Validating CX Cloud Agent Overview v2.2 Prod Problem. Diesen Artikel ignorieren

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
- Hintergrundinformationen
- Zugriff auf kritische Domänen
  - Spezifische Domänen des CX Cloud Agent-Portals
  - Für CX Cloud Agent OVA spezifische Domänen
- Von Cisco DNA Center unterstützte Version
  - Unterstützte Browser
  - Liste der unterstützten Produkte
- Verbinden von Datenquellen
  - Einrichten von CX Cloud Agent
    - Verbindung zwischen CX Cloud Agent und CX Cloud
  - Hinzufügen von Cisco DNA Center als Datenquelle
  - Andere Ressourcen als Datenquellen hinzufügen
    - Überblick
    - Discovery-Protokolle
    - Verbindungsprotokolle
    - Hinzufügen von Geräten mithilfe einer Seed-Datei
    - TelemetrieVerarbeitungsbeschränkungen für Geräte
    - Hinzufügen von Geräten mithilfe einer neuen Seed-Datei
    - Hinzufügen von Geräten mithilfe einer geänderten Seed-Datei
    - Hinzufügen von Geräten mithilfe von IP-Bereichen
    - Bearbeiten von IP-Bereichen
    - Planen von Diagnosescans
- Bereitstellung und Netzwerkkonfiguration
  - OVA-Bereitstellung
    - Installation von ThickClient ESXi 5.5/6.0
    - Installation von WebClient ESXi 6.0
    - WebClient vCenter-Installation
    - Installation von Oracle Virtual Box 5.2.30
    - Installation von Microsoft Hyper-V
  - Netzwerkkonfiguration
  - Alternativer Ansatz zum Generieren von Kopplungscode mithilfe der CLI
  - Konfigurieren von Cisco DNA Center für die Weiterleitung von Syslog an den CX Cloud Agent
    - Voraussetzungen
    - Syslog-Weiterleitungseinstellung konfigurieren
  - Konfigurieren anderer Ressourcen für die Weiterleitung von Syslog an den CX Cloud Agent
    - Vorhandene Syslog-Server mit Weiterleitungsfunktion
    - Bestehende Syslog-Server ohne Weiterleitungsfunktion ODER ohne Syslog-Server

Syslog-Einstellungen auf Informationsebene aktivieren
Backup und Wiederherstellung des CX Cloud VM
Sichern
Wiederherstellen
Sicherheit
Personen- und Gebäudeschutz
Kontosicherheit
Netzwerksicherheit
Authentifizierung
Härtung
Datensicherheit
Datenübertragung
Protokolle und Überwachung
Cisco Telemetrie-Befehle
Sicherheitszusammenfassung

Einleitung

In diesem Dokument wird der Cisco Customer Experience (CX) Cloud Agent beschrieben.

Voraussetzungen

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

Anforderungen

Voraussetzungen für die Bereitstellung:

- Jeder dieser Hypervisoren:
  - VMware ESXi Version 5.5 oder höher
  - Oracle Virtual Box 5.2.30 oder höher
  - Windows-Hypervisor Version 2012 bis 2022
- Der Hypervisor kann ein virtuelles System hosten, das Folgendes erfordert:
  - CPU mit 8 Kernen
  - 16 GB Arbeitsspeicher/RAM
  - 200 GB Festplattenspeicher
- Für Kunden, die ausgewiesene US-Rechenzentren als primäre Datenregion zur Speicherung von CX Cloud-Daten verwenden, muss der CX Cloud Agent in der Lage sein, eine Verbindung zu den hier gezeigten Servern herzustellen. Hierzu muss der FQDN (Fully Qualified Domain Name) verwendet werden und HTTPS auf TCP-Port 443:
  - FQDN: agent.us.csco.cloud
  - FQDN: ng.acs.agent.us.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com

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

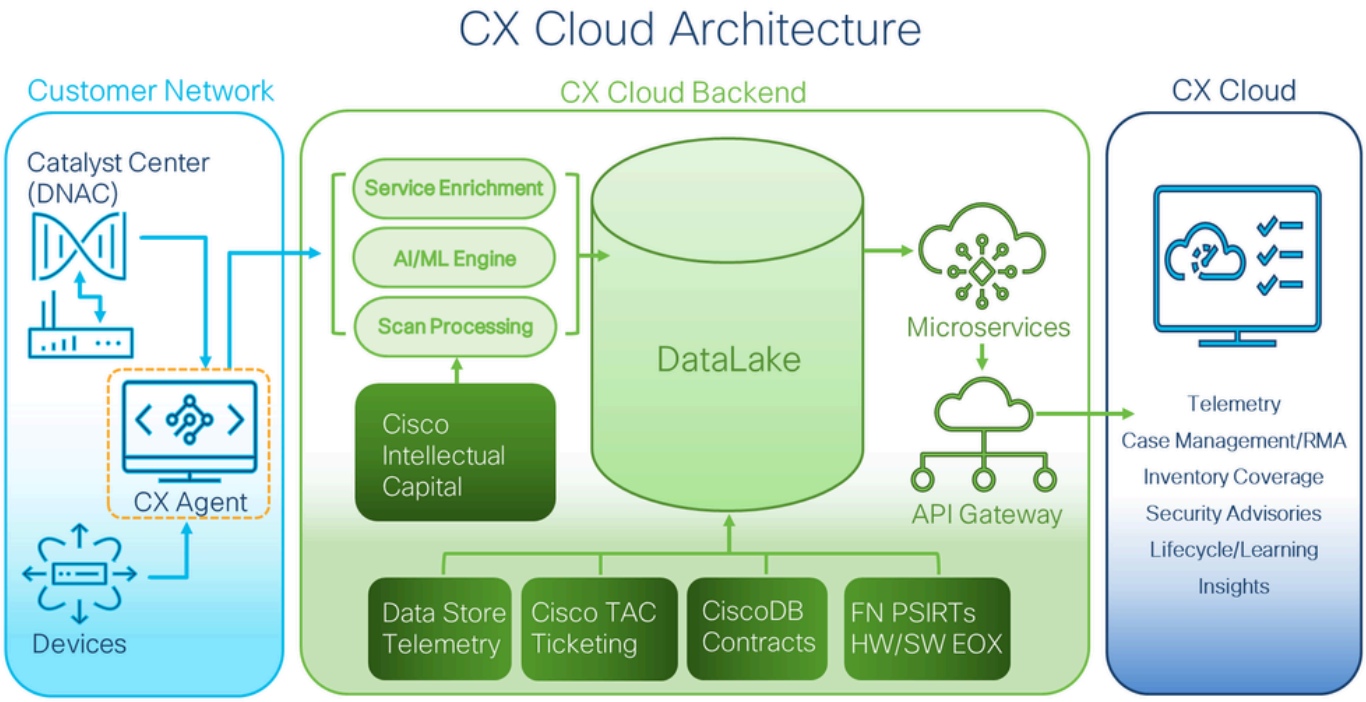
					Required for both Cisco DNA Center and Other Assets collected by CX Cloud Agent support	
					Mandatory TCP/7 Echo (ICMP) port must be combined with one of the other two ports (for device discovery process)	
CX Cloud Agent Traffic					Mandatory for other assets collected by CX Cloud Agent support	
Source	**Destination**		**Protocol**	**Port**	**Purpose**	**Type**
	IP Address	**Hostname**				
Data Collection and Transfer						
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.csco.cloud DNAC Servers Additionally, For Americas region, FQDN: ng.acs.agent.us.csco.cloud For EMEA region, FQDN: agent.emea.csco.cloud, and FQDN: ng.acs.agent.emea.csco.cloud For APJC region, FQDN: agent.apjc.csco.cloud, and FQDN: ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/ 443	Data collection via DNAC servers, Data transfer to CX Cloud, including upgrade functionality	Outbound connection to DNAC servers + Outbound to Cisco AWS regional data centers
Agent IP	Customer Device		SNMP	UDP/161	Collect OIDs and MIBs for other assets collected by CX Cloud Agent	Outbound to LAN
Devices	Agent IP		SYSLOG	UDP/514	Stream Syslog messages from Device to Agent	Inbound from LAN
Agent IP	Customer Device		SSH	TCP/22	Collect CLI commands	Outbound to LAN
Agent IP	Customer Device		Echo	TCP/7	Check the device reachability	Outbound to LAN
Agent IP	Customer Device		Telnet	TCP/23	Collect CLI commands	Outbound to LAN
Agent Administration Access						
Support VM	Agent IP		SSH	TCP/22	Agent Maintenance	Inbound from LAN

Hintergrundinformationen

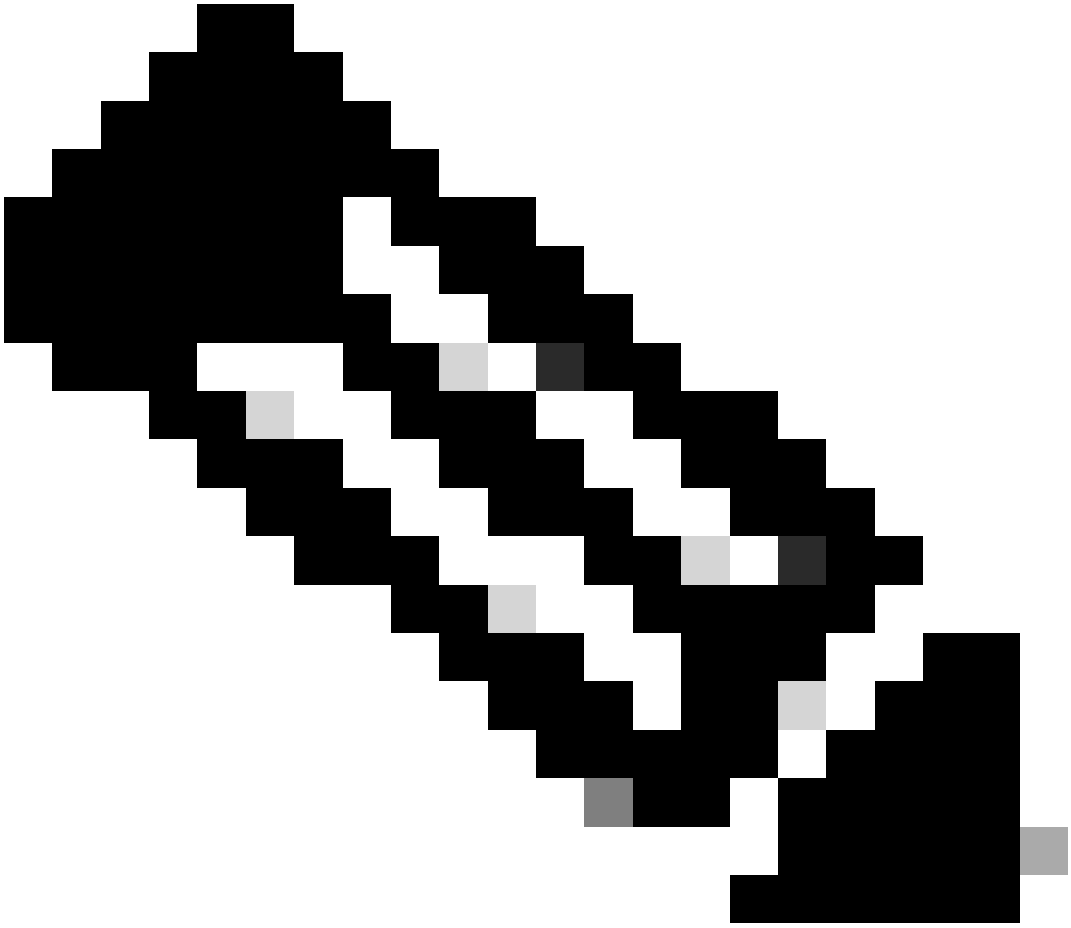
Der (CX) Cloud Agent von Cisco ist eine hochskalierbare Plattform, die Telemetriedaten von Netzwerkgeräten erfasst, um Kunden aussagekräftige Informationen zu liefern. CX Cloud Agent ermöglicht die Umwandlung von aktiven laufenden Konfigurationsdaten in proaktive und prädiktive Einblicke, die in der CX Cloud angezeigt werden, durch künstliche Intelligenz (KI)/maschinelles

Lernen (ML).

Dieses Handbuch bezieht sich speziell auf CX Cloud Agent v2.2 und höher. Auf der Seite Cisco CX Cloud Agent können Sie auf frühere Versionen zugreifen.



CX Cloud-Architektur



Hinweis: Die Bilder (und die darin enthaltenen Inhalte) dienen nur zu Referenzzwecken. Die tatsächlichen Inhalte können variieren.

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

Zugriff auf kritische Domänen

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

Spezifische Domänen des CX Cloud Agent-Portals

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

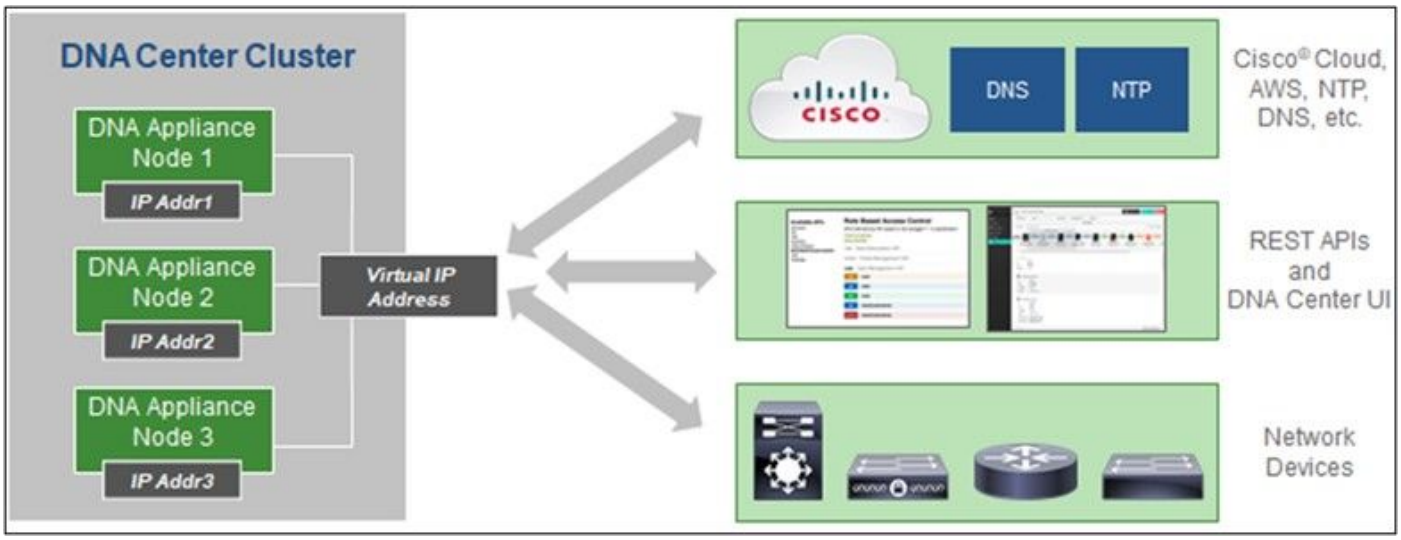
Für CX Cloud Agent OVA spezifische Domänen

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

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

Von Cisco DNA Center unterstützte Version

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



Cisco DNA Center mit HA-Cluster mit mehreren Knoten

Unterstützte Browser

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

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

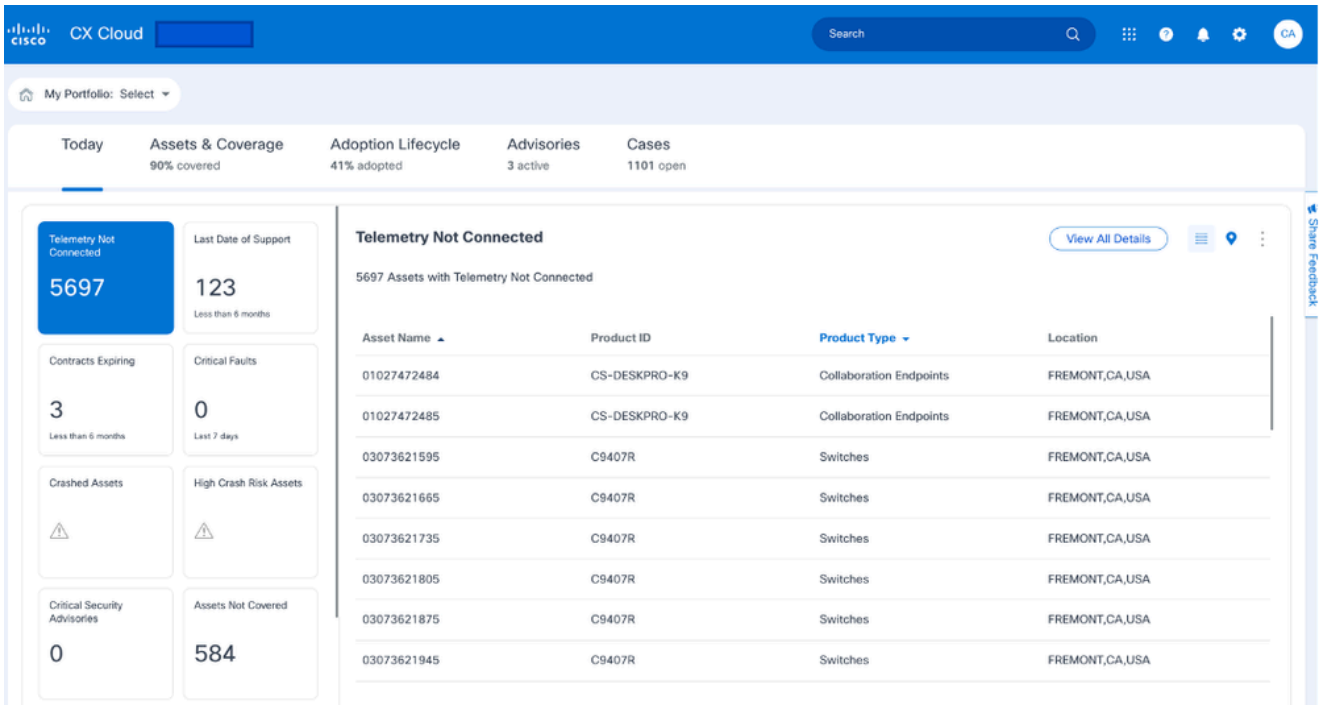
Liste der unterstützten Produkte

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

Verbinden von Datenquellen

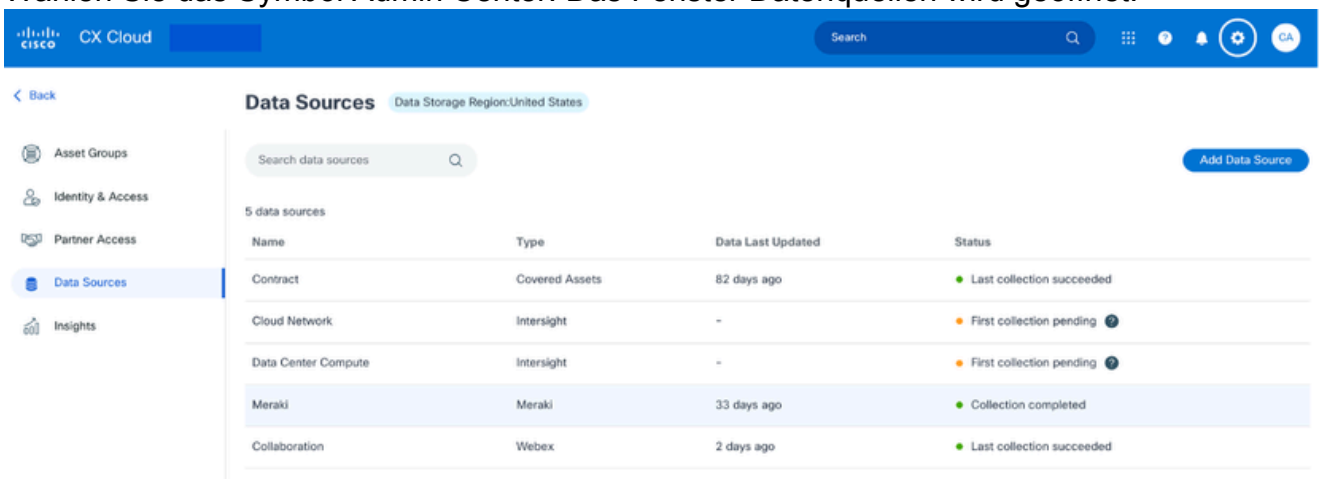
Datenquellen verbinden:

1. Klicken Sie auf cx.cisco.com, um sich bei CX Cloud anzumelden.



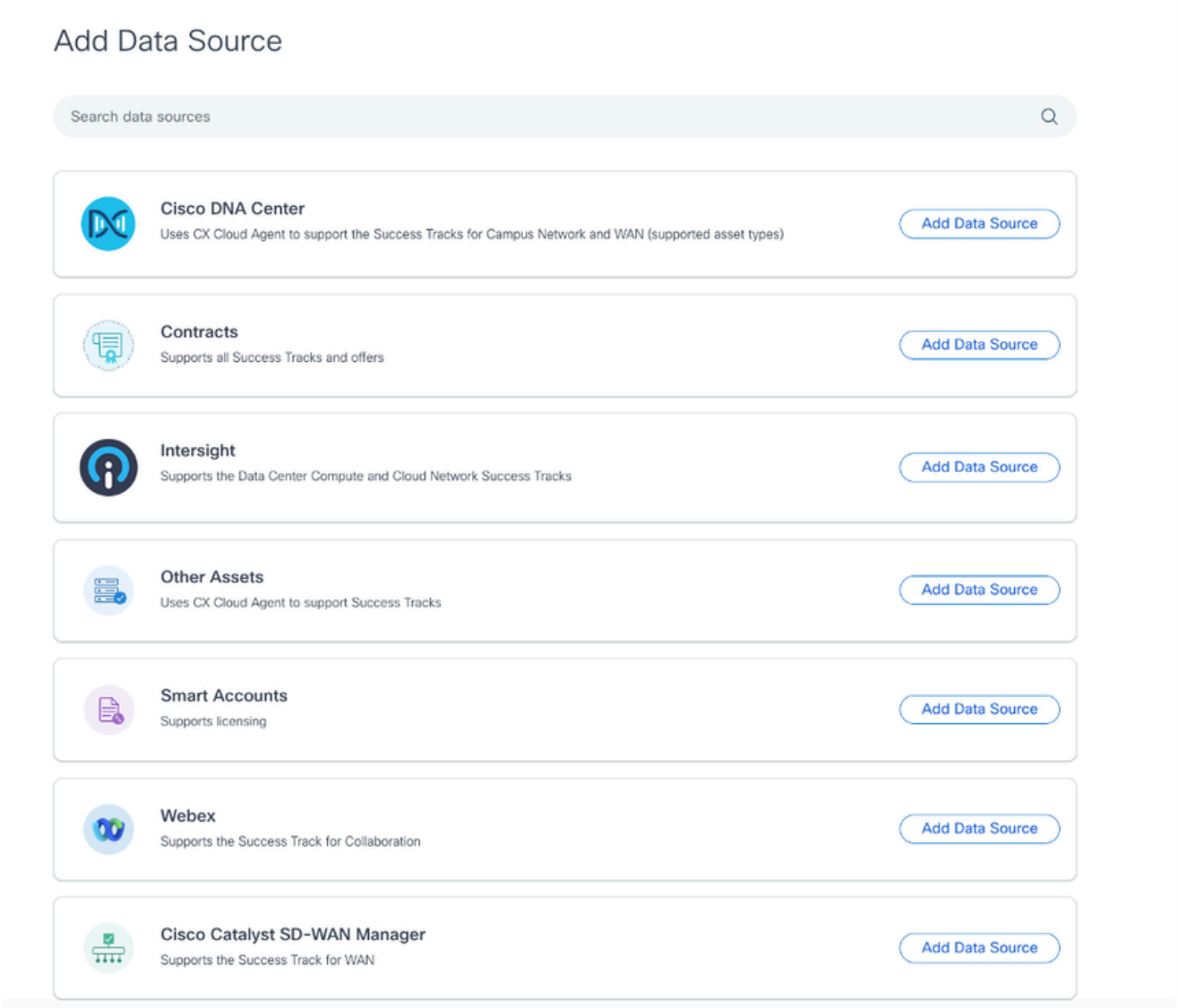
CX Cloud-Startseite

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



Datenquellen

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



Datenquelle hinzufügen

4. Klicken Sie auf Datenquelle hinzufügen, um die entsprechende Datenquelle auszuwählen. Wenn der CX Cloud Agent nicht zuvor eingerichtet wurde, wird das Fenster CX Cloud Agent einrichten geöffnet, in dem die Einrichtung abgeschlossen werden muss. Wenn die Einrichtung abgeschlossen ist, wird die Verbindung fortgesetzt. Lesen Sie einen der folgenden Abschnitte, um fortzufahren:

Einrichten von CX Cloud Agent

Hinzufügen von Cisco DNA Center als Datenquelle

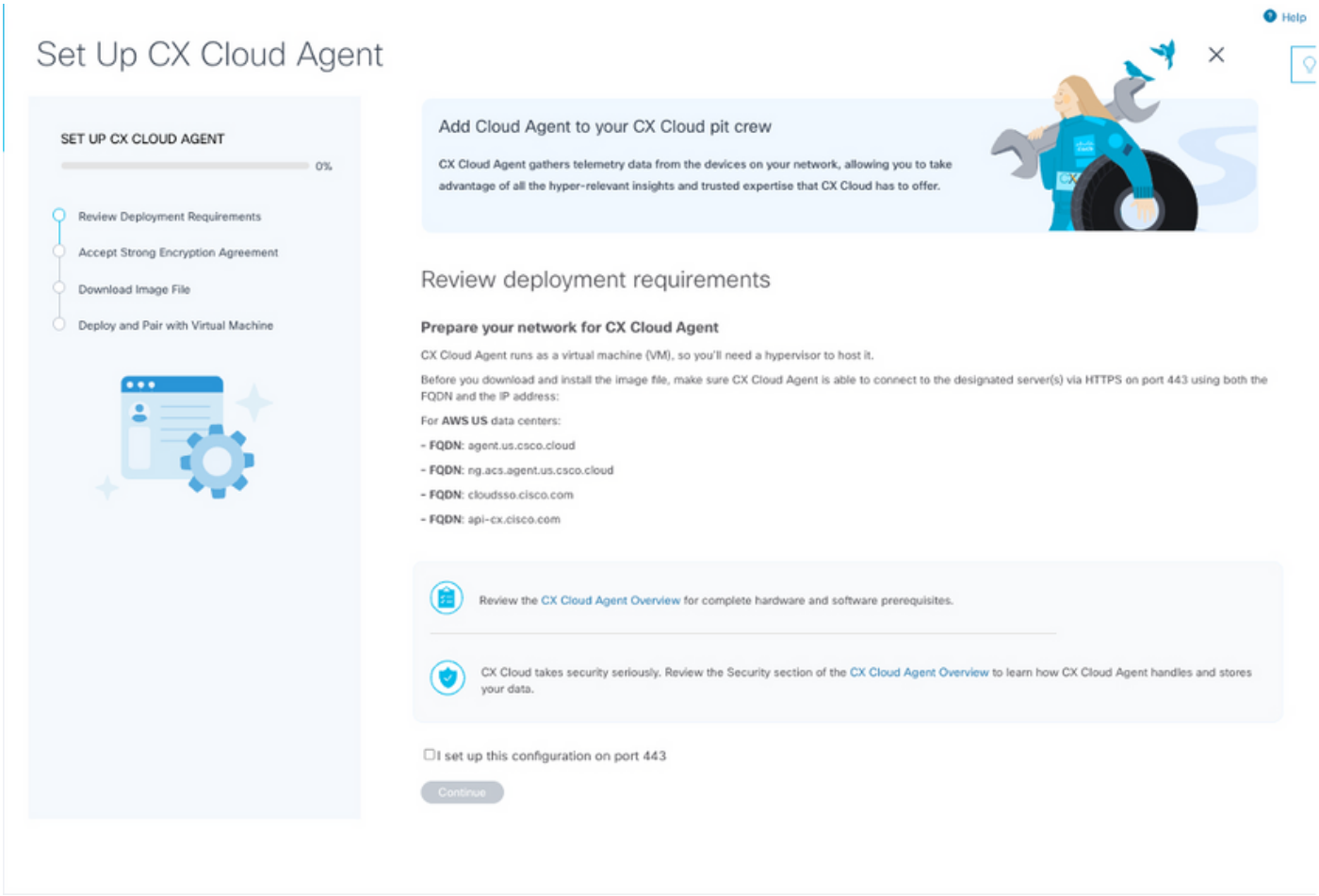
Andere Ressourcen als Datenquellen hinzufügen

Hinweis: Die Option "Andere Ressourcen" ist nur verfügbar, wenn zuvor keine direkte Geräteverbindung konfiguriert wurde.

Einrichten von CX Cloud Agent

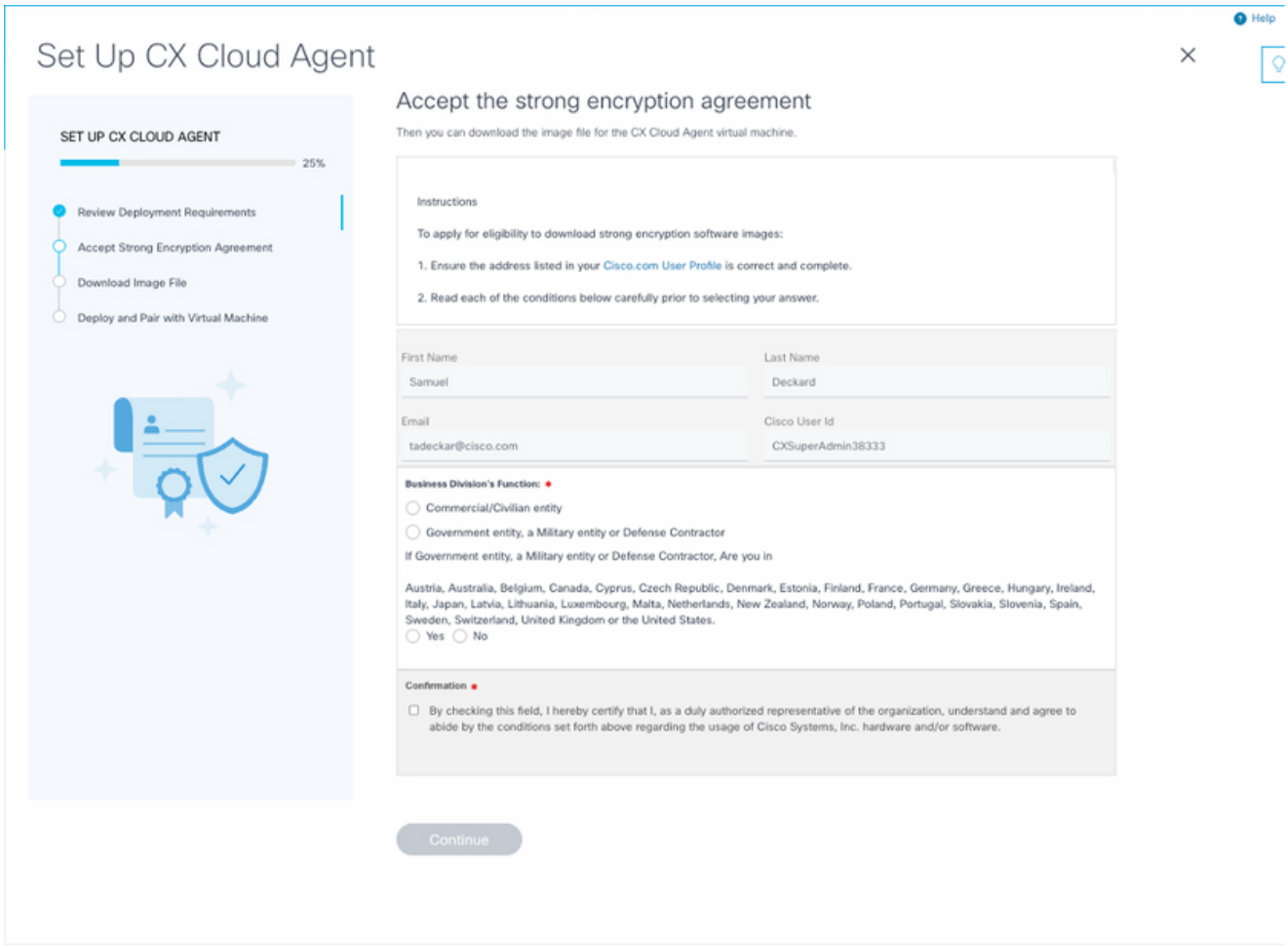
Die Einrichtung des CX Cloud Agent wird beim Verbinden von Datenquellen angefordert, wenn dies noch nicht erfolgt ist.

So richten Sie CX Cloud Agent ein:



Prüfung der Bereitstellungsvoraussetzungen

1. Überprüfen Sie die Bereitstellungsanforderungen, und aktivieren Sie das Kontrollkästchen Ich richte diese Konfiguration auf Port 443 ein.
2. Klicken Sie auf Continue (Weiter). Das Fenster CX Cloud Agent einrichten - Starke Verschlüsselungsvereinbarung akzeptieren wird geöffnet.



Verschlüsselungsvereinbarung

3. Überprüfen Sie die vorab ausgefüllten Informationen in den Feldern Vorname, Nachname, E-Mail und Cisco Benutzer-ID.
4. Wählen Sie die entsprechende Funktion des Geschäftsbereichs aus.
5. Aktivieren Sie das Kontrollkästchen Bestätigung, um den Nutzungsbedingungen zuzustimmen.
6. Klicken Sie auf Continue (Weiter). Das Fenster CX Cloud Agent einrichten - Bilddatei herunterladen wird geöffnet.

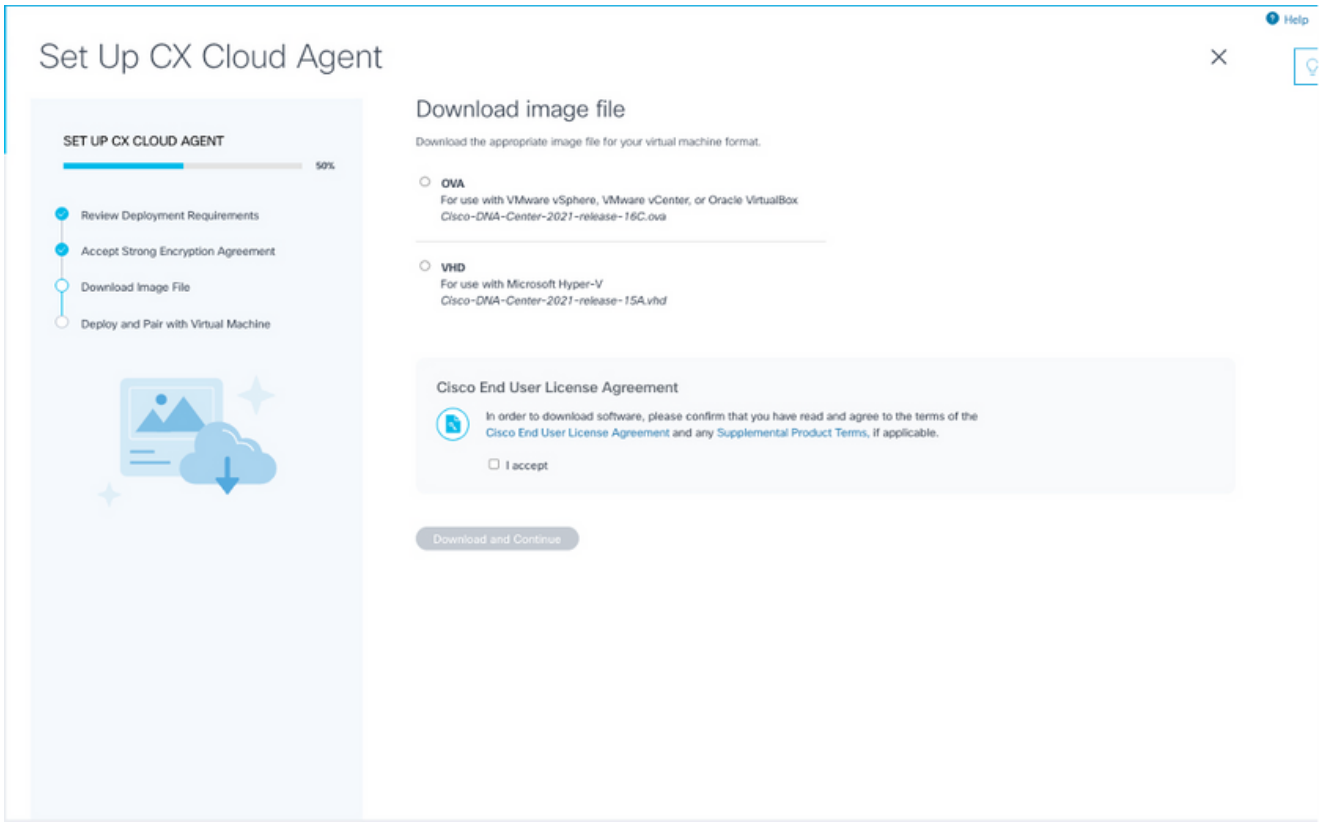


Image herunterladen

7. Wählen Sie das entsprechende Dateiformat aus, um die für die Installation erforderliche Image-Datei herunterzuladen.
8. Aktivieren Sie das Kontrollkästchen Ich akzeptiere, um der Cisco Endbenutzer-Lizenzvereinbarung zuzustimmen.
9. Klicken Sie auf Herunterladen und fortfahren. Das Fenster CX Cloud Agent einrichten - Bereitstellen und mit dem virtuellen System verbinden wird geöffnet.
10. Unter Netzwerkkonfiguration finden Sie den im nächsten Abschnitt erforderlichen Kopplungscode.

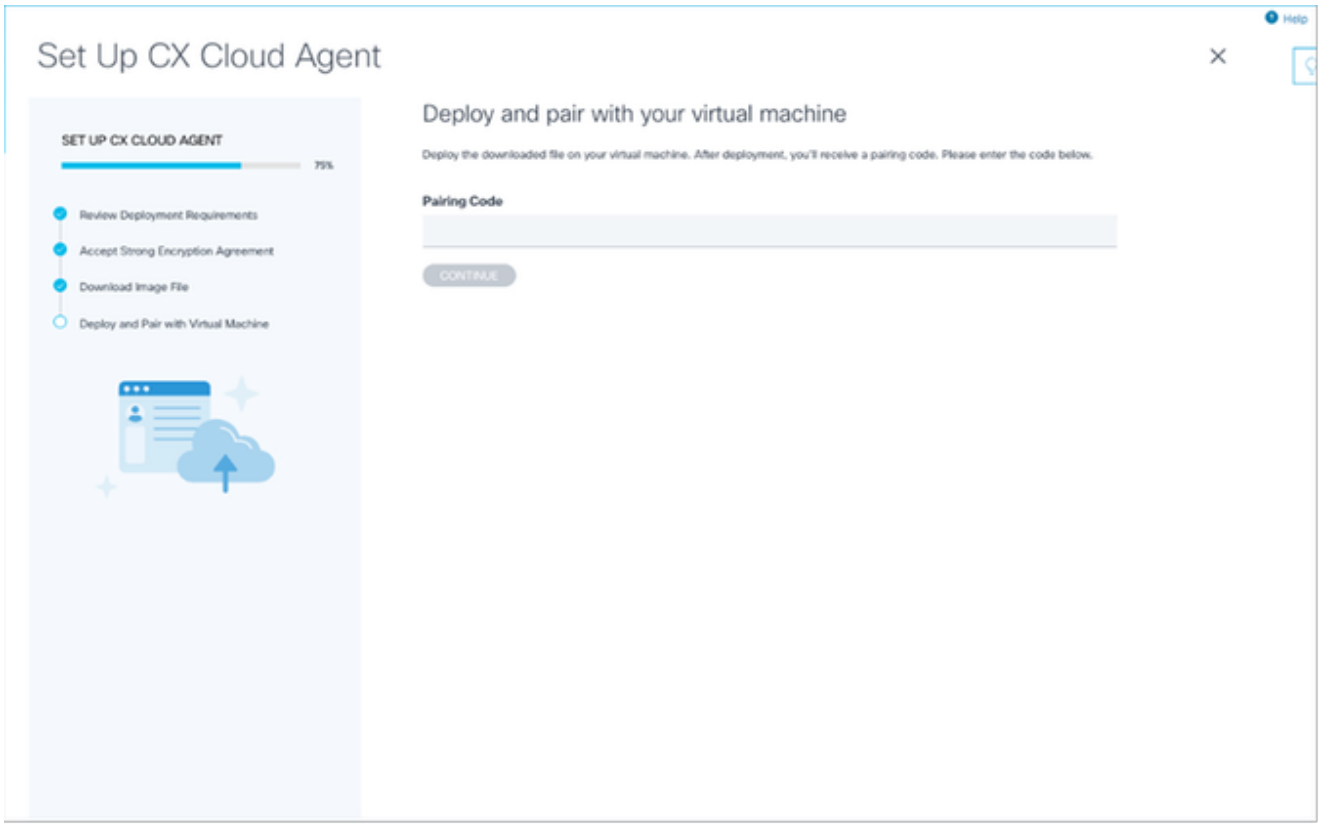
Verbindung zwischen CX Cloud Agent und CX Cloud

Damit die Telemetriesammlung beginnen kann, muss der CX Cloud Agent mit der CX Cloud verbunden werden, damit die Informationen in der Benutzeroberfläche aktualisiert werden können, um die aktuellen Ressourcen und Erkenntnisse anzuzeigen. In diesem Abschnitt finden Sie Details zum Abschließen der Verbindungs- und Fehlerbehebungsrichtlinien.

So verbinden Sie CX Cloud Agent mit CX Cloud:

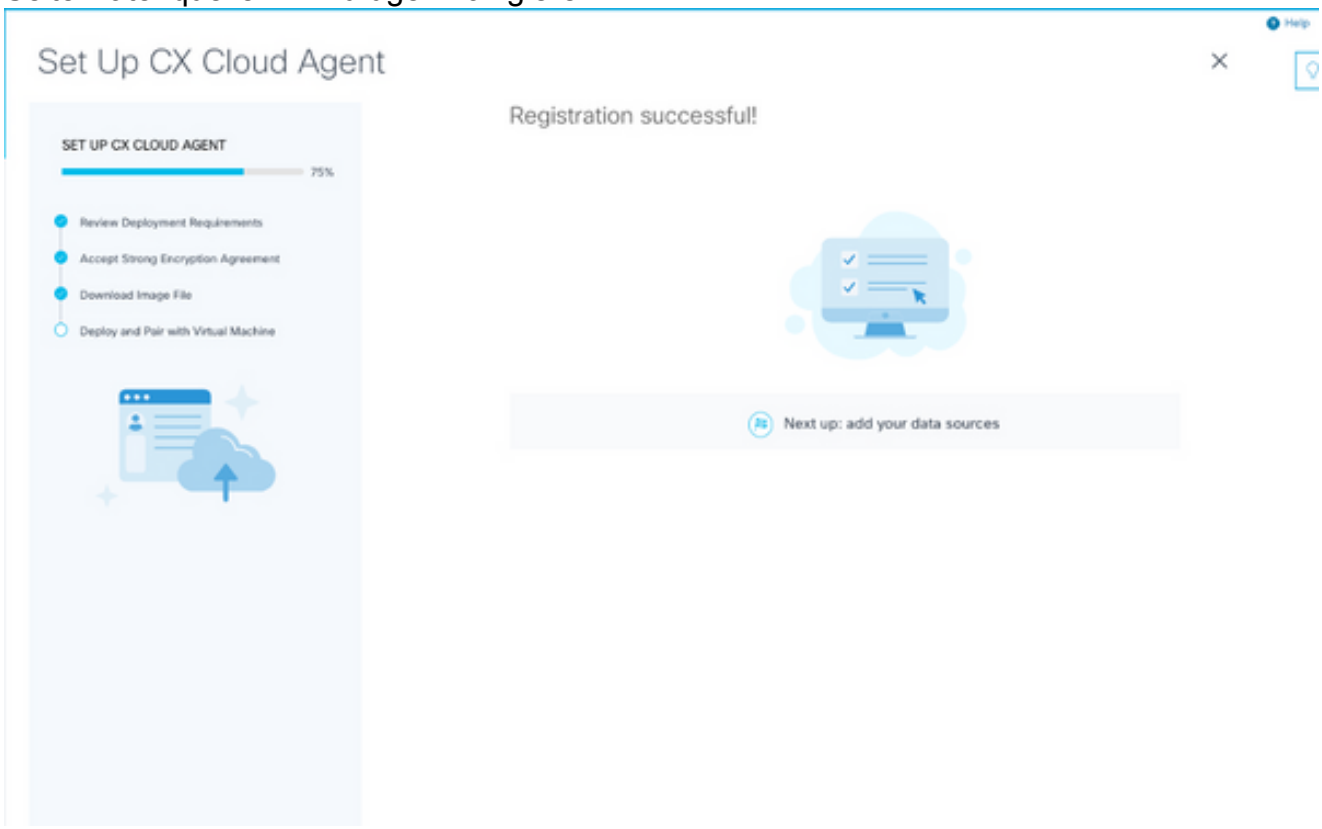
1. Geben Sie den Kopplungscode im Konsolendialog oder in der Befehlszeilenschnittstelle (CLI) der virtuellen Maschine ein, die über den Agenten verbunden ist.

> Hinweis: Der Kopplungscode wird nach der Bereitstellung der heruntergeladenen OVA-Datei empfangen.



Kopplungscode

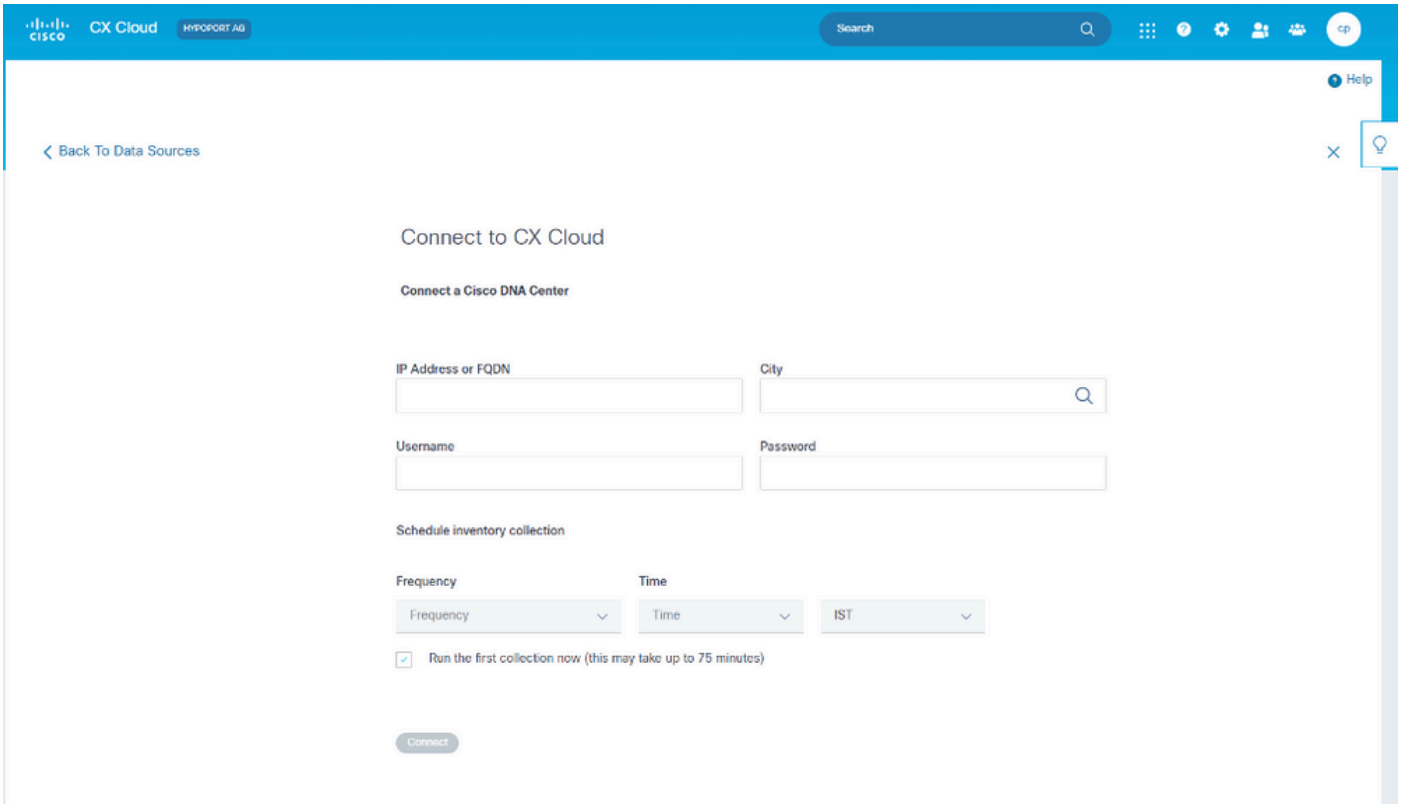
2. Klicken Sie auf Weiter, um den CX Cloud Agent zu registrieren. Das Fenster CX Cloud Agent einrichten - Registrierung erfolgreich wird kurz geöffnet, bevor Sie automatisch zur Seite Datenquellen hinzufügen navigieren.



Registrierung erfolgreich

Hinzufügen von Cisco DNA Center als Datenquelle

Wenn Cisco DNA Center aus dem Verbindungsfenster für Datenquellen ausgewählt wurde (siehe Bild "Datenquellen verbinden" im Abschnitt "Datenquellen verbinden"), wird dieses Fenster geöffnet:



Verbindung zur CX Cloud herstellen

So fügen Sie Cisco DNA Center als Datenquelle hinzu:

1. Geben Sie die Cisco DNA Center IP-Adresse oder virtuelle IP-Adresse oder FQDN, die Stadt (Ort des Cisco DNA Center), den Benutzernamen und das Kennwort ein.

   Hinweis: Verwenden Sie keine individuelle Cluster-Knoten-IP.

2. Planen Sie eine Bestandserfassung, indem Sie Häufigkeit und Zeit eingeben, um anzugeben, wie oft der CX Cloud Agent Netzwerkscans durchführen und Informationen auf verbundenen Geräten aktualisieren kann.

   Hinweis: Die erste Bestandserfassung kann bis zu 75 Minuten dauern.

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

Erfolgreich verbunden

4. Klicken Sie auf Add Another Cisco DNA Center, Done (Weiteres Cisco DNA-Center hinzufügen) oder Back to Data Sources (Zurück zu Datenquellen), um zum Fenster Datenquellen zurückzunavigieren.

Andere Ressourcen als Datenquellen hinzufügen

Überblick

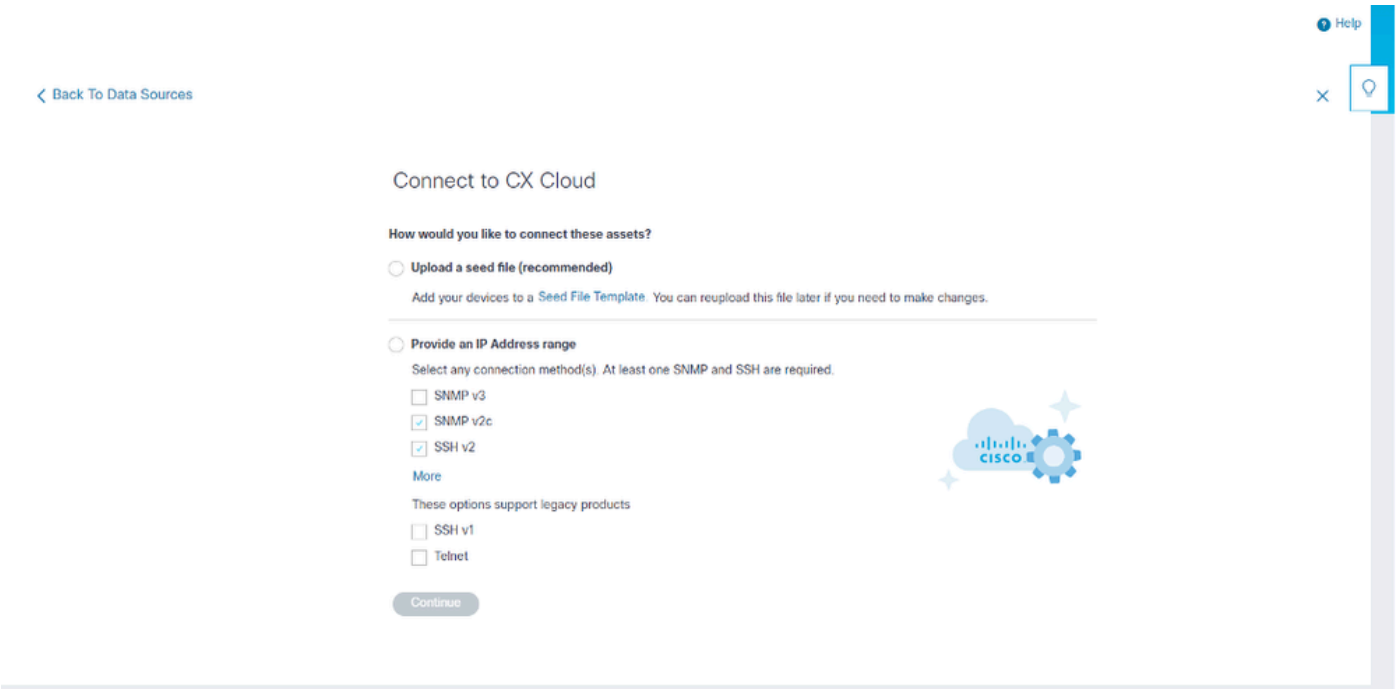
Die Telemetriesammlung wurde auf Geräte ausgedehnt, die nicht vom Cisco DNA Center verwaltet werden. Kunden können so aus Telemetriedaten gewonnene Erkenntnisse und Analysen abrufen und mit diesen interagieren, um eine breitere Palette an Geräten zu ermöglichen. Nach der Ersteinrichtung von CX Cloud Agent können Benutzer CX Cloud Agent für die Verbindung mit 20 weiteren Cisco DNA Centern innerhalb der von CX Cloud überwachten Infrastruktur konfigurieren. Benutzer können CX Cloud Agent auch direkt mit anderen Hardwarekomponenten in ihrer Umgebung verbinden, bis zu 10.000 direkt verbundene Geräte.

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

Anmerkung:
Es kann entweder die Seed-Datei oder der IP-Bereich verwendet werden. Diese Auswahl kann nach der Ersteinrichtung nicht mehr geändert werden.

Anmerkung:
Eine anfängliche Seed-Datei kann durch eine andere Seed-Datei ersetzt werden, während ein anfänglicher IP-Bereich in einen neuen IP-Bereich geändert werden kann.

Wenn im Fenster für die Datenquellenverbindung die Option Andere Ressourcen ausgewählt ist, wird dieses Fenster geöffnet:



Konfigurieren der Verbindung zur CX-Cloud

So fügen Sie andere Ressourcen als Datenquellen hinzu:

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

Discovery-Protokolle

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

SNMPV2c und SNMPV3 unterscheiden sich hinsichtlich der Sicherheit und des Remote-Konfigurationsmodells. SNMPV3 verwendet ein erweitertes kryptographisches Sicherheitssystem, das die SHA-Verschlüsselung unterstützt, um Nachrichten zu authentifizieren und ihre Privatsphäre zu gewährleisten. Es wird empfohlen, SNMPv3 in allen öffentlichen und mit dem Internet verbundenen Netzwerken zu verwenden, um den Schutz vor Sicherheitsrisiken und -bedrohungen zu gewährleisten. Auf der CX Cloud sollte SNMPv3 vorzugsweise konfiguriert

werden und nicht SNMPv2c, mit Ausnahme älterer Legacy-Geräte, die keine integrierte Unterstützung für SNMPv3 bieten. Wenn beide Versionen von SNMP vom Benutzer konfiguriert wurden, kann der CX Cloud Agent standardmäßig versuchen, mit den jeweiligen Geräten über SNMPv3 zu kommunizieren und auf SNMPv2c zurückzugreifen, wenn die Kommunikation nicht erfolgreich ausgehandelt werden kann.

Verbindungsprotokolle

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

Hinzufügen von Geräten mithilfe einer Seed-Datei

Informationen zur Seed-Datei

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

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

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

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

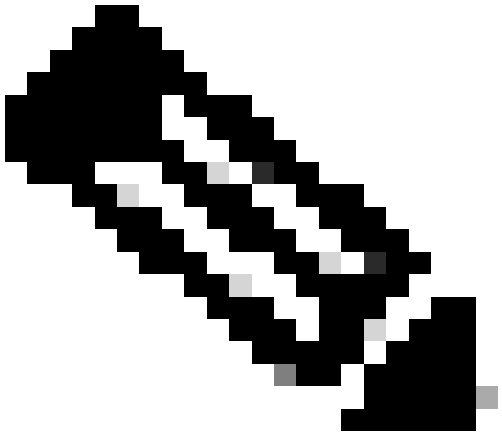
Hinweis: Diese PDF-Datei dient nur zu Referenzzwecken und kann zum Erstellen einer

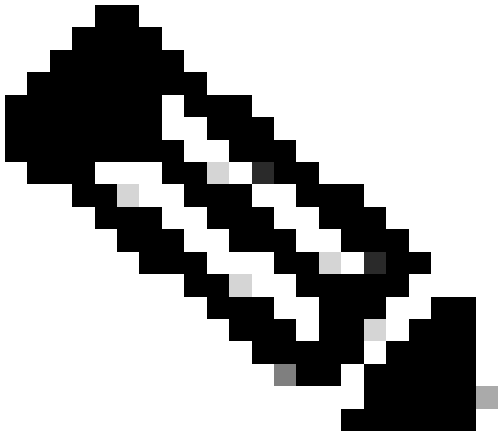
---

Seed-Datei verwendet werden, die im CSV-Format gespeichert werden muss.

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

Seed-Dateispalte	Spaltenüberschrift/-kennung	Zweck der Spalte
A	IP-Adresse oder Hostname	Geben Sie eine gültige, eindeutige IP-Adresse oder einen Hostnamen des Geräts an.
B	SNMP-Protokollversion	Das SNMP-Protokoll wird von CX Cloud Agent benötigt und zur Geräteerkennung im Kundennetzwerk verwendet. Werte können snmpv2c oder snmpv3 sein, aber aus Sicherheitsgründen wird snmpv3 empfohlen.
C	snmpRo : Erforderlich, wenn col#=3 als 'snmpv2c' ausgewählt ist	Wenn die ältere Variante von SNMPv2 für ein bestimmtes Gerät ausgewählt ist, müssen snmpRO-Anmeldeinformationen (schreibgeschützt) für die SNMP-Sammlung des Geräts angegeben werden. Andernfalls kann der Eintrag leer sein.
G	snmpv3UserName : Erforderlich, wenn col#=3 als 'snmpv3' ausgewählt ist	Wenn SNMPv3 für die Kommunikation mit einem bestimmten Gerät ausgewählt ist, muss der entsprechende Benutzername für die Anmeldung angegeben werden.
O	snmpv3AuthAlgorithm: Werte können MD5 oder SHA sein.	Das SNMPv3-Protokoll ermöglicht die Authentifizierung entweder über den MD5- oder den SHA-Algorithmus. Wenn das Gerät mit sicherer Authentifizierung konfiguriert ist, muss der entsprechende Auth-Algorithmus angegeben werden.

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

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

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

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

Einschränkungen bei der Telemetrieverarbeitung für Geräte

Bei der Verarbeitung von Telemetriedaten für Geräte gelten folgende Einschränkungen:

- Einige Geräte können in der Sammlungsübersicht als erreichbar angezeigt werden, sind jedoch auf der Seite CX Cloud Assets (CX-Cloud-Ressourcen) nicht sichtbar. Einschränkungen bei der Geräteausstattung verhindern die Verarbeitung solcher Gerätetelemetrie.

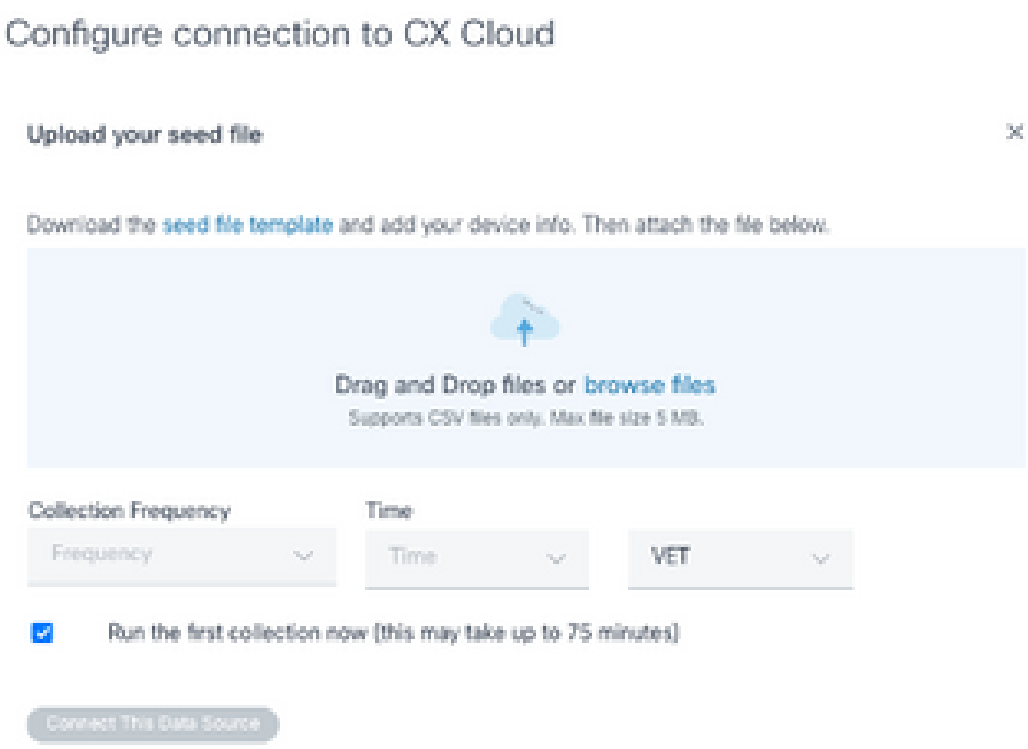
- Telemetrie-Attribute können auf der Seite CX Cloud-Ressourcen für Geräte, die nicht zum Campus Success Track gehören, ungenau sein oder fehlen.
- Wenn ein Gerät aus der Seed-Datei oder den Sammlungen des IP-Bereichs ebenfalls Teil des Cisco DNA Center-Inventars ist, wird das Gerät nur einmal für den Cisco DNA Center-Eintrag gemeldet. Der Eintrag für die Seed-Datei/den IP-Bereich wird nicht erfasst oder verarbeitet, um eine Duplizierung zu vermeiden.

Hinzufügen von Geräten mithilfe einer neuen Seed-Datei

So fügen Sie Geräte mithilfe einer neuen Seed-Datei hinzu:

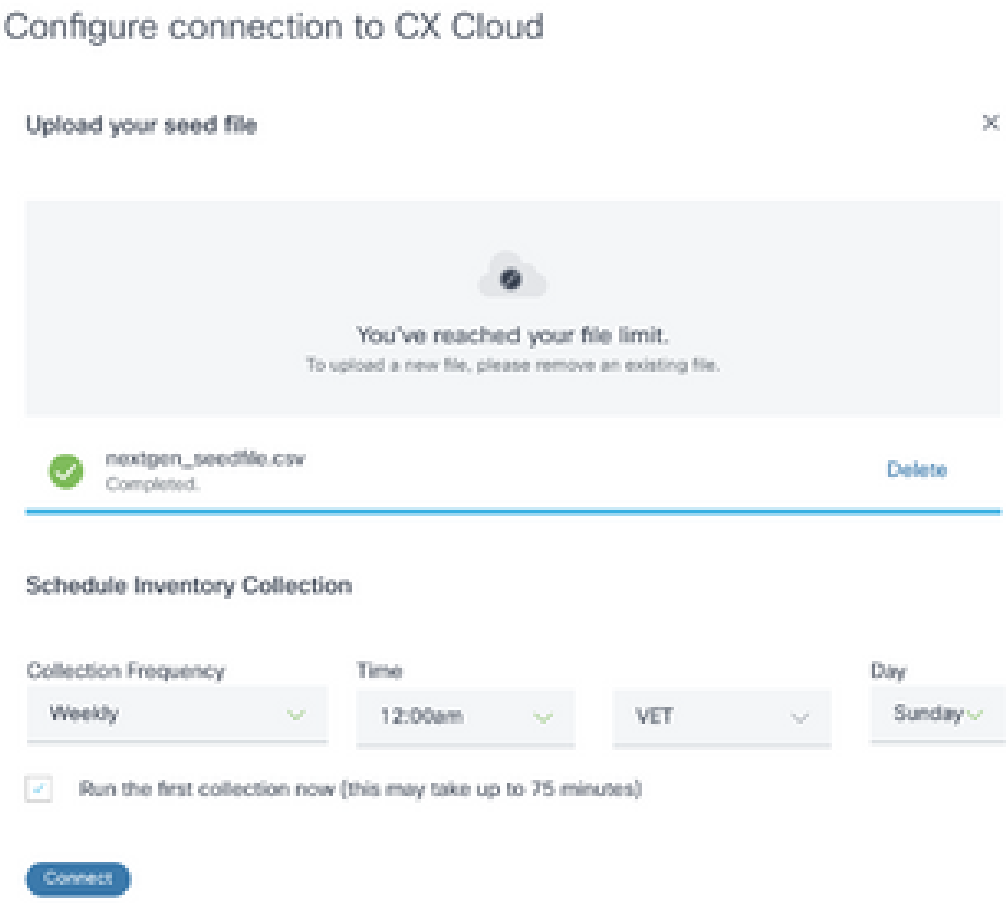
1. Laden Sie die Seed-Dateivorlage (PDF) über den eingebetteten Link in diesem Dokument (siehe Informationen zur Seed-Datei) oder über einen Link im Fenster "Configure Connection to CX Cloud" (Verbindung mit CX-Cloud konfigurieren) herunter.

   Hinweis: Der Link im Fenster Verbindung mit CX Cloud konfigurieren ist nach dem Herunterladen der ersten Seed-Datei nicht mehr verfügbar.



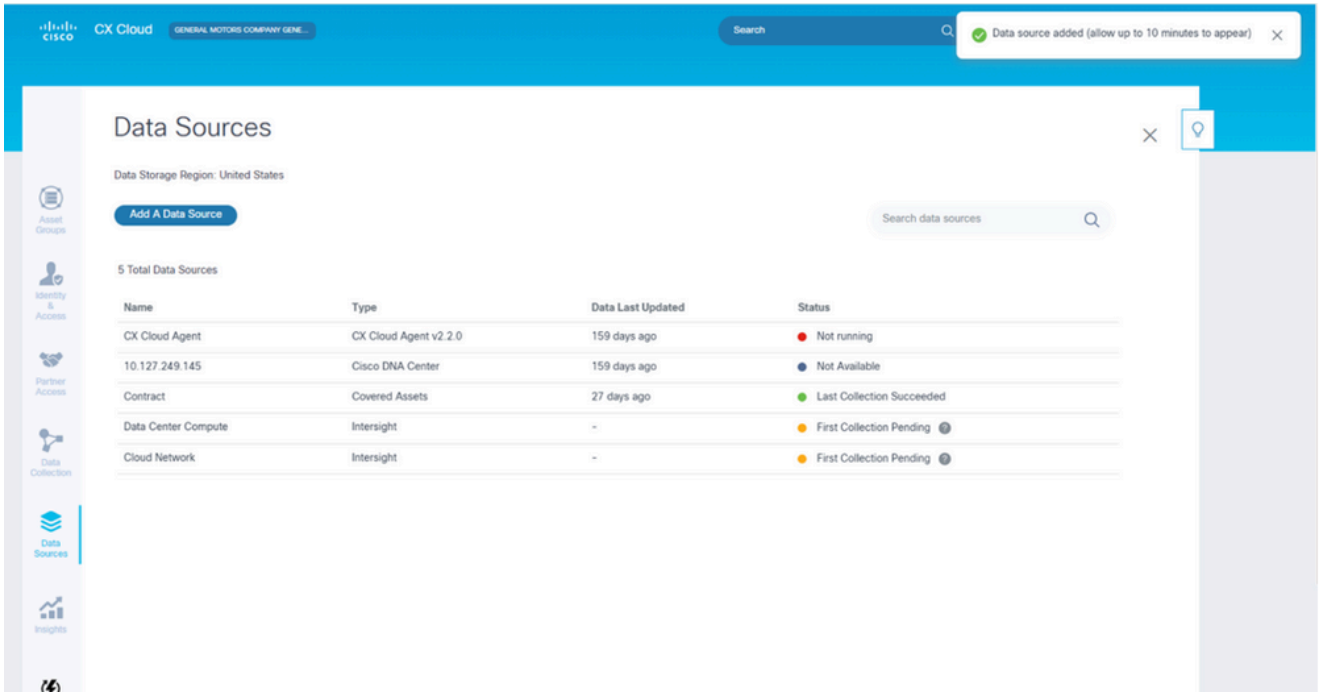
Fenster "Connect to CX Cloud" konfigurieren

2. Öffnen Sie eine Excel-Tabelle (oder eine beliebige bevorzugte Tabelle), und geben Sie die Überschriften wie in der Vorlage dargestellt ein.
3. Geben Sie Daten manuell ein, oder importieren Sie Daten in die Datei.
4. Speichern Sie die Vorlage abschließend als CSV-Datei, um die Datei in CX Cloud Agent zu importieren.



Fenster "Seed-Datei hochladen"

5. Ziehen Sie im Fenster Upload your seed file (Startdatei hochladen) die neu erstellte CSV-Datei, und legen Sie sie dort ab, oder klicken Sie auf Browse files (Dateien durchsuchen), und navigieren Sie zur CSV-Datei.
6. Füllen Sie den Abschnitt Schedule Inventory Collection aus, und klicken Sie auf Verbinden. Das Fenster Datenquellen wird geöffnet, und es wird eine Bestätigungsmeldung angezeigt.
7. 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.



Bestätigungsmeldung

Hinzufügen von Geräten mithilfe einer geänderten Seed-Datei

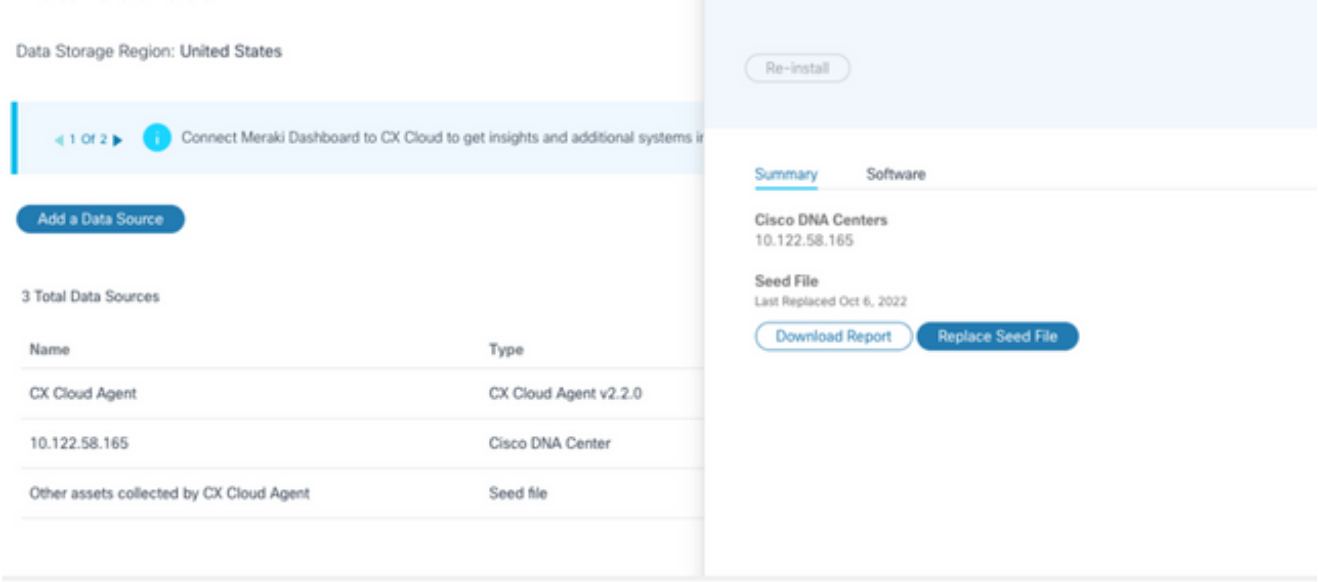
So fügen Sie Geräte mithilfe der aktuellen Seed-Datei hinzu, ändern oder löschen sie:

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

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

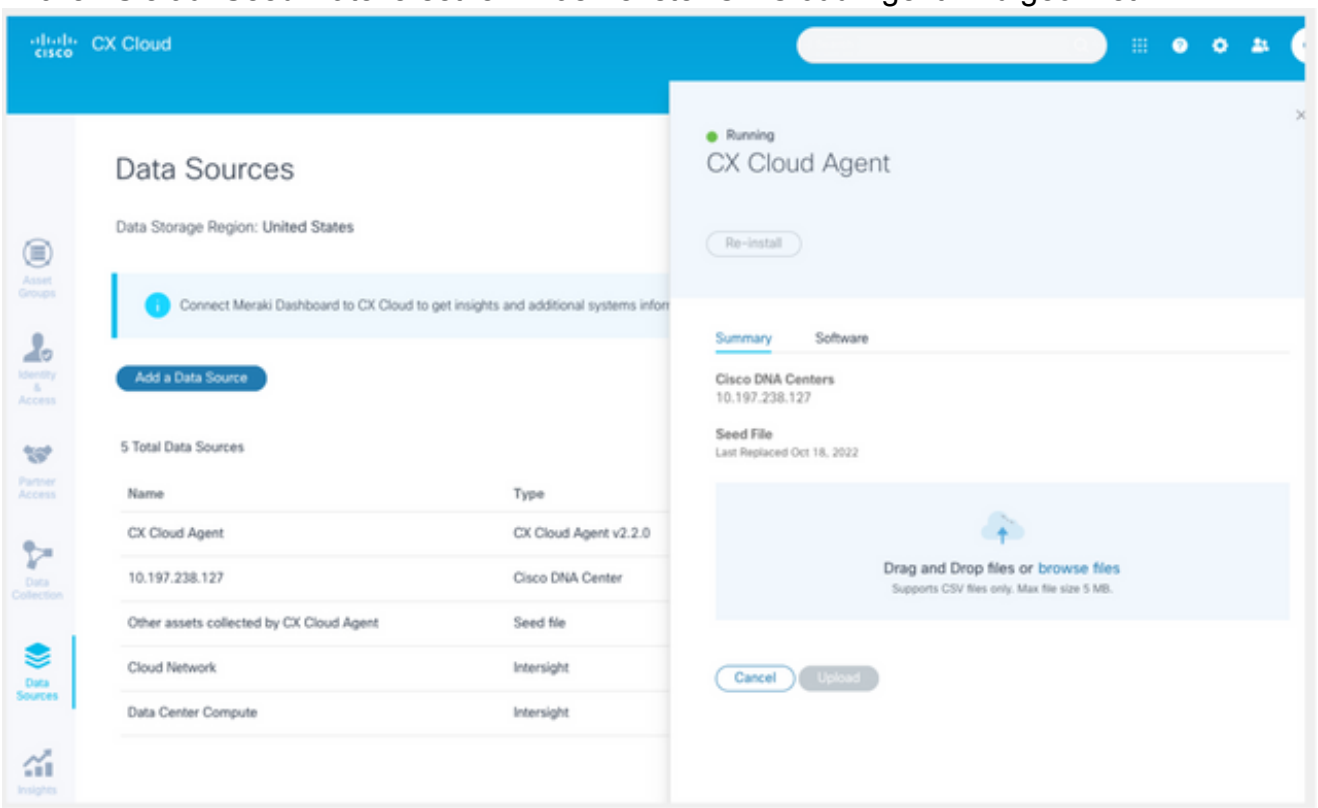
---

2. Wählen Sie auf der Seite Datenquellen eine Datenquelle mit dem Typ CX Cloud Agent aus. Ein Detailfenster mit den Registerkarten Zusammenfassung und Software wird geöffnet.



Detailfenster

3. Klicken Sie auf Bericht herunterladen, um einen Bericht über alle Ressourcen für die ausgewählte Datenquelle zu erstellen. Der Bericht enthält Informationen zu IP-Adresse, Seriennummer, Erreichbarkeit, Befehlstyp, Befehlsstatus und Befehlsfehler, falls zutreffend.
4. Klicken Sie auf Seed-Datei ersetzen. Das Fenster CX Cloud Agent wird geöffnet.



Fenster "CX Cloud Agent"

5. Ziehen Sie die geänderte Seed-Datei in das Fenster, oder suchen Sie die Datei, und fügen Sie sie dem Fenster hinzu.
6. Klicken Sie auf Hochladen.

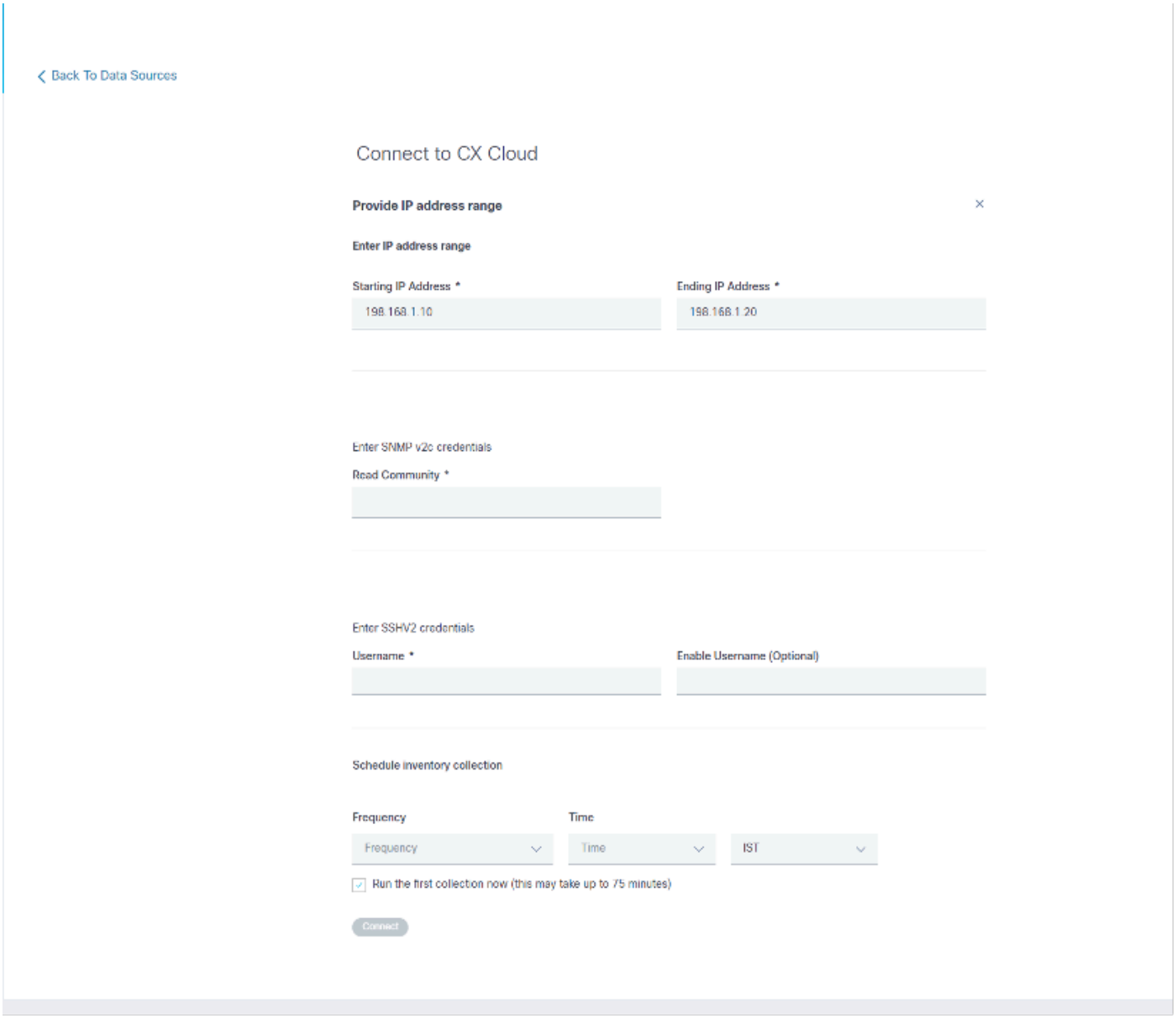
Hinzufügen von Geräten mithilfe von IP-Bereichen

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

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

Der CX Cloud Agent kann versuchen, eine Verbindung mit den Geräten herzustellen, kann jedoch nicht jedes Gerät verarbeiten, um es in der Ansicht "Ressourcen" anzuzeigen, falls die PIDs oder Seriennummern nicht ermittelt werden können.

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



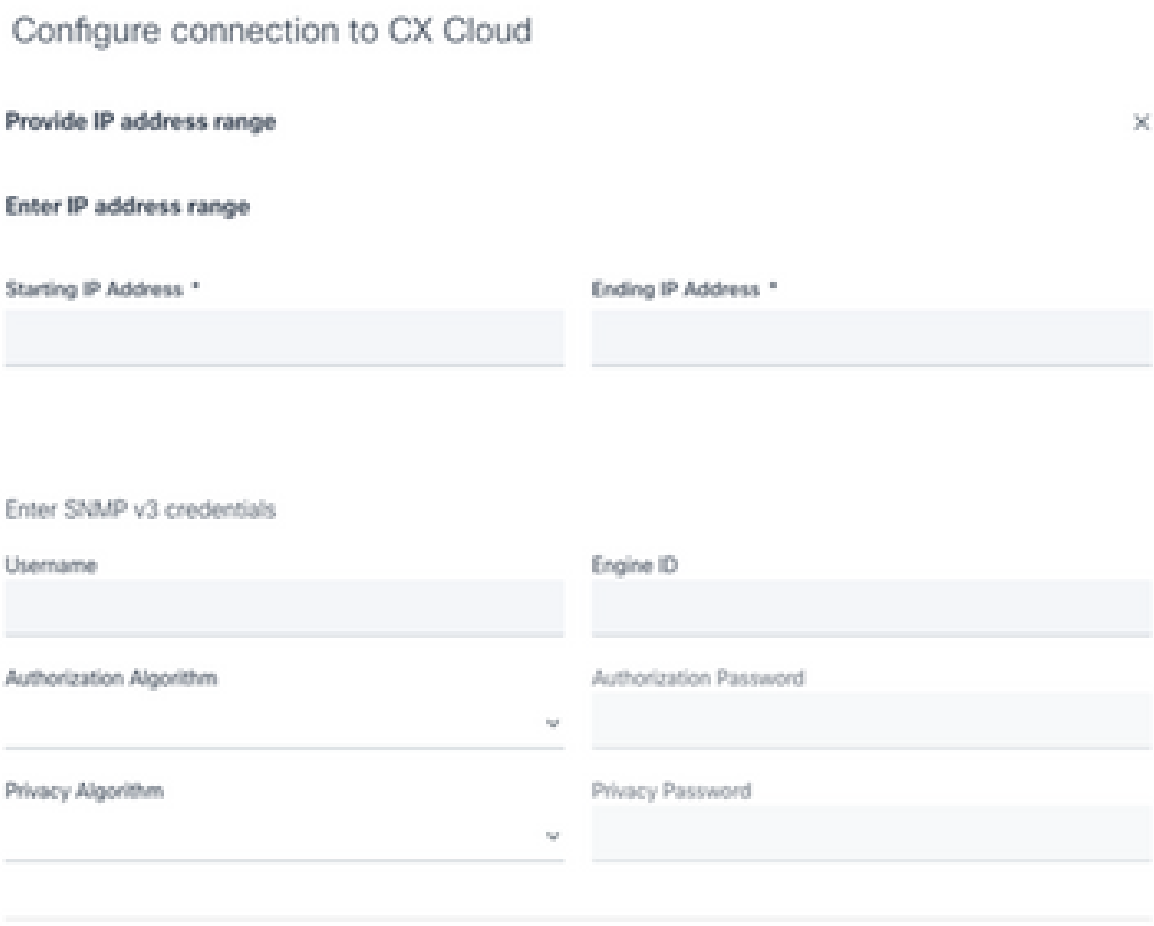
Fenster "Initial IP Address Range"

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

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

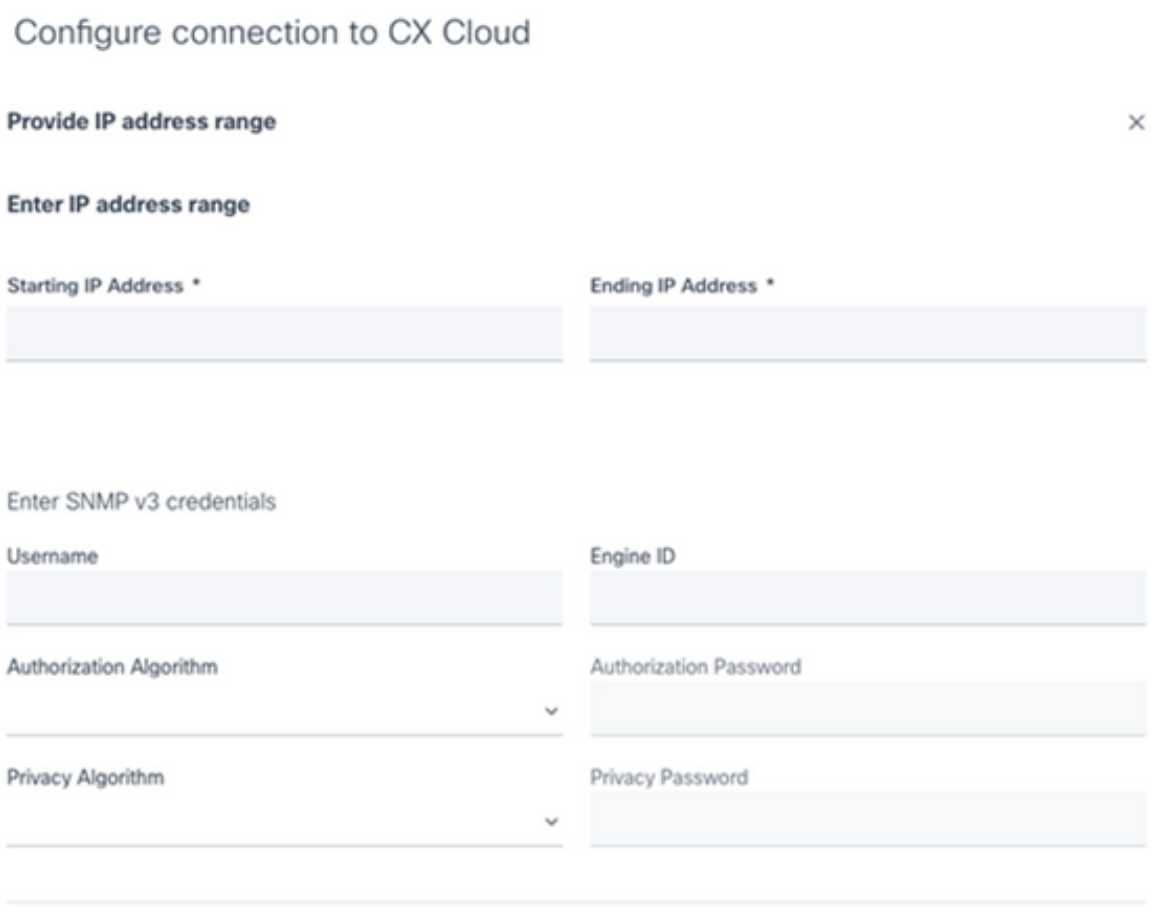
So fügen Sie Geräte über den IP-Bereich hinzu:

1. Wählen Sie im Fenster Verbindung mit CX Cloud konfigurieren die Option IP-Adressbereich bereitstellen aus.

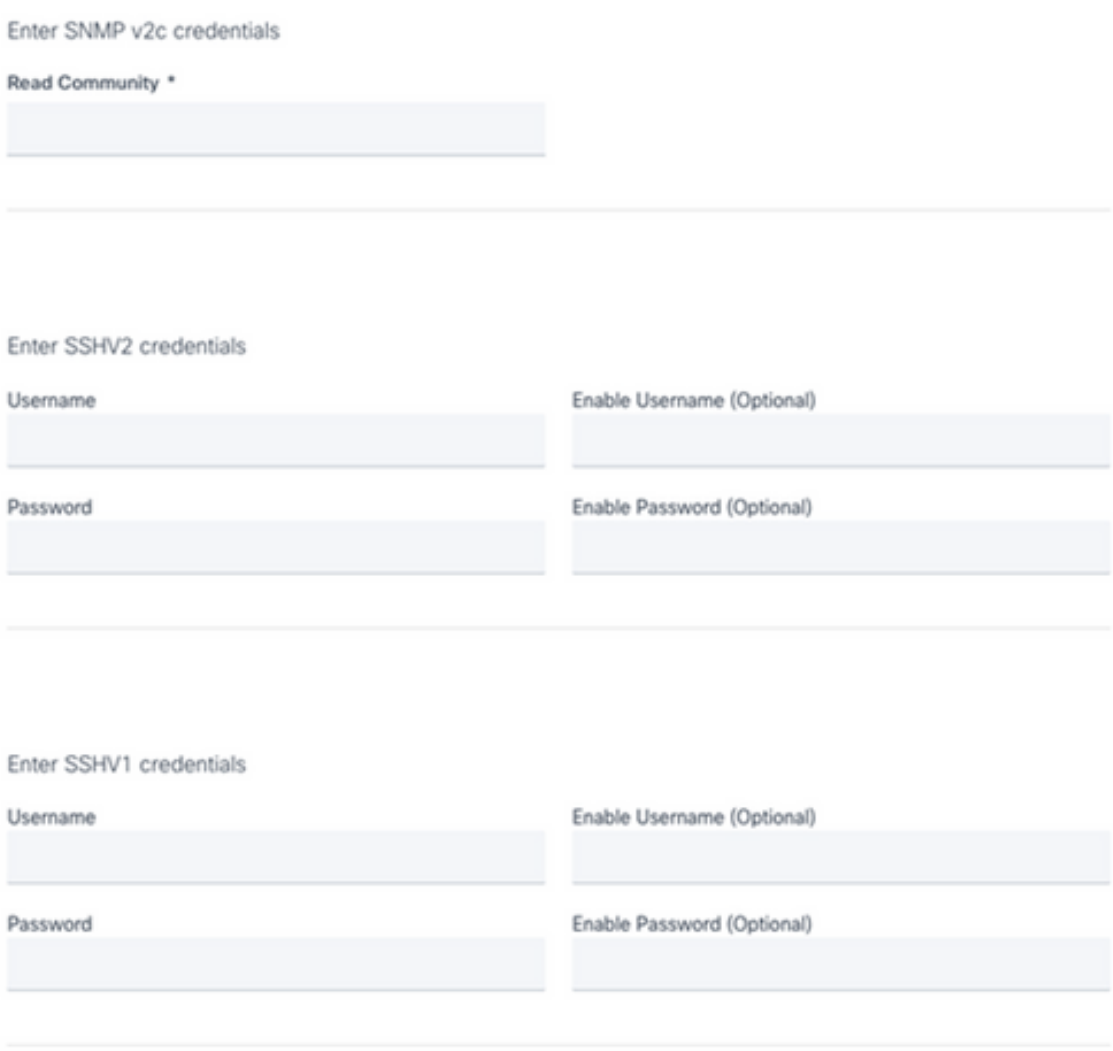


Hinzufügen von Geräten mithilfe des Formulars "IP-Adressen"

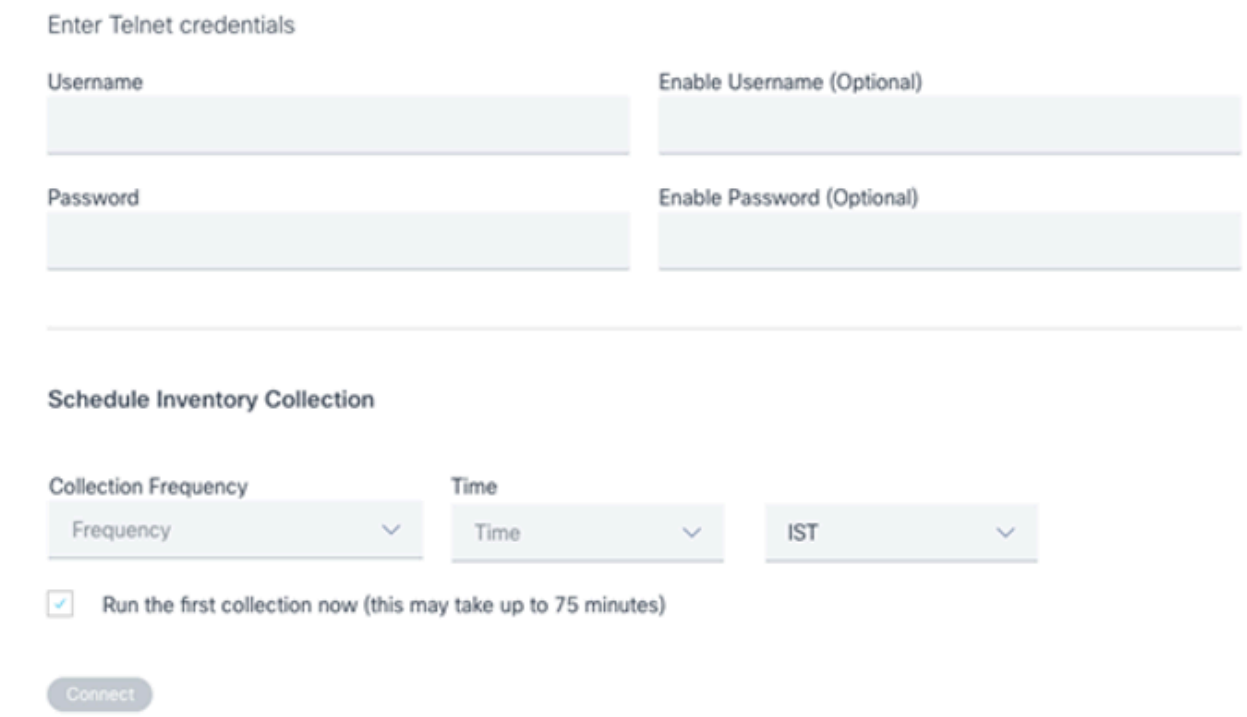
2. Füllen Sie das Formular mit den entsprechenden Informationen aus.
3. Es können mehrere Verbindungsoptionen ausgewählt werden. Auf diesen Bildschirmen werden die Anmeldeinformationen für die Konfiguration der Optionen angezeigt. Eine Beschreibung der Anmeldeinformationsfelder für jede Verbindungsoption finden Sie unter About the Seed File (Informationen zur Seed-Datei).



SNMP v3-Anmeldeinformationen

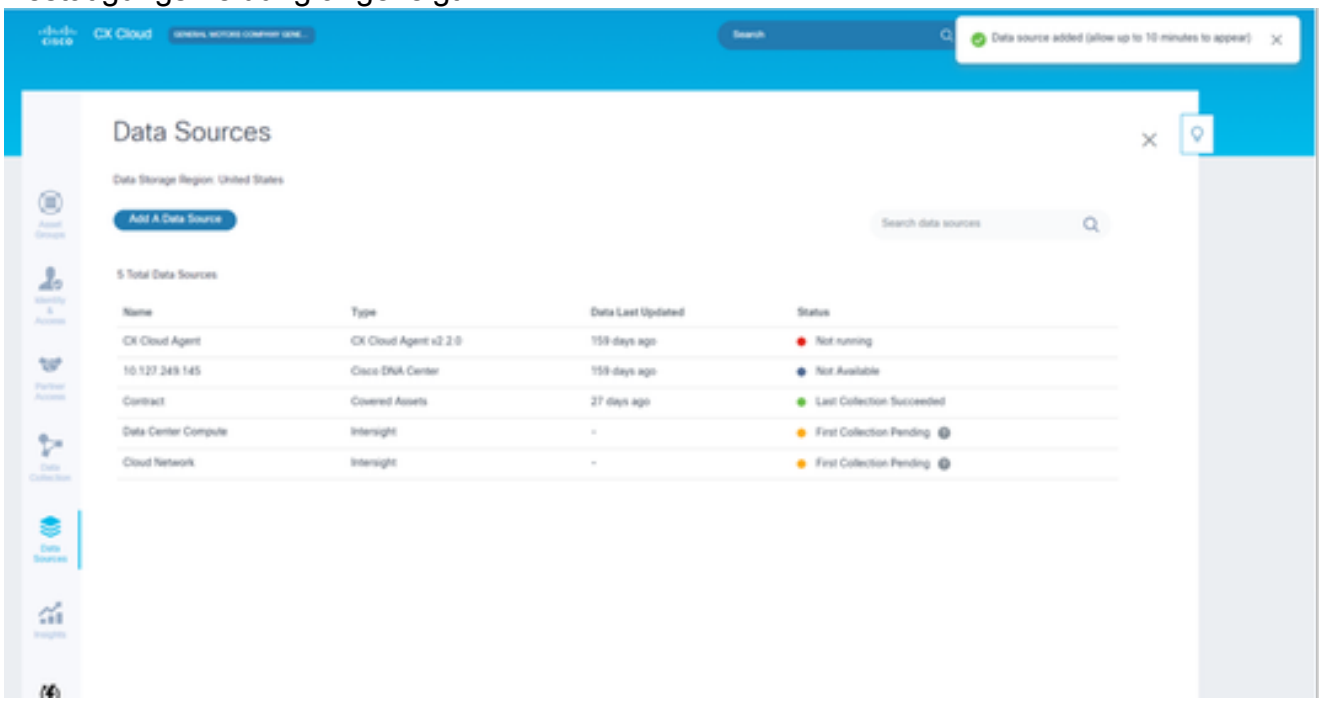


SNMP v2-, SSHV2- und SSHV1-Anmeldedaten



Telnet-Anmeldedaten und Zeitplan für Netzwerksuche

4. Klicken Sie auf Verbinden. Das Fenster Datenquellen wird geöffnet, und es wird eine Bestätigungsmeldung angezeigt.

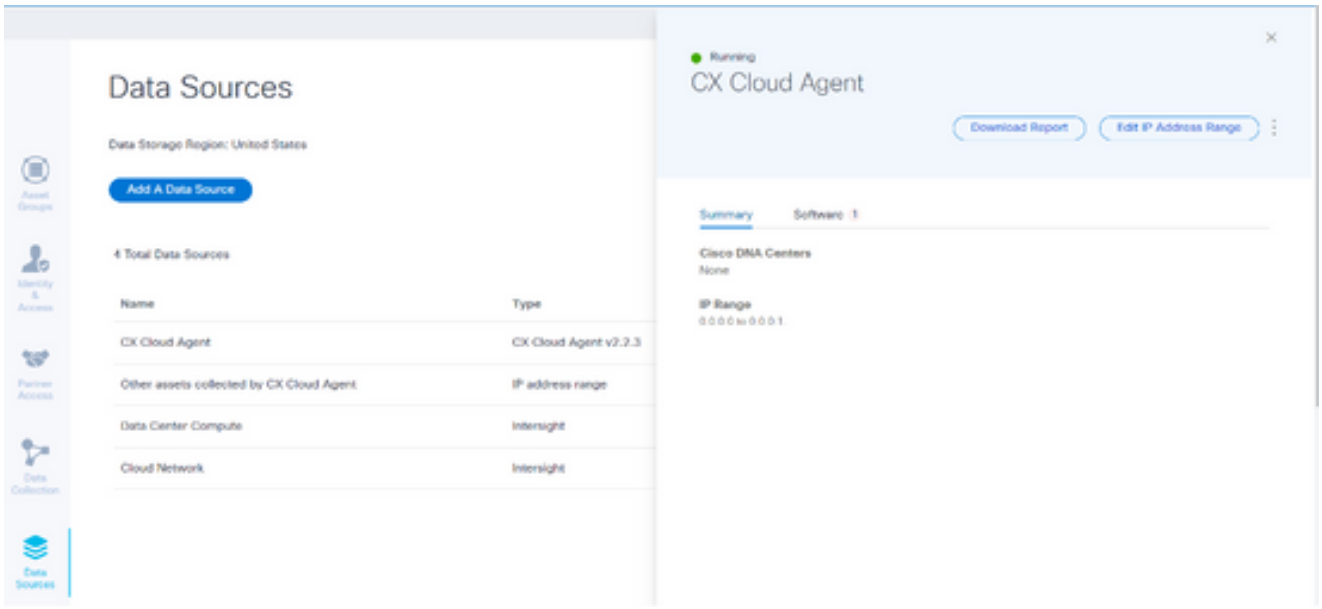


Bestätigung

Bearbeiten von IP-Bereichen

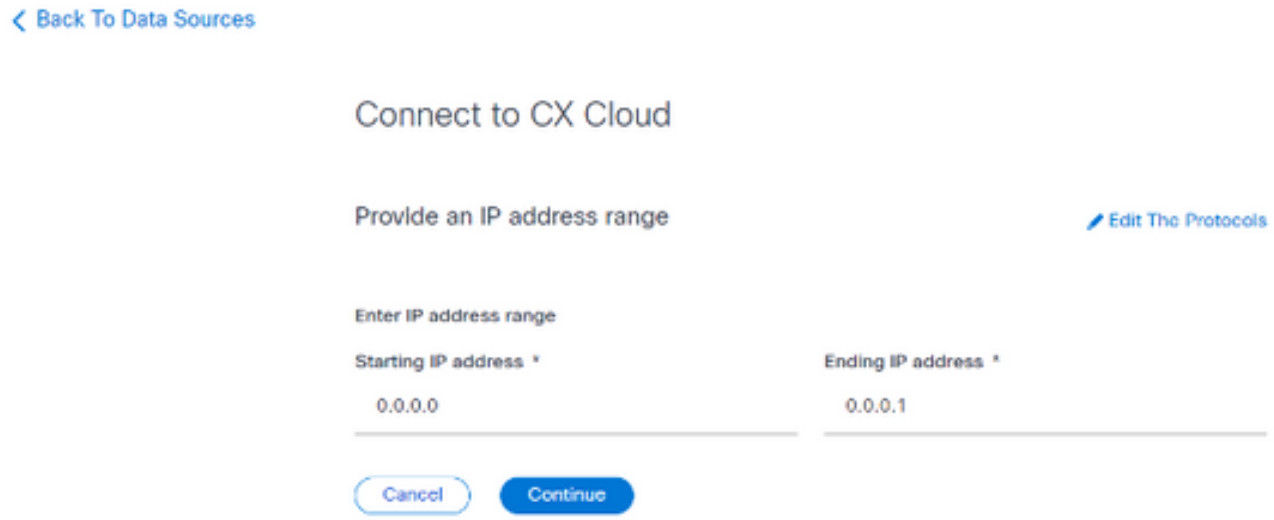
So bearbeiten Sie einen IP-Bereich

1. Navigieren Sie in das Fenster Datenquellen.



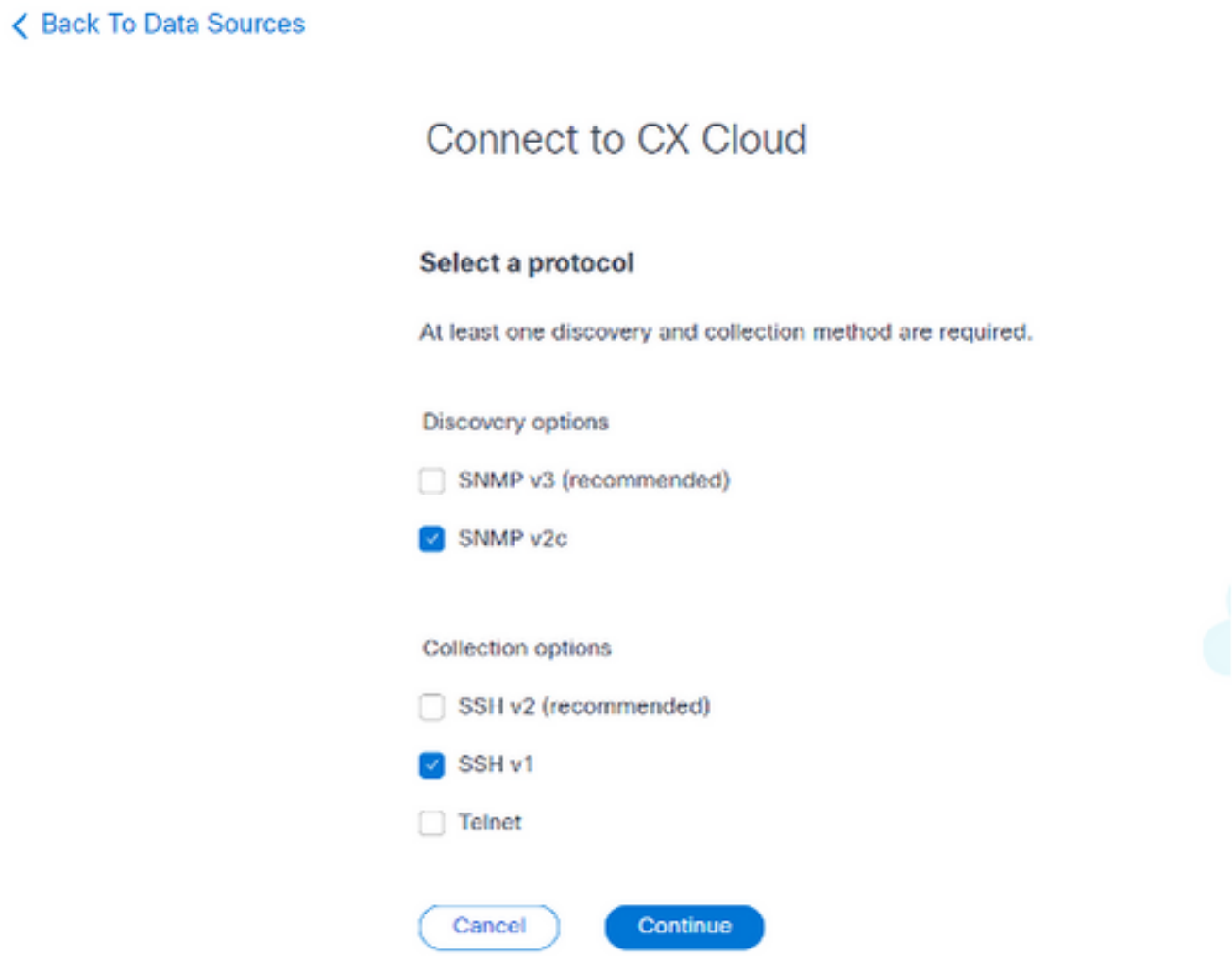
Datenquellen

2. Klicken Sie auf den CX Cloud Agent, der die Bearbeitung des IP-Bereichs in Datenquellen erfordert. Das Detailfenster wird geöffnet.
3. Klicken Sie auf IP-Adressbereich bearbeiten. Das Fenster Verbindung mit CX Cloud herstellen wird geöffnet.



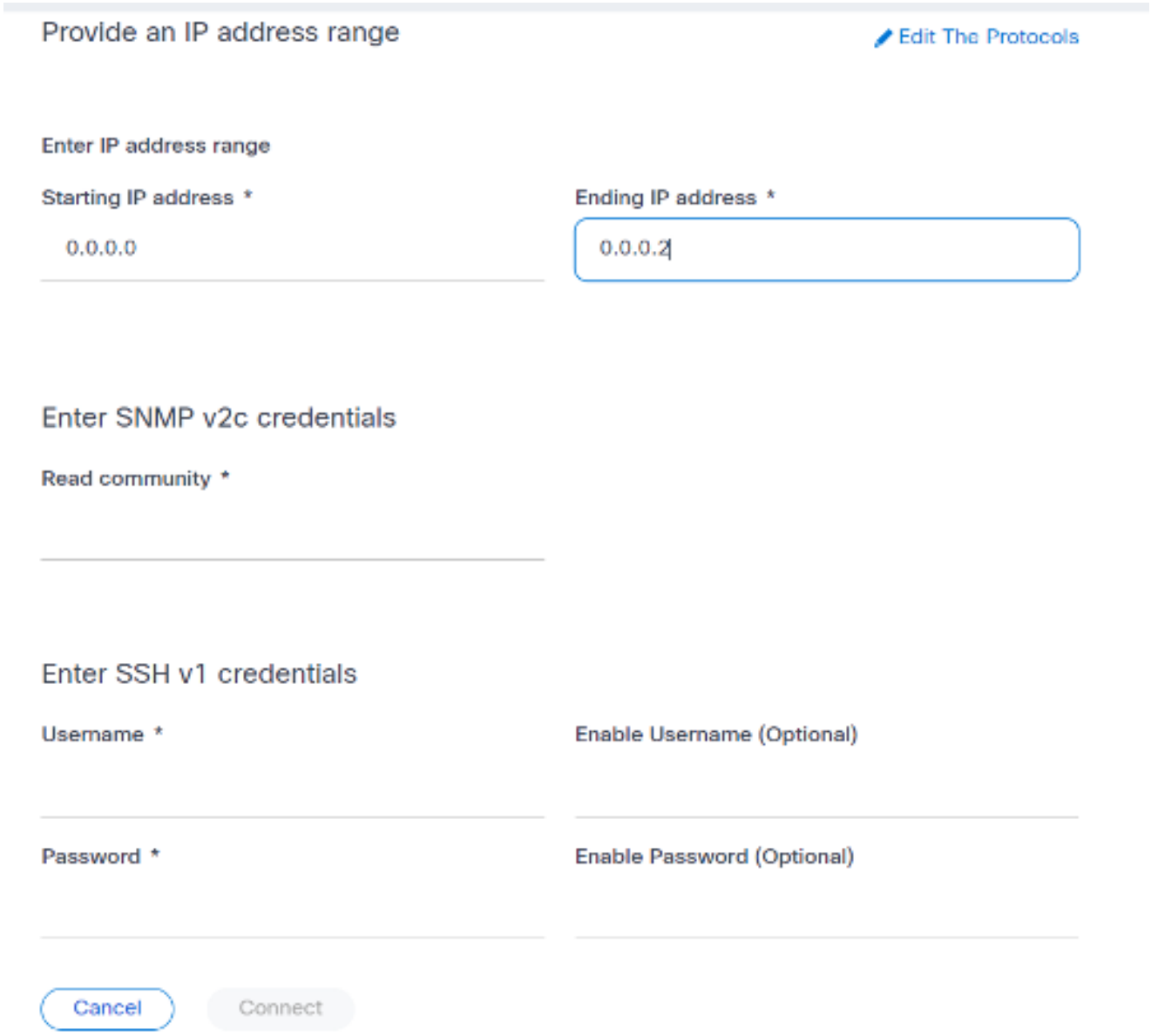
Bereitstellen eines IP-Bereichs

4. Aktualisieren Sie die neuen IPs in den Feldern für die Start-IP-Adresse und die End-IP-Adresse.
5. Klicken Sie auf den Link Protokolle bearbeiten. Das Fenster Verbindung mit der CX Cloud herstellen - Protokoll auswählen wird geöffnet.



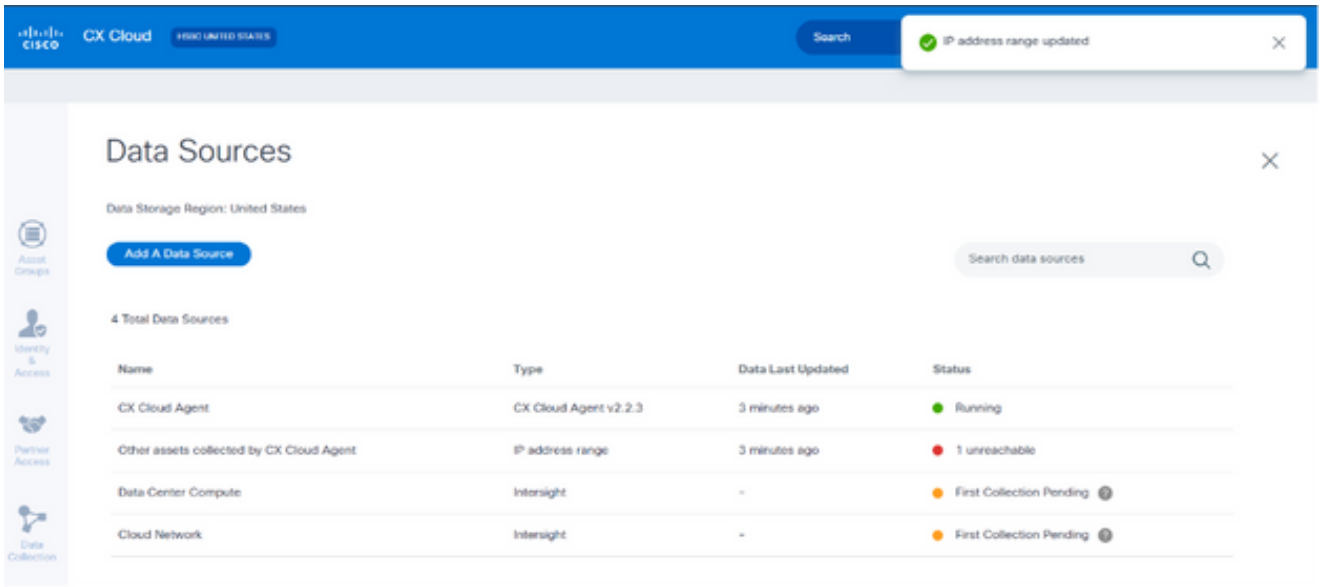
Protokoll auswählen

6. Wählen Sie die entsprechenden Protokolle aus, indem Sie auf die entsprechenden Kontrollkästchen klicken.
7. Klicken Sie auf Continue (Weiter). Das Fenster Geben Sie einen IP-Adressbereich ein wird geöffnet.



Anmeldeinformationen eingeben

8. Geben Sie die Anmeldeinformationen für die Konfiguration ein.
9. Klicken Sie auf Verbinden. Das Fenster Datenquellen wird geöffnet, und es wird eine Bestätigungsmeldung angezeigt.



Bestätigung

Hinweis: Die Bestätigungsmeldung stellt nicht sicher, dass die Geräte im bearbeiteten Bereich erreichbar sind und die Anmeldedaten akzeptiert wurden.

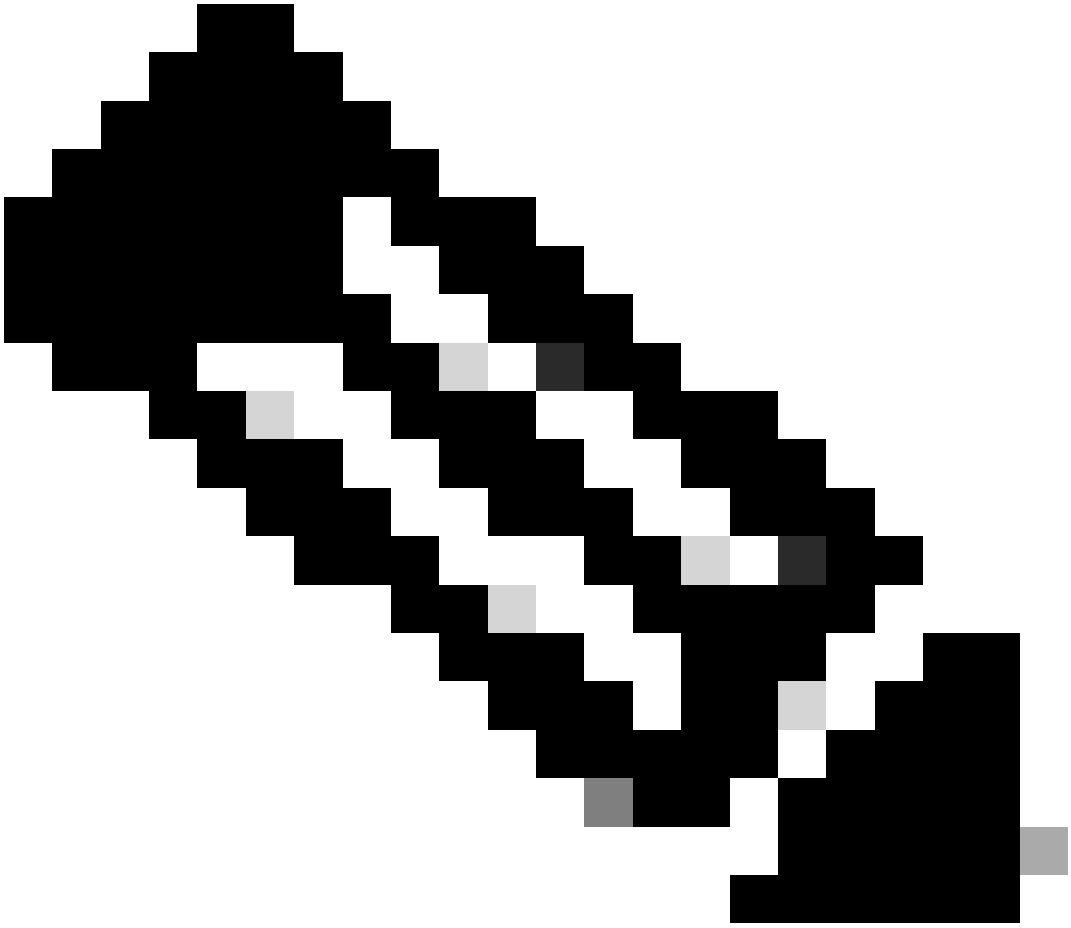
Von mehreren Controllern erkannte Geräte

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

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

Planen von Diagnosescans

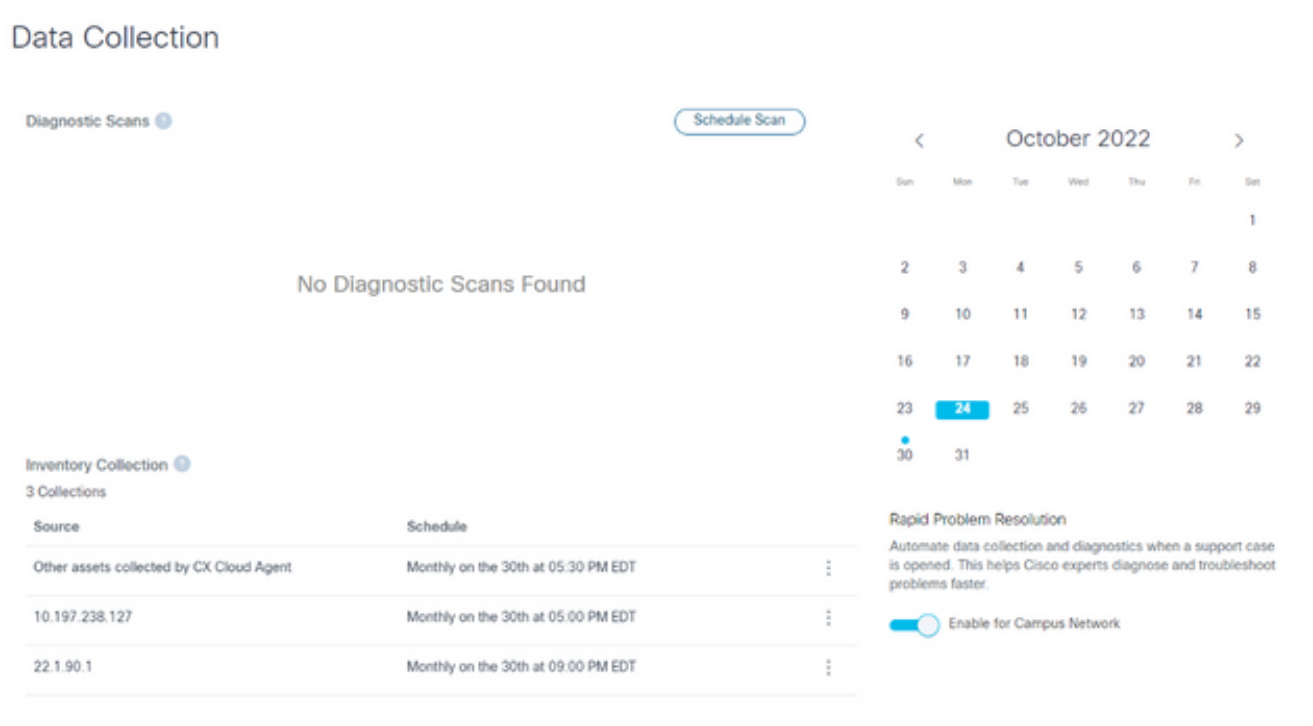
Kunden können On-Demand-Diagnosen in der CX Cloud planen.



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

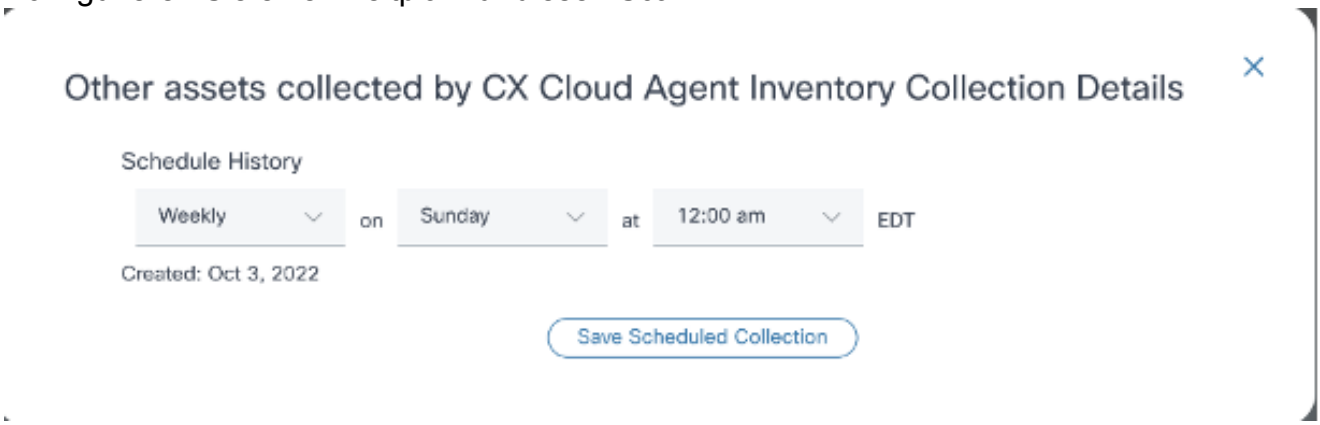
So planen Sie Diagnosescans:

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



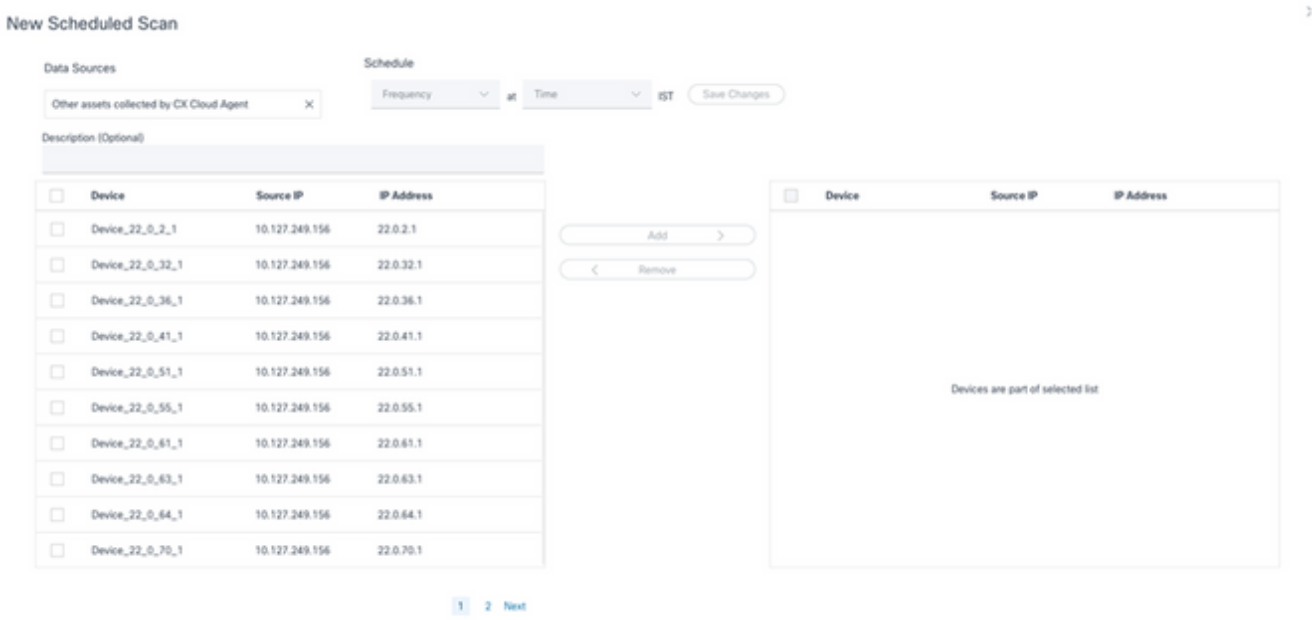
Datensammlung

4. Konfigurieren Sie einen Zeitplan für diesen Scan.



Scan-Zeitplan konfigurieren

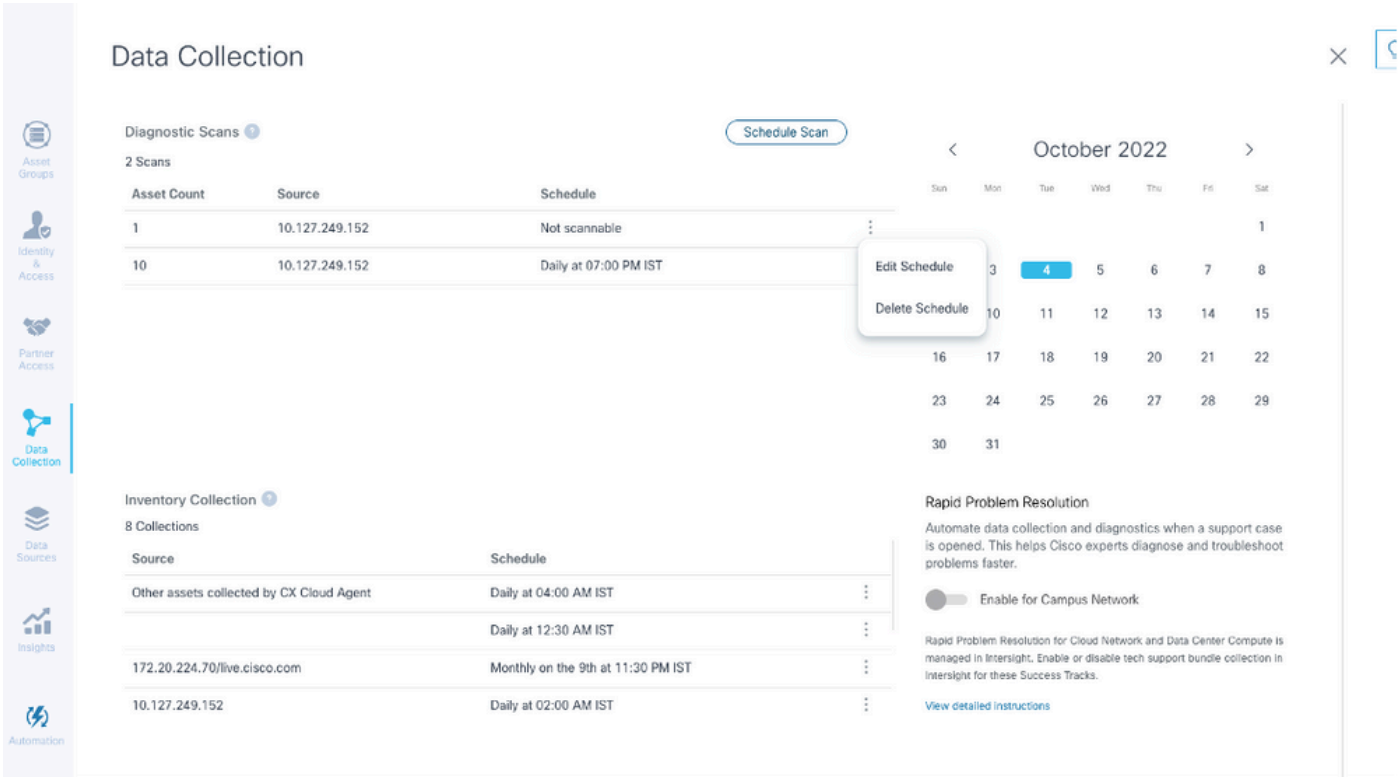
5. Wählen Sie in der Geräteliste alle Geräte für den Scan aus, und klicken Sie auf Hinzufügen.



Einen Scan ansetzen

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

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



Datenerfassung mit Optionen zum Bearbeiten und Löschen von Zeitplänen

Bereitstellung und Netzwerkkonfiguration

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

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

OVA-Bereitstellung

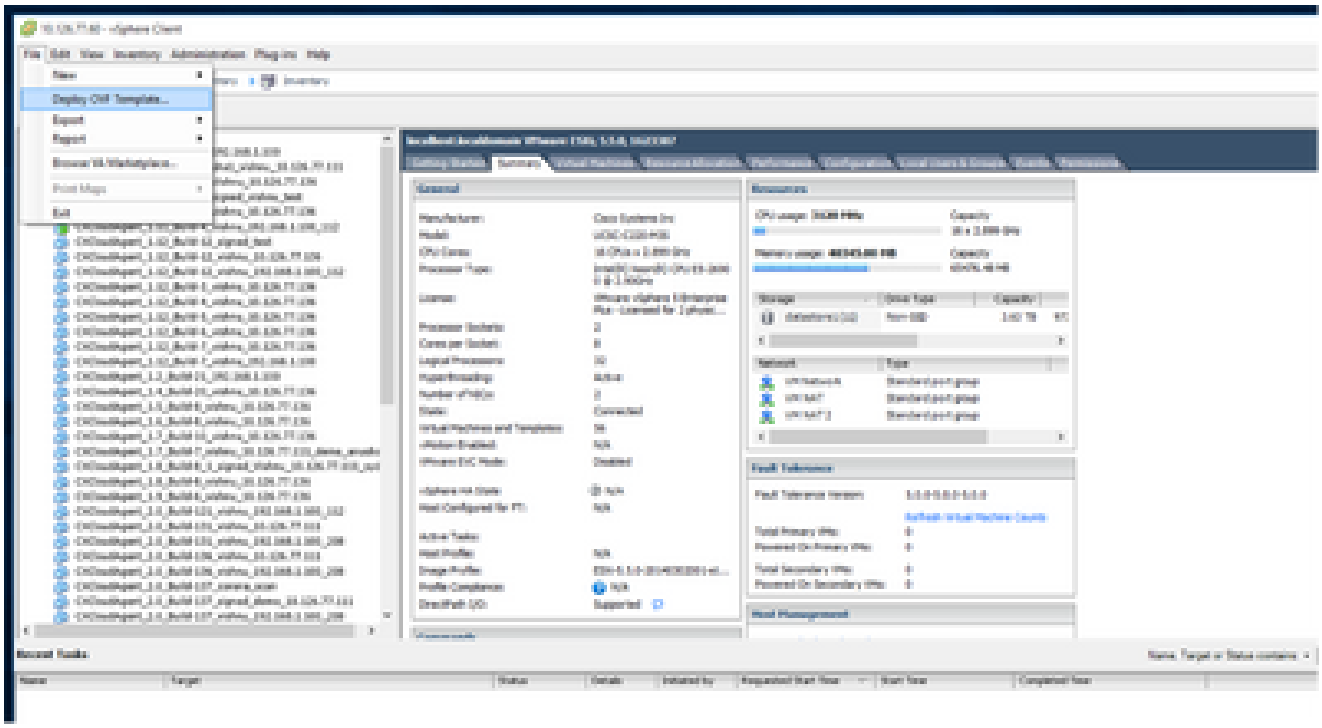
Installation von Thick Client ESXi 5.5/6.0

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

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

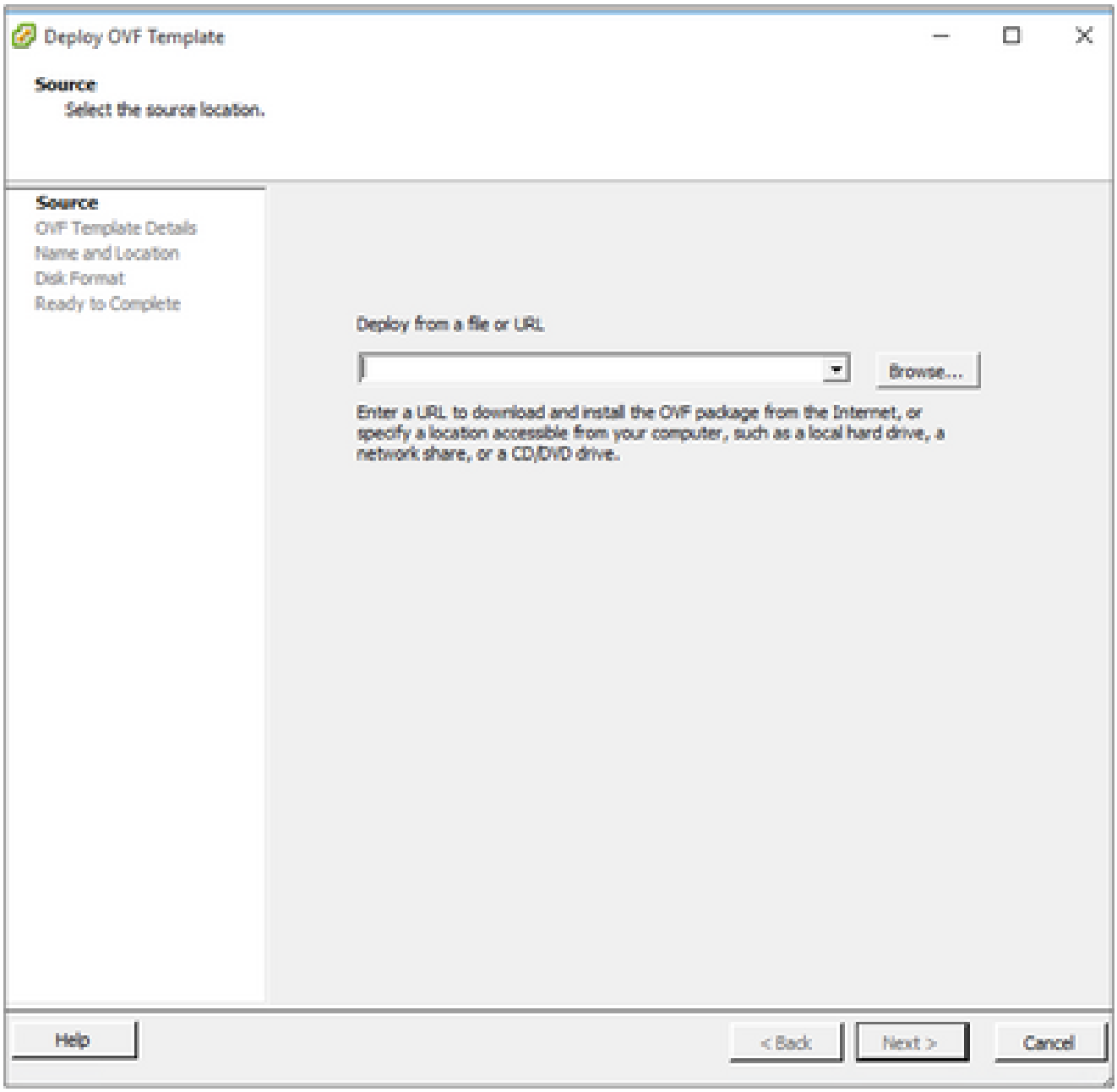
Anmelden

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



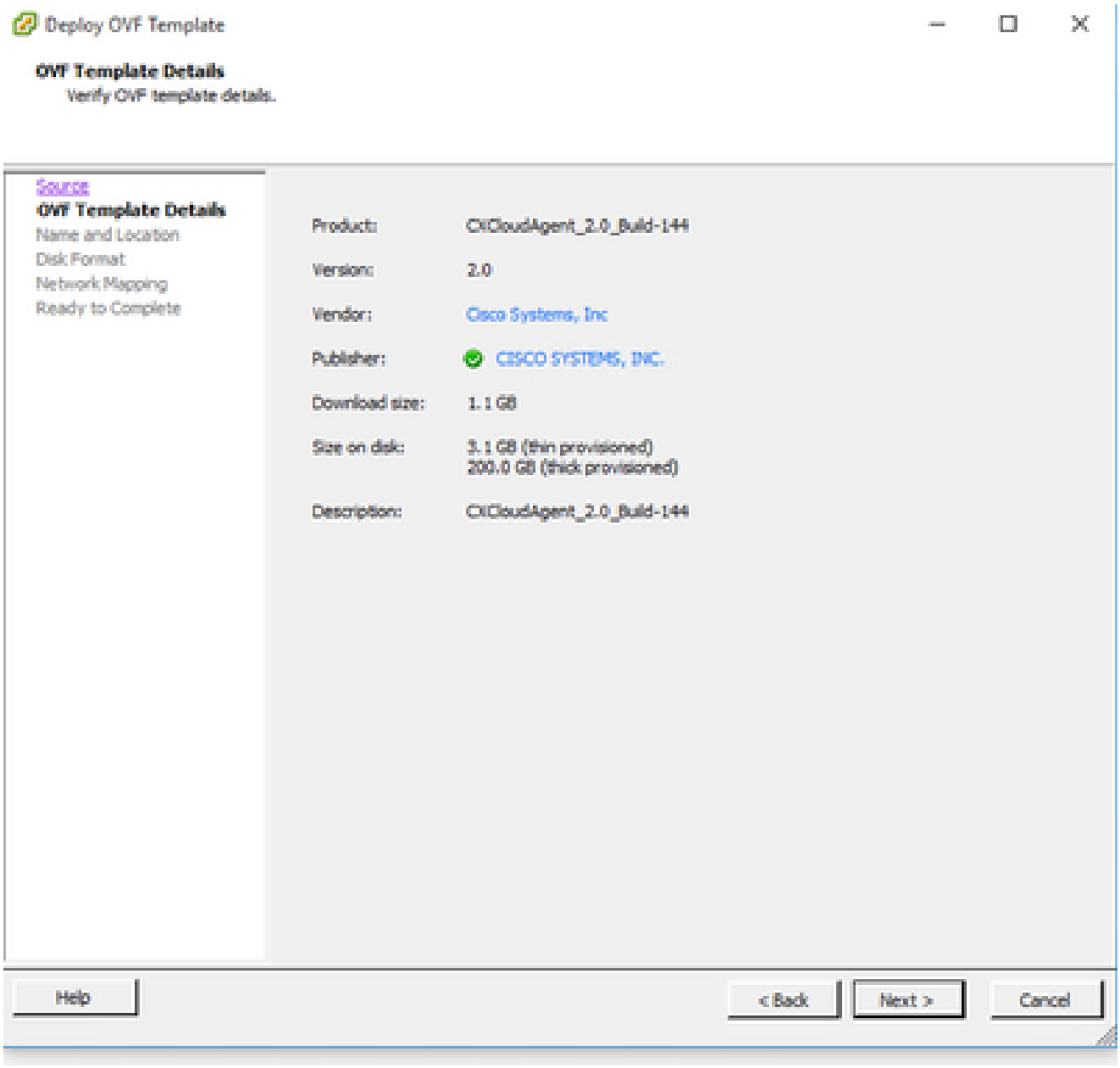
vSphere-Client

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



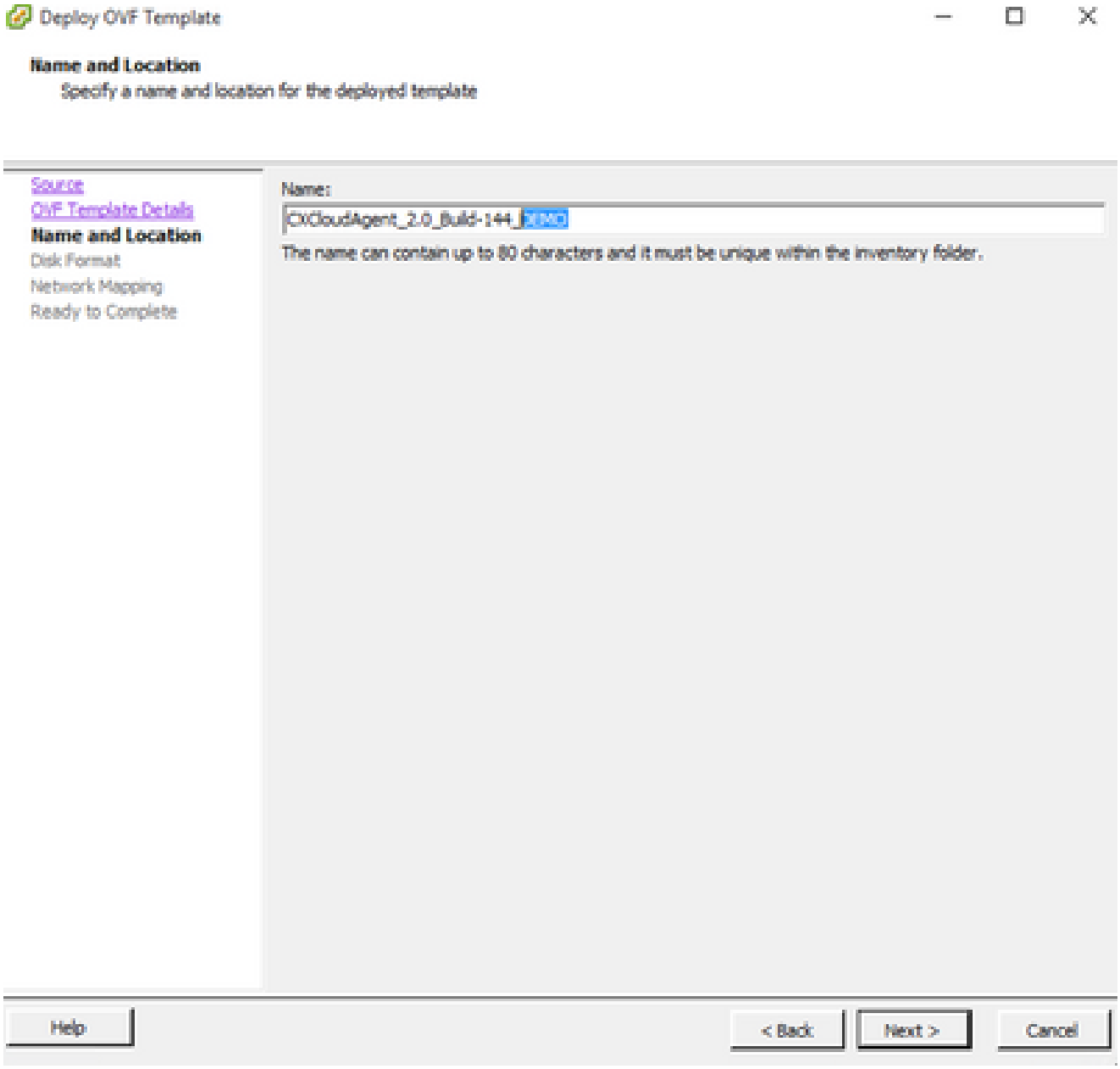
OVA-Pfad

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



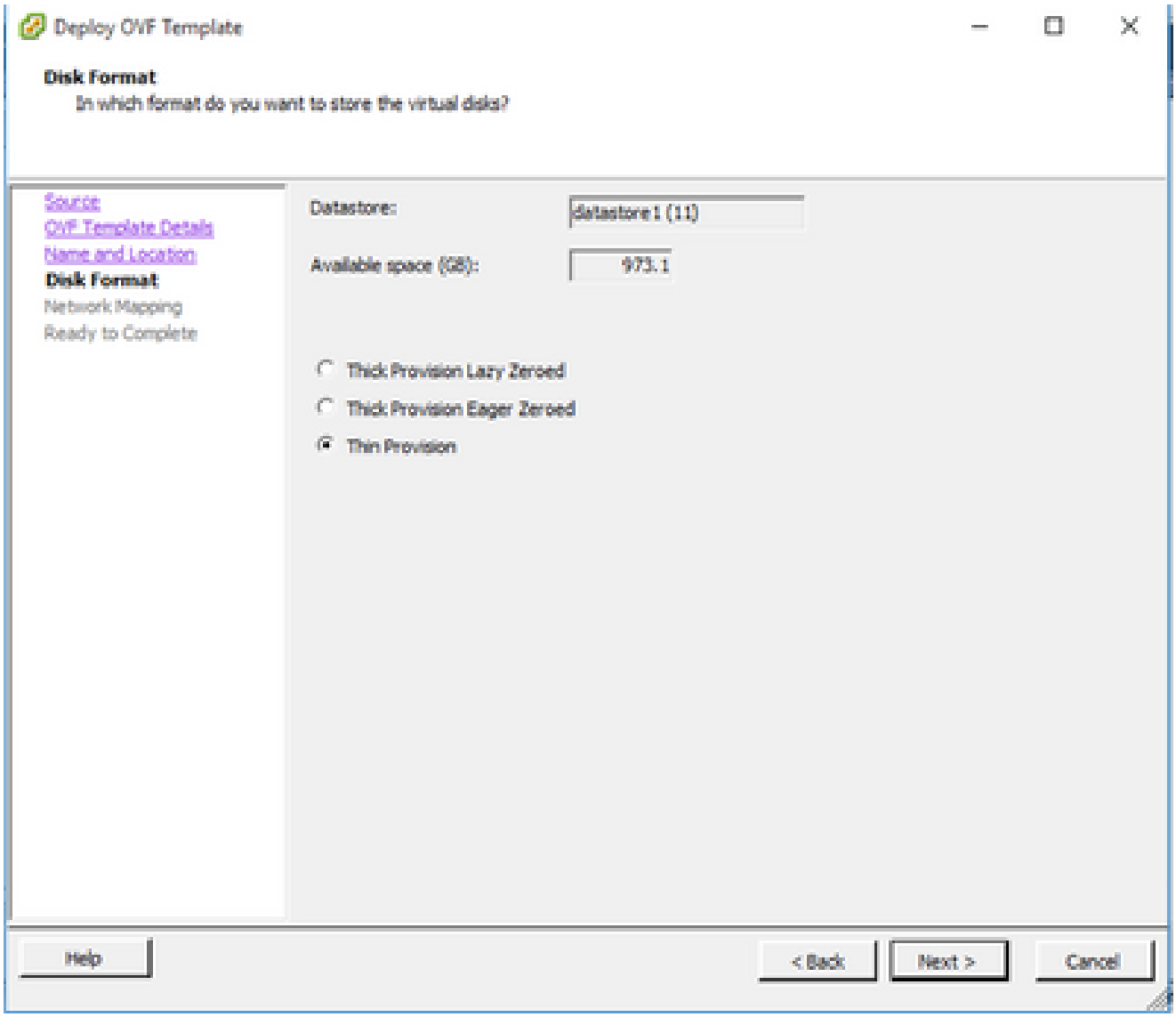
Vorlagendetails

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



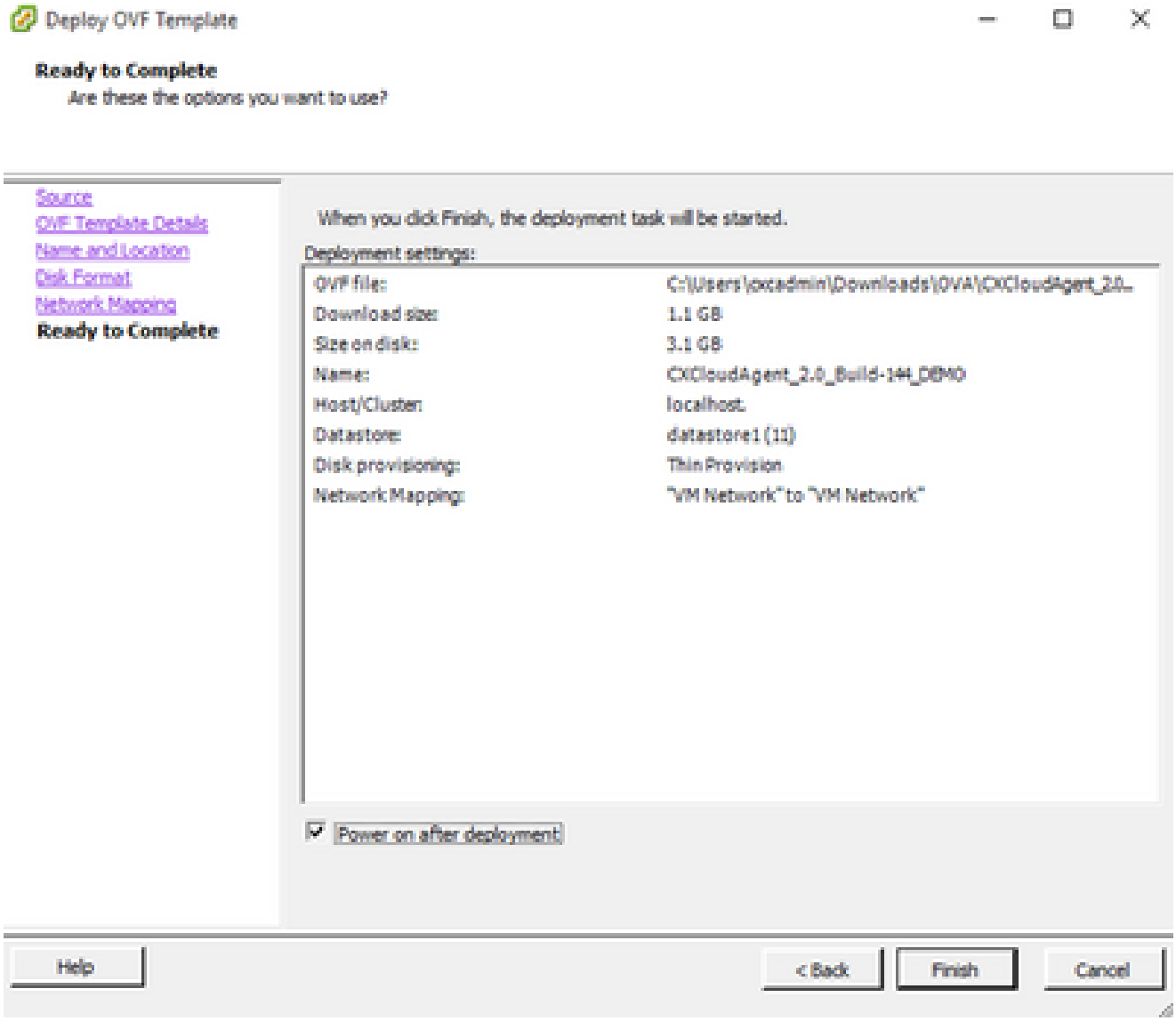
Name und Standort

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



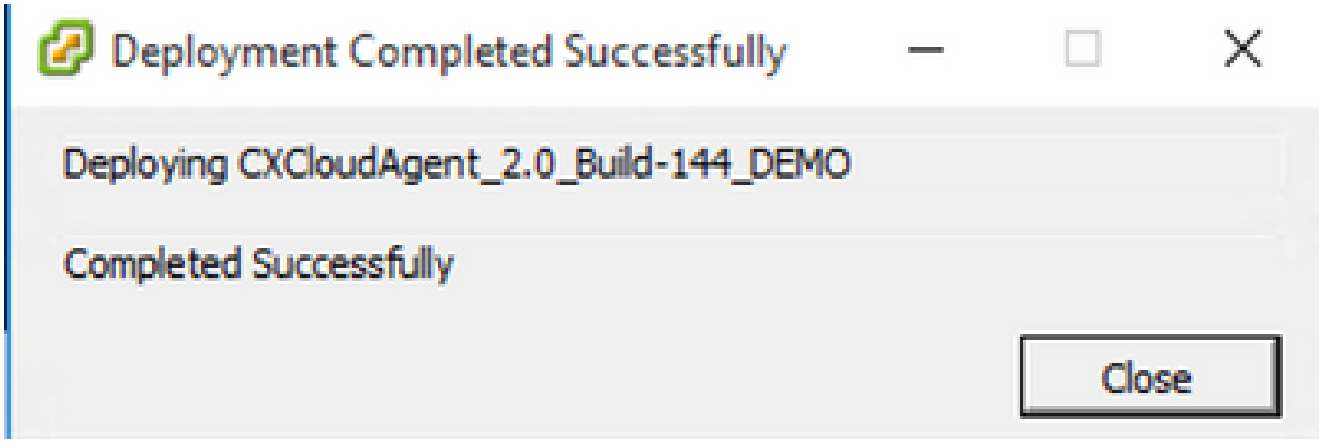
Datenträgerformatierung

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



Bereit zur Fertigstellung

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



Bereitstellung abgeschlossen

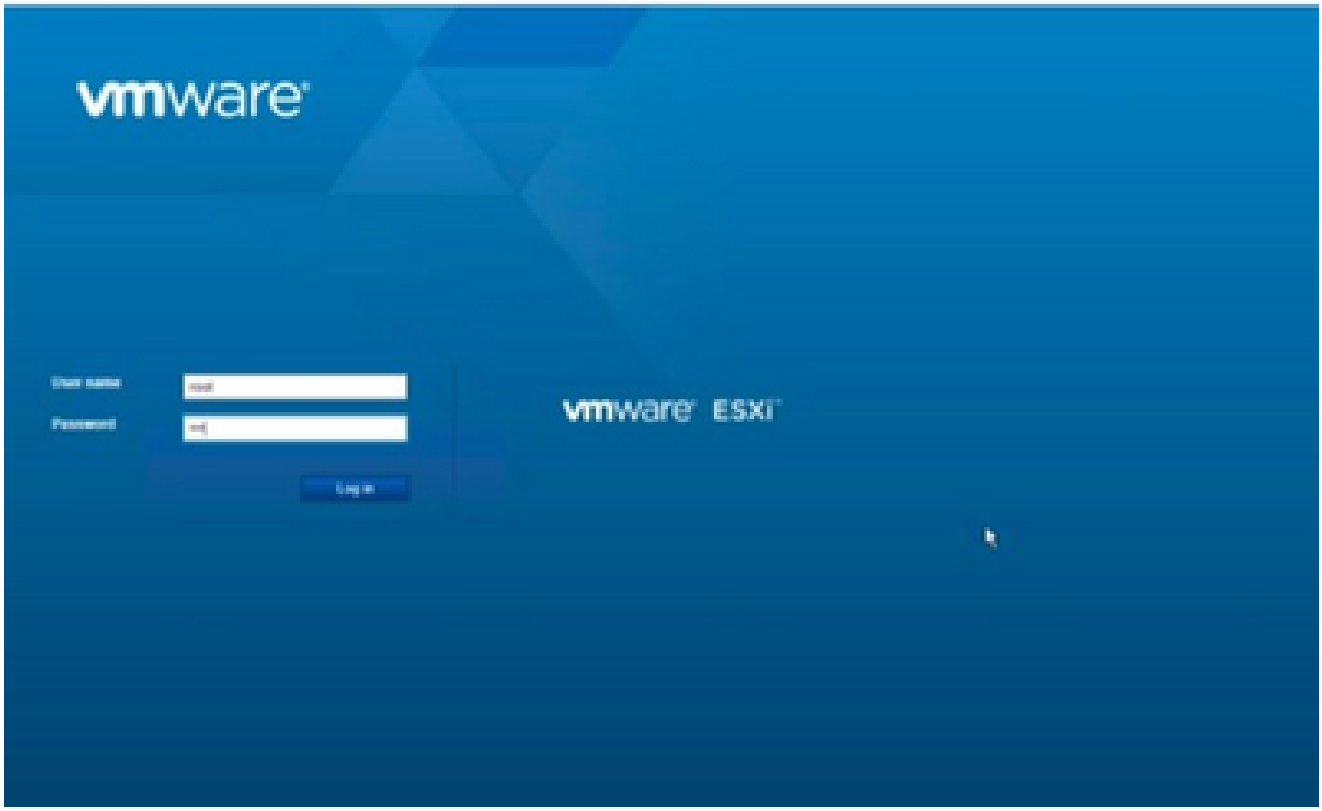
8. Wählen Sie das bereitgestellte virtuelle System aus, öffnen Sie die Konsole, und gehen Sie

zu Network Configuration, um mit den nächsten Schritten fortzufahren.

Installation von Web Client ESXi 6.0

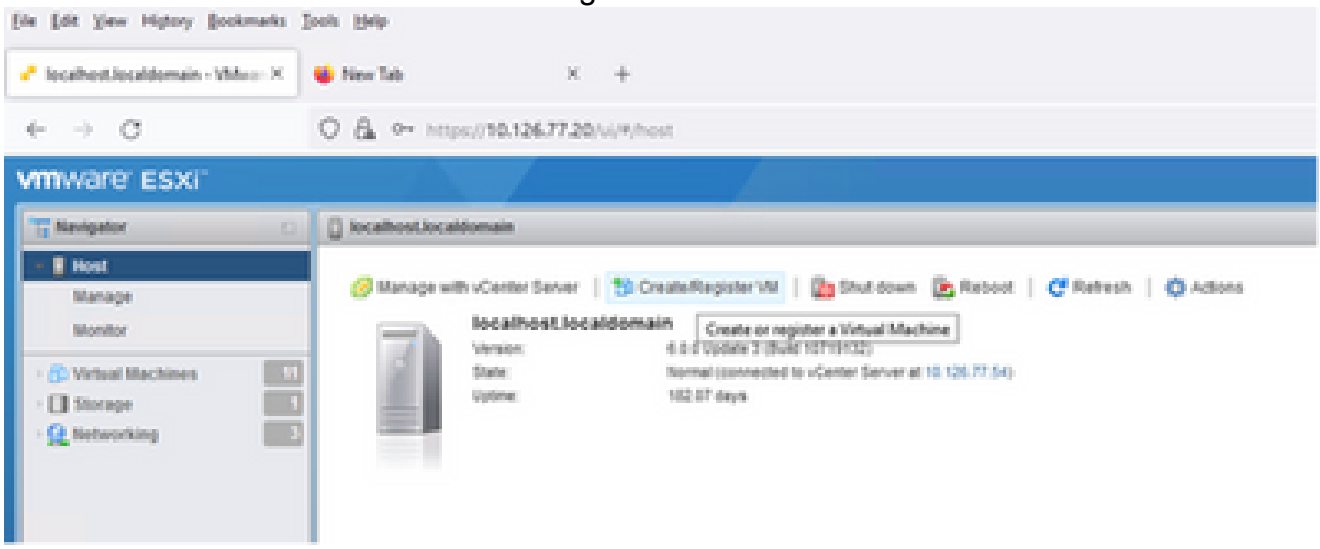
Dieser Client stellt CX Cloud Agent OVA mithilfe von vSphere Web bereit.

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



VMware ESXi-Anmeldung

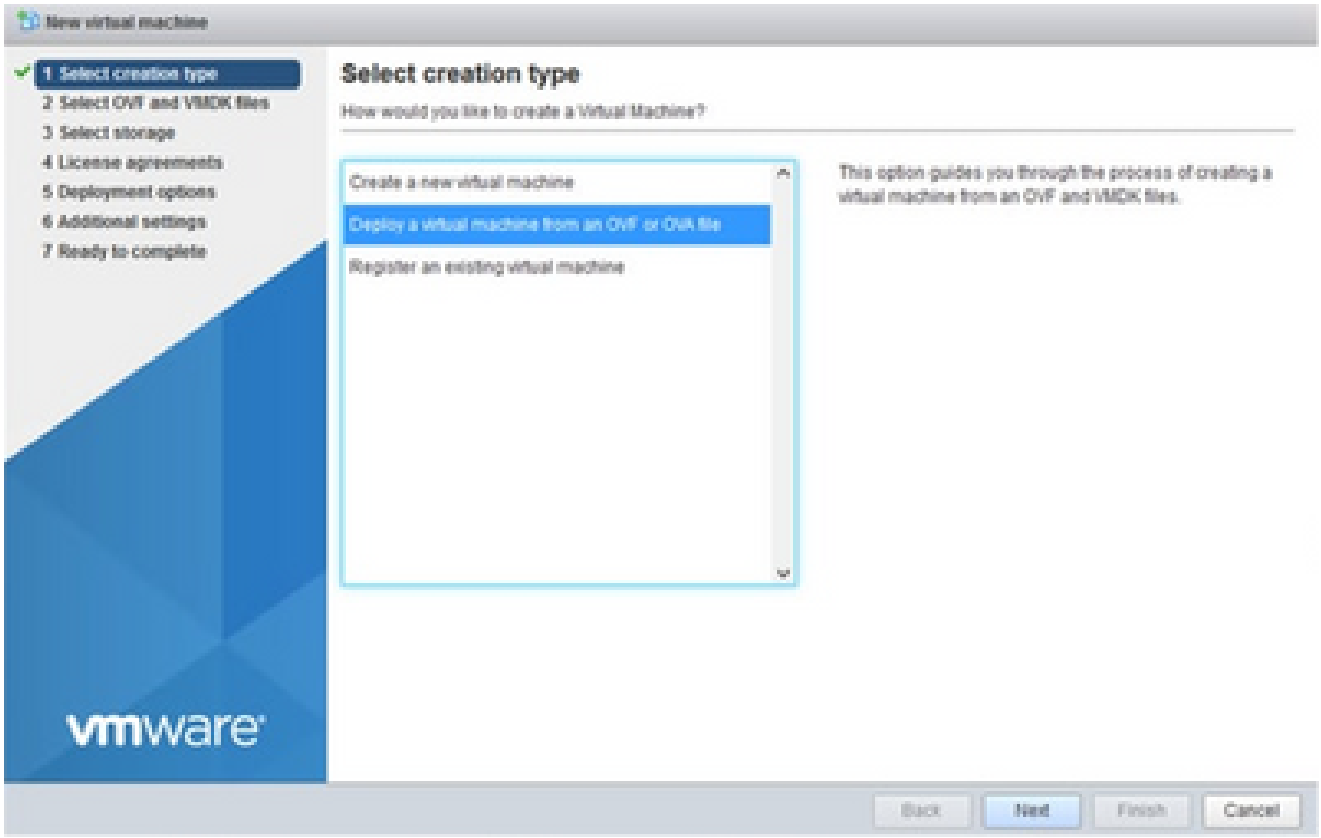
2. Wählen Sie Virtual Machine > Create/Register VM aus.



VM erstellen

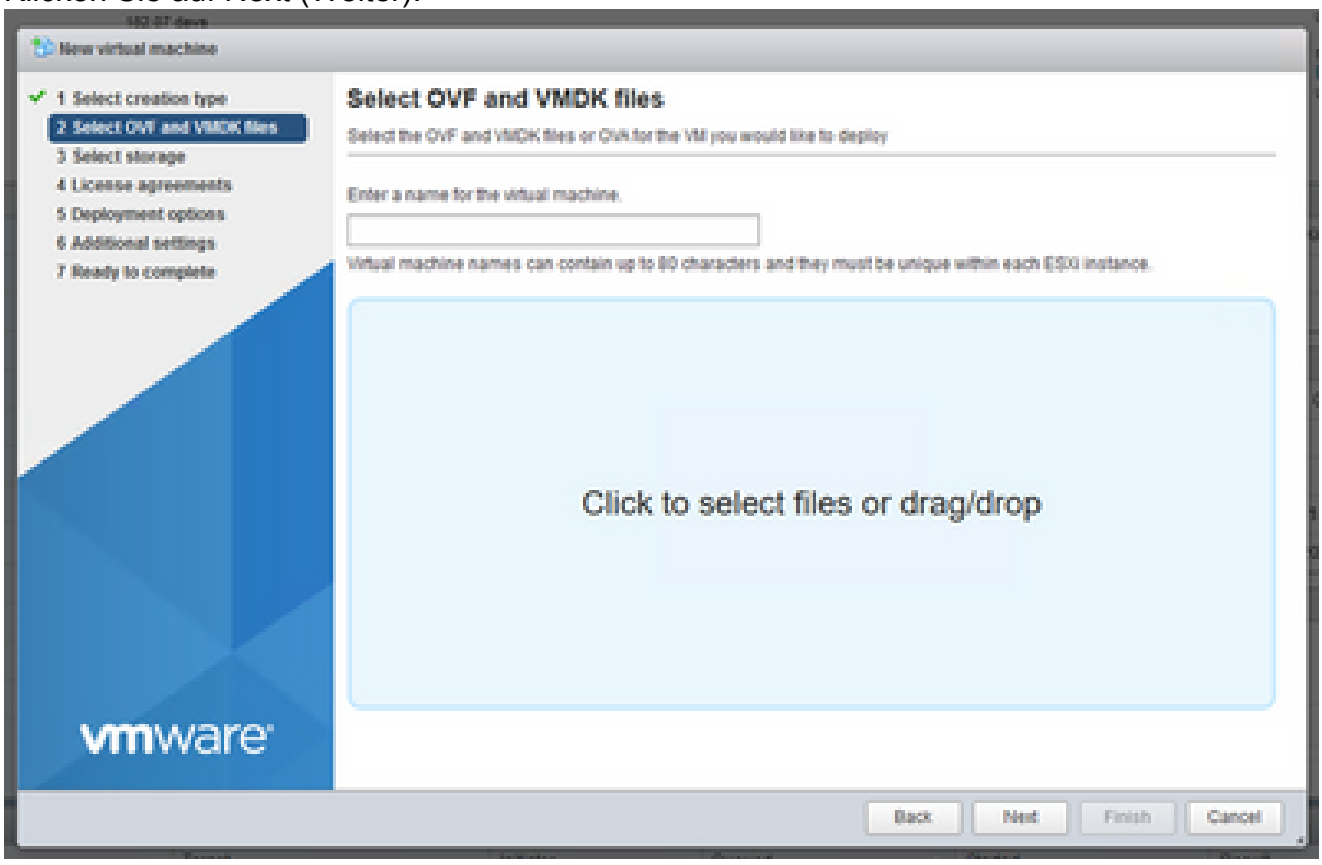
3. Wählen Sie Virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen aus und klicken

Sie auf Weiter.



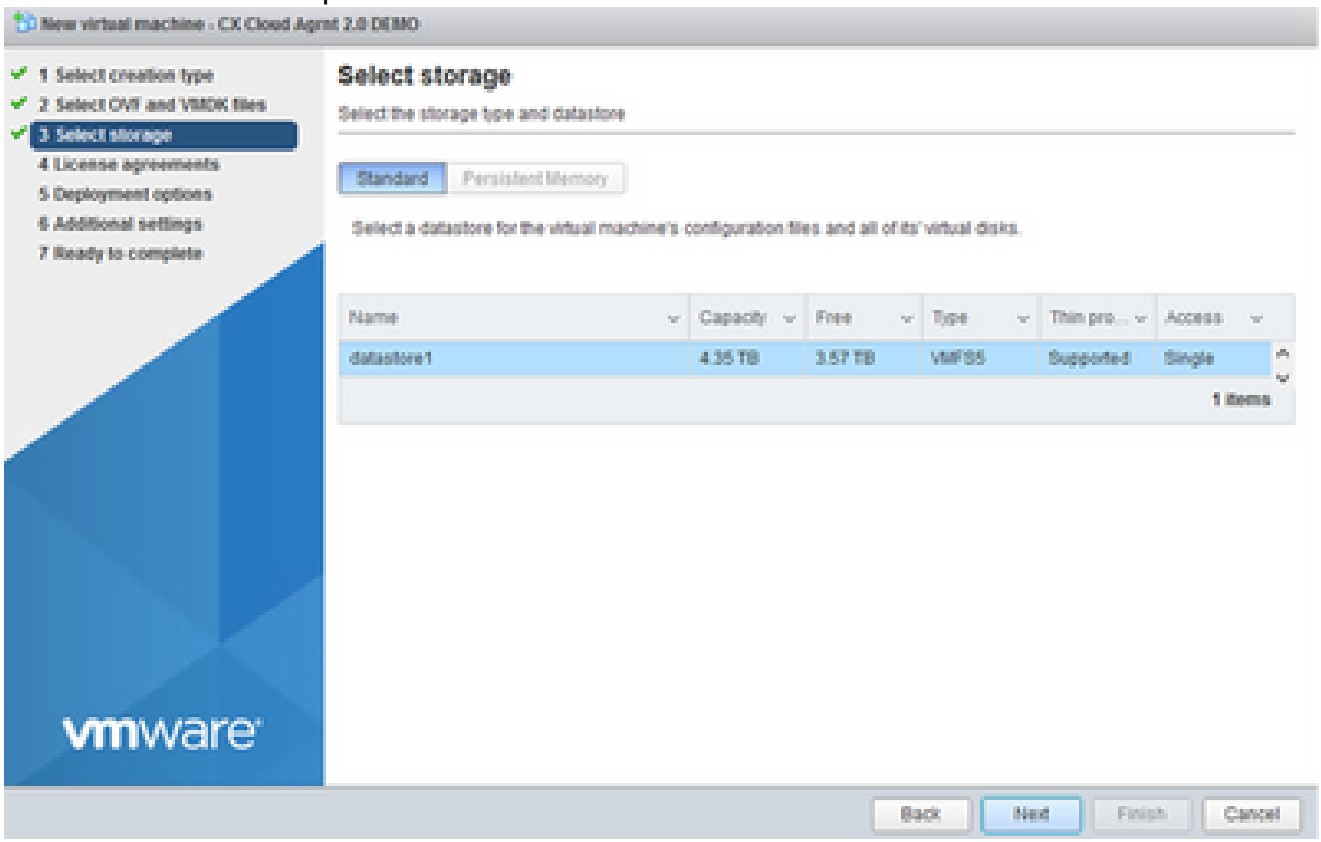
Erstellungstyp auswählen

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



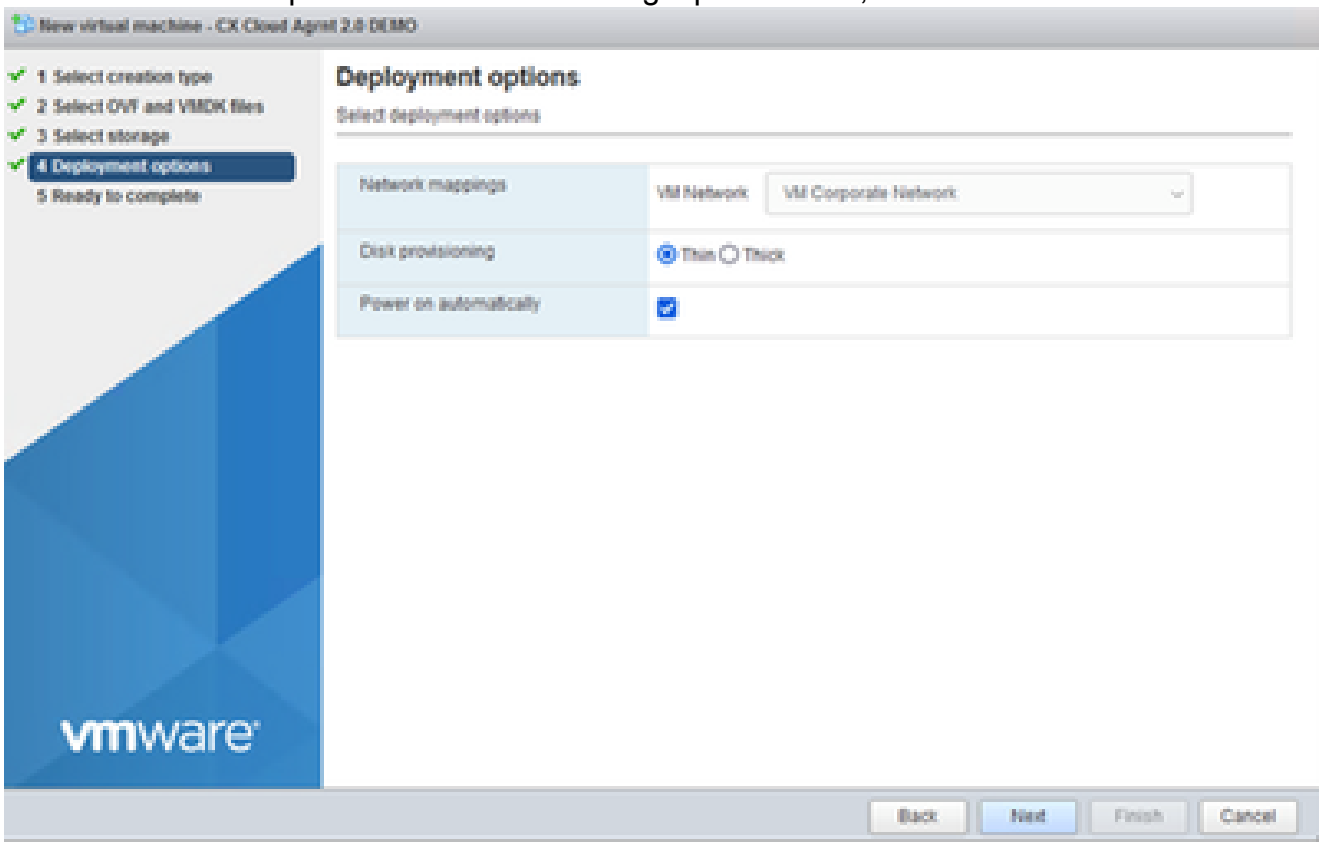
OVA-Auswahl

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



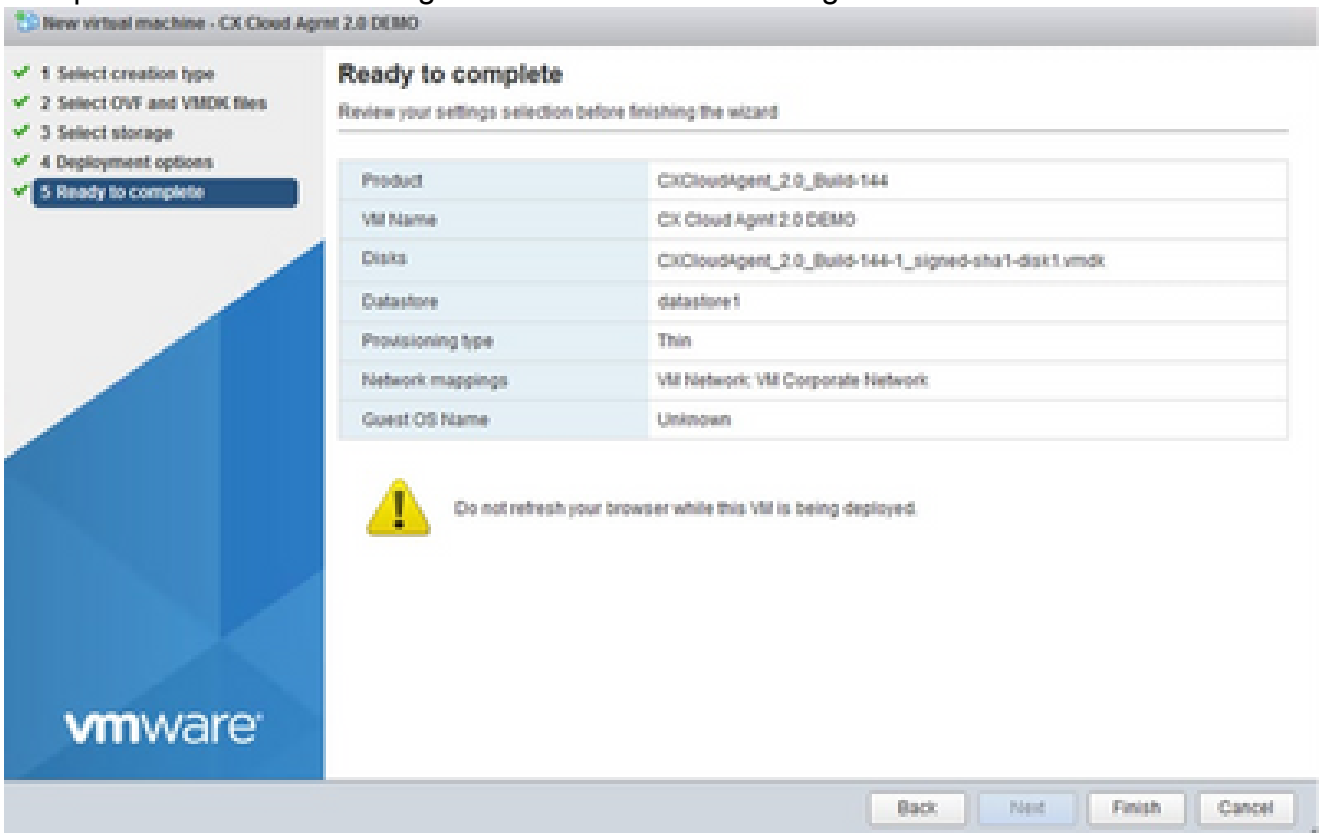
Auswahl von externem Speicher

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

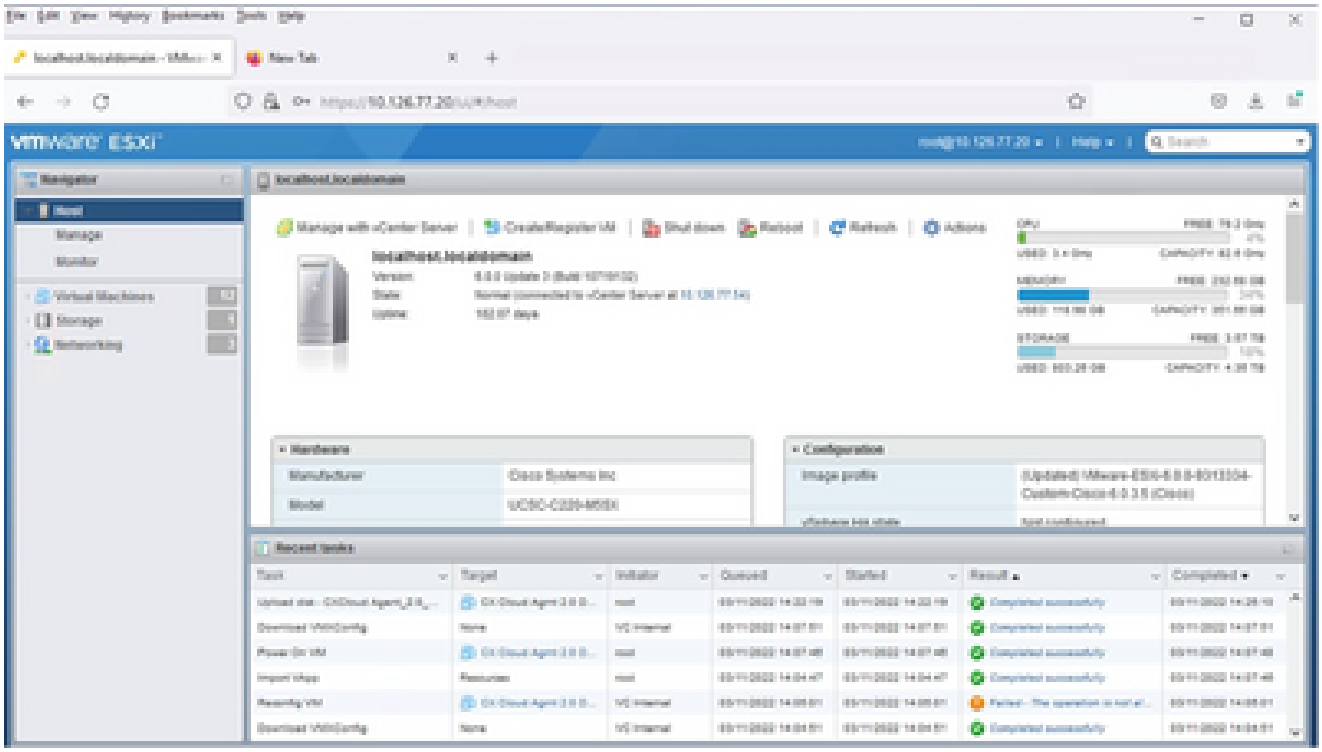


Bereitstellungsoptionen

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

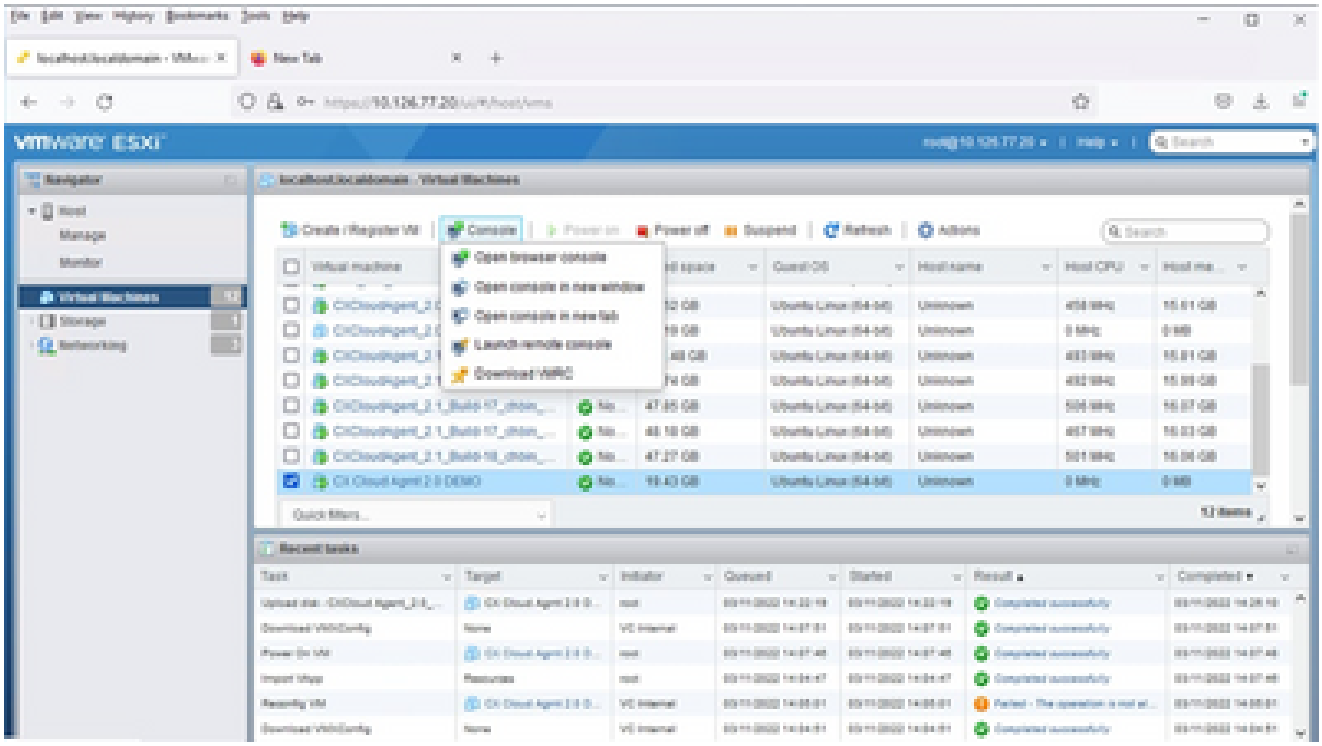


Bereit zur Fertigstellung



Abschluss erfolgreich

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



Konsole

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

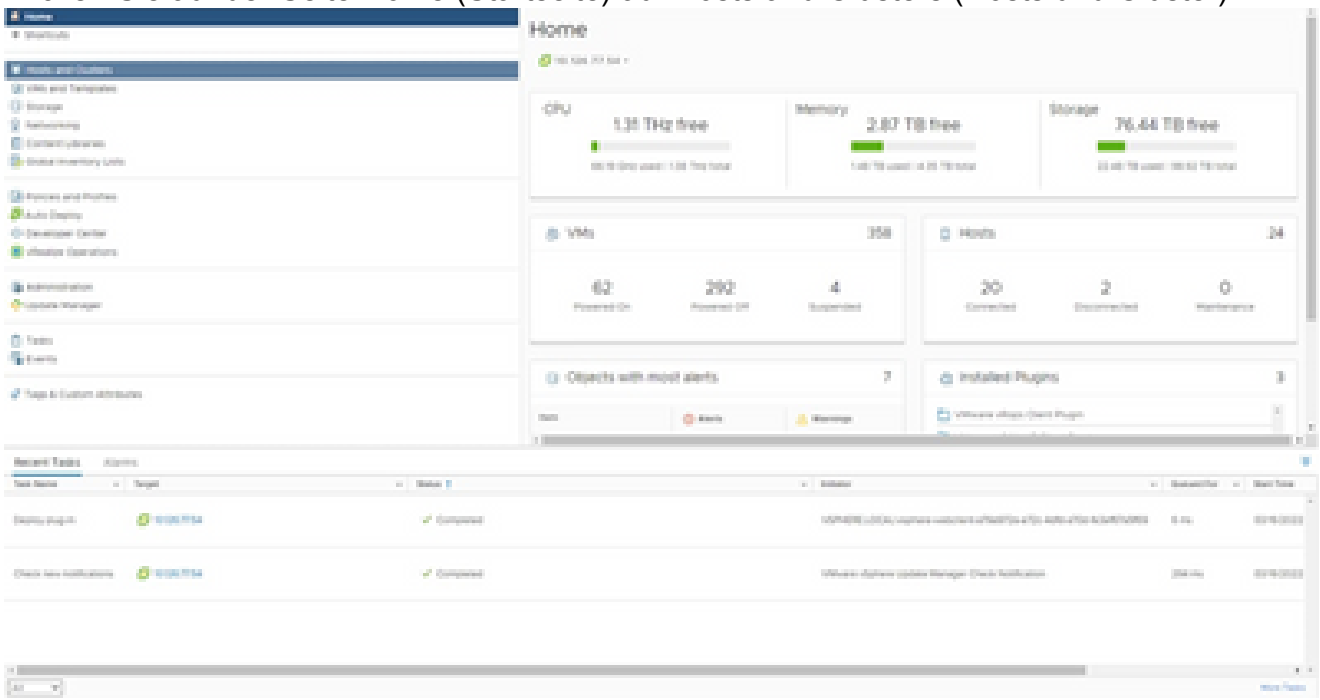
Installation von Web Client vCenter

Führen Sie die folgenden Schritte aus:

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

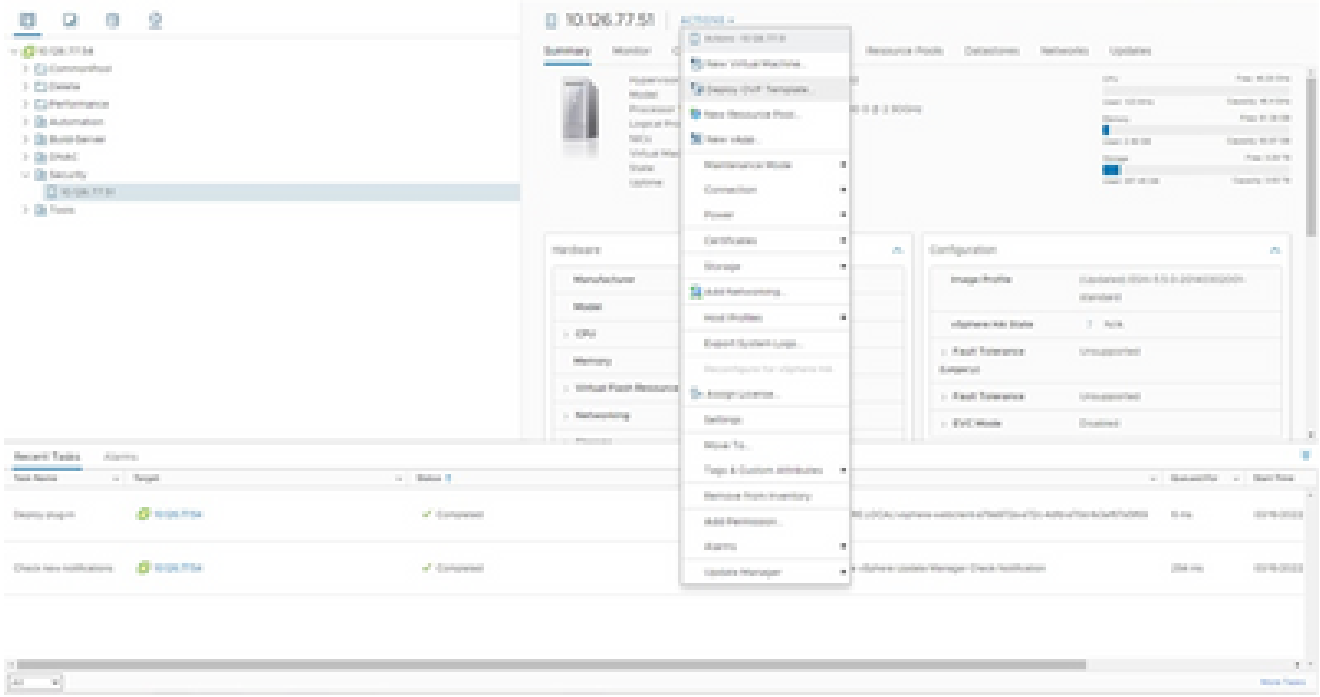
Anmelden

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

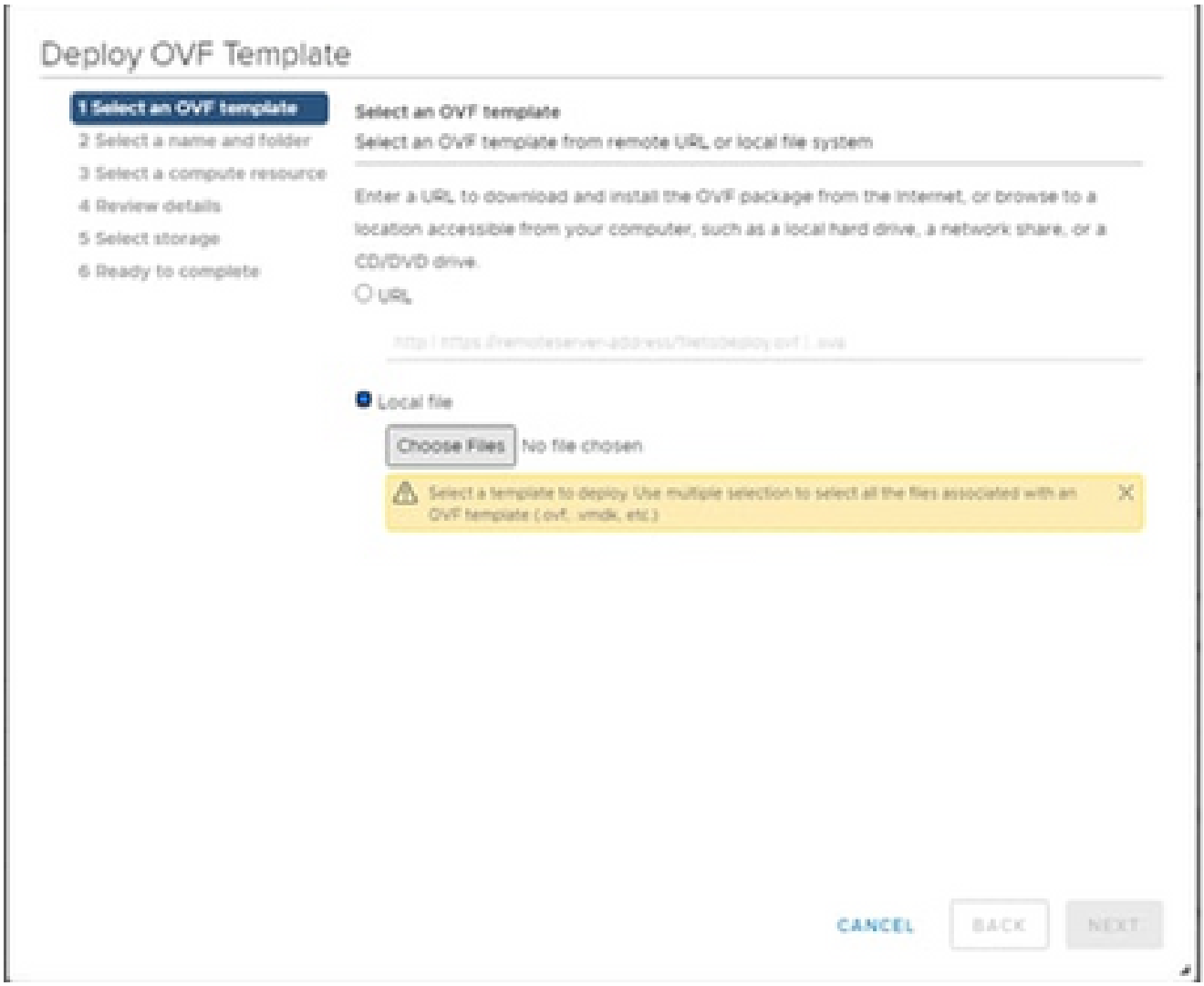


Startseite

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

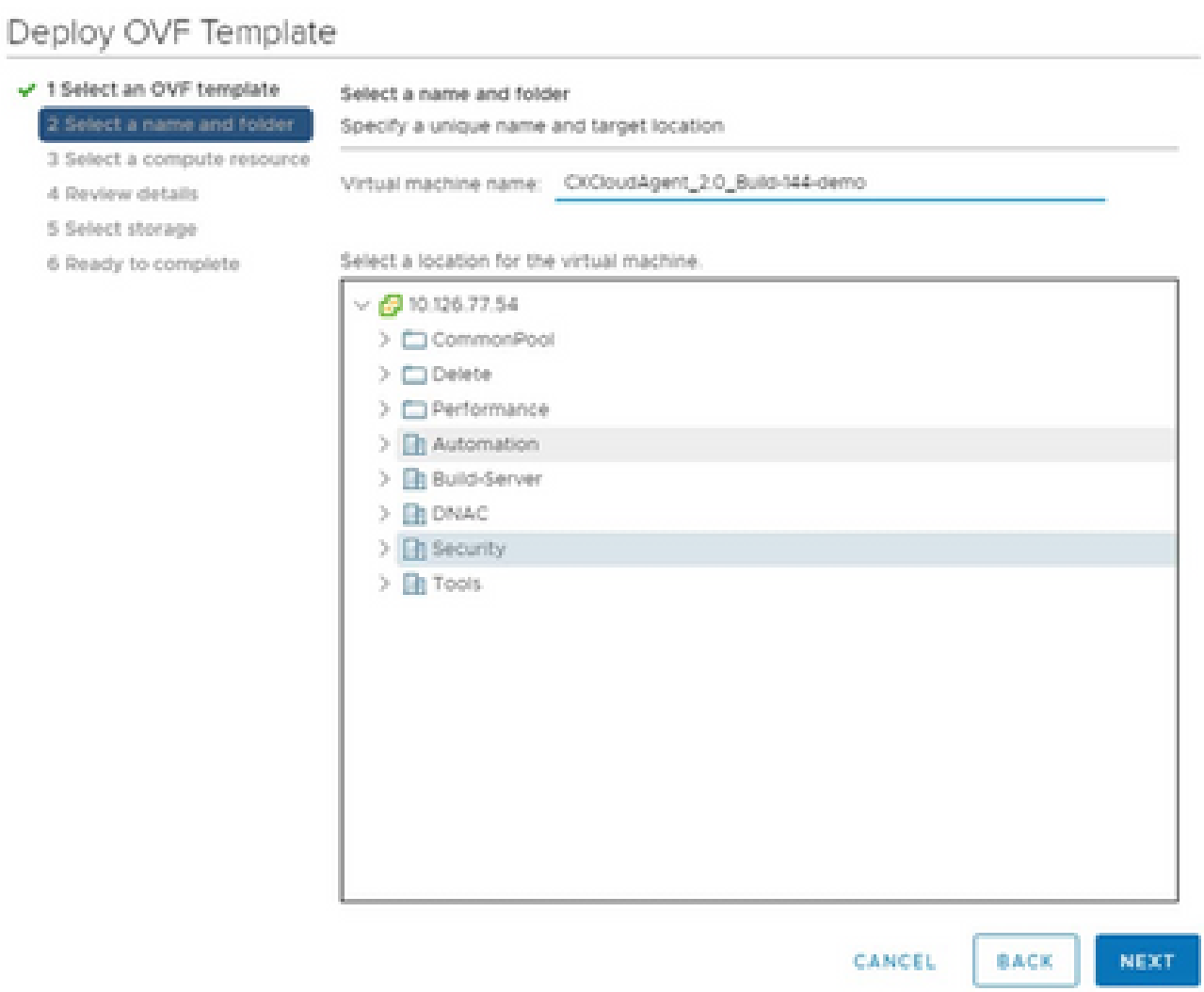


Aktionen



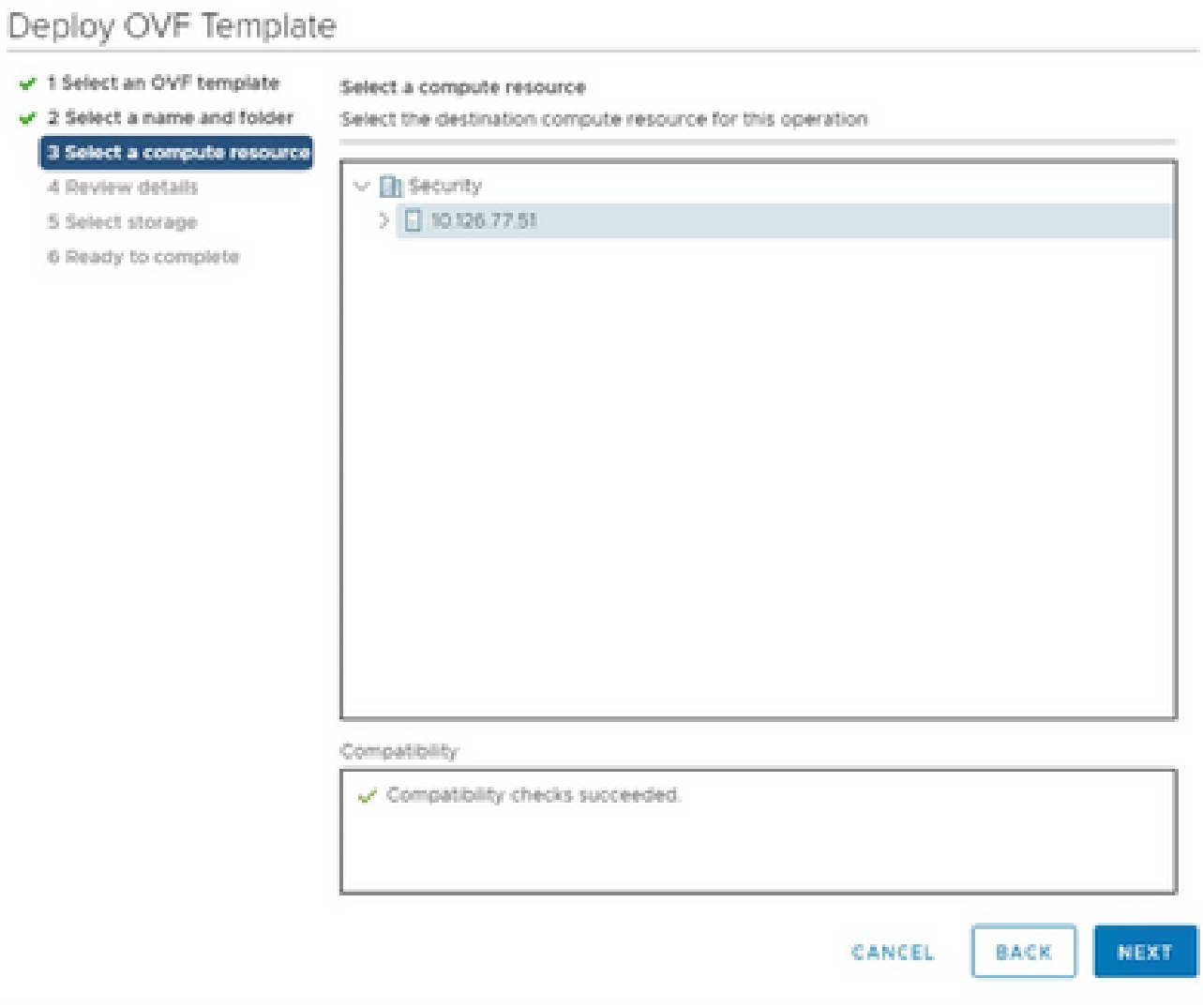
Vorlage auswählen

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



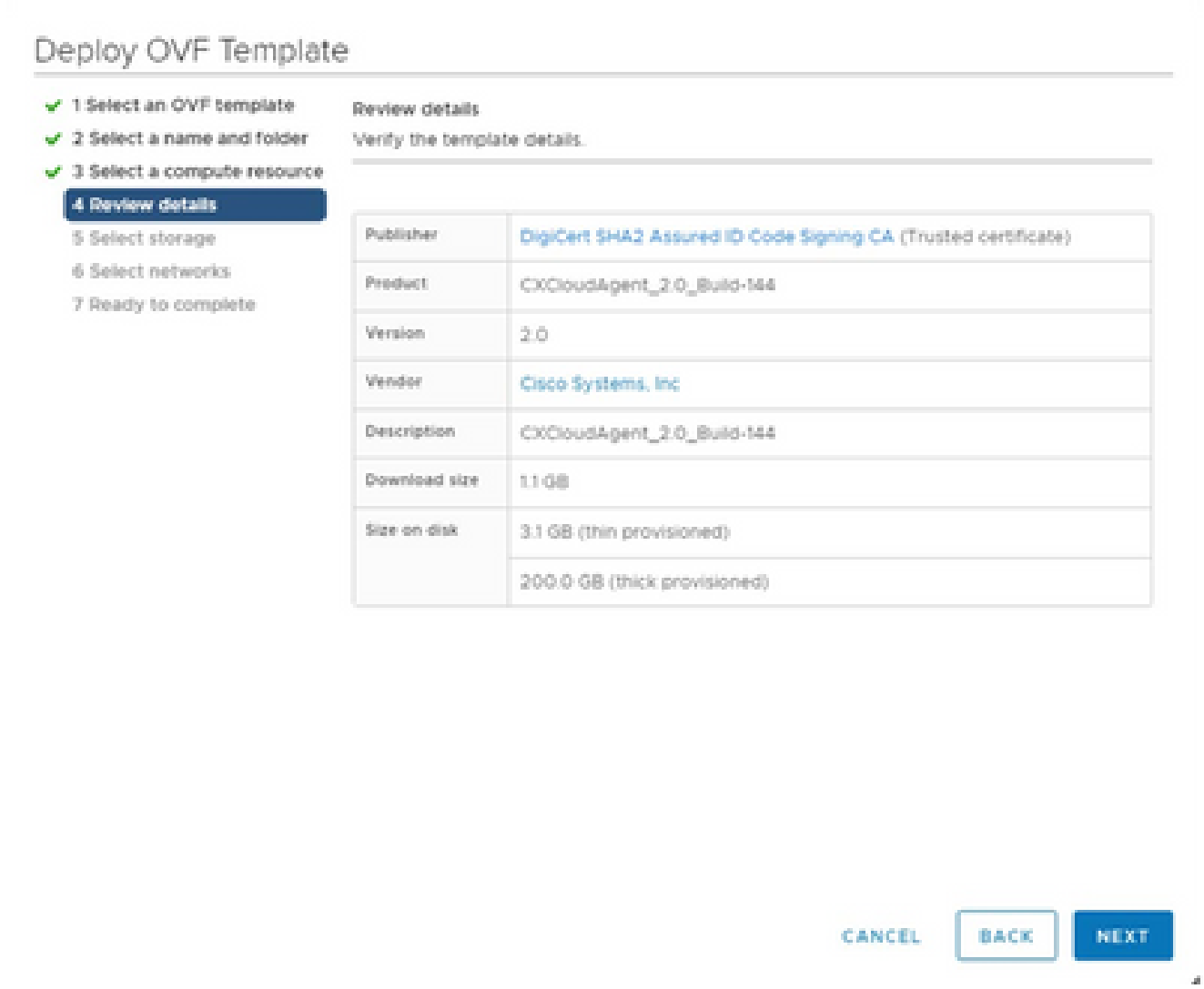
Name und Ordner

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



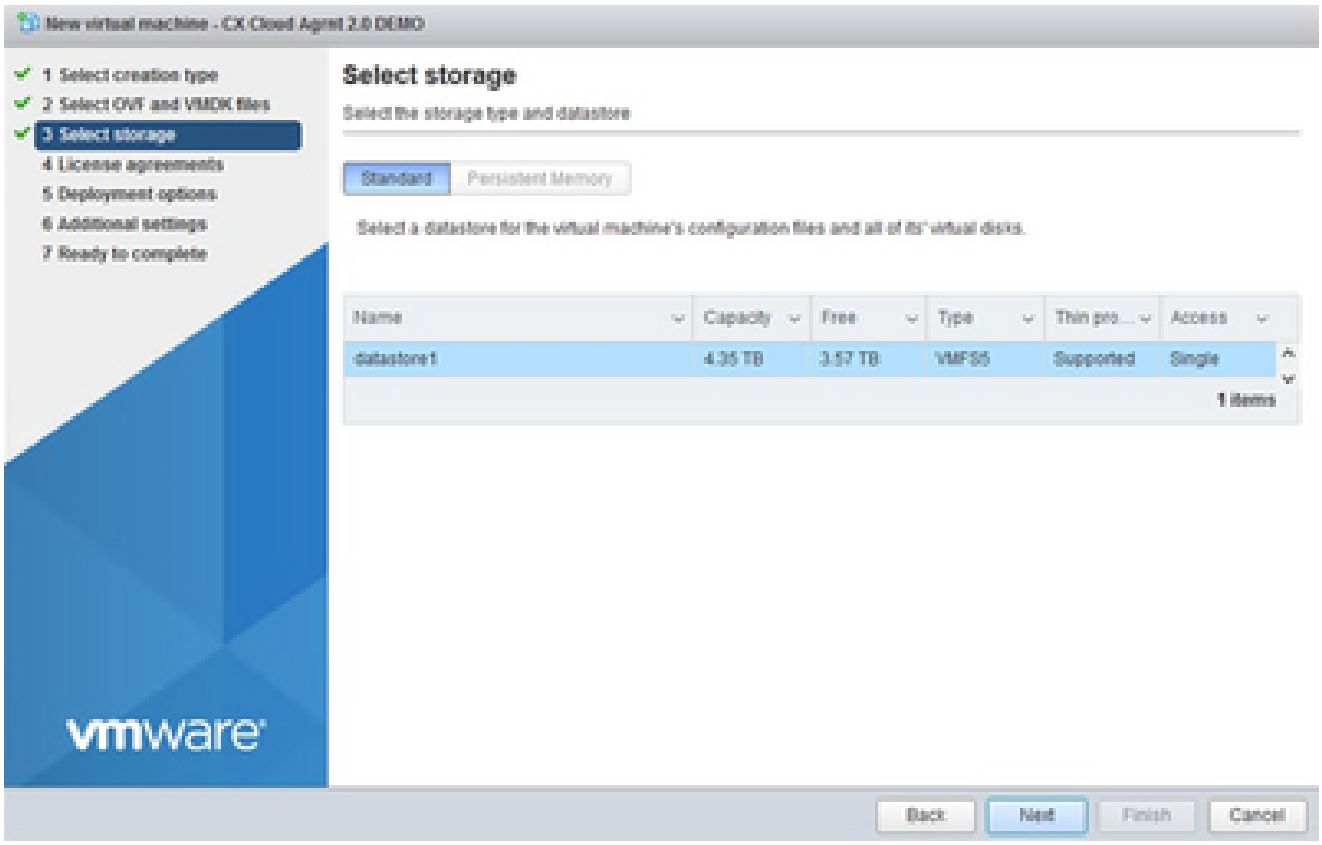
Computerressource auswählen

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



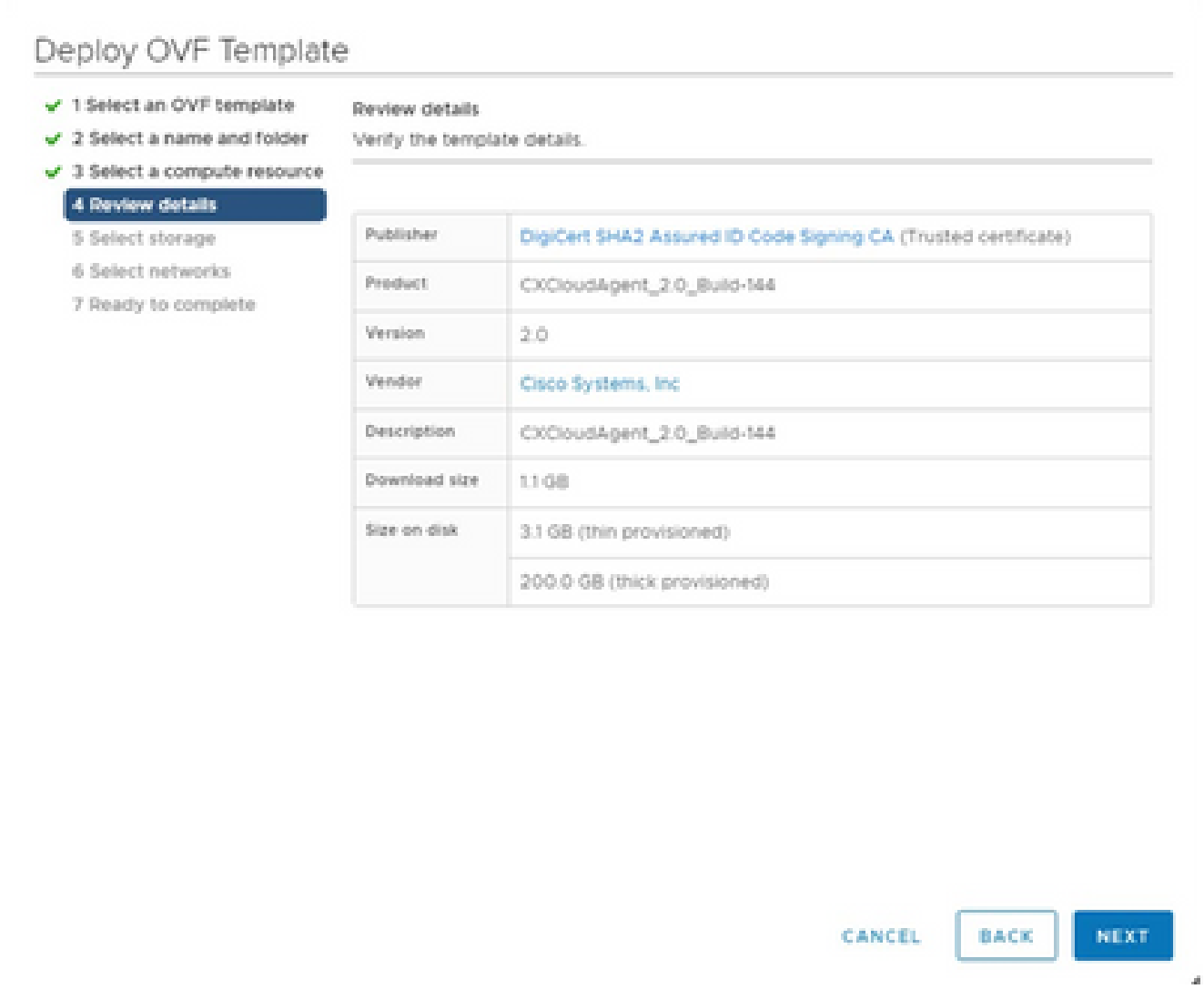
Details überprüfen

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



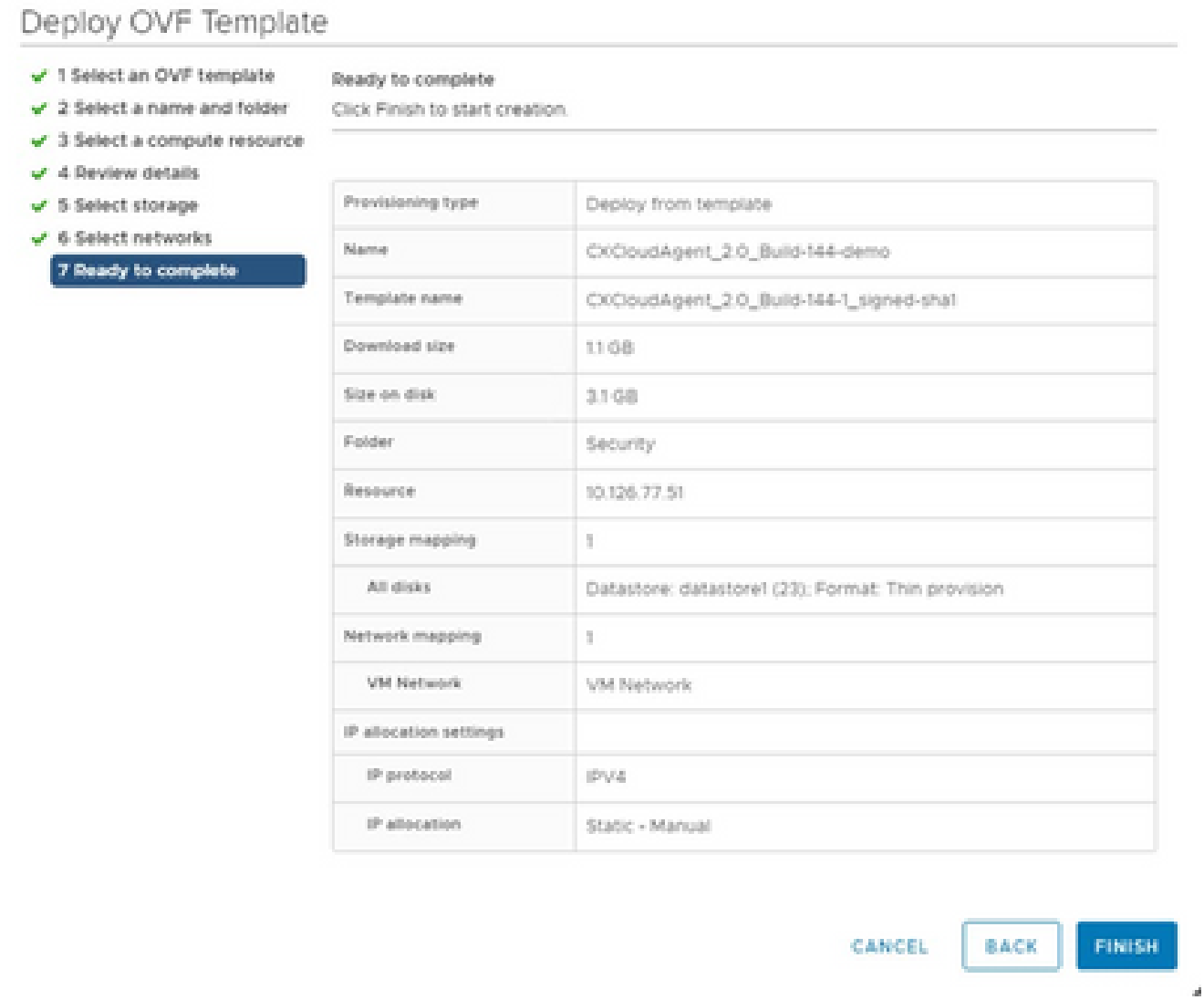
Auswahl von externem Speicher

10. Klicken Sie auf Next (Weiter).



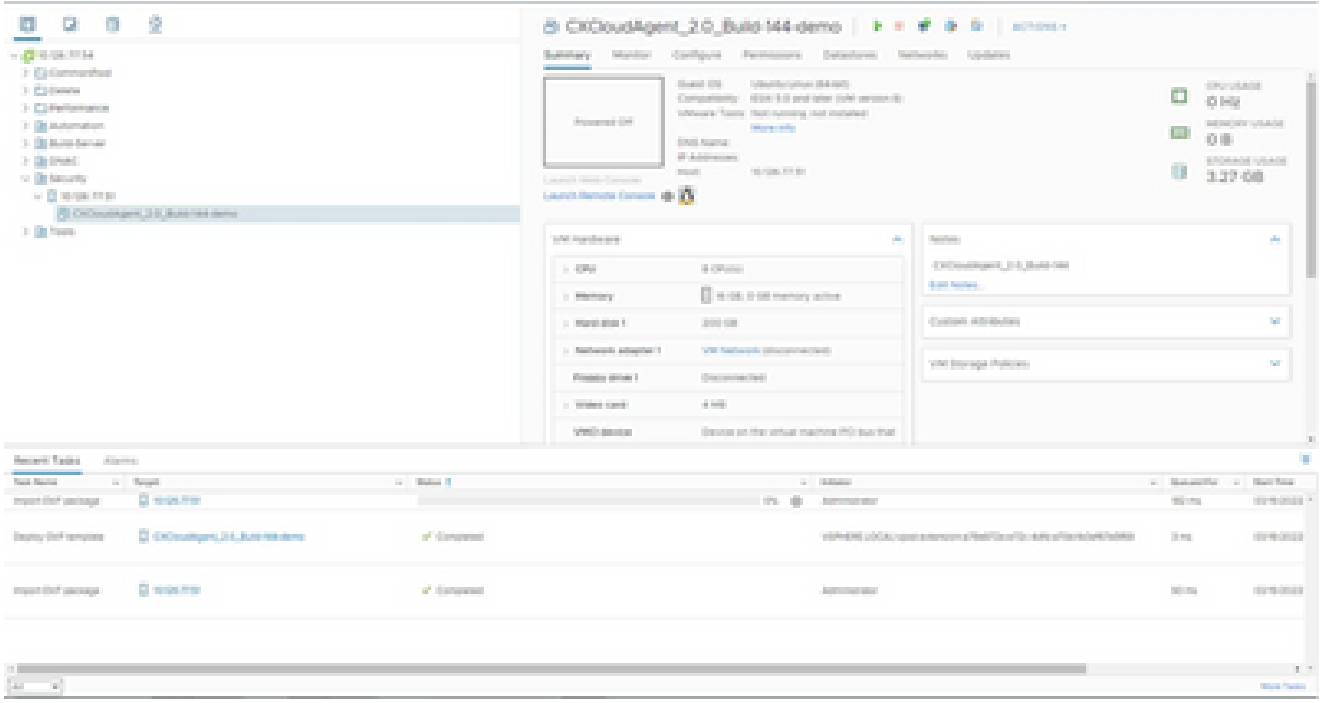
Netzwerk auswählen

11. Klicken Sie auf Beenden.



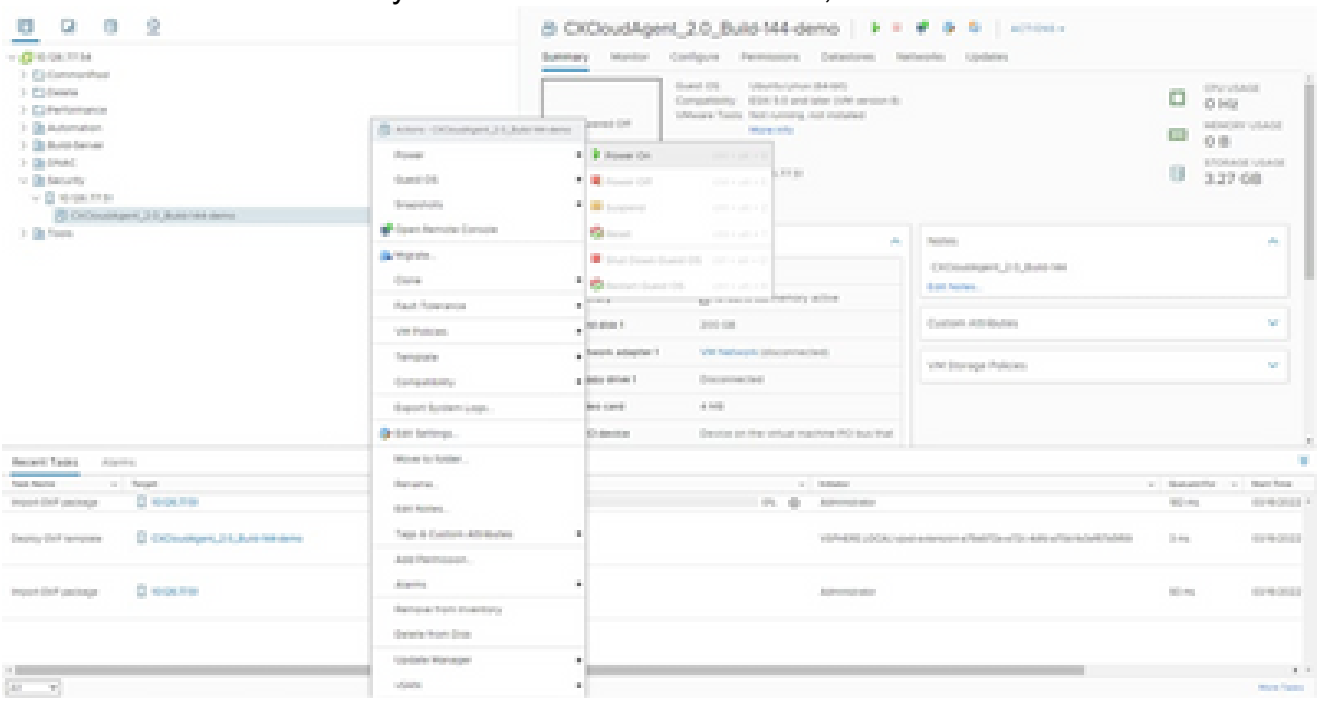
Bereit zur Fertigstellung

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



VM hinzugefügt

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



Konsole öffnen

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

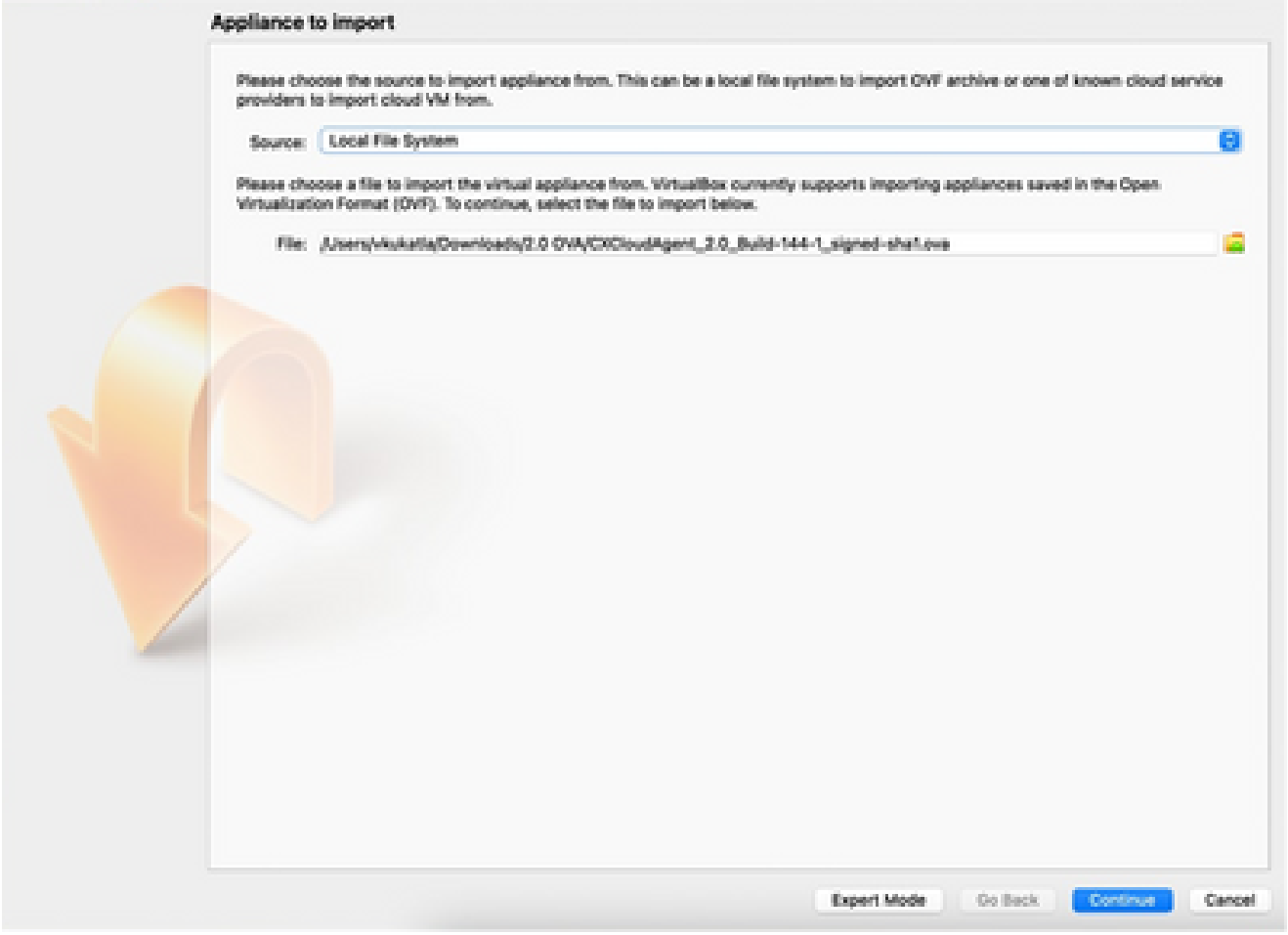
Installation von Oracle VirtualBox 5.2.30

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

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

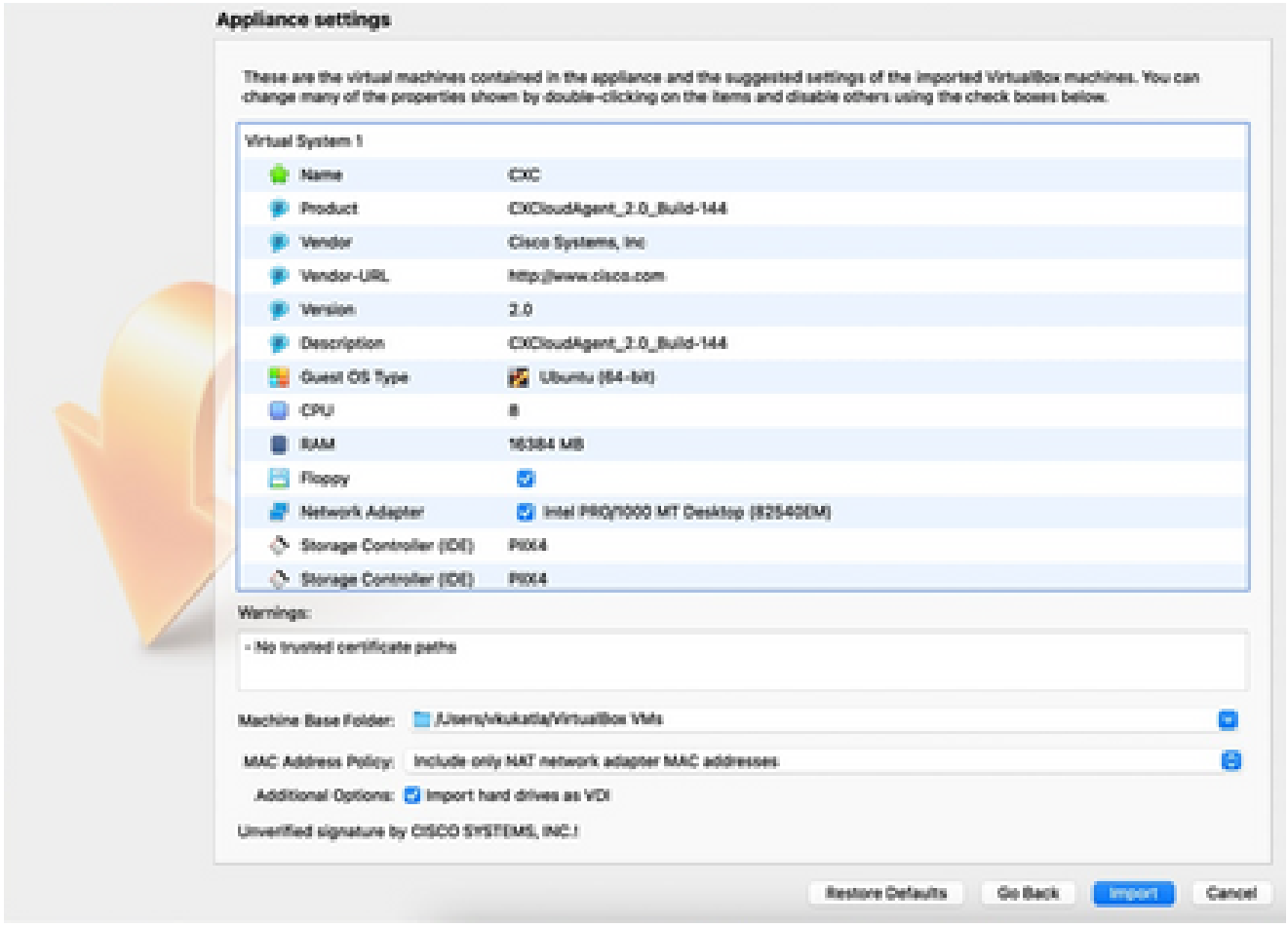
Oracle VM

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



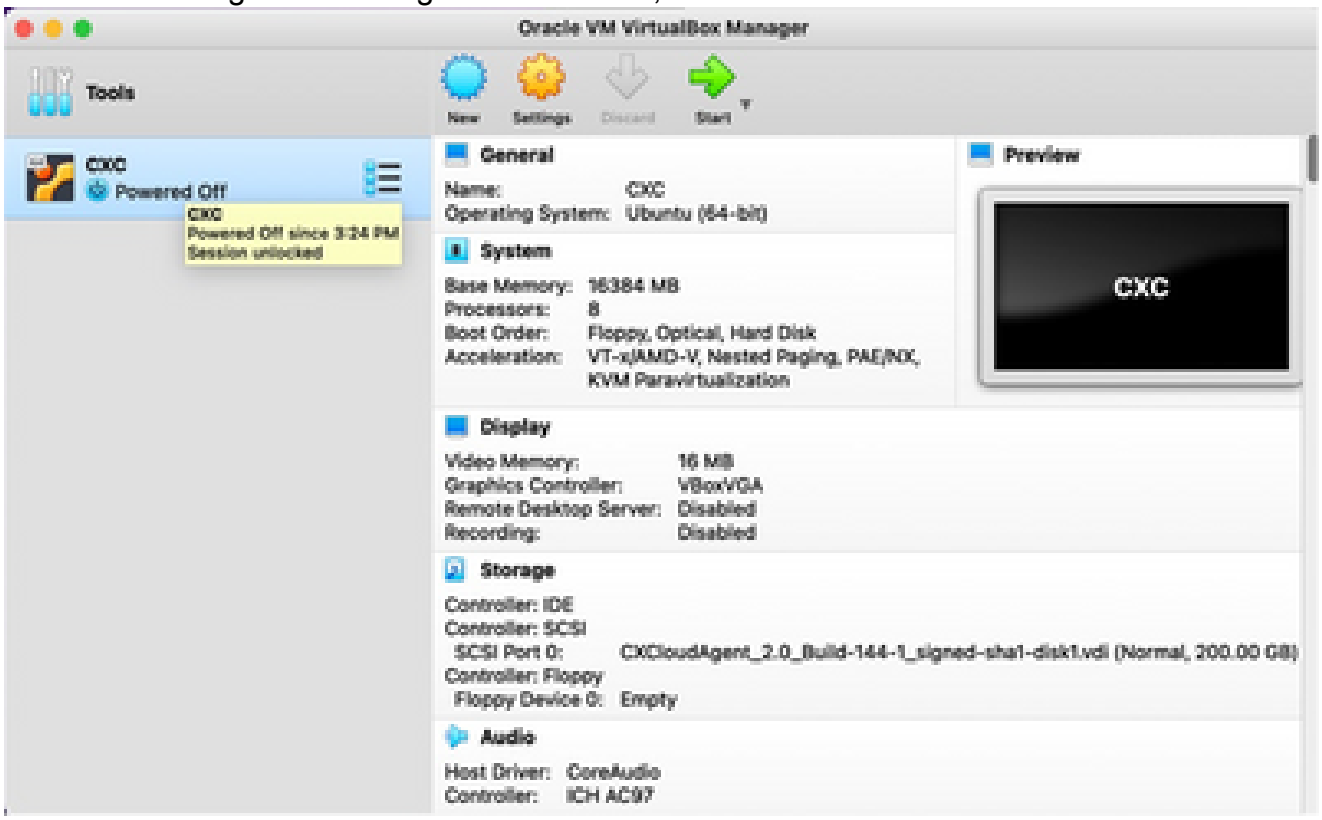
Datei auswählen

3. Klicken Sie auf Importieren.

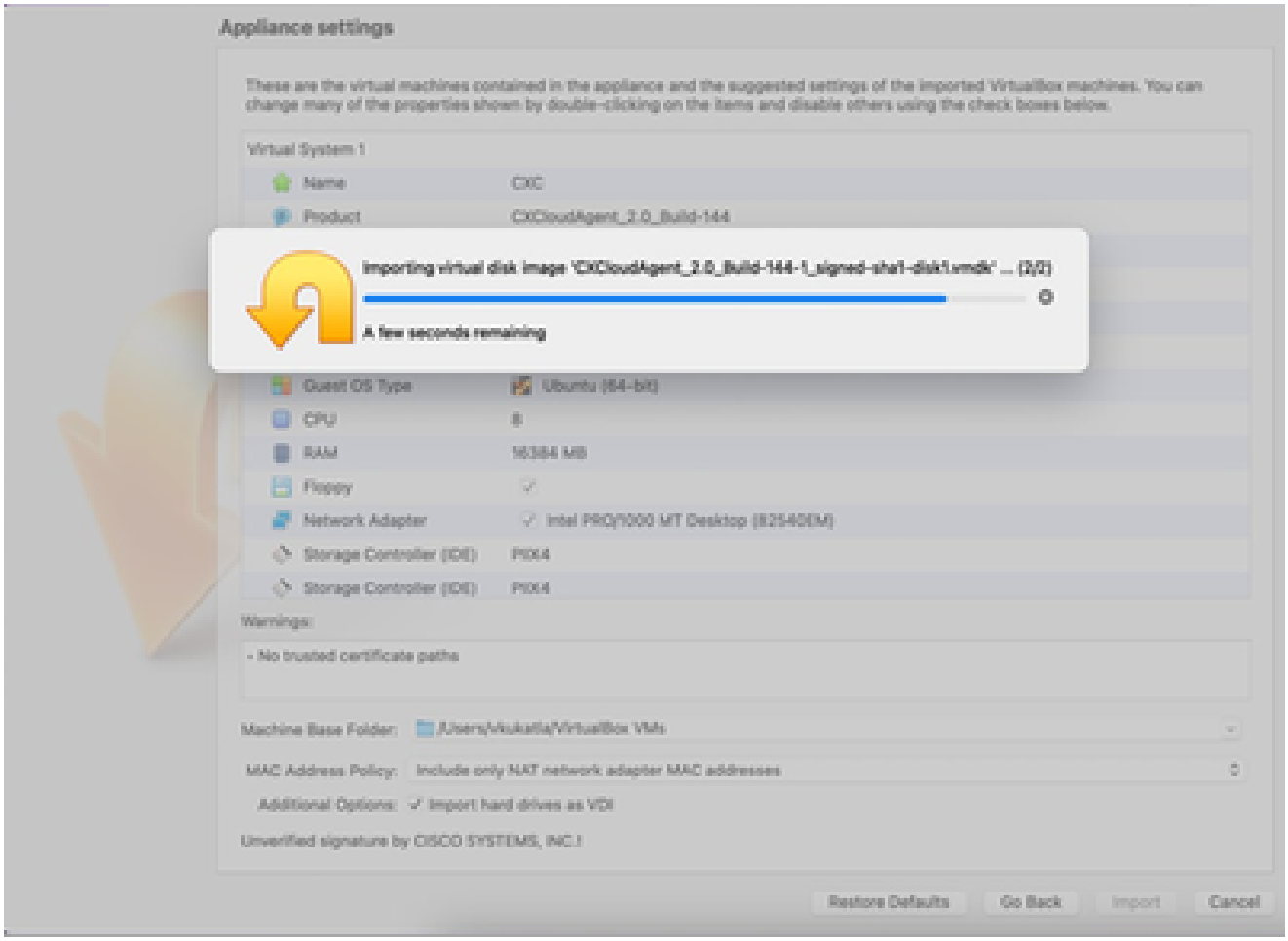


Datei importieren

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

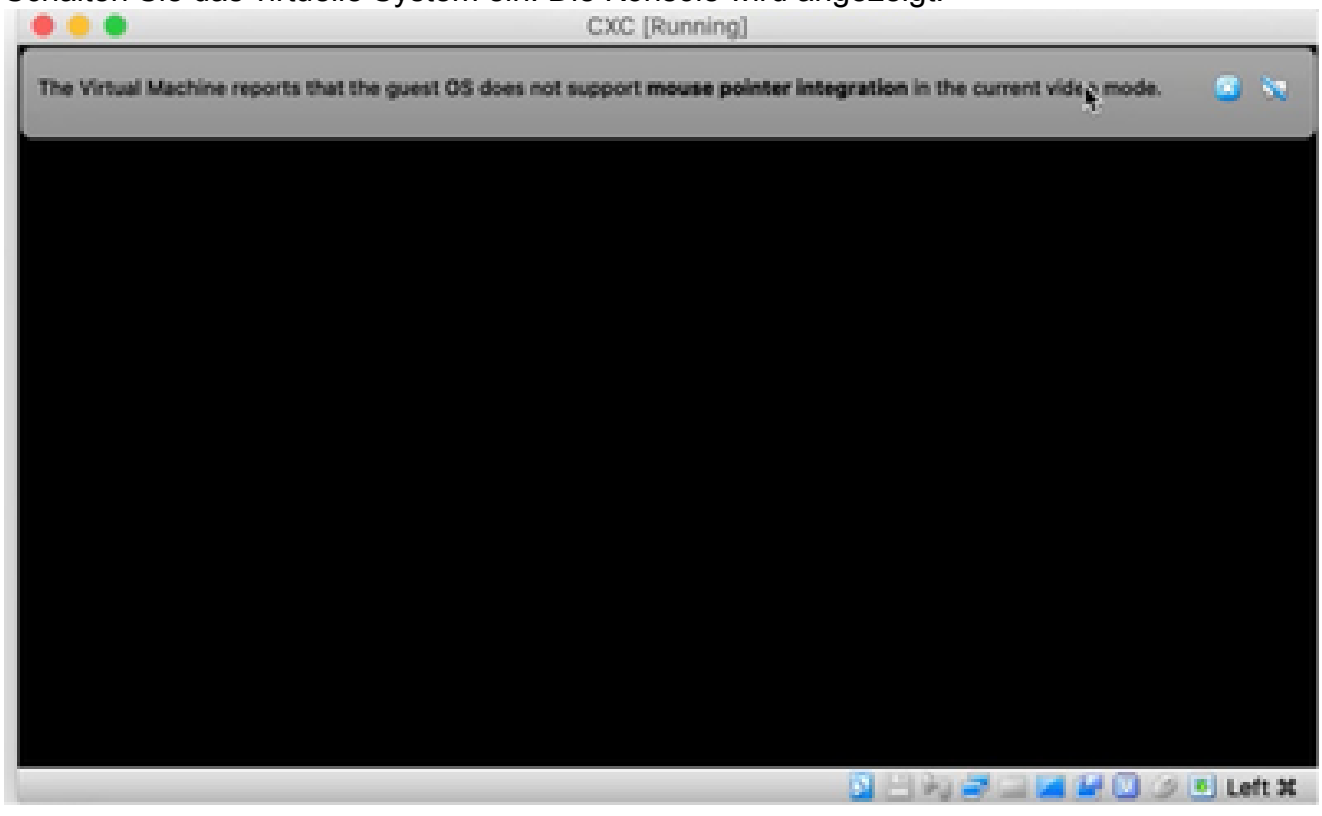


Start der VM-Konsole



Import in Bearbeitung

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



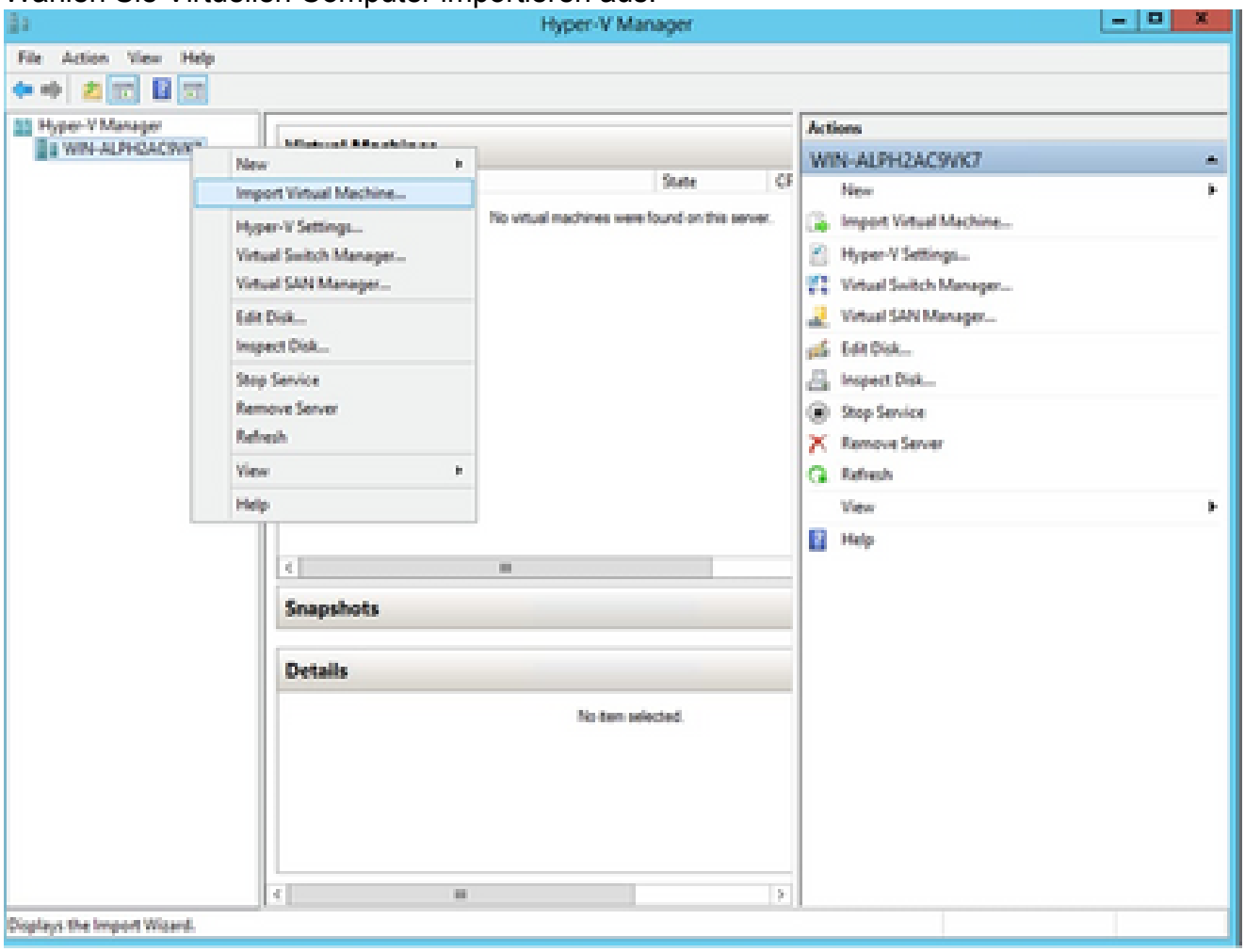
Konsole öffnen

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

Installation von Microsoft Hyper-V

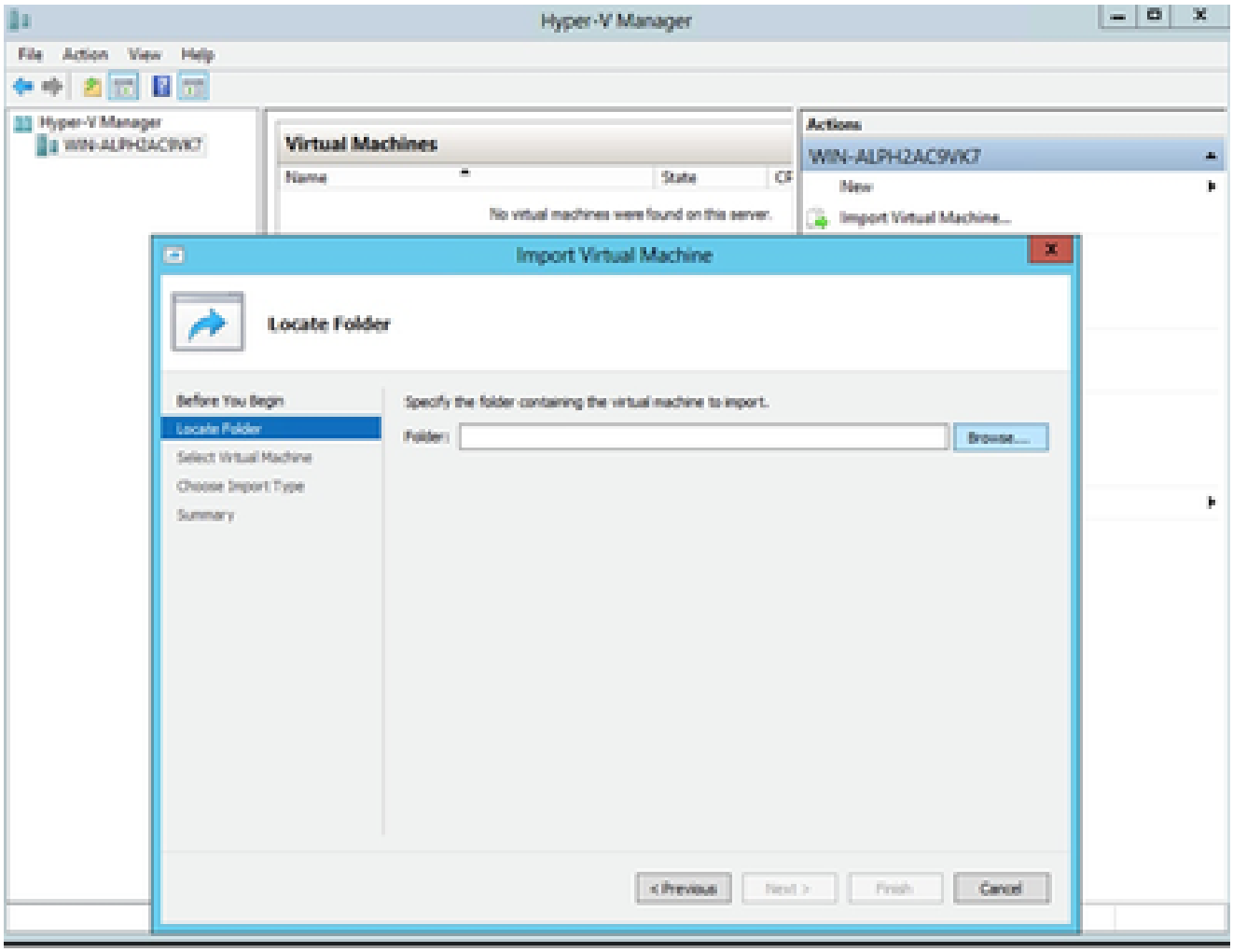
Führen Sie die folgenden Schritte aus:

1. Wählen Sie Virtuellen Computer importieren aus.



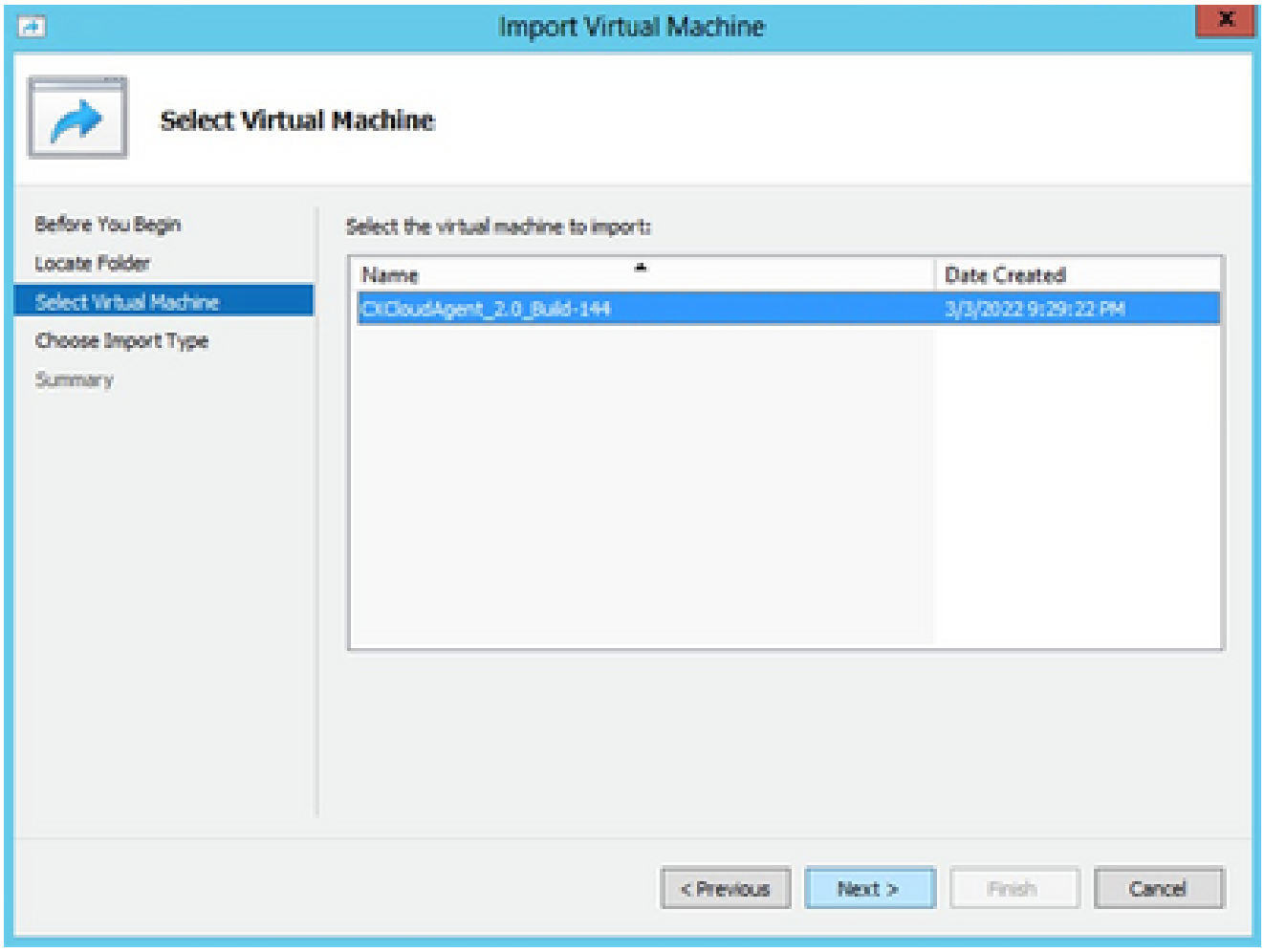
Hyper-V-Manager

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



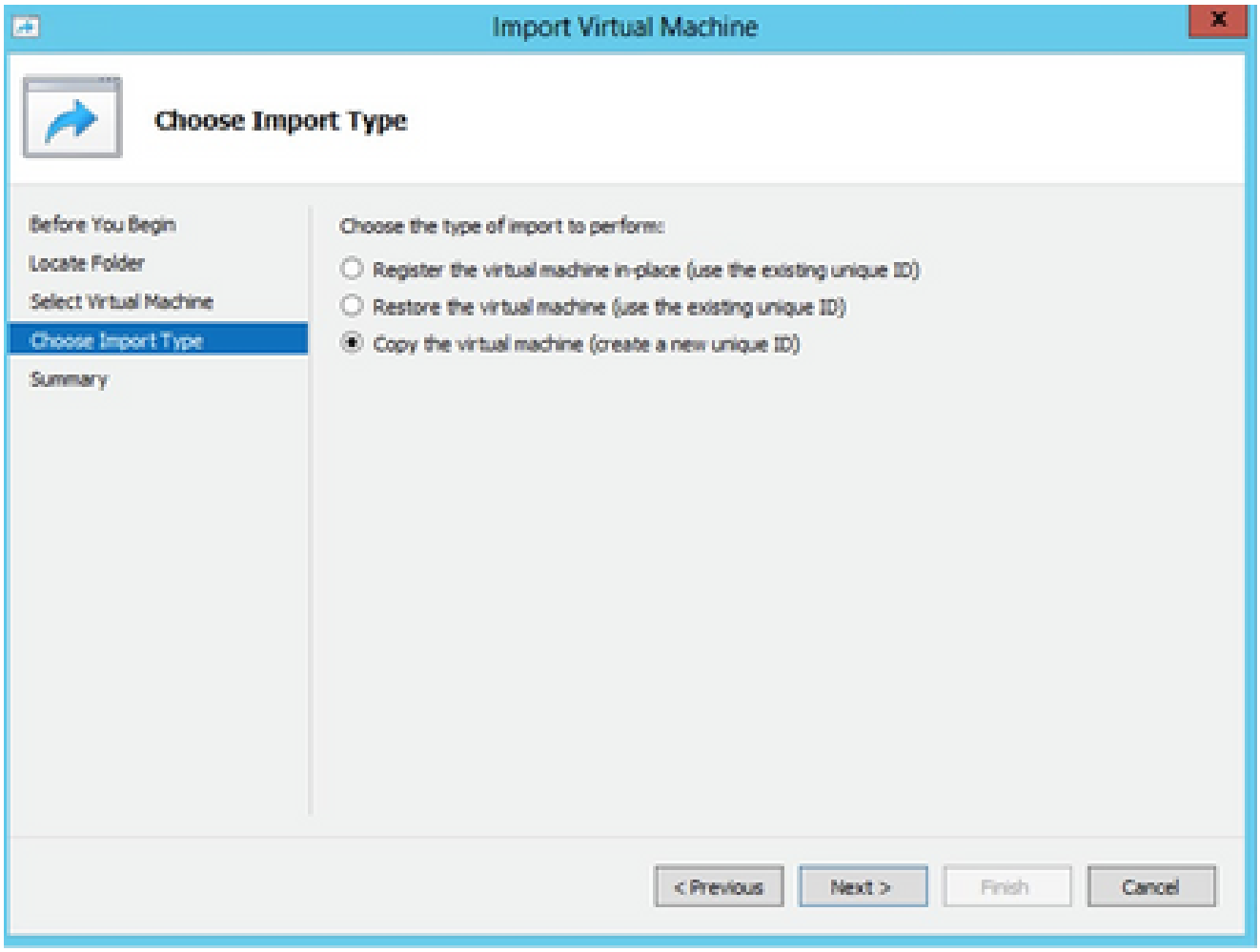
Zu importierender Ordner

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



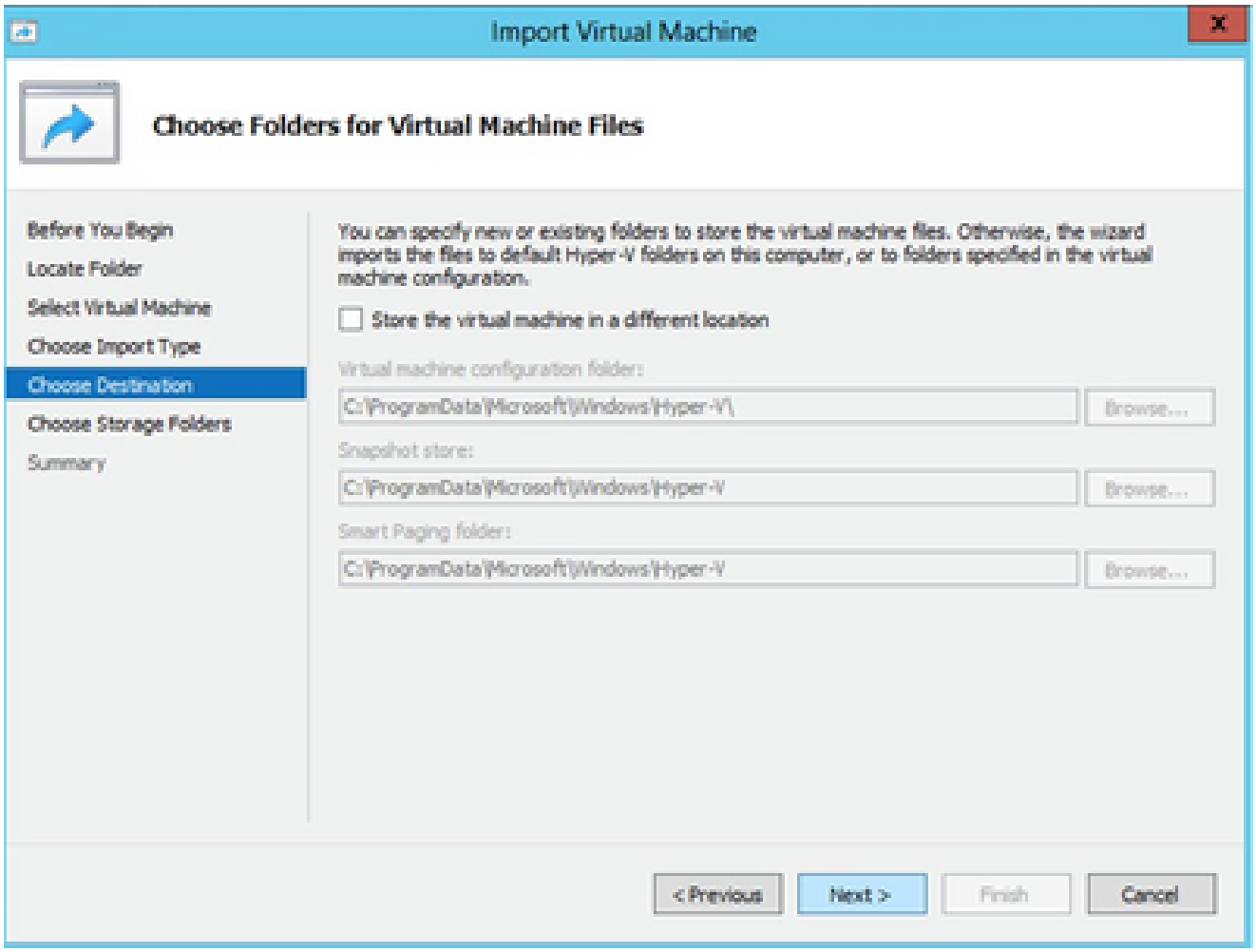
VM auswählen

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



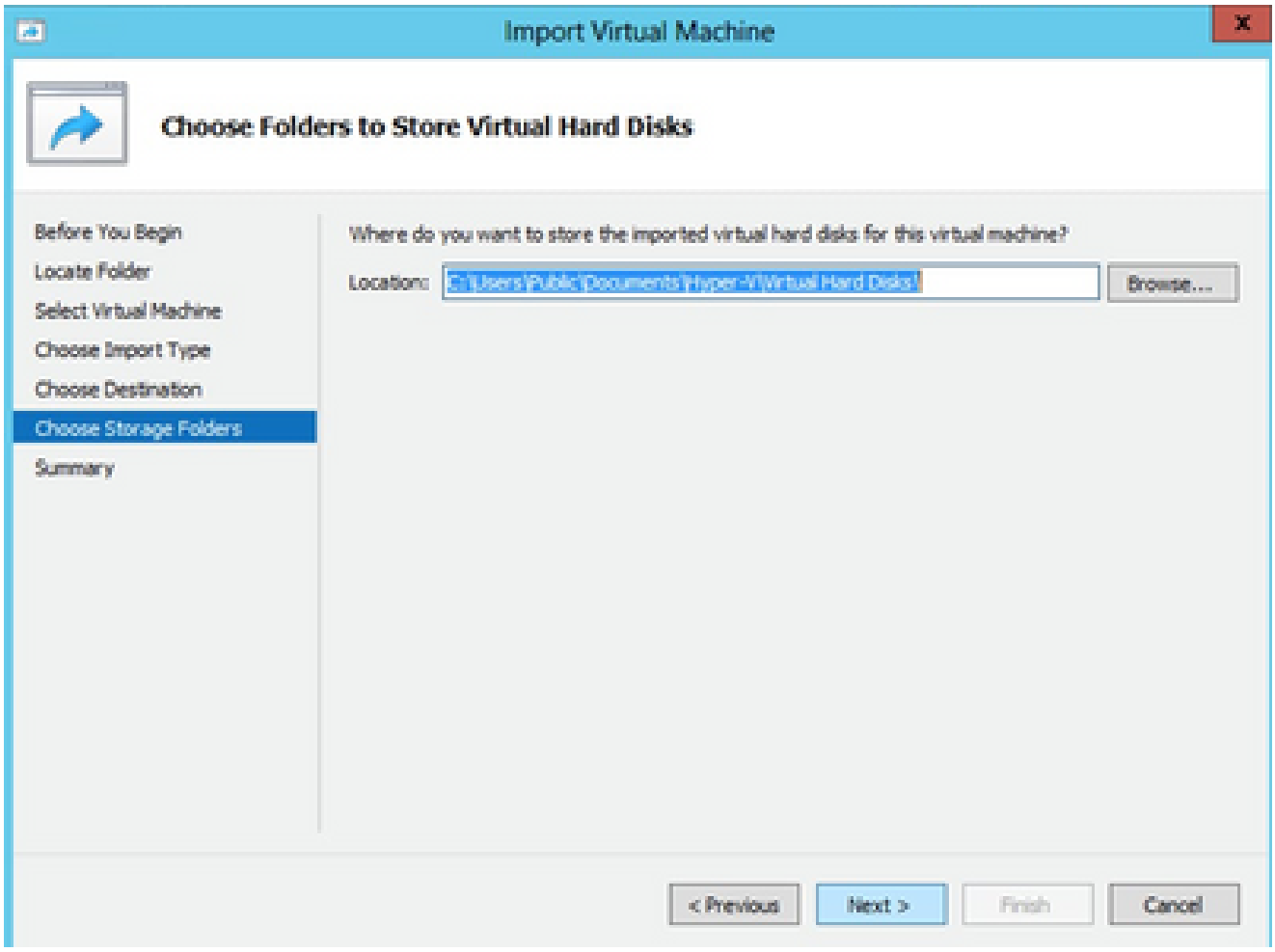
Importtyp

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



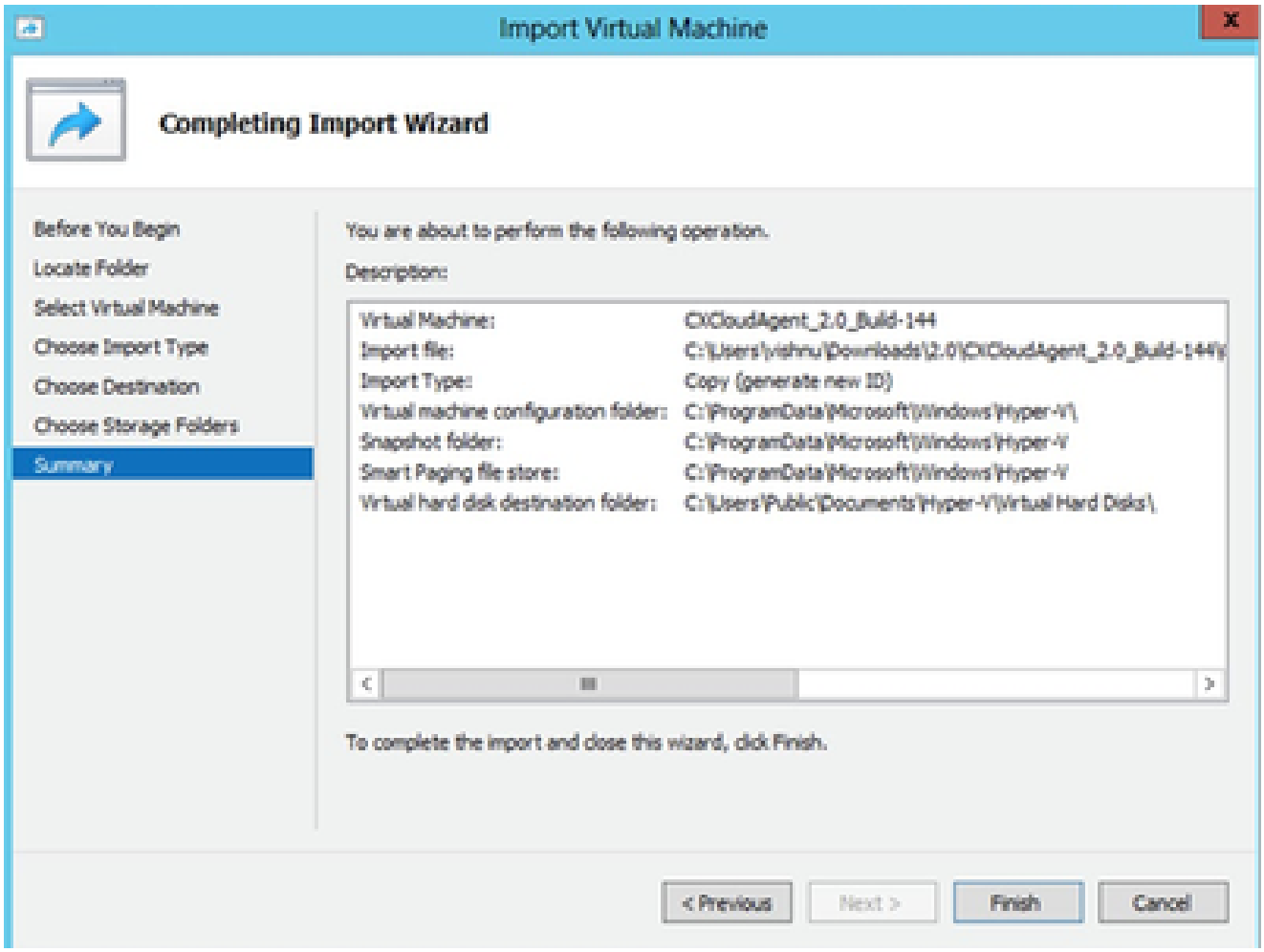
Ordner für Dateien virtueller Systeme auswählen

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



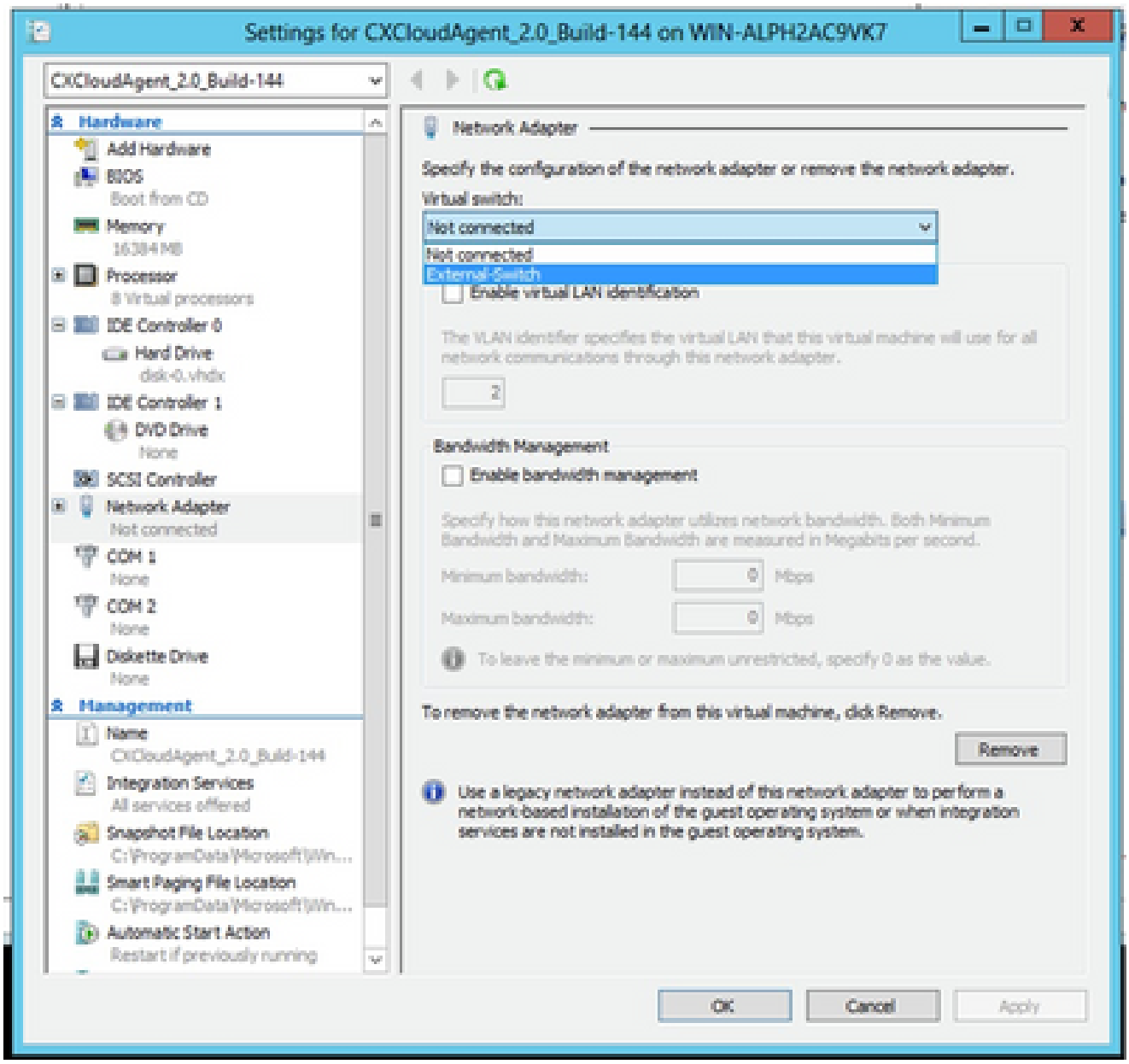
Ordner zum Speichern der virtuellen Festplatten

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



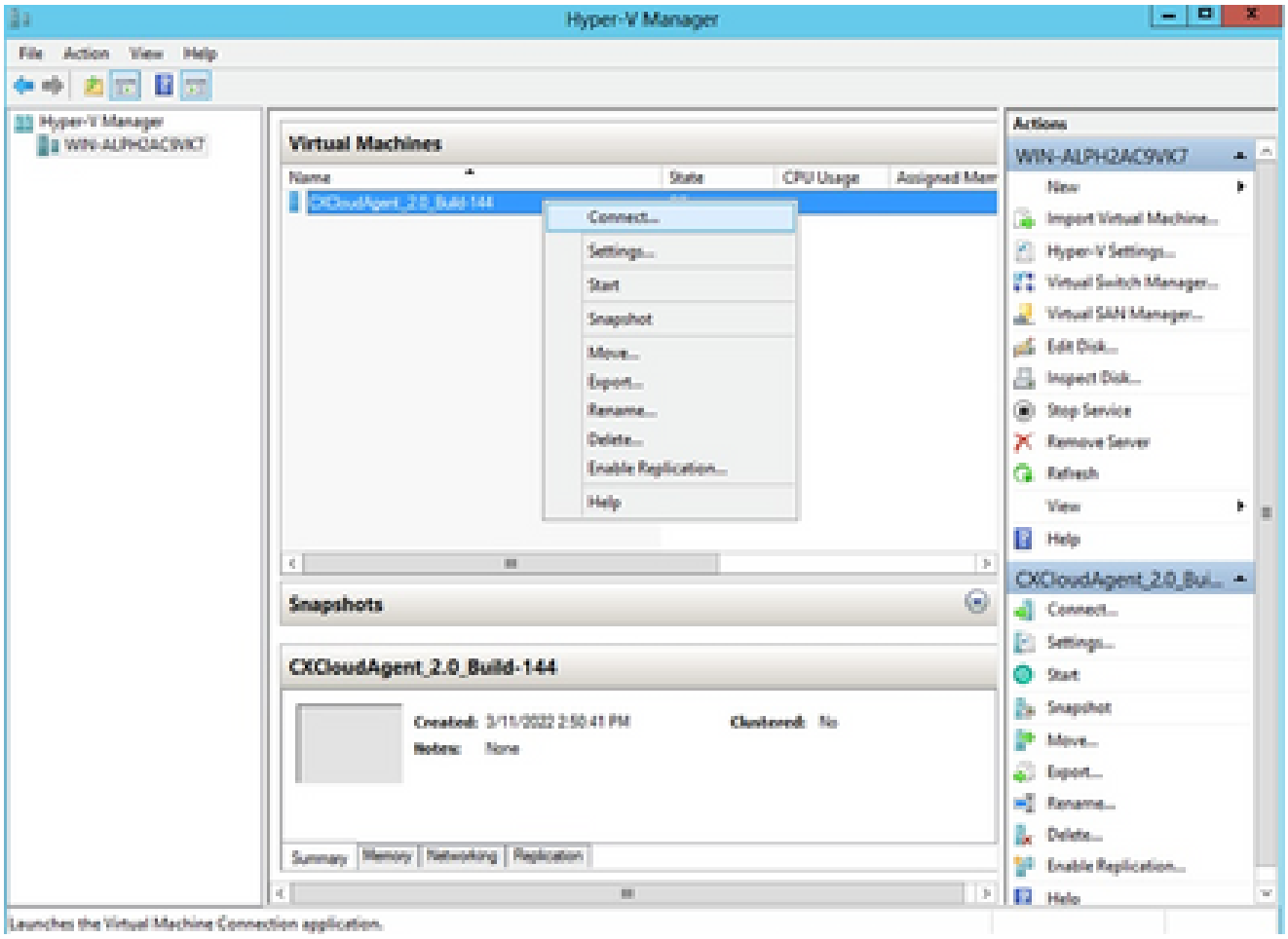
Zusammenfassung

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



Virtueller Switch

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

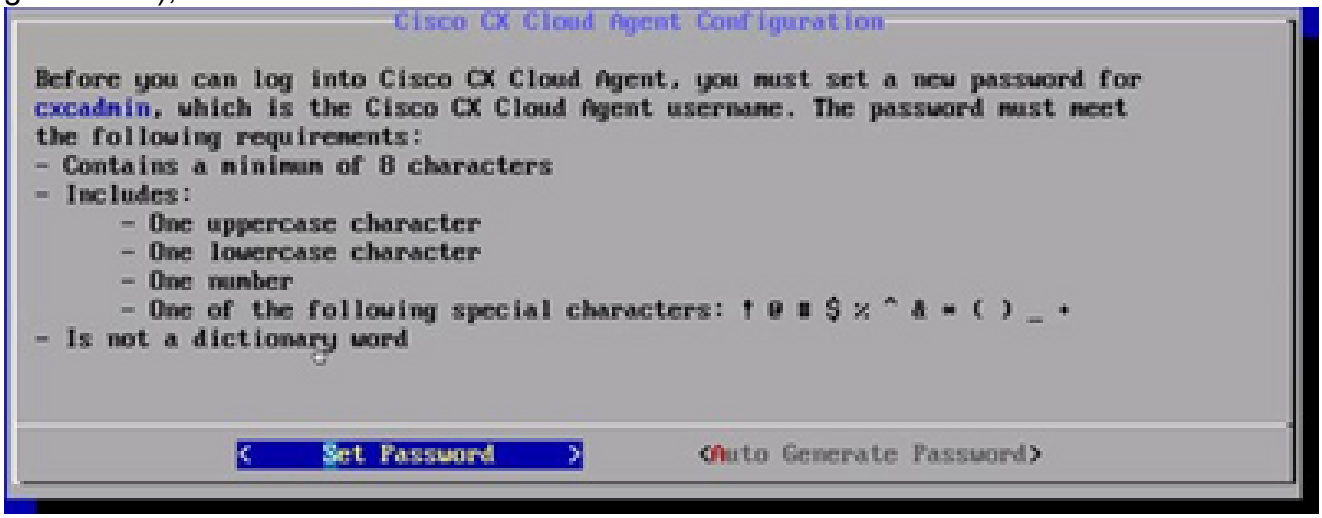


VM wird gestartet

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

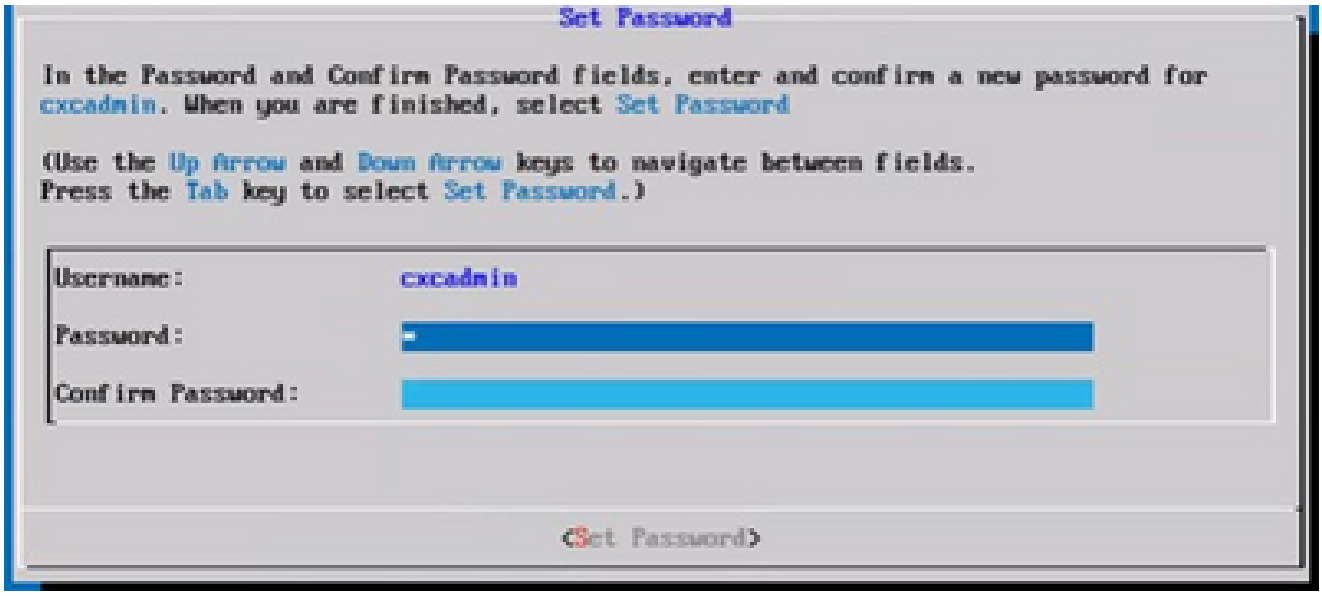
Netzwerkkonfiguration

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



Passwort festlegen

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



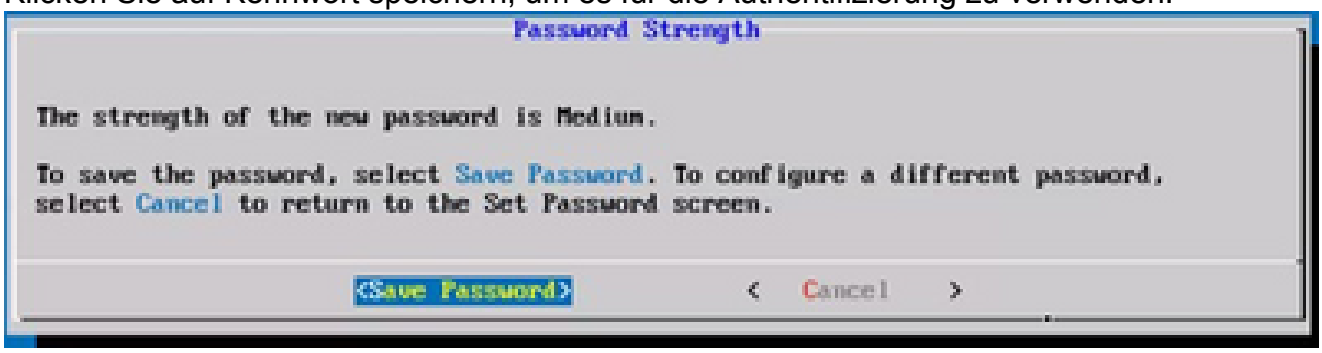
Neues Kennwort

ODER

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

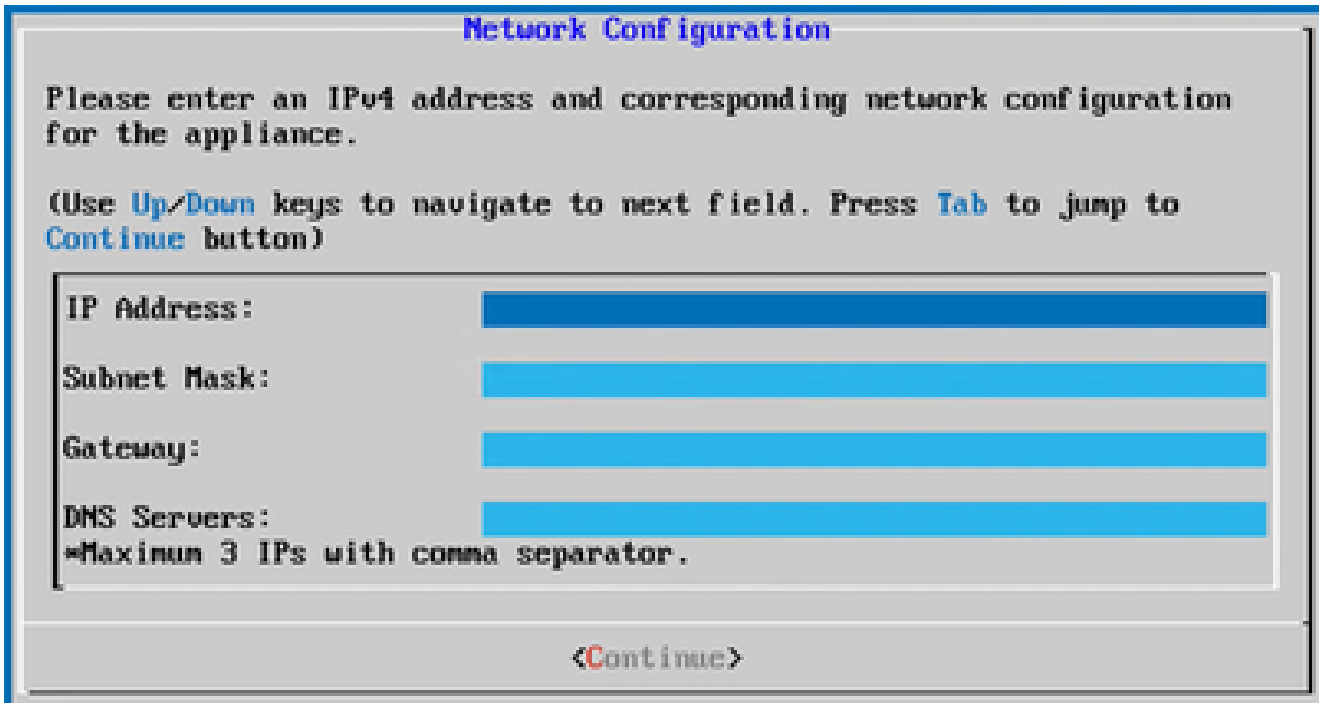
Auto Generated Password (Automatisch generiertes Kennwort)

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



Passwort speichern

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



Netzwerkkonfiguration

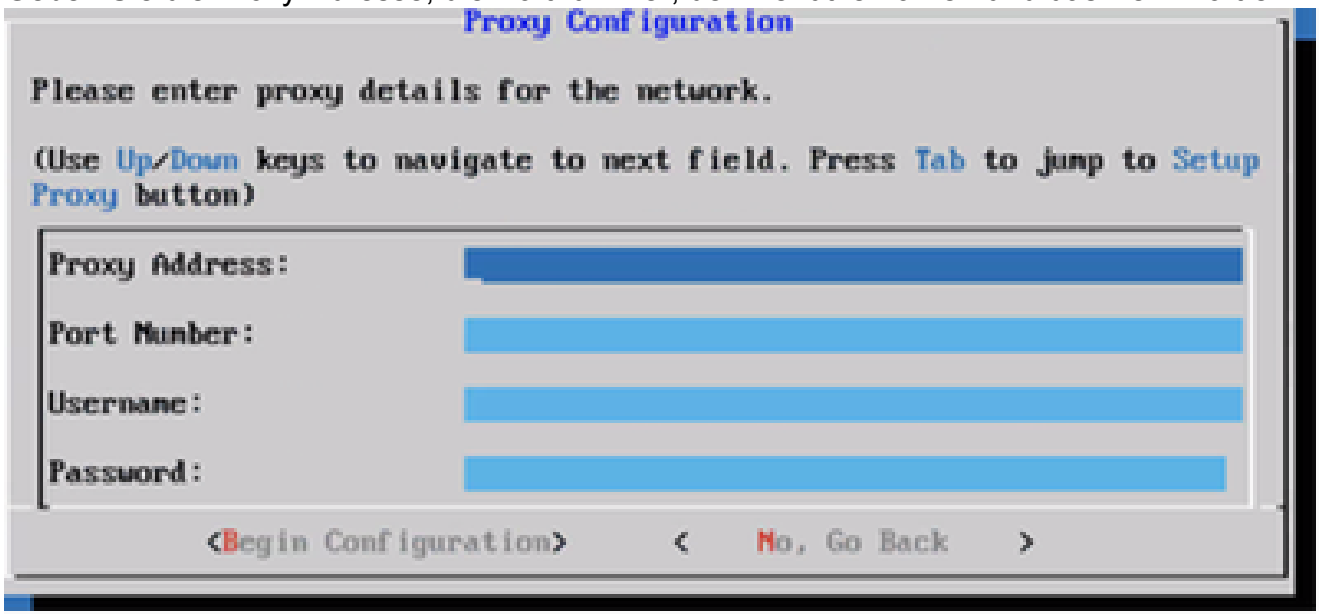
5. Bestätigen Sie die Eingaben, und klicken Sie auf Ja, weiter.

Konfiguration

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

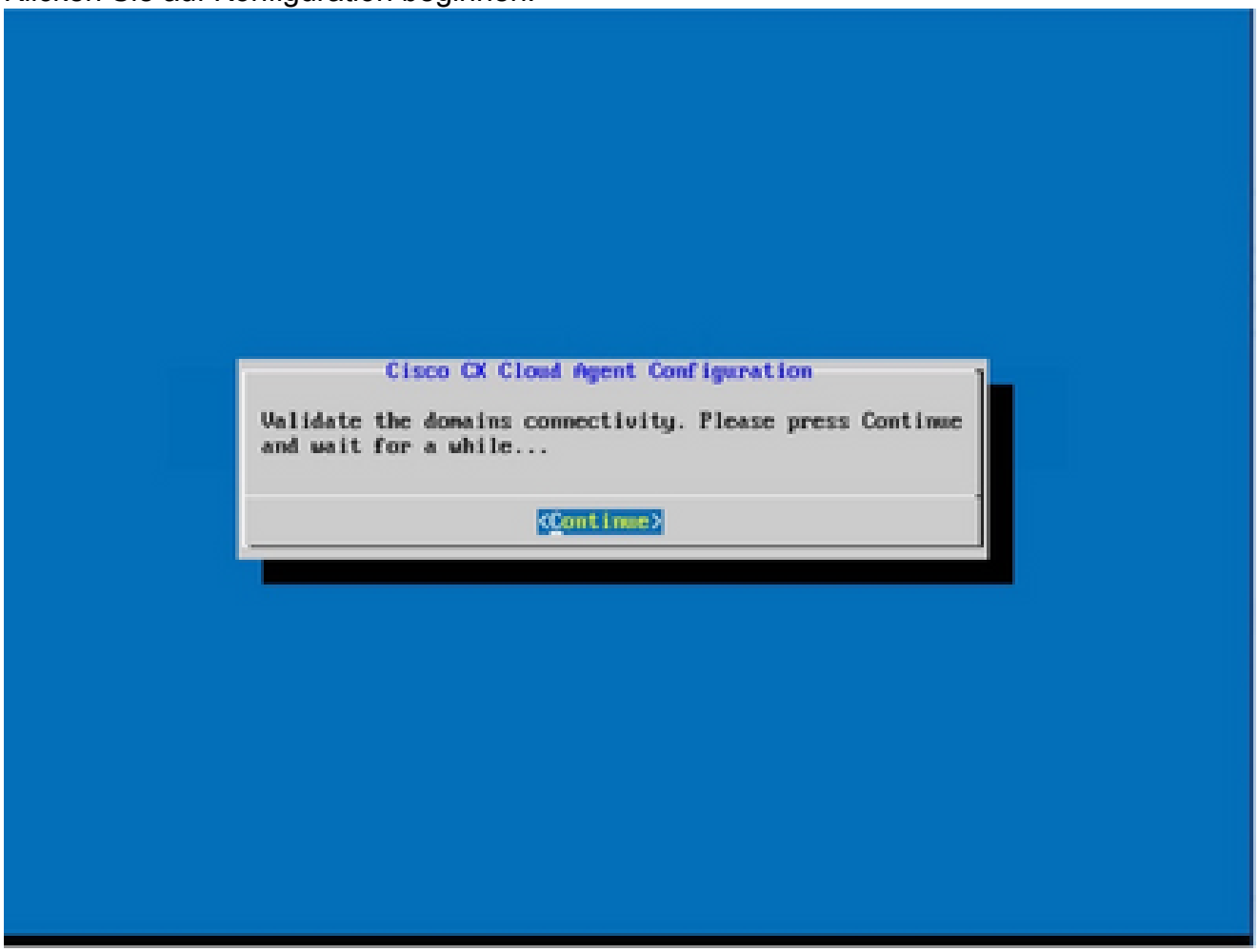
Proxy-Einrichtung

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



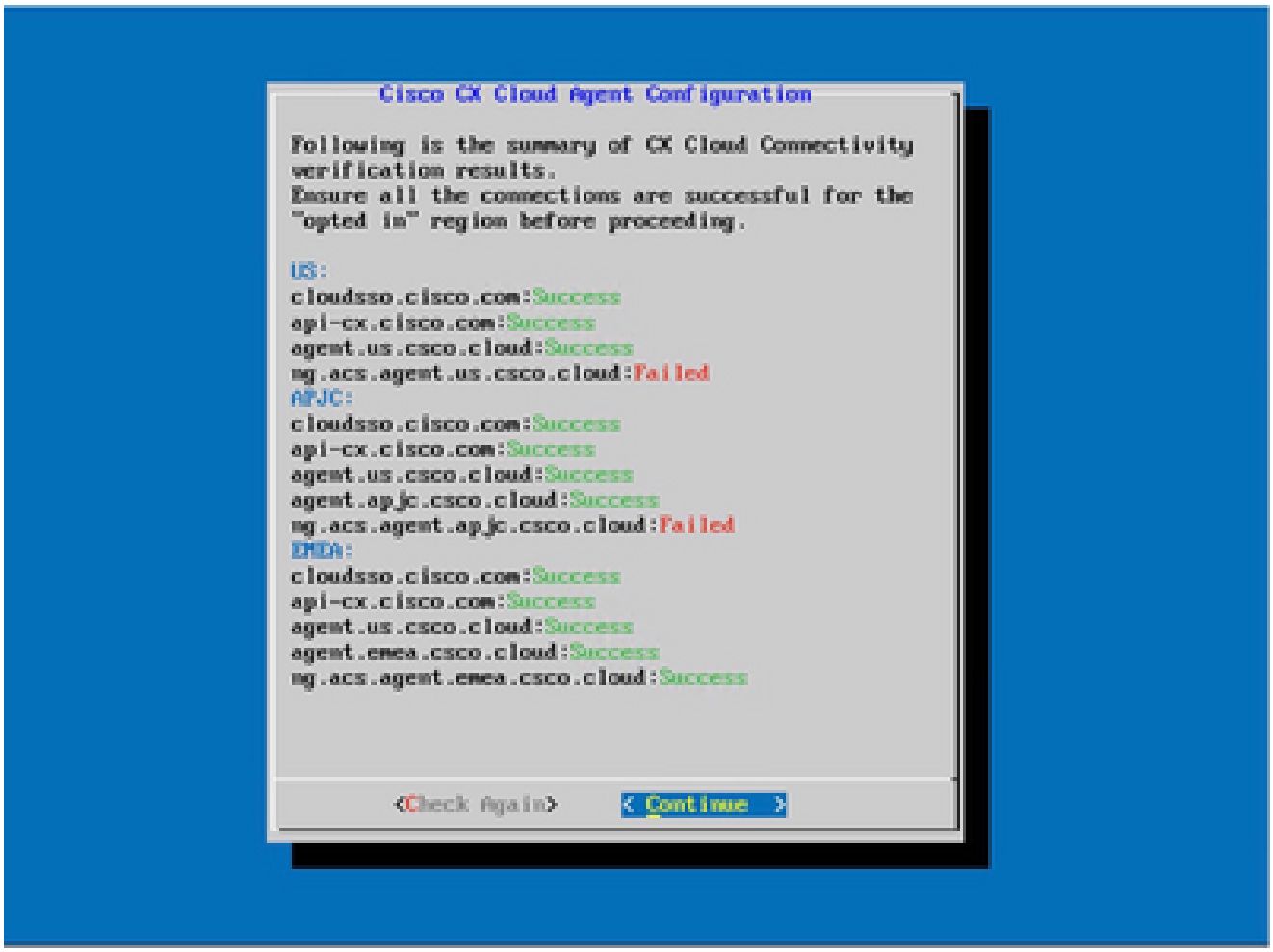
Proxy-Konfiguration

8. Klicken Sie auf Konfiguration beginnen.



Konfiguration beginnen

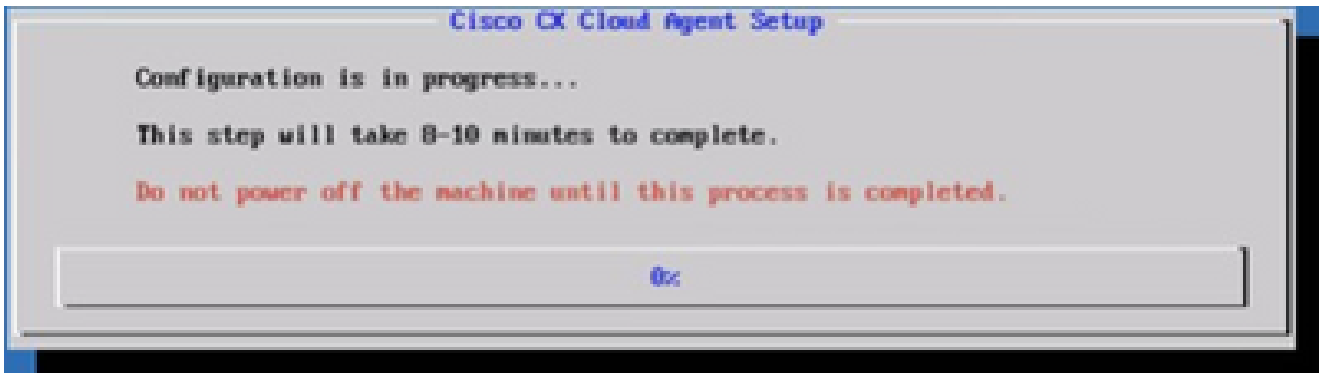
9. Klicken Sie auf Continue (Weiter).



Konfiguration wird fortgesetzt

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

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

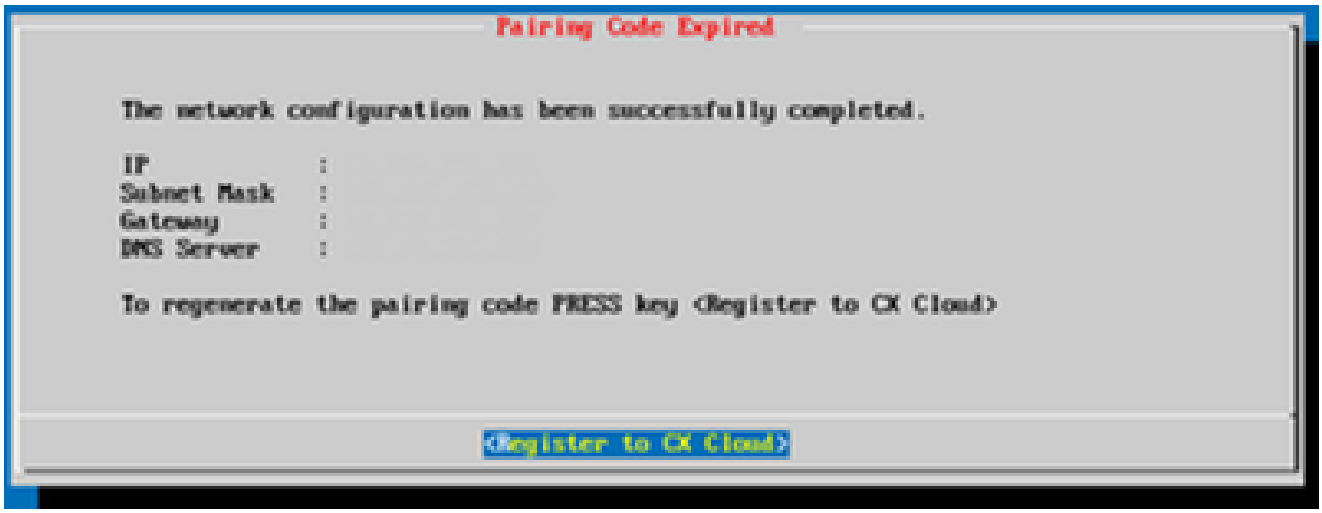


Konfiguration in Bearbeitung

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

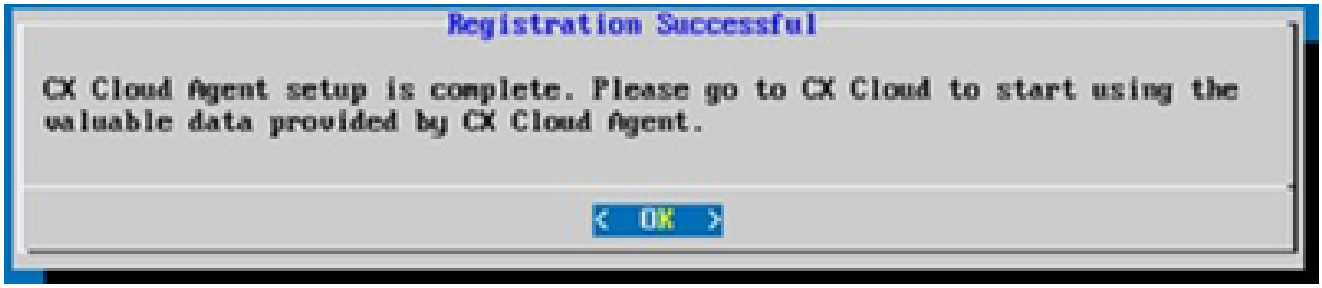
Kopplungscode

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



Code abgelaufen

13. Klicken Sie auf OK.



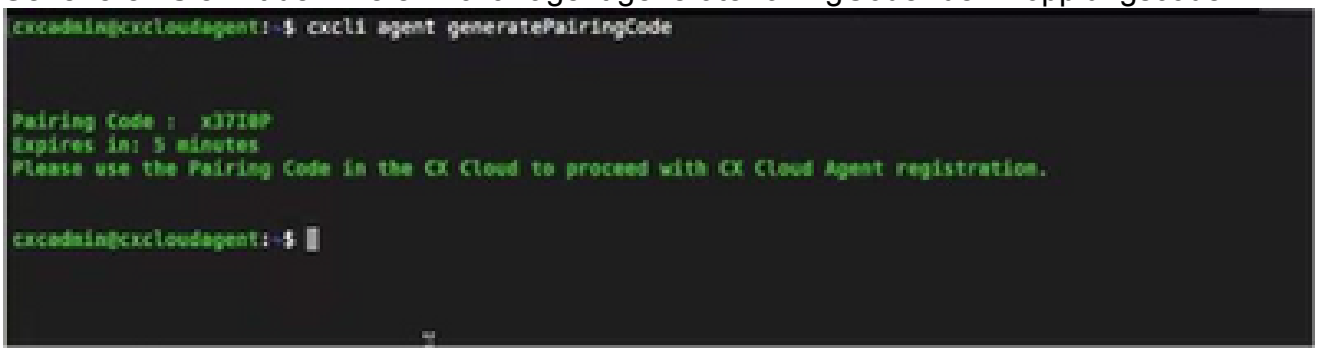
Registrierung erfolgreich

Alternativer Ansatz zum Generieren von Kopplungscode mithilfe der CLI

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

So generieren Sie einen Kopplungscode über die CLI:

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



Kopplungscode-CLI generieren

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

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

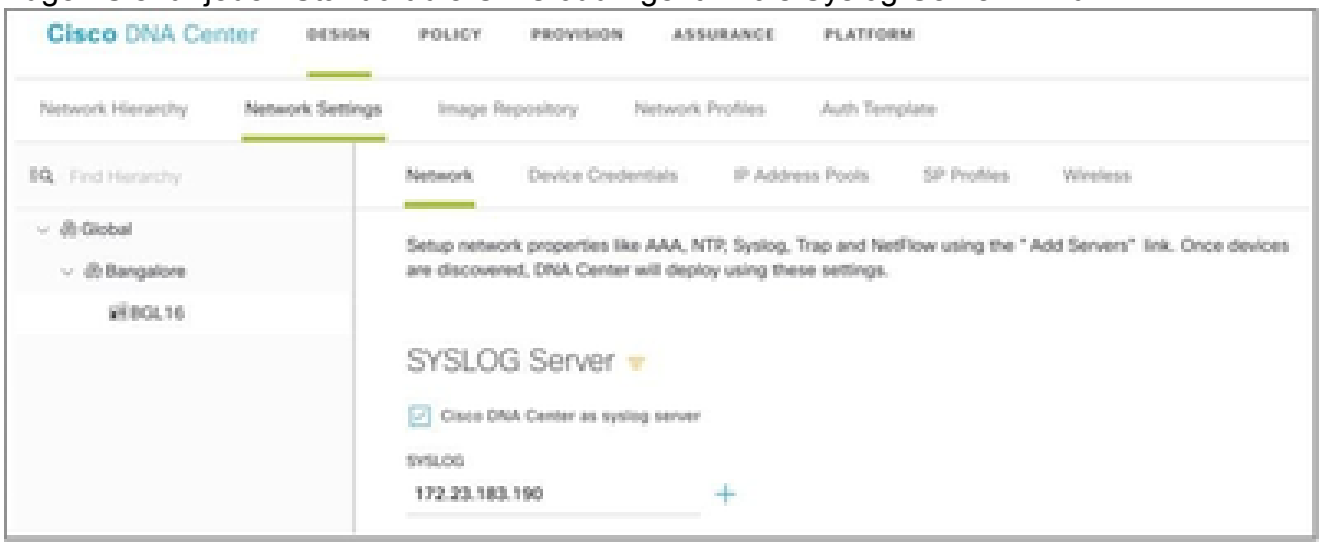
Voraussetzungen

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

Syslog-Weiterleitungseinstellung konfigurieren

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

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



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

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

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

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

Vorhandene Syslog-Server mit Weiterleitungsfunktion

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

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

Vorhandene Syslog-Server ohne Weiterleitungsfunktion ODER ohne Syslog-Server

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

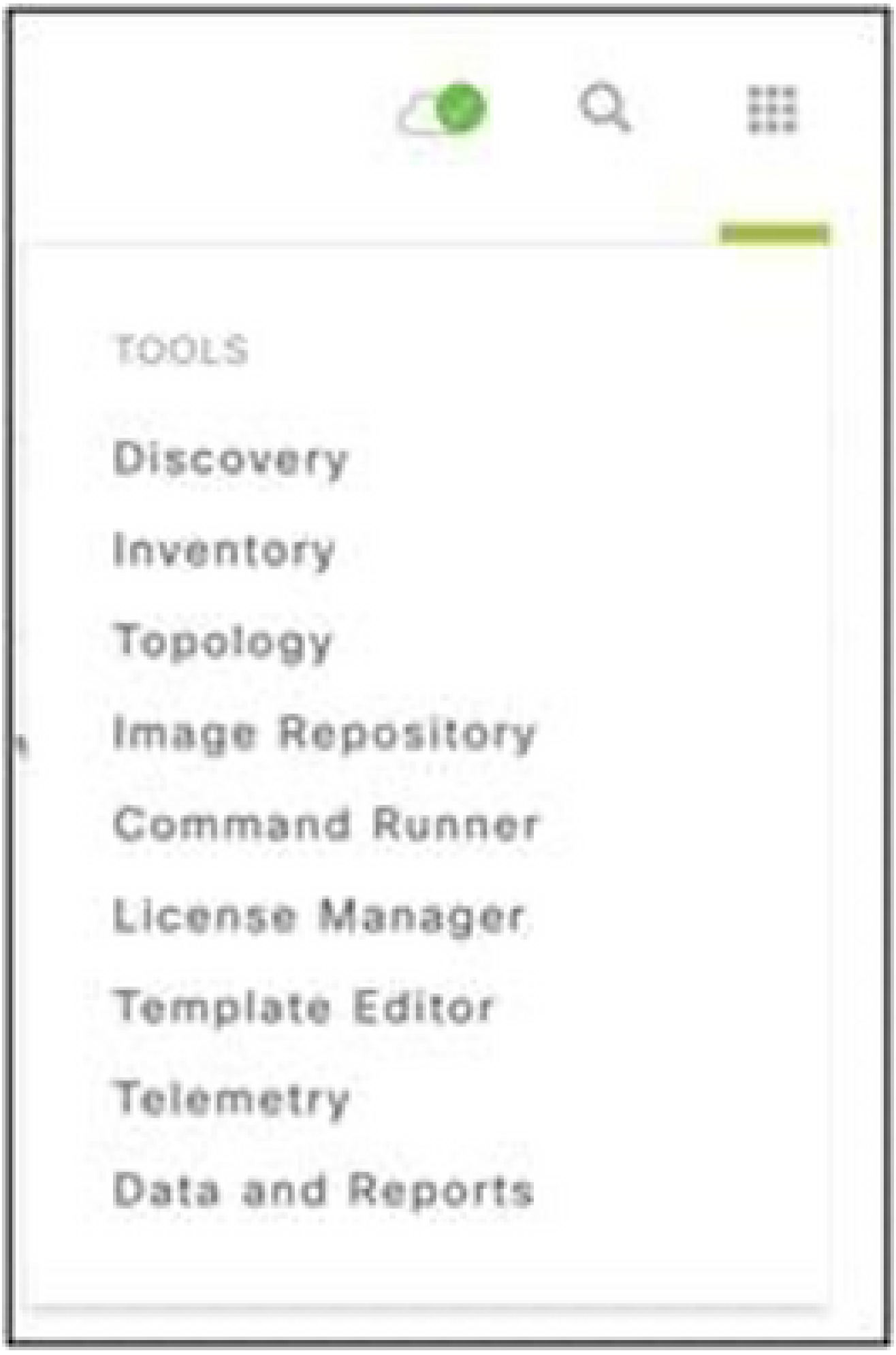
Cisco IOS® XE Konfigurationsleitfaden

Konfigurationsanleitung für den AireOS Wireless Controller

Syslog-Einstellungen auf Informationsebene aktivieren

So machen Sie die Syslog-Informationen sichtbar:

1. Navigieren Sie zu Extras> Telemetrie.


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

Menü Extras

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

Standortansicht

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

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

Aktionen

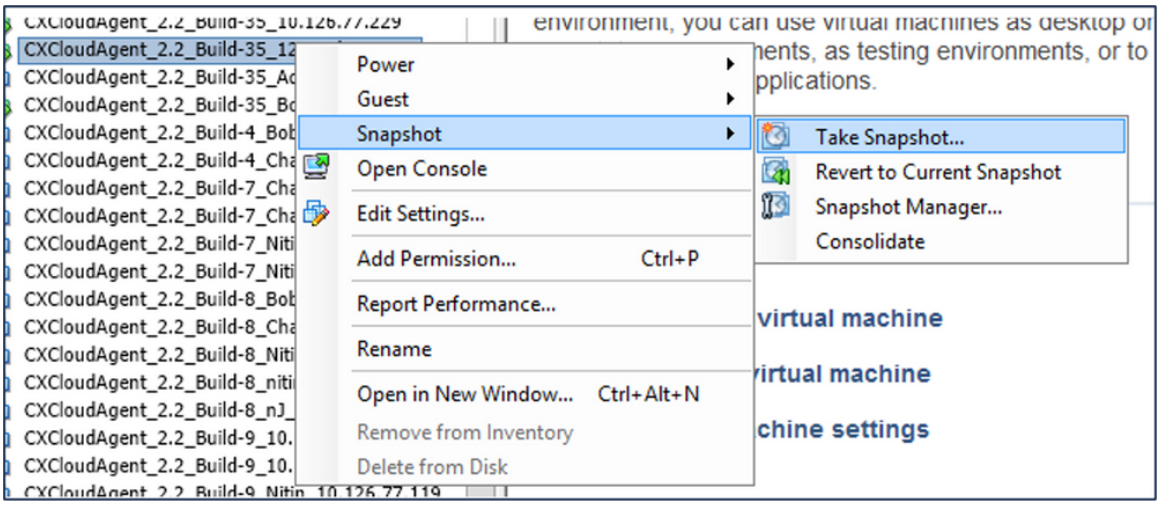
Backup und Wiederherstellung des CX Cloud VM

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

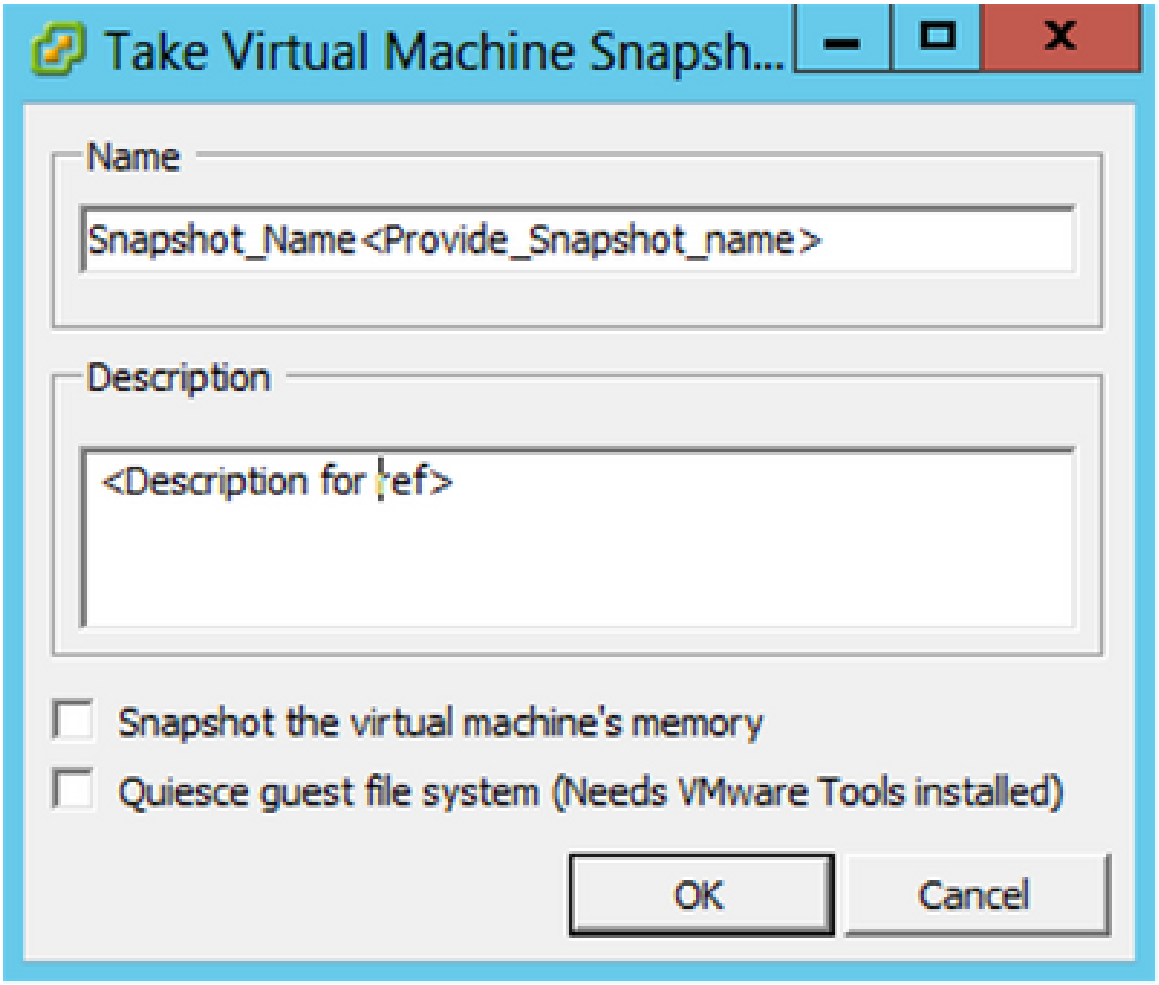
Sichern

So sichern Sie die CX Cloud VM:

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



VM auswählen



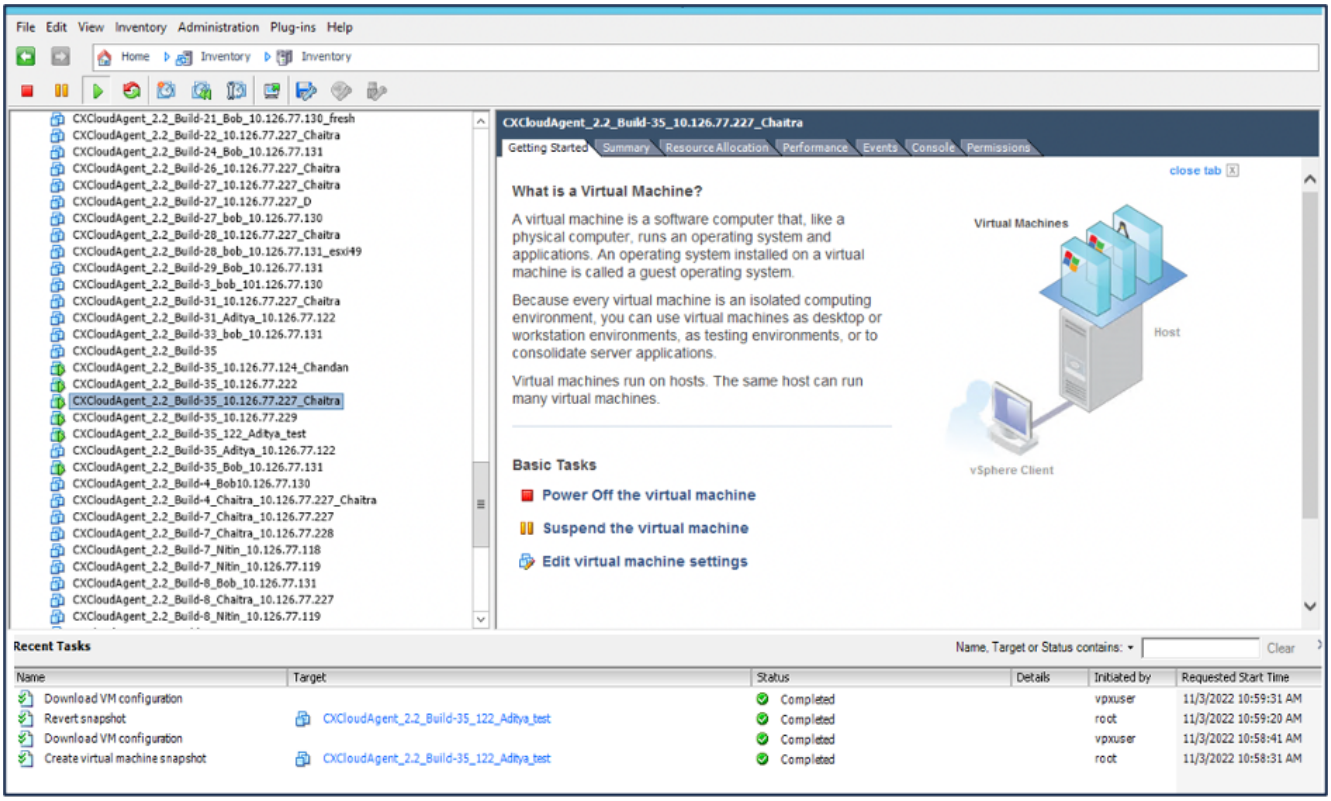
Snapshot des virtuellen Systems erstellen

2. Geben Sie einen Namen und eine Beschreibung ein.

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

---

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

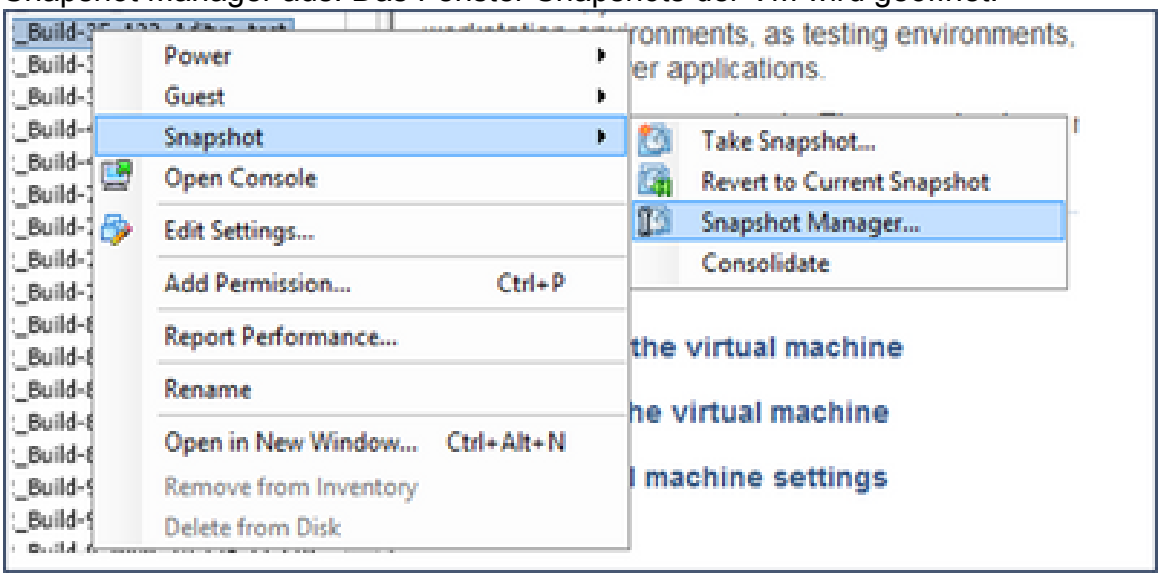


Zuletzt durchgeführte Aufgaben

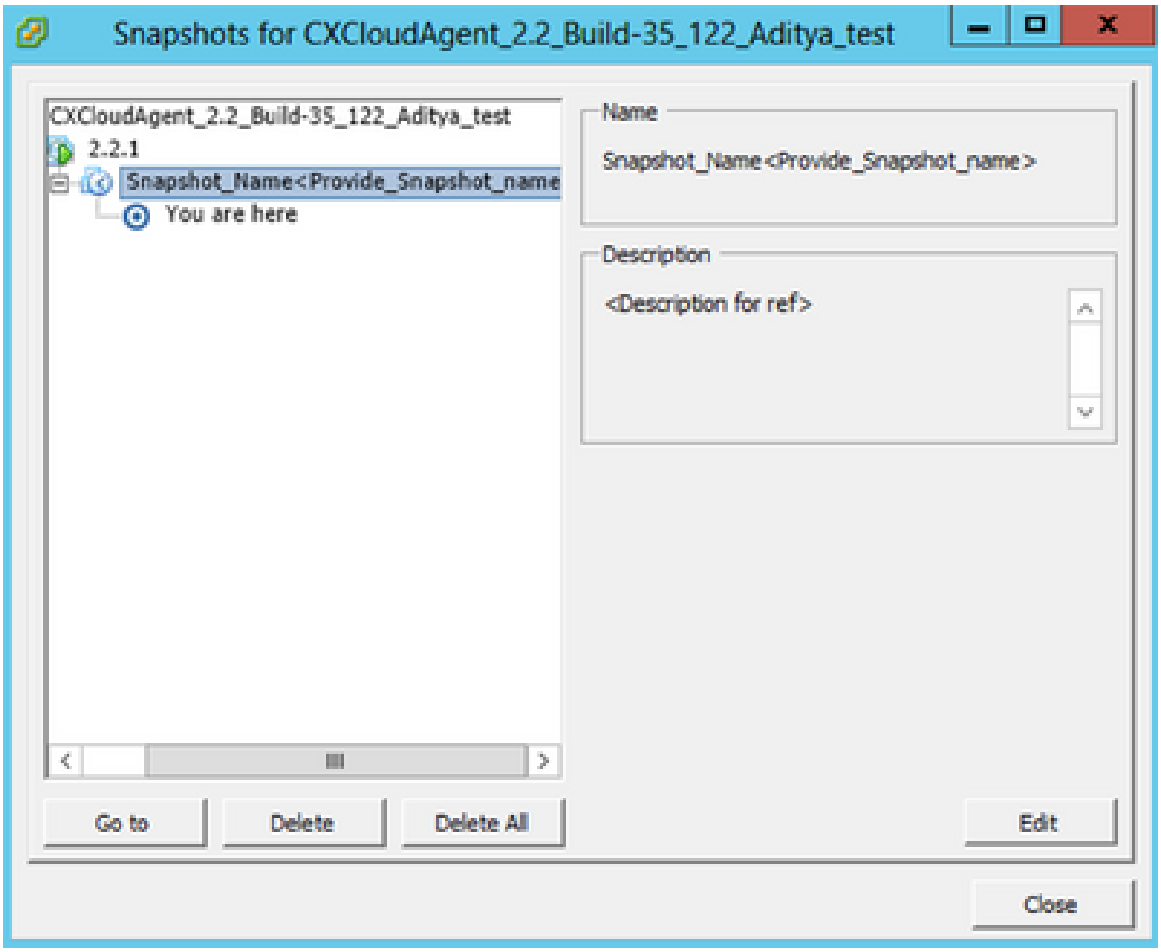
Wiederherstellen

So stellen Sie die CX Cloud VM wieder her:

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

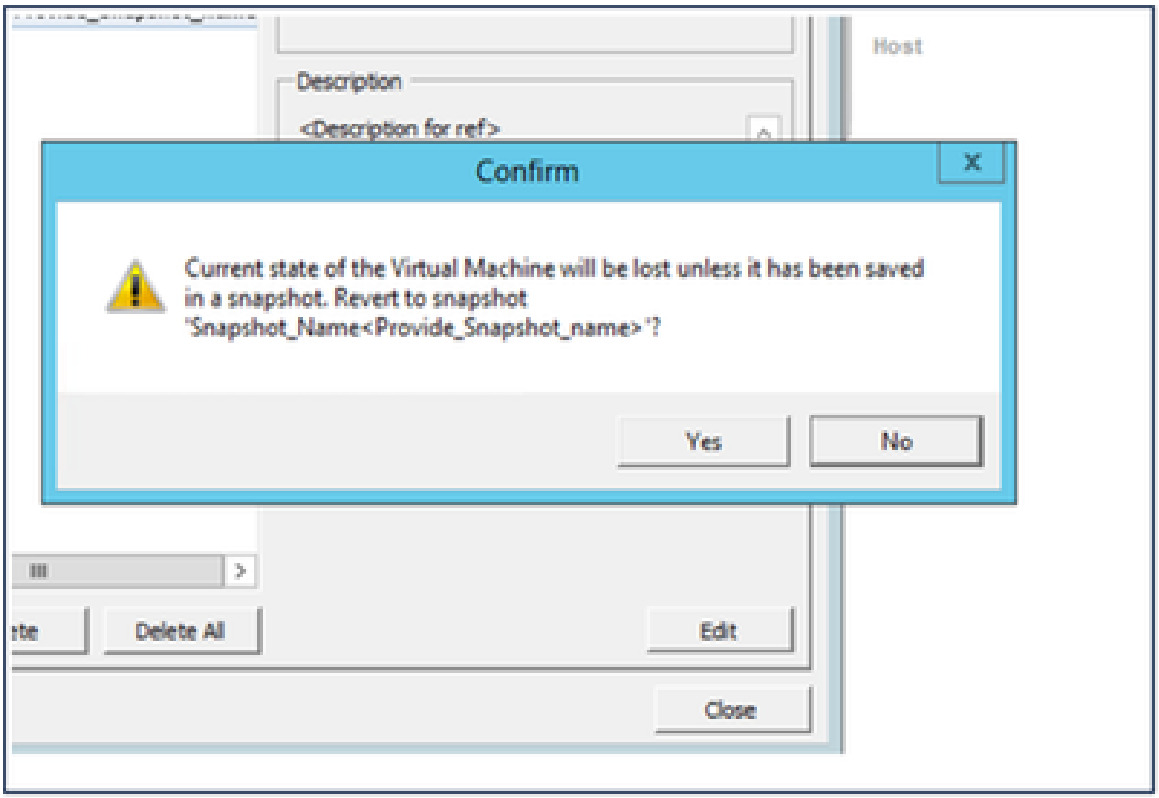


Fenster "VM auswählen"



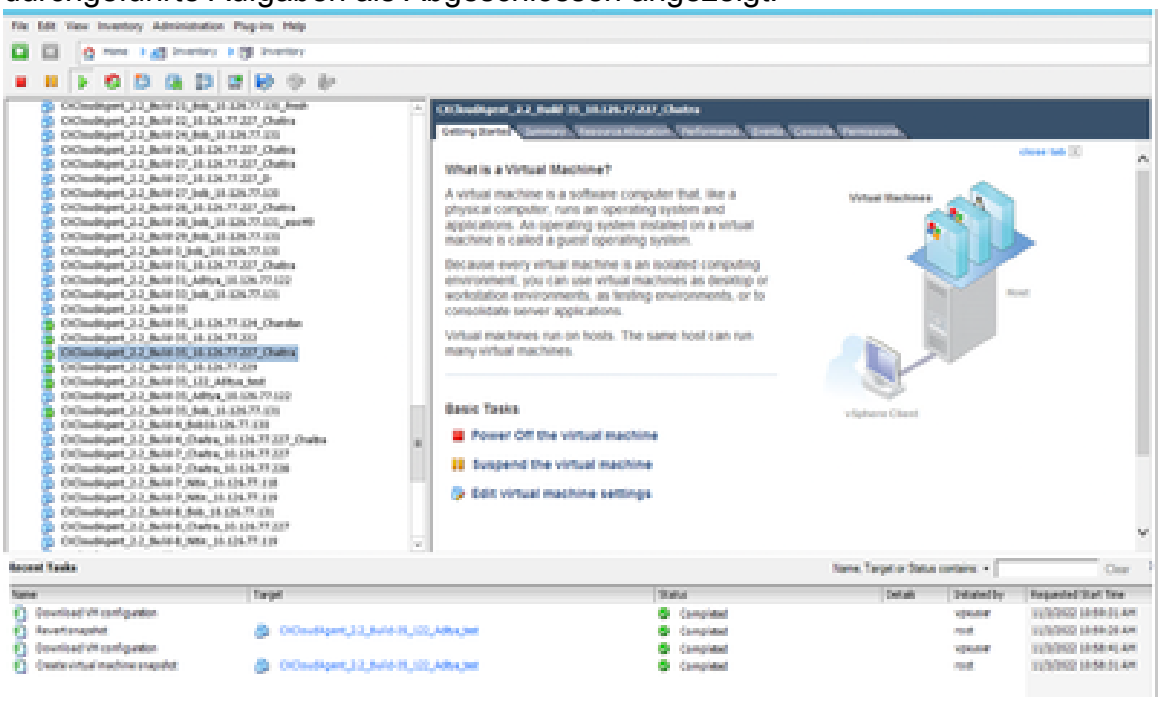
Fenster Snapshots

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



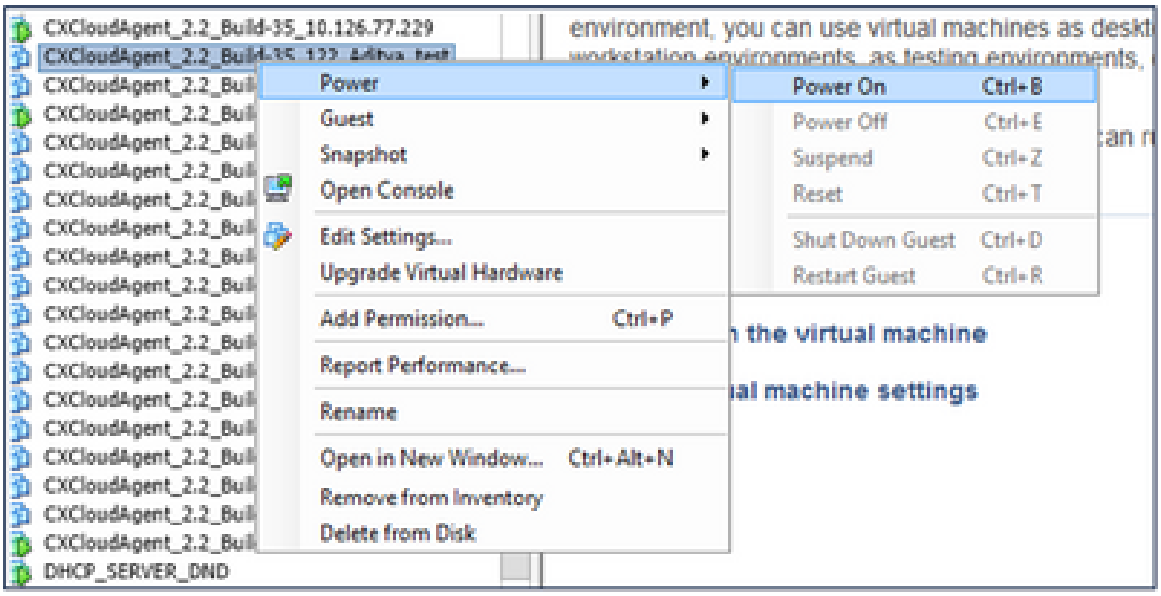
Fenster bestätigen

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



Zuletzt durchgeführte Aufgaben

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



Sicherheit

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

Personen- und Gebäudeschutz

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

Kontosicherheit

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

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

Netzwerksicherheit

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

Authentifizierung

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

- Privilegierte Aktionen auf der Appliance mit SSH rooten.

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

Härtung

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

Datensicherheit

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

Datenübertragung

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

Protokolle und Überwachung

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

Cisco Telemetrie-Befehle

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

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

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

Sicherheitszusammenfassung

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

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

Informationen zu dieser Übersetzung

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