator Guide).

Obwohl die Liste der Telemetrie-Befehle nicht angepasst und die Datenmaskierungsregeln nicht geändert werden können, können Kunden steuern, auf welche Ressourcen die Telemetrie-CX-Cloud zugreift. Hierzu geben sie Datenquellen an, wie in der Produktsupportdokumentation für Controller-verwaltete Geräte oder im Abschnitt "Verbinden von Datenquellen" dieses Dokuments (für andere von CX Cloud Agent erfasste Ressourcen) beschrieben.

Sicherheitszusammenfassung

Sicherheitsfunktionen	Beschreibung
Bootloader-Kennwort	Für das Bootloader-Kennwort (Einzelbenutzermodus) wird ein zufälliges, eindeutiges Kennwort festgelegt. Benutzer müssen in den FAQ sein Bootloader-Passwort (Einzelbenutzermodus) festlegen.
Benutzerzugriff	SSH: ·Für den Zugriff auf die Appliance mit dem Benutzer cxcadmin sind die Anmeldeinformationen erforderlich, die während der Installation erstellt wurden. · Für den Zugriff auf die Appliance über den Benutzer "cxcroot" müssen die Anmeldeinformationen von autorisierten Mitarbeitern über das SWIM-Portal entschlüsselt werden.
Benutzerkonten	· cxcadmin: Standard-Benutzerkonto erstellt; Benutzer kann CX Cloud Agent-Anwendungsbefehle mit cxcli ausführen und hat die geringsten Rechte auf der Appliance; cxcroot-Benutzer und sein verschlüsseltes Kennwort werden mit cxcadmin-Benutzer generiert. · cxcroot: cxcadmin kann diesen Benutzer mithilfe des Dienstprogramms remoteaccount erstellen; Benutzer können root-Berechtigungen mit diesem Konto erlangen.
cxcadmin-	·Das Kennwort wird mit SHA-256 unidirektional gehasht und sicher

Kennwortrichtlinie	gespeichert. · Mindestens acht (8) Zeichen mit drei dieser Kategorien: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
cxcroot-Kennwortrichtlinie	·Das Kennwort für cxcroot ist mit RSA/ECB/PKCS1v1_5 verschlüsselt ·Die generierte Passphrase muss im SWIM-Portal entschlüsselt werden. · Der Benutzer cxcroot und das Passwort sind zwei Tage gültig und können mit cxcadmin user regeneriert werden.
Richtlinie für das SSH-Anmeldekennwort	· Mindestens acht Zeichen, die drei der folgenden Kategorien enthalten: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. · Fünf fehlgeschlagene Anmeldeversuche sperren das System für 30 Minuten; das Kennwort läuft in 90 Tagen ab.
Ports	Offene eingehende Ports – 514 (Syslog) und 22 (SSH)
Datensicherheit	·Keine Kundeninformationen gespeichert. ·Keine Gerätedaten gespeichert. ·Anmeldeinformationen für den Cisco DNA Center-Server sind verschlüsselt und werden in der Datenbank gespeichert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.