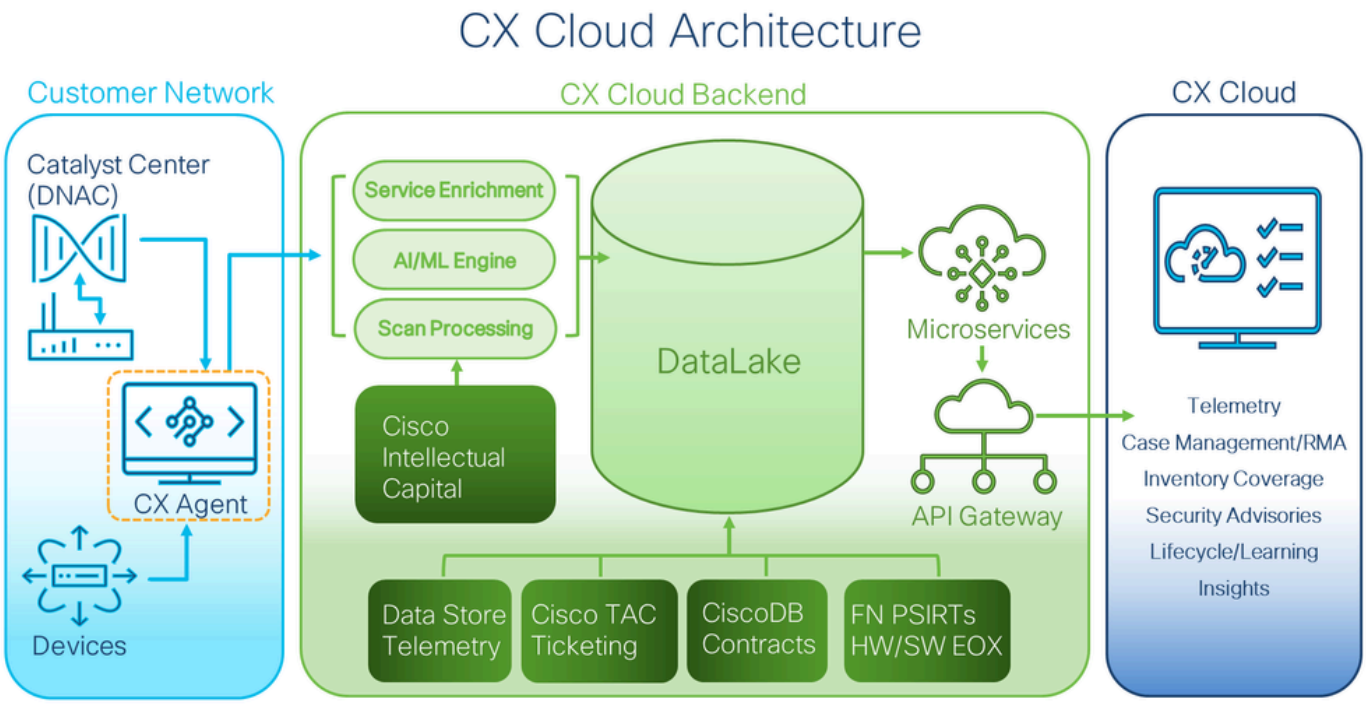
CX Agent - Übersichtshandbuch v3.1

Inhalt

Einleitung

In diesem Dokument wird der Customer Experience (CX) Agent von Cisco beschrieben. Cisco CX Agent ist eine hochgradig skalierbare Plattform, die Telemetriedaten von Kundennetzwerkgeräten erfasst, um Kunden aussagekräftige Informationen zu liefern. CX Agent ermöglicht die Umwandlung von aktiven laufenden Konfigurationsdaten in proaktive und prädiktive Einblicke, die in der CX Cloud angezeigt werden (einschließlich Success Tracks, Smart Net Total Care (SNTC) und Business Critical Services (BCS) oder Lifecycle Services (LCS)), mithilfe von künstlicher Intelligenz (KI)/maschinellem Lernen (ML).



CX Cloud-Architektur

Dieses Handbuch ist nur für CX Cloud- und Partner-Administratoren bestimmt. Benutzer mit Super User Admin (SUA)- und Admin-Rollen verfügen über die erforderlichen Berechtigungen, um die in diesem Handbuch beschriebenen Aktionen auszuführen.

Dieses Handbuch bezieht sich speziell auf CX Agent v3.1. Auf der Seite Cisco CX Agent finden Sie Informationen zu früheren Versionen.

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

Voraussetzungen

CX Agent wird als virtuelles System (VM) ausgeführt und kann als offene virtuelle Appliance (OVA) oder virtuelle Festplatte (VHD) heruntergeladen werden.

Bereitstellungsanforderungen

- Für eine Neuinstallation ist einer der folgenden Hypervisoren erforderlich:
  - VMware ESXi v5.5 oder spätere Version

    - Oracle Virtual Box v5.2.30 oder spätere Version
    - Windows Hypervisor-Version 2012 bis 2022 und Version 2025
- Die Konfigurationen in der folgenden Tabelle sind für die Bereitstellung von VM erforderlich:

Bereitstellungstyp des CX-Agenten	Anzahl der CPU-Kerne	RAM	Festplatte	* Maximale Anzahl direkter Ressourcen verbunden mit CX Agent	Unterstützte Hypervisoren
Kleine OVA	8 C	16 GB	200 GB	10,000	VMware ESXi, Oracle VirtualBox und Windows Hyper-V
Mittlere OVA	16 C	32 GB	600 GB	20,000	VMware ESXi
Große OVA	32 C	64 GB	1200 GB	50,000:	VMware ESXi

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

Hinweis:RADKit-Service ist exklusiv für CX Agent-Bereitstellungen vom Typ "Medium" und "Large OVA" verfügbar.

- Für Kunden, die ausgewiesene US-Rechenzentren als primäre Datenregion zur Speicherung von CX Cloud-Daten verwenden, muss der CX Agent in der Lage sein, eine Verbindung zu den hier dargestellten Servern herzustellen. Hierzu muss er den FQDN (Fully Qualified Domain Name) verwenden und HTTPS auf TCP-Port 443 verwenden:
    - FQDN: agent.us.csco.cloud
    - FQDN: ng.acs.agent.us.csco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Für Kunden, die ausgewiesene Rechenzentren in Europa als primäre Datenregion für die Speicherung von CX Cloud-Daten verwenden: Der CX Agent muss in der Lage sein, über den FQDN und HTTPS auf dem TCP-Port 443 eine Verbindung zu beiden hier gezeigten Servern herzustellen:
    - FQDN: agent.us.csco.cloud
    - FQDN: agent.emea.csco.cloud
    - FQDN: ng.acs.agent.emea.csco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Für Kunden, die bestimmte Rechenzentren im Asien-Pazifik-Raum als primäre Datenregion

für die Speicherung von CX Cloud-Daten verwenden: Der CX Agent muss in der Lage sein, über den FQDN und HTTPS auf dem 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 verwenden, ist die Verbindung mit FQDN: agent.us.csco.cloud ist 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.
- Für Kunden, die RADKit mit FQDN und HTTPS an TCP-Port 443 verwenden:
    - US-FQDN: radkit.us.csco.cloud
    - EMEA-FQDN: radkit.emea.cisco.cloud
    - APJC-FQDN: radkit.apjc.csco.cloud
- Damit RADKit eine Ausgabe an eine Serviceanfrage anhängen kann, muss der Zugriff auf den FQDN cxd.cisco.com für den CX-Agenten möglich 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 radkit.emea.csco.cloud Catalyst Center AMER region: ng.acs.agent.us.csco.cloud EMEA region: agent.emea.csco.cloud ng.acs.agent.emea.csco.cloud APJC region: agent.apjc.csco.cloud ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- Eine IP wird automatisch erkannt, wenn das Dynamic Host Configuration Protocol (DHCP) in der VM-Umgebung aktiviert ist. Andernfalls müssen eine kostenlose IPv4-Adresse, Subnetzmaske, IP-Adresse des Standard-Gateways und IP-Adresse des DNS-Servers (Domain Name Service) verfügbar sein.
- Nur IPv4 wird unterstützt.
- Die zertifizierten Einzelknoten- und Hochverfügbarkeits-Cluster Catalyst Center-Versionen sind 2.1.2.x bis 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x sowie Catalyst Center Virtual Appliance und

Catalyst Center Virtual Appliance.
- Wenn das Netzwerk über eine SSL-Überwachung verfügt, geben Sie die IP-Adresse des CX-Agenten 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

Zum Starten der CX Cloud benötigen Benutzer Zugriff auf folgende Domänen. Verwenden Sie nur die angegebenen Hostnamen. keine statischen IP-Adressen verwenden.

Spezifische Domänen des CX Agent-Portals

Hauptdomänen	Andere Domänen
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

Für CX Agent OVA spezifische Domänen

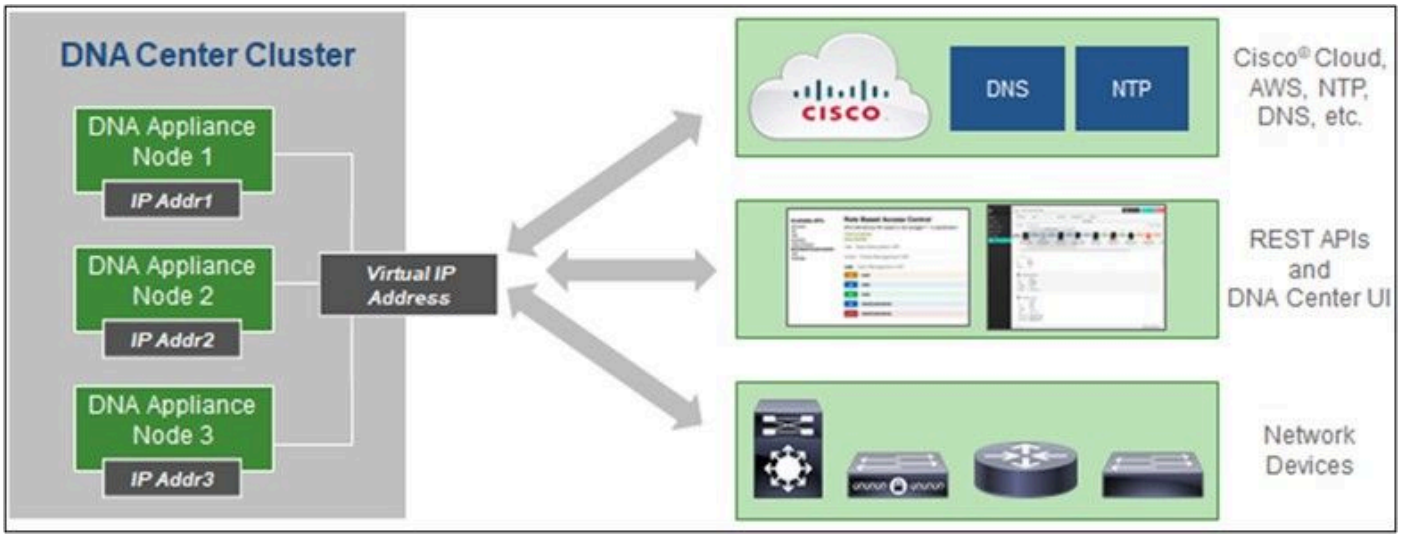
NORD- UND SÜDAMERIKA	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud

	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Anmerkung: Der ausgehende Zugriff muss bei aktivierter Umleitung auf Port 443 für die angegebenen FQDNs zugelassen werden.

Unterstützte Catalyst Center-Versionen

Die unterstützten Einzelknoten- und HA-Cluster-Versionen von Catalyst Center sind 2.1.2.x bis 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x sowie Catalyst Center Virtual Appliance und Catalyst 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 Agent unterstützten Produkte finden Sie in der Liste der unterstützten Produkte.

Upgrade/Installation von CX Agent v3.1

- Bestehende Kunden, die ein Upgrade auf die neue Version durchführen, finden weitere Informationen unter Upgrade CX Agent v3.1.
- Neue Kunden, die eine neue, flexible OVA v3.1-Installation implementieren, sollten sich an Adding CX Agent wenden.

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.

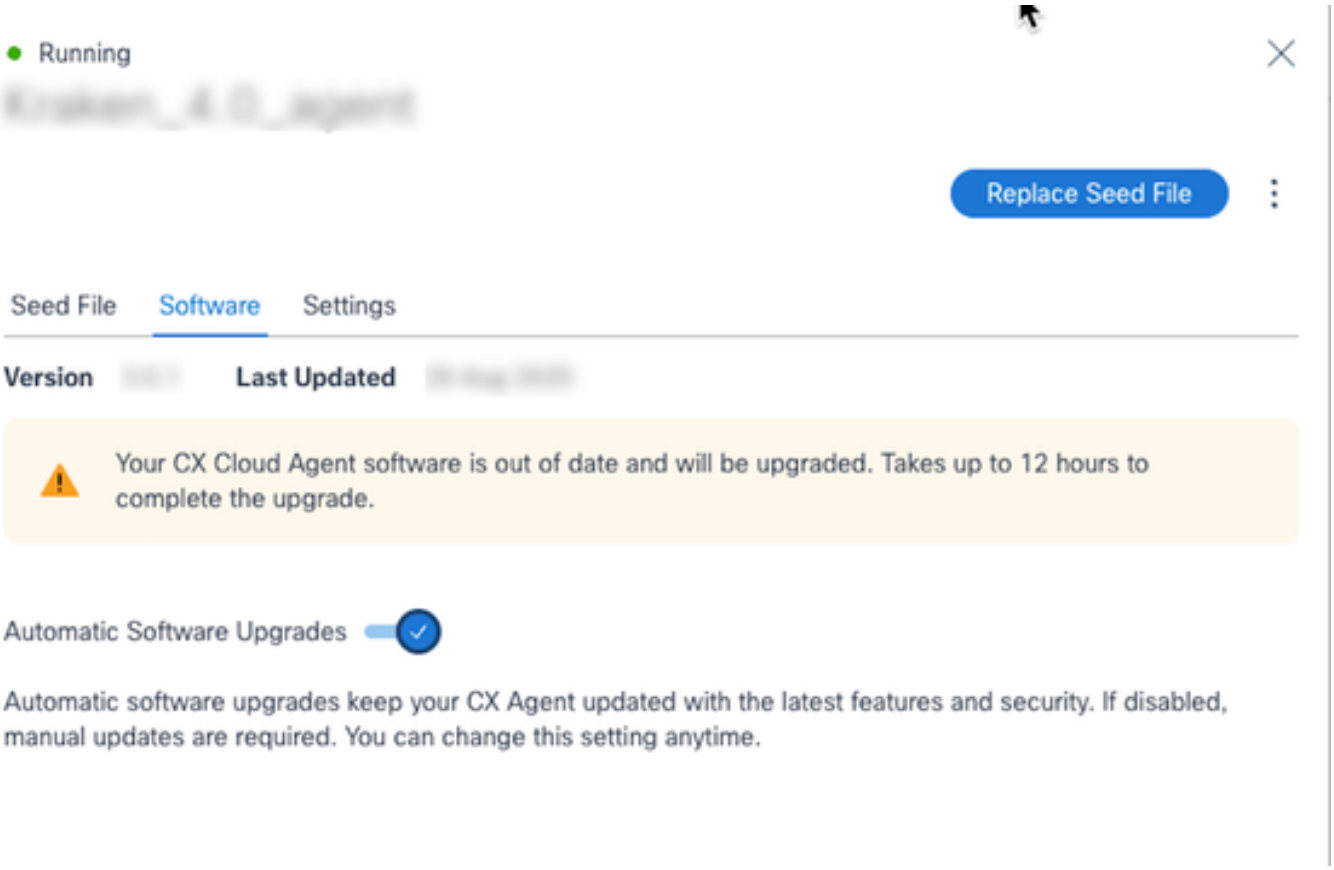
Informationen zum Upgrade der vorhandenen VM-Konfiguration von klein auf mittel oder groß finden Sie im Abschnitt Upgrading CX Agent VMs to medium and large configuration.

Upgrade auf CX Agent v3.1

Bestehende Kunden können ein Upgrade auf die neueste Version durchführen, indem sie automatische Upgrades aktivieren oder ein manuelles Upgrade von der vorhandenen Version durchführen.

Automatische Upgrades

Kunden können den Umschalter "Automatisches Software-Upgrade" aktivieren, um sicherzustellen, dass ihr System aktualisiert wird, wenn die neuen Versionen veröffentlicht werden. Diese Option ist standardmäßig für neue Installationen aktiviert, kann jedoch jederzeit geändert werden, um sie an Unternehmensrichtlinien anzupassen oder um Upgrades während geplanter Wartungsfenster zu planen.



Automatische Upgrades

Hinweis: Die automatischen Upgrades sind standardmäßig für vorhandene CX Agent-

Instanzen deaktiviert, Benutzer können sie jedoch jederzeit aktivieren.

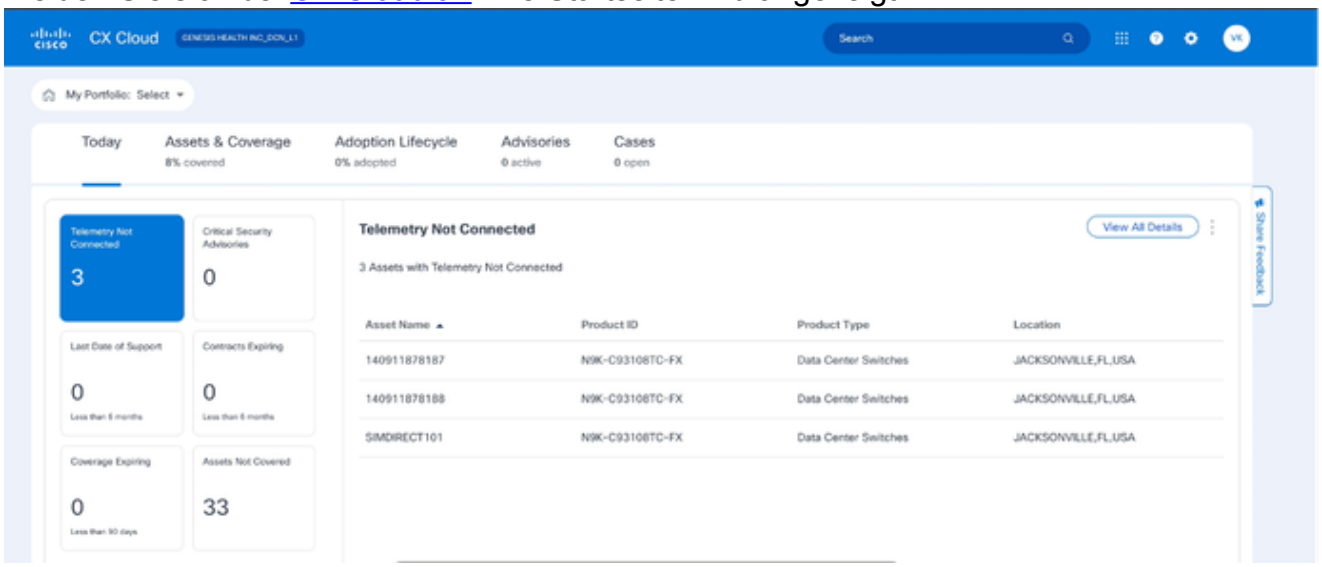
Manuelle Upgrades

Kunden, die keine automatischen Upgrades verwenden möchten und die automatischen Software-Upgrades nicht aktiviert haben, können die Aktualisierung manuell vornehmen. CX Agent v2.4.x und höher unterstützen ein direktes Upgrade auf v3.1, indem Sie die in diesem Abschnitt beschriebenen Schritte ausführen.

Hinweis: Kunden mit CX Agent v2.3.x und niedriger sollten vor dem Upgrade auf v3.1 inkrementell auf v2.4.x aktualisieren oder eine neue OVA-Installation durchführen.

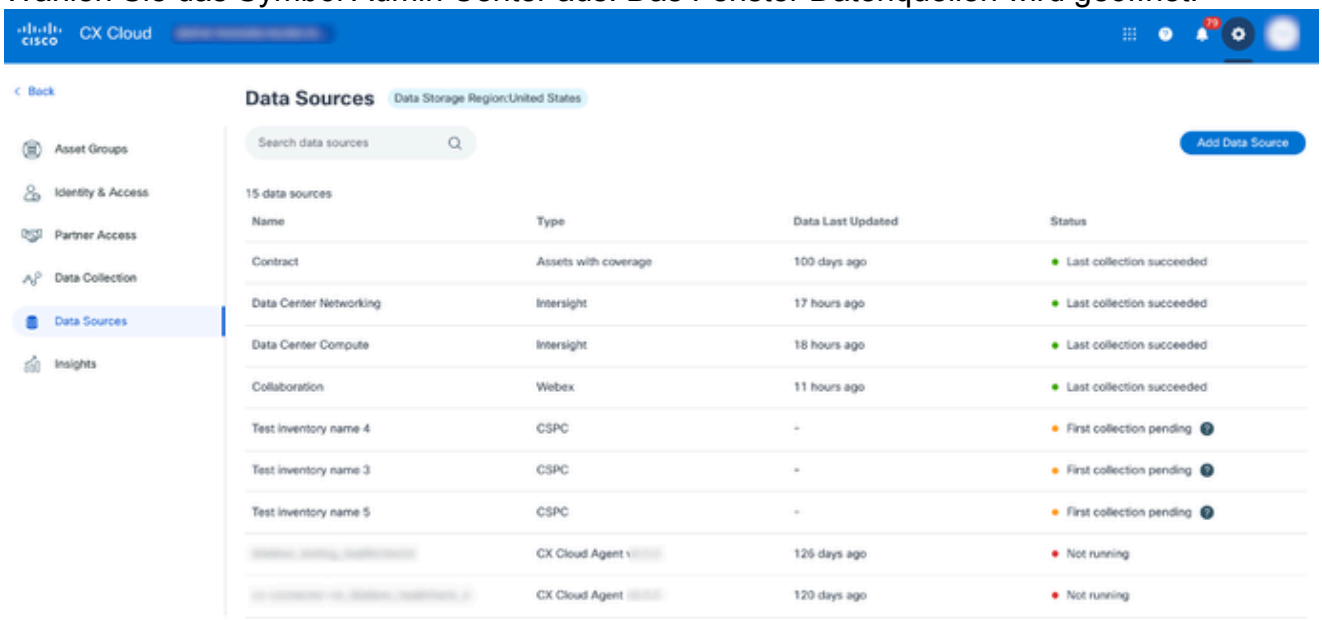
So installieren Sie das CX Agent-Upgrade v3.1 von der CX Cloud:

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



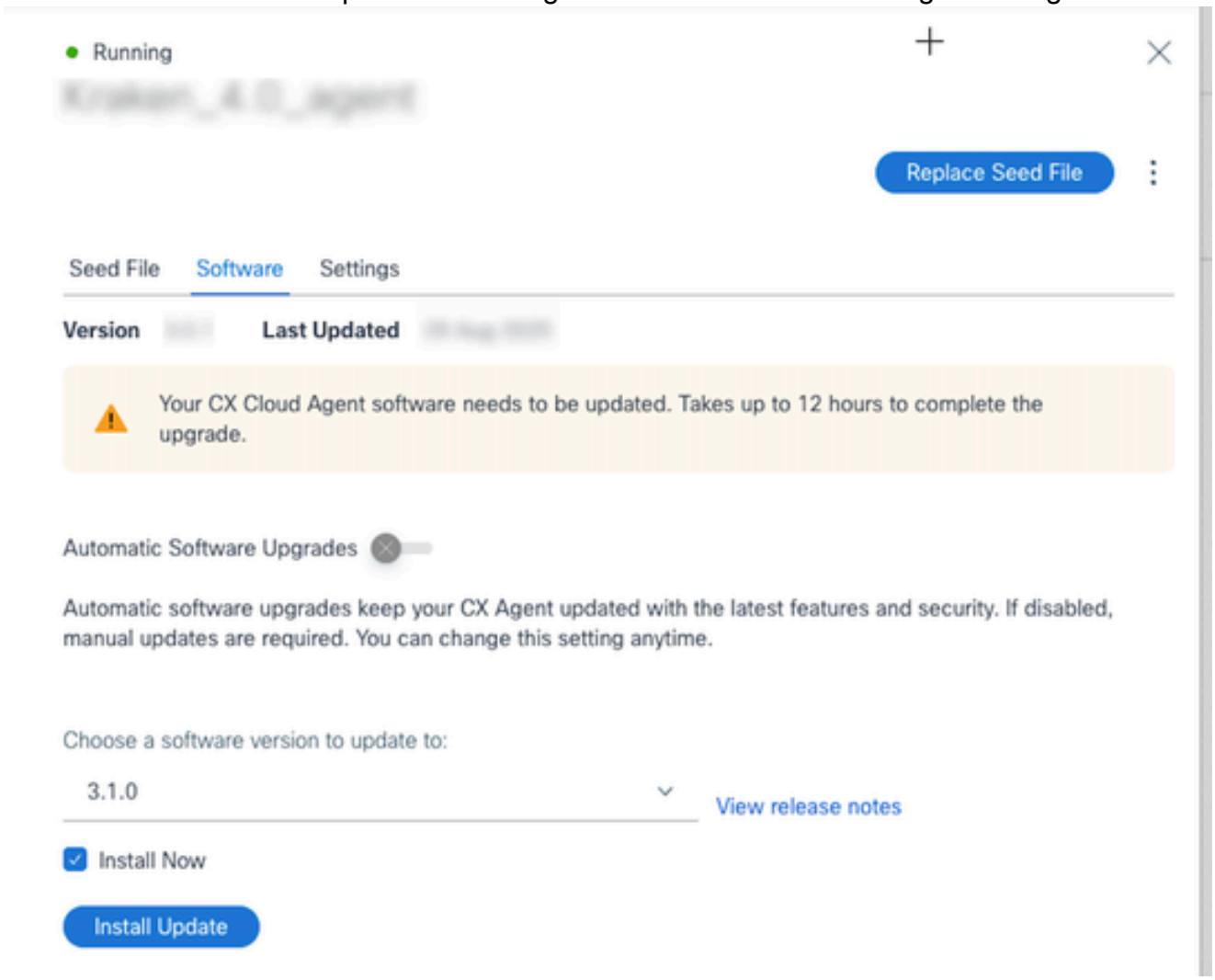
CX Cloud-Startseite

2. Wählen Sie das Symbol Admin Center aus. Das Fenster Datenquellen wird geöffnet.



Datenquellen

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



Manuelle Upgrades

4. Wählen Sie die Softwareversion 3.1.0 aus der Dropdown-Liste Wählen Sie eine Softwareversion aus, die aktualisiert werden soll.
5. Klicken Sie auf Update installieren, um CX Agent v3.1 zu installieren.

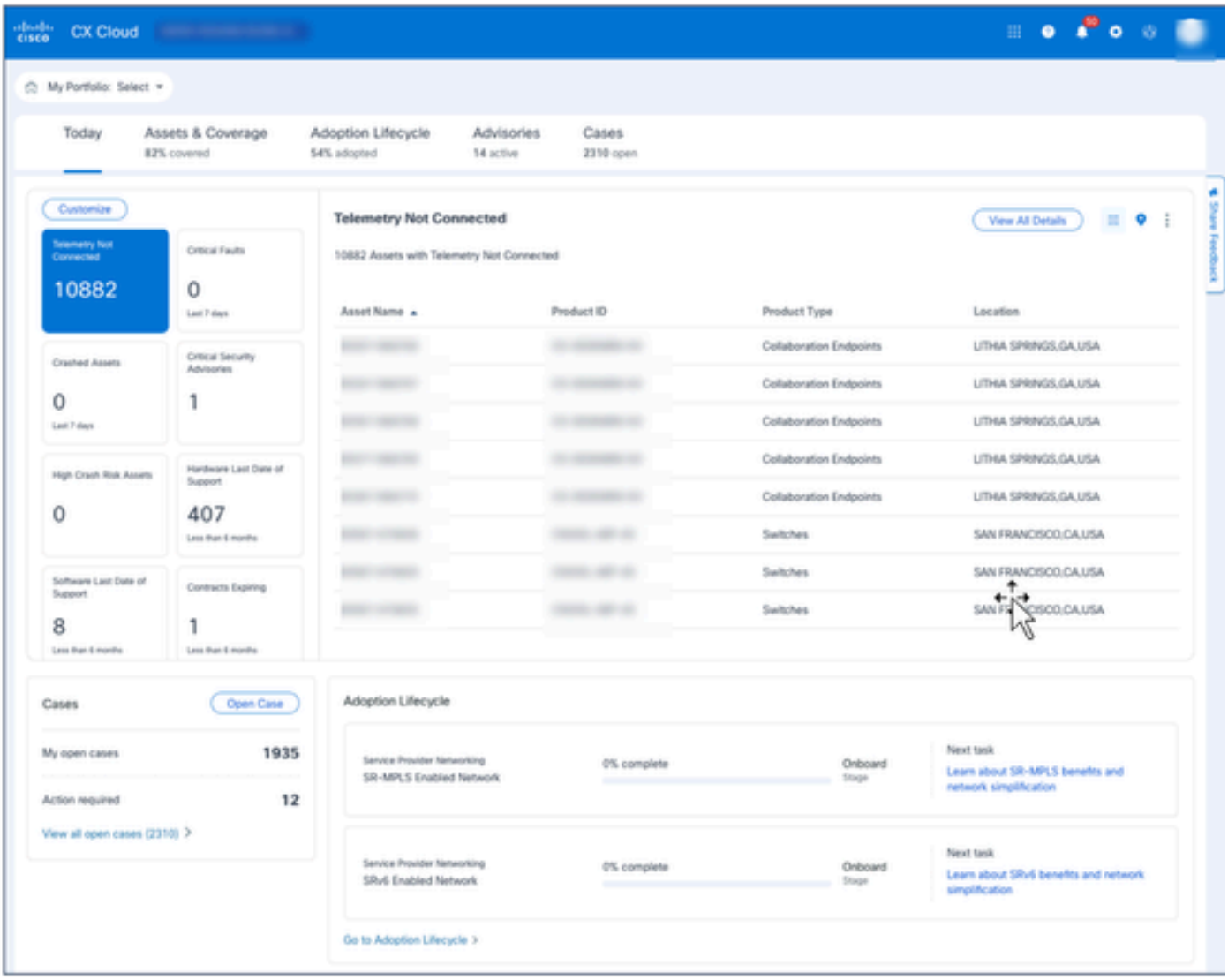
Hinweis: Kunden können die Aktualisierung für einen späteren Zeitpunkt planen, indem sie das Kontrollkästchen Jetzt installieren deaktivieren, das Planungsoptionen anzeigt.

Hinzufügen des CX-Agenten

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

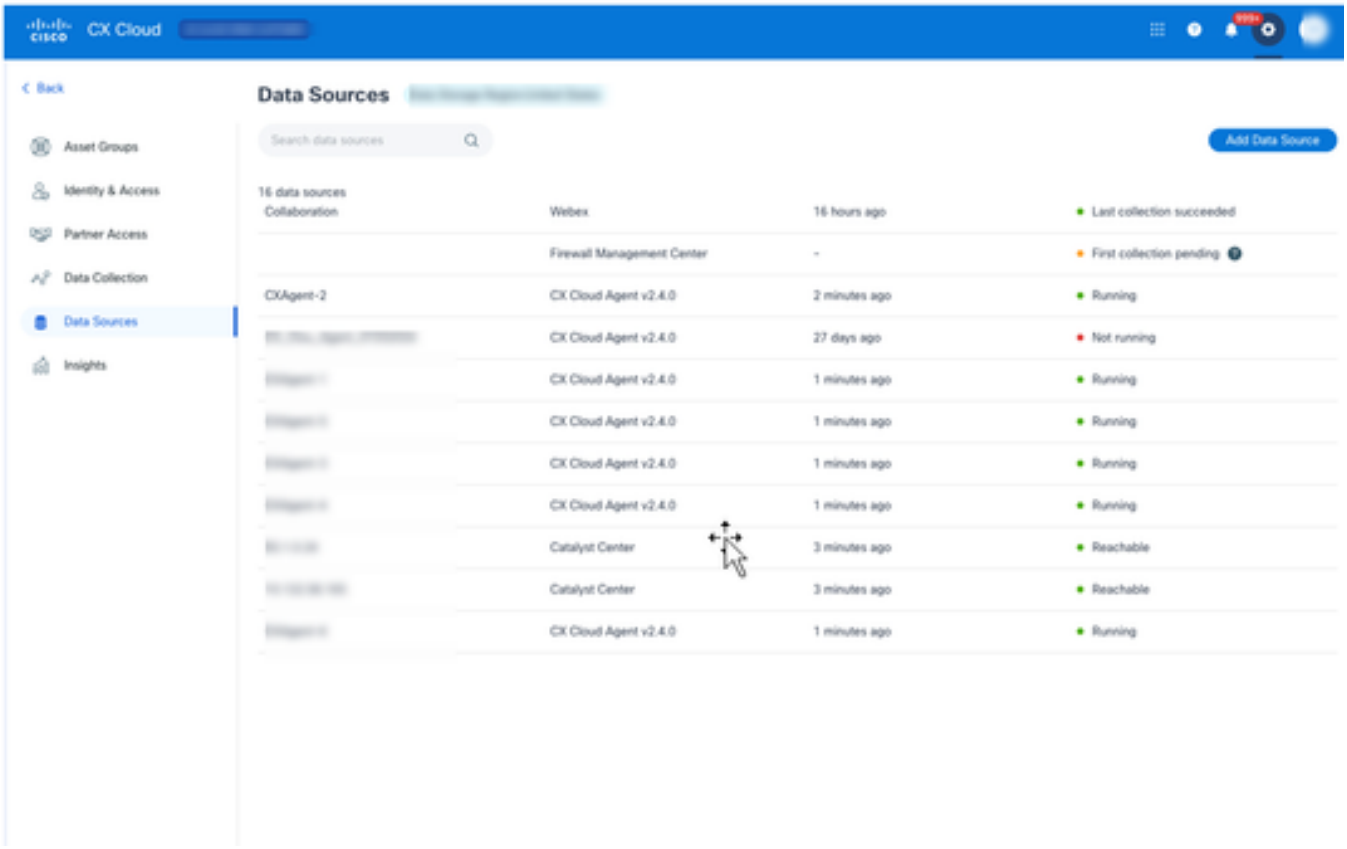
So fügen Sie einen CX-Agenten hinzu:

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



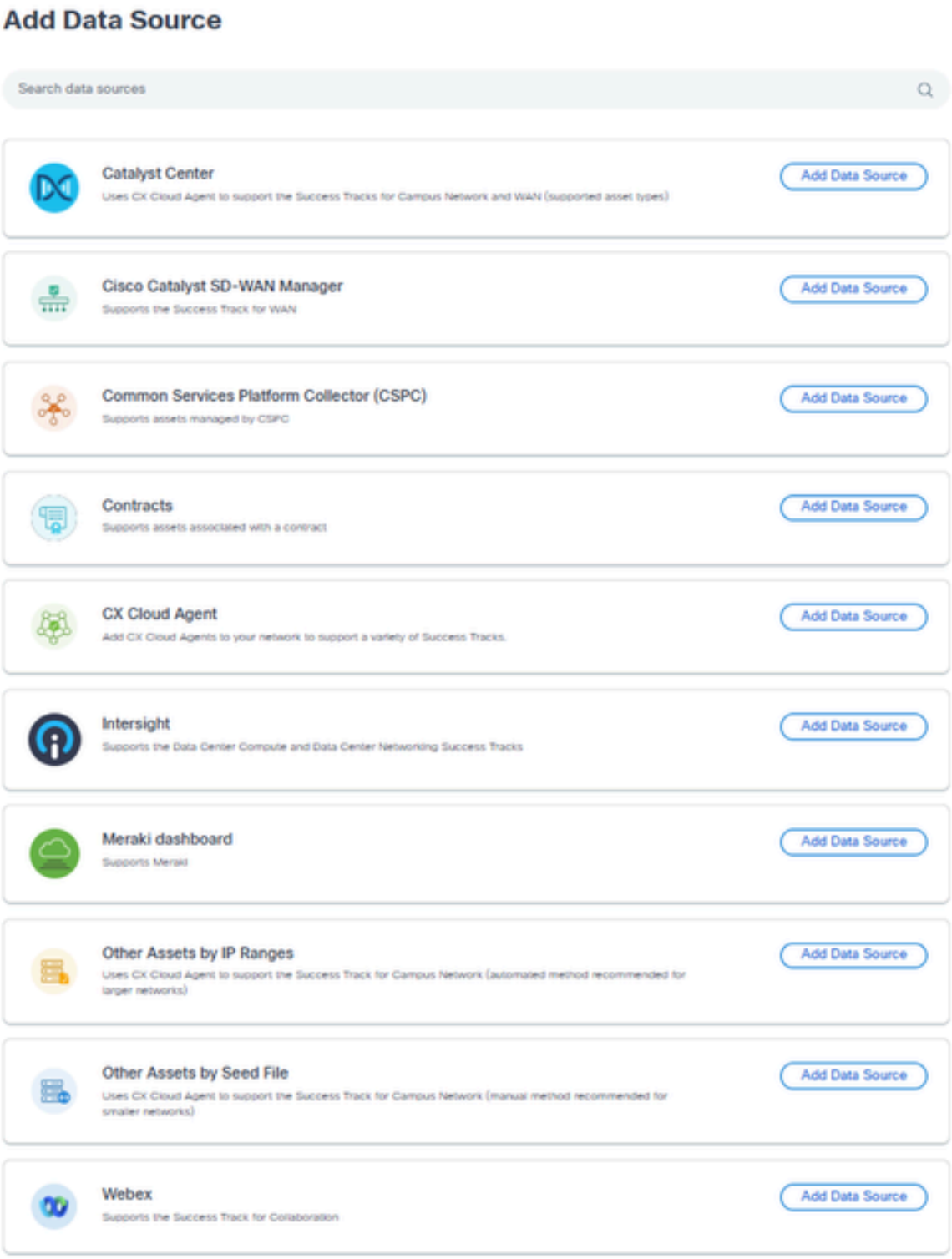
CX Cloud-Startseite

2. Wählen Sie das Symbol Admin Center aus. Das Fenster Datenquellen wird geöffnet.



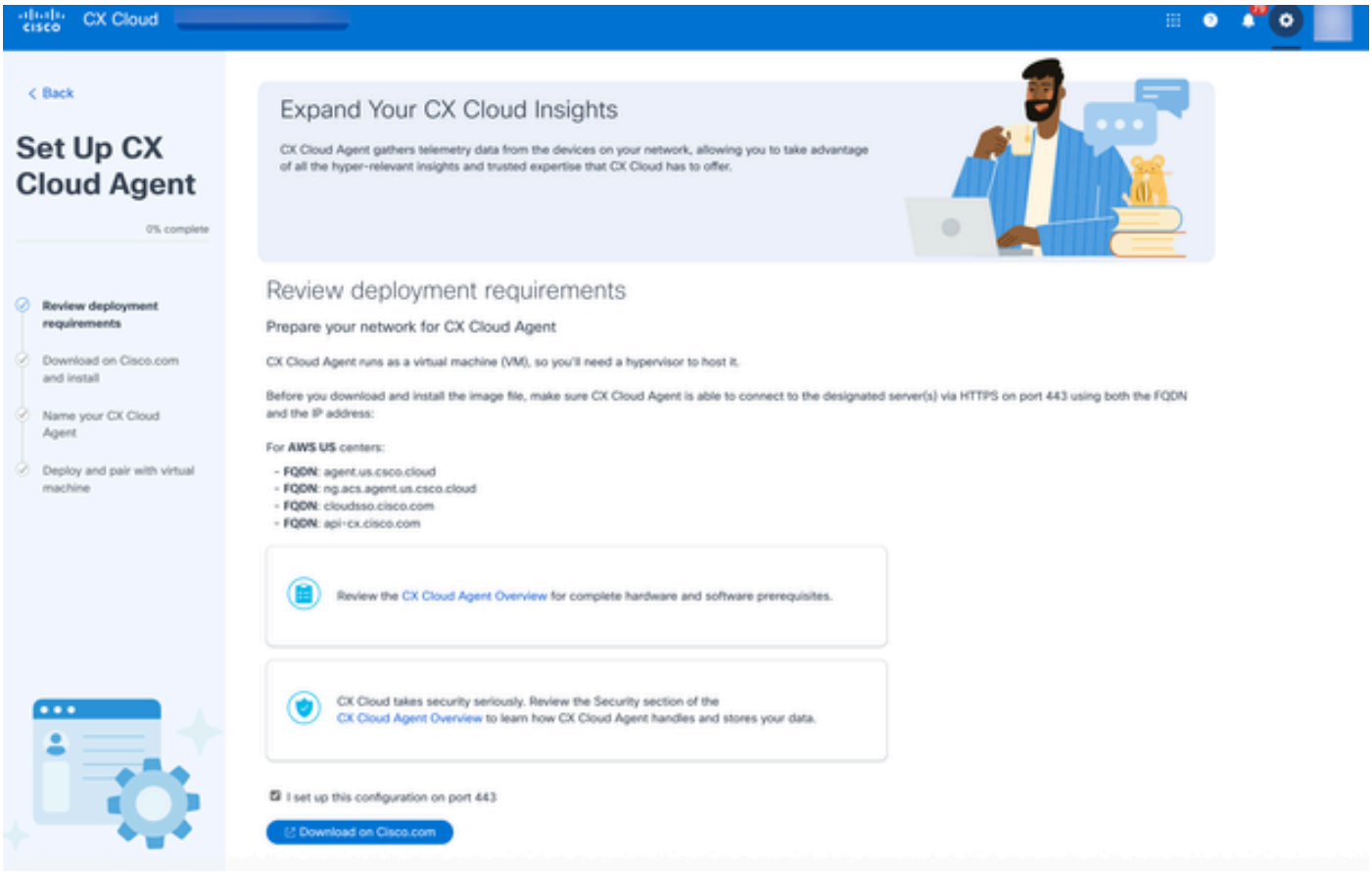
Datenquellen

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



Datenquelle hinzufügen

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



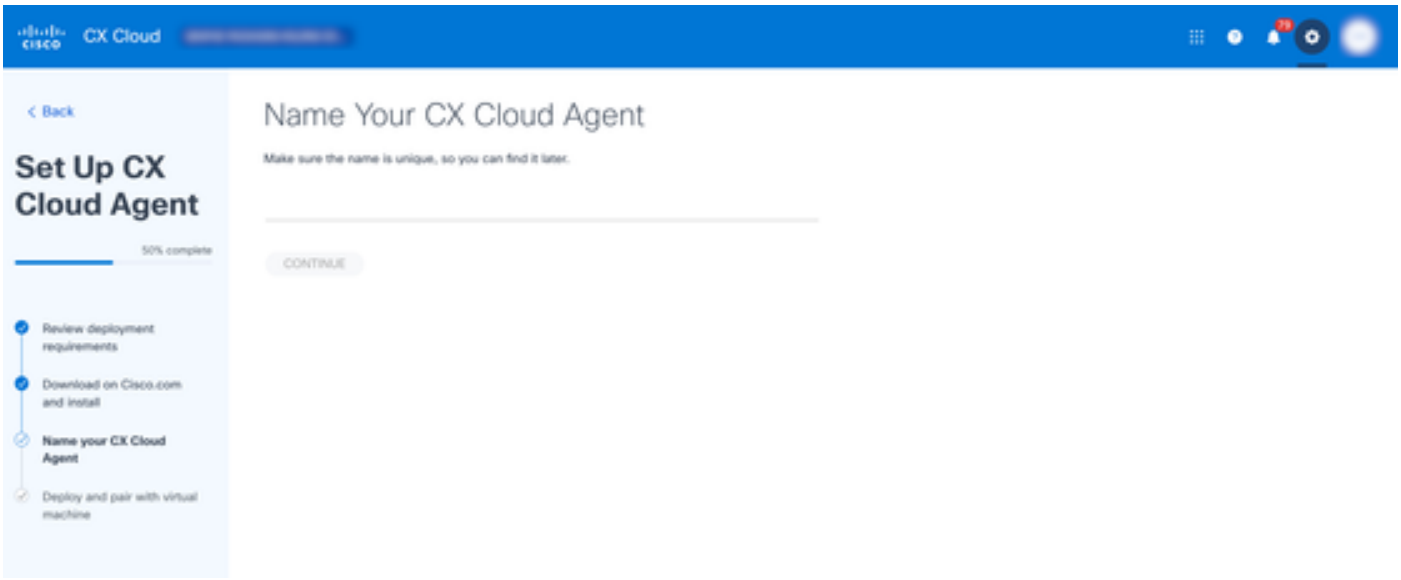
Hinzufügen des CX-Agenten

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. Das Fenster Software Download wird in einer anderen Registerkarte geöffnet.
7. Laden Sie die OVA-Datei "CX Agent v3.1.0" herunter.

Hinweis: Nach der Bereitstellung der OVA-Datei wird ein Kopplungscode generiert, der zum Abschließen des CX Agent-Setups erforderlich ist.

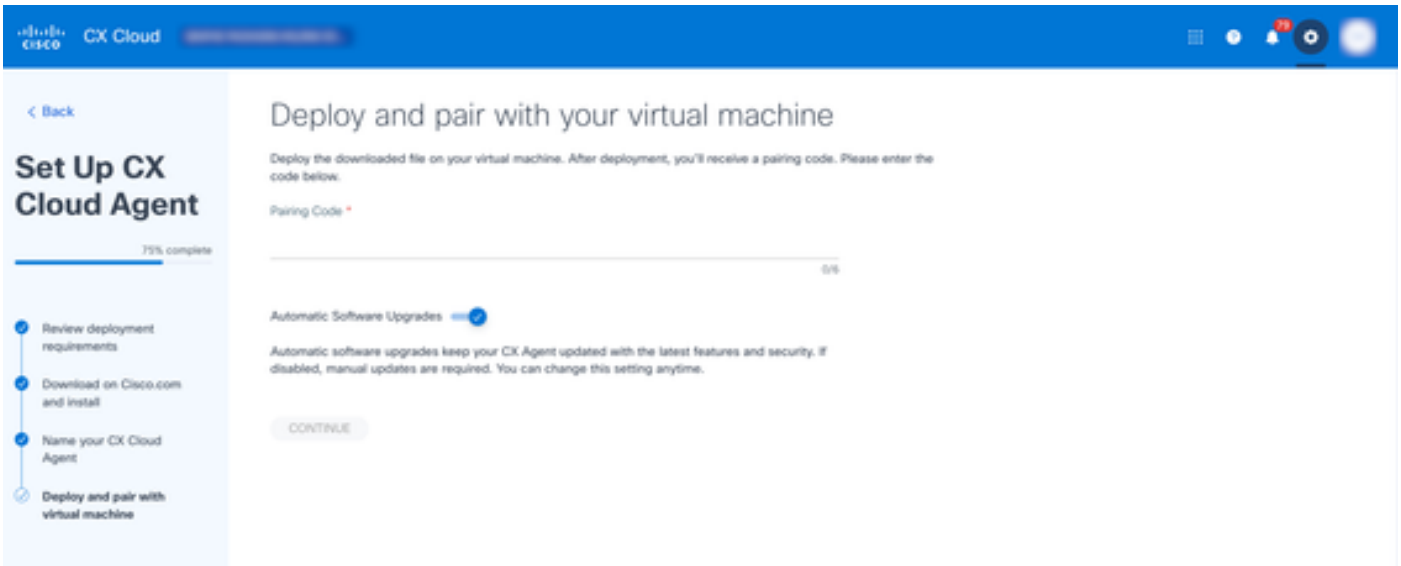
---

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



CX-Agent benennen

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



Kopplungscode

10. Geben Sie den Kopplungscode ein, der nach der Bereitstellung der heruntergeladenen OVA-Datei empfangen wurde.

11. Klicken Sie auf Weiter. Der Registrierungsstatus wird angezeigt, gefolgt von einer Bestätigungsmeldung.

Anmerkung: Wiederholen Sie die obigen Schritte, um weitere CX Agent-Instanzen als Datenquelle hinzuzufügen.

Konfigurieren von CX Agent für BCS/LCS

Die neue Converged Collection-Funktion von Cisco optimiert die Konfiguration von CX Agent v3.1 für BCS/LCS und vereinfacht die Kundenerfahrung.

Hinweis: Diese Konfiguration richtet sich speziell an Cisco Support-Techniker, die für das Collector Setup für BCS/LCS-Kunden verantwortlich sind.

BCS-/LCS-Kunden können die CX Cloud Community besuchen, um mehr über die Benutzerintegration und andere relevante Informationen zu erfahren.

Voraussetzungen

Support-Techniker mit Super User Administrator (SUA)- und Administratorzugriff können nur die CX Agent-Konfiguration für BCS/LCS durchführen.

Konfigurieren des CX-Agenten

Wenn Sie CX Agent für BCS/LCS konfigurieren möchten, wenden Sie sich an den Cisco Support.

RADKit-Funktionen konfigurieren

CX Agent v3.1 bietet eine optionale RADKit-Konfiguration zur Optimierung der Remote-Verwaltung und Fehlerbehebung von Cisco Geräten in der CX Cloud. Wenn diese Funktion aktiviert ist, können autorisierte Benutzer Vorgänge wie Datenerfassung, Konfiguration und Software-Upgrades sicher remote durchführen. Diese Einstellungen können je nach den betrieblichen Anforderungen des Kunden jederzeit aktiviert oder deaktiviert werden.

Ausführliche Informationen zu RADKit finden Sie unter Cisco RADKit.

Integration von RADKit Client über CLI

Um den RADKit-Client-Dienst zu integrieren, erstellen Sie ein Administratorkonto, und registrieren Sie den Dienst, indem Sie die folgenden Schritte ausführen:

Hinweis: Für die folgenden Schritte ist Root-Zugriff auf die CX Agent VM erforderlich.

---

1. Öffnen Sie das Terminal und Secure Shell (SSH) mithilfe der entsprechenden Anmeldeinformationen in einem virtuellen System. Beispiel:

```
ssh your_username@your_vm_ip
```

2. Führen Sie den folgenden Befehl aus, um die Netzwerkverbindung zu aktivieren:

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

```
kubectl netpol löschen deny-from-other-namespaces
```

3. Senden Sie auf dem lokalen Computer eine POST-Anforderung an den Manager-Endpunkt, um ein Administratorkonto zu erstellen. Die Antragsstelle sollte Folgendes umfassen:

- admin_name (erforderlich): Der Benutzername für das Administratorkonto
- E-Mail (optional): Die E-Mail-Adresse für das Administratorkonto
- Vollständiger_Name (optional): Vollständiger Name des Administrators
- Beschreibung (optional): Eine Beschreibung des Administratorkontos

Das folgende Beispiel zeigt, wie diese Anforderung mit cURL gesendet wird:

```
curl -X POST \

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

  -H "Inhaltstyp: Anwendung/Json" \

  -d '{

        "admin_name": "admin_user123",

        E-Mail: "admin@example.com",

        "Vollständiger_Name": "Administrator-Benutzer",

        "Beschreibung": "Administratorkonto für die Verwaltung des
Systems"

      }'
```

Nach erfolgreicher Erstellung eines Administratorkontos antwortet der Server mit einer Bestätigungsmeldung, dass das Administratorkonto erfolgreich erstellt wurde. Diese Antwort beinhaltet auch ein temporäres Kennwort, das bei der ersten Anmeldung geändert werden muss. Wenn das Administratorkonto jedoch bereits vorhanden ist, gibt der Server einen Statuscode von 400 mit der Meldung "Admin already created" (Admin bereits erstellt) zurück.

4. Öffnen Sie den Webbrowser, und navigieren Sie zur RADKit-Webbenutzeroberfläche: https://<your_vm_ip>:30101/.
5. Melden Sie sich mit dem Administrator-Benutzernamen (admin_name) und dem in der Antwort angegebenen temporären Kennwort an.

✎ Anmerkung: Nach der ersten Anmeldung werden die Benutzer aufgefordert, das Kennwort zu ändern. Befolgen Sie die Anweisungen, um ein neues Kennwort festzulegen.

---

6. Führen Sie den RADKit-Client auf dem lokalen Computer aus, um den Dienst zu registrieren.
7. Generieren Sie nach der Authentifizierung ein einmaliges Kennwort, indem Sie den folgenden Befehl ausführen:

```
grant_service_otp()
```

8. Senden Sie auf dem lokalen System eine POST-Anforderung an das Manager-Endgerät, um den Service zu registrieren. Die Antragsstelle sollte Folgendes umfassen:

- OTP (erforderlich): Die einmalige Kennwortzeichenfolge

Das folgende Beispiel zeigt, wie diese Anforderung mit cURL gesendet wird:

```
curl -X POST \

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

  -H "Inhaltstyp: Anwendung/Json" \

  -d '{

        "einmalig": "PROD:1234-1234-1234"

      }'
```

Nach erfolgreicher Registrierung wird eine Bestätigungsmeldung angezeigt, und Benutzer können den RADKit-Dienst über ein Administratorkonto verwalten.

Führen Sie den folgenden Befehl aus, um die Netzwerkverbindung zu deaktivieren:

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

Konfigurieren des Tresors für vorhandene CX-Agenten

Die optionale Vault-Konfigurationsfunktion ermöglicht der CX Cloud die sichere Verbindung mit einem Vault-Service für den Zugriff auf vertrauliche Daten wie Token und Inventarlisten unter Verwendung der neuesten Anmeldeinformationen. Wenn diese Option aktiviert ist, verwendet CX Cloud automatisch die konfigurierte Adresse und das Token. Diese Einstellung kann jederzeit aktiviert oder deaktiviert werden. Derzeit wird nur die Tresorkonfiguration von HashiCorp unterstützt.

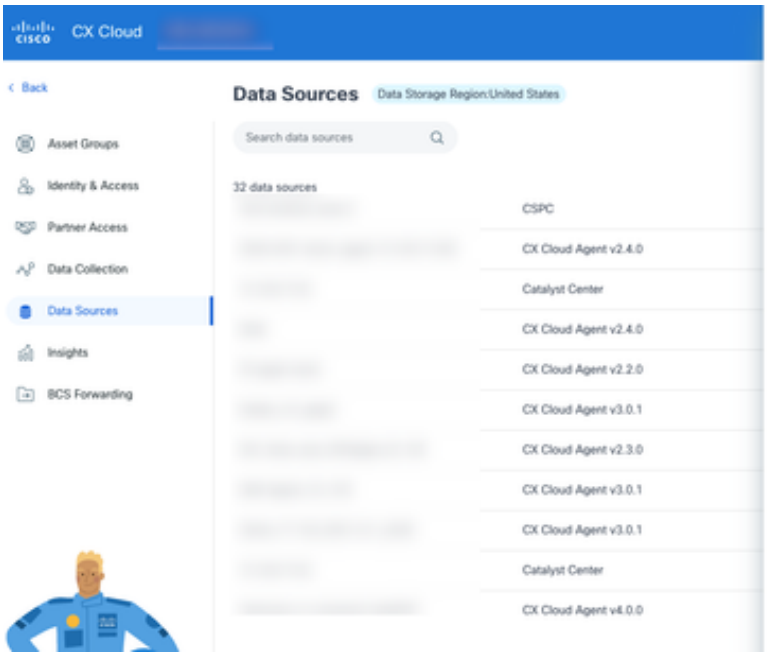
Der Tresor kann auf zwei Arten konfiguriert werden:

- Obwohl CX Cloud-Benutzeroberfläche
- Über CLI

Konfigurieren von HashiCorp Vault in der CX Cloud-Benutzeroberfläche

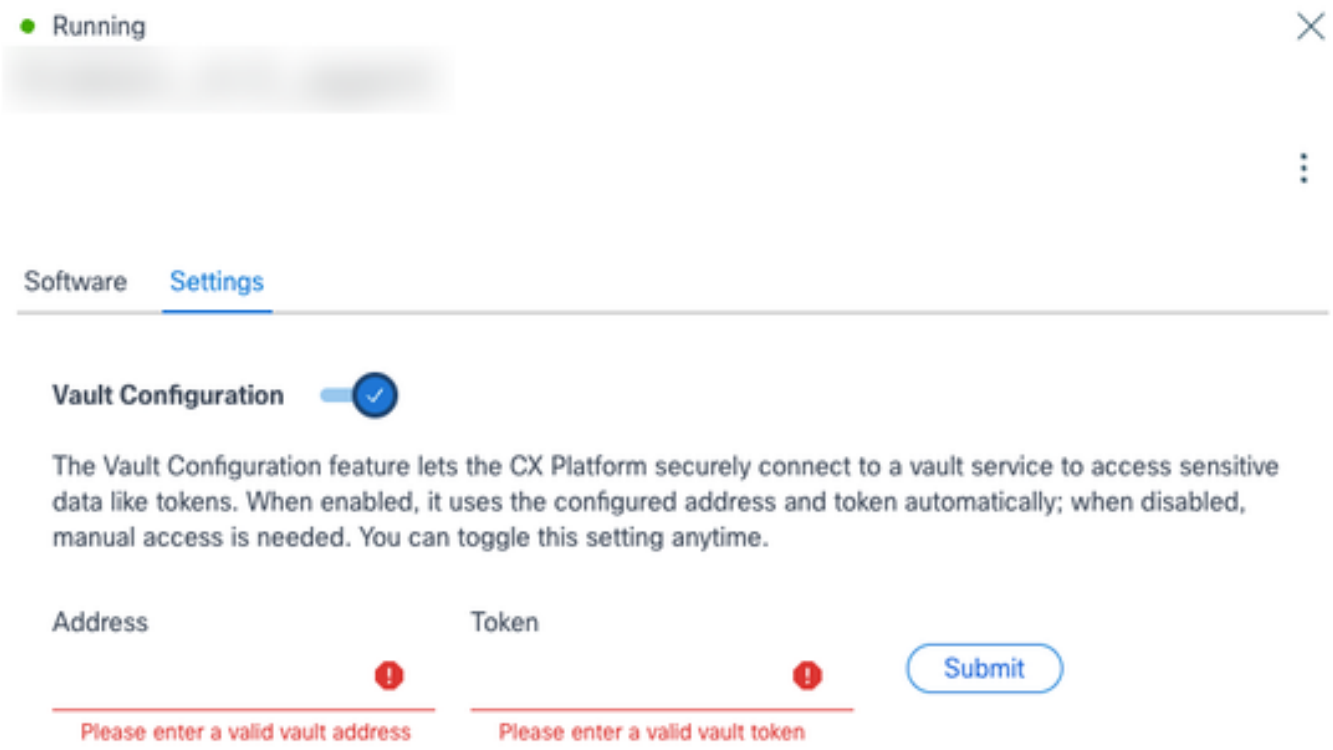
So konfigurieren Sie den HashiCorp-Tresor für einen vorhandenen CX-Agenten:

1. Wählen Sie das Symbol Admin Center aus. Das Fenster Datenquellen wird geöffnet.
2. Klicken Sie auf die Datenquelle des CX-Agenten. Das Detailfenster CX Agent wird geöffnet.



Einstellungen

3. Klicken Sie auf die Registerkarte Einstellungen.
4. Aktivieren Sie den Umschalter Vault-Konfiguration.



Vault-Konfiguration

5. Geben Sie Details in die Felder Adresse und Token ein.

6. Klicken Sie auf Senden. Daraufhin werden eine Bestätigung und die hinzugefügte IP-Adresse angezeigt.

Kunden können den konfigurierten Tresor entfernen, indem sie auf Entfernen klicken.

Integration von CX Agent mit HashiCorp Vault über CLI

In diesem Abschnitt wird das Verfahren zum Konfigurieren der Verbindung zwischen dem Cisco CX Agent und einer HashiCorp Vault-Instanz beschrieben. Diese Integration ermöglicht die sichere Speicherung und den Abruf von Geräteanmeldedaten und verbessert so den allgemeinen Sicherheitsstatus.

Voraussetzungen

- CXROOT-Zugriff auf CX Agent VM
- Eine laufende und zugängliche Vault-Instanz

Integration mit HashiCorp Vault

- Führen Sie den folgenden Befehl aus, um die Vault-Integration zu aktivieren:

```
cxcli-Agententresor auf
```

- Führen Sie den folgenden Befehl aus, um die Vault-Integration zu deaktivieren:

```
cxcli agent vault off
```

- Führen Sie den folgenden Befehl aus, um den aktuellen Status der Vault-Integration zu überprüfen:

```
cxcli agent Vault-Status
```

Aktivieren der HashiCorp Vault-Integration

So aktivieren Sie die Vault-Integration:

1. Melden Sie sich mit dem Benutzerkonto cxcroot beim CX-Agenten über SSH an, um auf den CX-Agenten zuzugreifen.
2. Wechseln Sie zum Root-Benutzer, um Berechtigungen zu erweitern, indem Sie den folgenden Befehl ausführen:

```
sudo su
```

3. Führen Sie den folgenden Befehl aus, um den aktuellen Status der Vault-Integration zu überprüfen:

```
root@cxcloudagent: /home/cxcroot# cxcli-Agententresorstatus
```

Vault-Integration deaktiviert

4. Führen Sie den folgenden Befehl aus, um die Vault-Integration zu aktivieren:

```
cxcli-Agententresor auf
```

5. Aktualisieren Sie die folgenden Felder:

- Vault-Adresse
- Vault-Stamm-Token

6. Überprüfen Sie den Status der Integration in den Tresor, um dies zu überprüfen. Die Antwortnachricht sollte bestätigen, dass die Integration aktiviert ist:

```
root@cxcloudagent: /home/cxcroot# cxcli-Agententresor auf

Geben Sie die HashiCorp Vault-Adresse ein:

HashiCorp-Tresortoken eingeben:

Aktivierung der Vault-Integration root@cxcloudagent: /home/cxcroot#
```

Deaktivieren der HashiCorp Vault-Integration

So greifen Sie auf den CX-Agenten zu:

1. Melden Sie sich mit dem cxcroot-Benutzerkonto über SSH beim CX-Agenten an.
2. Wechseln Sie zum Root-Benutzer, um Berechtigungen zu erweitern, indem Sie den folgenden Befehl ausführen:

```
sudo su
```

3. Führen Sie den folgenden Befehl aus, um die HashiCorp Vault-Integration zu deaktivieren:

```
root@cxcloudagent: /home/cxcroot# cxcli-Agententresor aus

Vault-Integration deaktiviert

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

HashiCorp Schema der Vault-Geräteanmeldedaten

Schema der Vault-Anmeldedaten: Wenn Sie detaillierte Informationen zu den verfügbaren Optionen und unterstützten Feldern für Geräteanmeldedaten benötigen, laden Sie die Datei "Vault-Anmeldedaten-Schema" (vault-dentials-schema.json) herunter.

Beispiel: Im Folgenden finden Sie ein Beispiel für JSON-Anmeldeinformationen, die auf dem Schema basieren:

-

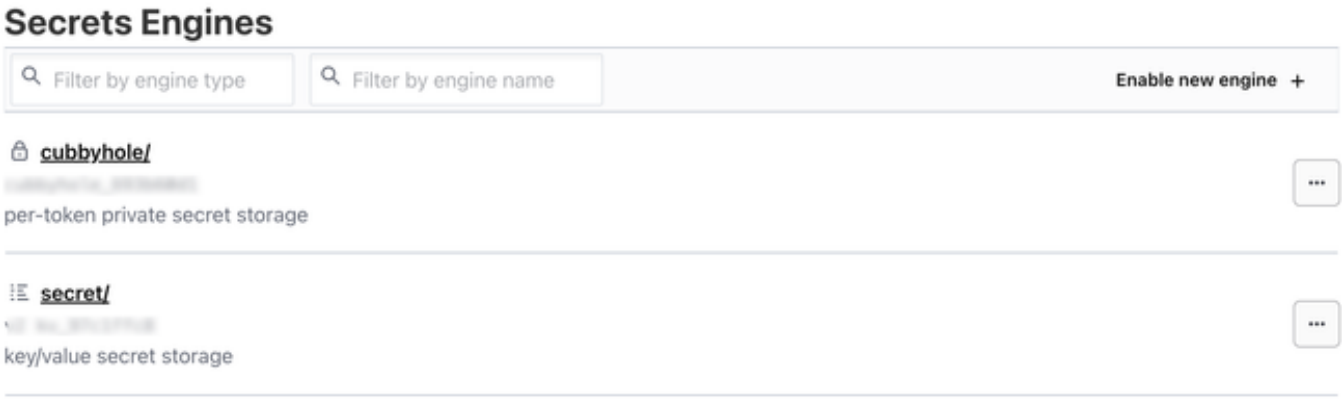
```
{
"targetIp": "5.0.1.*",
```

```
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
"password": "*******",
"enableUser": "cisco",
"enablePassword": "*******"
}
}
}
```

Hinweis: Benutzer können mehrere Protokolle innerhalb einer JSON-Datei mit einzelnen Anmeldeinformationen angeben. Vermeiden Sie es jedoch, doppelte Protokolle aus derselben Familie zu verwenden (z. B. sollten Sie SNMPv2c und SNMPv3 nicht in derselben Anmeldeinformationsdatei speichern).

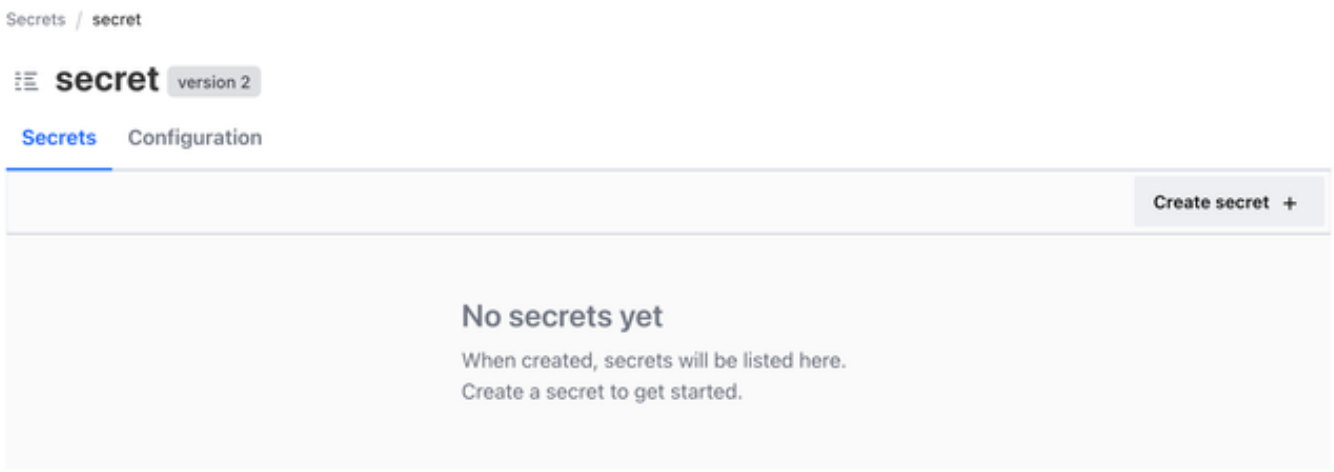
Konfigurieren von Geräteanmeldedaten in HashiCorp Vault (beim ersten Mal)

1. Melden Sie sich bei einer Vault-Instanz an.



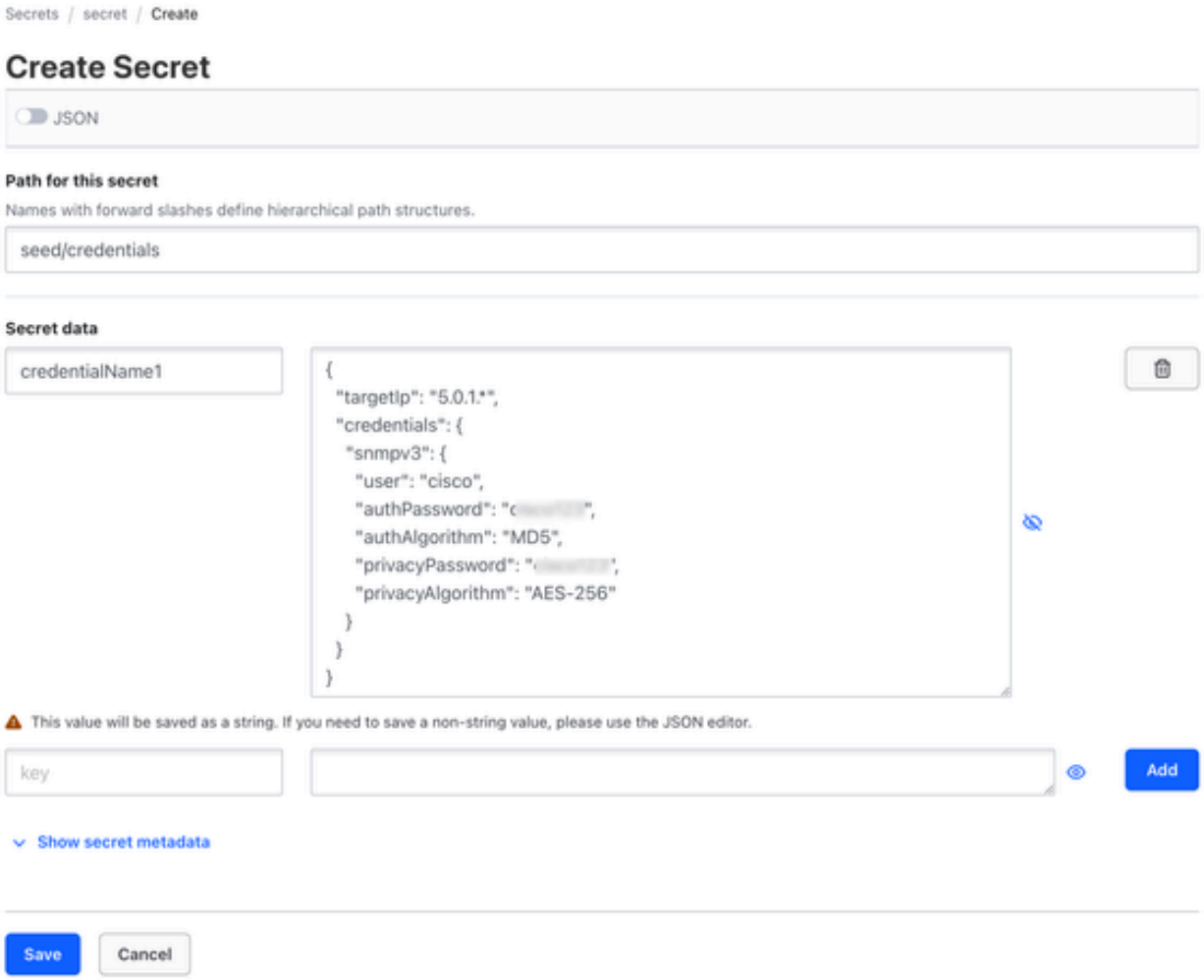
Geheim

2. Erstellen Sie einen neuen Schlüssel-Wert-Schlüssel über den folgenden Pfad: geheim/Seed/Zugangsdaten.
3. Wählen Sie die Schlüssel-Wert-Geheimspeicher-Engine (geheim/) aus.



Schlüssel Wert geheim

4. Klicken Sie auf Geheimnis erstellen. Das Fenster Geheim erstellen wird geöffnet.



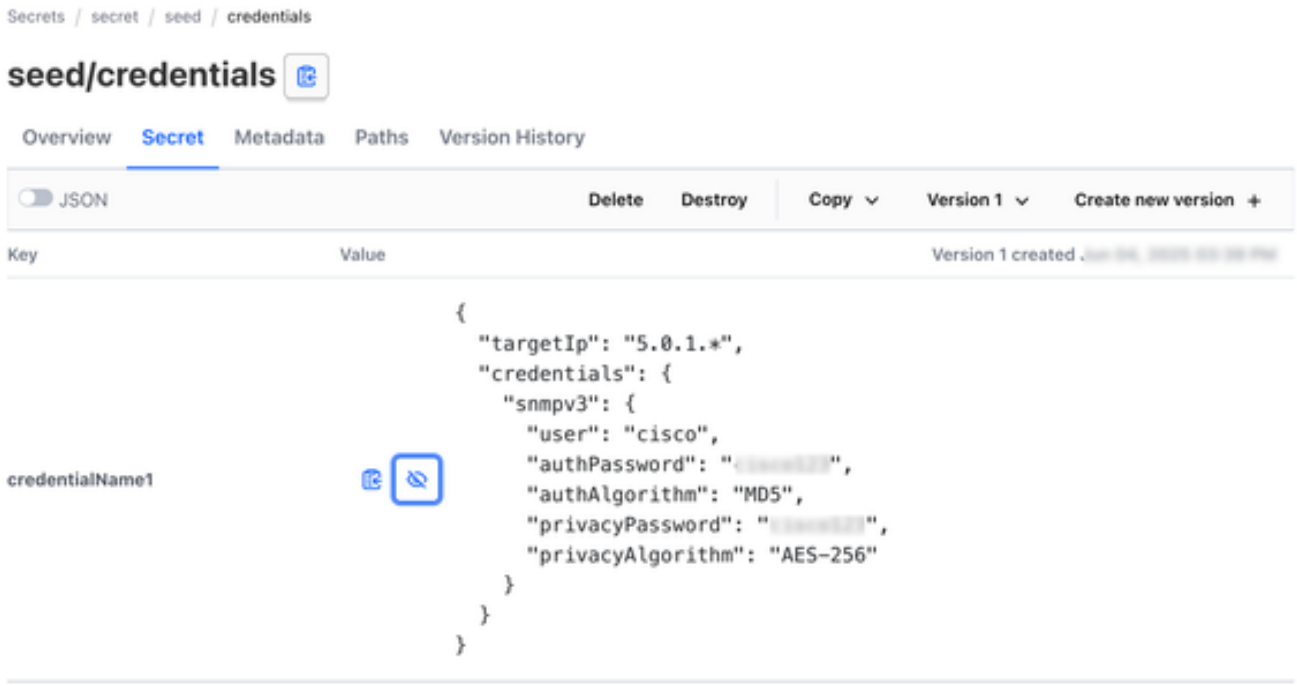
Client-Schlüssel

5. Aktualisieren Sie die folgenden Felder:

- Pfad für geheim: Seed/Zugangsdaten
- Geheime Daten: Schlüsselsammlung - Wertgeheimnisse

- wichtigste: benutzerdefinierter eindeutiger Anmeldename
- wert: Anmeldedaten JSON

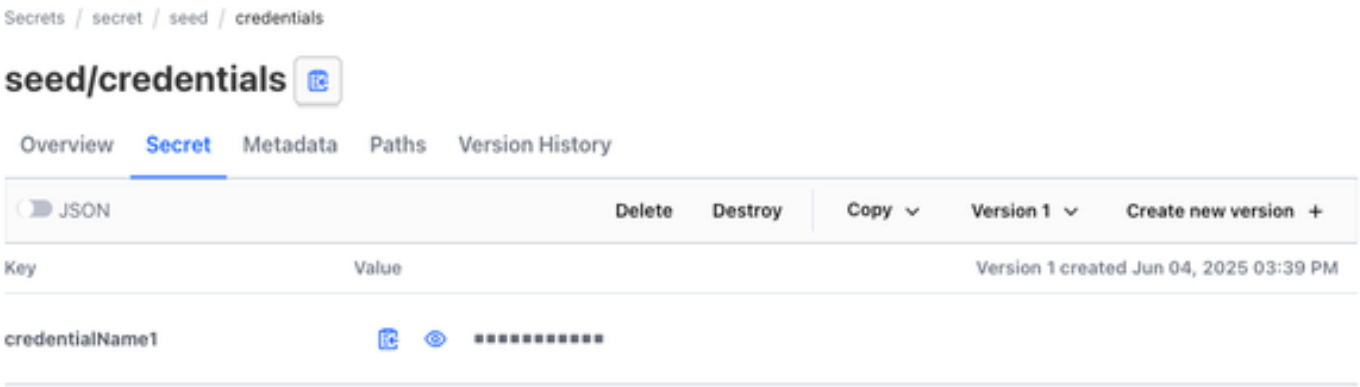
6. Klicken Sie auf Speichern. Das Geheimnis sollte nun im HashiCorp Tresor gespeichert werden.



Anmeldeinformationen

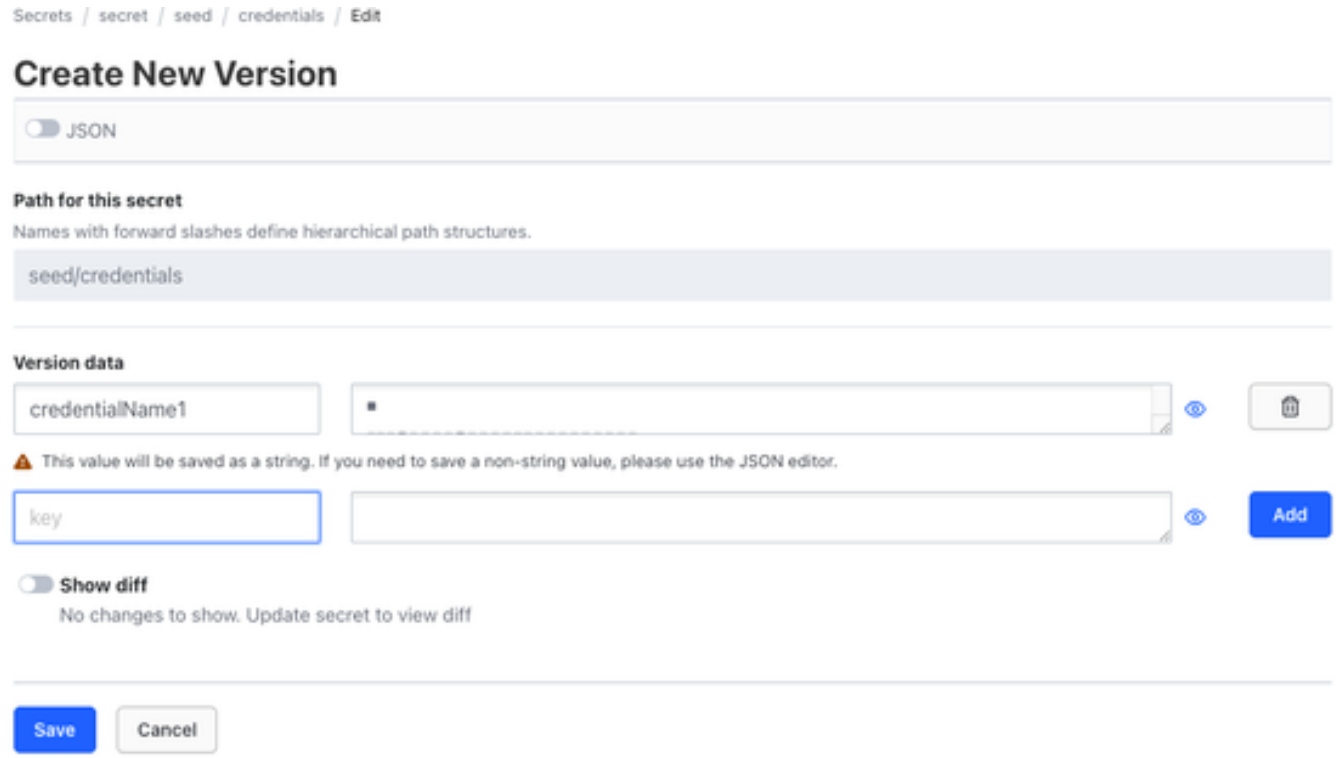
Hinzufügen weiterer Anmeldeinformationen zu HashiCorp Vault

1. Melden Sie sich bei einer HashiCorp-Vault-Instanz an.



Anmeldeinformationen hinzufügen

2. Navigieren Sie zu dem bereits erstellten geheimen Schlüssel "Geheim/Seed/Zugangsdaten".



Version erstellen

3. Klicken Sie auf Neue Version erstellen.

4. Fügen Sie neue Geheimnisse hinzu, indem Sie nach Bedarf eine beliebige Anzahl von Schlüssel-Wert-Paaren bereitstellen.

5. Klicken Sie auf Speichern.

CX Cloud Seed-Datei mit Standard-Anmeldedaten

- Seed-Datei vereinfachen: Wenn Sie Anmeldeinformationen verwenden, die über den Hashicorp-Tresor konfiguriert wurden, vereinfachen Sie die Seed-Datei, indem Sie vertrauliche Informationen auslassen.
- Geben Sie nur die IP-Adresse oder den Hostnamen an: Benutzer können nur die IP-Adresse oder den Hostnamen in die Seed-Datei übergeben, während andere Felder leer bleiben.

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

IP- oder Hostname

- Anmeldeinformationen für HashiCorp-Tresor und Seed-Datei verwenden: Bereitstellung von Anmeldeinformationen für einige Geräte in der Seed-Datei, während die Anmeldeinformationen für andere Geräte über den Tresor verwaltet werden

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

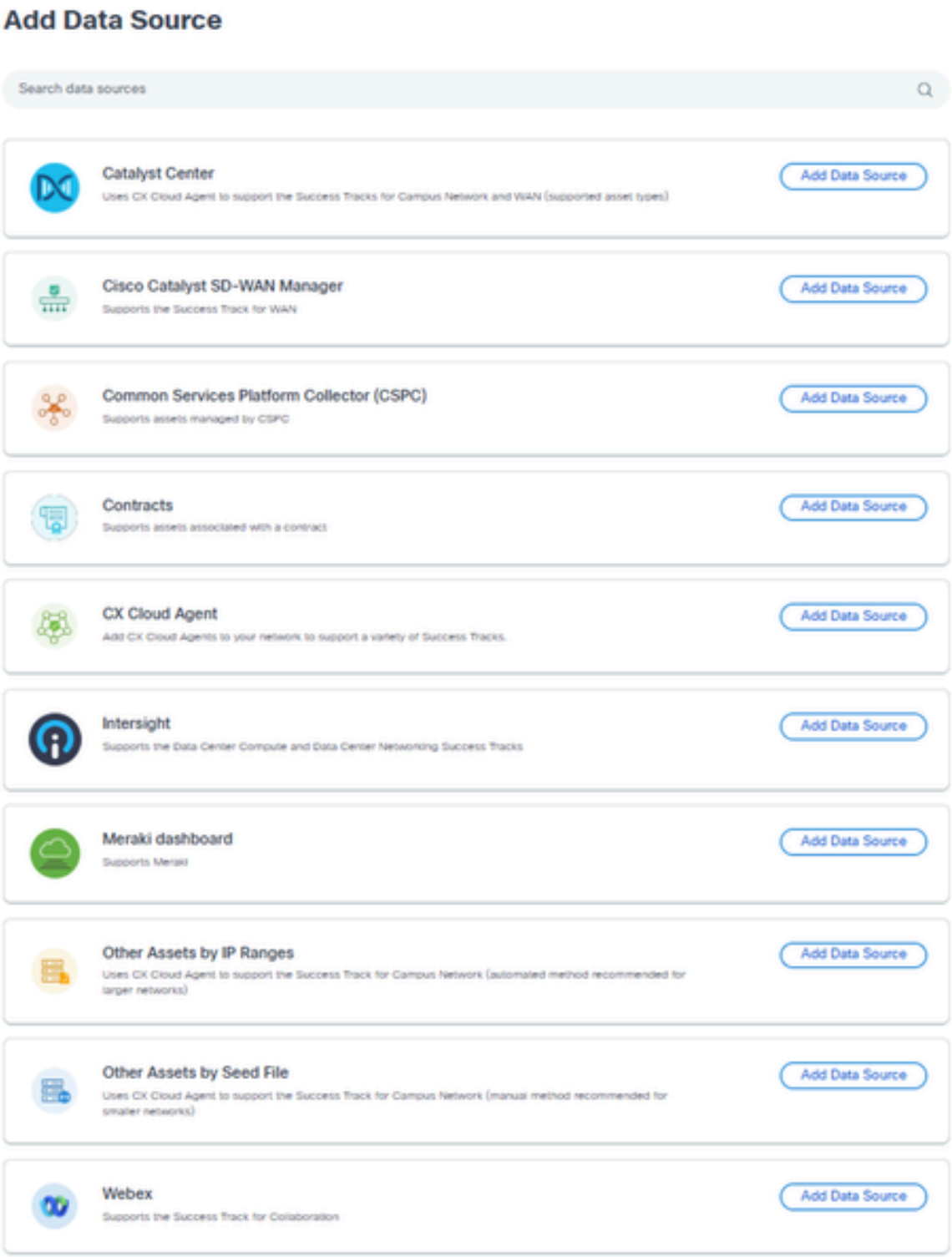
IP- oder Hostname

Hinzufügen von Catalyst Center als Datenquelle

Benutzer mit der Rolle "Super Administrator User" können die Catalyst Center-Datenquelle hinzufügen.

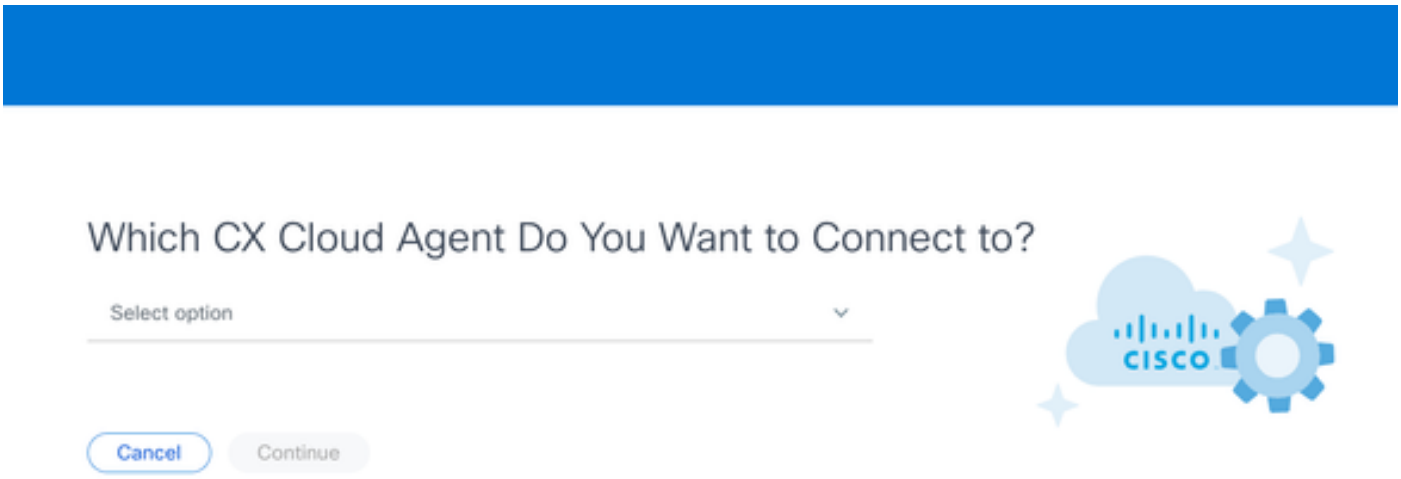
Catalyst Center als Datenquelle hinzufügen:

1. Klicken Sie auf das Symbol Admin Center. Das Fenster Datenquellen wird geöffnet.
2. Klicken Sie auf Datenquelle hinzufügen. Die Seite Datenquelle hinzufügen wird angezeigt.



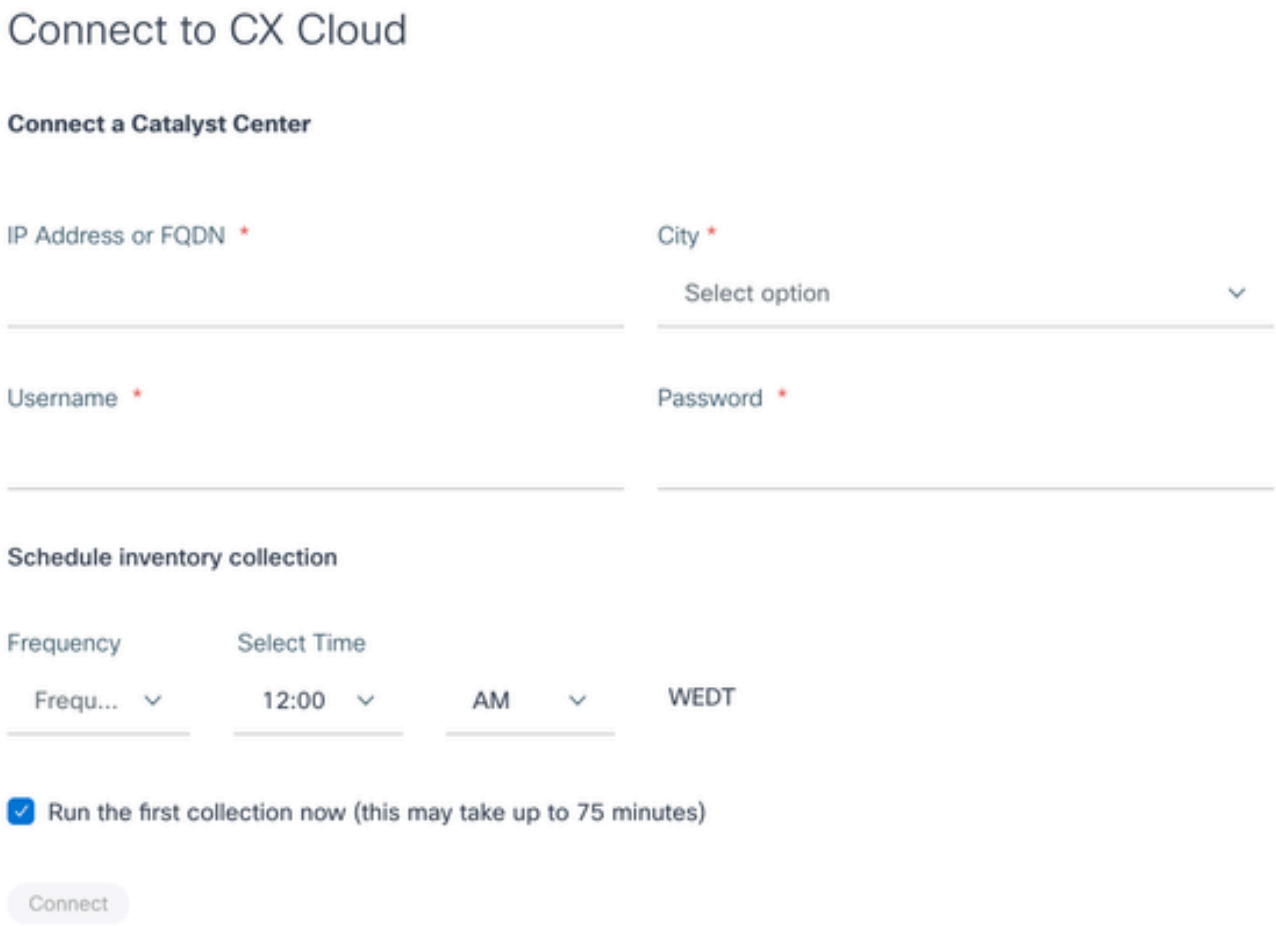
Datenquelle hinzufügen

3. Klicken Sie in der Option Catalyst Center auf Datenquelle hinzufügen.



CX-Agent auswählen

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



Häufigkeit

6. Geben Sie die folgenden Details ein:

- Virtuelle IP-Adresse oder FQDN (d. h. Catalyst Center-IP-Adresse)
- Stadt (d. h. der Standort des Catalyst Centers)
- Benutzername
- Kennwort
- Häufigkeit und Zeit auswählen, um anzugeben, wie oft der CX-Agent Netzwerkscans in den Abschnitten Schedule Inventory Collection durchführen soll

Anmerkung: Aktivieren Sie das Kontrollkästchen Erste Sammlung jetzt ausführen, um die Sammlung jetzt auszuführen.

7. Klicken Sie auf Verbinden. Es wird eine Bestätigung mit der Catalyst Center-IP-Adresse angezeigt.

Hinzufügen von SolarWinds® als Datenquelle

Anmerkung: Wenn Sie die Datenquelle SolarWinds® hinzufügen möchten, wenden Sie sich an den Cisco Support.

BCS/LCS-Kunden können nun die CX Agent-Funktion nutzen, um sich extern in SolarWinds® zu integrieren. Dies sorgt für mehr Transparenz, eine verbesserte Verwaltbarkeit und eine verbesserte Benutzererfahrung durch eine verbesserte Automatisierung. Der CX Agent sammelt Inventar- und andere erforderliche Daten, um verschiedene Berichte zu erstellen, die hinsichtlich Format, Datenvollständigkeit und Datengenauigkeit konsistent sind. Aktuelle Berichte, die von Operational Insights Collector CX Agent generiert werden, unterstützen die Integration mit SolarWinds®, indem ein BCS/LCS-Kunde OIC durch CX Agent ersetzen kann, um Daten von Solarwinds® zu sammeln. Diese Funktion, einschließlich der Datenquelle Solarwinds®, steht ausschließlich BCS/LCS-Kunden zur Verfügung.

Der CX-Agent muss vor der ersten Erfassung in BCS Forwarding konfiguriert werden. Andernfalls werden Dateien nicht verarbeitet. Weitere Informationen zur Konfiguration der BCS-Weiterleitung finden Sie im Abschnitt Configuring CX Agent for BCS or LCS.

Hinweise:

- Mehrere Sammlungen derselben SolarWinds®-Instanz überschreiben vorherige Dateien (spätere Uploads haben Vorrang)
- Es werden mehrere Quellen unterstützt, aber jede SolarWinds®-Instanz muss eine eindeutige IP- und Geräte-ID haben.

Andere Ressourcen als Datenquellen hinzufügen

Die Erfassung von Telemetriedaten wurde auf Geräte erweitert, die nicht vom Catalyst Center verwaltet werden. So können Benutzer Informationen und Analysen aus Telemetriedaten abrufen und mit diesen interagieren, um eine breitere Palette von Geräten zu unterstützen. Nach der Ersteinrichtung von CX Agent haben Benutzer die Möglichkeit, CX Agent so zu konfigurieren, dass

eine Verbindung zu 20 weiteren Catalyst Centern innerhalb der von CX Cloud überwachten Infrastruktur hergestellt wird.

Benutzer können Geräte identifizieren, die in die CX Cloud integriert werden sollen, indem sie diese Geräte eindeutig mithilfe einer Seed-Datei oder durch Angabe eines IP-Bereichs identifizieren, der von CX Agent gescannt werden sollte. Beide Ansätze nutzen SNMP (Simple Network Management Protocol) zur Erkennung und SSH (Secure Shell) für die Verbindung. Diese müssen ordnungsgemäß konfiguriert werden, damit die Telemetriesammlung erfolgreich durchgeführt werden kann.

Um andere Ressourcen als Datenquellen hinzuzufügen, verwenden Sie eine der folgenden Optionen:

- Hochladen einer Seed-Datei mithilfe einer Seed-Dateivorlage
- Bereitstellen eines IP-Adressbereichs

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 der CX Agent unterstützt SNMPv2c und SNMPv3, und es können entweder eine oder beide Versionen konfiguriert werden. Dieselben Informationen, die weiter unten 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 Sicherheit und Remote-Konfigurationsmodell. SNMPV3 verwendet ein erweitertes kryptografisches Sicherheitssystem, das die SHA-Verschlüsselung unterstützt, um Nachrichten zu authentifizieren und ihre Privatsphäre zu gewährleisten. Es wird empfohlen, SNMPv3 in allen öffentlichen und internetbasierten Netzwerken zu verwenden, um Schutz vor Sicherheitsrisiken und -bedrohungen zu bieten. In 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 werden, versucht der CX-Agent standardmäßig, mit jedem entsprechenden Gerät über SNMPv3 zu kommunizieren, und kehrt zu SNMPv2c zurück, wenn die Kommunikation nicht erfolgreich verlaufen kann ausgehandelt.

Verbindungsprotokolle

Bei der Einrichtung der direkten Geräteverbindung müssen Benutzer Details zum Geräteverbindungsprotokoll angeben: SSH (oder alternativ Telnet). SSHv2 sollte 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 kompromittiert werden, wenn sie sich auf SSHv1 verlassen. Telnet ist auch unsicher. Anmeldeinformationen (z. B. Benutzernamen und Kennwörter), die über Telnet übermittelt werden, sind nicht verschlüsselt und daher gefährdet, da

keine zusätzliche Sicherheit gegeben ist.

Einschränkungen bei 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.
- Wenn ein Gerät aus der Seed-Datei oder der Sammlung von IP-Adressbereichen ebenfalls Teil des Catalyst Center-Bestands ist, wird das Gerät nur einmal für den Catalyst Center-Eintrag gemeldet. Die entsprechenden Geräte innerhalb der Seed-Datei oder des IP-Bereichs werden übersprungen, um eine Duplizierung zu vermeiden.
- Cisco IP-Telefone werden von CX Cloud für die Datenerfassung durch CX Agent nicht unterstützt. Cisco IP-Telefone werden daher nicht in der Ressourcenliste angezeigt.

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 die Telemetrie von CX Agent erfasst werden soll. 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 Agent versucht, eine Verbindung mit den Geräten herzustellen, kann diese jedoch möglicherweise nicht verarbeiten, um sie auf den Seiten "Ressourcen" anzuzeigen, falls er nicht in der Lage ist, die PIDs oder Seriennummern zu ermitteln.

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.

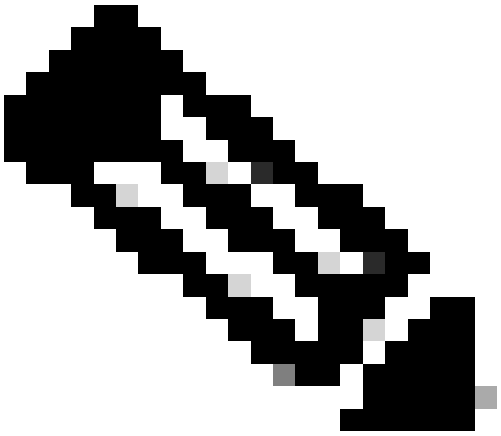
Benutzer können eine Common Services Platform Collector (CSPC)-Seed-Datei auf die gleiche Weise hochladen wie eine Standard-CX Cloud-Seed-Datei, und jede erforderliche Neuformatierung wird in der CX-Cloud verwaltet.

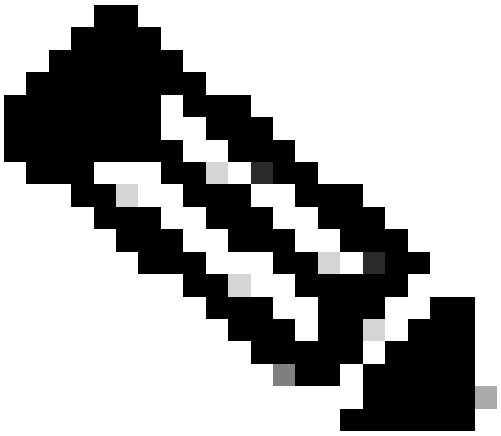
Für CX Agent v3.1 und höher können Kunden Seed-Dateien im CSPC- oder CX-Format hochladen. nur das CX-Format Seed File wird für frühere CX Agent-Versionen unterstützt.

Es ist wichtig, dass das Format der Beispiel-Seed-Datei, einschließlich der Spaltenüberschriften, in keiner Weise geändert wird.

In der folgenden Tabelle werden alle erforderlichen Seed-Dateispalten und die Daten angegeben, 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 Agent benötigt und zur Geräteerkennung im Kundennetzwerk verwendet. Werte können snmpv2c oder snmpv3 sein, aber aus Sicherheitsgründen wird snmpv3 empfohlen.
C	snmpRo: Obligatorisch, 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	snmpv3Benutzername: Obligatorisch, 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.
O	snmpv3AuthAlgorithmus: Werte können MD5 oder SHA sein.	Das SNMPv3-Protokoll ermöglicht die Authentifizierung entweder über Message Digest (MD5) oder Secure Hash Algorithm (SHA). Wenn das Gerät mit sicherer Authentifizierung konfiguriert ist, muss der jeweilige Auth-Algorithmus angegeben werden.

Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
		 Anmerkung: 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
		 Anmerkung: 56-Bit-Schlüssel, die vom Data Encryption Standard (DES) verwendet werden, gelten als zu kurz, um kryptografische Sicherheit zu bieten, und der Triple Data Encryption Standard (3DES) kann auf allen Geräten verwendet werden, die ihn 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 ID für Gerät, Engine-ID angeben, wenn manuell auf 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 Agent als Referenz gesendet. Wenn der Kunde die EngineID manuell konfiguriert, muss die entsprechende EngineID angegeben werden.
J	CLI-Protokoll: Werte können 'telnet', 'sshv1', 'sshv2' sein. Wenn leer, kann standardmäßig 'sshv2' eingestellt werden	Die Befehlszeilenschnittstelle (CLI, Command Line Interface) ist für die direkte Interaktion mit dem Gerät vorgesehen. CX Agent verwendet dieses Protokoll für die CLI-Erfassung für ein bestimmtes Gerät. Diese CLI-Erfassungsdaten werden für Ressourcen- und andere Insights-

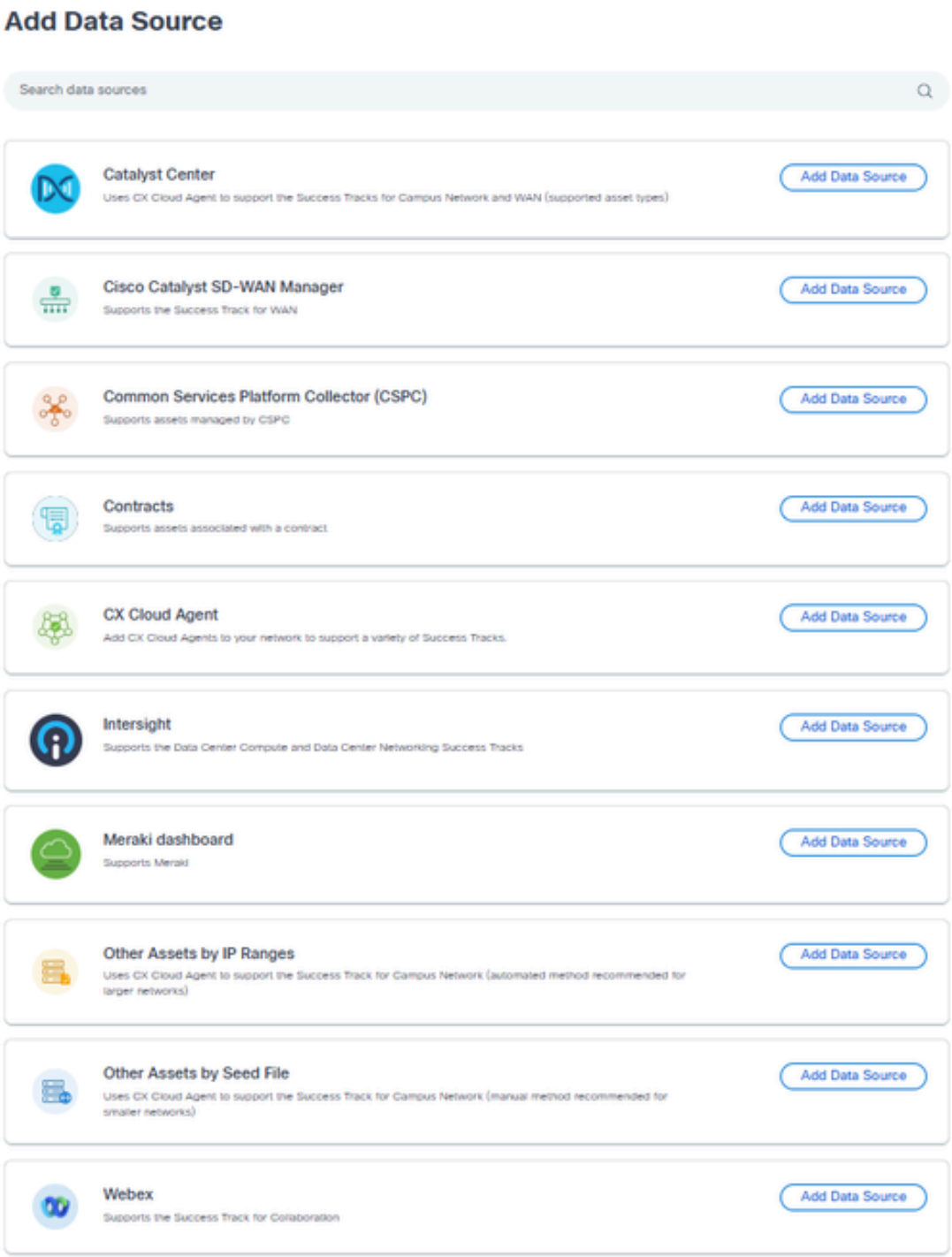
Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
		Berichte in der CX Cloud verwendet. SSHv2 wird empfohlen; ohne andere Netzwerksicherheitsmaßnahmen SSHv1 und Telnet-Protokolle allein keine ausreichende Transportsicherheit bieten.
K	CLI-Port: CLI-Protokoll-Portnummer	Wenn ein CLI-Protokoll ausgewählt wird, muss die entsprechende Portnummer angegeben werden. Beispiel: 22 für SSH und 23 für Telnet.
L	CLI-Benutzer: CLI-Benutzername (entweder CLI-Benutzername/Kennwort oder BEIDE können angegeben werden, ABER beide Spalten (Spalte#=12 und Spalte#=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	CLI-Kennwort: CLI-Benutzerkennwort (entweder CLI-Benutzername/Kennwort oder BEIDE können angegeben werden, ABER beide Spalten (Spalte#=12 und Spalte#=13) dürfen nicht leer sein.)	Das entsprechende CLI-Kennwort des Geräts muss angegeben werden. Dies wird von CX 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.

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

Hinzufügen weiterer Ressourcen mit einer neuen Seed-Datei

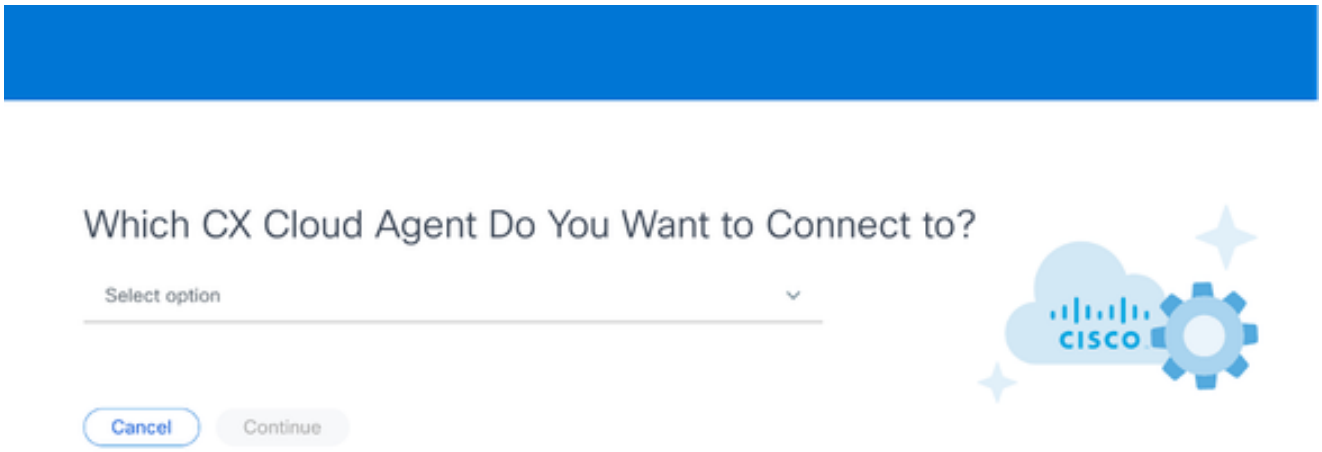
So fügen Sie andere Ressourcen mit einer neuen Seed-Datei hinzu:

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



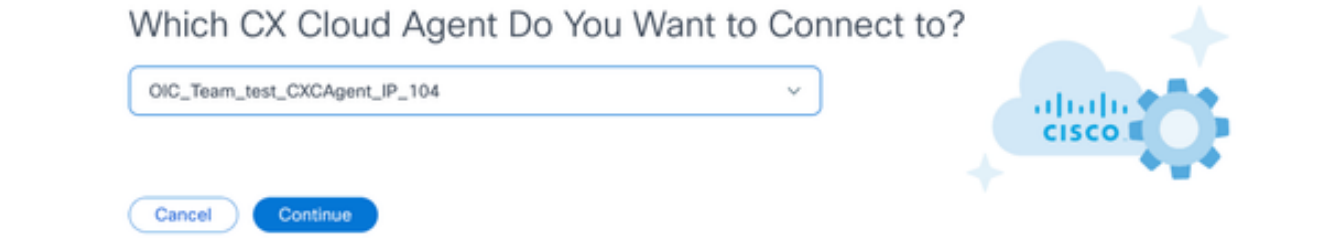
Datenquelle hinzufügen

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



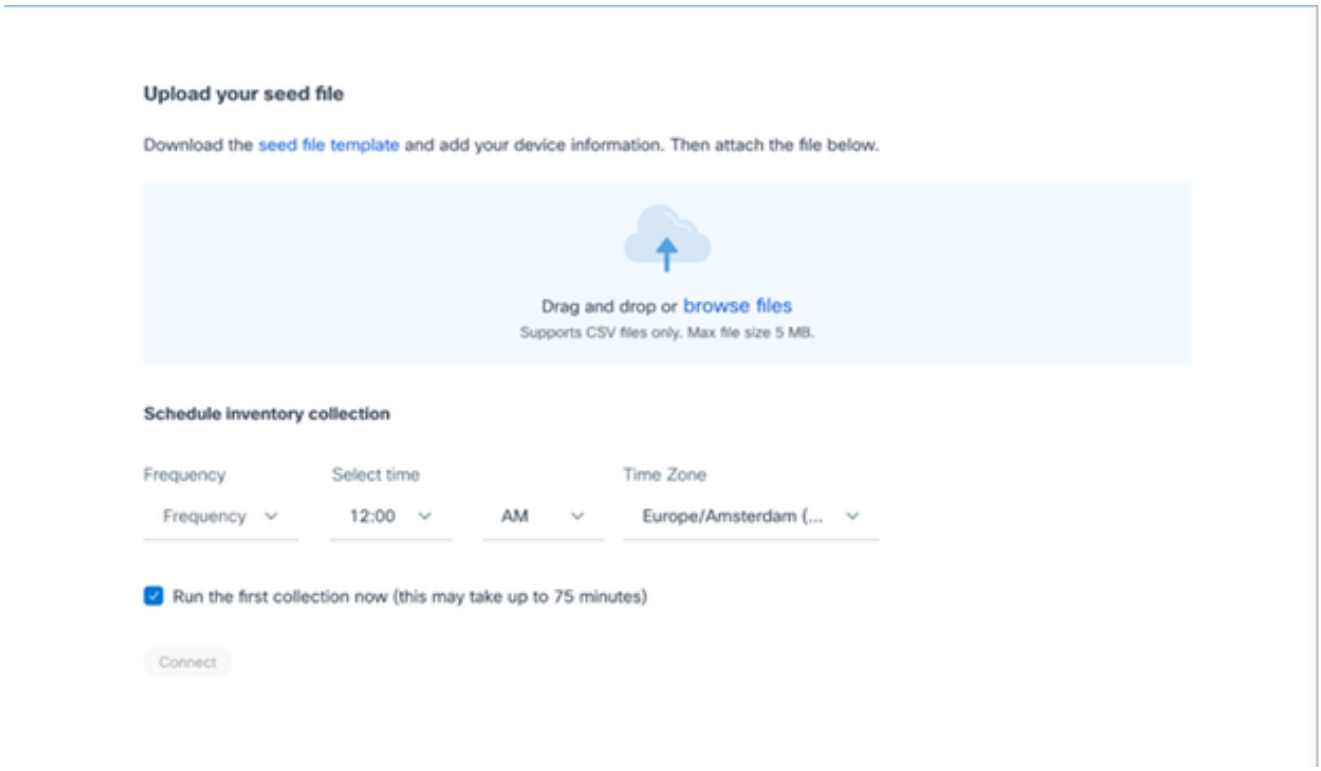
CX-Agent auswählen

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



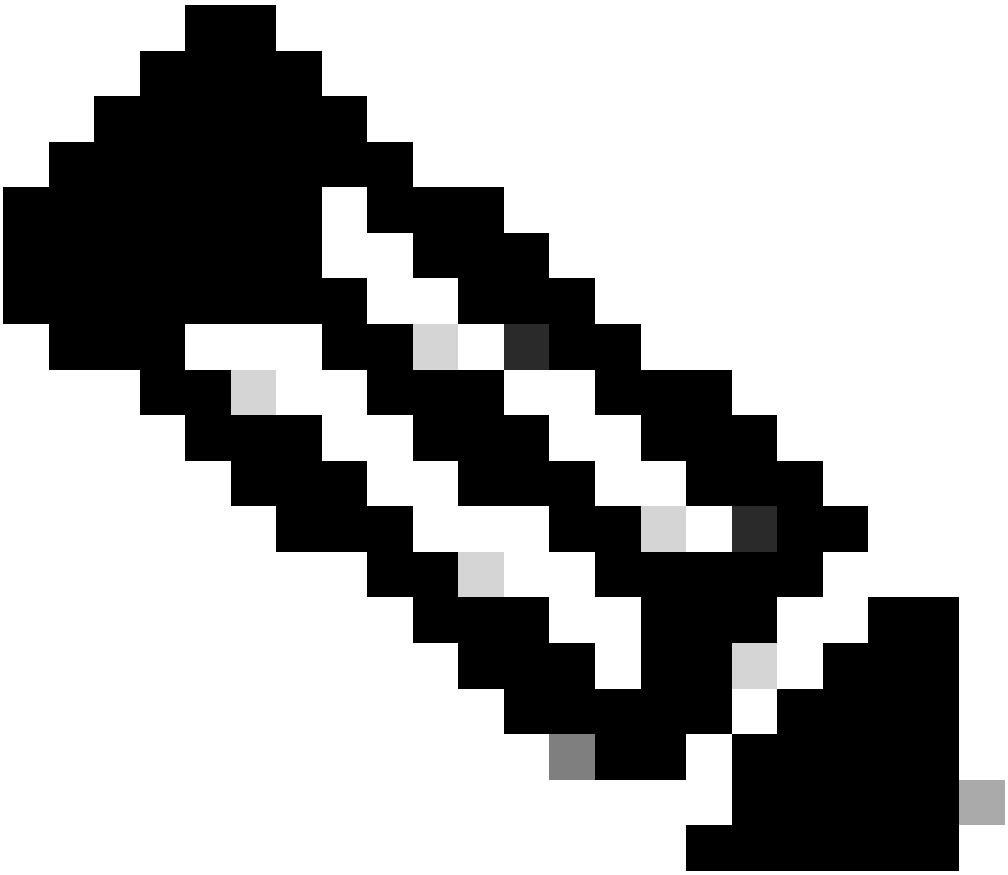
Fortfahren

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 den CX 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.



Anmerkung: Bevor die Erstkonfiguration der CX Cloud abgeschlossen ist, muss der CX Cloud Agent die erste Telemetriesammlung durchführen, indem er die Seed-Datei verarbeitet und eine Verbindung mit allen identifizierten Geräten herstellt. 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.

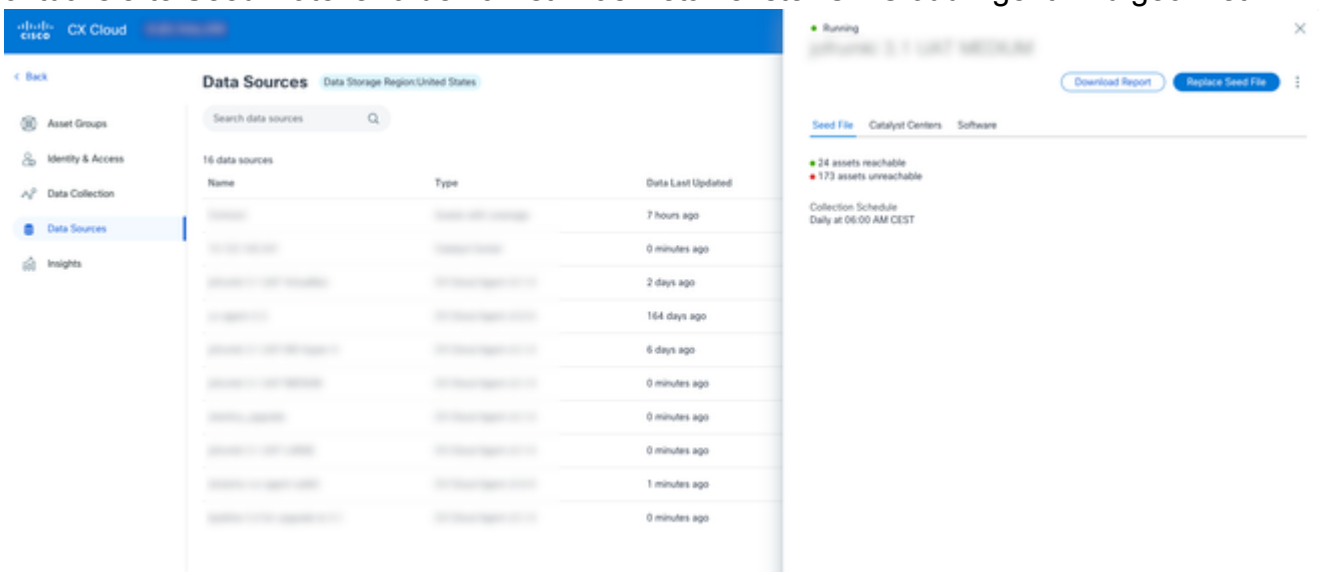
Hinzufügen weiterer Ressourcen mit einer geänderten Seed-Datei

So fügen Sie Geräte mit 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.

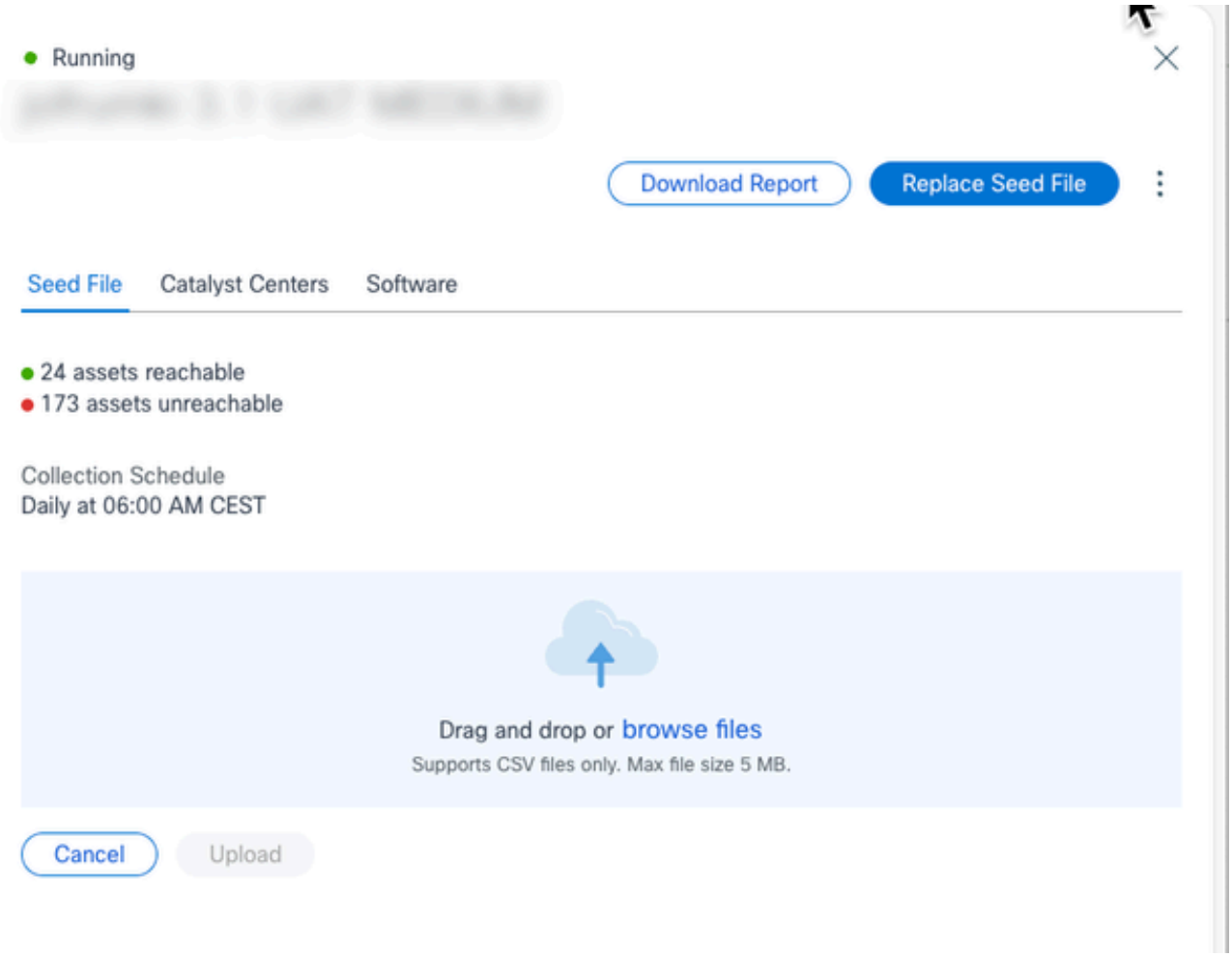
Anmerkung: Um der Seed-Datei Assets hinzuzufügen, fügen Sie diese Assets an die zuvor erstellte Seed-Datei an, und laden Sie die Datei neu. Dies ist notwendig, da das Hochladen einer neuen Seed-Datei die aktuelle Seed-Datei ersetzt. Nur die zuletzt hochgeladene Seed-Datei wird für die Erkennung und Sammlung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

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



Startdatei

3. Klicken Sie auf Seed-Datei ersetzen.



Seed-Datei ersetzen

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

Standardanmeldeinformationen für die Seed-Datei

CX Agent stellt die Standardanmeldeinformationen bereit, die Kunden lokal in Agent einrichten können. Dadurch müssen keine sensiblen Kennwörter direkt in die Seed-Datei aufgenommen werden. Dadurch wird die Sicherheit erhöht, da vertrauliche Informationen nicht weitergegeben werden müssen und ein wichtiges Anliegen des Kunden behoben werden muss.

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-Agenten 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 der CX 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 Agent die vom Benutzer bereitgestellten Anmeldeinformationen mit jeder IP verwenden. Beispiele: 172.16.*.* lässt die Verwendung der Anmeldeinformationen für alle Geräte im Subnetz 172.16.0.0/16 zu.
- 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 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 das CX Agent-Erfassungsinventar aufzunehmen.

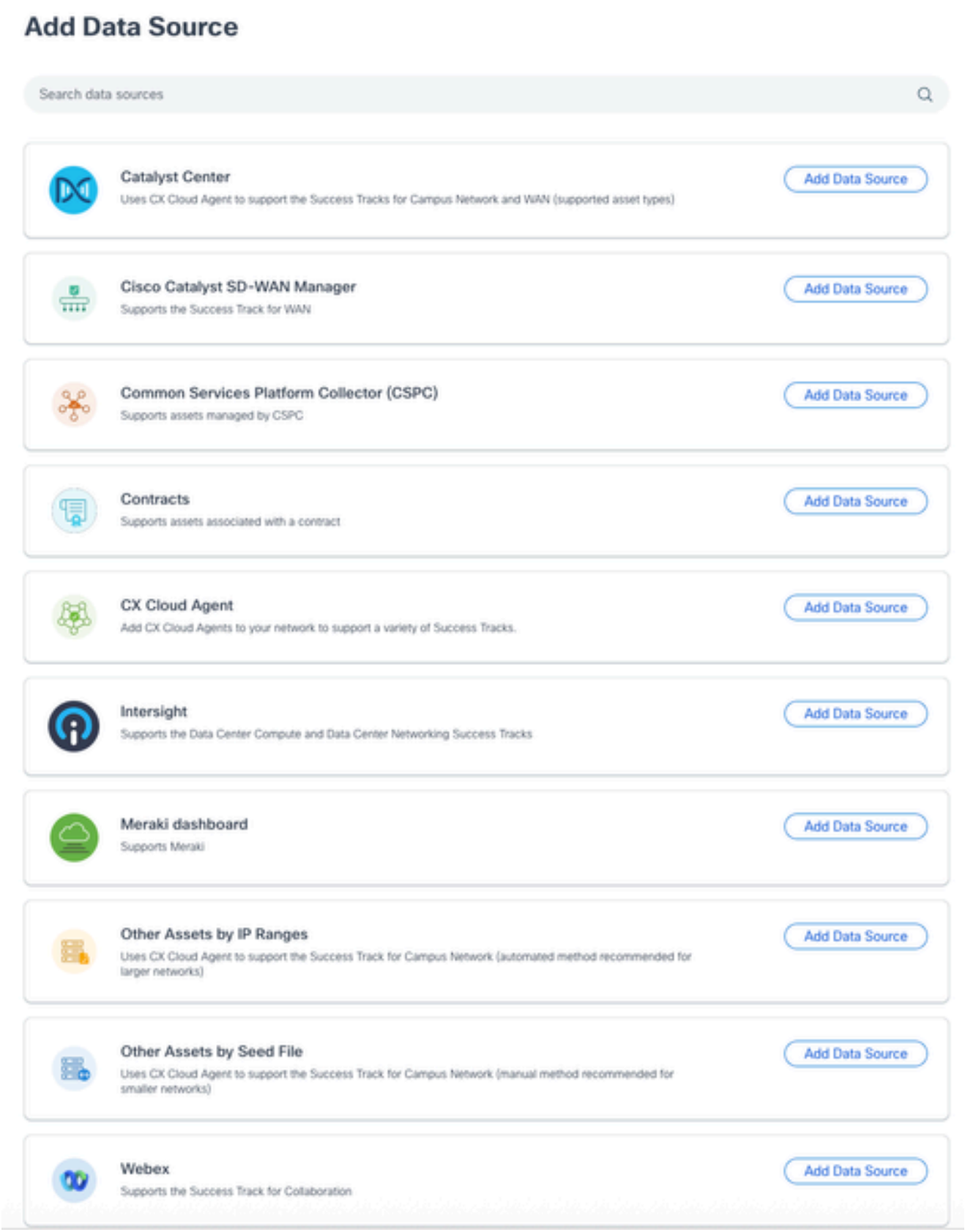
Um Geräte über einen IP-Bereich hinzuzufügen, müssen Benutzer alle anwendbaren Anmeldeinformationen über die Konfigurations-Benutzeroberfläche angeben. Die sichtbaren Felder variieren je nach den Protokollen, die in den vorherigen Fenstern ausgewählt wurden. Wenn mehrere Optionen für dasselbe Protokoll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

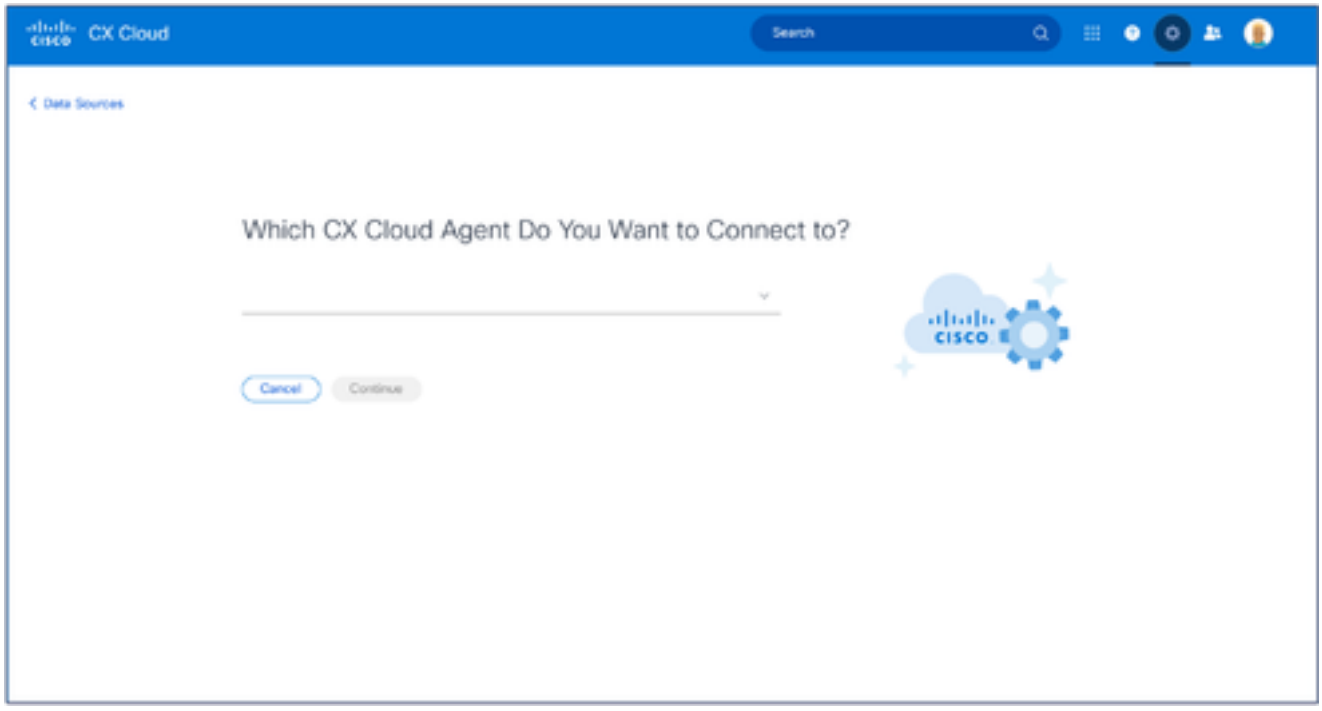
So fügen Sie Geräte über den IP-Bereich hinzu:

1. Wählen Sie das Symbol Admin Center. Das Fenster Datenquellen wird geöffnet.
2. Klicken Sie im Fenster Admin Center > Datenquellen auf Datenquelle hinzufügen.



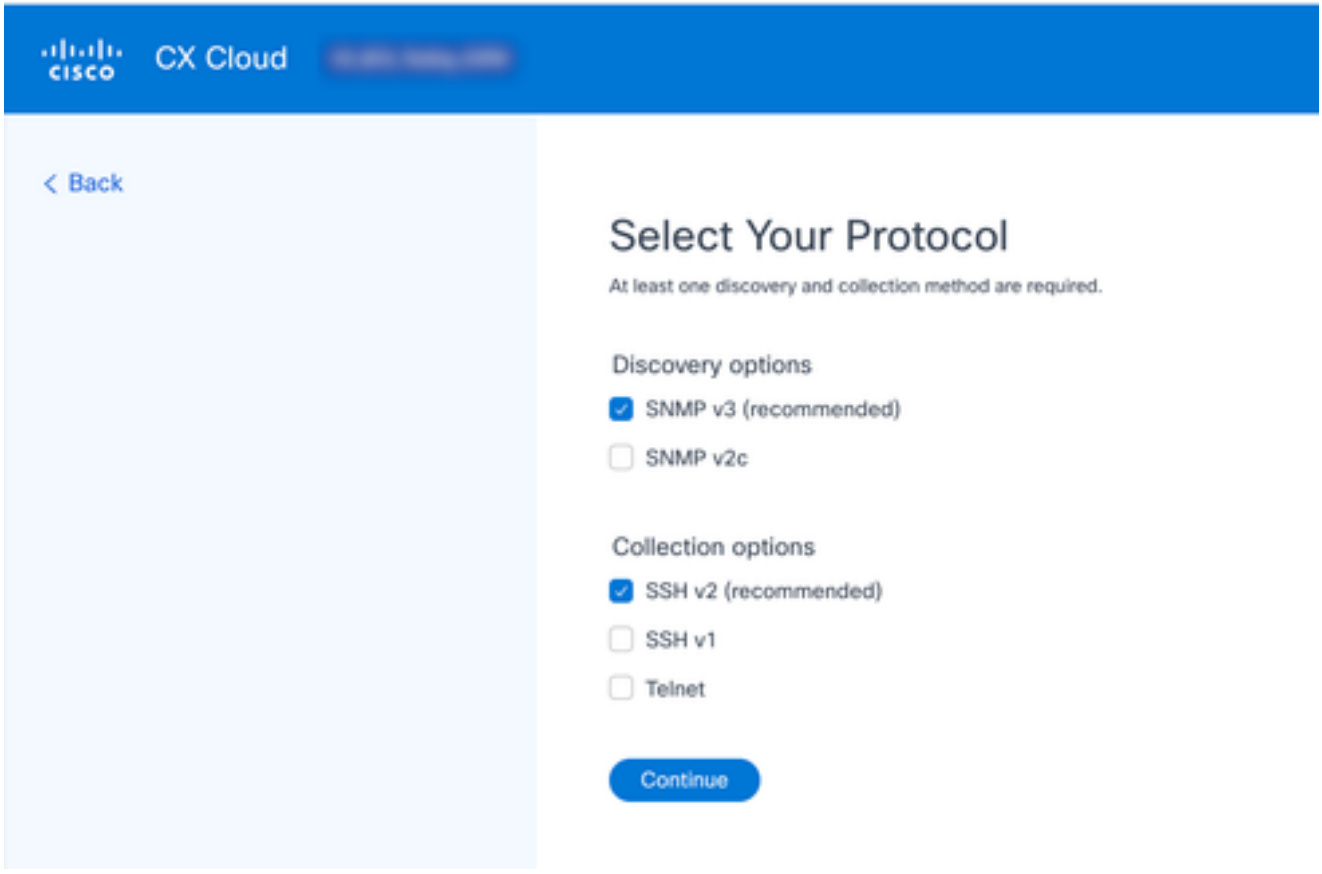
Datenquelle hinzufügen

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



CX Cloud Agent auswählen

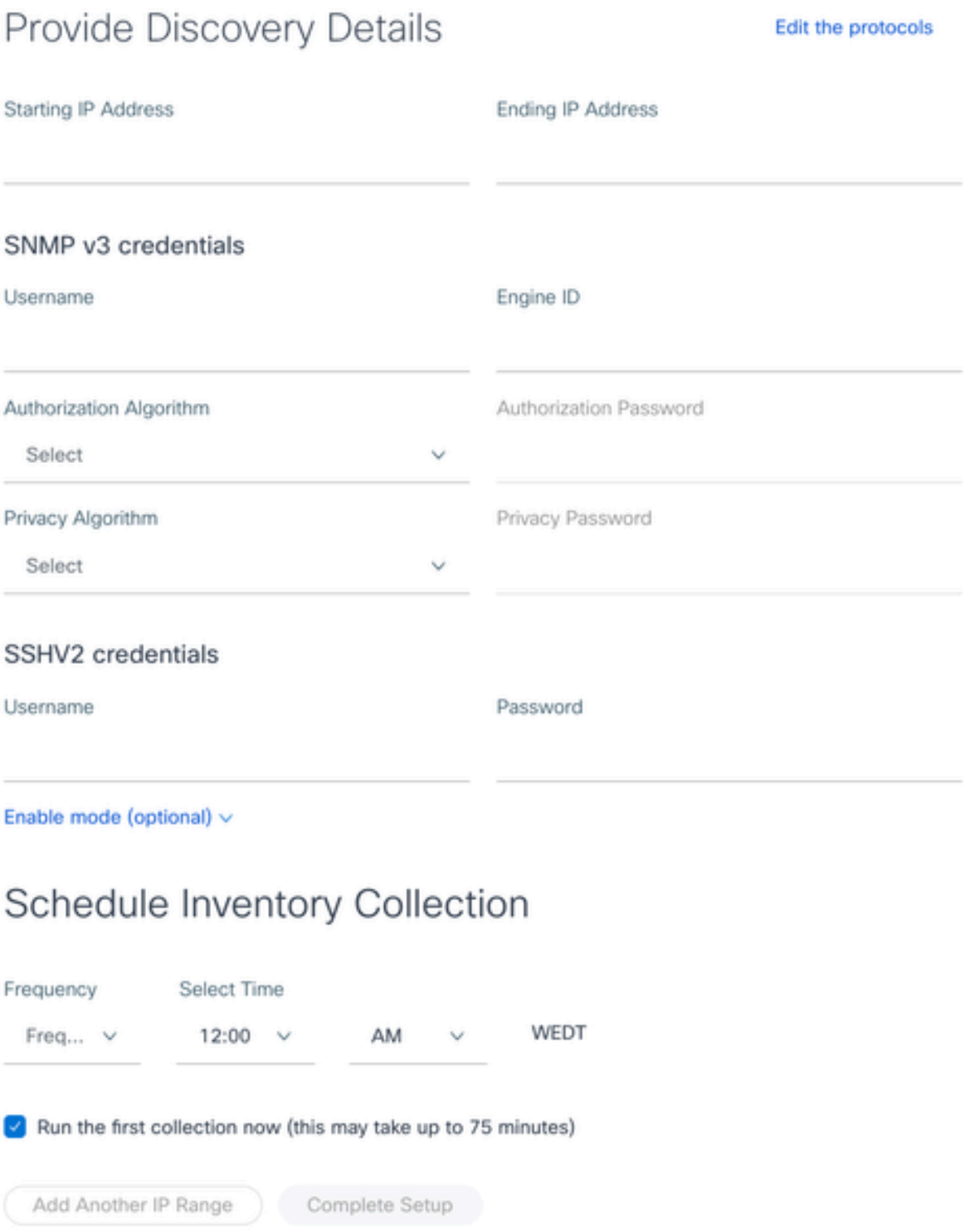
4. Wählen Sie den CX-Agenten aus der Dropdown-Liste Welchen CX Cloud-Agenten möchten Sie verbinden mit aus.
5. Klicken Sie auf Continue (Weiter). Das Fenster Protokoll auswählen wird geöffnet.



Protokoll auswählen

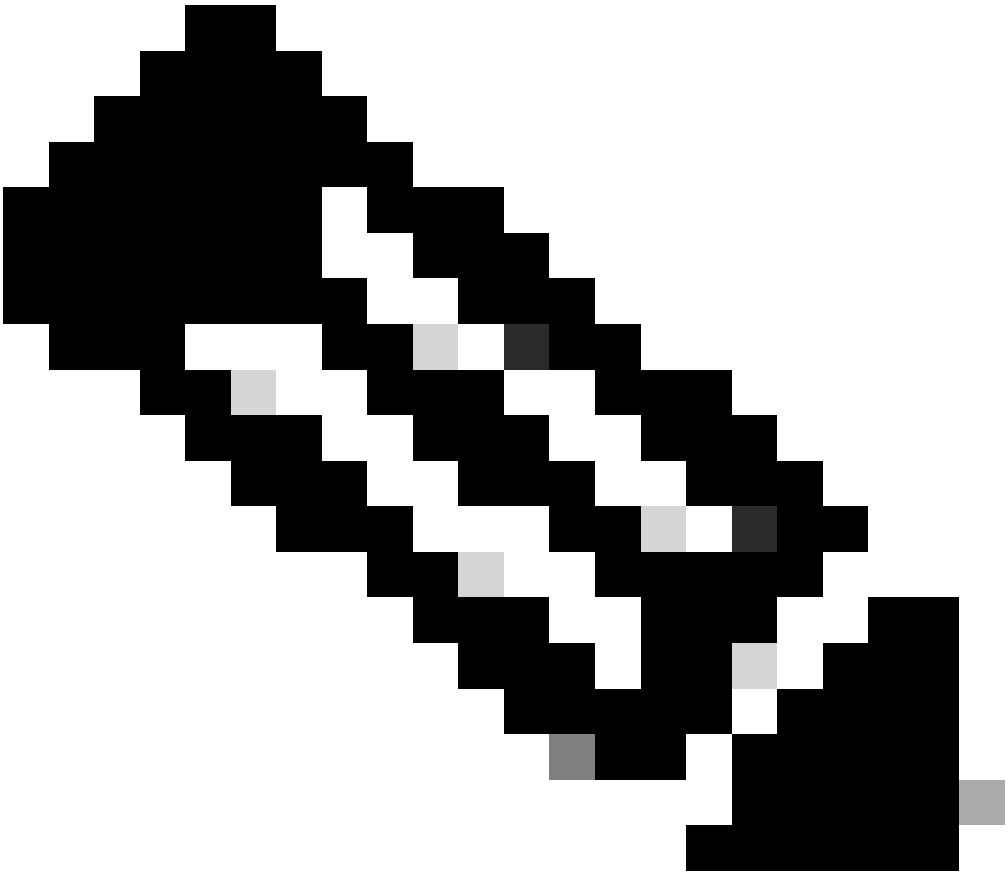
6. Aktivieren Sie die entsprechenden Kontrollkästchen für die Erkennungsoptionen und die Erfassungsoptionen.

7. Klicken Sie auf Continue (Weiter).



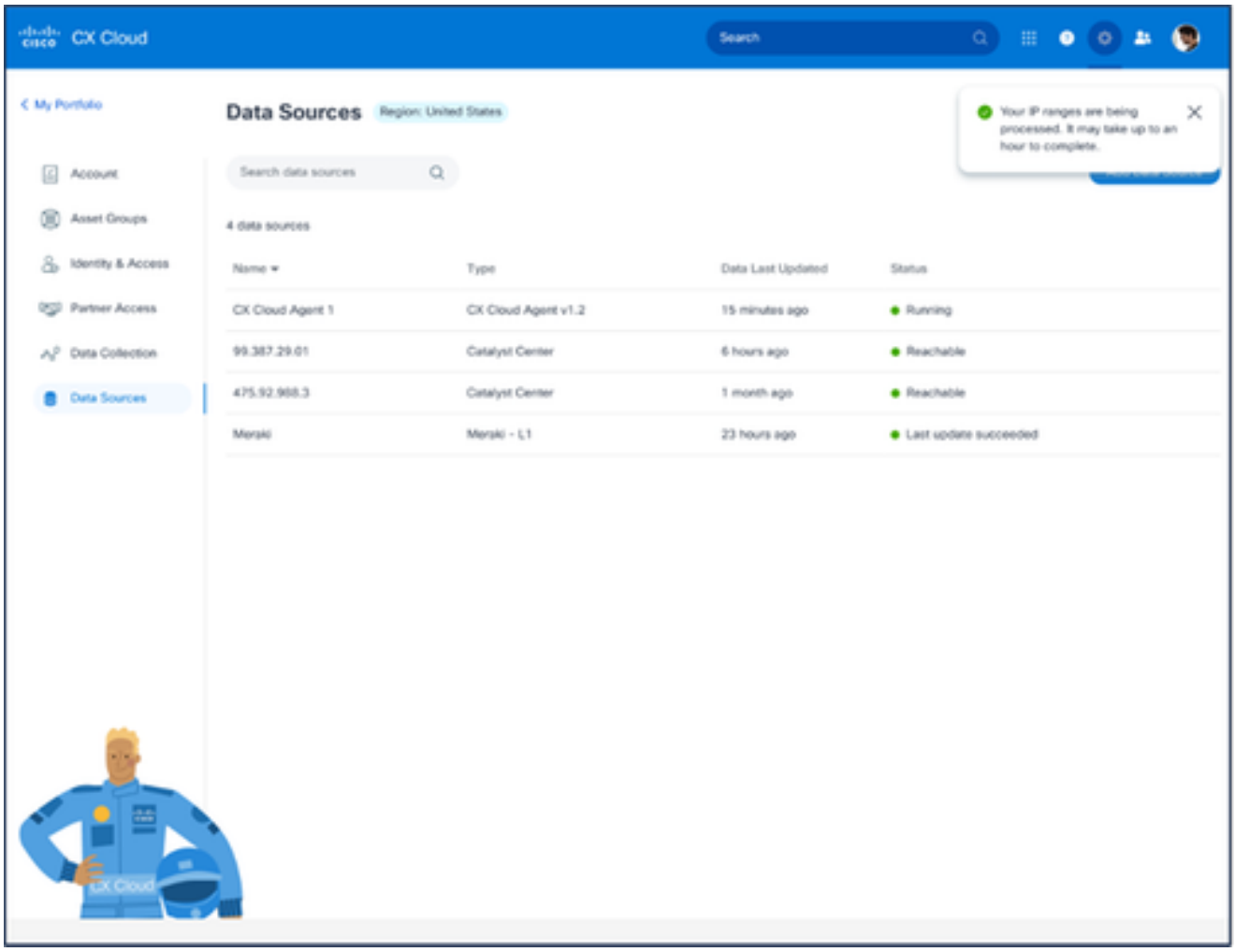
Erkennungsdetails

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



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

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

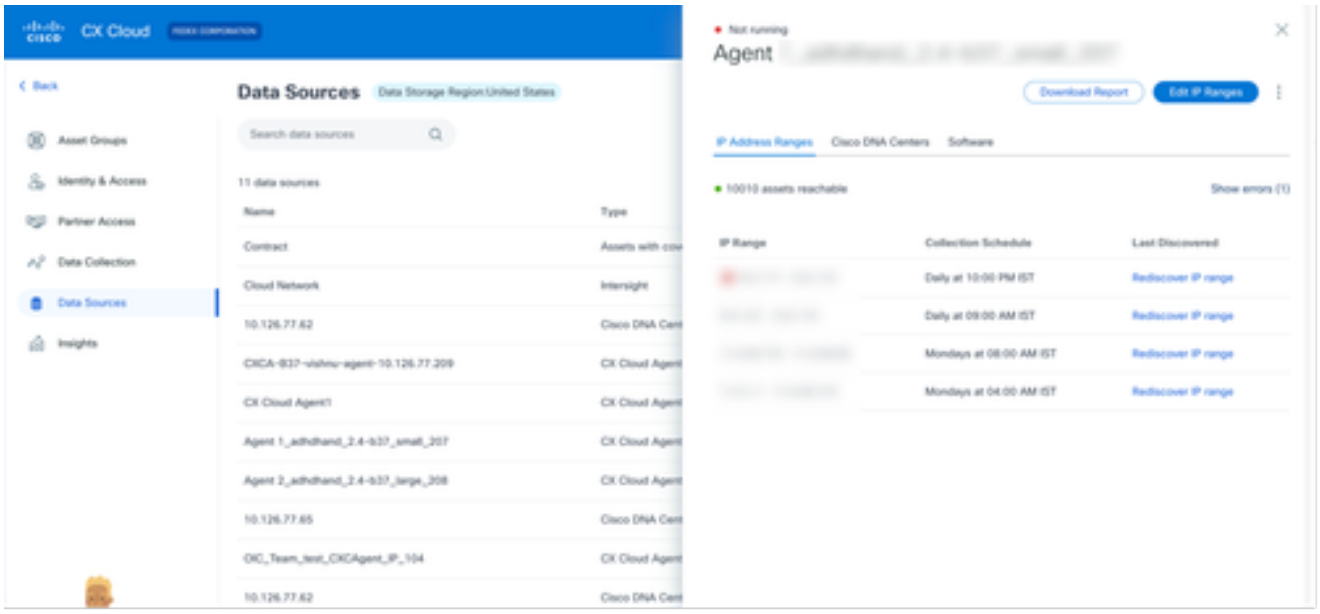


Bestätigungsmeldung

Bearbeiten von IP-Bereichen

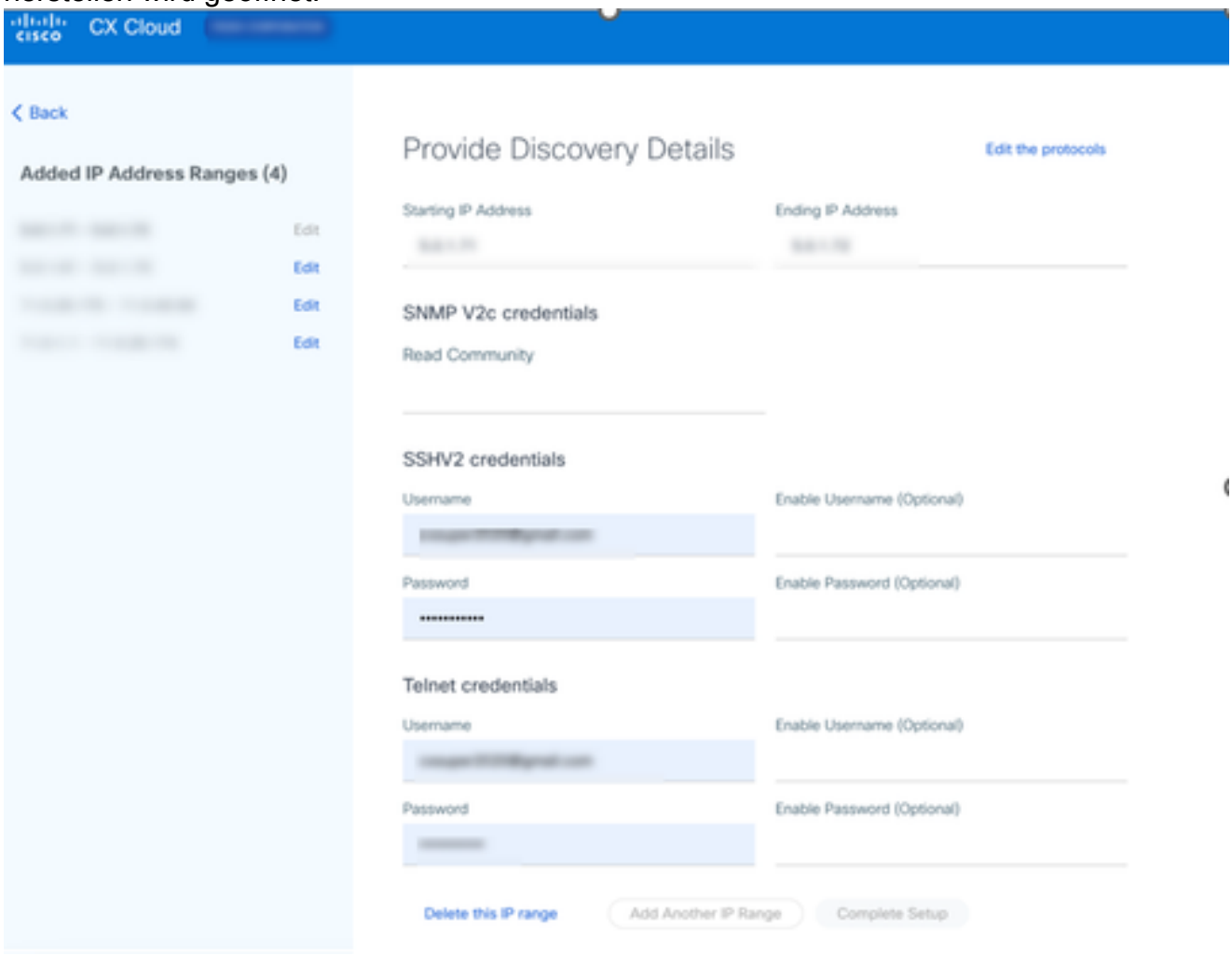
So bearbeiten Sie einen IP-Bereich:

1. Navigieren Sie in das Fenster Datenquellen.
2. Klicken Sie auf den CX-Agenten, für den die Bearbeitung des IP-Bereichs in Datenquellen erforderlich ist. Das Detailfenster wird geöffnet.

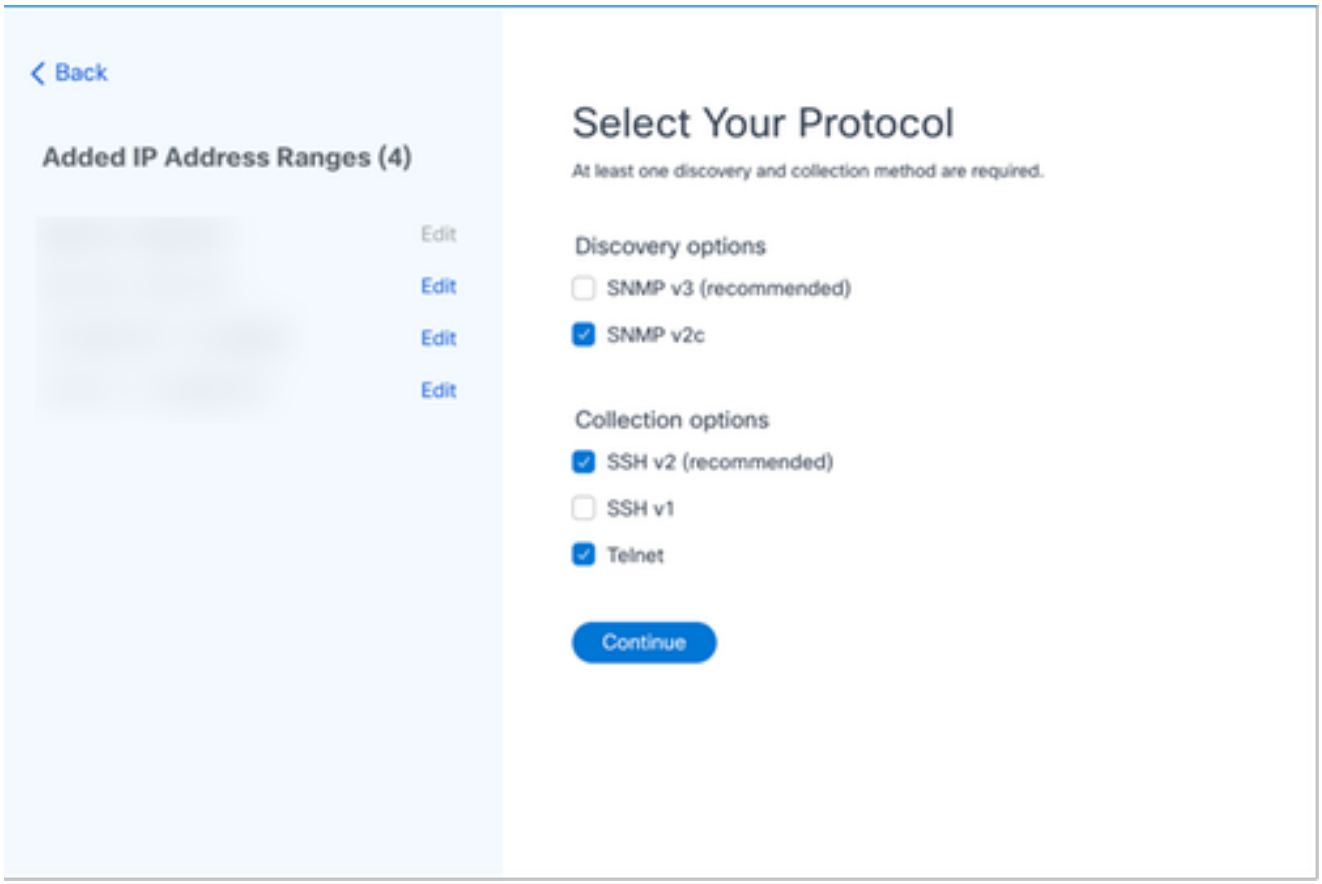


Datenquellen

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

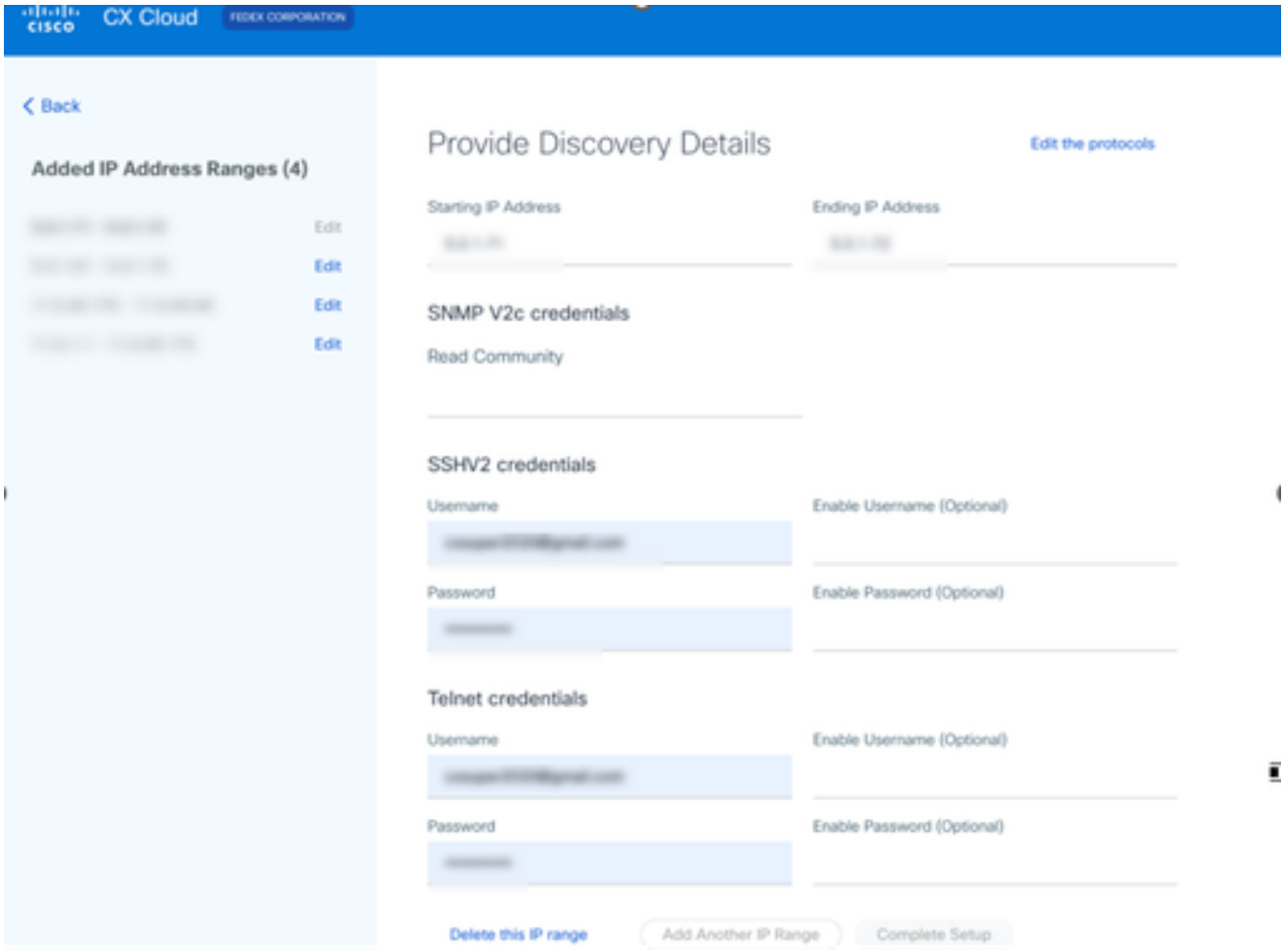


4. Klicken Sie auf Protokolle bearbeiten. Das Fenster Protokoll auswählen wird geöffnet.



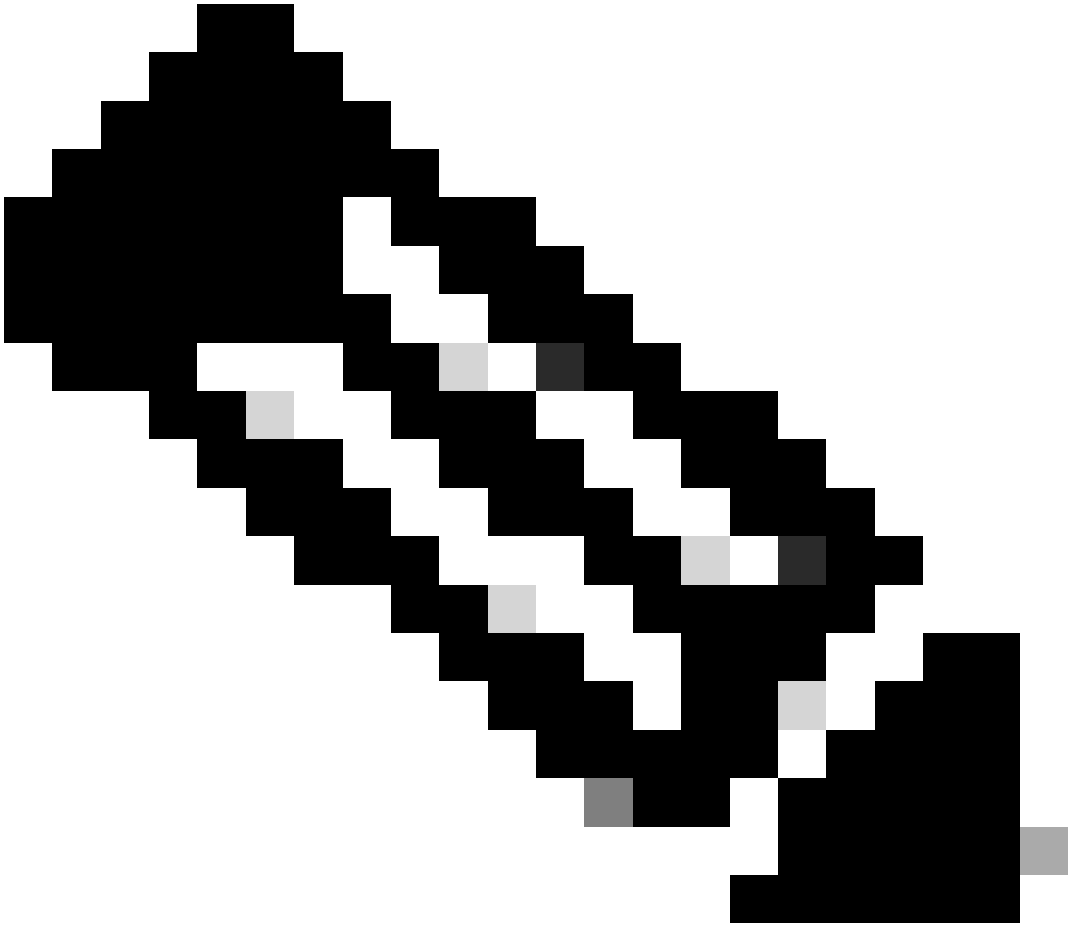
Protokoll auswählen

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.

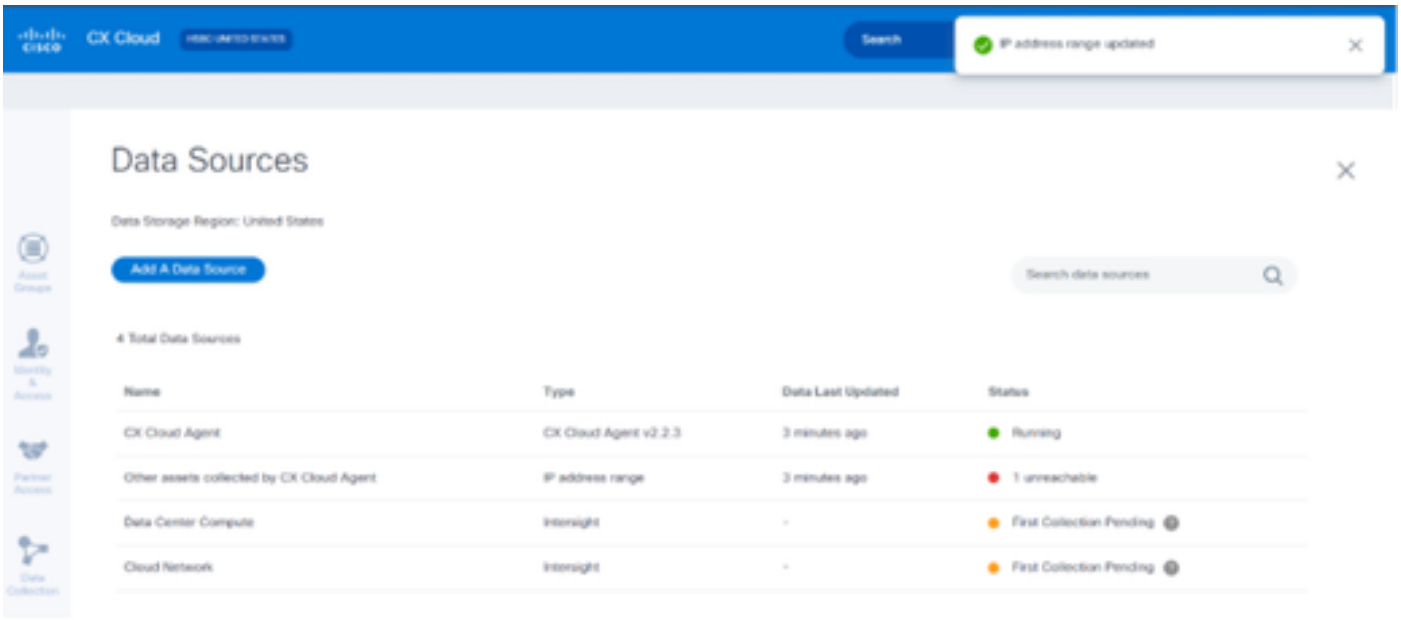


Bereitstellung von Erkennungsdetails

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.



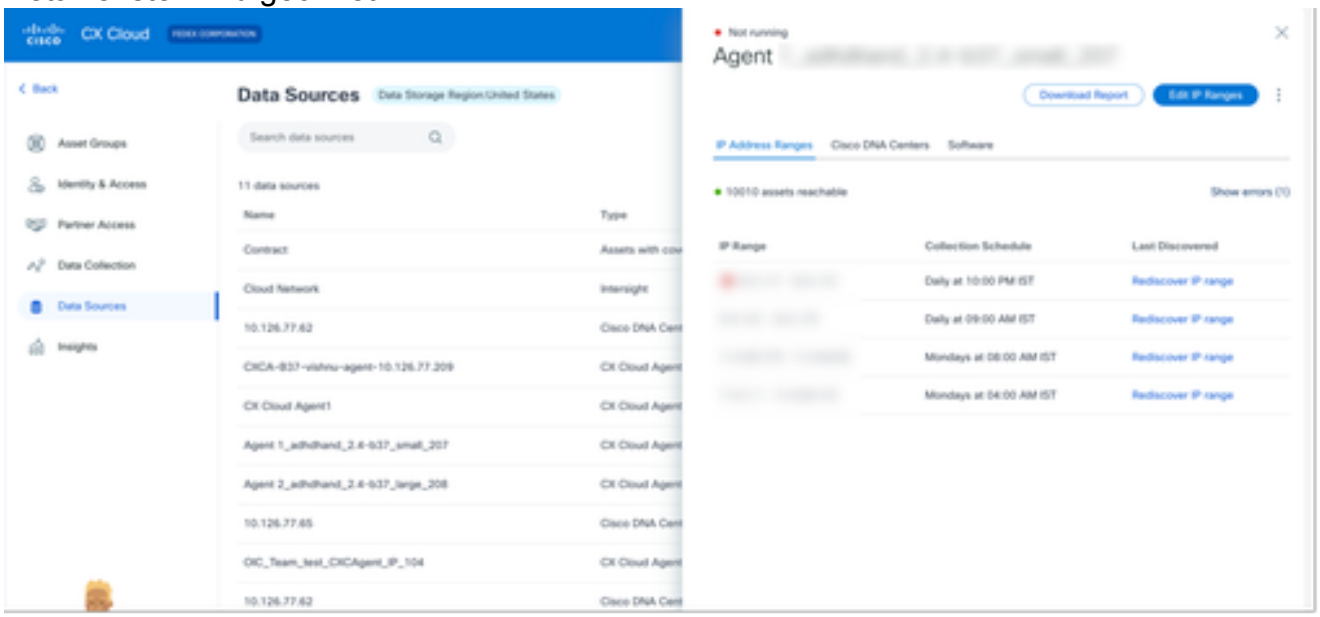
Anmerkung: Mit dieser Bestätigungsmeldung wird nicht überprüft, ob Geräte innerhalb des geänderten Bereichs erreichbar sind oder ob ihre Anmeldeinformationen akzeptiert werden. Diese Bestätigung erfolgt, wenn der Kunde den Erkennungsprozess initiiert.



IP-Bereich wird gelöscht

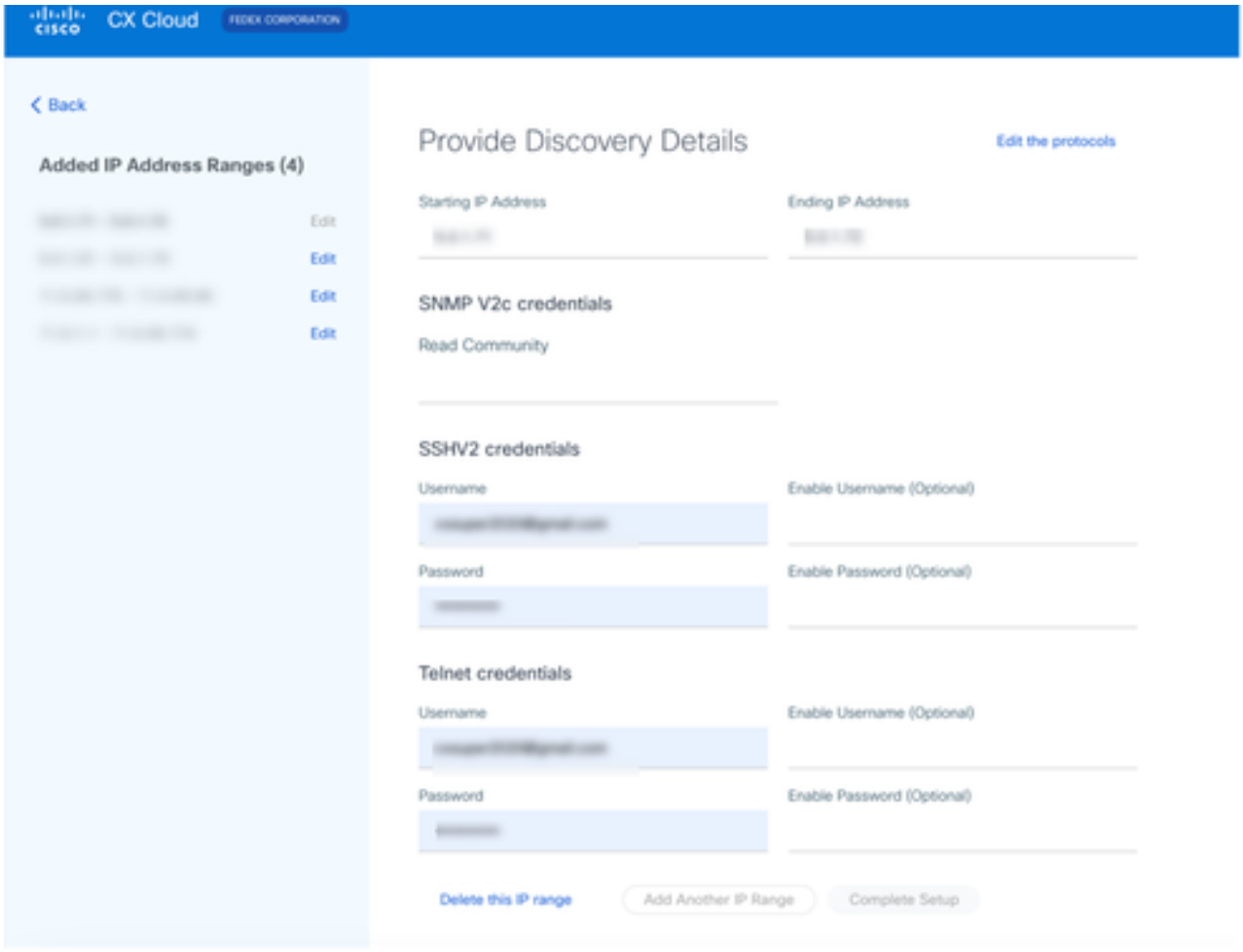
So löschen Sie einen IP-Bereich:

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



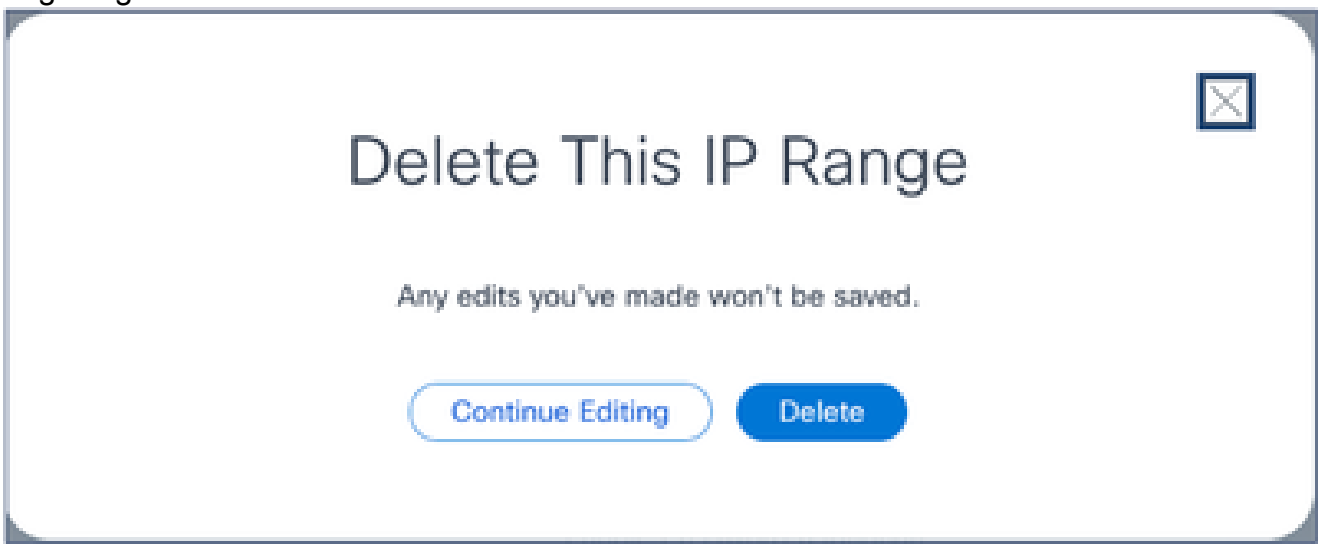
Datenquellen

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



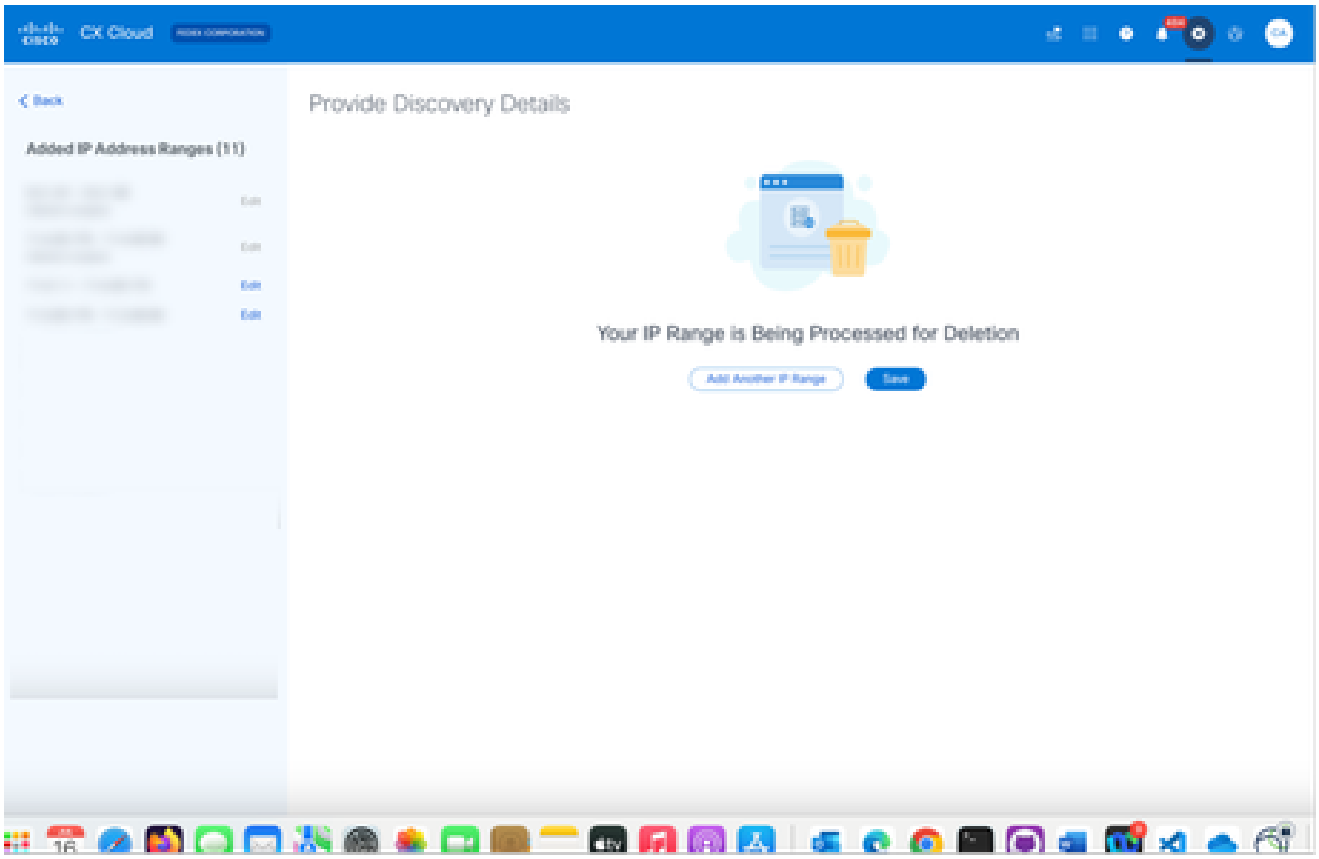
Bereitstellung von Erkennungsdetails

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



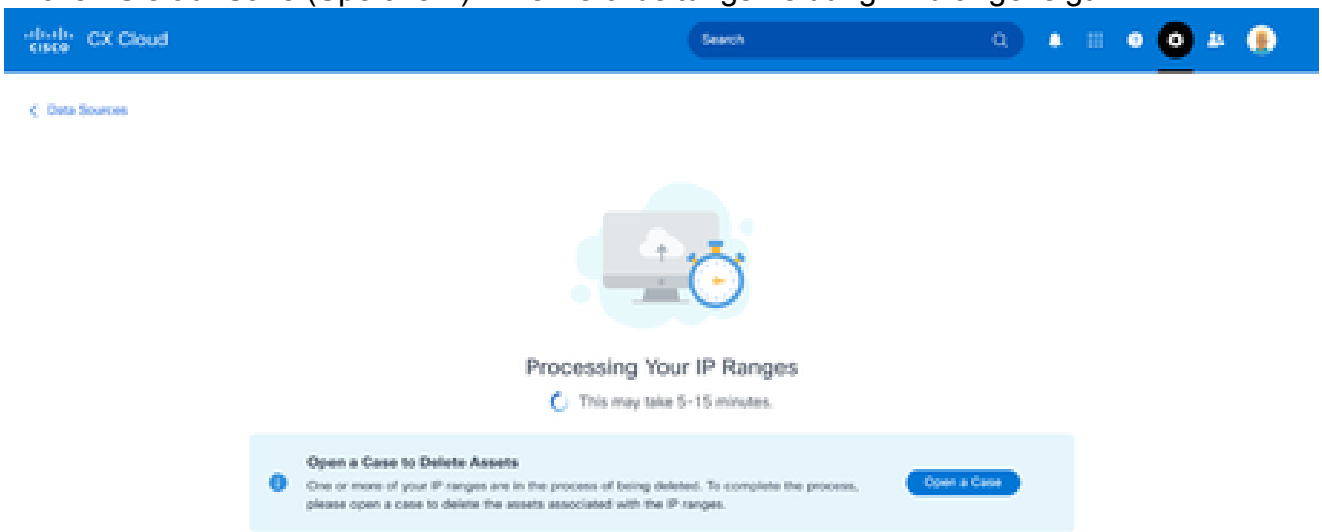
Löschen der Nachricht bestätigen

5. Klicken Sie auf Löschen.



Löschen des IP-Bereichs

6. Klicken Sie auf Save (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.

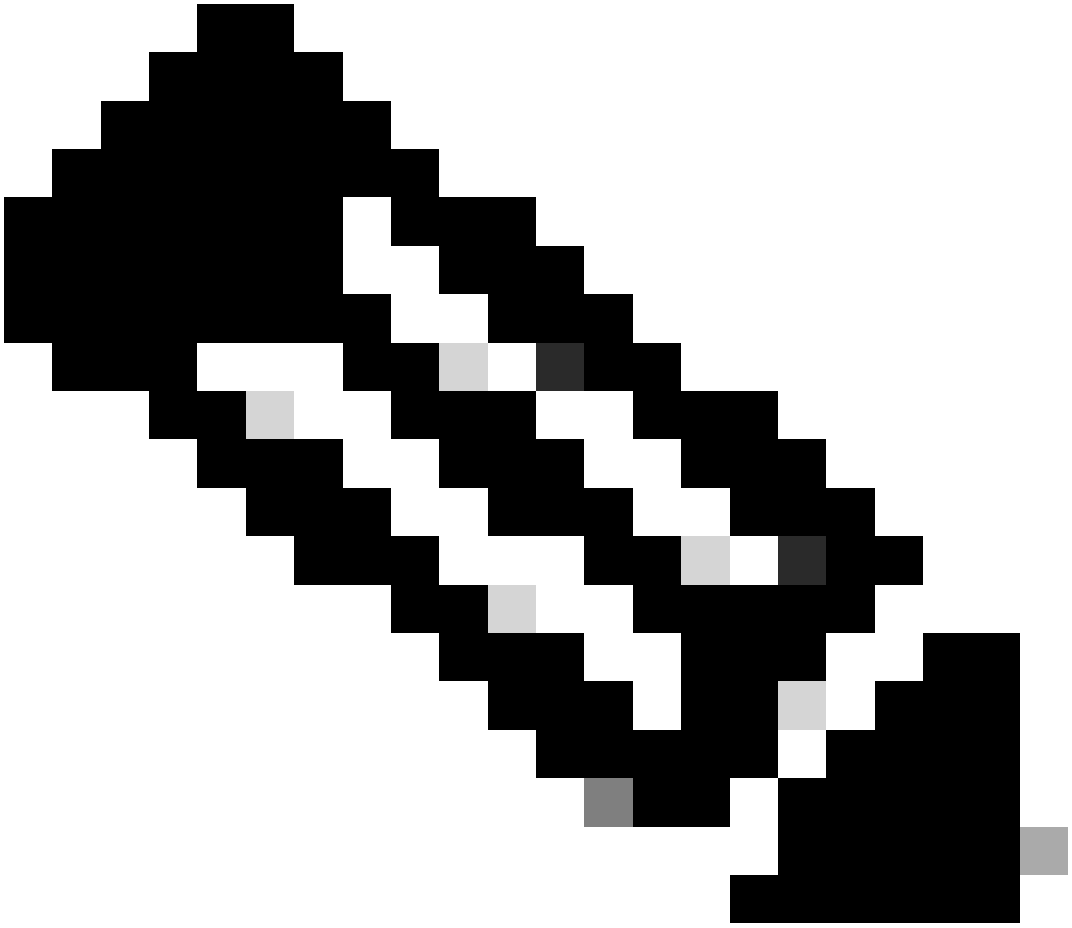
Von mehreren Controllern erkannte Geräte

Wenn sich das Catalyst Center und andere von CX Agent erfasste Ressourcen (Direct Device Connection) auf demselben CX Agent befinden, kann es sein, dass einige Geräte sowohl vom Cisco Catalyst Center als auch von der direkten Geräteverbindung zum CX Agent erkannt werden, wodurch doppelte Daten von diesen Geräten erfasst 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 der CX Agent die Geräte verwaltet.

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

Planen von Diagnosescans

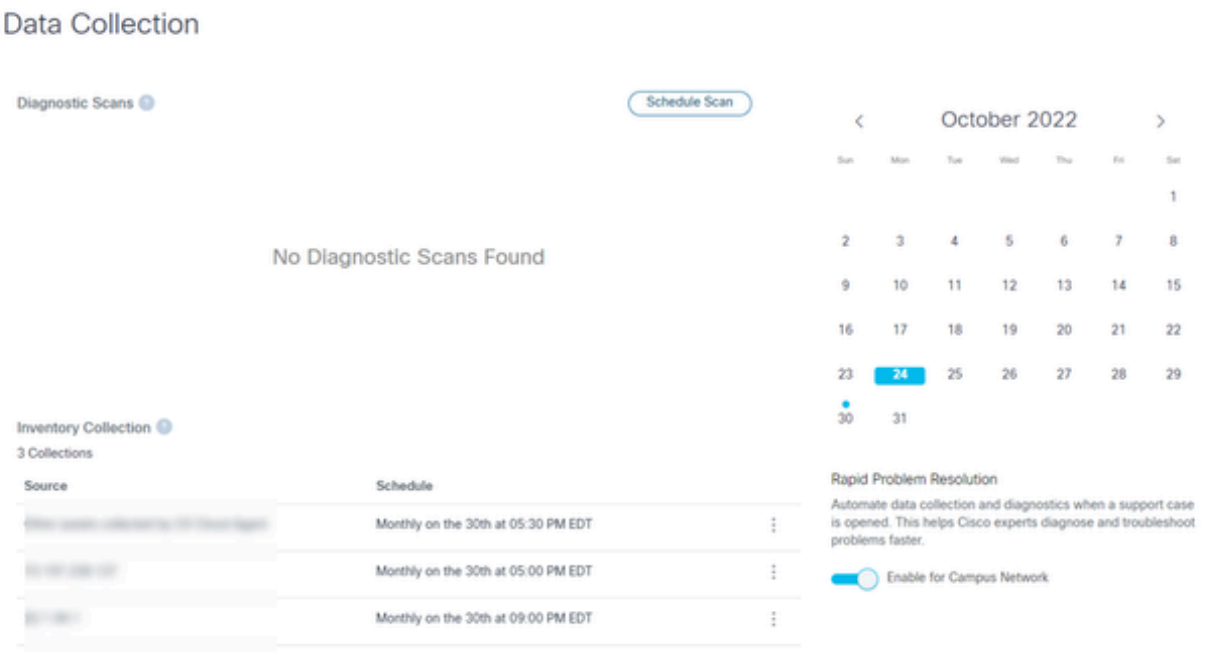
Kunden können in der CX Cloud On-Demand-Diagnosescans für qualifizierte Success Tracks und die entsprechenden Geräte planen, um die Priority Bugs in Advisories auszufüllen.



Anmerkung: Cisco empfiehlt, Diagnosescans zu planen oder bedarfsgesteuerte Scans einzuleiten, die sich mindestens sechs bis sieben Stunden von den Zeitplänen für die Bestandserfassung unterscheiden, damit sie sich nicht überschneiden. Die gleichzeitige Ausführung mehrerer Diagnosescans kann den Scanvorgang verlangsamen und möglicherweise zu Scanfehlern führen.

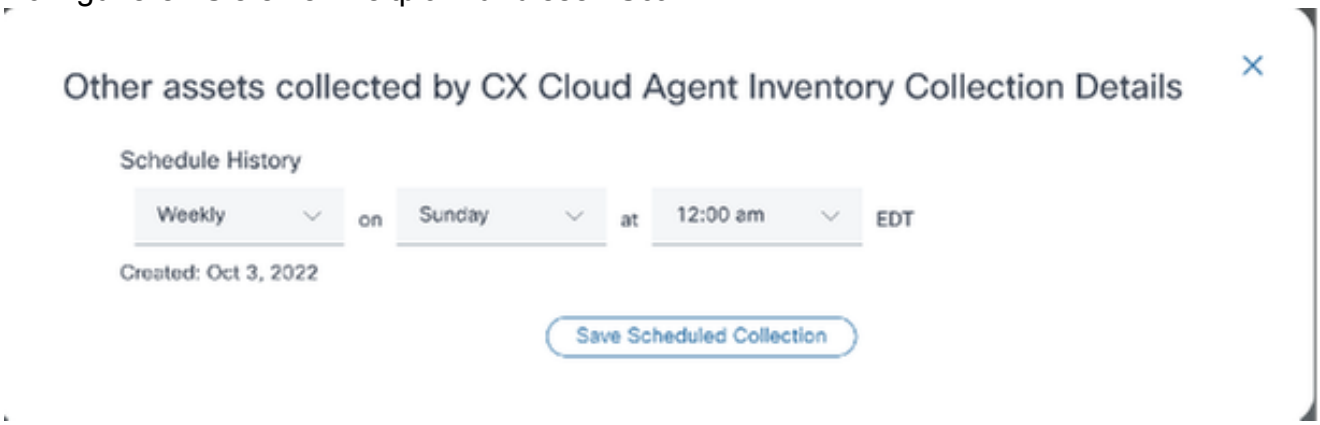
So planen Sie Diagnosescans:

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.



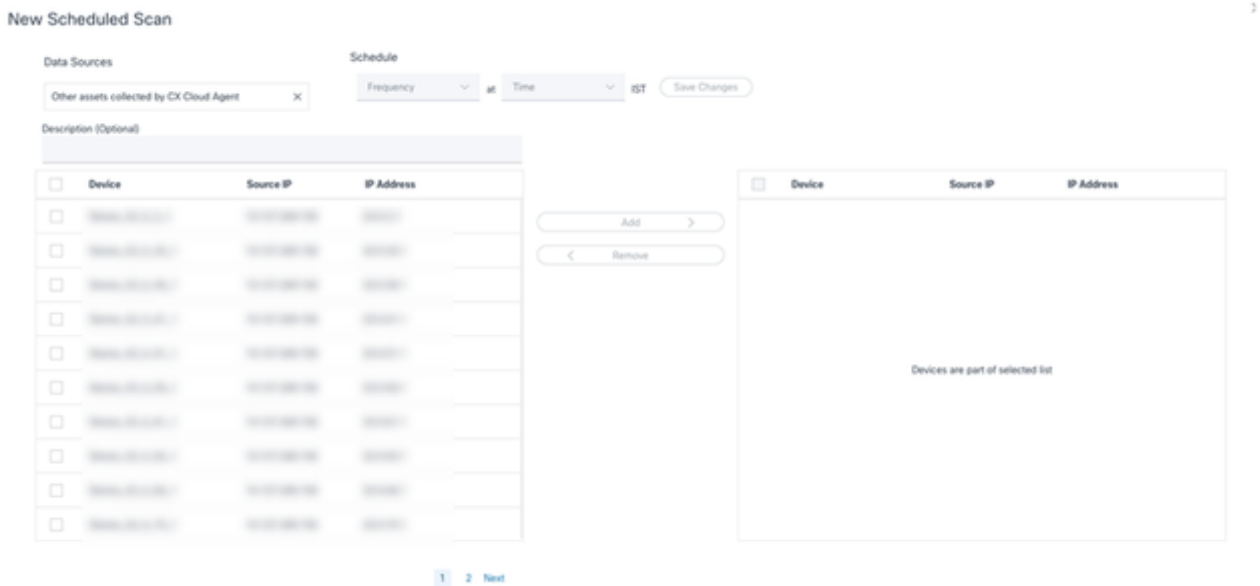
Planen von Scans

4. Konfigurieren Sie einen Zeitplan für diesen Scan.



Scan-Zeitplan konfigurieren

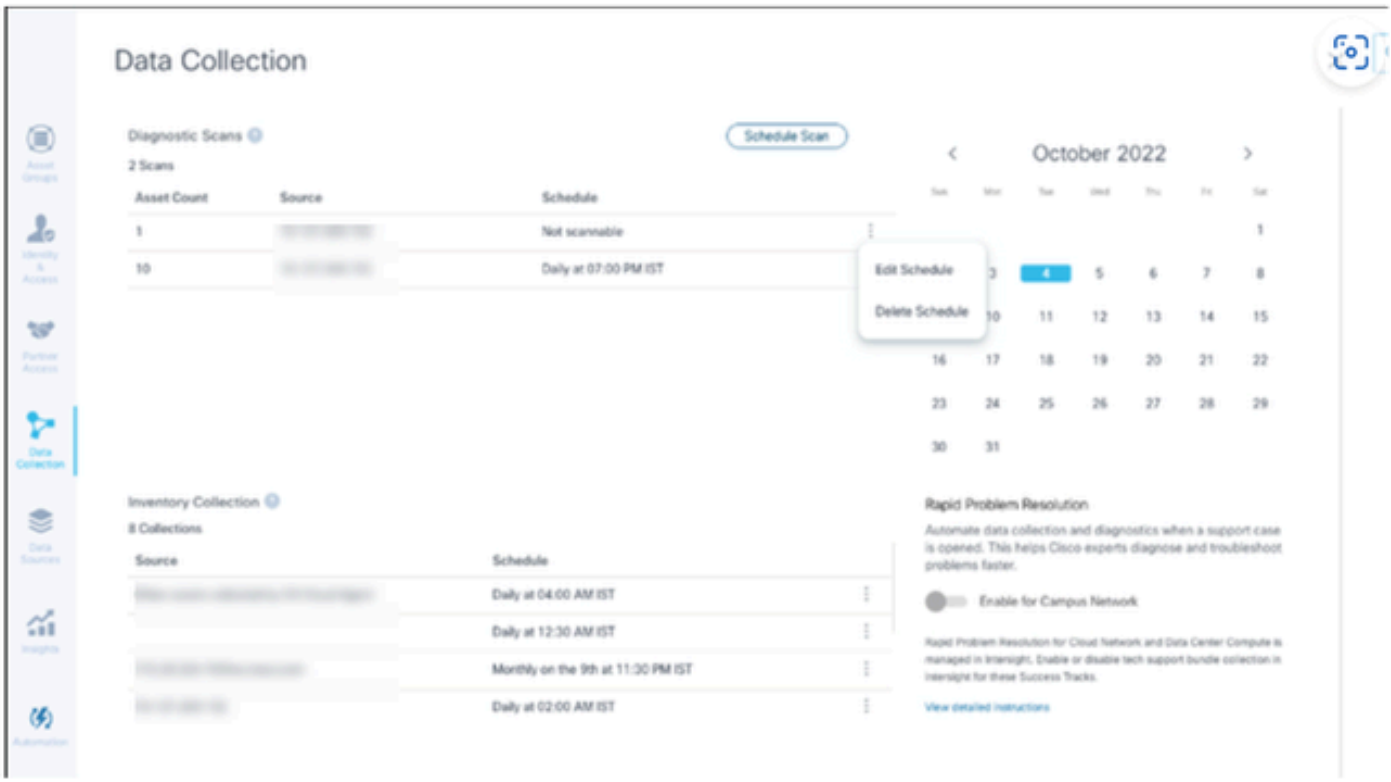
5. Wählen Sie in der Geräteliste alle Geräte für den Scan aus, und klicken Sie auf Hinzufügen.



Zeitgesteuerte Suche

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 Agent VMs auf mittlere und große Konfigurationen

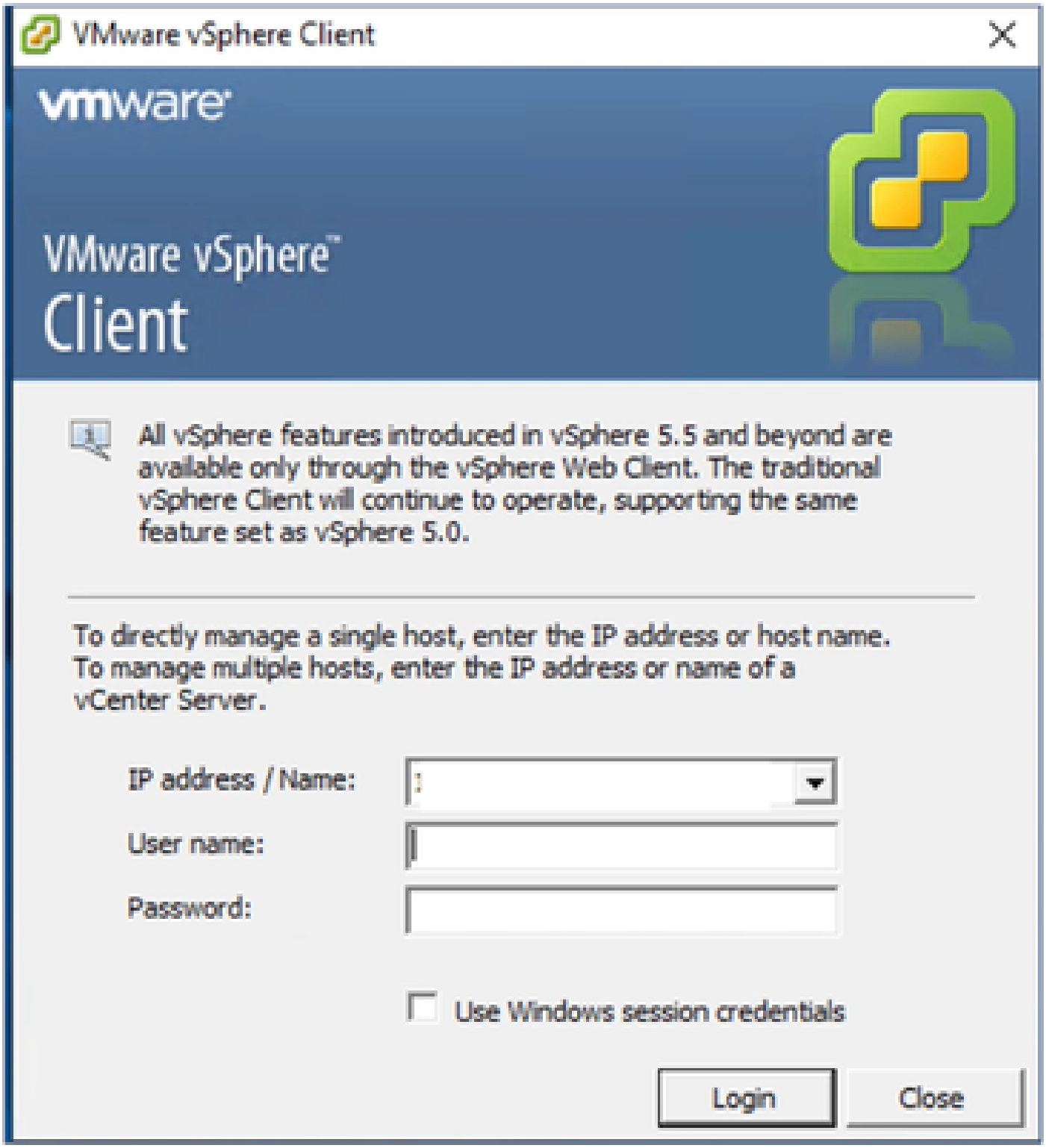
Nach dem Upgrade von VMs ist Folgendes nicht möglich:

- 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.

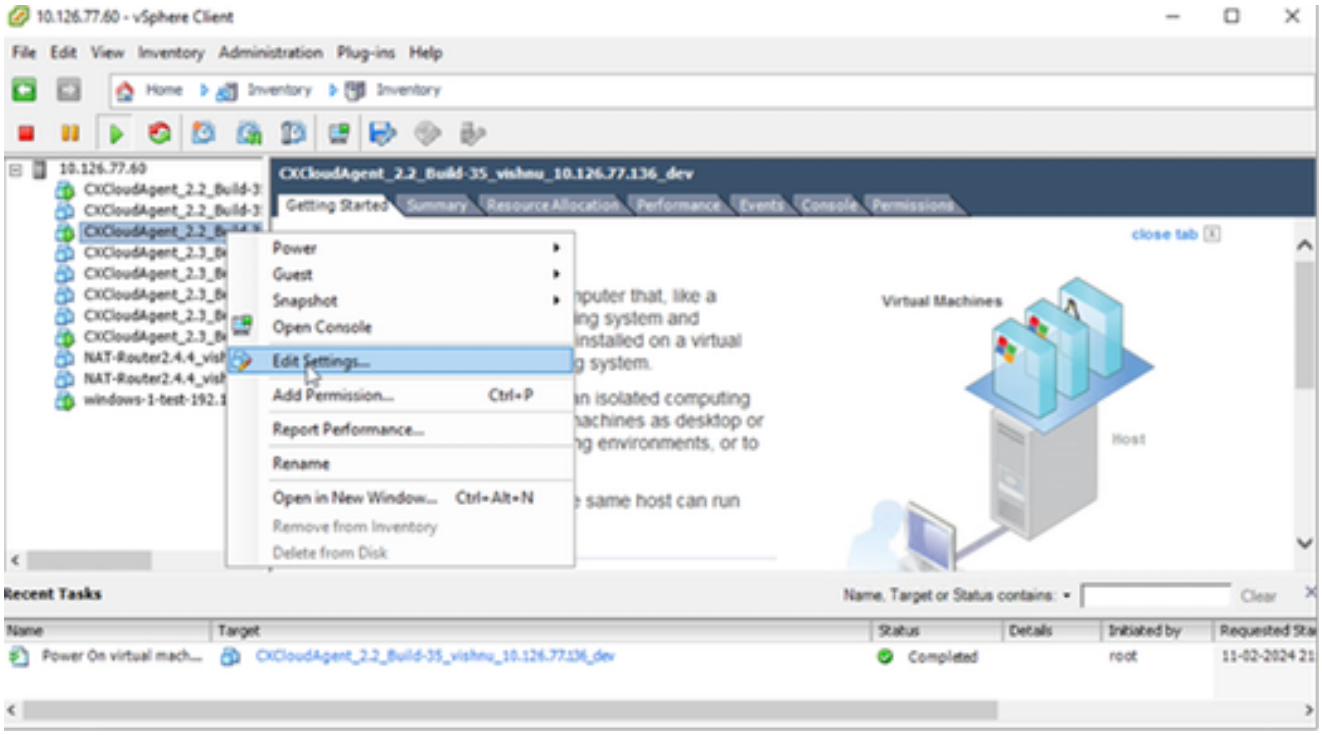
Neukonfiguration mit VMware vSphere Thick Client

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



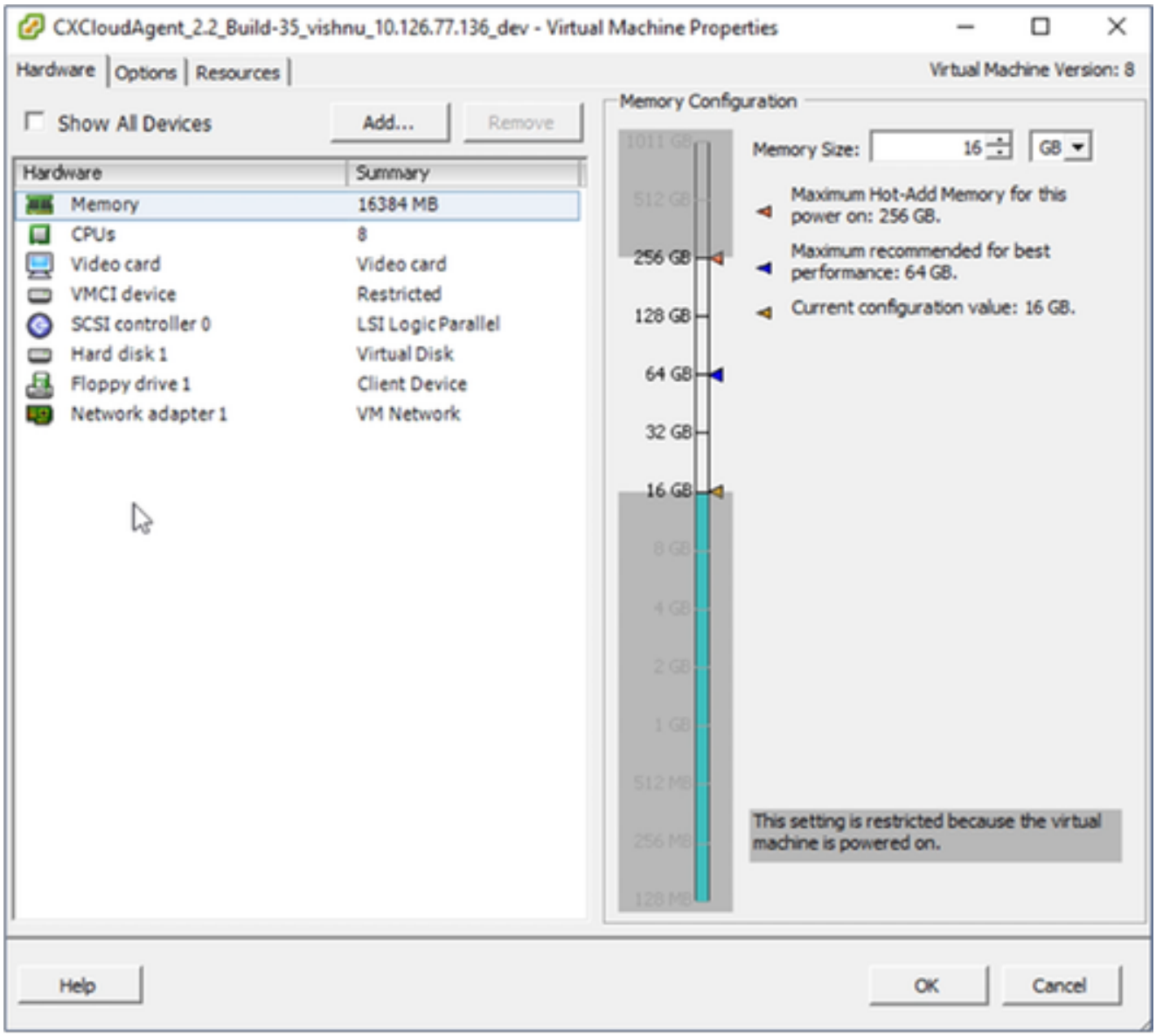
vSphere-Client

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



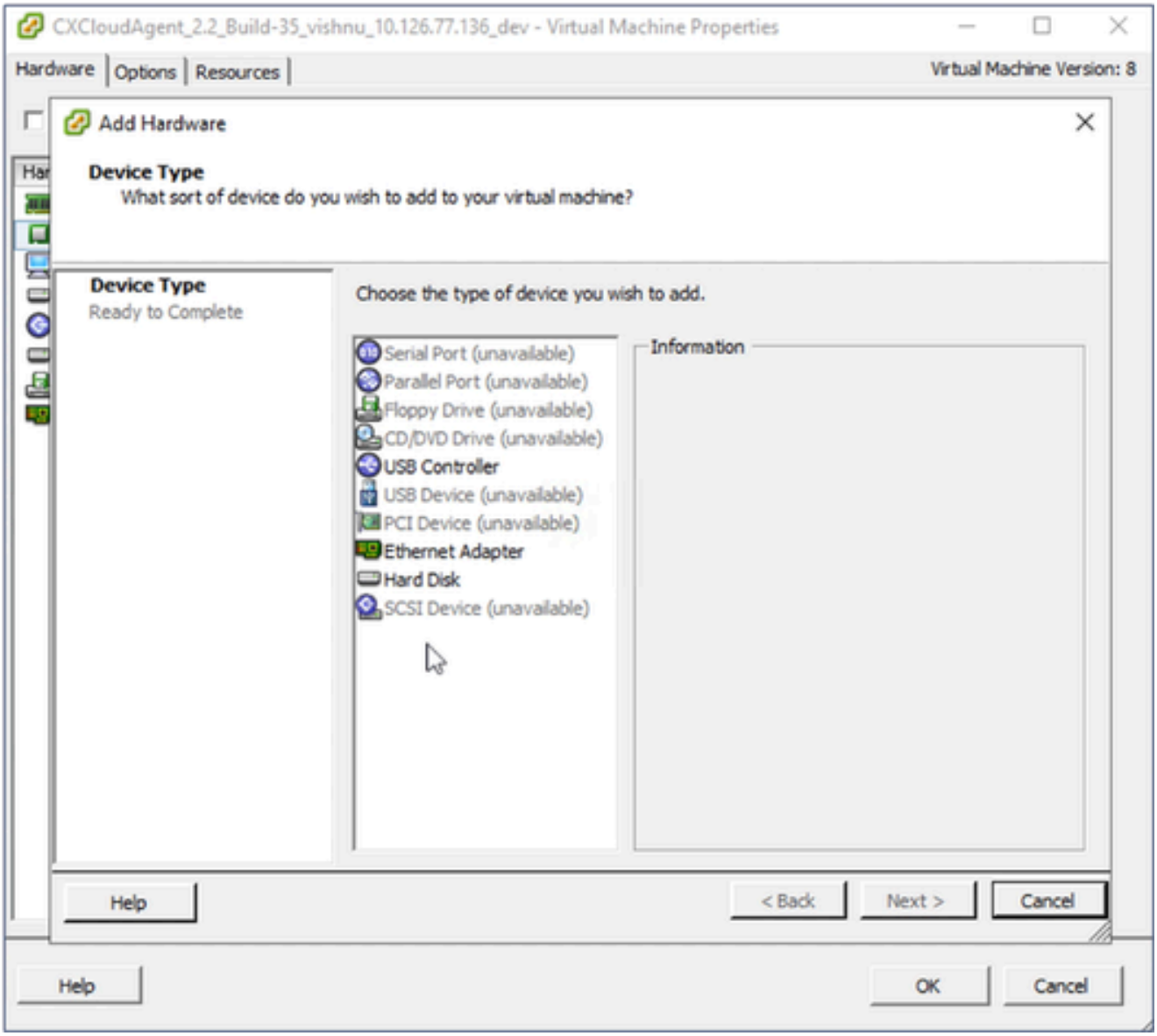
Einstellungen bearbeiten

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.



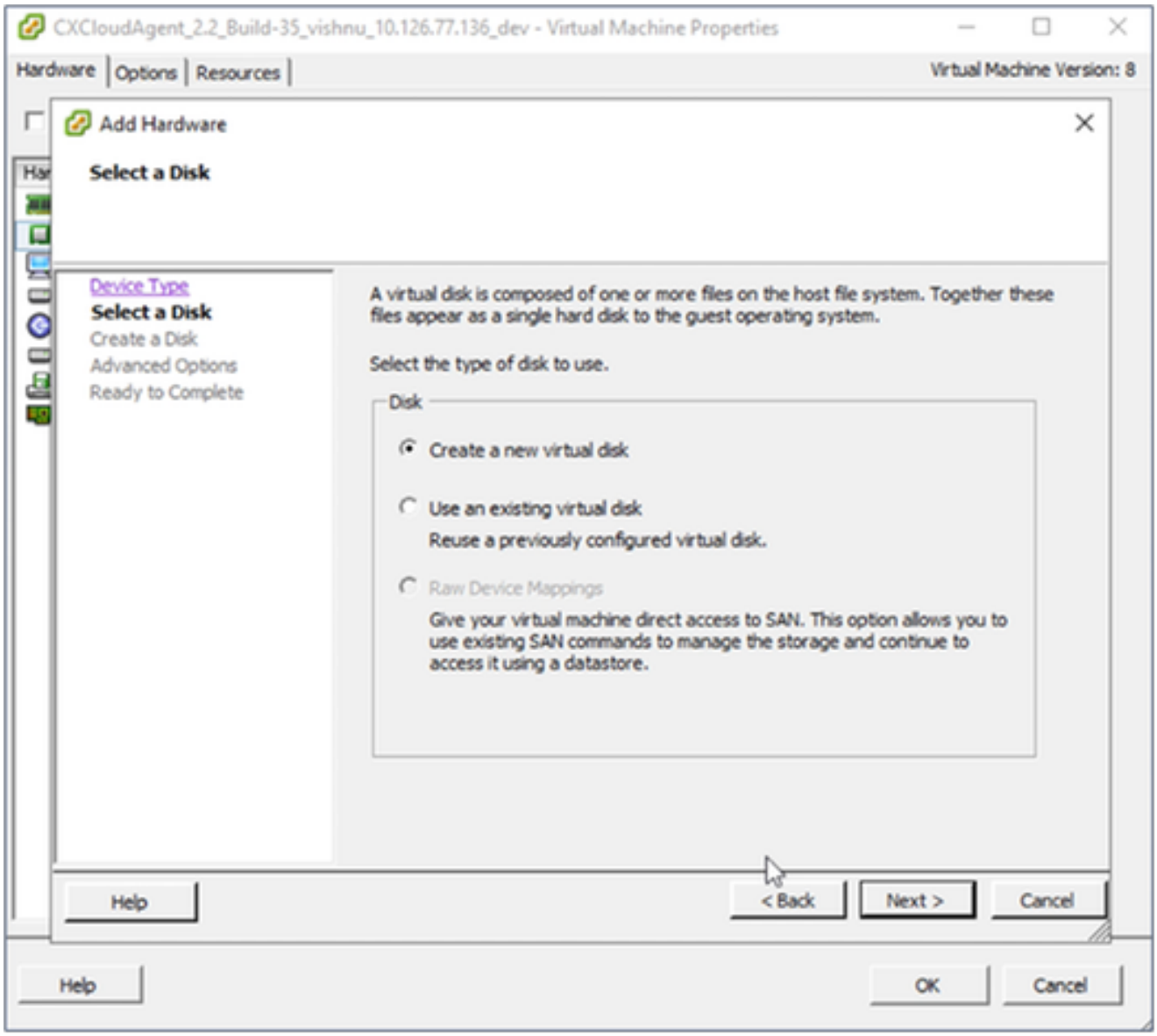
VM-Eigenschaften

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.



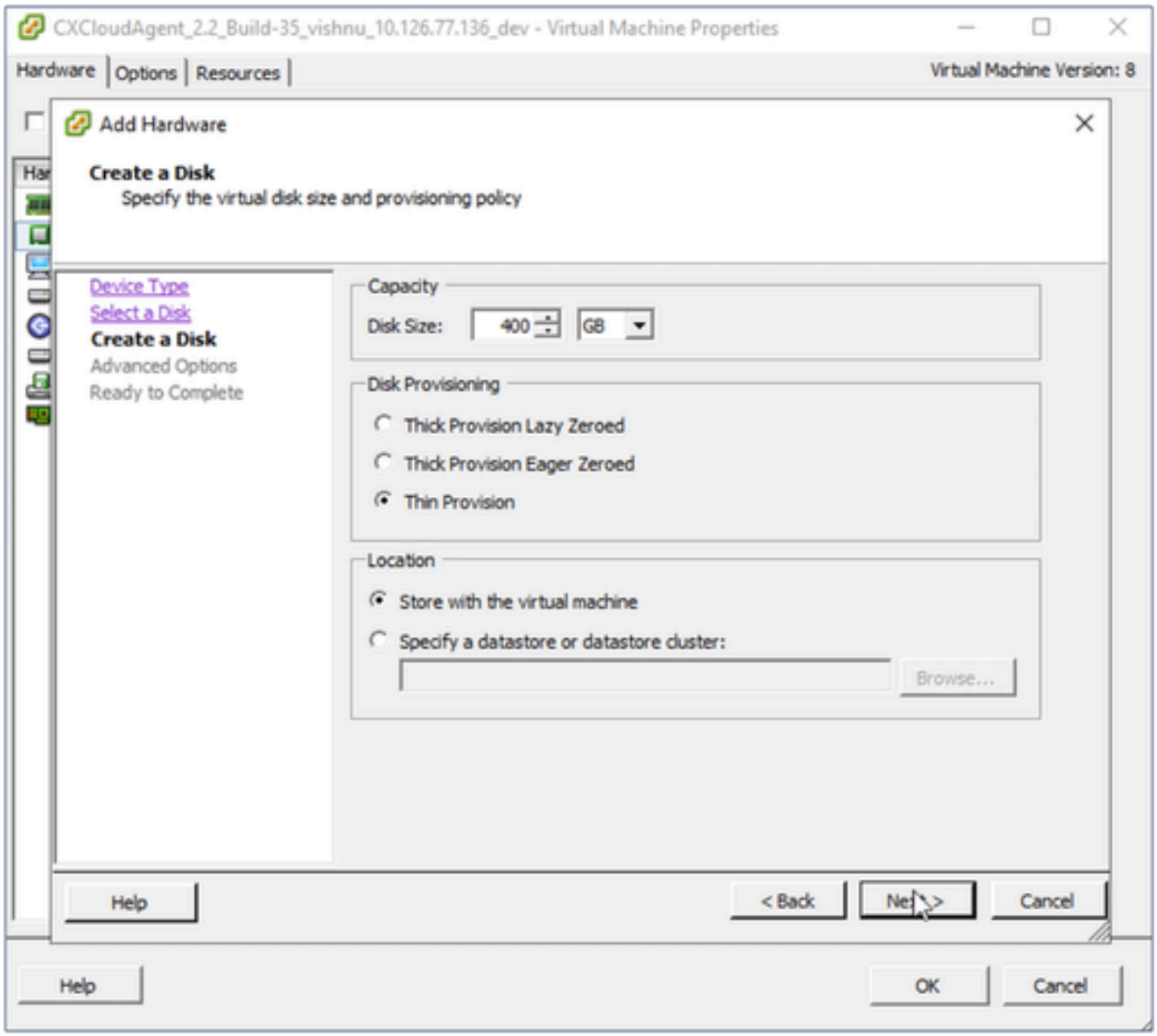
Gerätetyp

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



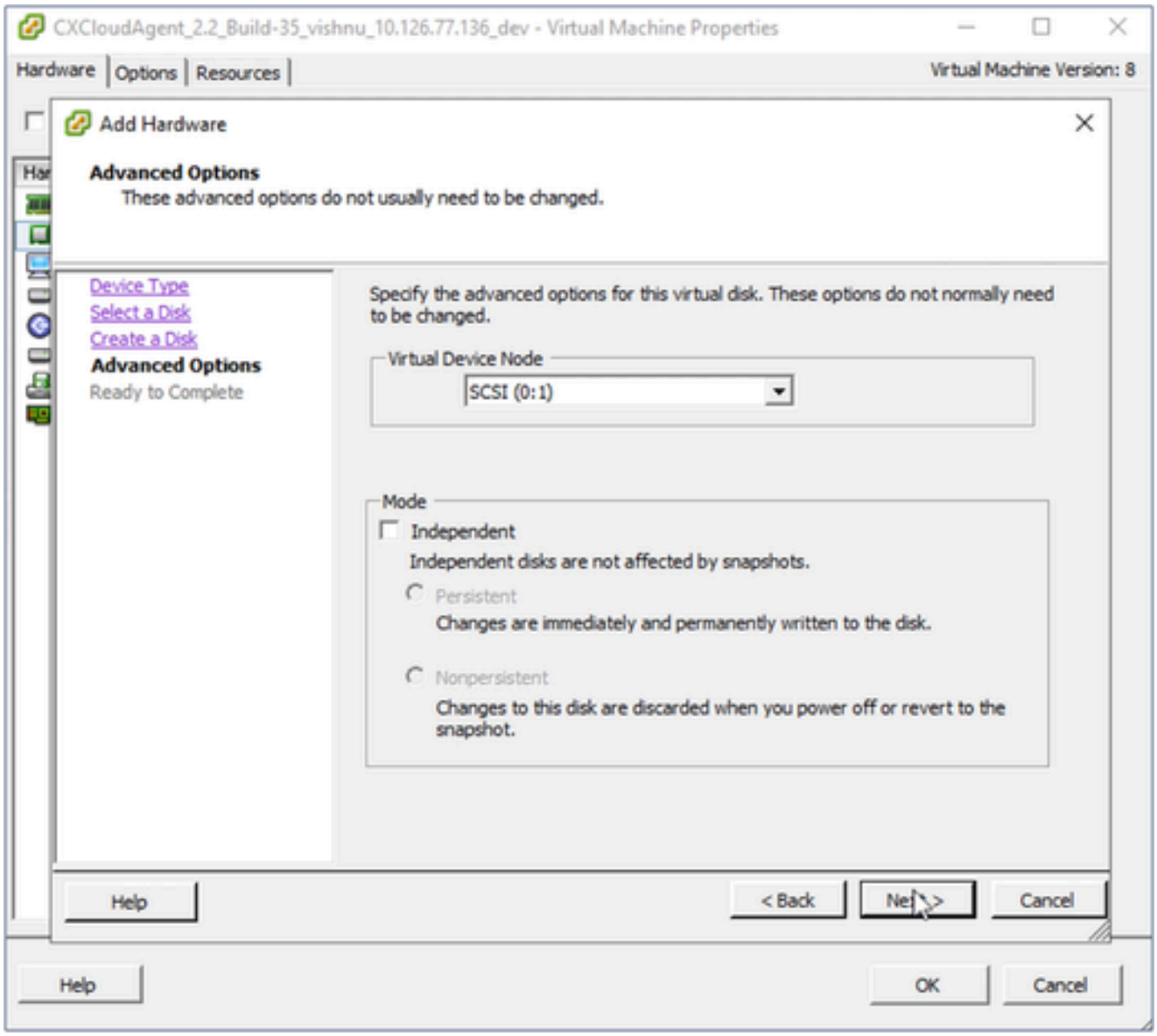
Festplatte auswählen

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



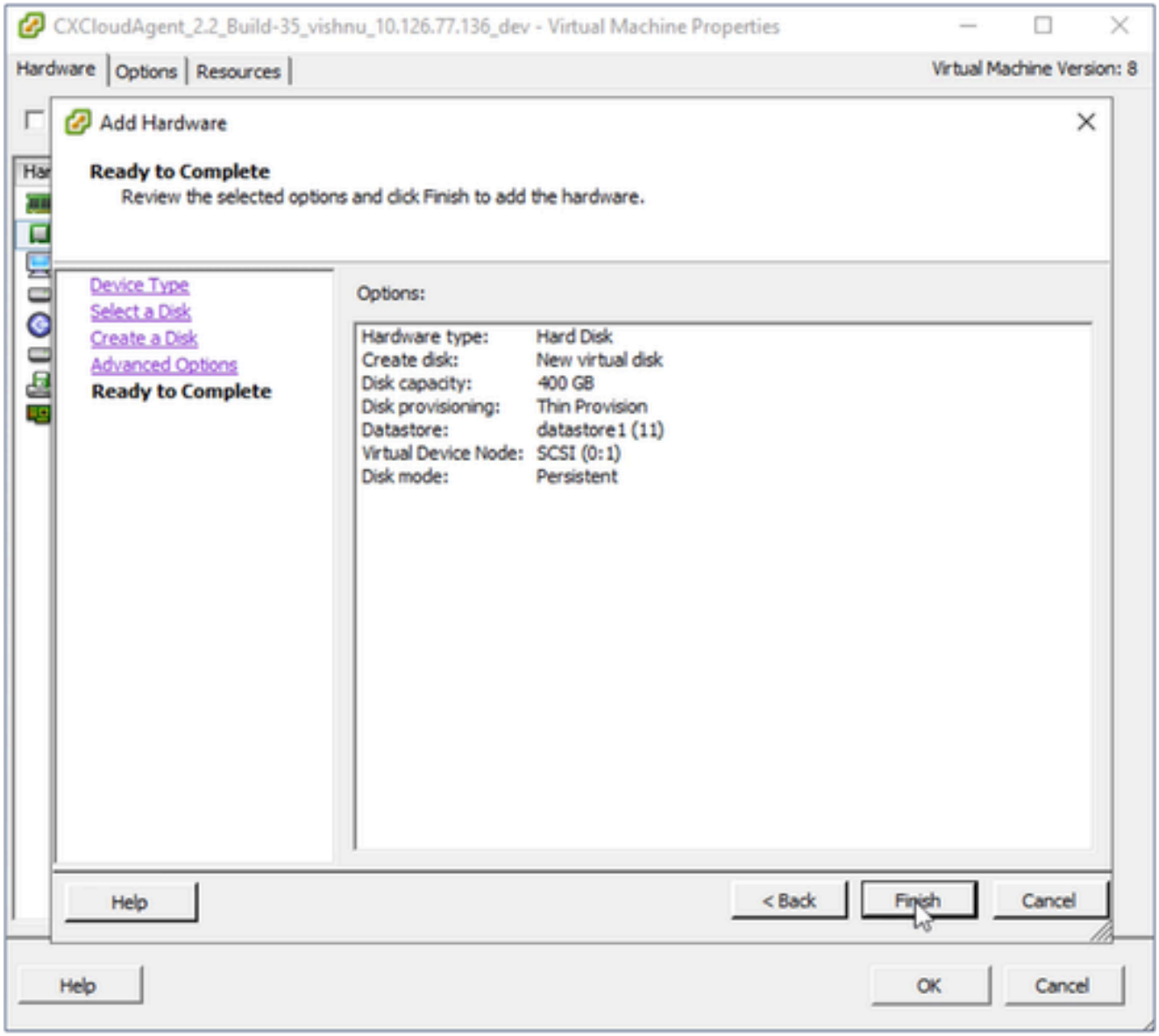
Datenträger erstellen

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.



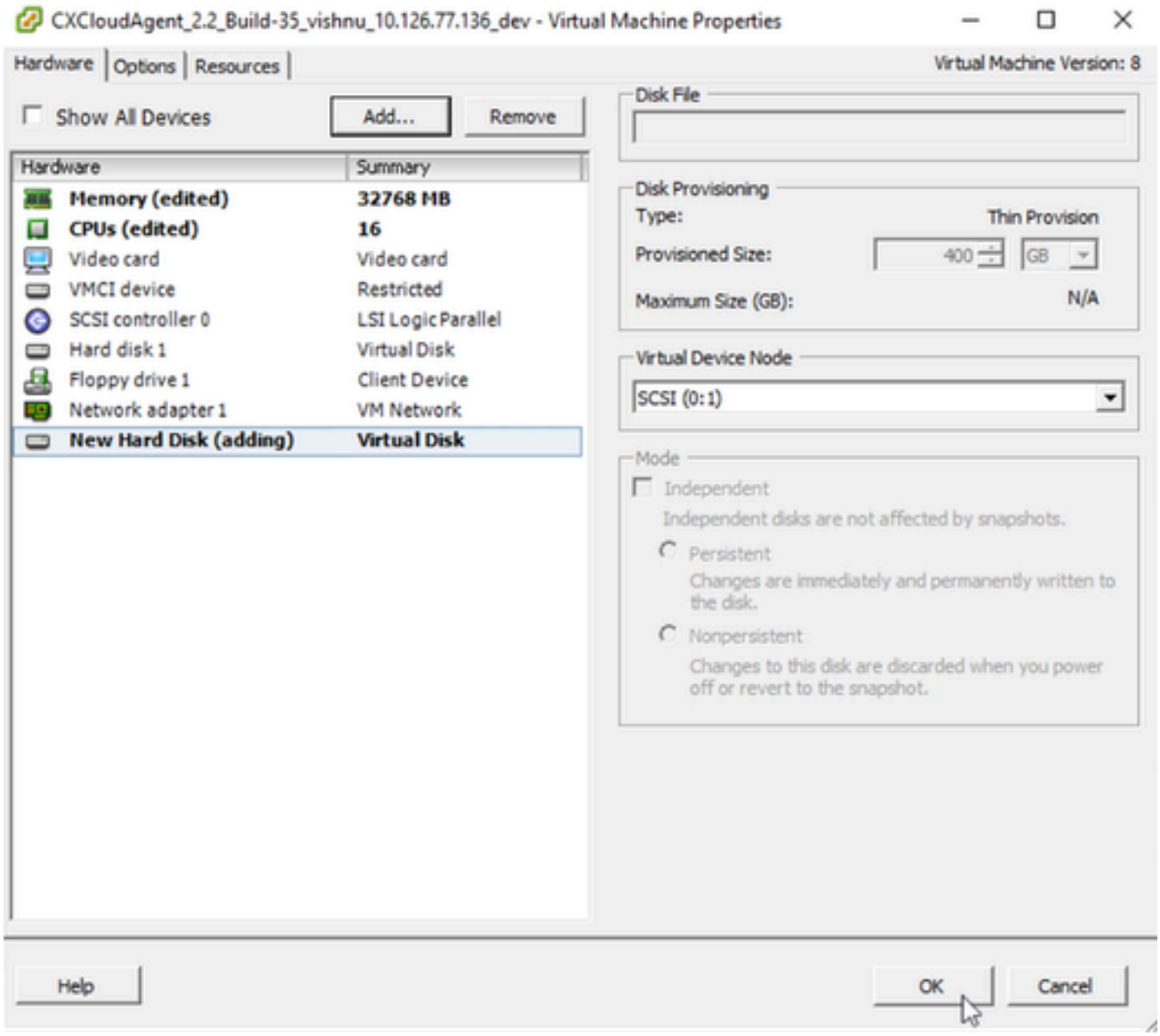
Erweiterte Optionen

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



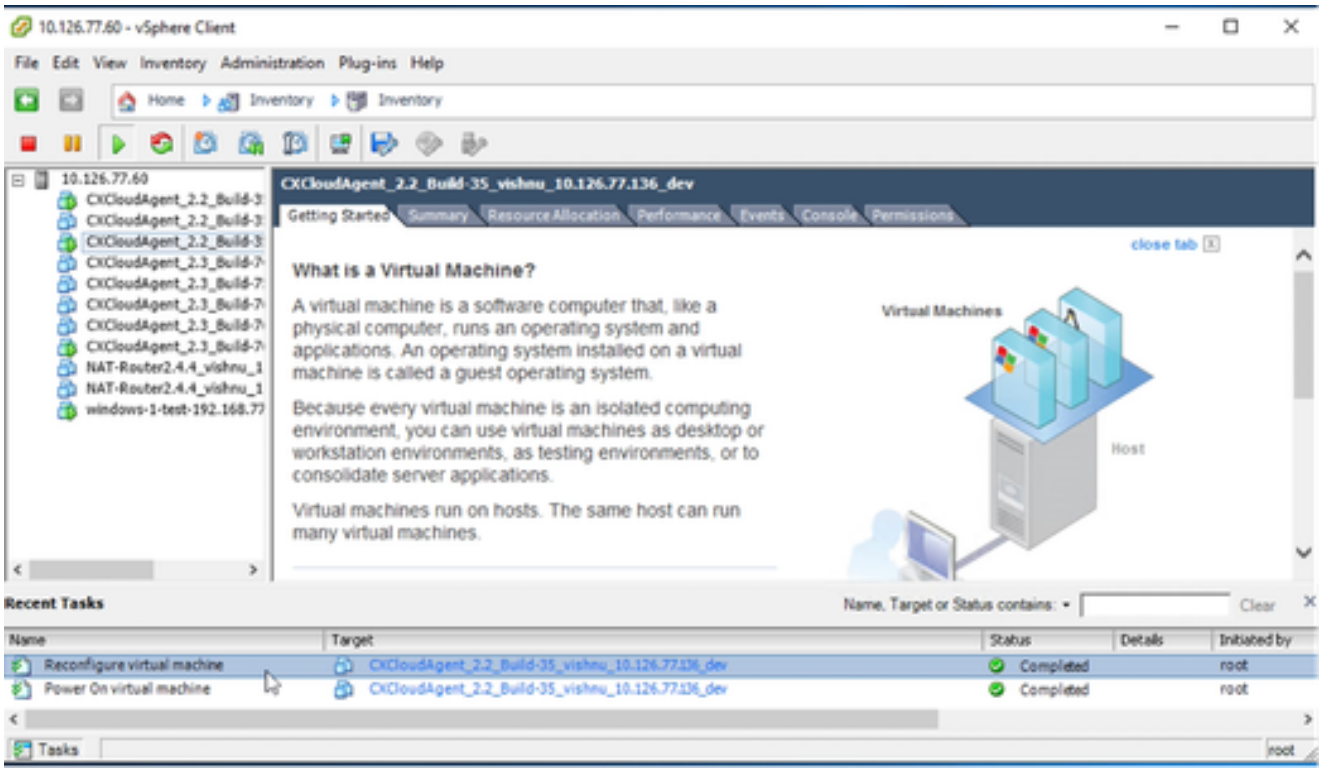
Bereit zur Fertigstellung

13. Klicken Sie auf Beenden.

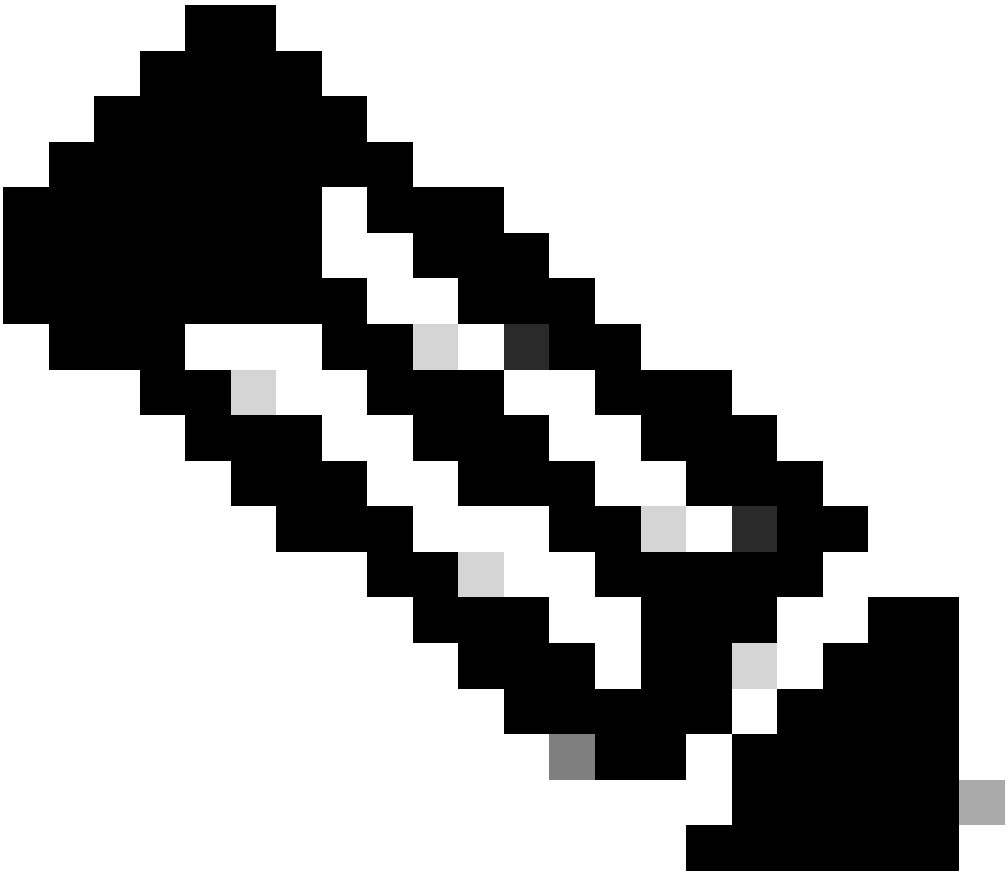


Hardware

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



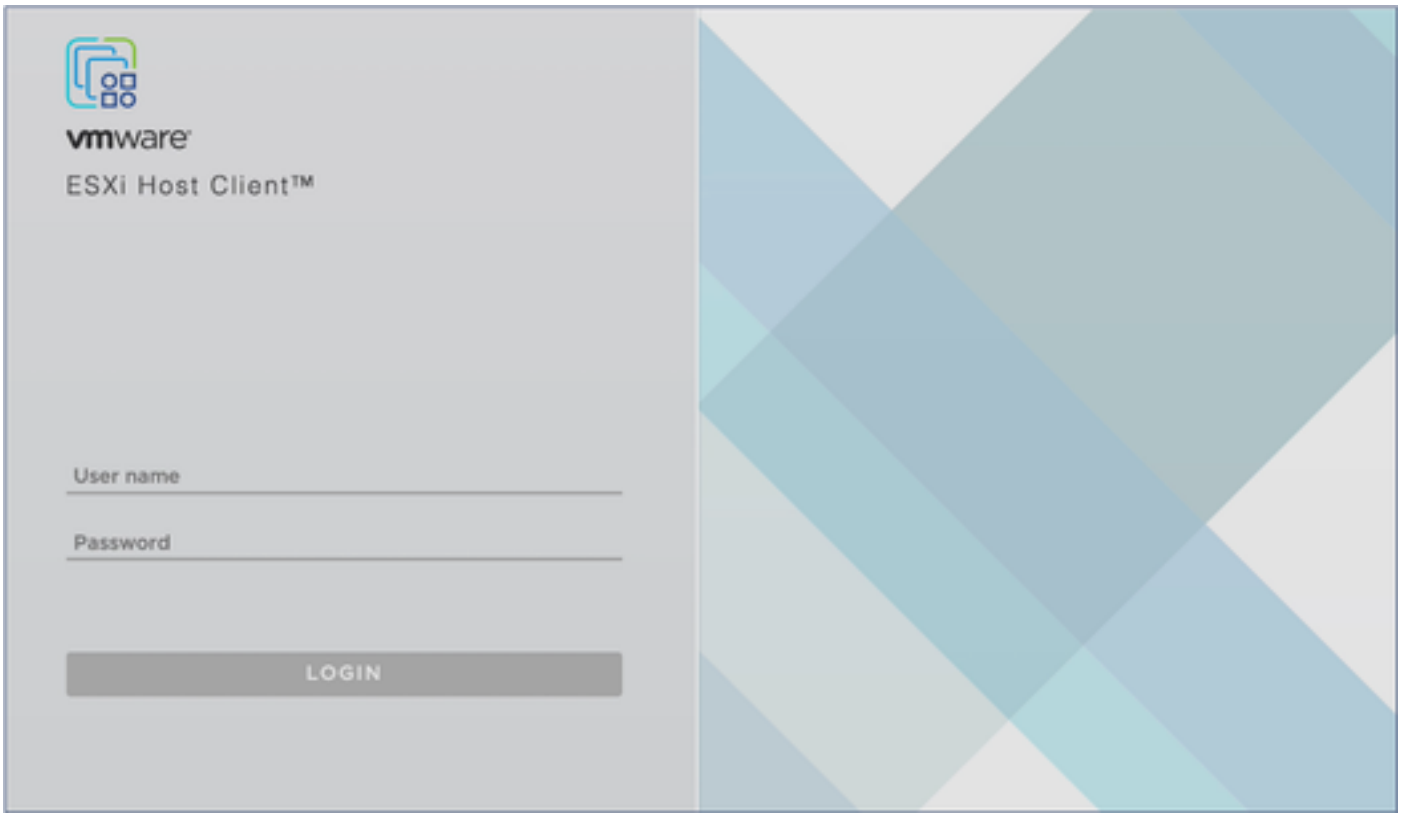
Zuletzt durchgeführte Aufgaben



Anmerkung: Konfigurationsänderungen können nur etwa fünf Minuten in Anspruch nehmen.

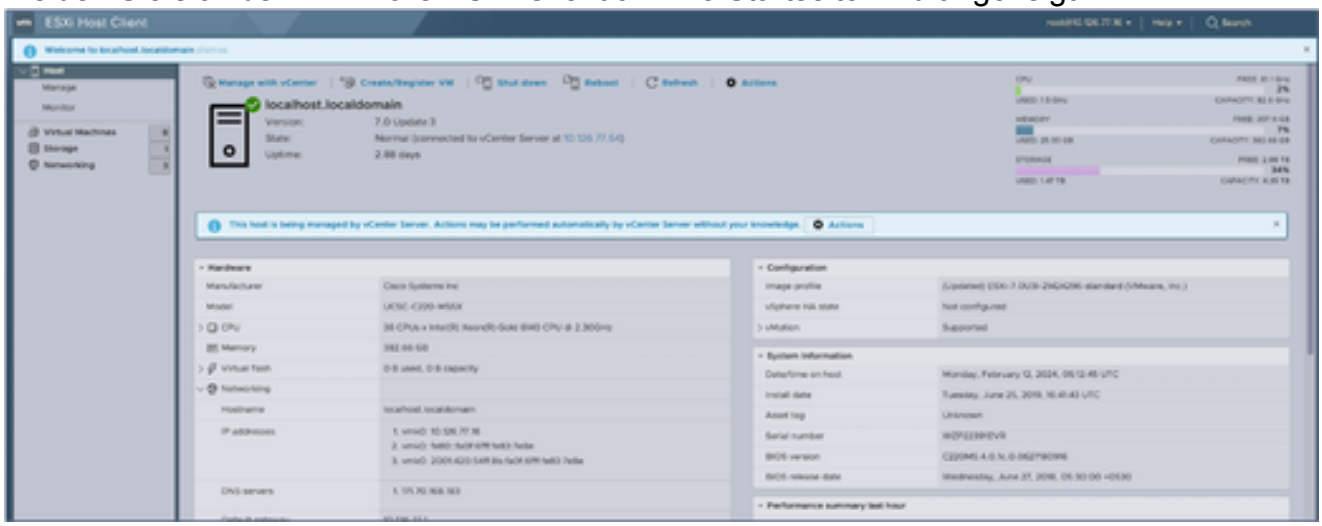
Neukonfiguration mit Web-Client ESXi v6.0

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



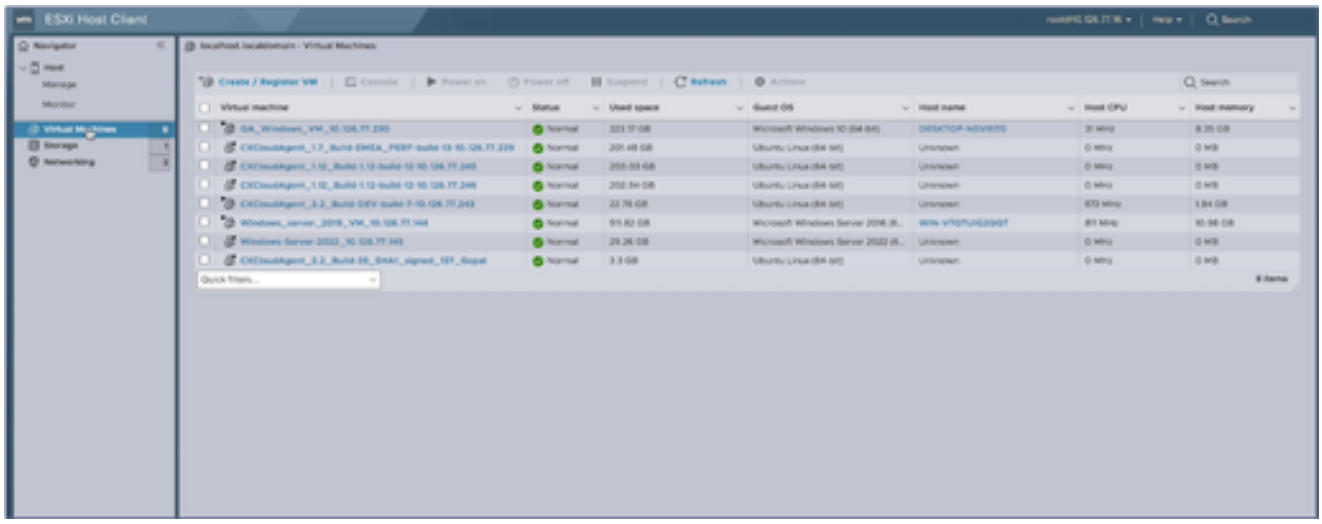
ESXi-Client

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



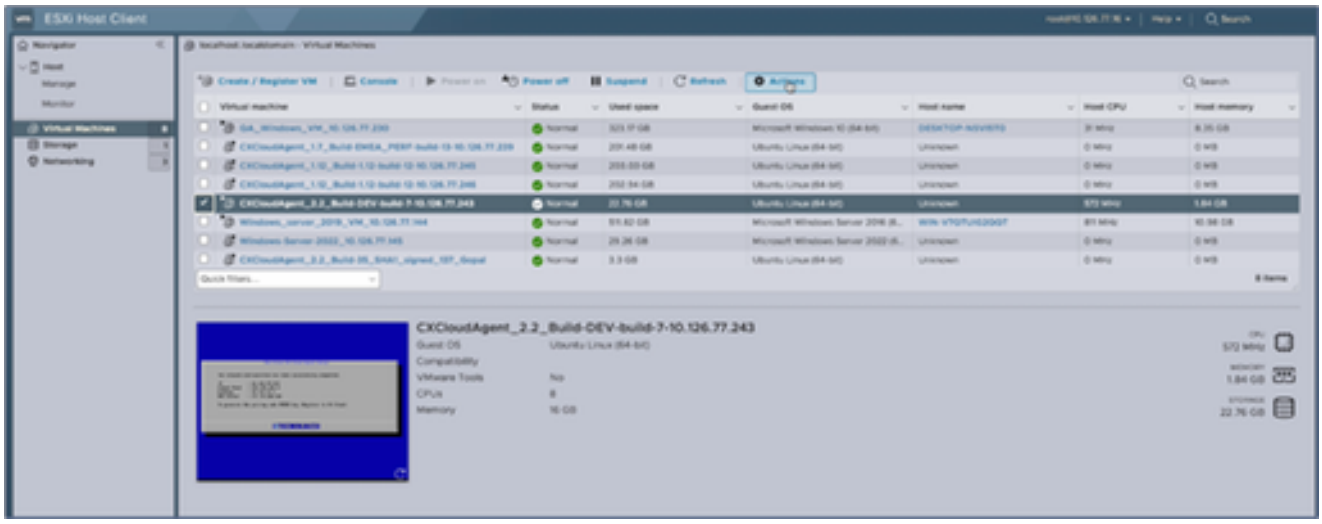
ESXi-Startseite

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



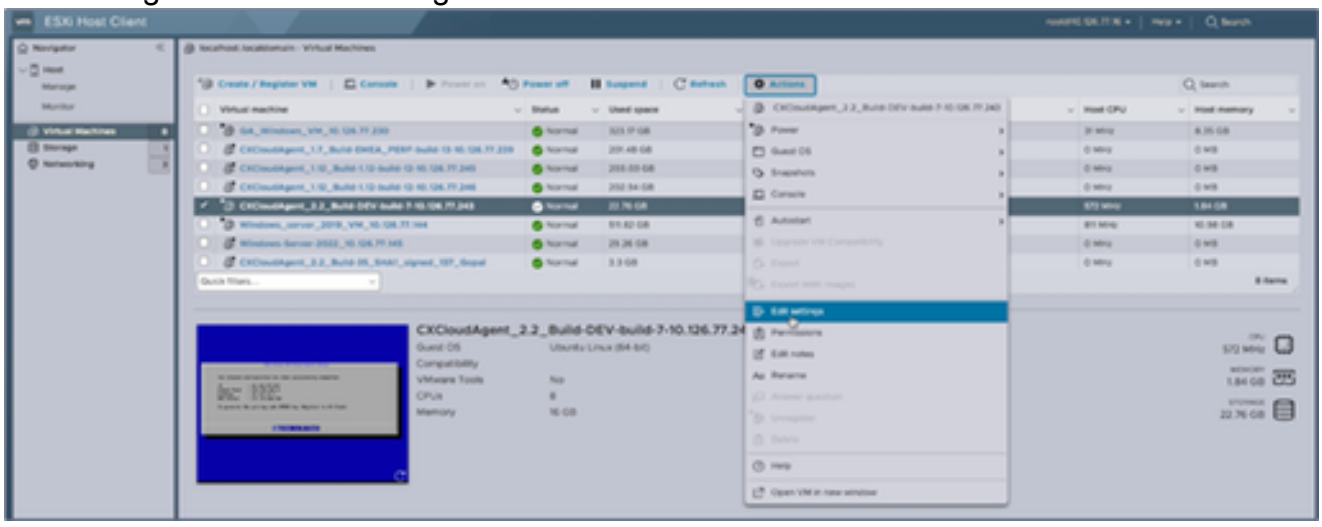
Liste der VMs

3. Wählen Sie die Ziel-VM aus.

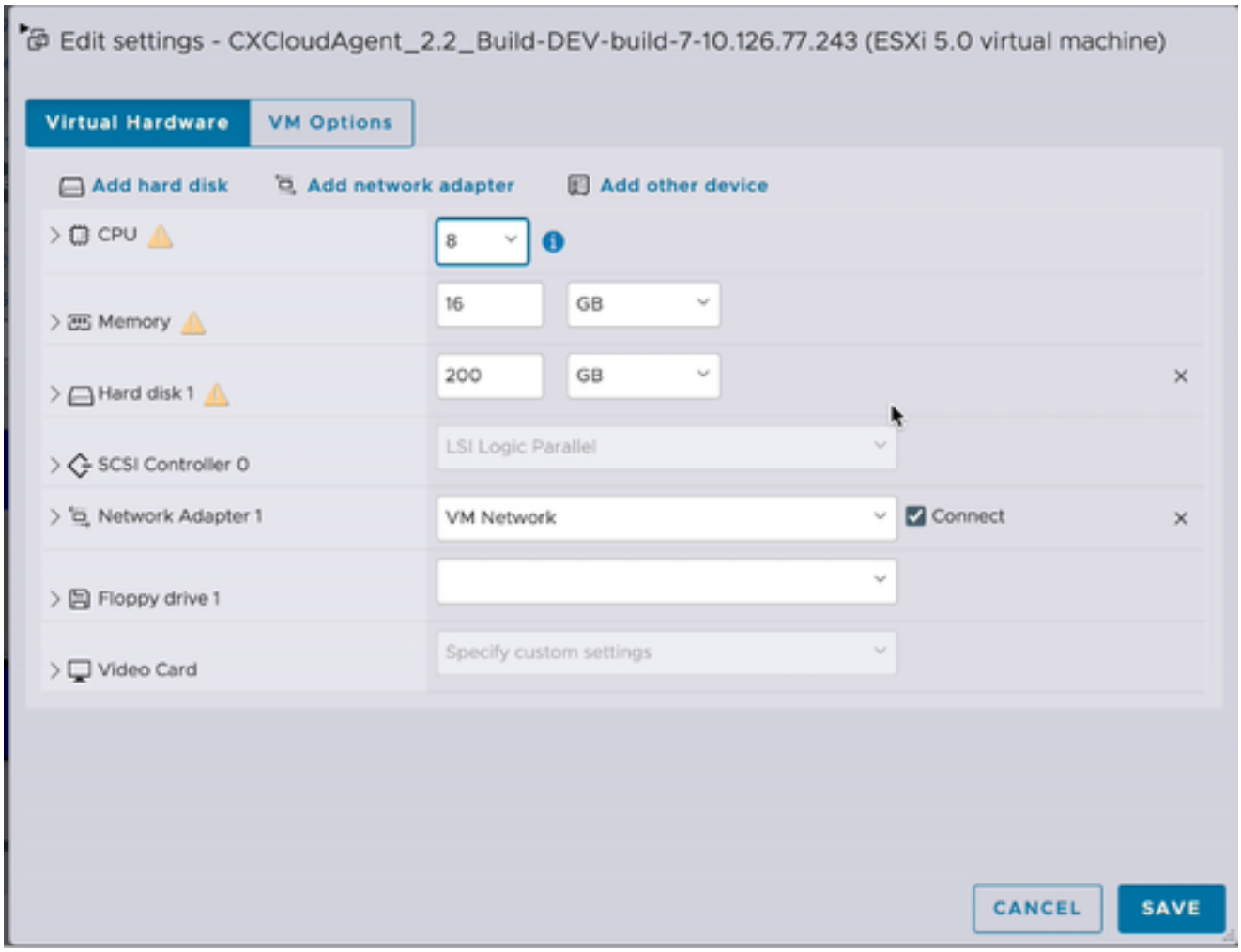


Ziel-VM

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

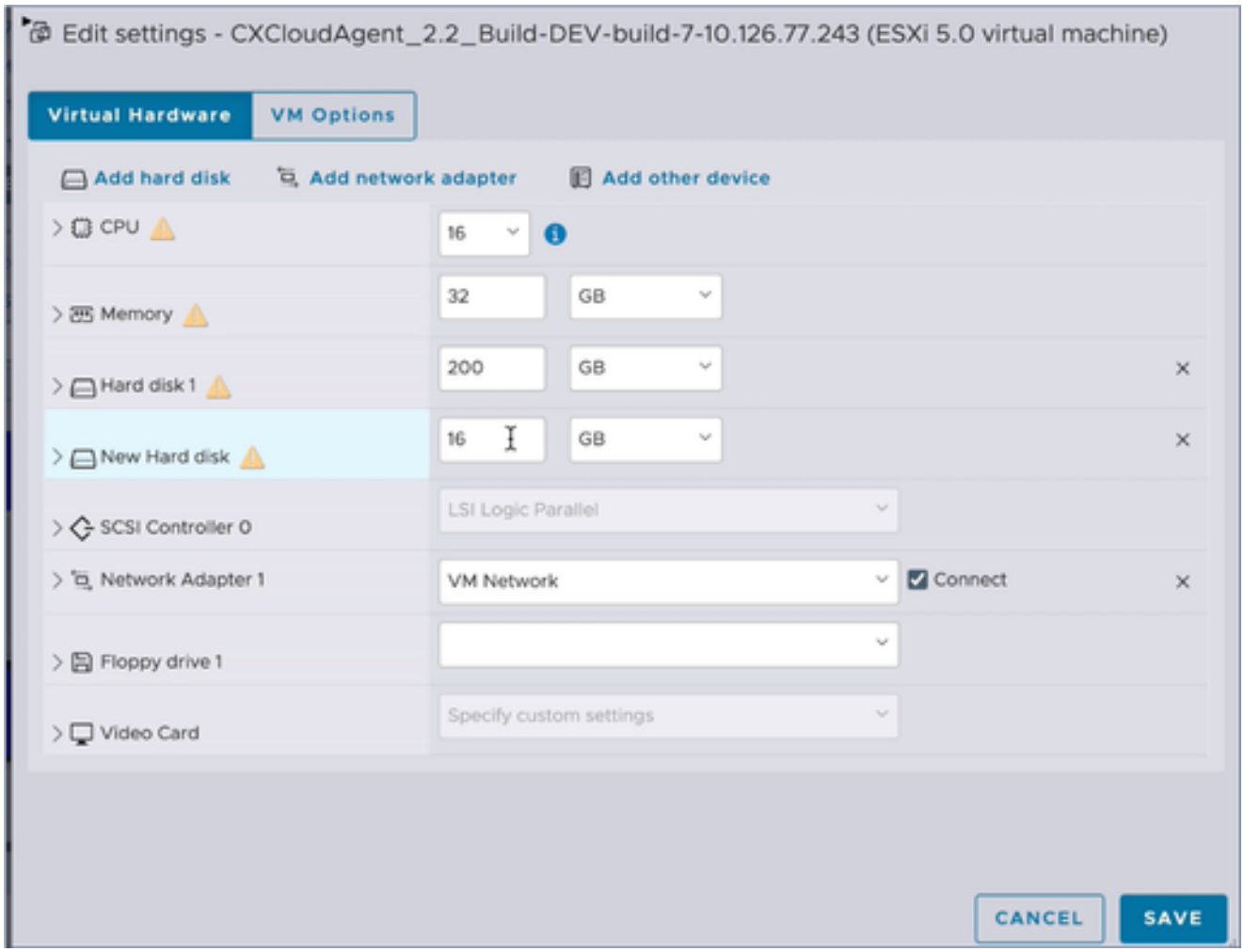


Aktionen



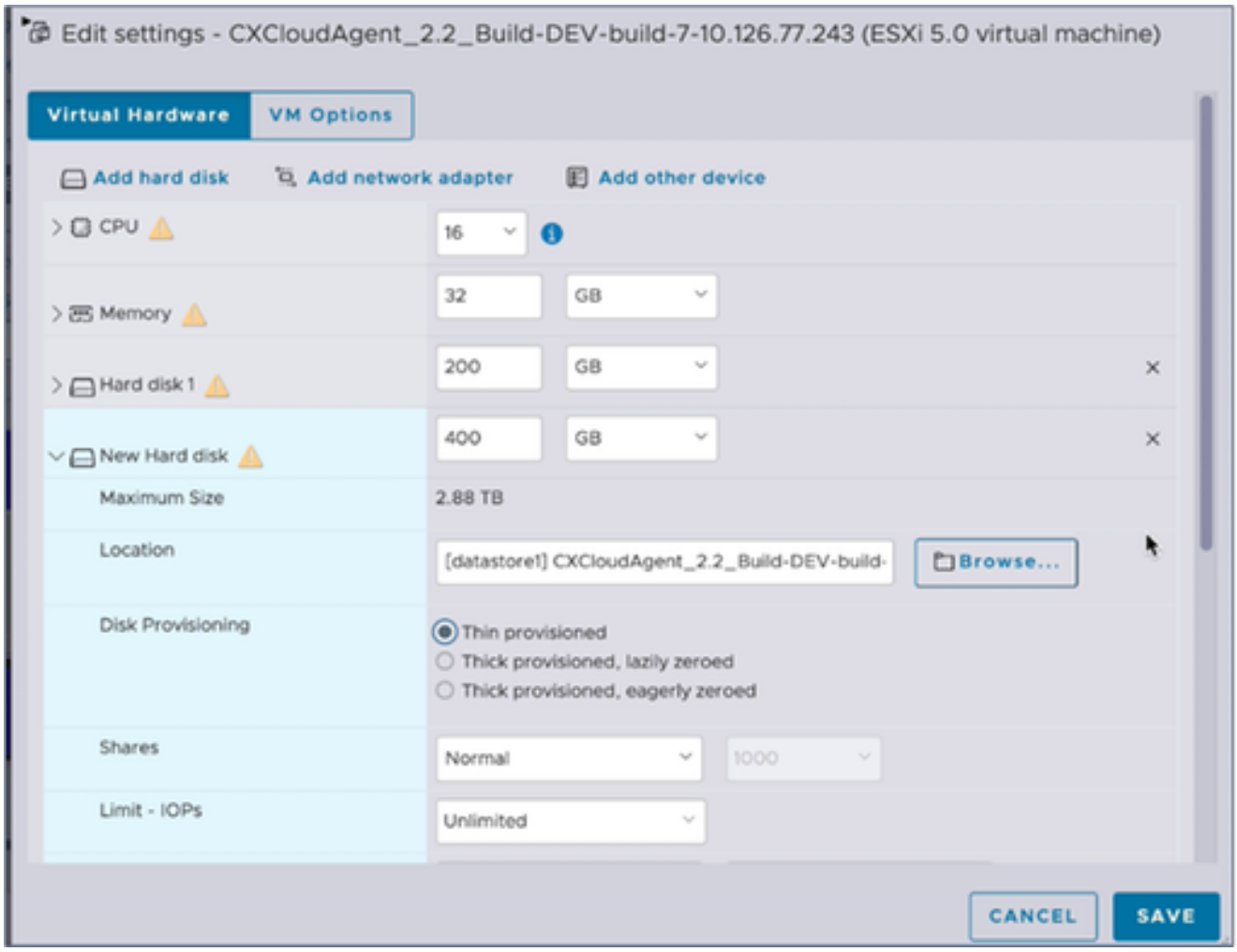
Einstellungen bearbeiten

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.



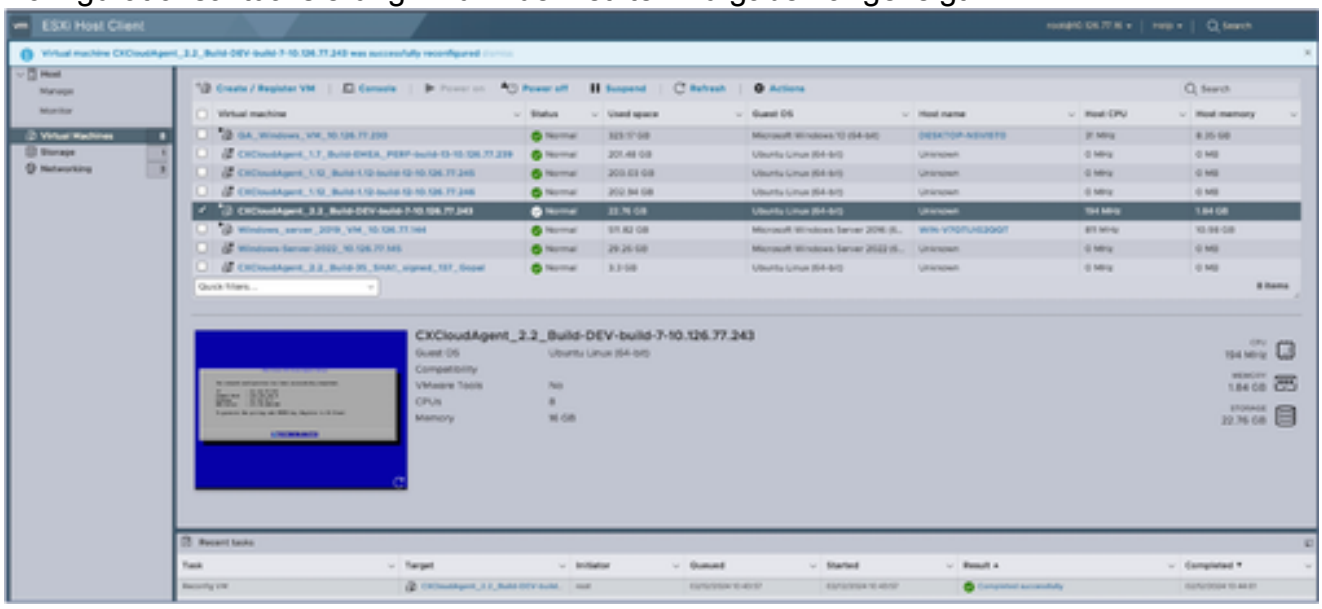
Einstellungen bearbeiten

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.



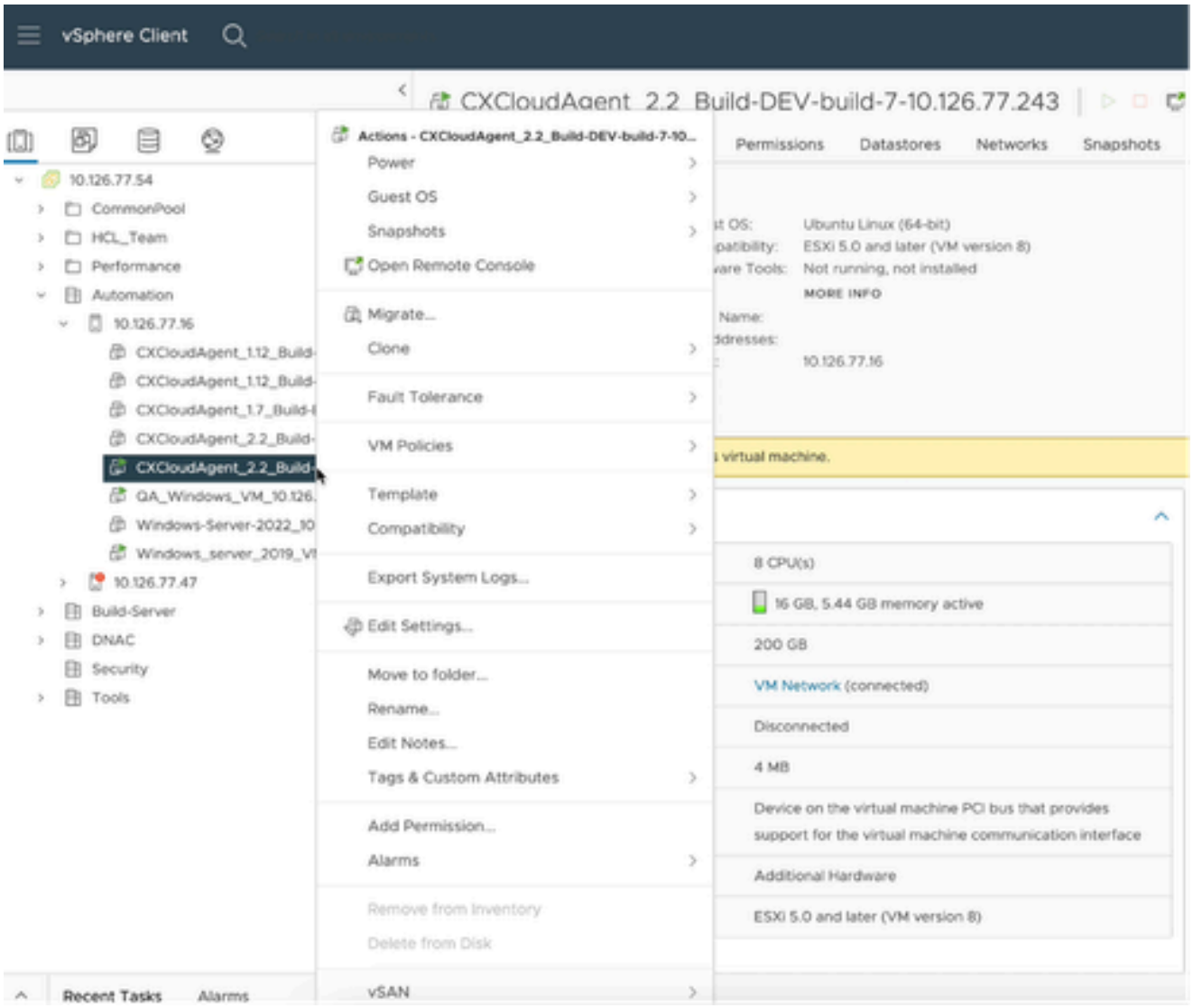
Zuletzt durchgeführte Aufgaben

Neukonfiguration mit Web Client vCenter

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

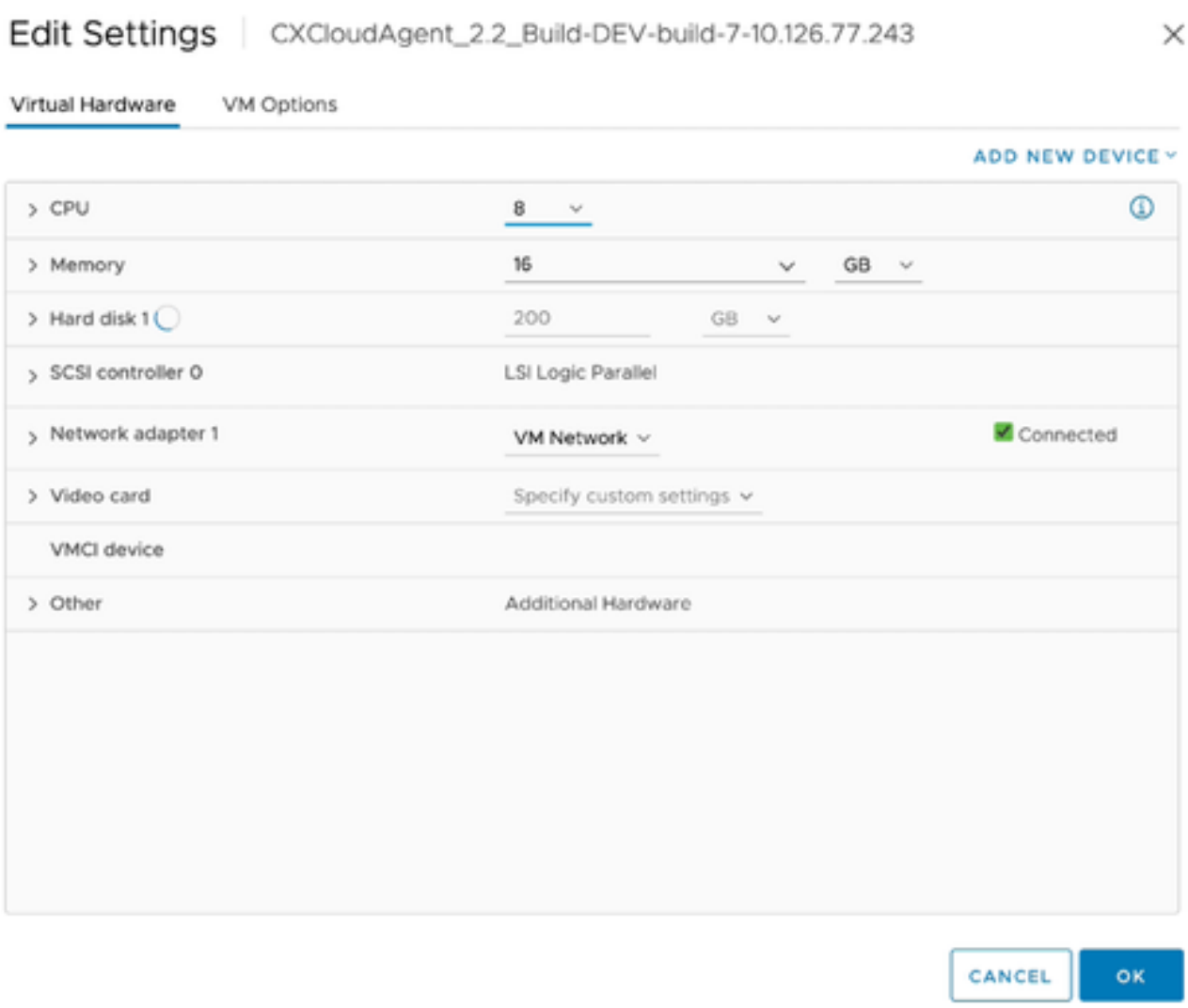
vCenter

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



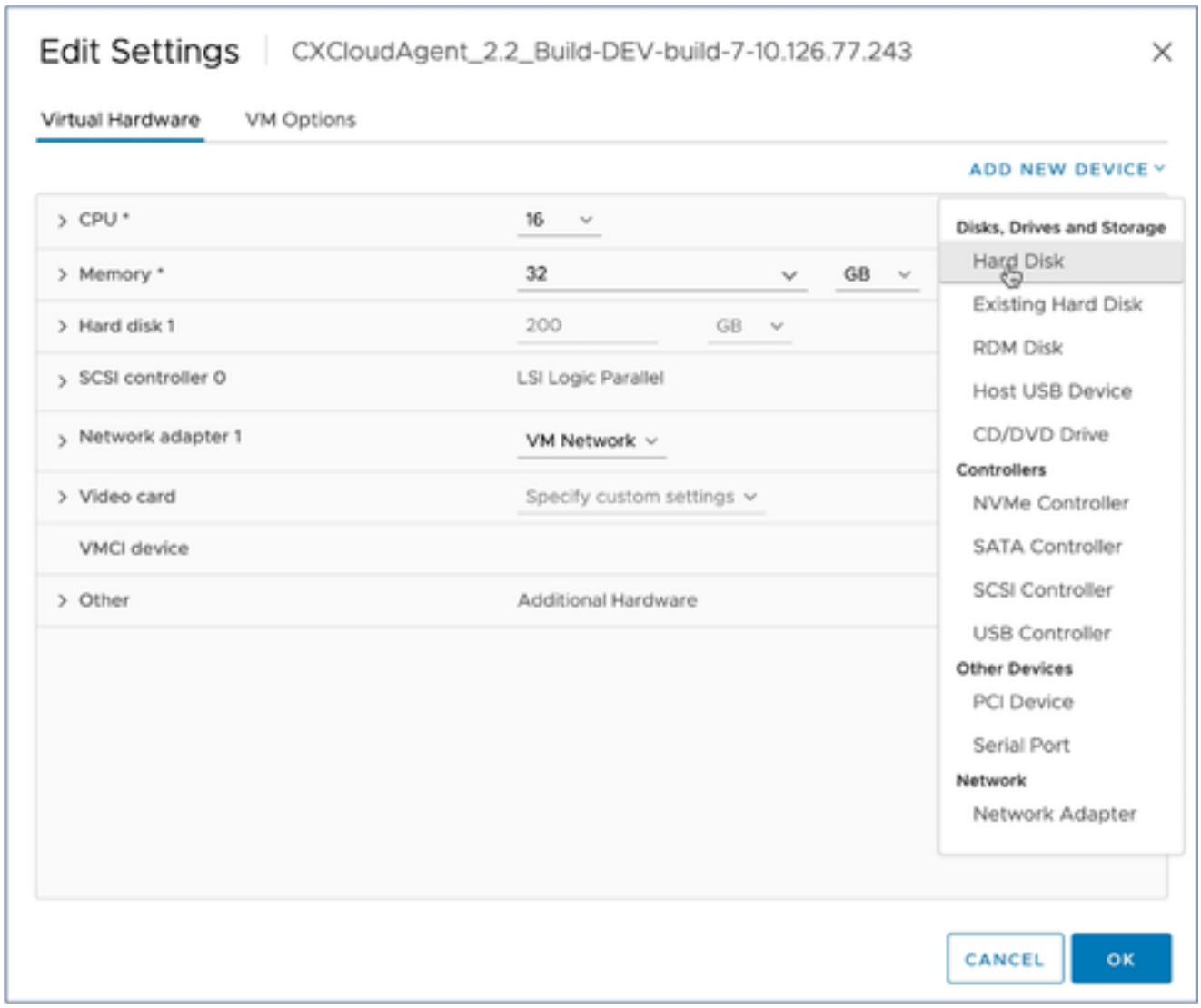
Liste der VMs

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.



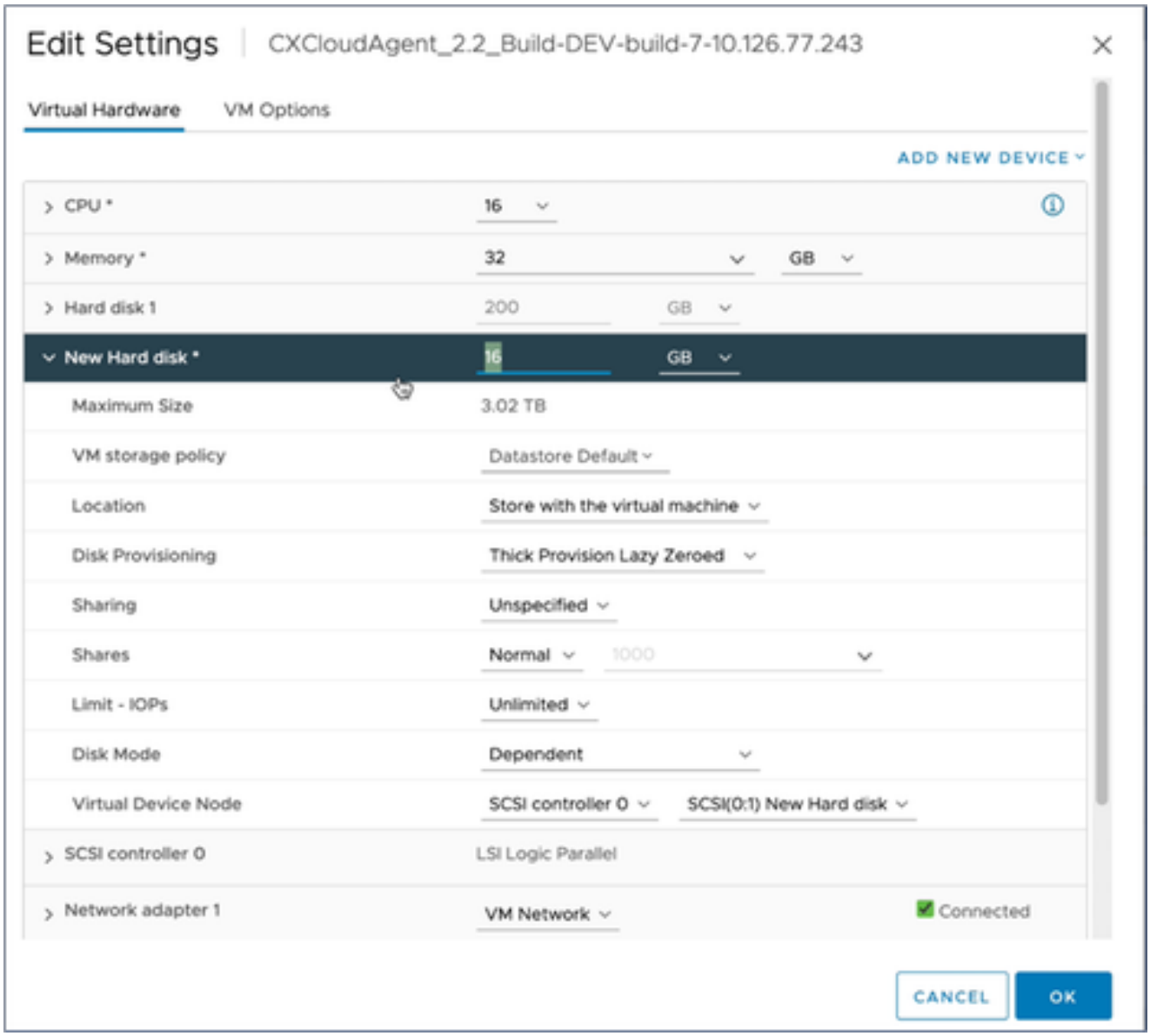
Einstellungen bearbeiten

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



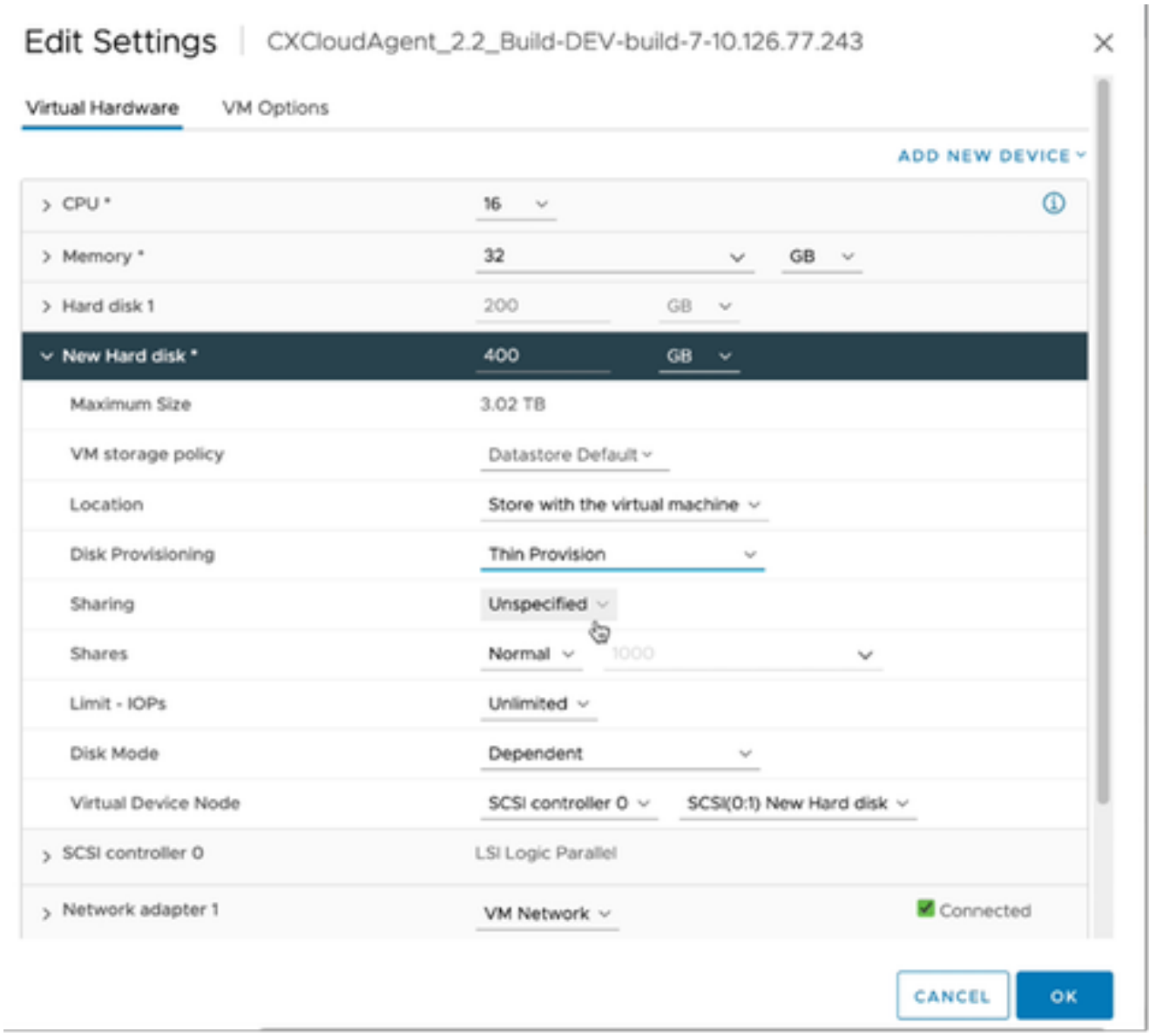
Einstellungen bearbeiten

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-Agenten bereitzustellen:

- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0
- Installation von VMware vSphere/vCenter Web Client ESXi 6.0 oder Web Client vCenter
- Oracle VirtualBox 7.0.12
- Installation von Microsoft Hyper-V

OVA-Bereitstellung

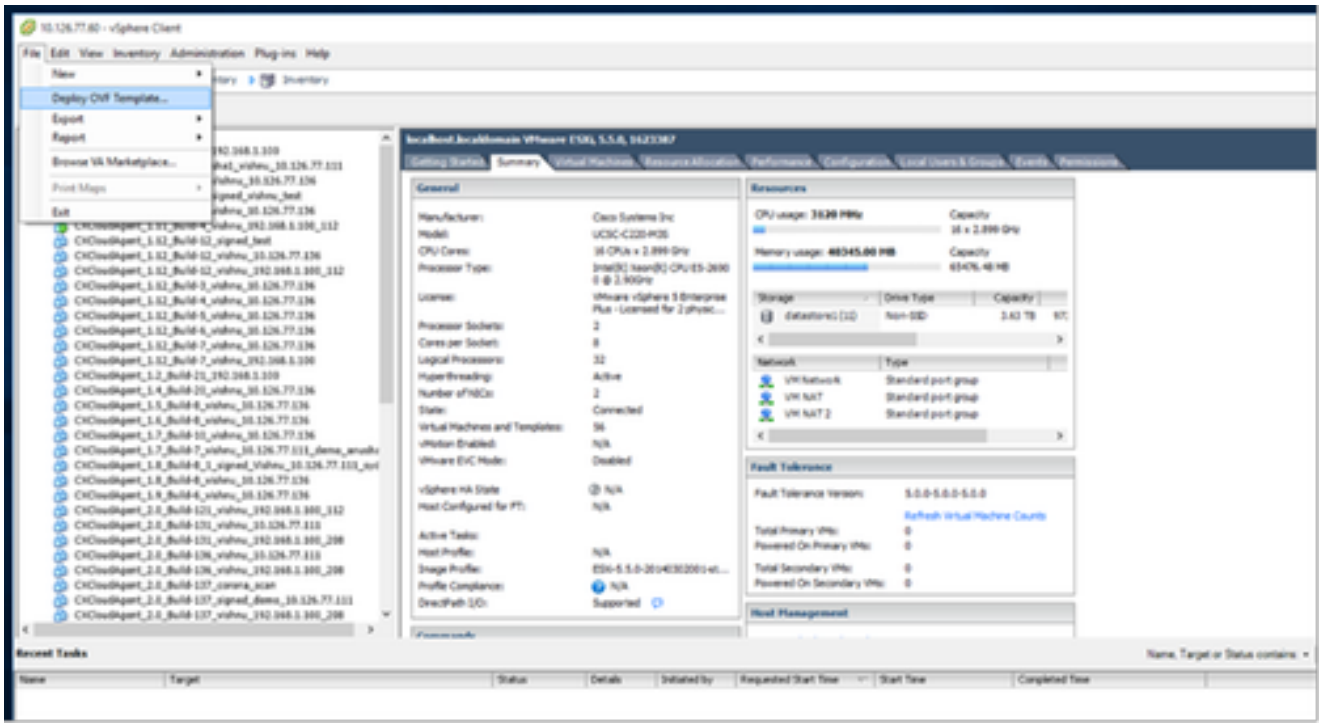
Installation von Thick Client ESXi 5.5/6.0

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

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

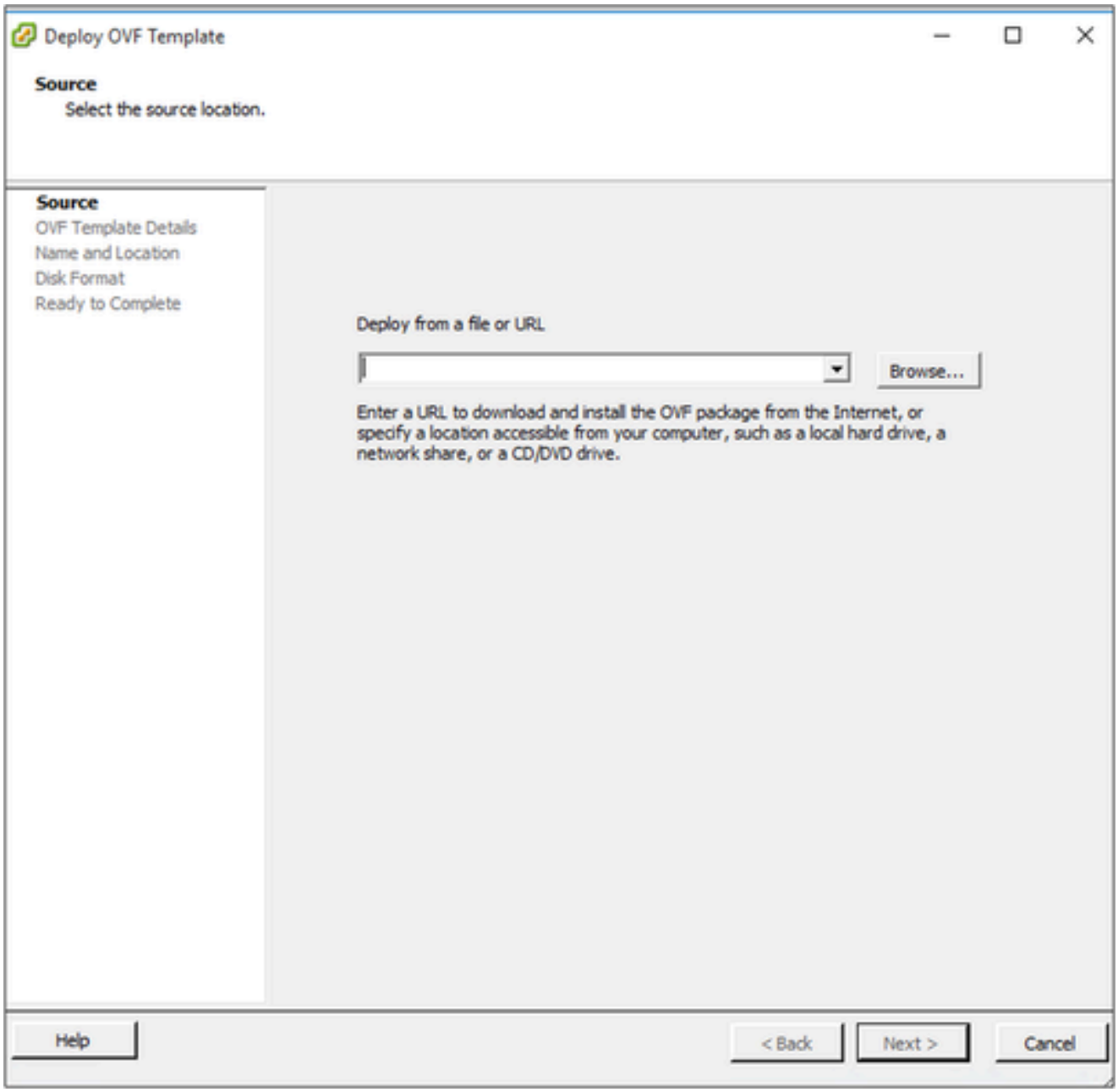
Anmelden

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



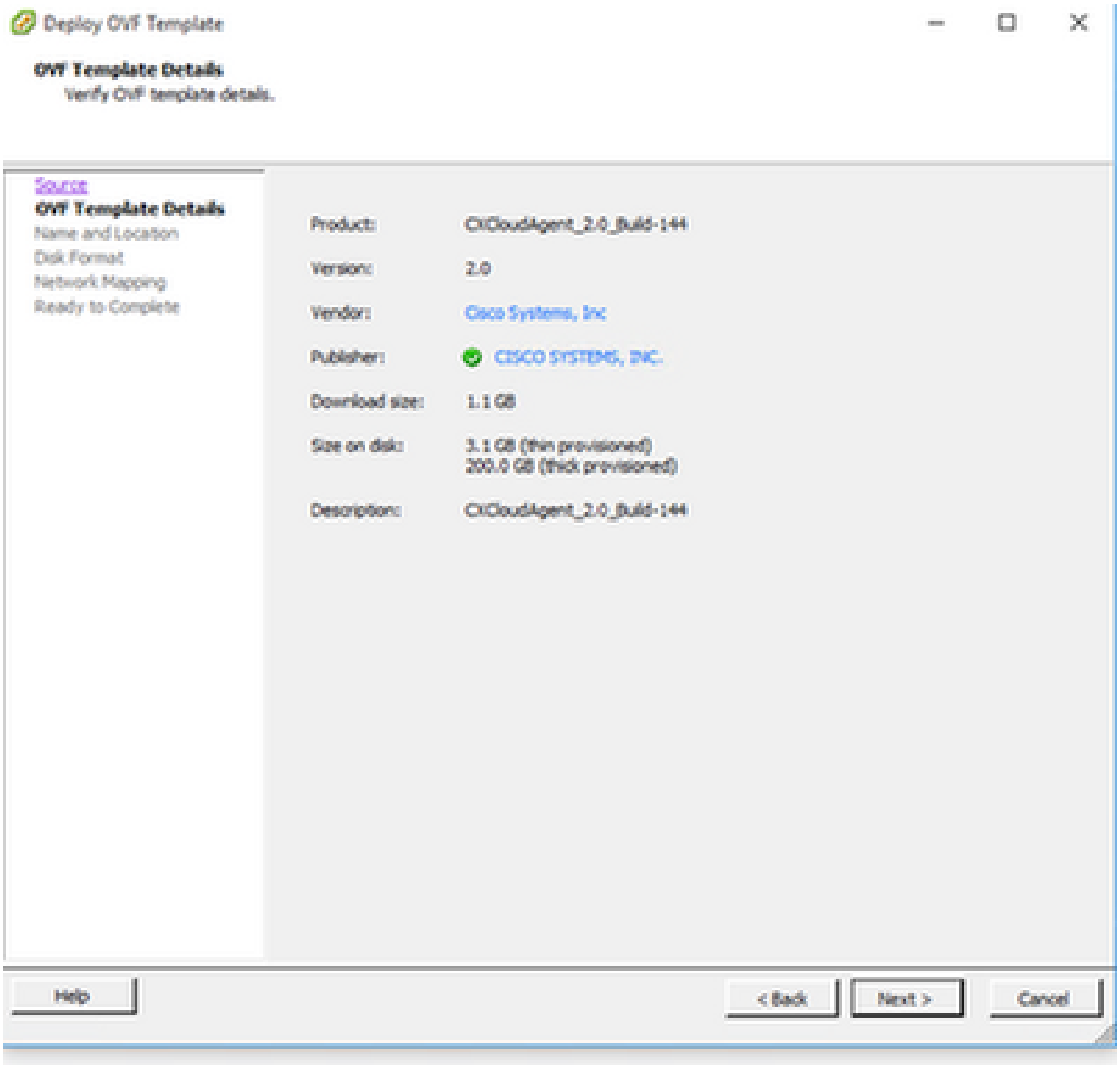
vSphere-Client

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



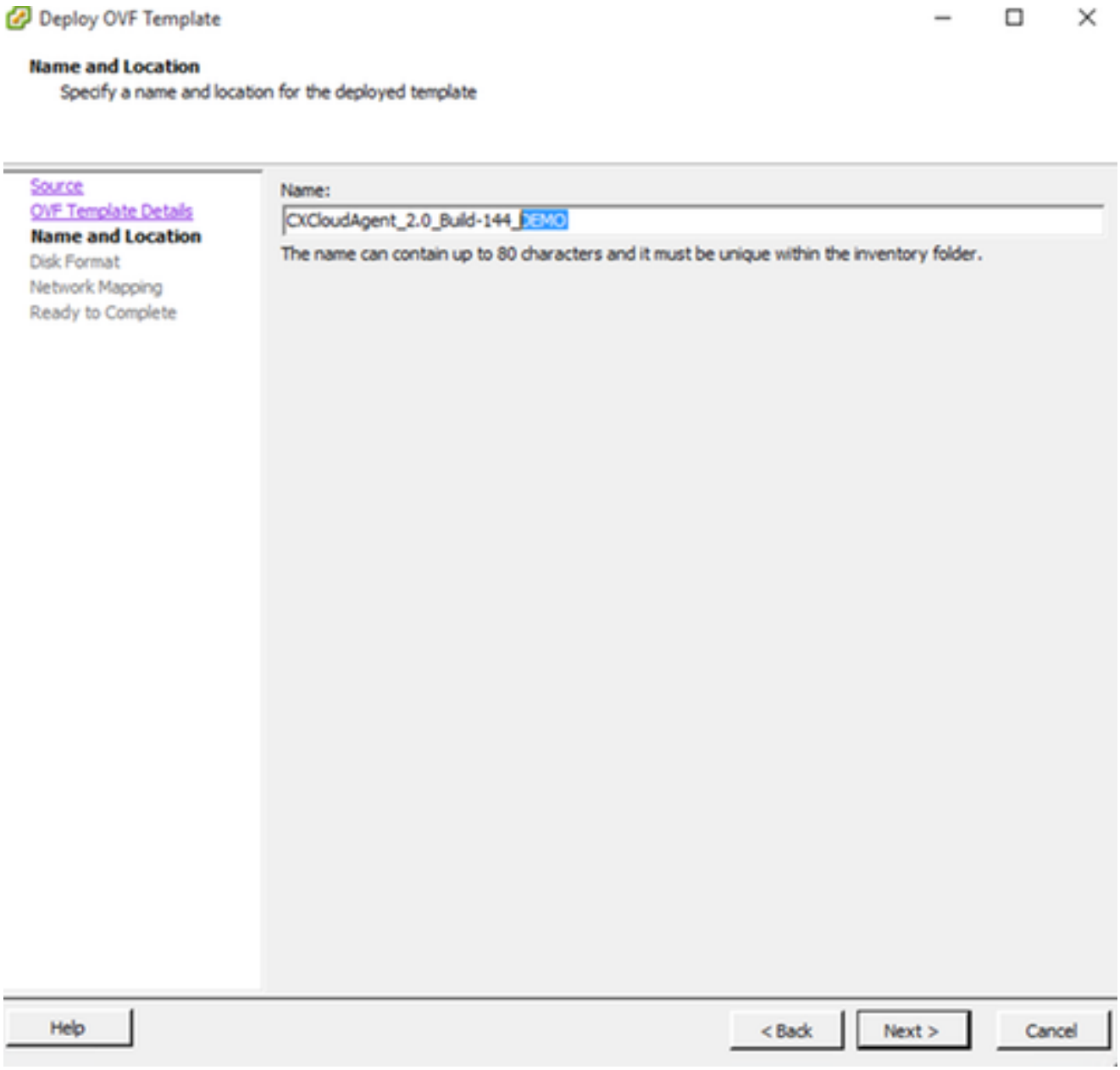
OVA-Pfad

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



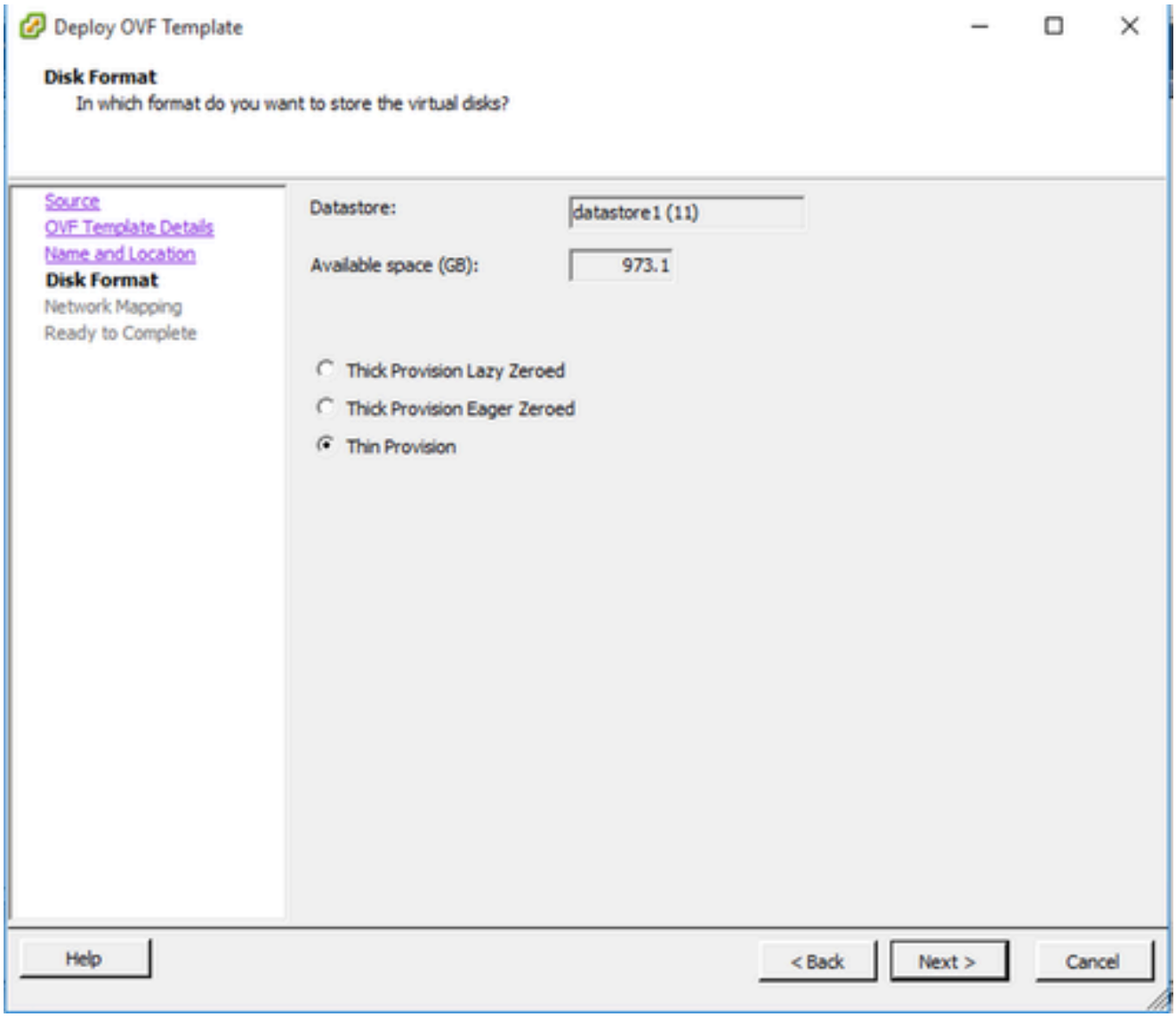
Vorlagendetails

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



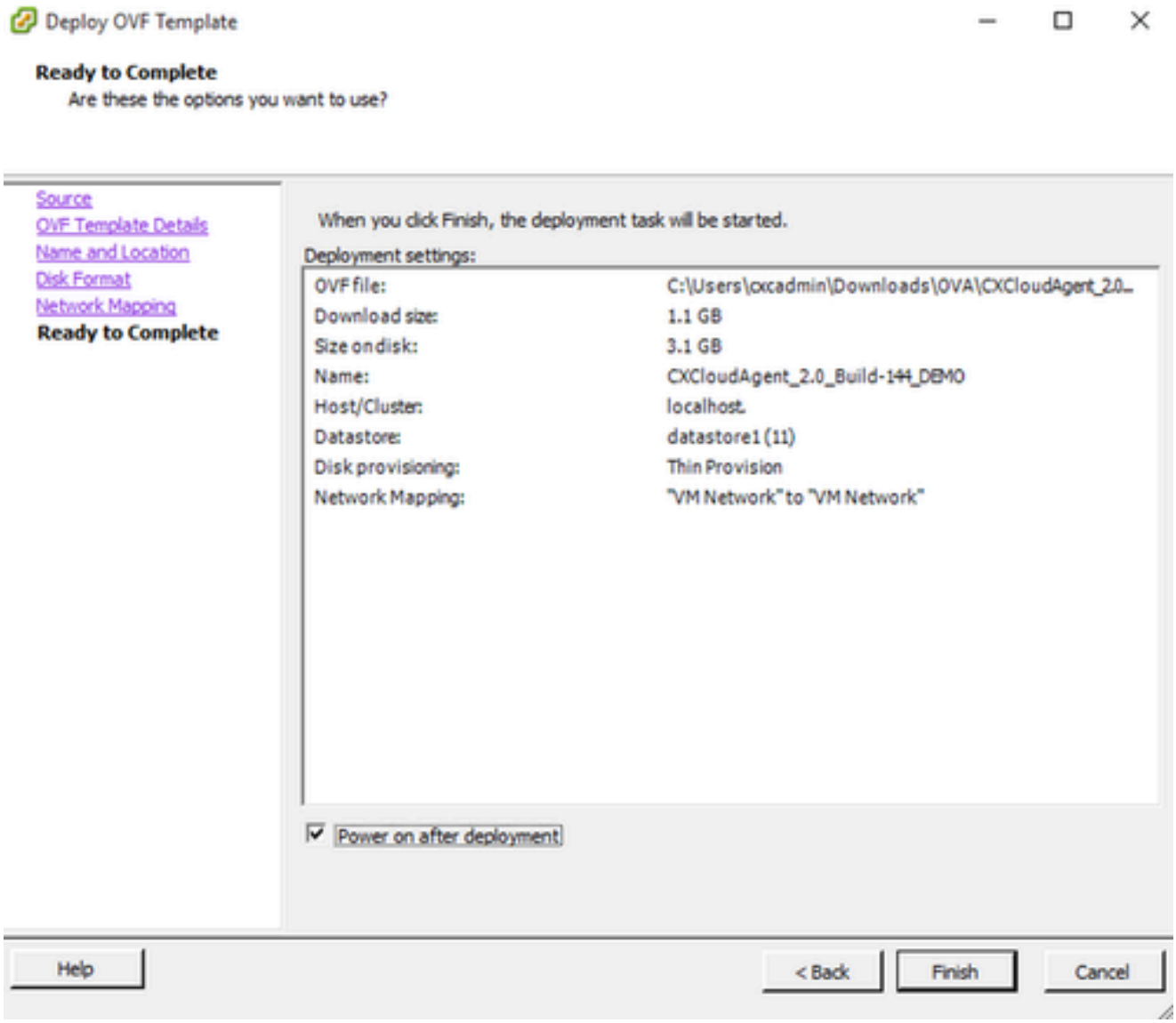
Name und Standort

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



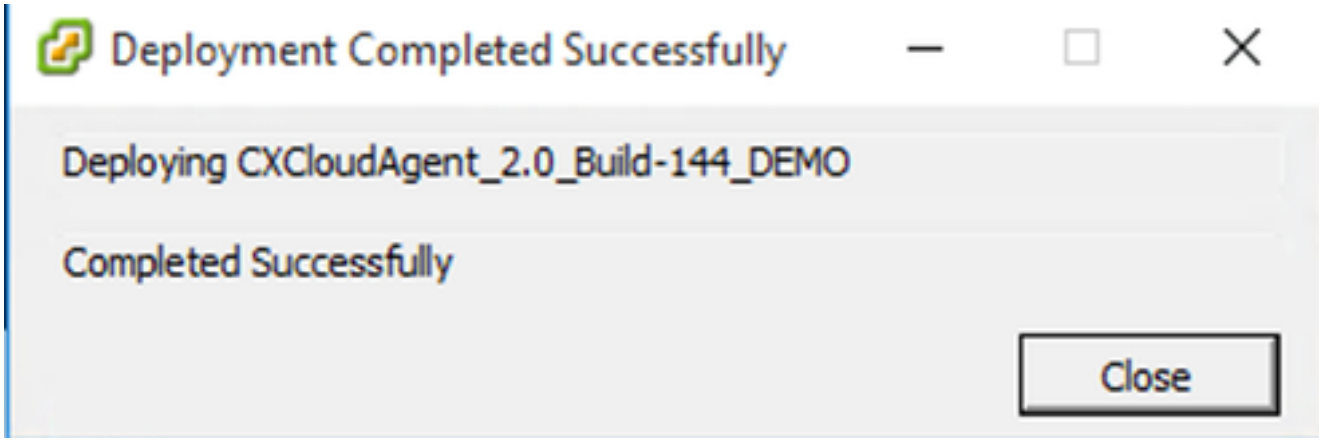
Datenträgerformatierung

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.



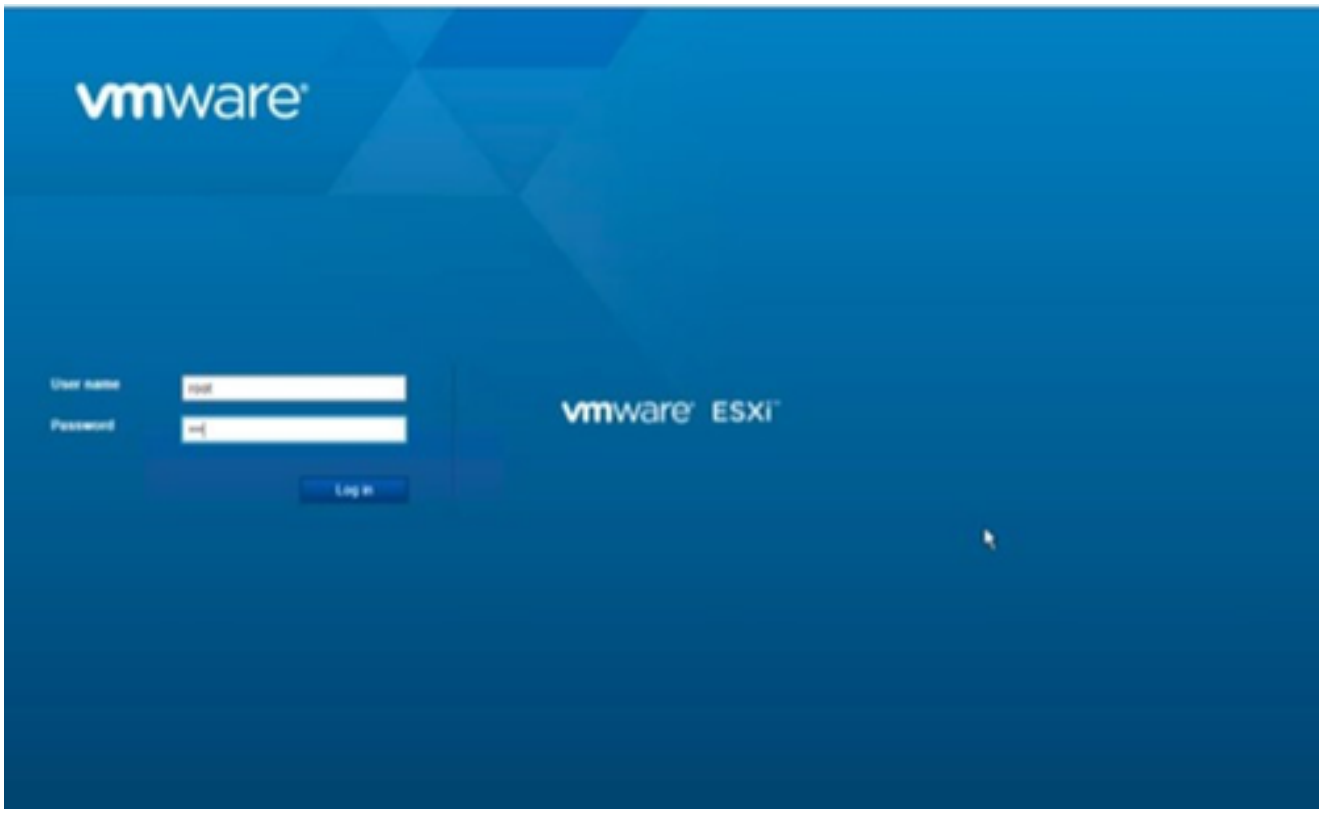
Bereitstellung abgeschlossen

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

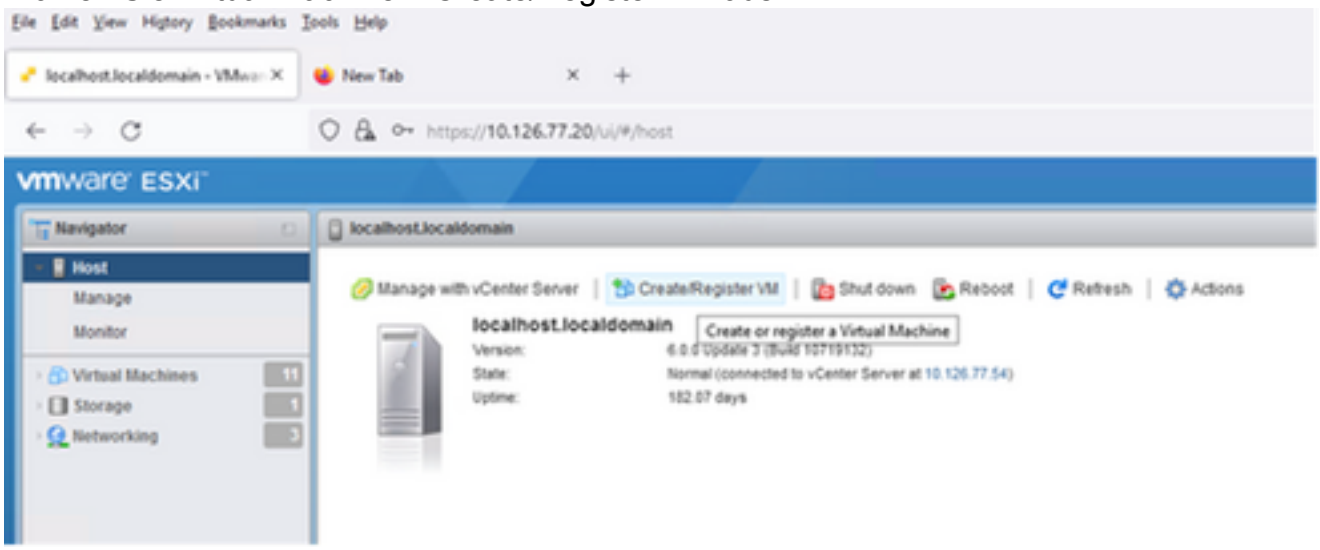
Dieser Client stellt CX Cloud OVA mithilfe von vSphere Web bereit.

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



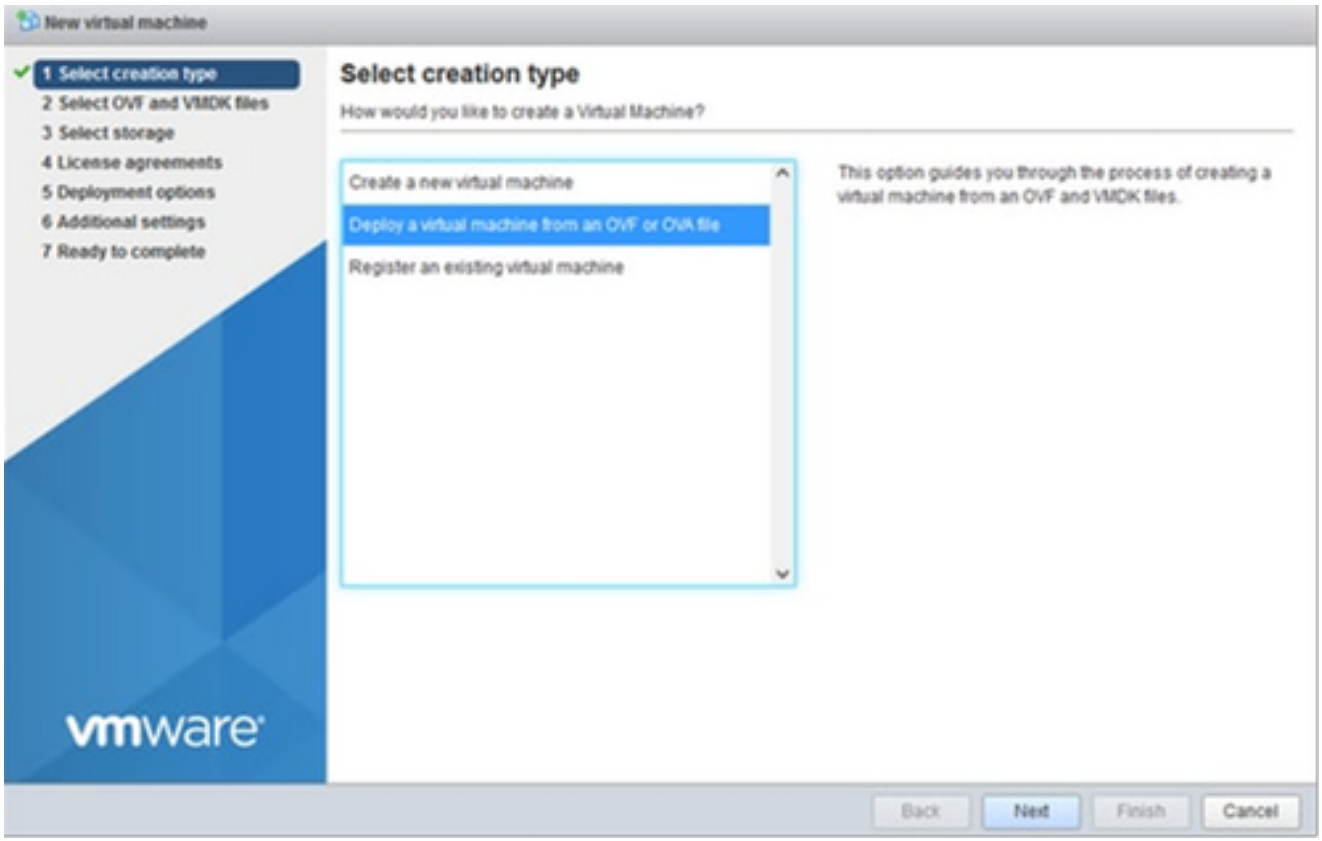
VMware ESXi-Anmeldung

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



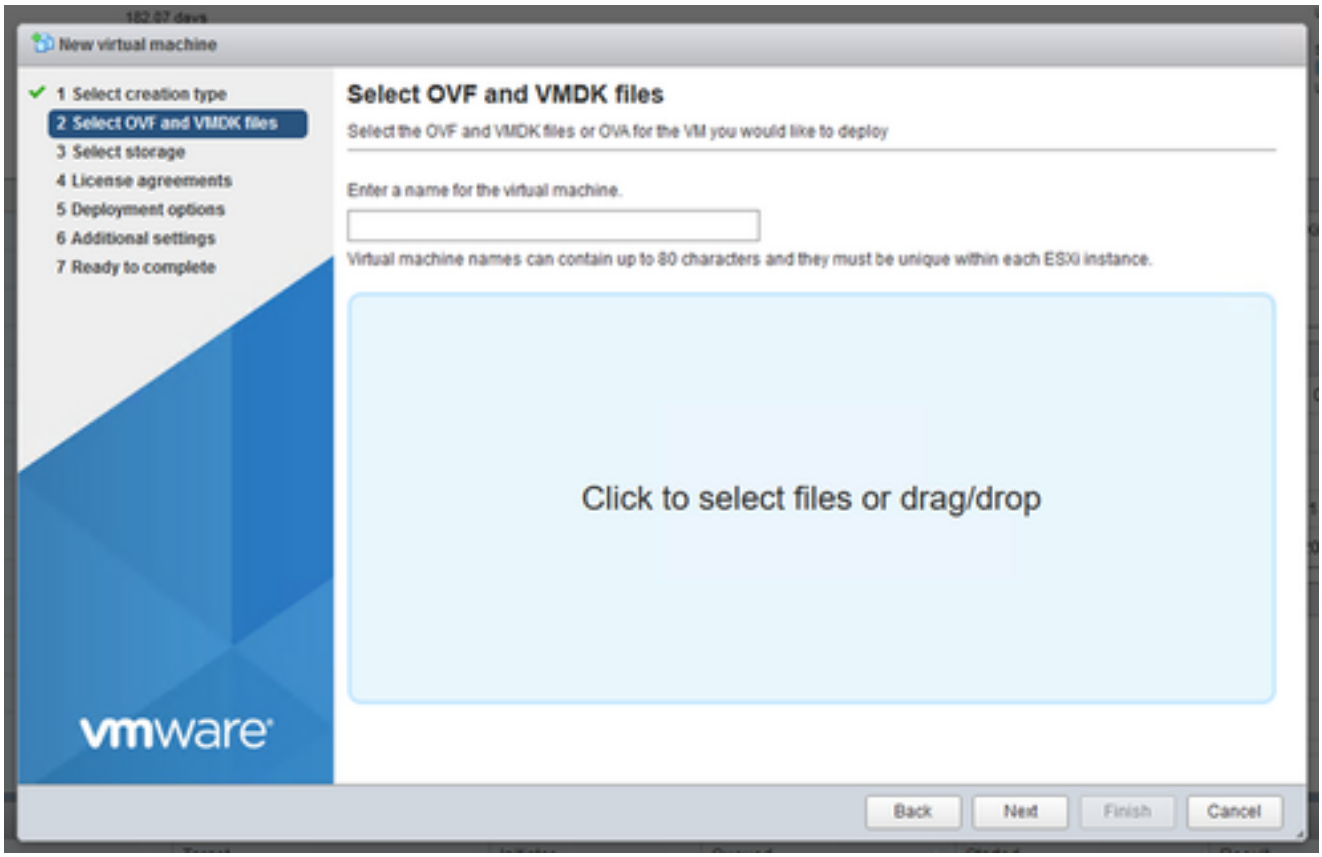
VM erstellen

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



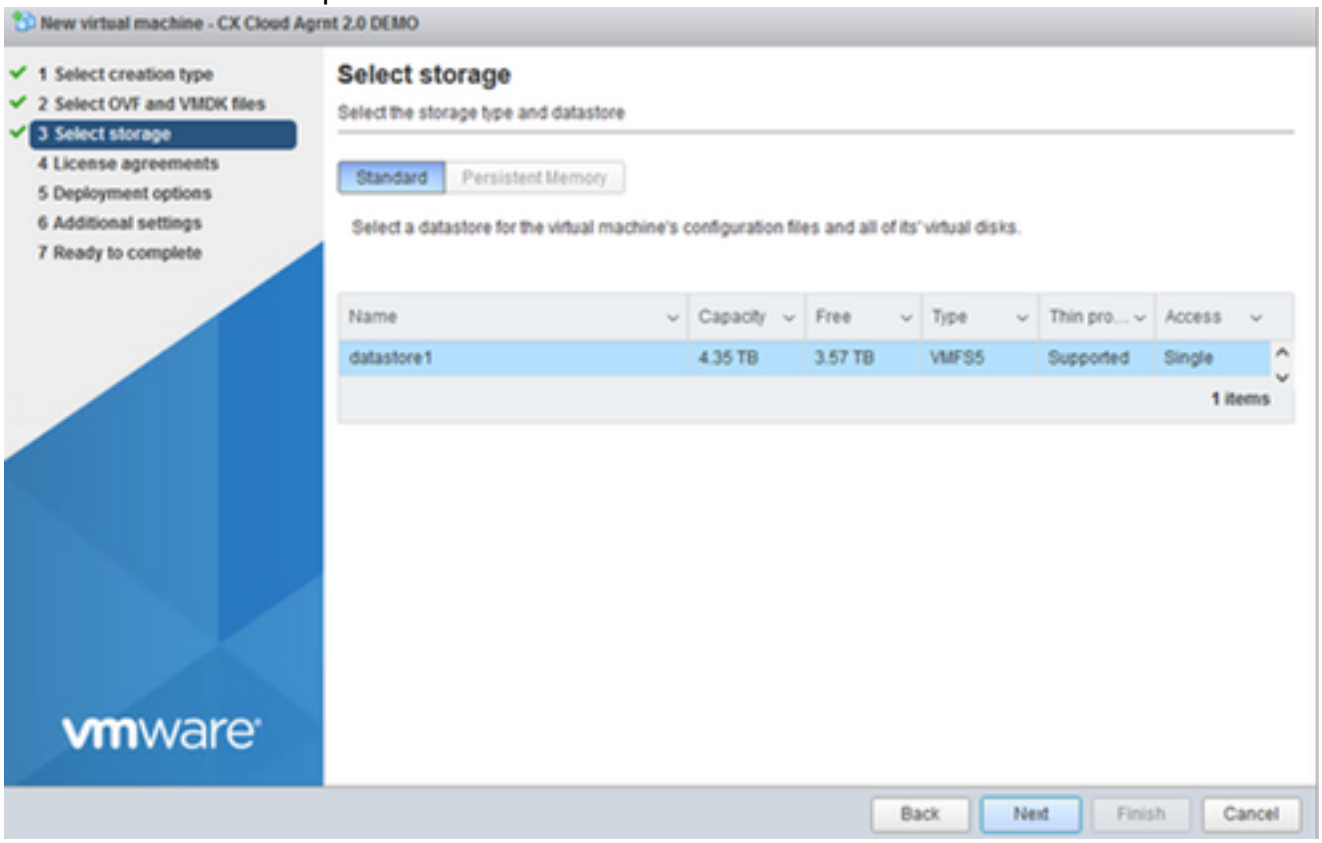
Erstellungstyp auswählen

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).



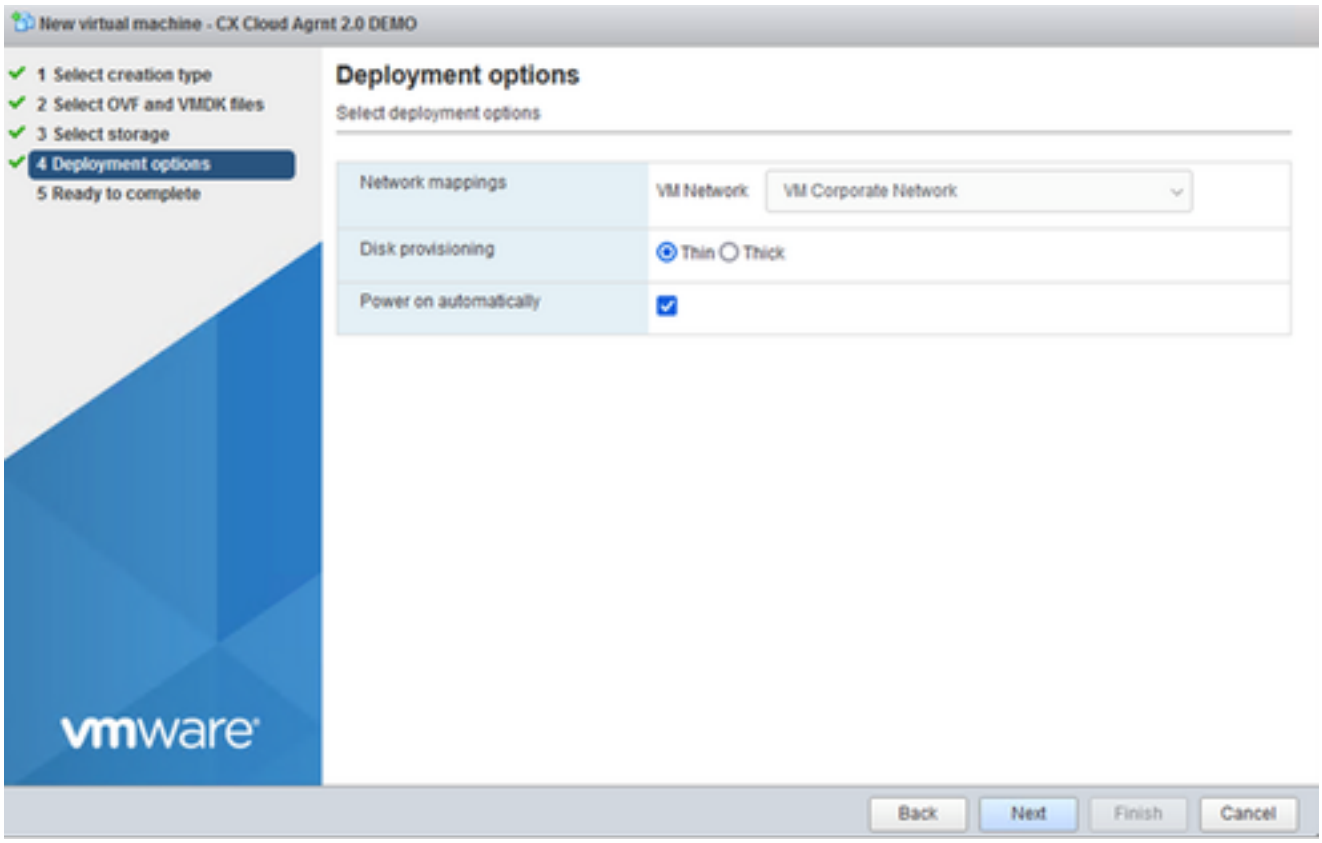
OVA-Auswahl

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



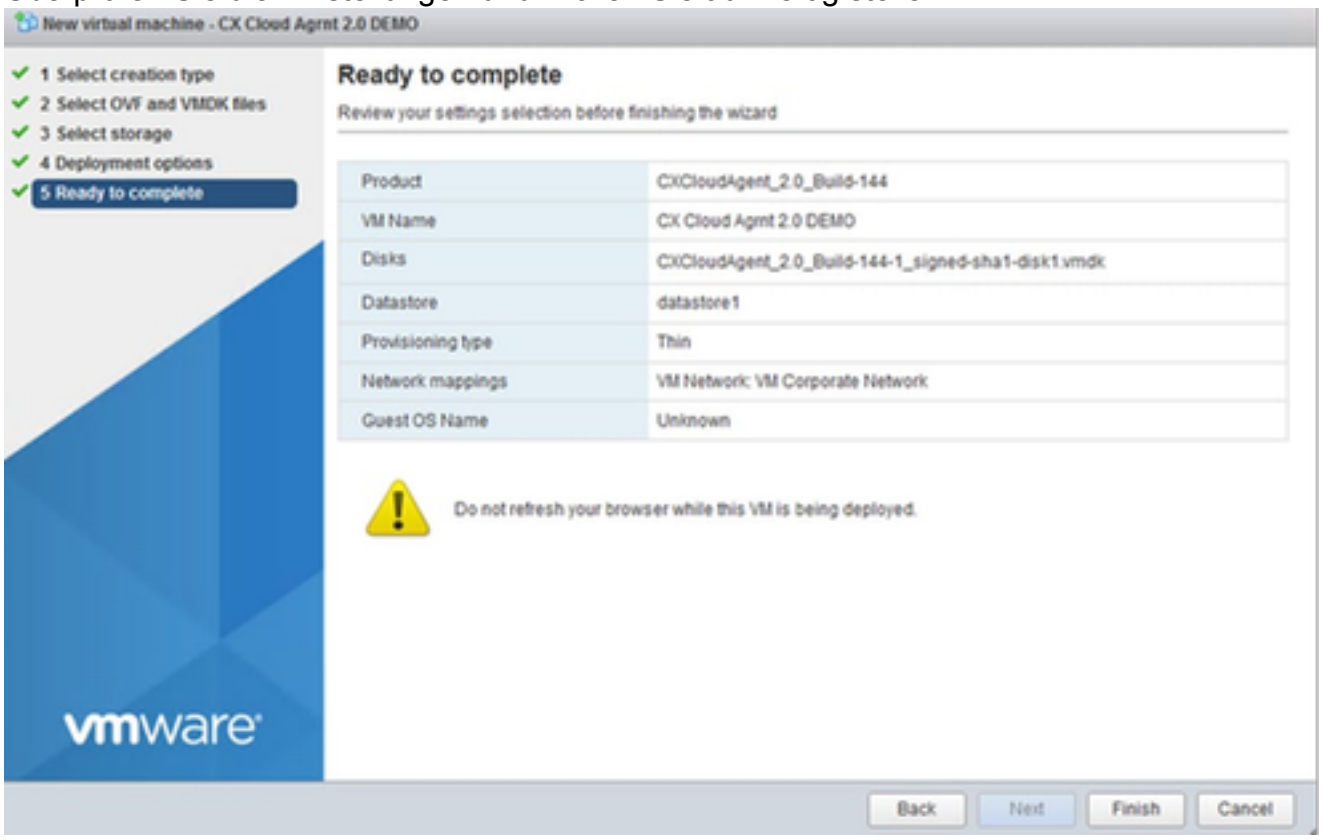
Auswahl von externem Speicher

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

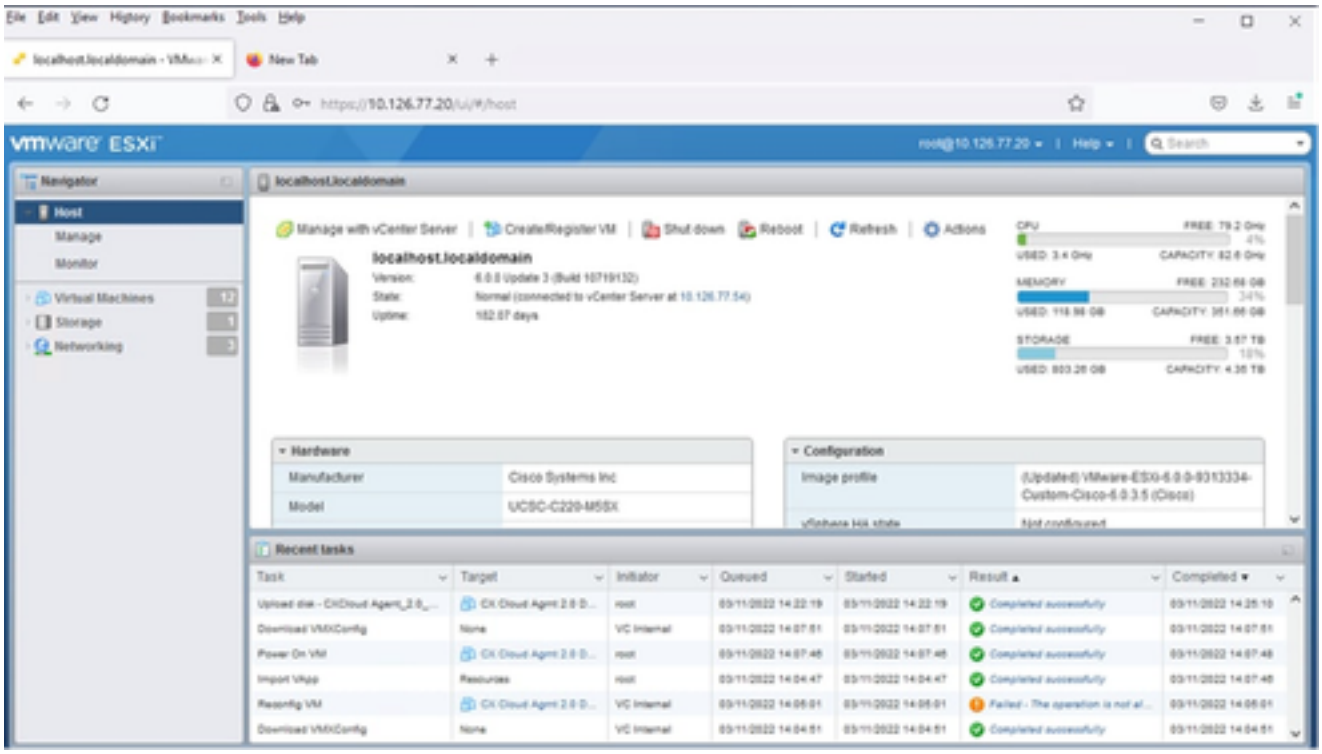


Bereitstellungsoptionen

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

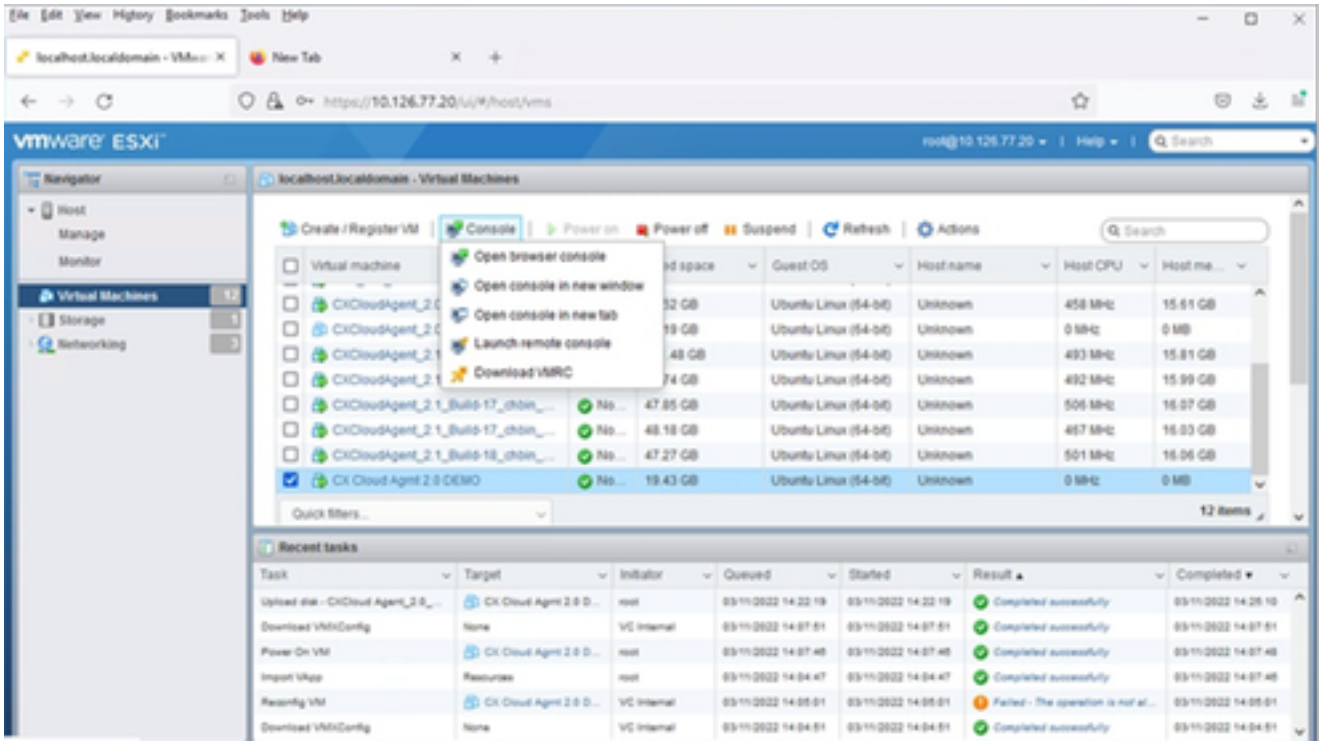


Bereit zur Fertigstellung



Abschluss erfolgreich

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



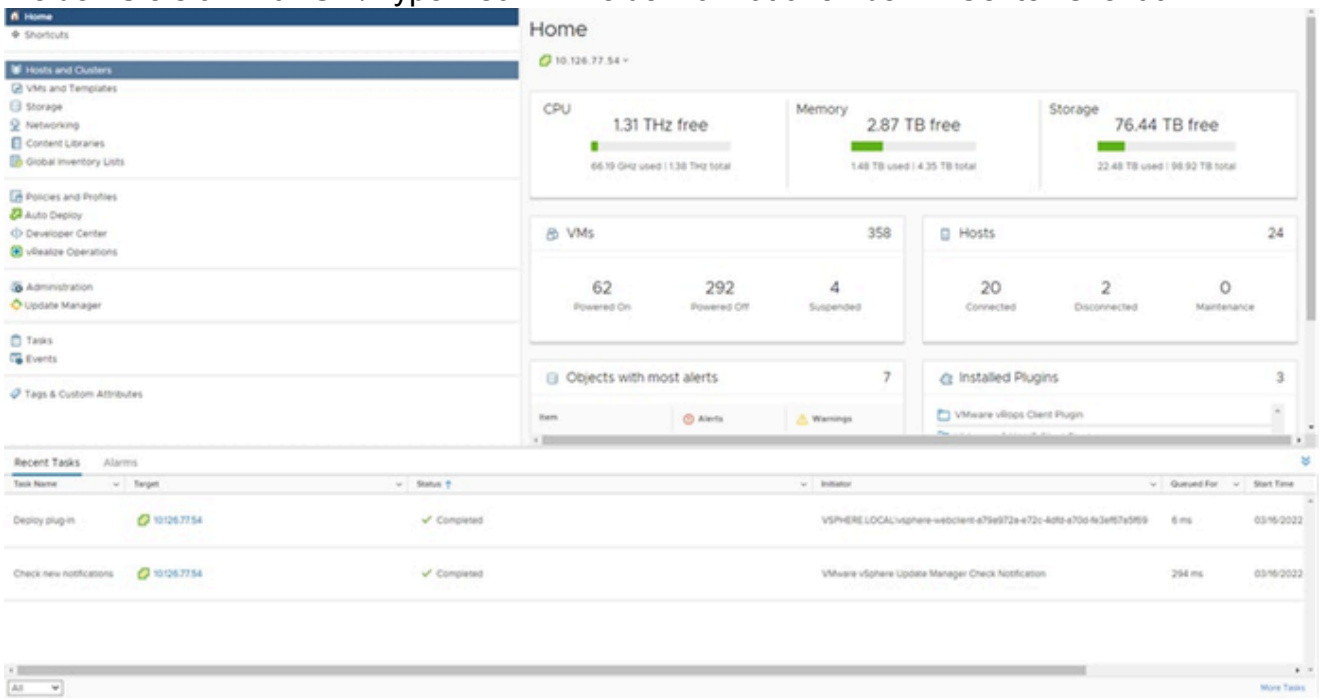
Konsole

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

Installation von Web Client vCenter

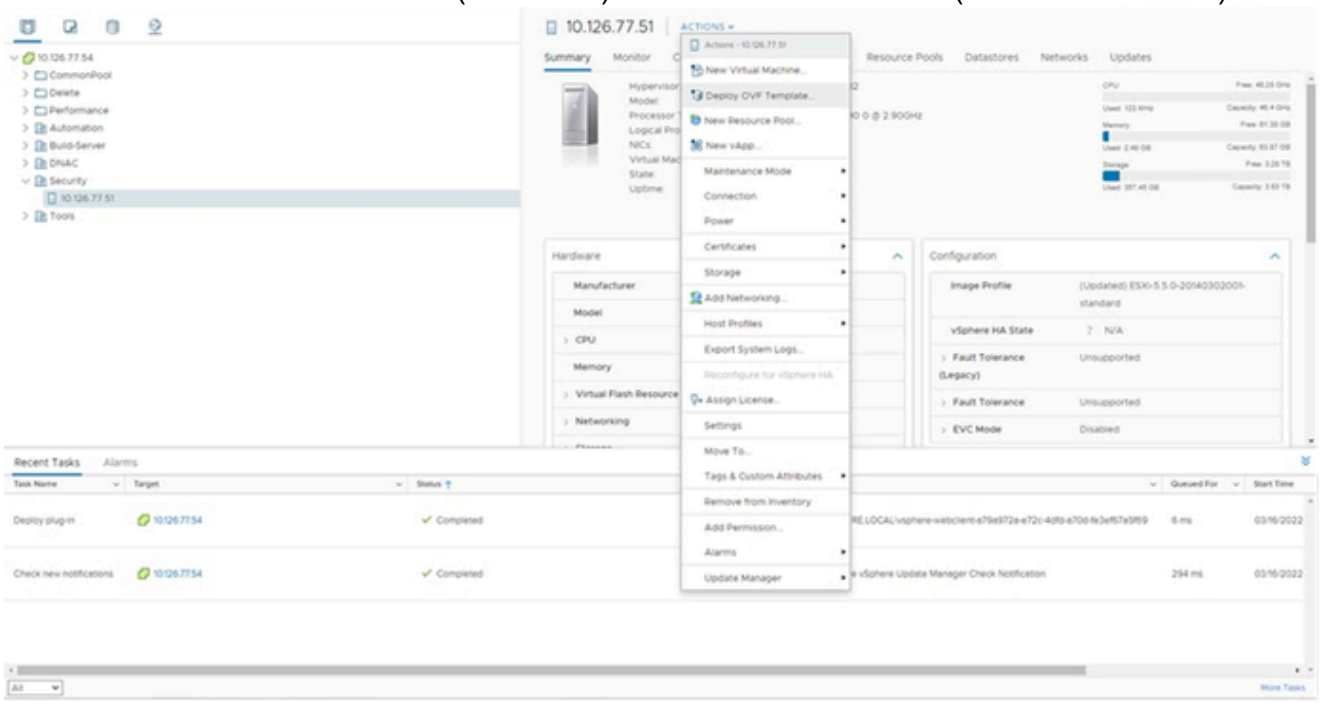
Dieser Client ermöglicht die Bereitstellung von CX Agent OVA mithilfe von Web Client vCenter.

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



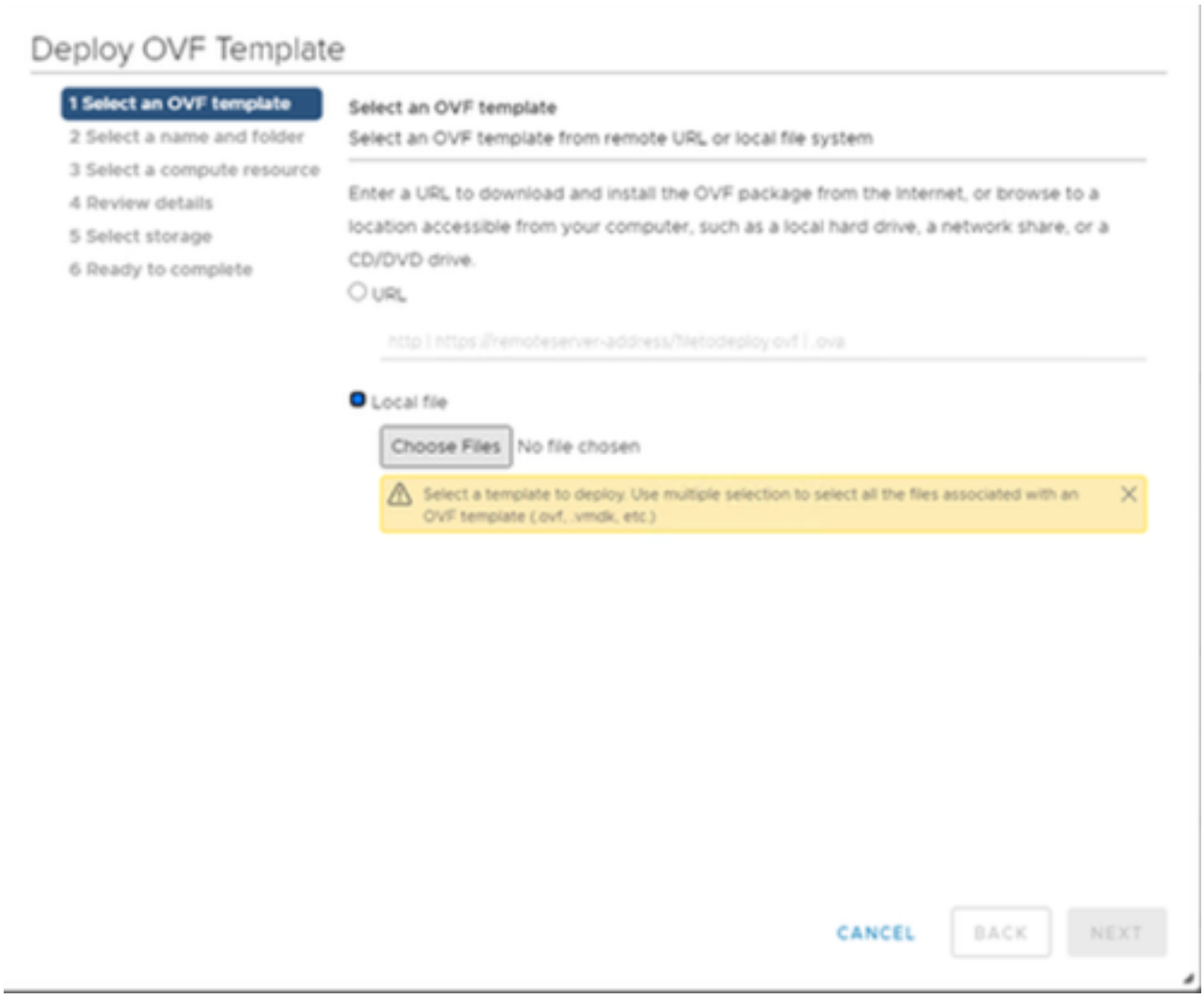
Startseite

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



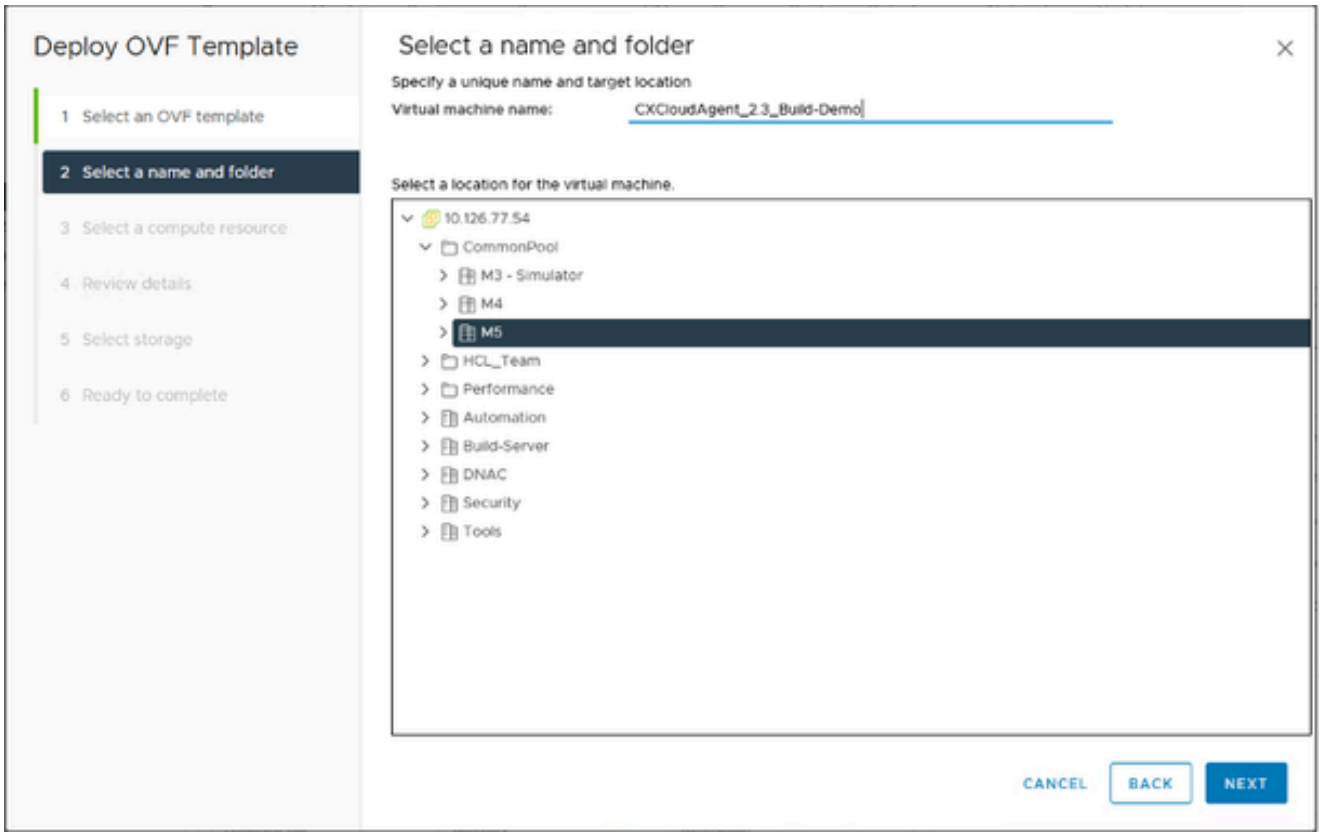
Hosts und Cluster

3. Wählen Sie die VM aus, und klicken Sie auf Action > Deploy OVF Template (Aktion > OVF-Vorlage bereitstellen).



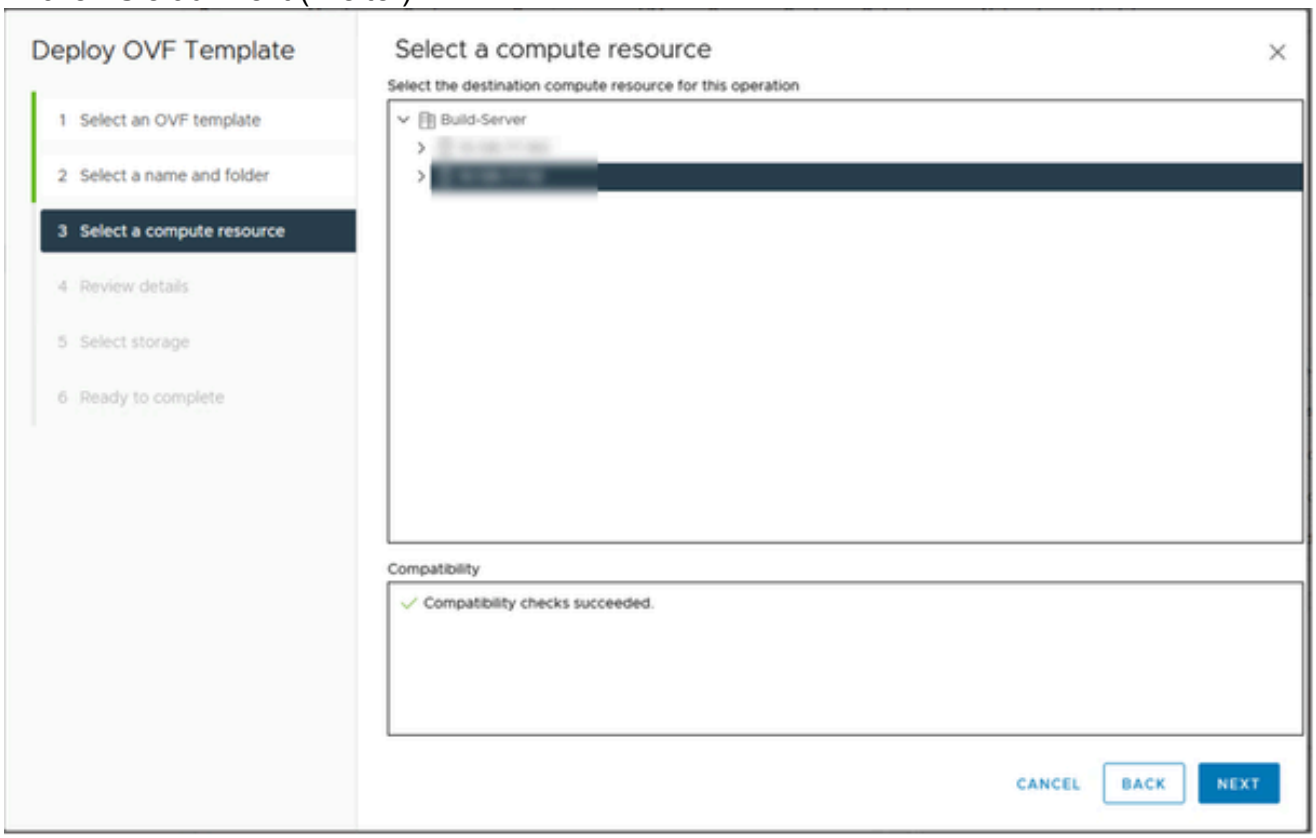
OVF bereitstellen

4. Fügen Sie die URL direkt hinzu, oder wählen Sie die OVA-Datei aus.
5. Klicken Sie auf Next (Weiter).



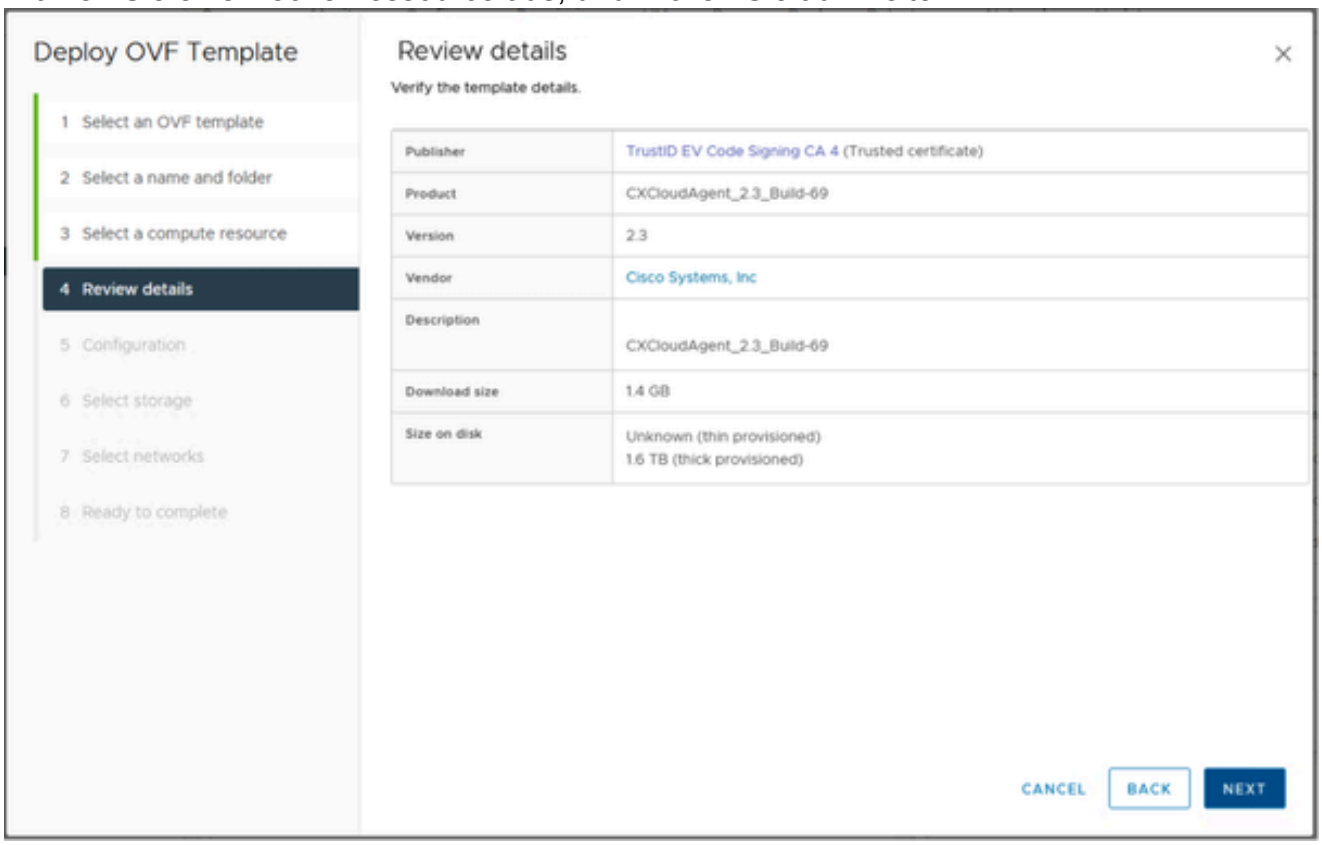
Name und Ordner

6. Geben Sie einen eindeutigen Namen ein, und navigieren Sie ggf. zum gewünschten Speicherort.
7. Klicken Sie auf Next (Weiter).



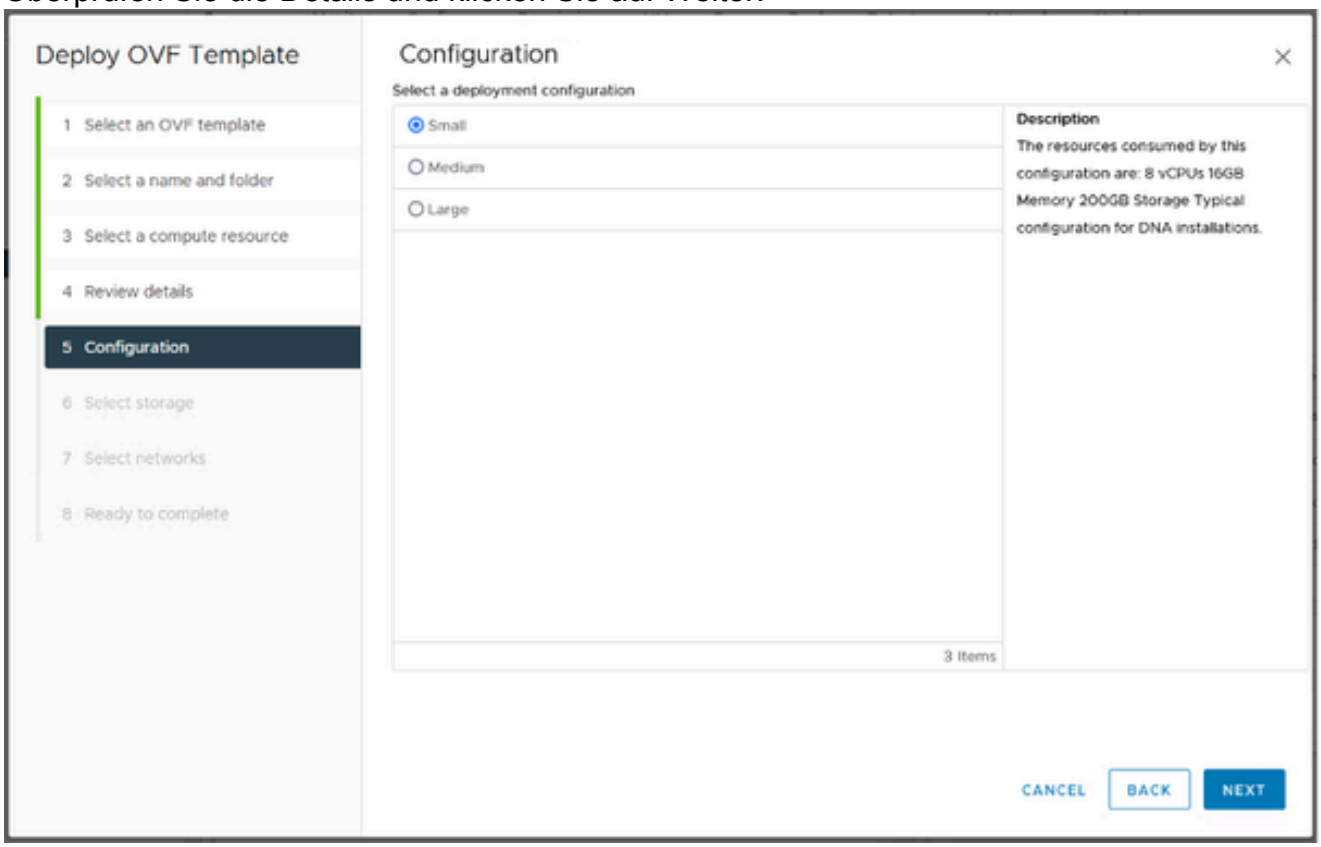
Rechenressource auswählen

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



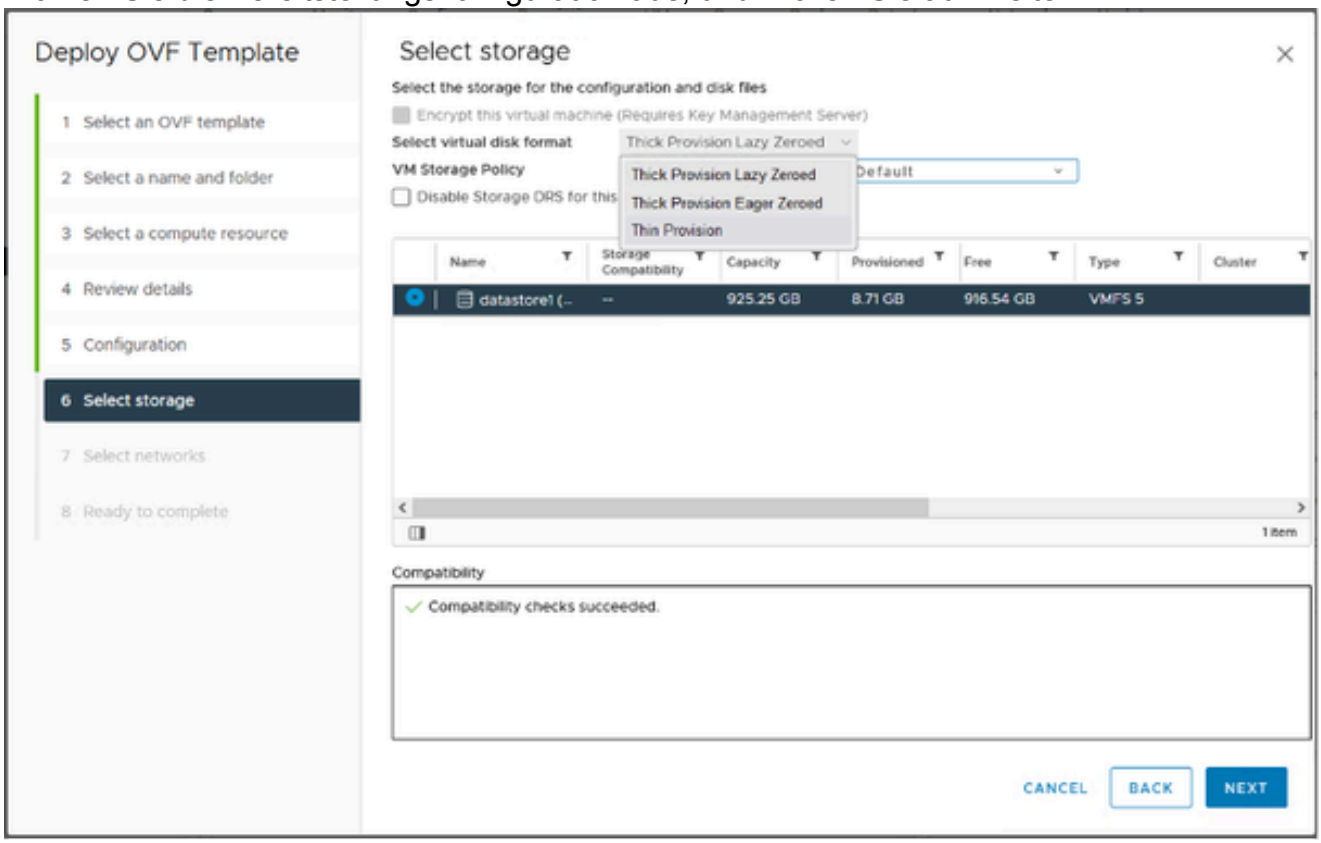
Details überprüfen

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



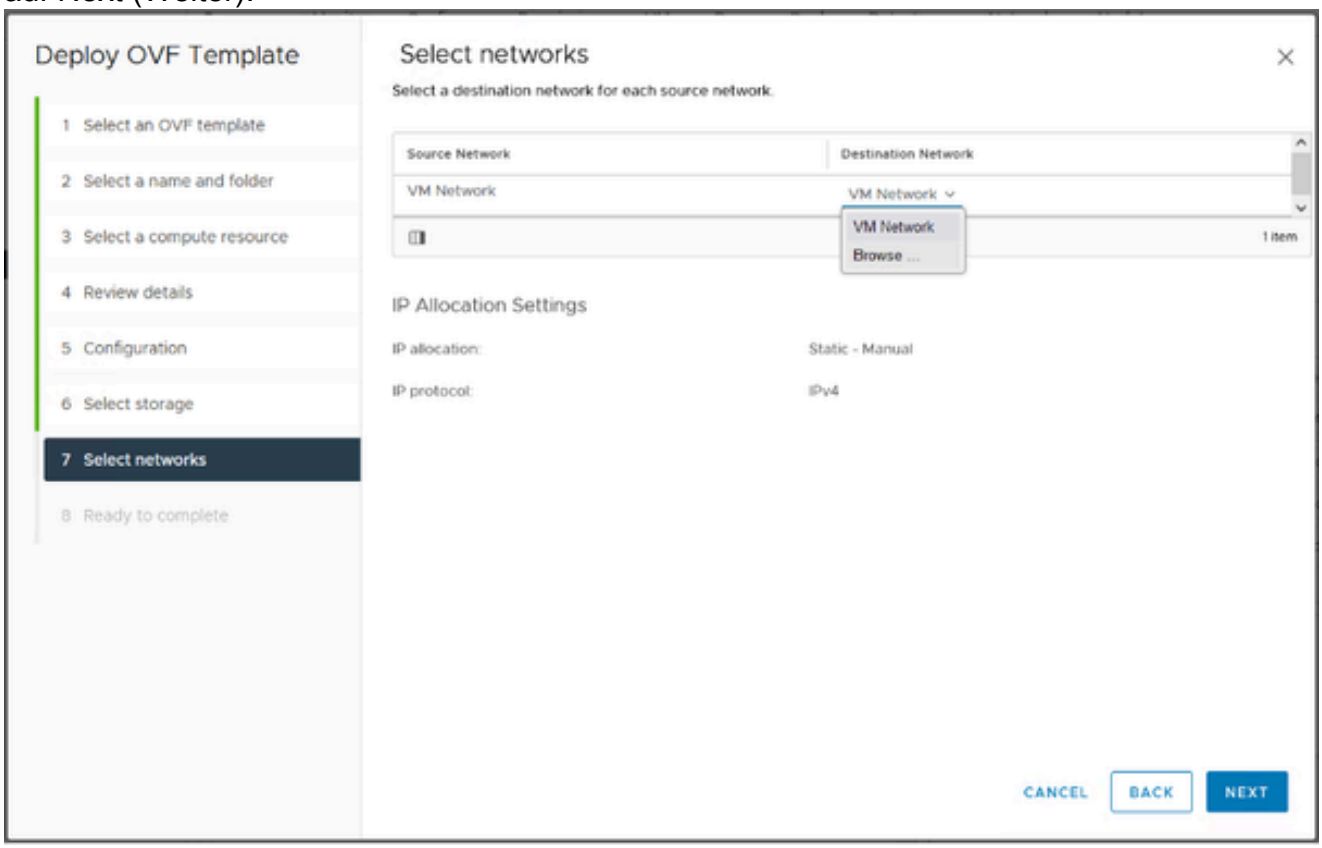
Konfiguration

10. Wählen Sie die Bereitstellungskonfiguration aus, und klicken Sie auf Weiter.



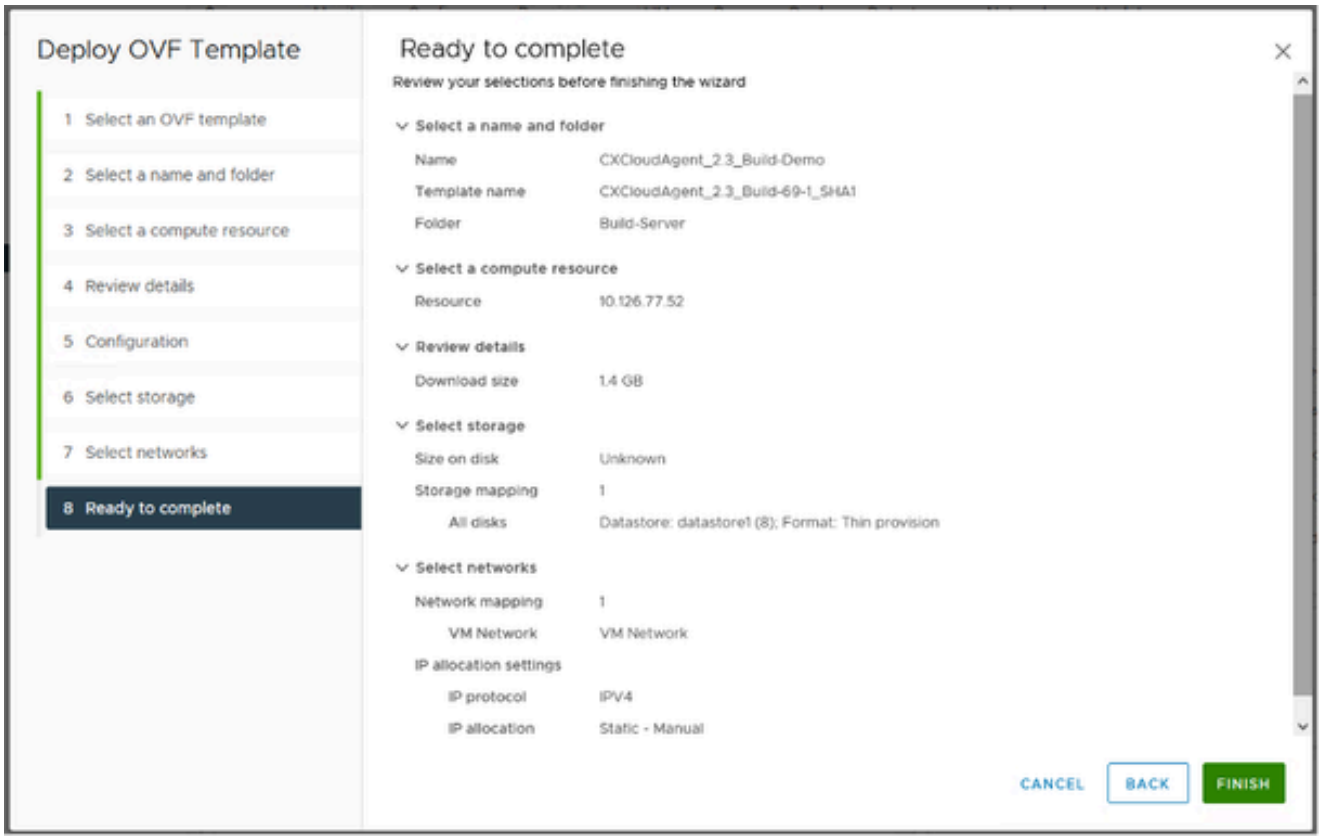
Konfiguration

11. Wählen Sie Storage > Select virtual disk format aus der Dropdown-Liste aus, und klicken Sie auf Next (Weiter).



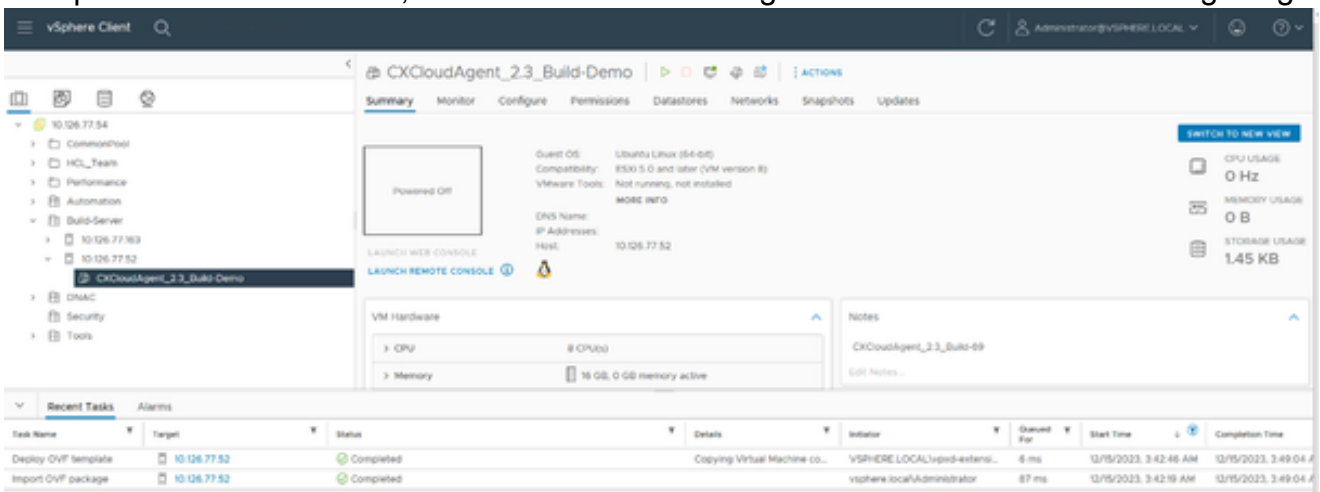
Netzwerke auswählen

12. Wählen Sie die entsprechenden Optionen unter Netzwerke auswählen aus, und klicken Sie auf Weiter.



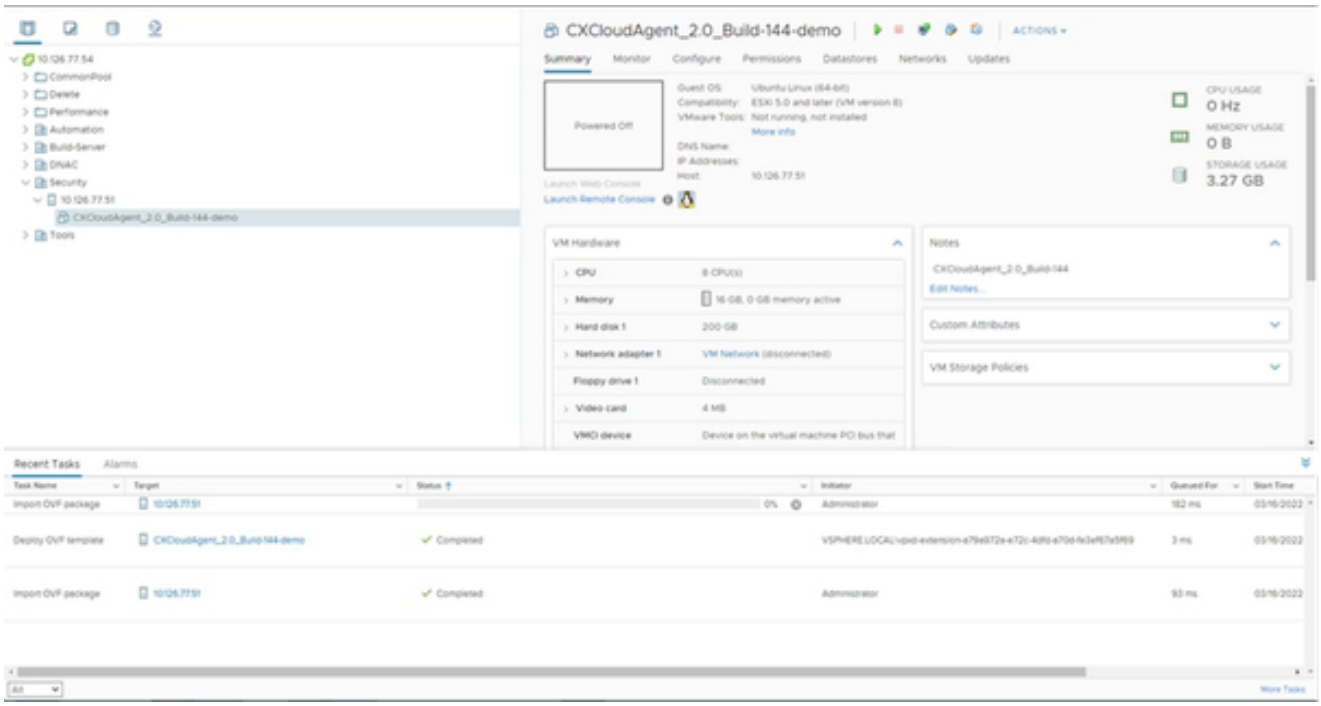
Bereit zur Fertigstellung

13. Überprüfen Sie die Auswahl, und klicken Sie auf Fertig stellen. Die Startseite wird angezeigt.



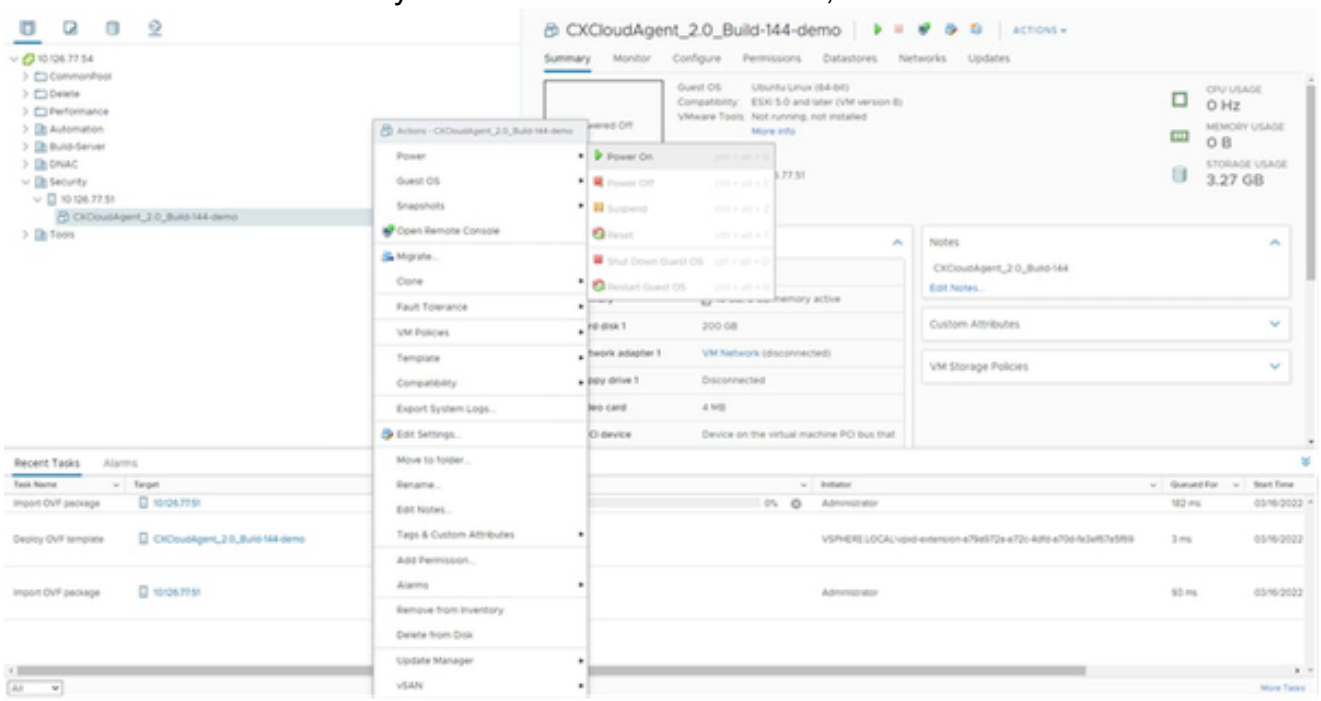
VM hinzugefügt

14. Klicken Sie auf das neu hinzugefügte virtuelle System, um den Status anzuzeigen.



VM hinzugefügt

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



Konsole öffnen

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

Installation von Oracle VirtualBox 7.0.12

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

1. Laden Sie die OVA CXCloudAgent_3.1 in das Windows-Fenster eines beliebigen Ordners herunter.

2. Navigieren Sie über die Befehlszeilenschnittstelle zum Ordner.
3. Entpacken Sie die OVA-Datei mit dem Befehl tar -xvf D:\CXCloudAgent_3.1_Build-xx.ova.

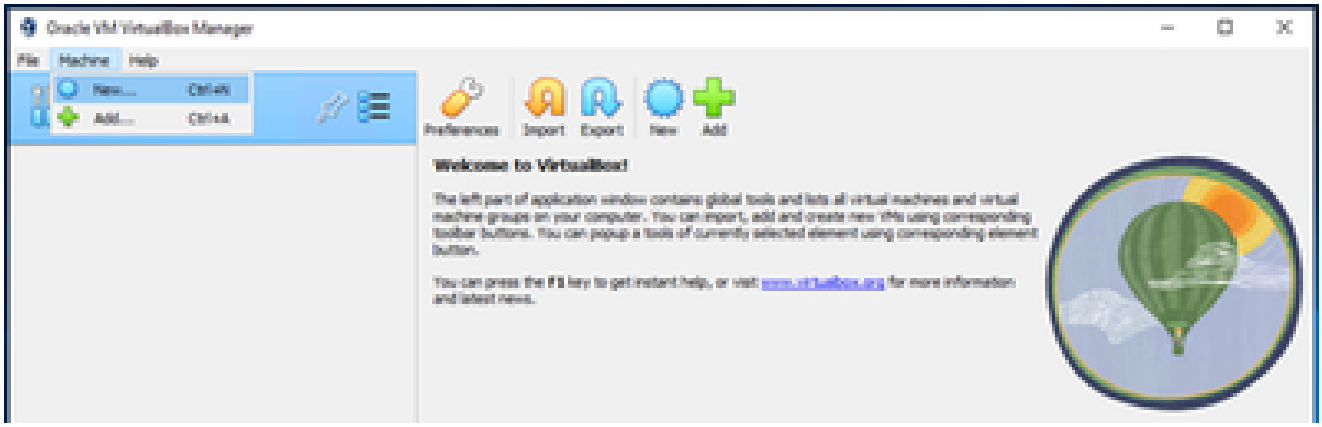
```
D:\>cd CXCAGENT

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

D:\CXCAGENT>_
```

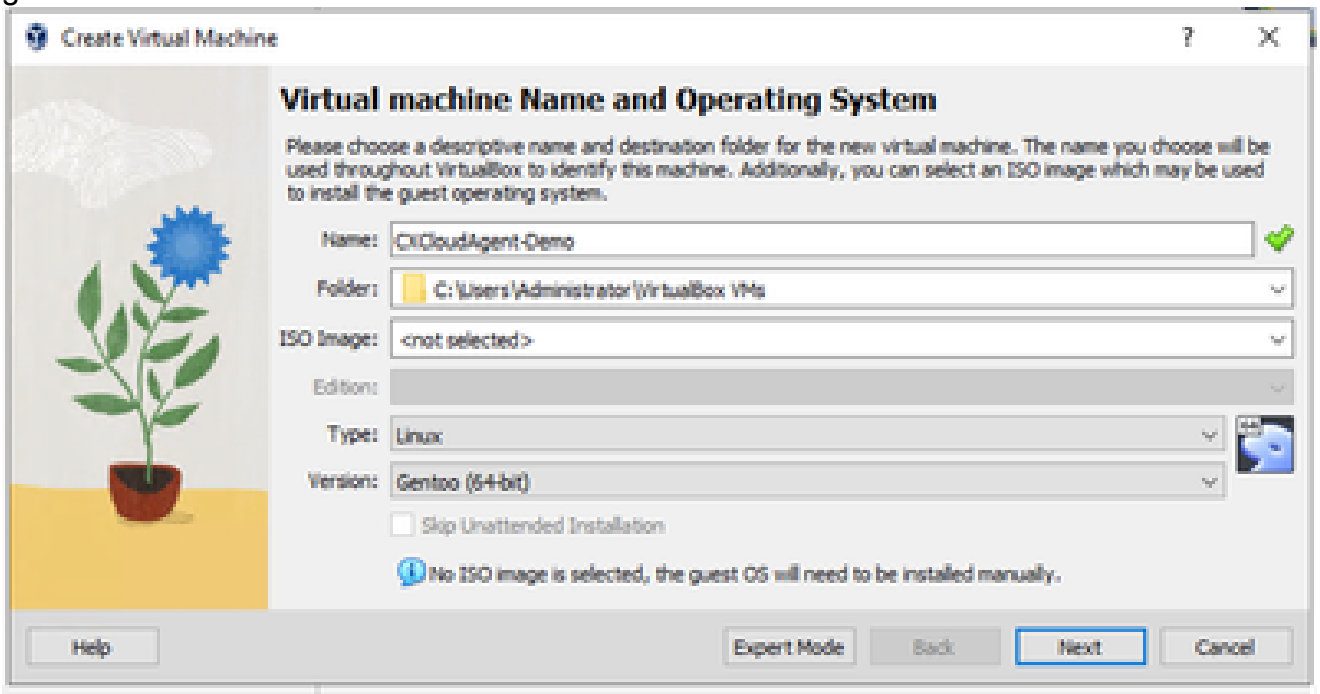
OVA-Datei entpacken

4. Öffnen Sie die Oracle VM-Benutzeroberfläche.



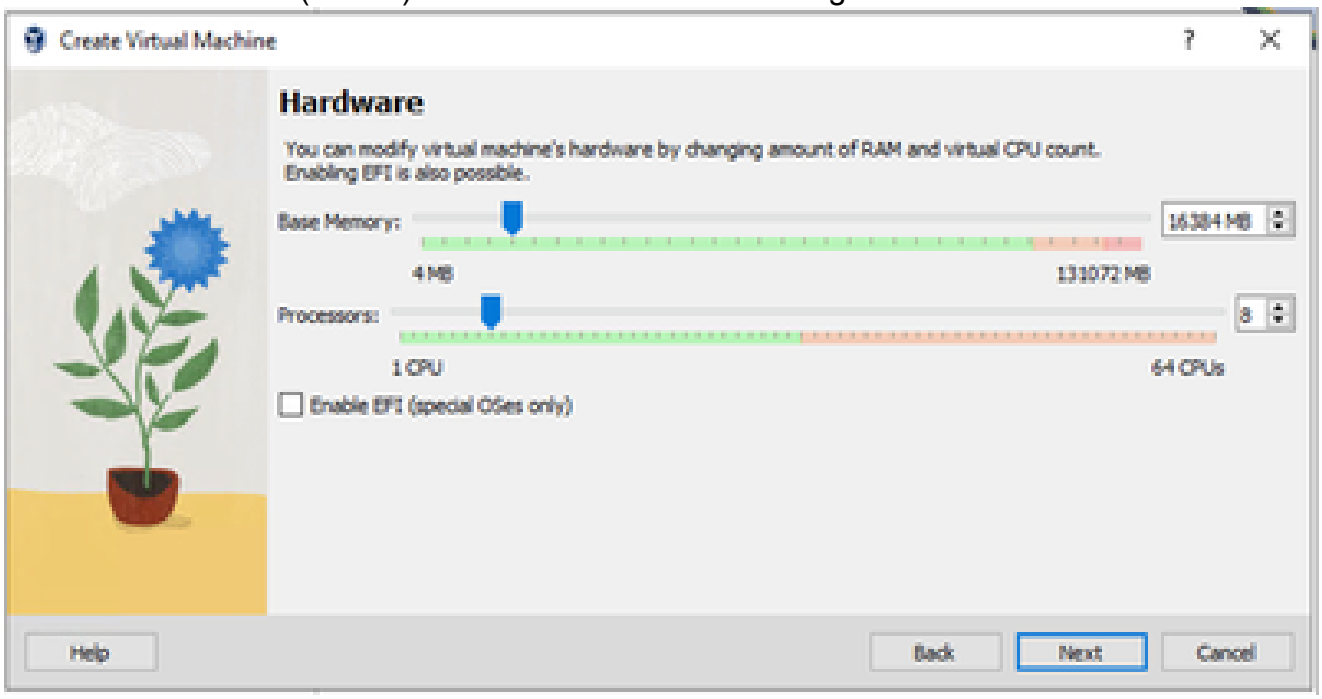
Oracle VM

5. Wählen Sie im Menü Maschine > Neu. Das Fenster Virtuellen Computer erstellen wird geöffnet.



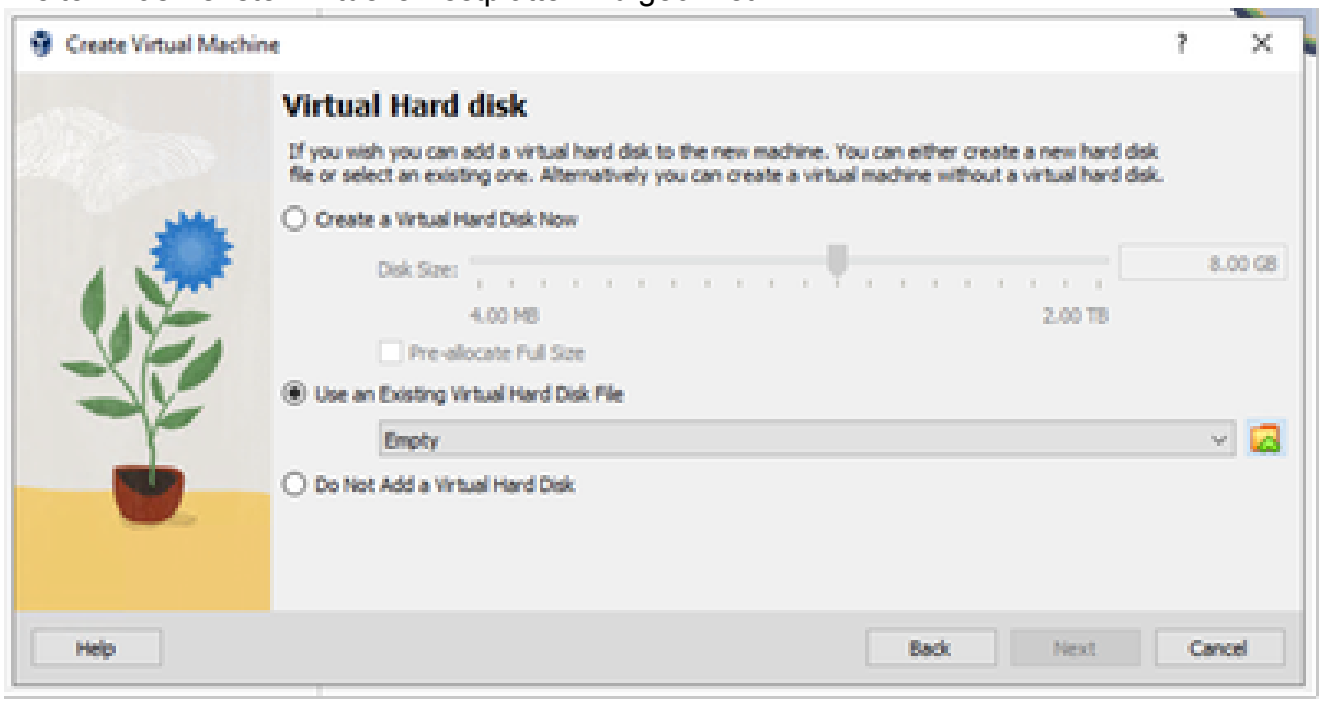
Virtuellen Computer erstellen

6. Geben Sie im Fenster Name des virtuellen Systems und Betriebssystem die folgenden Details ein.
   Name: VM-Name
   Ordner: Speicherort der VM-Daten
   ISO-Image: none
   Typ: Linux
   Version: Gentoo (64 Bit)
7. Klicken Sie auf Next (Weiter). Das Fenster Hardware wird geöffnet.



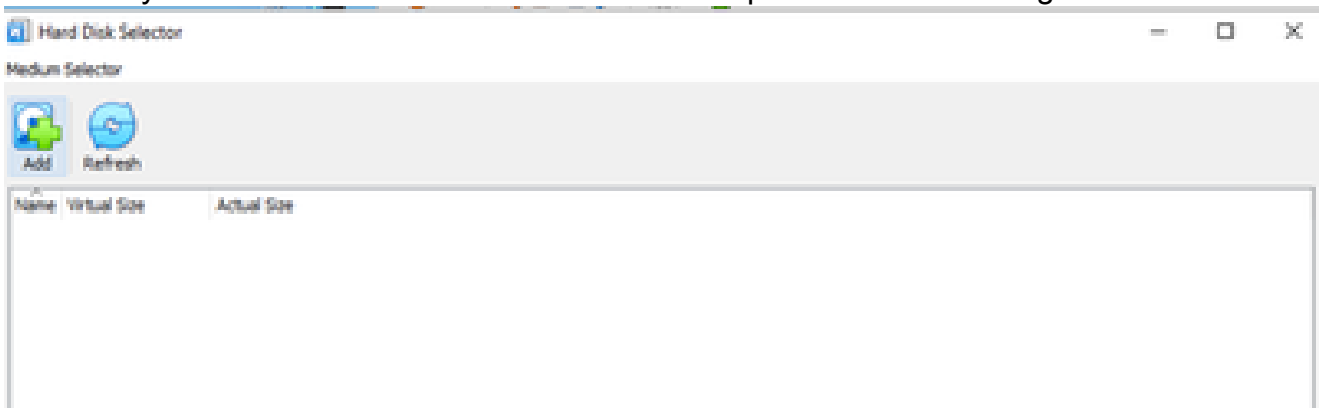
Hardware

8. Geben Sie Basisspeicher (16384 MB) und Prozessoren (8 CPU) ein, und klicken Sie auf Weiter. Das Fenster Virtuelle Festplatte wird geöffnet.



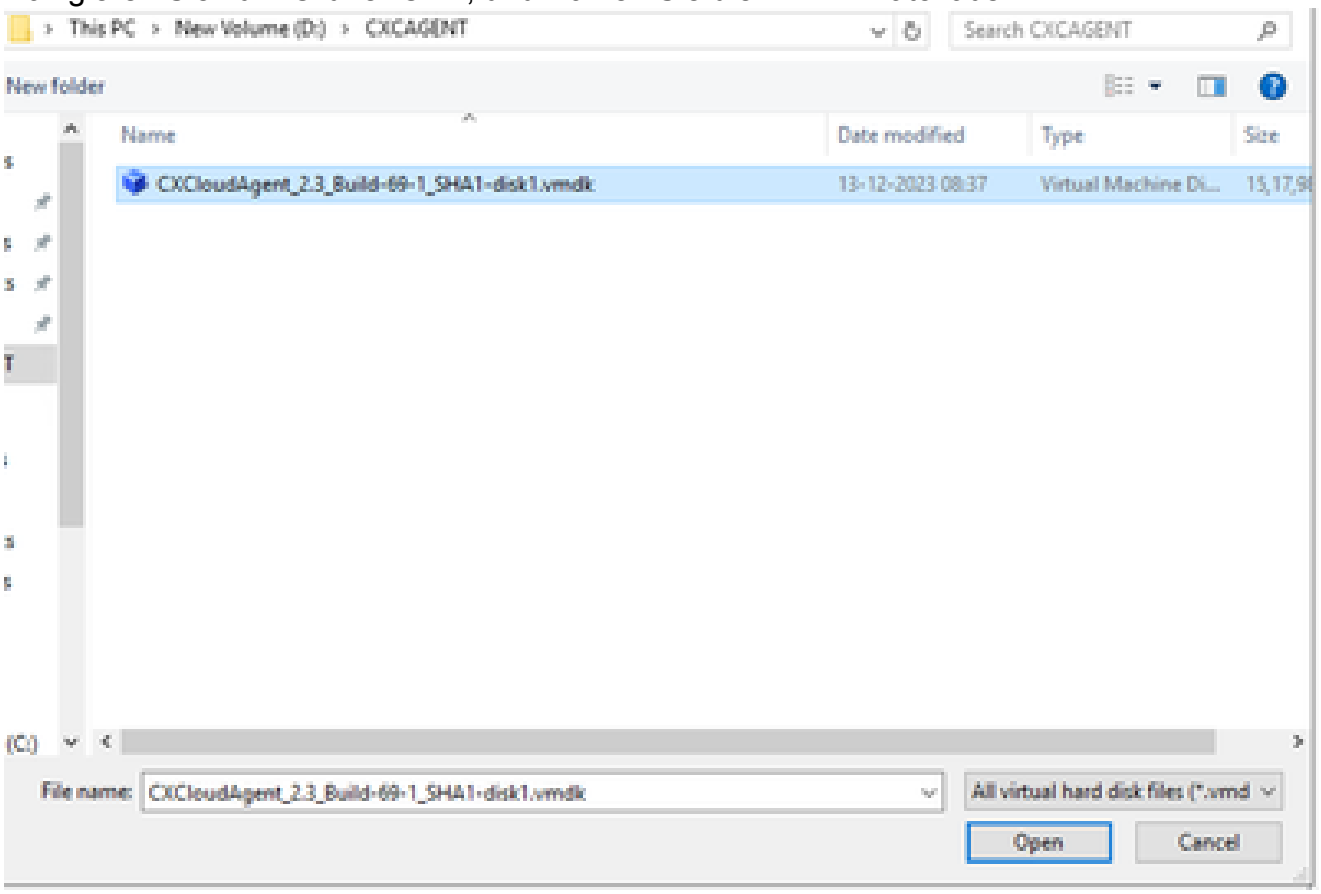
Virtuelle Festplatte

9. Aktivieren Sie das Optionsfeld Vorhandene virtuelle Festplattendatei verwenden, und wählen Sie das Symbol Durchsuchen aus. Das Fenster Festplattenauswahl wird geöffnet.



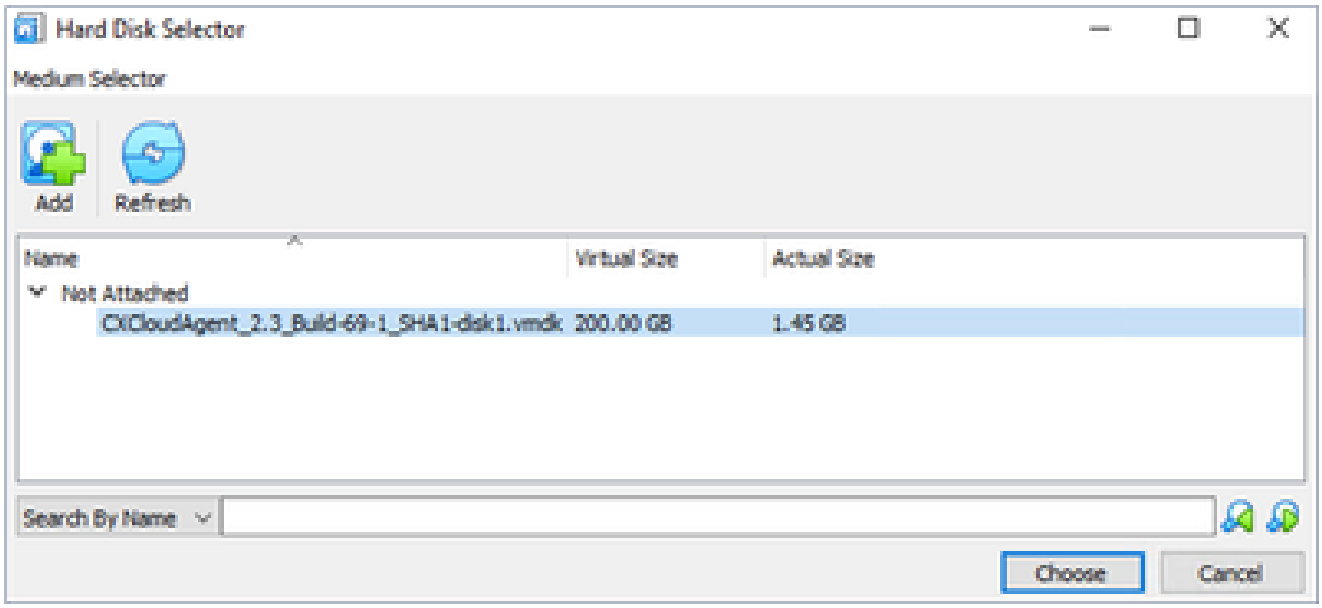
Festplattenauswahl

10. Navigieren Sie zum Ordner OVA, und wählen Sie die VMDK-Datei aus.



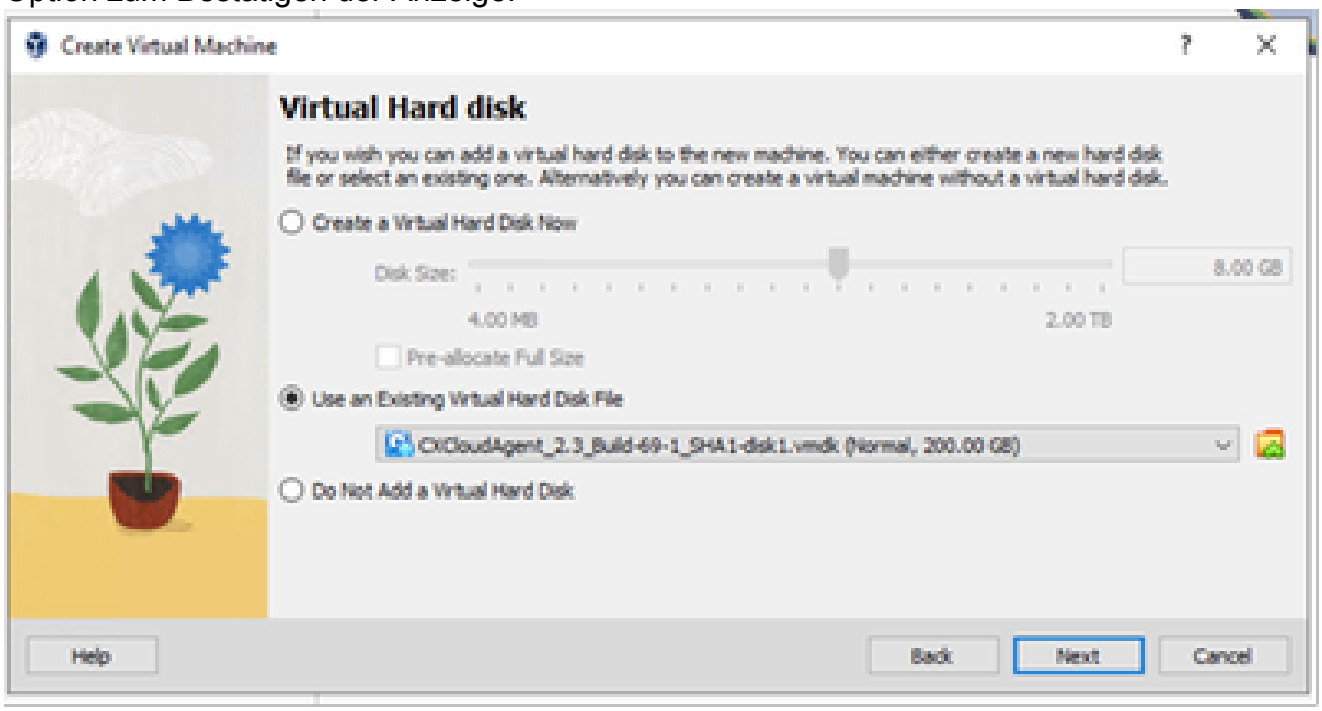
OVA-Ordner

11. Klicken Sie auf Öffnen. Die Datei wird im Fenster Hardware Disk Selector (Festplattenauswahl) angezeigt.



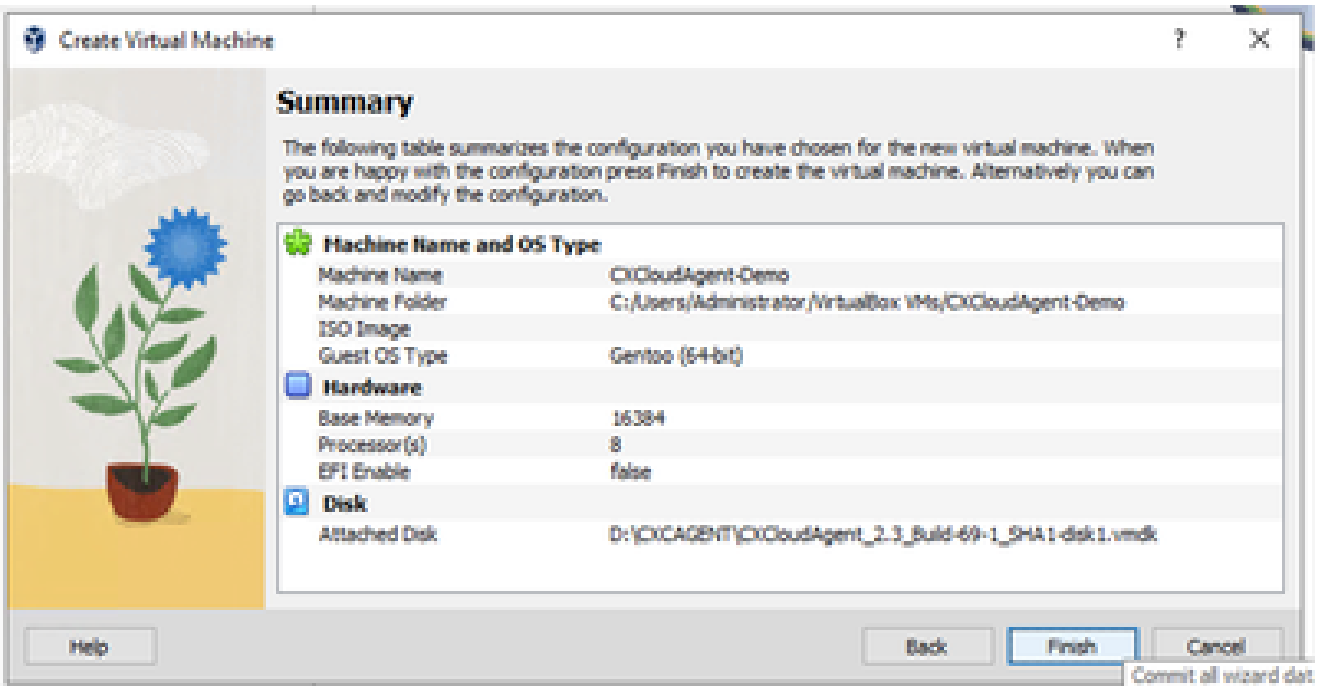
Festplattenauswahl

12. Klicken Sie auf Auswählen. Das Fenster Virtuelle Festplatte wird geöffnet. Aktivieren Sie die Option zum Bestätigen der Anzeige.



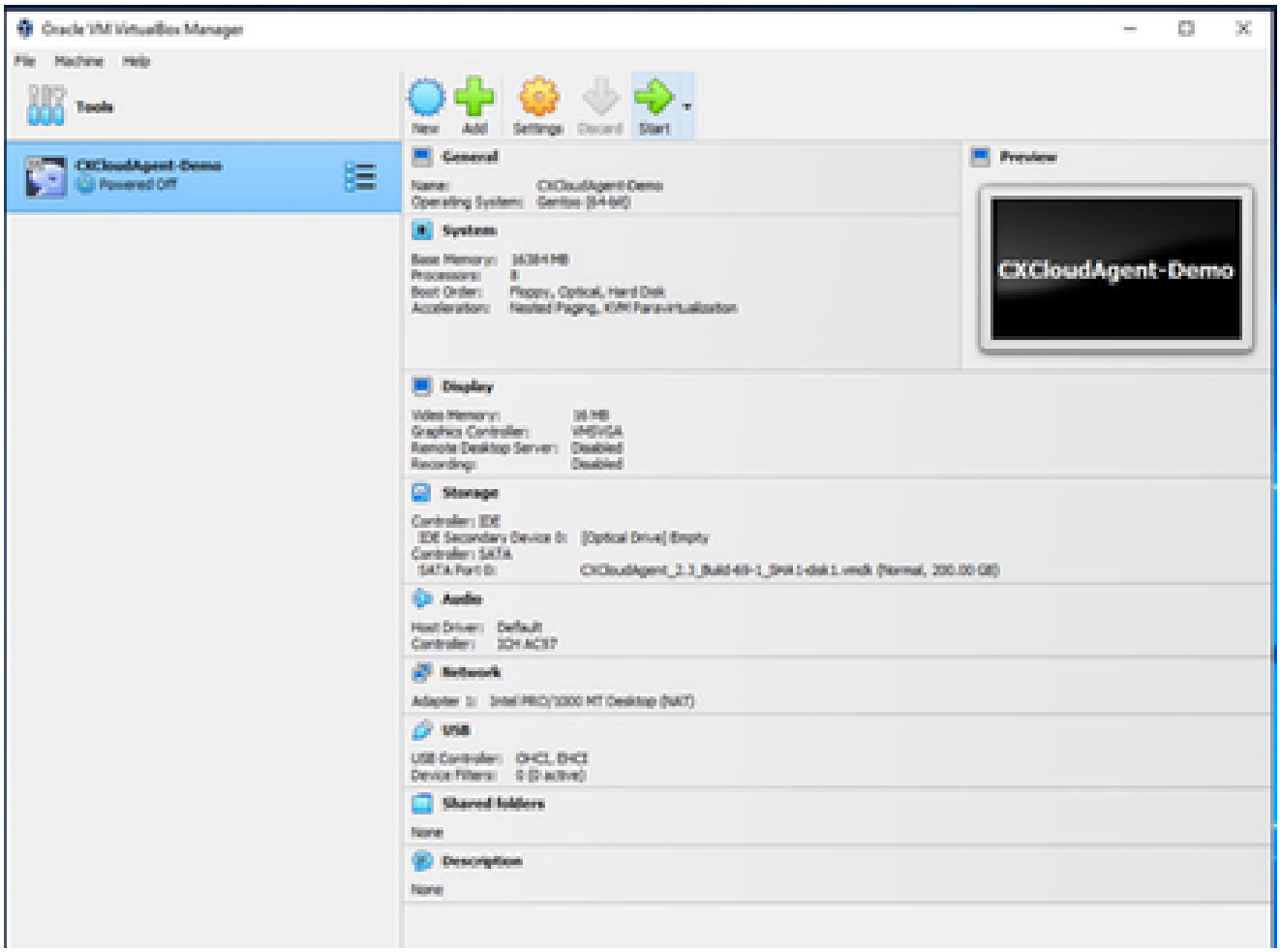
Datei auswählen

13. Klicken Sie auf Next (Weiter). Das Fenster Übersicht wird geöffnet.



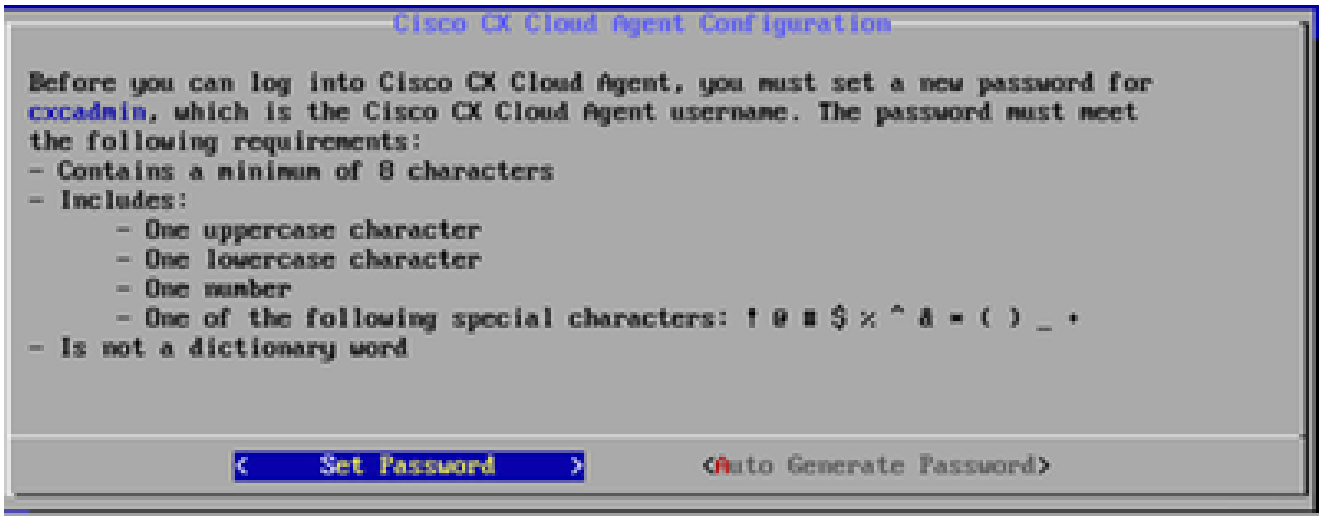
Zusammenfassung

14. Klicken Sie auf Beenden.



Start der VM-Konsole

15. Wählen Sie die bereitgestellte VM aus, und klicken Sie auf Start. Das virtuelle System wird eingeschaltet, und der Konsolenbildschirm wird zur Einrichtung angezeigt.



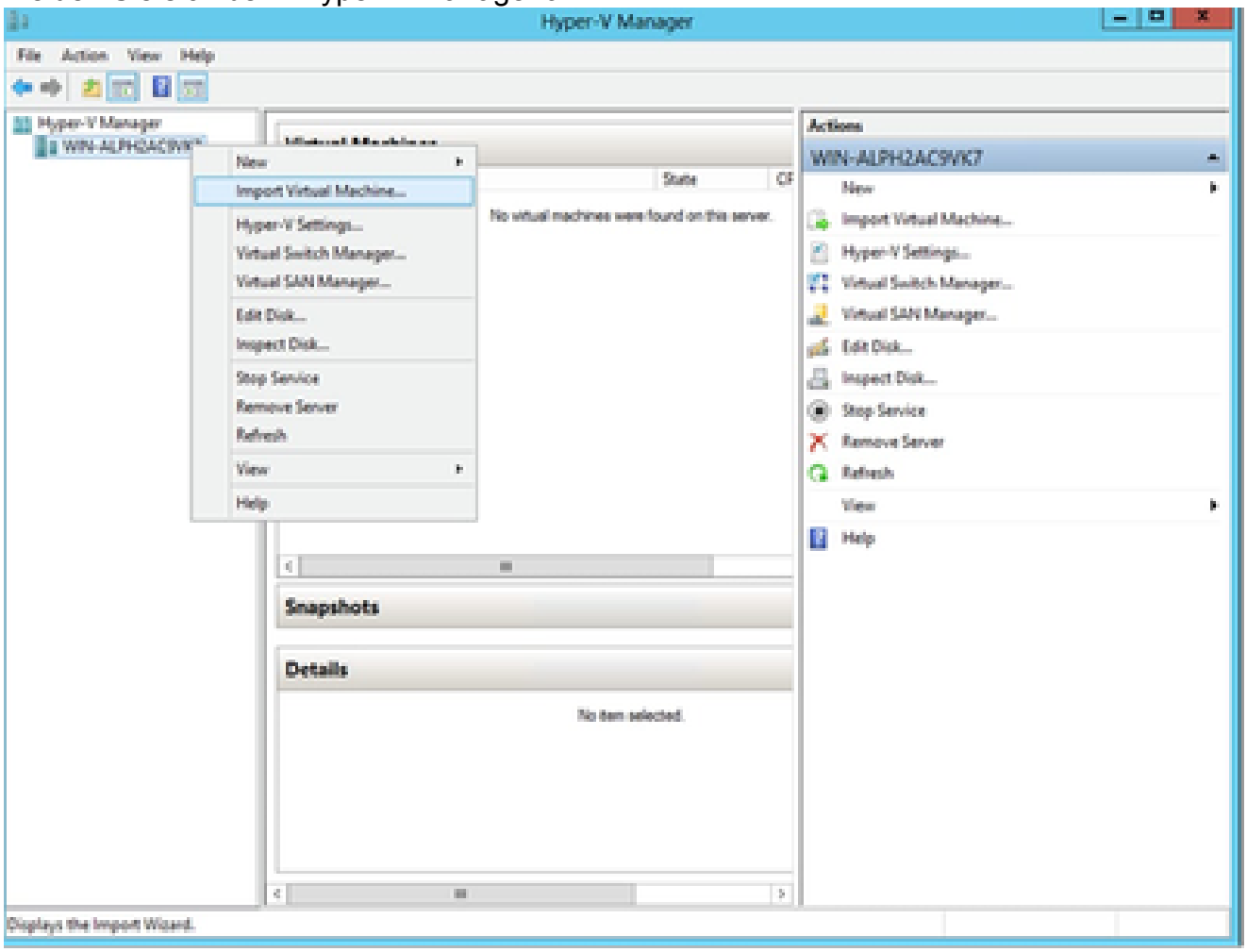
Konsole öffnen

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

Installation von Microsoft Hyper-V

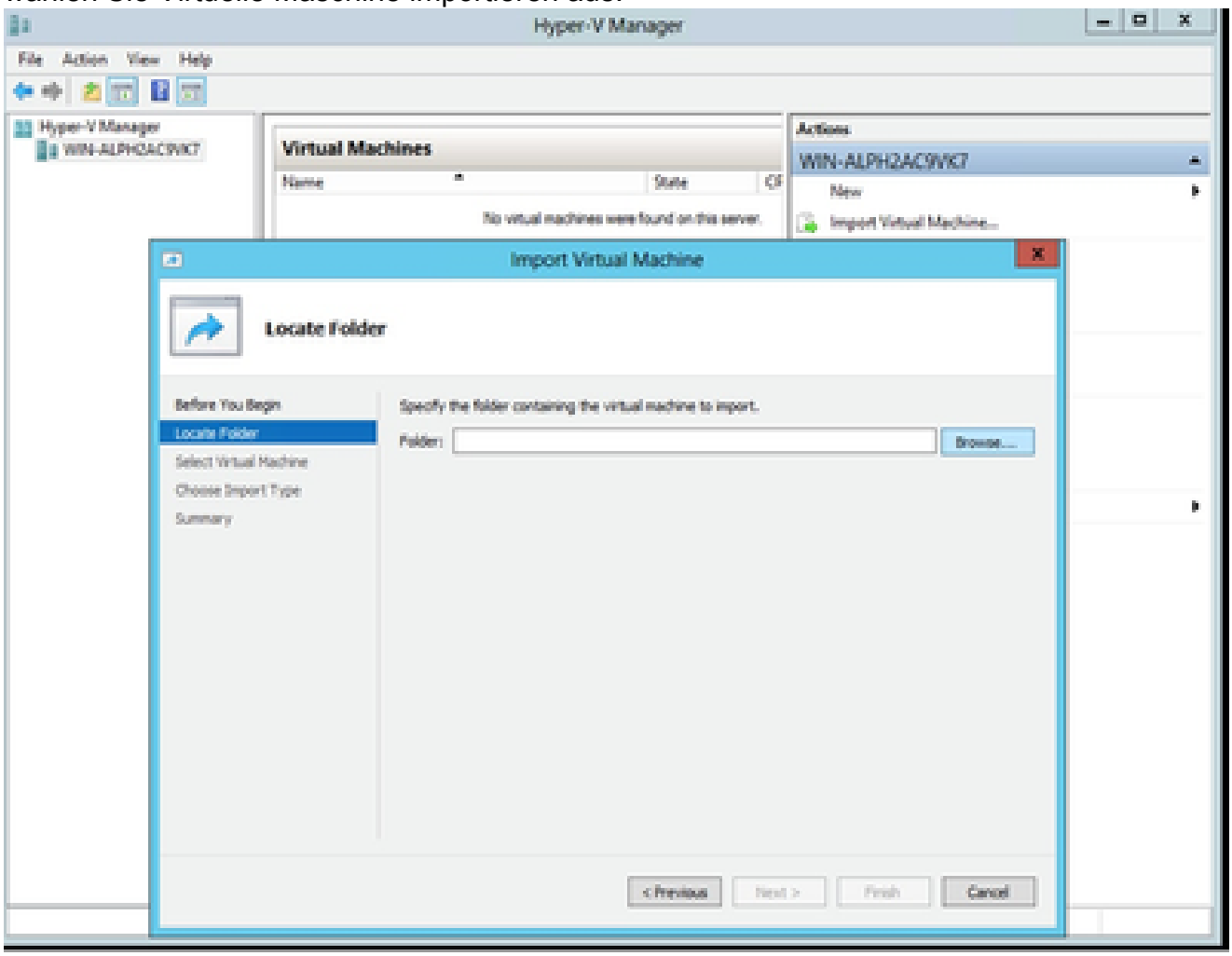
Dieser Client stellt CX Agent OVA über die Microsoft Hyper-V-Installation bereit.

1. Melden Sie sich beim Hyper-V Manager an.



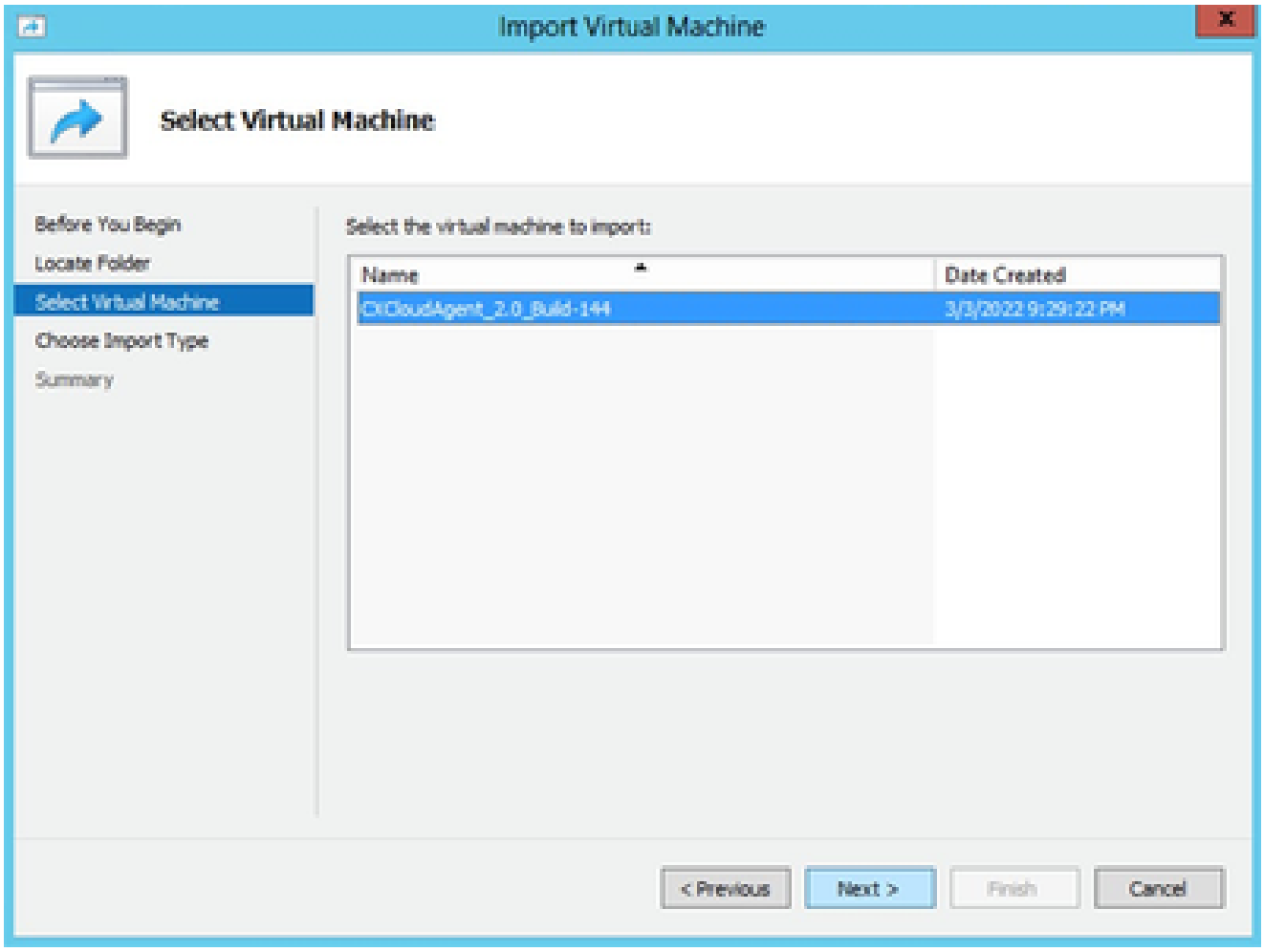
Hyper-V-Manager

2. Wählen Sie Ziel-VM, klicken Sie mit der rechten Maustaste, um das Menü zu öffnen, und wählen Sie Virtuelle Maschine importieren aus.



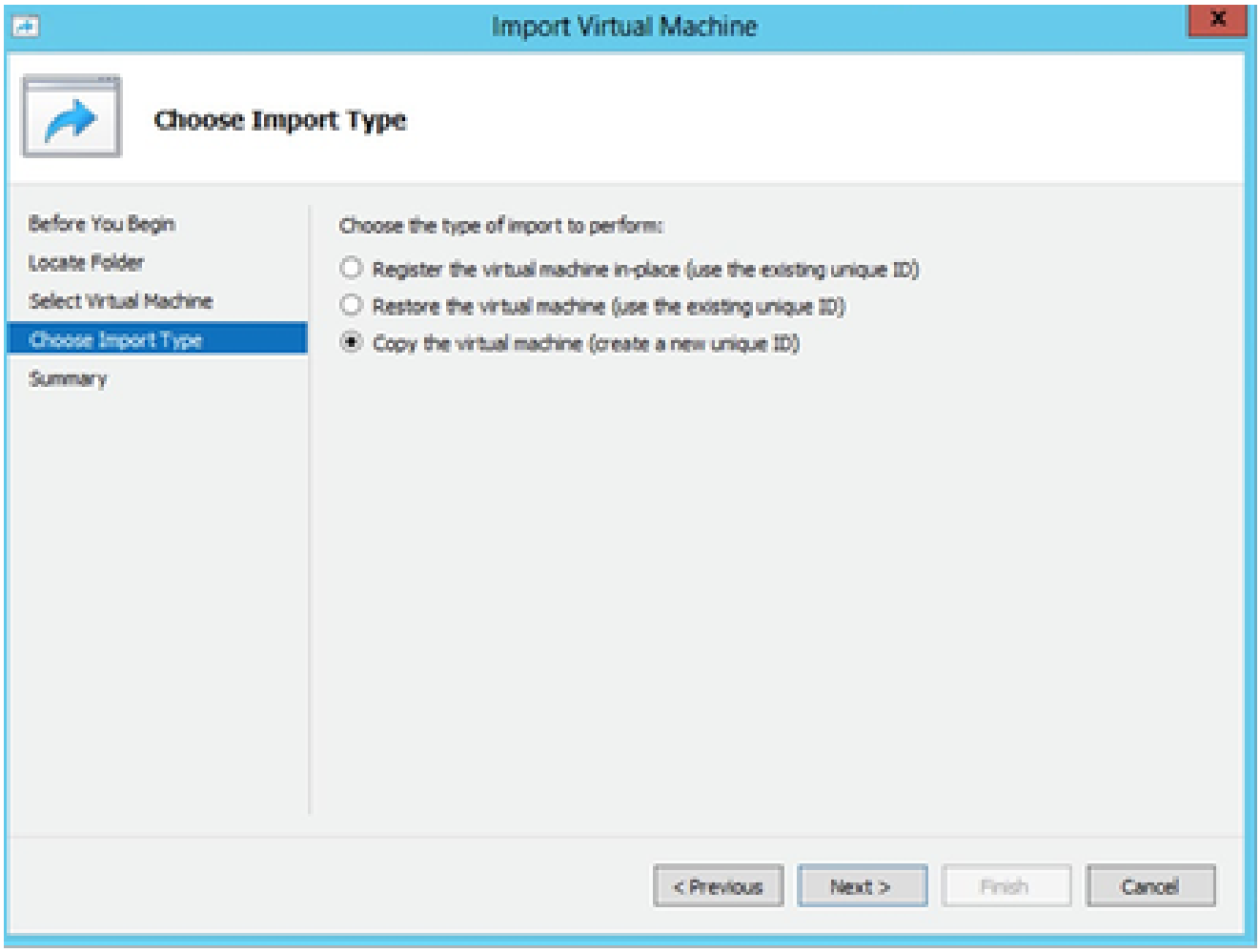
Zu importierender Ordner

3. Navigieren Sie zum Download-Ordner, wählen Sie ihn aus, und klicken Sie auf Weiter.



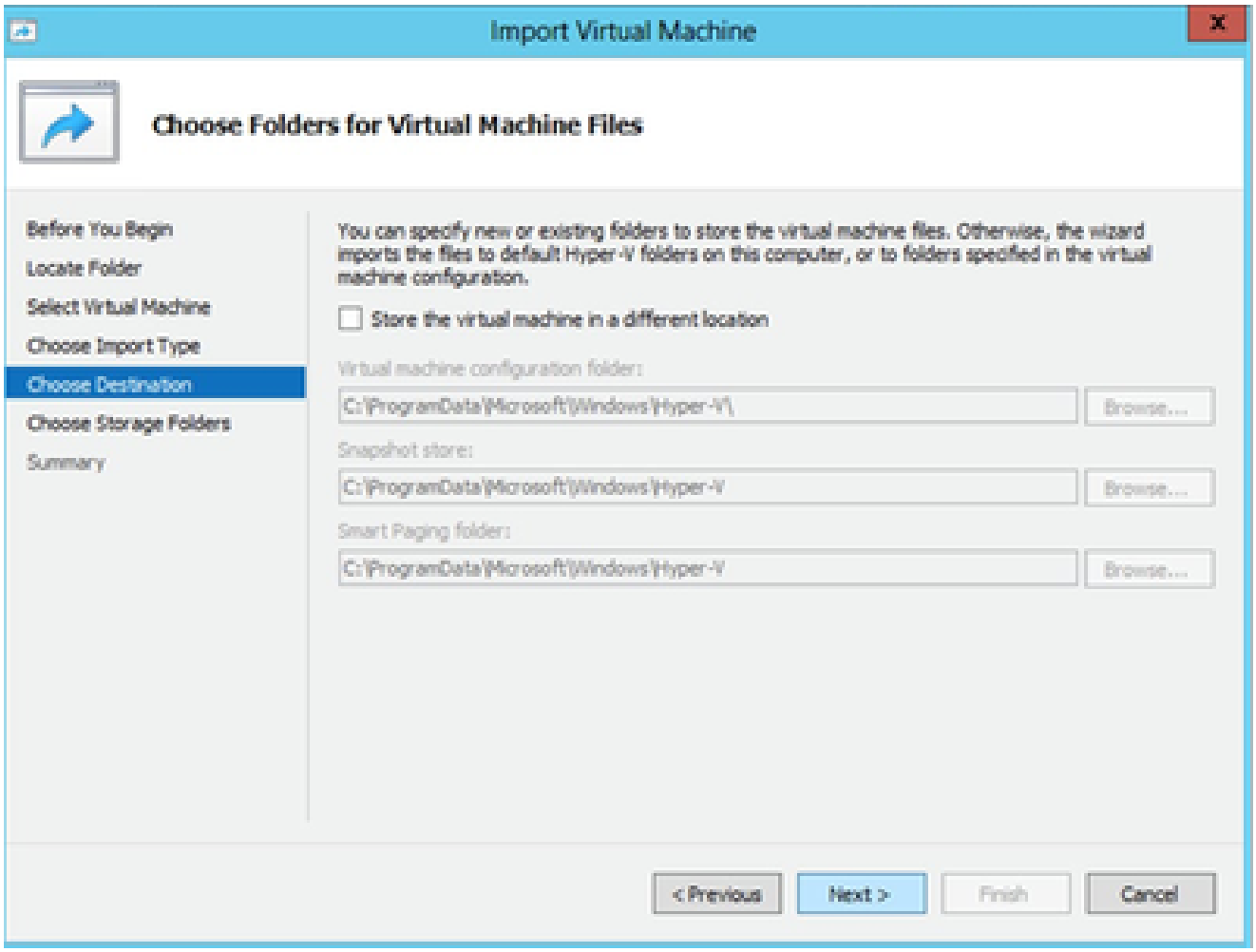
VM auswählen

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



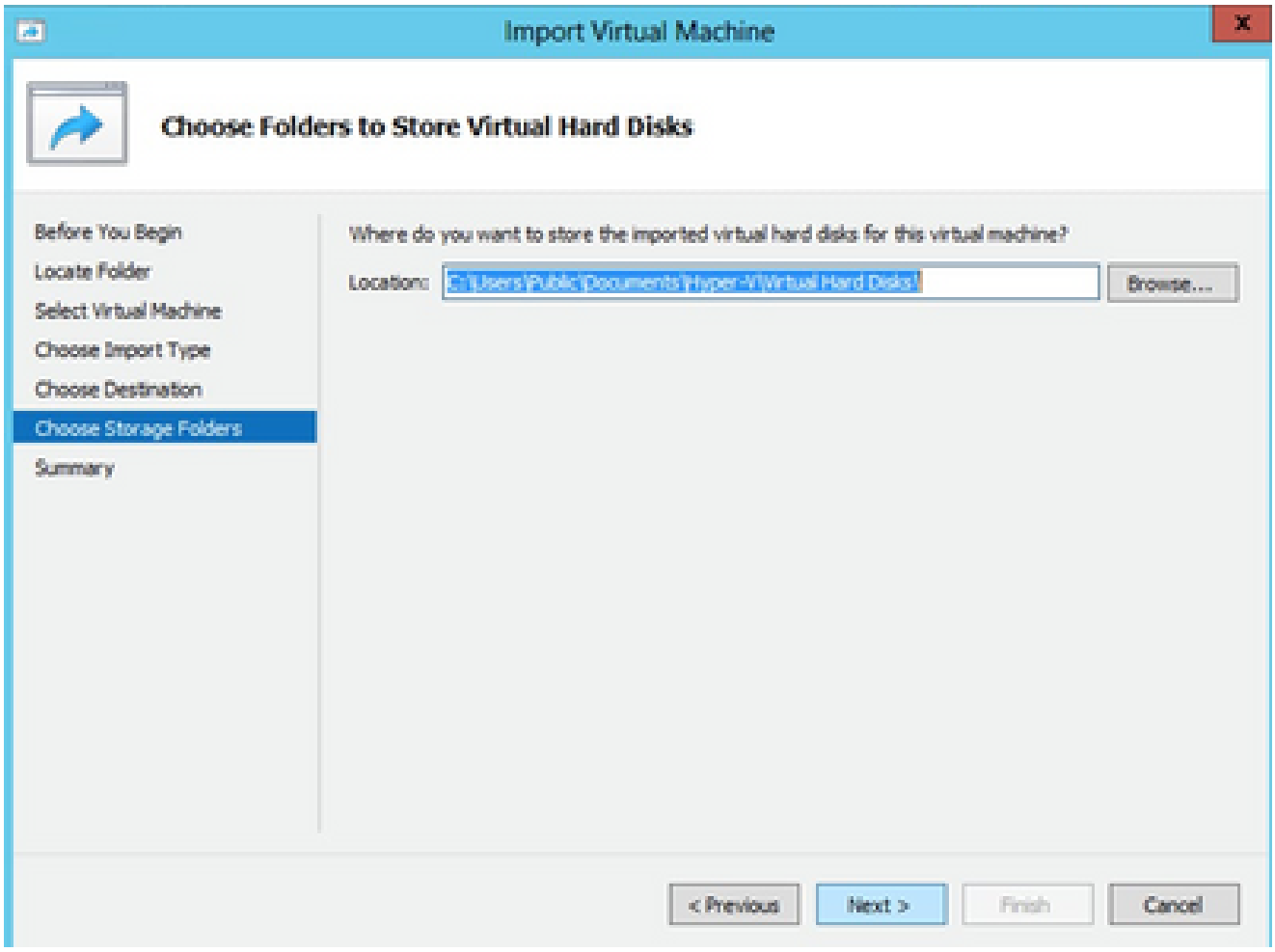
Importtyp

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



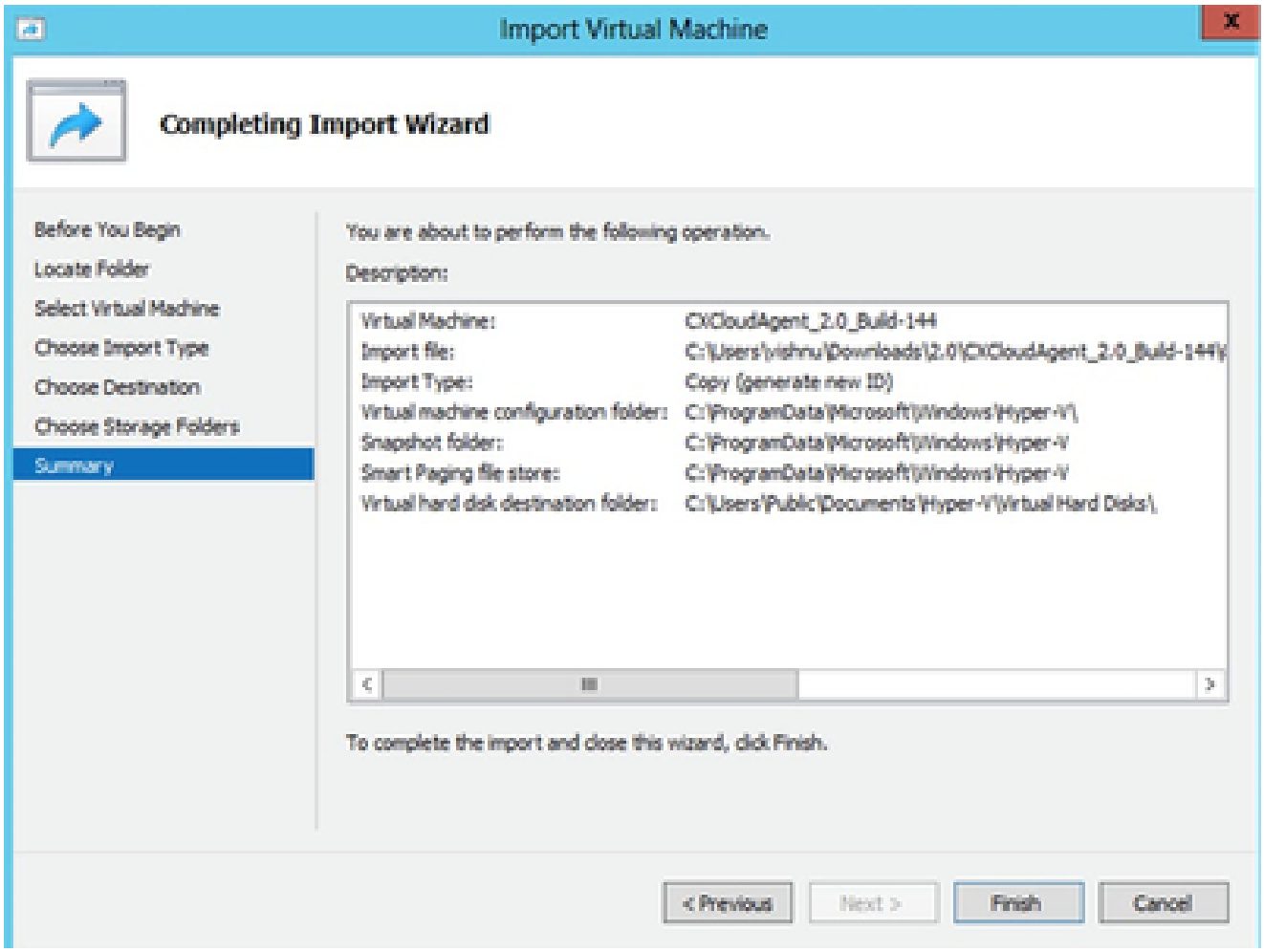
Ordner für Dateien virtueller Systeme auswählen

6. Klicken Sie auf "Durchsuchen", um den Ordner für VM-Dateien auszuwählen. Cisco empfiehlt die Verwendung der Standardpfade.
7. Klicken Sie auf Next (Weiter).



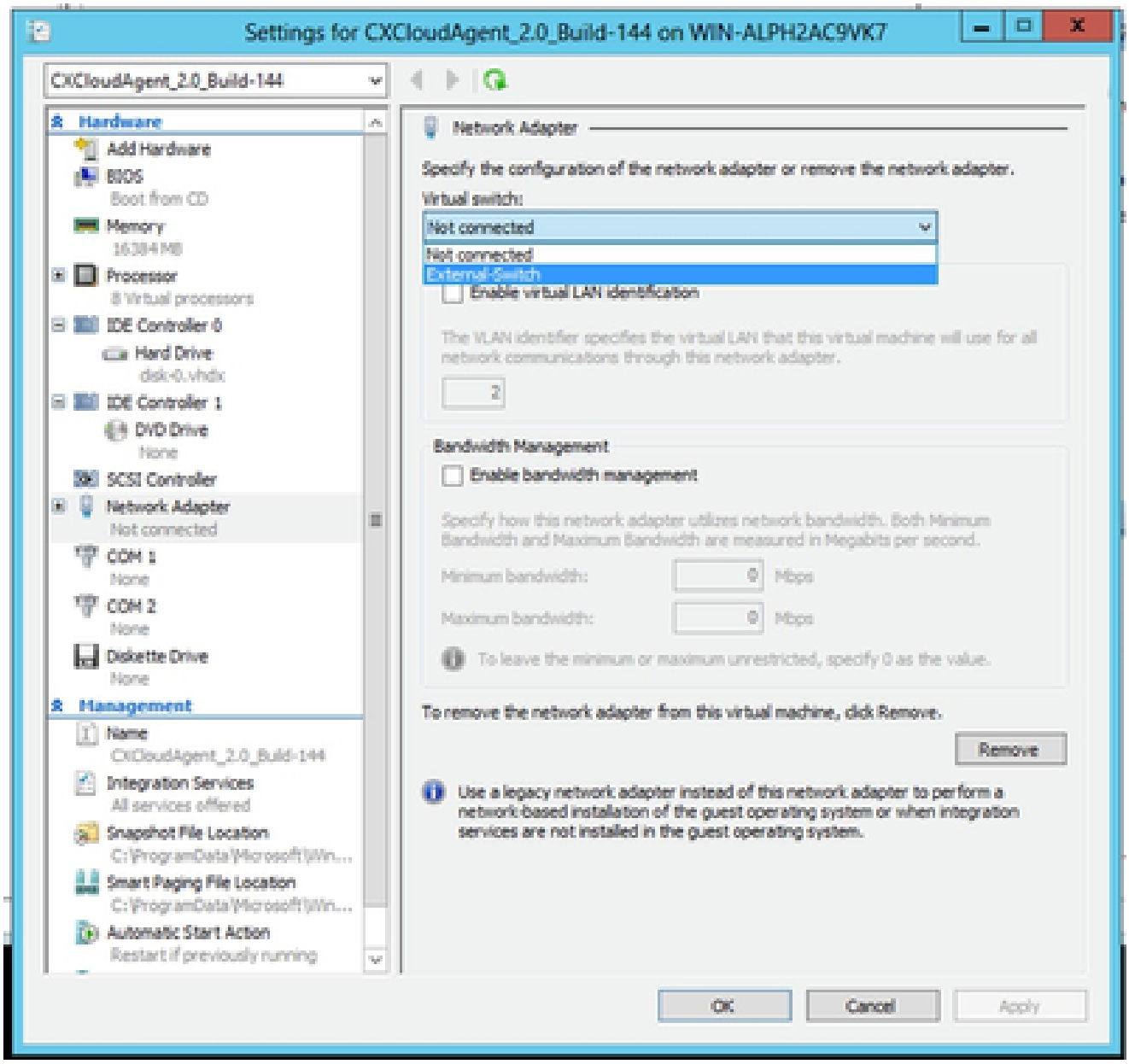
Ordner zum Speichern der virtuellen Festplatten

8. Durchsuchen Sie den Ordner, in dem die VM-Festplatten gespeichert werden sollen, und wählen Sie ihn aus. Cisco empfiehlt die Verwendung der Standardpfade.
9. Klicken Sie auf Next (Weiter). Die VM-Übersicht wird angezeigt.



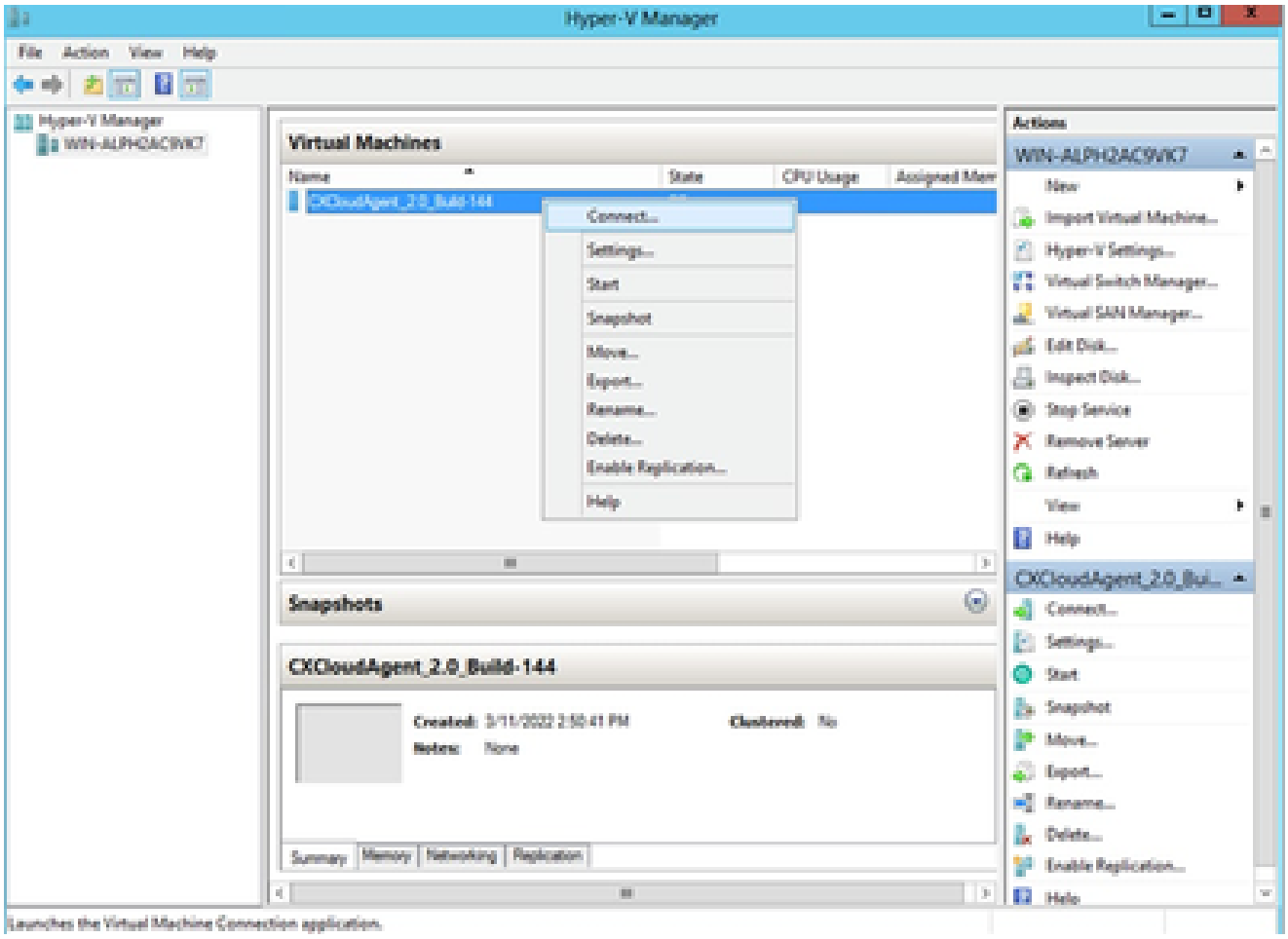
Zusammenfassung

10. Überprüfen Sie alle Eingaben, und klicken Sie auf Fertig stellen.
11. Sobald der Import erfolgreich abgeschlossen ist, wird eine neue VM auf Hyper-V erstellt. Öffnen Sie die VM-Einstellungen.



Virtueller Switch

12. Wählen Sie den Netzwerkadapter aus dem linken Bereich und dann den verfügbaren virtuellen Switch aus der Dropdown-Liste aus.

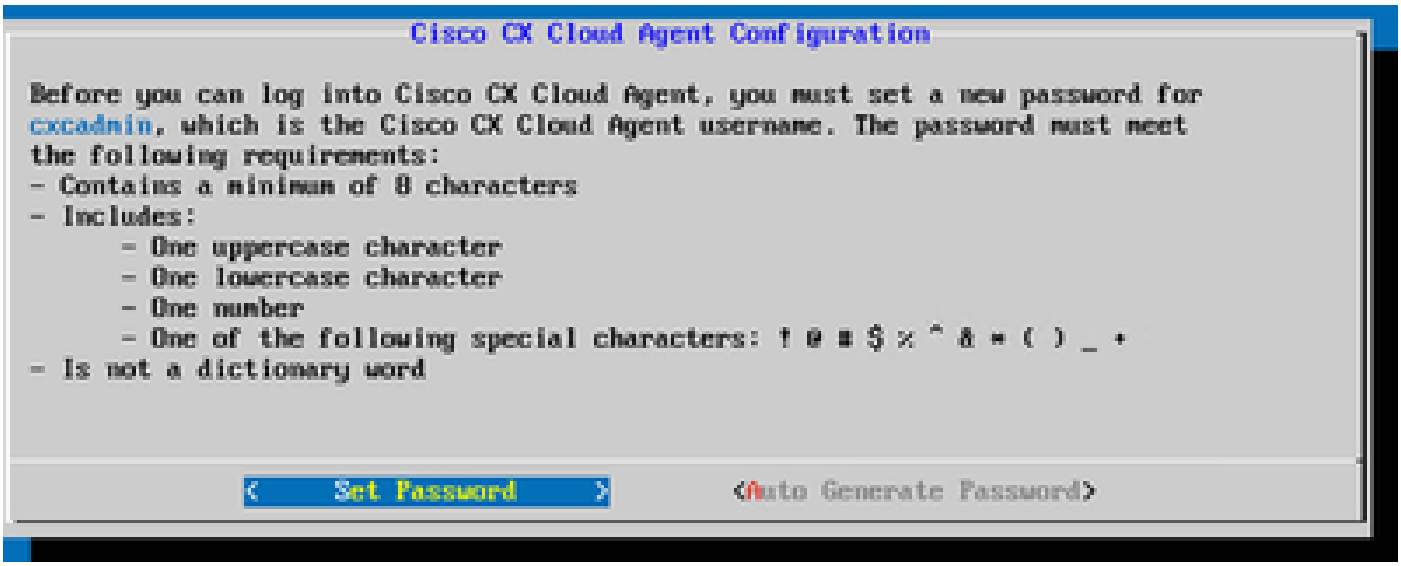


VM wird gestartet

13. Wählen Sie Verbinden, um das virtuelle System zu starten.
14. Navigieren Sie zu Network Configuration, um mit den nächsten Schritten fortzufahren.

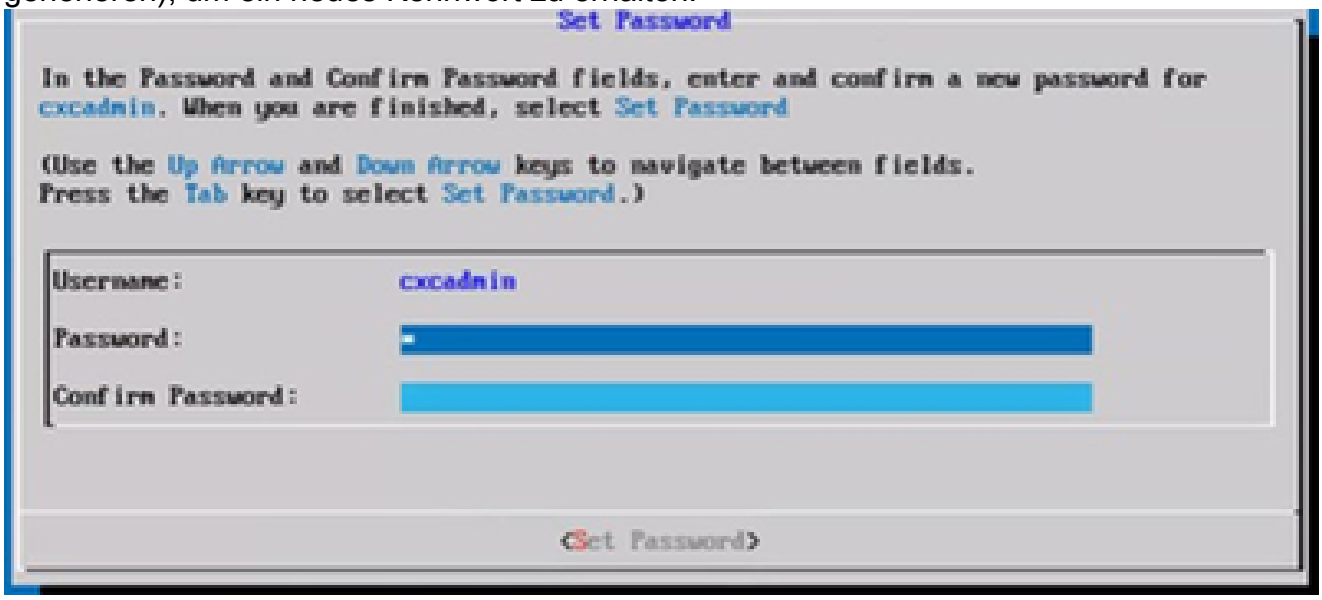
Netzwerkkonfiguration

So legen Sie das CX Cloud Agent-Kennwort für den cxcadmin-Benutzernamen fest:



Passwort festlegen

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.



Neues Kennwort

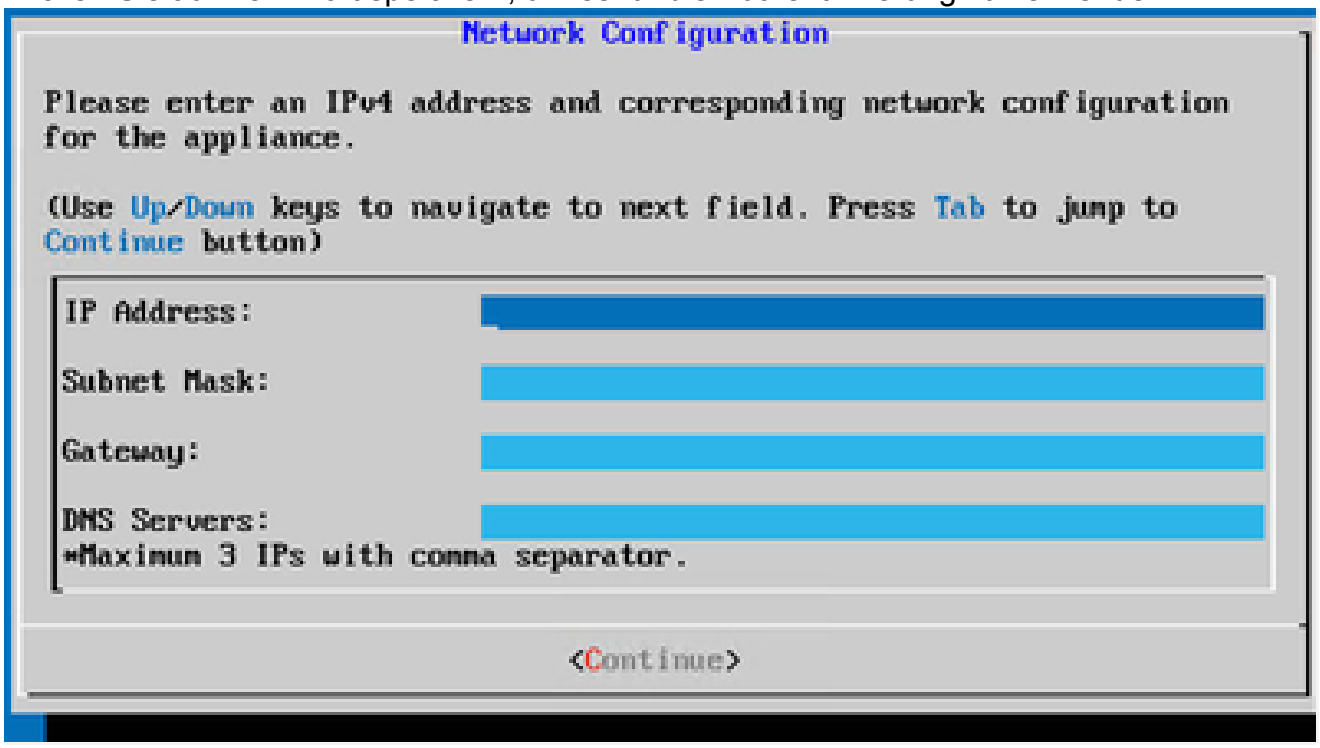
2. Wenn Sie sich für Kennwort festlegen entscheiden, geben Sie das Kennwort für cxcadmin ein und bestätigen Sie es. Klicken Sie auf Kennwort festlegen und fahren Sie mit Schritt 3 fort.
   ODER

   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)

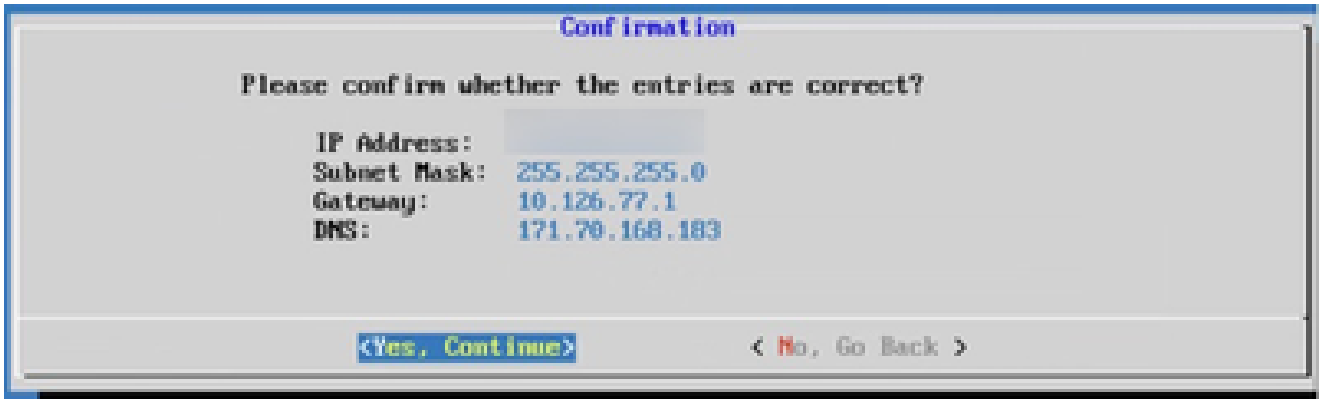
Passwort speichern

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



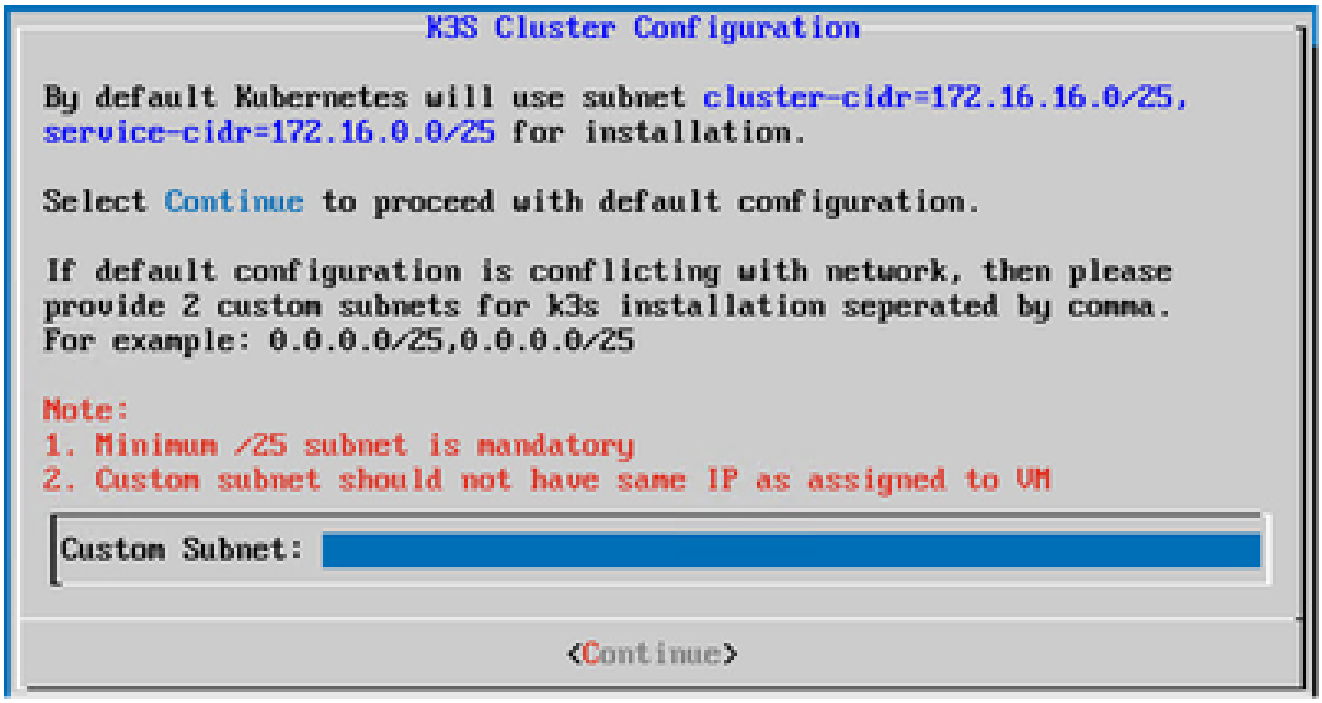
Netzwerkkonfiguration

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



Bestätigung

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

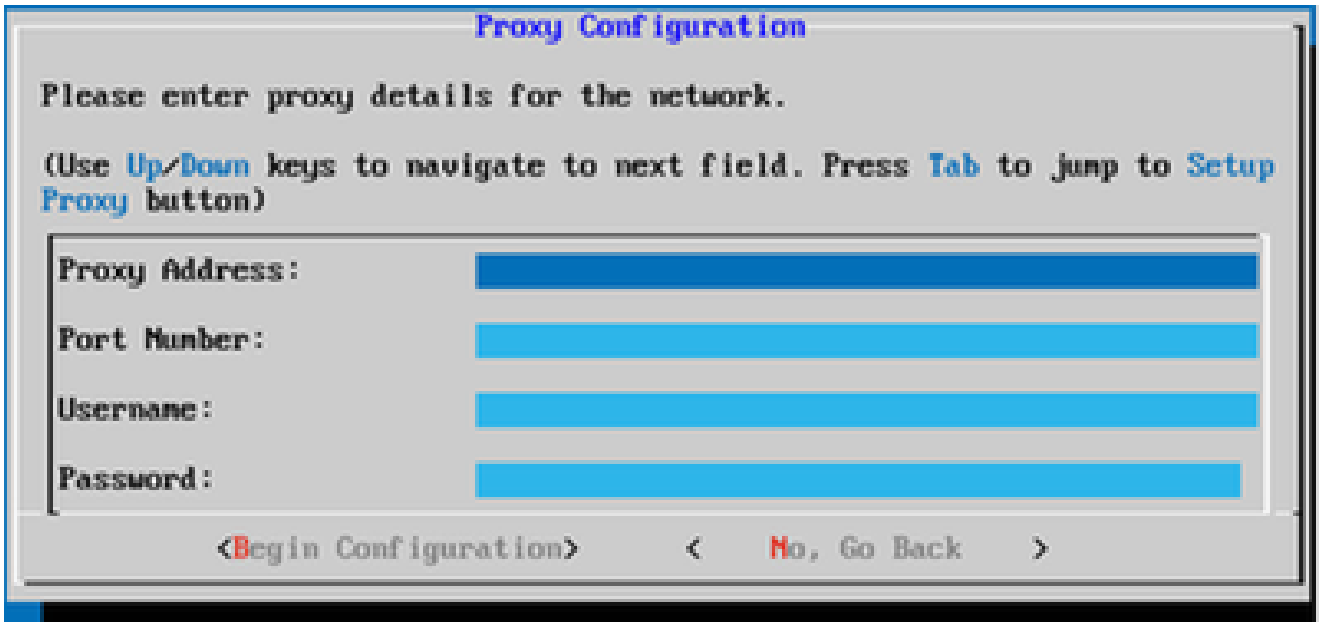


Benutzerdefiniertes Subnetz

6. Geben Sie die benutzerdefinierte Subnetz-IP für die K3S-Cluster-Konfiguration ein (wählen Sie ein anderes benutzerdefiniertes Subnetz aus, wenn das Standard-Subnetz eines Kunden mit dem Netzwerk des Kunden in Konflikt steht).
7. Klicken Sie auf Continue (Weiter).

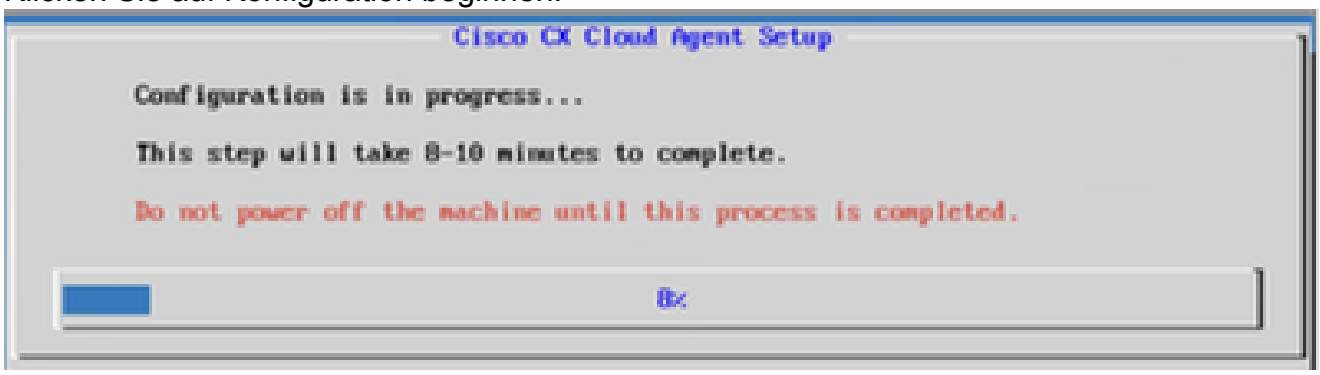
Proxy-Einrichtung

8. Klicken Sie auf Ja, Proxy einrichten, um die Proxydetails festzulegen, oder klicken Sie auf Nein, Konfiguration fortsetzen, um direkt mit Schritt 11 fortzufahren.

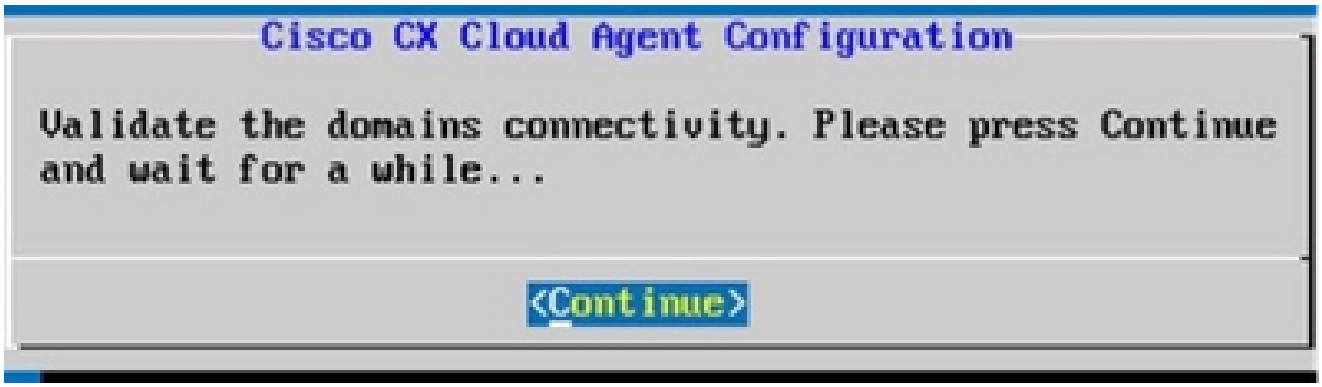


Proxy-Konfiguration

9. Geben Sie die Proxy-Adresse, die Portnummer, den Benutzernamen und das Kennwort ein.
10. Klicken Sie auf Konfiguration beginnen.

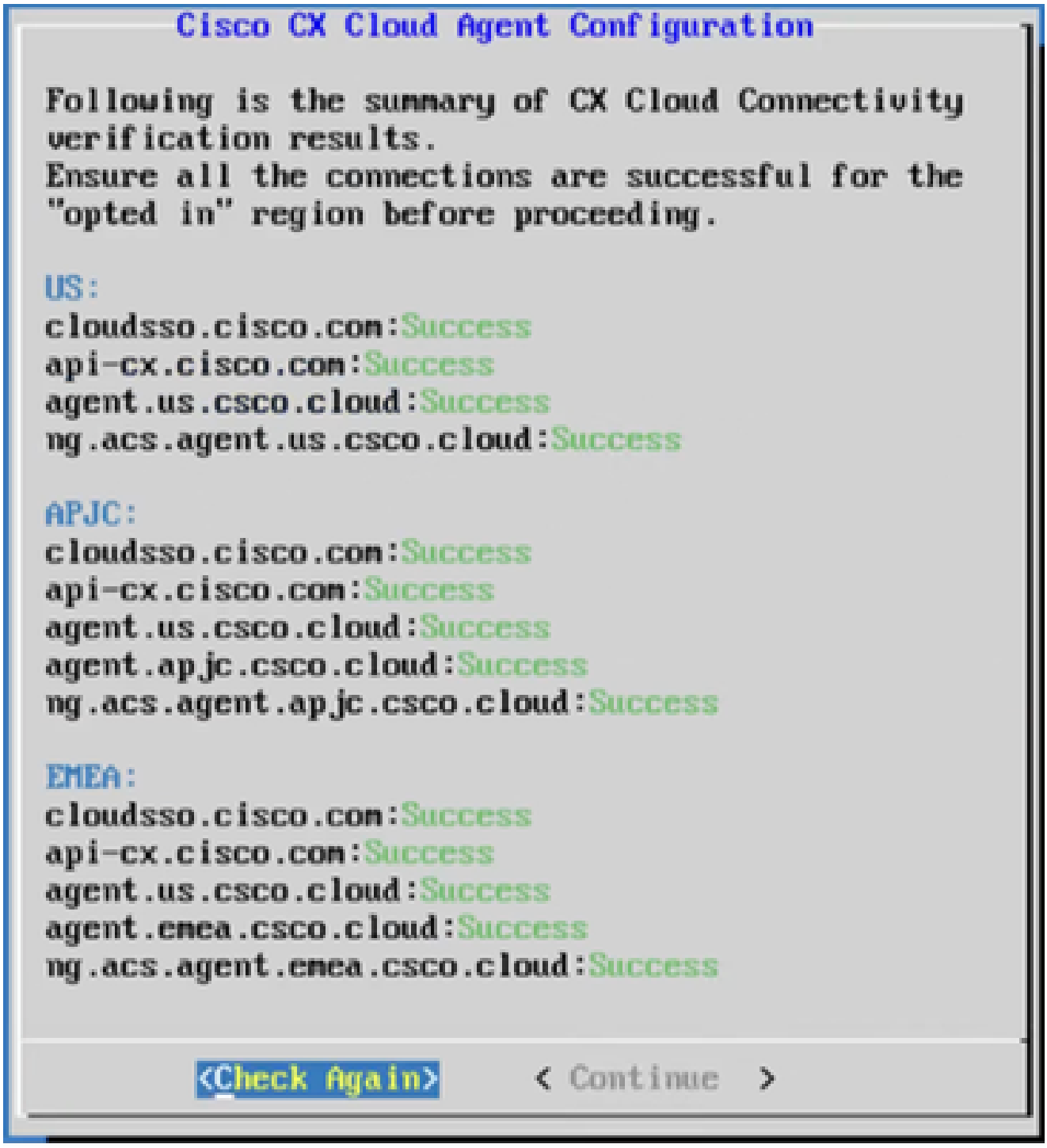


Einrichtung des CX Cloud Agent



CX Cloud Agent-Konfiguration

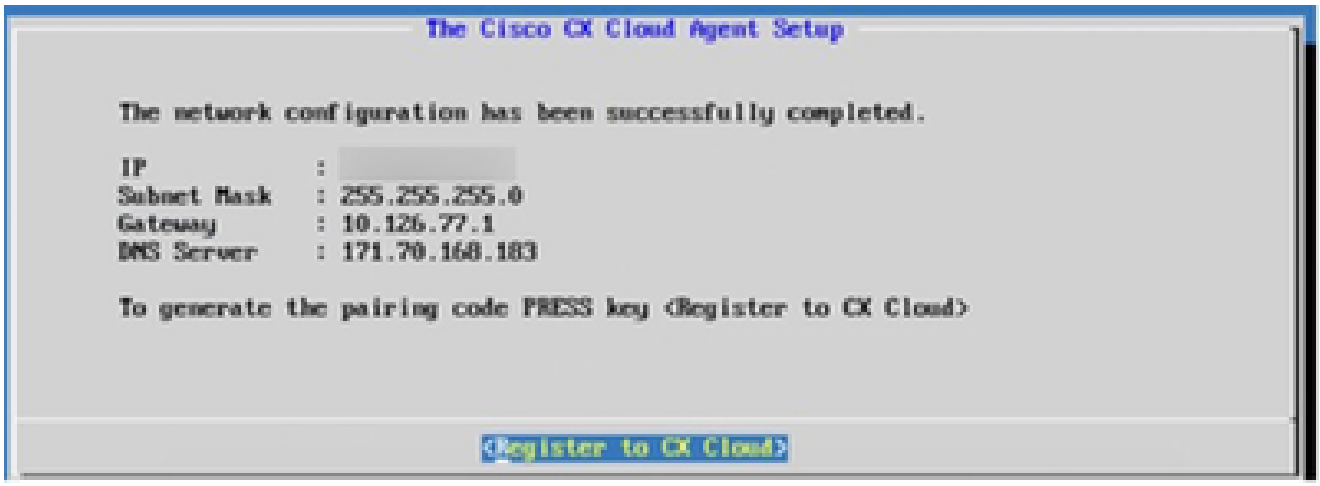
11. Klicken Sie auf Continue (Weiter).



Konfiguration wird fortgesetzt

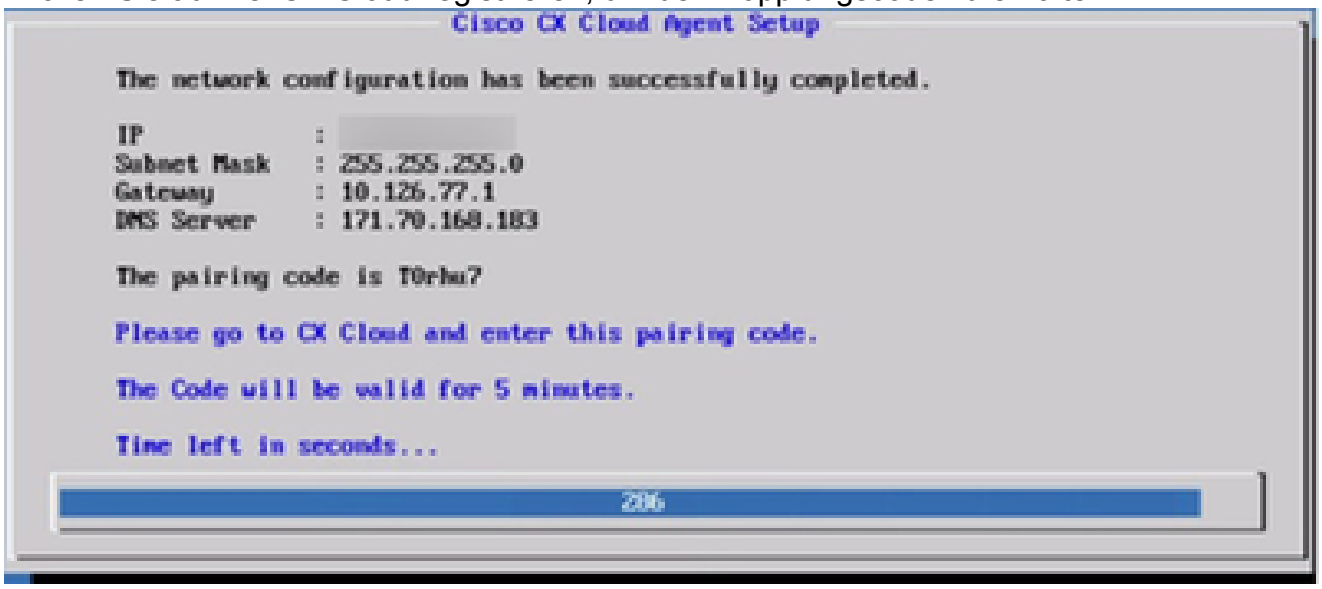
12. Klicken Sie auf Continue (Weiter), um mit der Konfiguration fortzufahren, damit die Domäne erreicht werden kann. Die Konfiguration kann einige Minuten in Anspruch nehmen.

Anmerkung: 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.



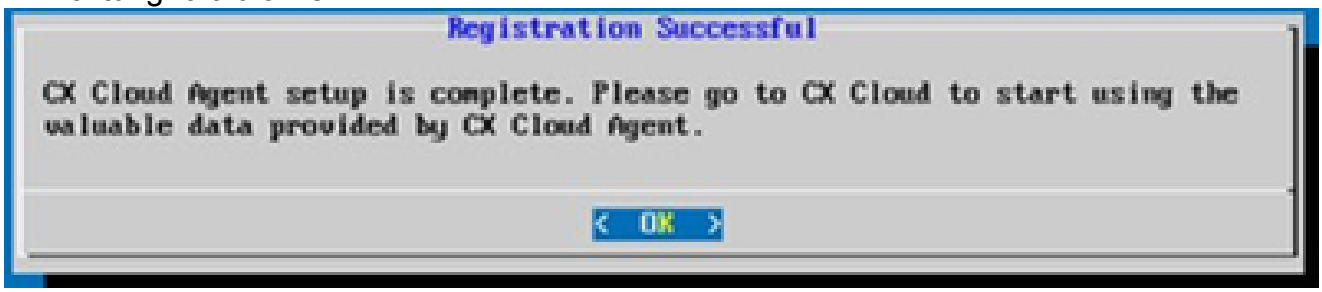
Bei CX Cloud registrieren

13. Klicken Sie auf Bei CX Cloud registrieren, um den Kopplungscode zu erhalten.



Kopplungscode

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



Registrierung erfolgreich

Anmerkung: Wenn der Kopplungscode abläuft, klicken Sie auf Bei CX Cloud registrieren, um einen neuen Kopplungscode zu generieren (Schritt 13).

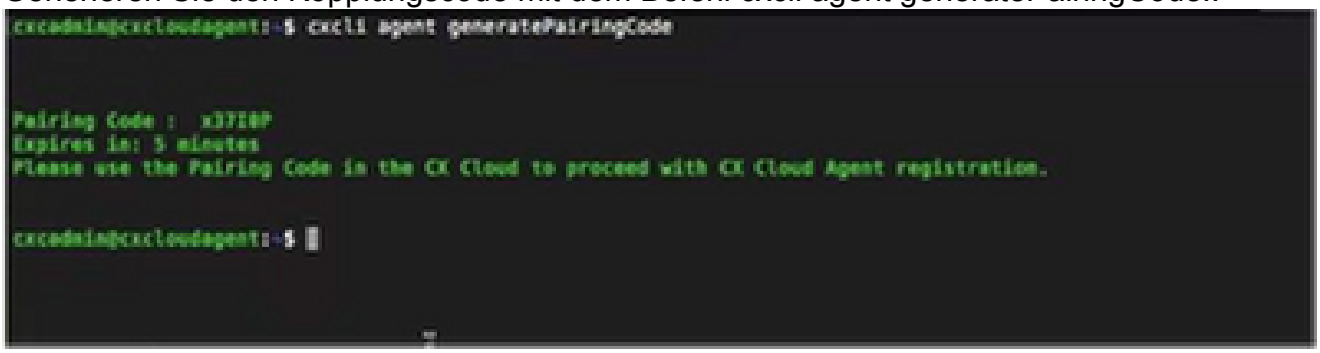
15. Klicken Sie auf OK.

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 den Kopplungscode mit dem Befehl cxcli agent generatePairingCode..



Kopplungscode-CLI generieren

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

Konfigurieren von Geräten für die Weiterleitung von Syslog an den CX Cloud Agent

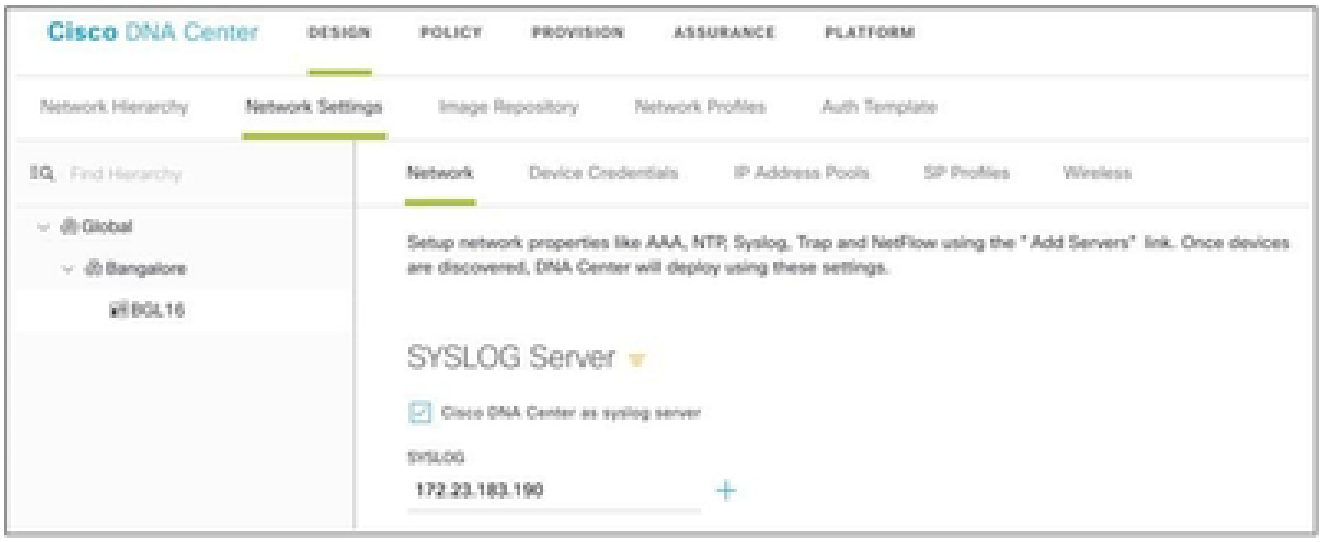
Voraussetzungen

Unterstützte Cisco Catalyst 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 Catalyst Center Virtual Appliance

Syslog-Weiterleitungseinstellung konfigurieren

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

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



Syslog-Server

Anmerkung: Nach der Konfiguration werden alle Geräte, die diesem Standort zugeordnet sind, so konfiguriert, dass sie Syslog mit der für den CX-Agenten kritischen Stufe senden. 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 mit diesem Standort verbundenen Geräte automatisch auf die Standardstufe "Kritisch" gesetzt.

Konfigurieren anderer Ressourcen (direkte Gerätesammlung) zum Weiterleiten von Syslog an den CX-Agenten

Die Geräte müssen so konfiguriert werden, dass sie Syslog-Meldungen an den CX-Agenten senden, damit die Fehlerverwaltungsfunktion der CX Cloud verwendet werden kann.

Anmerkung: Der CX Agent meldet nur Syslog-Informationen von Campus Success Track Level 2-Ressourcen an die CX Cloud. Bei anderen Ressourcen wird die Konfiguration des Syslog-Protokolls für CX Agent verhindert, und die Syslog-Daten werden nicht in CX Cloud gemeldet.

Vorhandene Syslog-Server mit Weiterleitungsfunktion

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

Anmerkung: 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-Agenten

gesendet werden. Spezifische Konfigurationsschritte finden Sie in dieser Dokumentation.

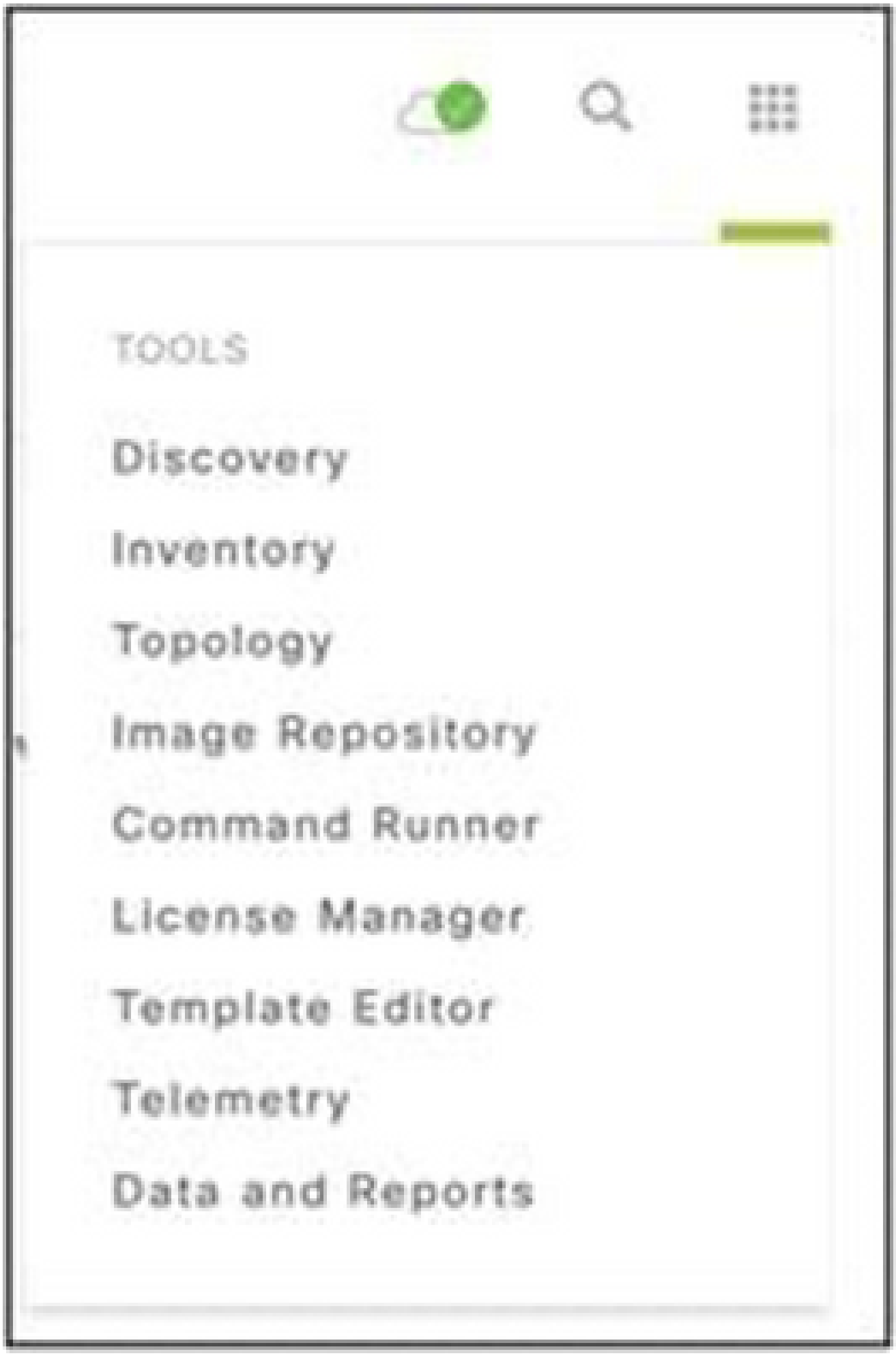
Cisco IOS® XE Konfigurationsleitfaden

Konfigurationsanleitung für den AireOS Wireless Controller

Aktivieren der Syslog-Einstellungen auf Informationsebene für Cisco Catalyst Center

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

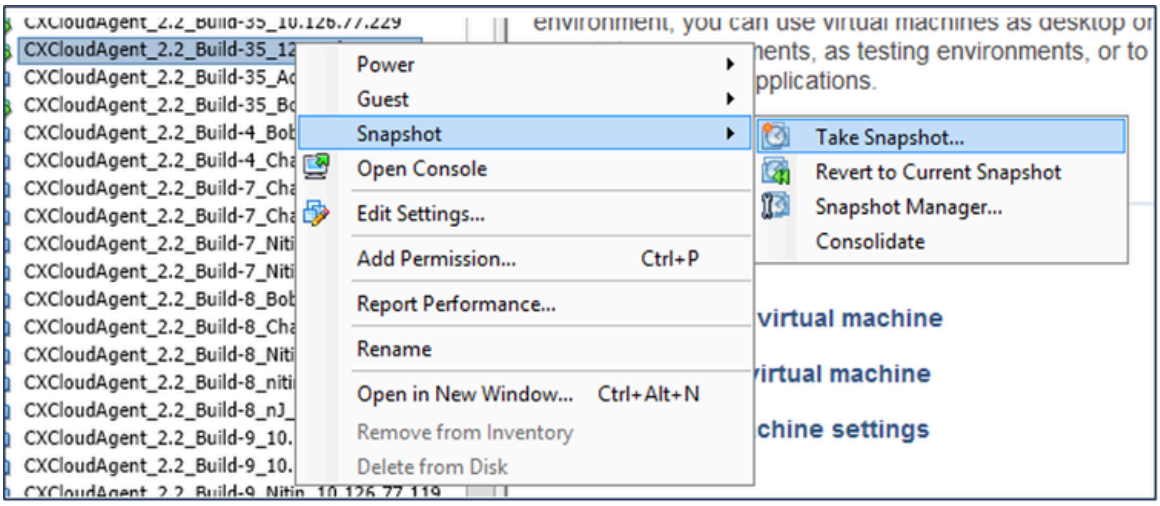
Backup und Wiederherstellung der CX Cloud VM

Es wird empfohlen, den Status und die Daten einer CX 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.

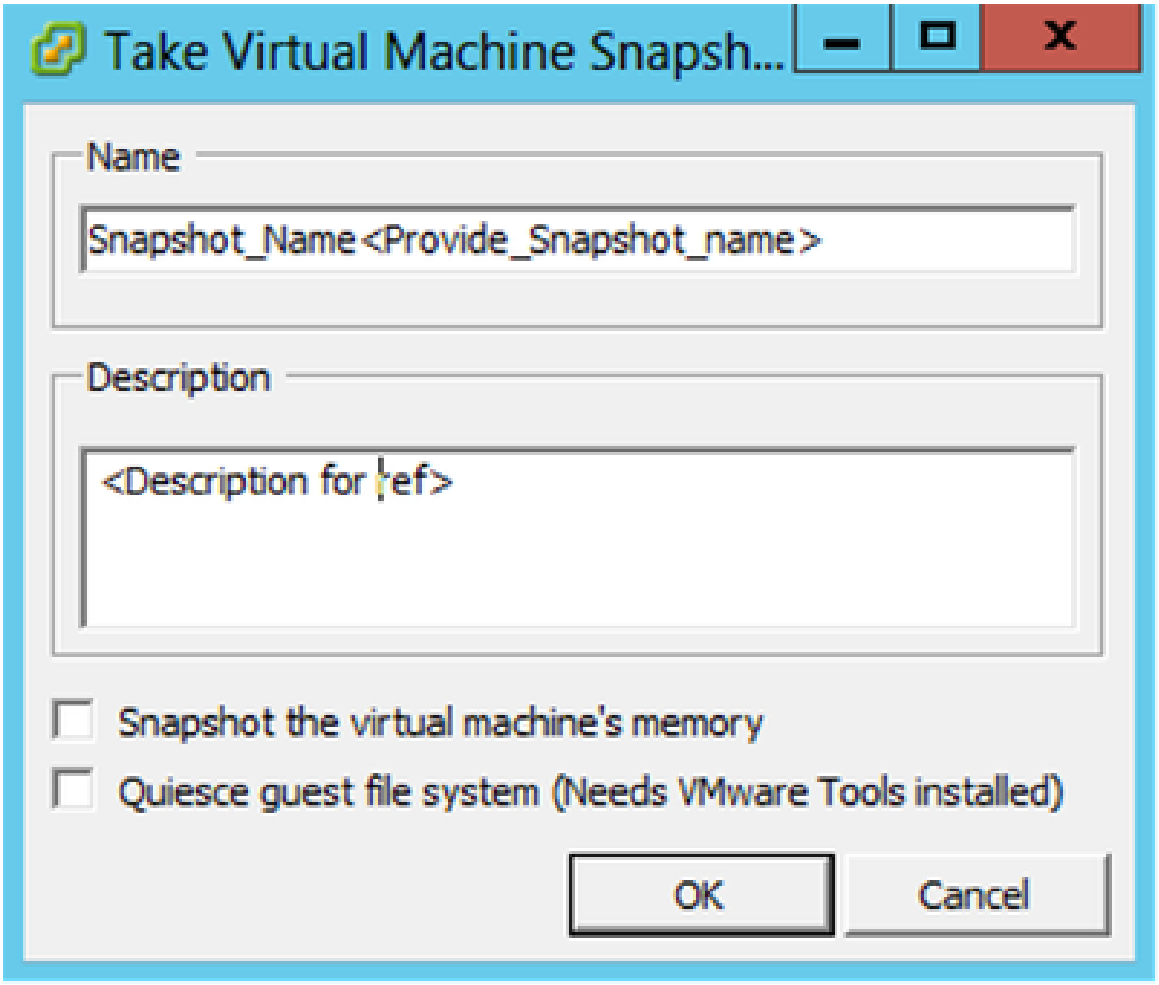
Backup des CX Cloud VM

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



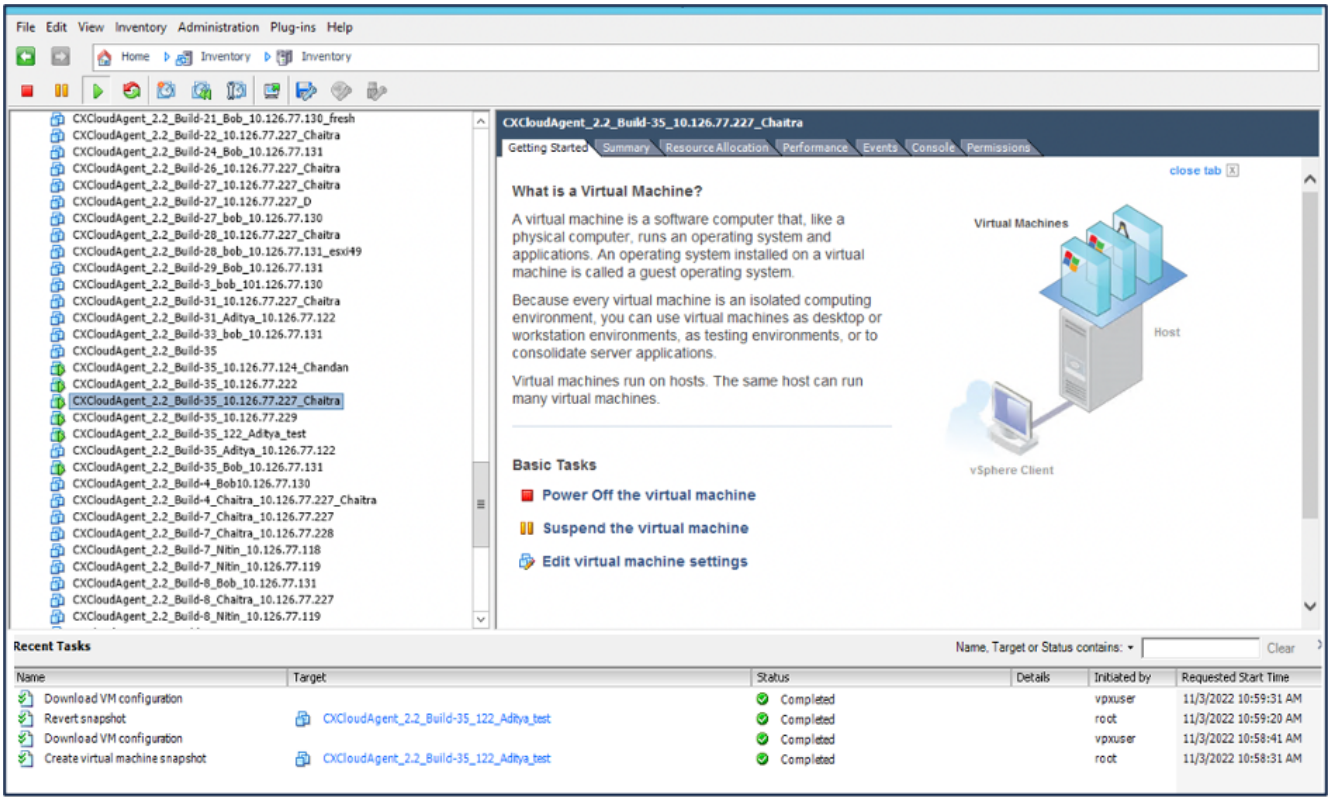
Snapshot des virtuellen Systems erstellen

2. Geben Sie einen Namen und eine Beschreibung ein.

Anmerkung: Vergewissern Sie sich, 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.

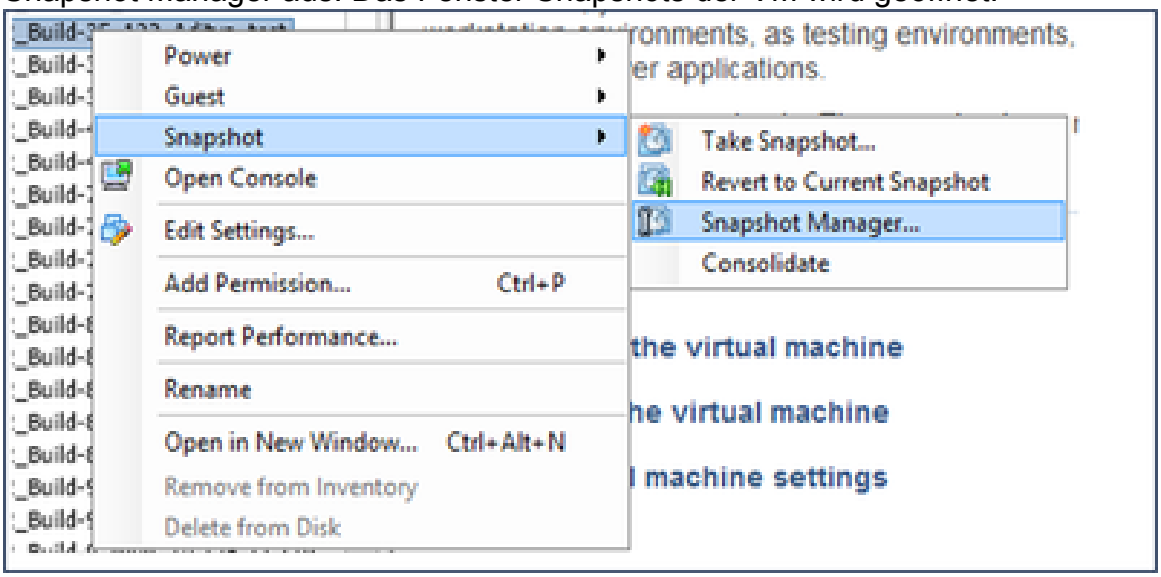


Zuletzt durchgeführte Aufgaben

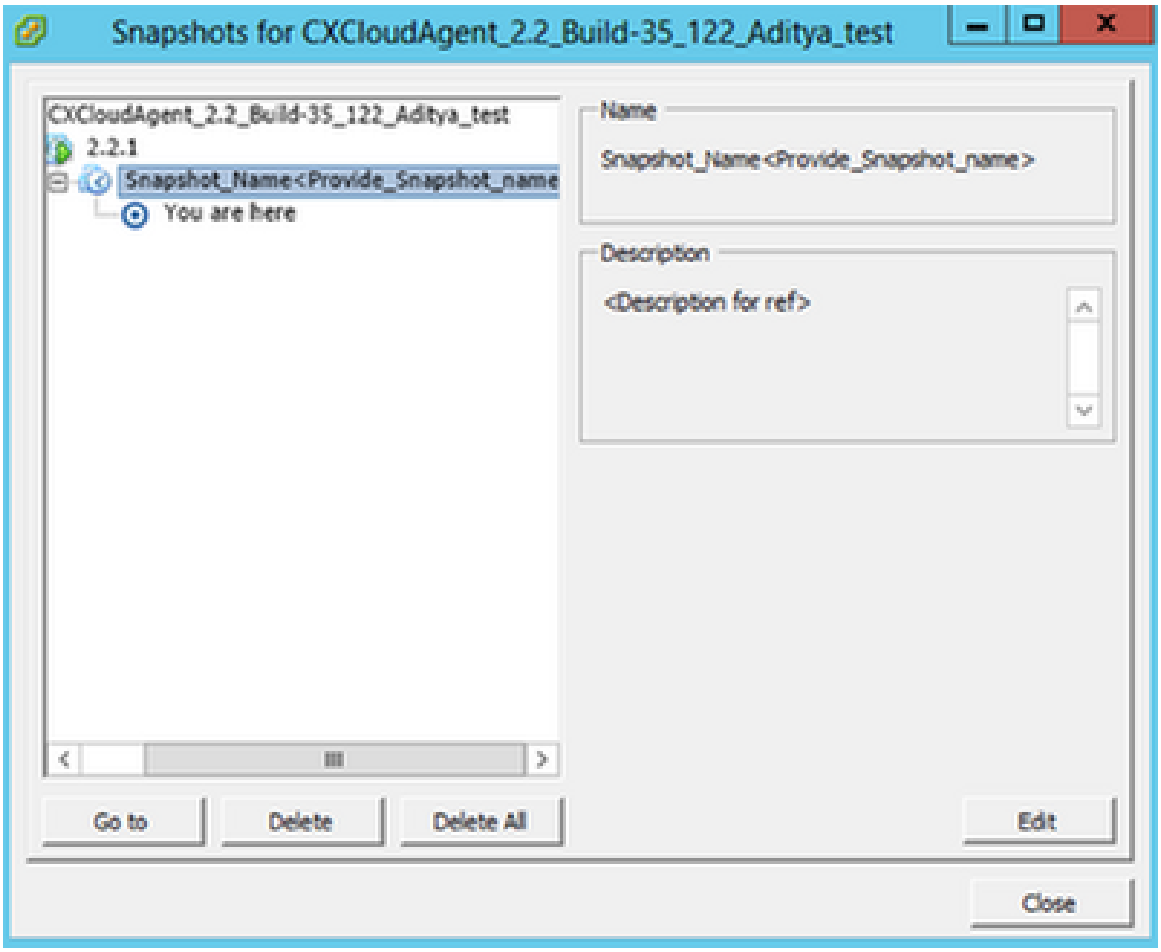
Wiederherstellen des CX Cloud VM

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.

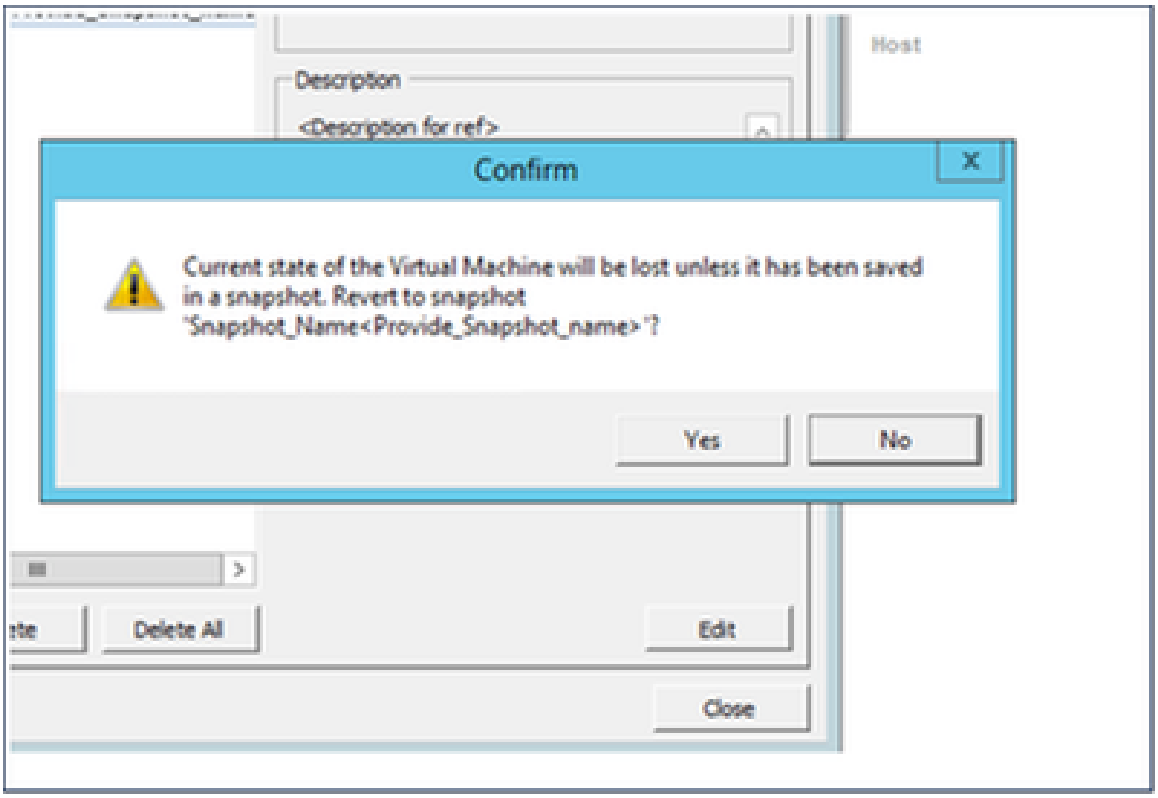


Fenster "VM auswählen"



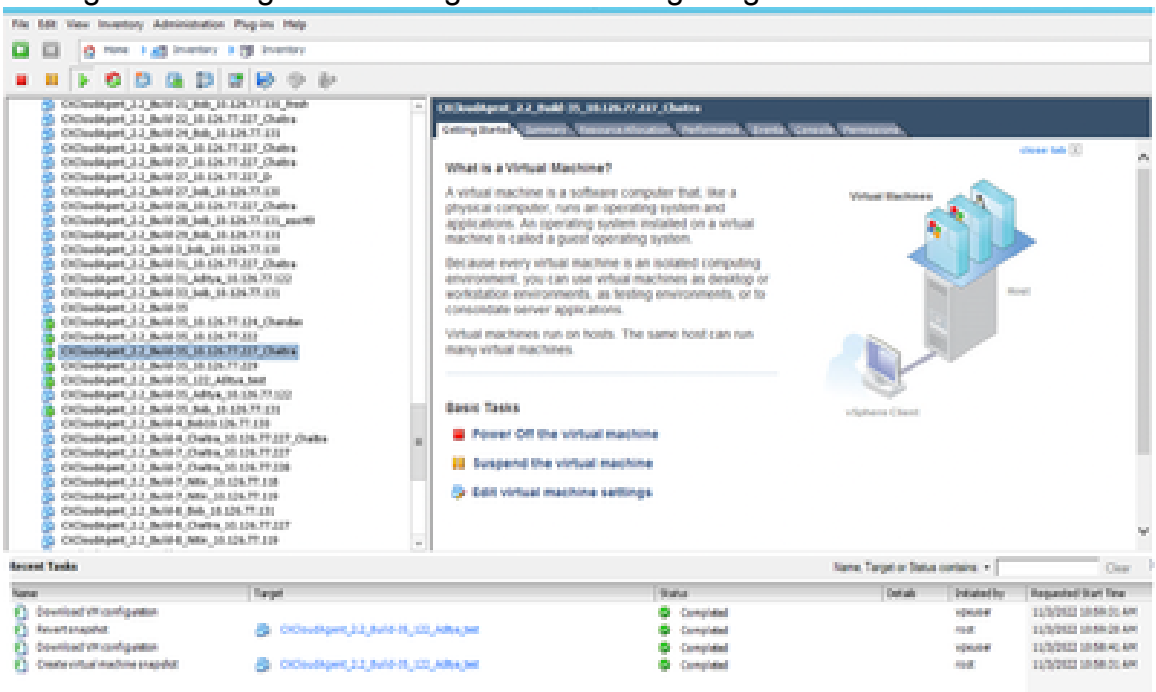
Fenster Snapshots

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



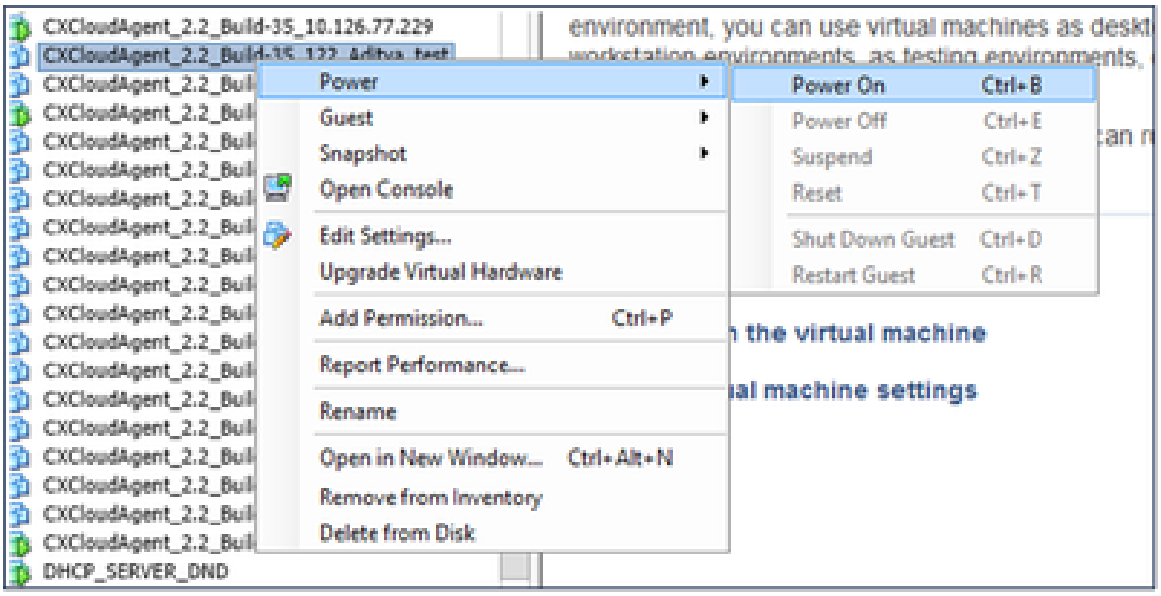
Fenster bestätigen

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 Agent gewährleistet dem Kunden durchgängige Sicherheit. Die Verbindung zwischen CX Cloud und CX 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 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. Die Benutzer sind gezwungen, während der Erstkonfiguration ein Kennwort festzulegen. cxcadmin-Benutzer/Anmeldeinformationen werden verwendet, um sowohl auf die CX Agent-APIs zuzugreifen als auch um eine Verbindung zur Appliance über SSH herzustellen.

cxcadmin-Benutzer haben eingeschränkten Zugriff mit den geringsten Rechten. Das Kennwort "cxcadmin" folgt der Sicherheitsrichtlinie und wird einseitig gehasht. Die Gültigkeitsdauer beträgt 90 Tage. cxcadmin-Benutzer können einen cxcroot-Benutzer mithilfe des Dienstprogramms remoteaccount erstellen. cxcroot-Benutzer können Root-Berechtigungen erhalten.

Netzwerksicherheit

Auf die CX Agent VM kann über SSH mit cxcadmin-Benutzeranmeldeinformationen zugegriffen werden. Eingehende Ports sind auf 22 (SSH), 514 (Syslog) beschränkt.

Authentifizierung

Kennwortbasierte Authentifizierung: Die Appliance unterhält einen einzelnen Benutzer (cxcadmin), über den sich der Benutzer authentifizieren und mit dem CX-Agenten 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 autorisiertes Personal hat Zugriff auf dieses Portal. cxcroot-Benutzer können mit diesem entschlüsselten Kennwort Root-Berechtigungen erlangen. Die Passphrase ist nur zwei Tage lang gültig. Benutzer von cxcadmin müssen das Konto neu erstellen und das Kennwort beim Ablauf des Kennworts im SWIM-Portal erhalten.

Härtung

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

Datensicherheit

Die CX Agent-Appliance speichert keine persönlichen Kundendaten. 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 Catalyst Center-Inventar, die Diagnose-Bridge, Intersight, Compliance Insights, Faults und alle anderen vom CX Agent erfassten Telemetriequellen.

Vertrauliche Informationen aus der Asset-Telemetrie werden vor der Übertragung in die Cloud

maskiert. Der CX Agent maskiert vertrauliche Daten für alle erfassten Ressourcen, die Telemetrie direkt an den CX 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-Agenten 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 Catalyst Center Administratorleitfaden).

Obwohl die Liste der Telemetriekommandos 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 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: Standardbenutzerkonto erstellt; Der Benutzer kann CX Agent-Anwendungsbefehle mit "cxcli" ausführen und hat die geringsten Berechtigungen auf der Appliance. Benutzer cxcroot und das zugehörige verschlüsselte Kennwort werden über den Benutzer cxcadmin generiert. ·cxcroot: cxcadmin kann diesen Benutzer mithilfe des Dienstprogramms remoteaccount erstellen; Der Benutzer kann mit diesem Konto Root-Berechtigungen erhalten.
cxcadmin-Kennwortrichtlinie	·Das Kennwort wird mit SHA-256 unidirektional gehasht und sicher gespeichert.

	· Mindestens acht (8) Zeichen mit drei der folgenden Kategorien: Großbuchstaben, 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: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen. · Fünf fehlgeschlagene Anmeldeversuche sperren die Box 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. · Cisco Catalyst Center-Serveranmeldeinformationen werden verschlüsselt und 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.