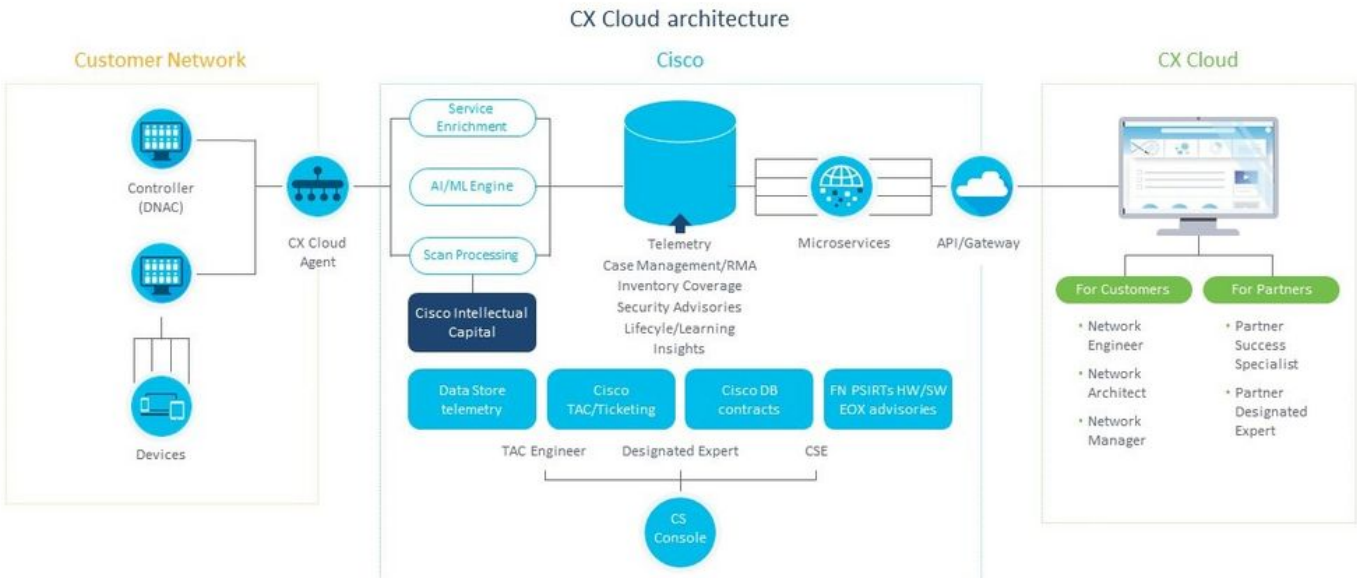
CX Cloud Agent - Überblick v2.0

Inhalt

Einleitung

In diesem Dokument wird der Cisco Customer Experience (CX) Cloud Agent beschrieben. Der (CX) Cloud Agent von Cisco ist eine modernisierte modulare Softwareplattform vor Ort, die leichte containerisierte Microservice-Funktionen hostet. Diese Funktionen können vor Ort über die Cloud installiert, konfiguriert und verwaltet werden. CX Cloud Agent beschleunigt die Monetarisierung neuer Angebote, skaliert Funktionen und unterstützt die Entwicklung von Services der nächsten Generation, die auf Big Data, Analysen, Automatisierung, maschinellem Lernen/künstlicher Intelligenz (ML/AI) und Streaming basieren.

> **Anmerkung:** Dieses Handbuch richtet sich an Benutzer von CX Cloud Agent v2.0. Weitere Informationen finden Sie unter Cisco CX Cloud Agent.



Architektur von CX Cloud Agent

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

Voraussetzungen

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

Voraussetzungen für die Bereitstellung:

- Jeder dieser Hypervisoren: VMWare ESXi Version 5.5 oder höherOracle VirtualBox 5.2.30Windows Hypervisor Version 2012 bis 2016

- Der Hypervisor kann eine VM hosten, die Folgendes erfordert: CPU mit 8 Kernen16 GB Arbeitsspeicher/RAM200 GB Festplattenspeicher
- Für Kunden, die bestimmte Cisco UCS-Rechenzentren als primäre Datenregion für die Speicherung von CX Cloud-Daten verwenden:
  Der CX Cloud Agent muss in der Lage sein, über den FQDN und HTTPS auf dem TCP-Port 443 eine Verbindung zu den hier gezeigten Servern herzustellen:
  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 Cisco Europe-Rechenzentren als primäre Datenregion für die Speicherung von CX Cloud-Daten verwenden:
  Der CX Cloud 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.cisco.cloud
  FQDN: ng.acs.agent.emea.csco.cloud
  FQDN: cloudsso.cisco.com
  FQDN: api-cx.cisco.com
- Für Kunden, die bestimmte Cisco 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 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 die ausgewiesenen Rechenzentren von Cisco in Europa und im Cisco Asien-Pazifik-Raum als primäre Datenregion nutzen, gilt: 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.

Weitere Hinweise zum CX Cloud Agent:

- Eine IP wird automatisch erkannt, wenn 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 verfügbar sein.
- Nur IPv4 wird unterstützt, nicht IPv6.
- Die zertifizierten Single Node- und High Availability (HA)-Cluster Cisco Digital Network Architecture (DNA) Center-Versionen von 1.2.8 bis 1.3.3.9 und 2.1.2.0 bis 2.2.3.5 sind erforderlich.
- Wenn das Netzwerk über eine SSL-Überwachung verfügt, geben Sie die IP-Adresse des CX Cloud Agent an.

Zugriff auf kritische Domänen

Um mit der CX Cloud zu beginnen, benötigen Benutzer Zugriff auf diese Domänen.

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

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

Voraussetzungen für Upgrade auf CX Cloud Agent v2.0

Die in diesem Abschnitt beschriebenen Voraussetzungen müssen vor dem Upgrade auf CX Cloud Agent v2.0 erfüllt sein.

1. Stellen Sie sicher, dass CX Cloud Agent v1.12.x oder höher vor Beginn des Upgrades installiert werden muss.
2. Führen Sie die folgenden Schritte aus, um den Domain Name Server zu konfigurieren, wenn er noch nicht konfiguriert ist:
   Melden Sie sich an der CLI-Konsole (Command Line Interface) der CX Cloud Agent Virtual Machine an.Führen Sie den Befehl *cxcli agent configureDNS* aus.Geben Sie die DNS-IP-Adresse ein.Klicken Sie auf Exit.
3. Stellen Sie sicher, dass das Netzwerk des Kunden den Domänennamen in Critical Domain Access ermöglicht, die Neuregistrierung des Cloud Agent während der Migration abzuschließen. CX Cloud Agent muss diese Domänen erreichen können, und auch die Domänen müssen vom DNS-Server auflösbar sein. Wenden Sie sich an das Netzwerkteam, wenn eine Domäne nicht erreichbar ist.
4. Erstellen Sie einen Snapshot des virtuellen Cloud Agent, bevor Sie ein Upgrade auf v2.0 starten (ordnungsgemäßer Zugriff erforderlich).

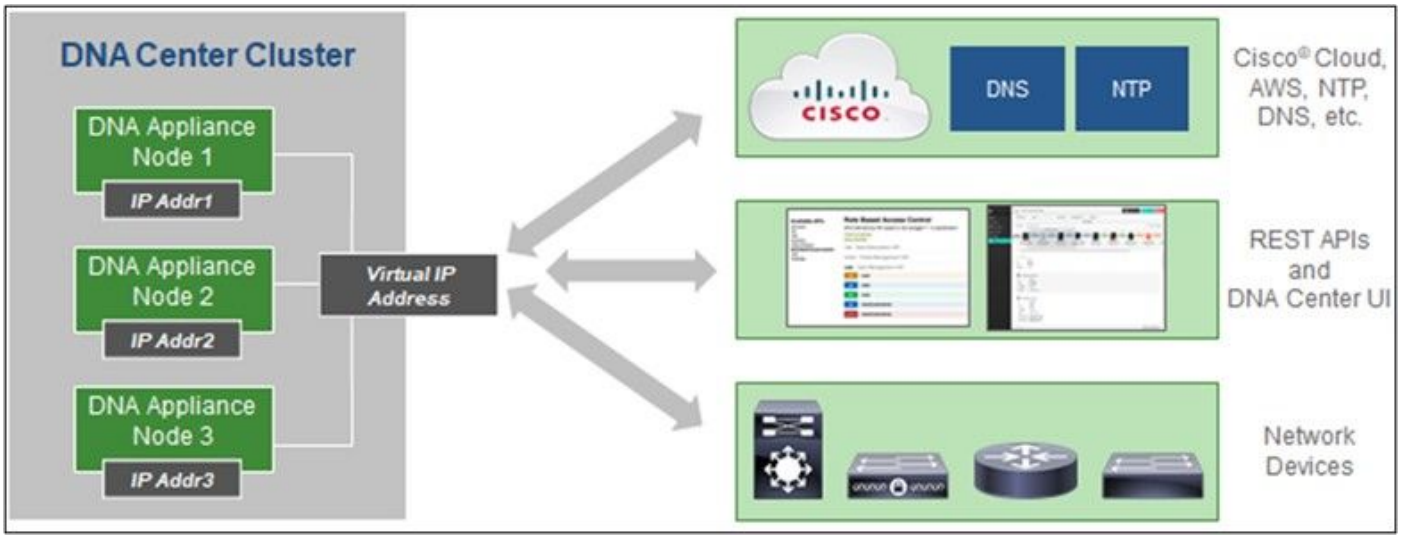
   Anmerkung: Versionen vor 1.10 müssen zuerst auf v1.10 aktualisiert werden, gefolgt von inkrementellen Upgrades auf v1.12.x und dann auf v2.0. Benutzer können im CX Cloud-Portal von "Admin Settings > Data Sources" (Admin-Einstellungen > Datenquellen) ein Upgrade durchführen. Klicken Sie auf View Update um das Upgrade abzuschließen.

Die folgenden Bedingungen müssen für eine erfolgreiche Einrichtung erfüllt werden:

1. Liste der DNACs und ihrer Anmeldeinformationen
2. DNAC-Benutzer mit **Admin**- oder **Observer**-Rollenzugriff
3. Virtuelle IP-Adresse oder eigenständige/physische IP-Adresse für DNAC-Cluster
4. Erfolgreiche Erreichbarkeit zwischen Cloud Agent und DNAC
5. Für DNAC muss mindestens ein verwaltetes Gerät vorhanden sein.

Für Cisco DNA Center zertifizierte Versionen

Die zertifizierten Versionen von Cisco DNA Center für Einzelknoten und HA-Cluster reichen von 1.2.8 bis 1.3.3.9 und von 2.1.2.0 bis 2.2.3.5.



Cisco DNA Center mit HA-Cluster mit mehreren Knoten

Unterstützte Browser

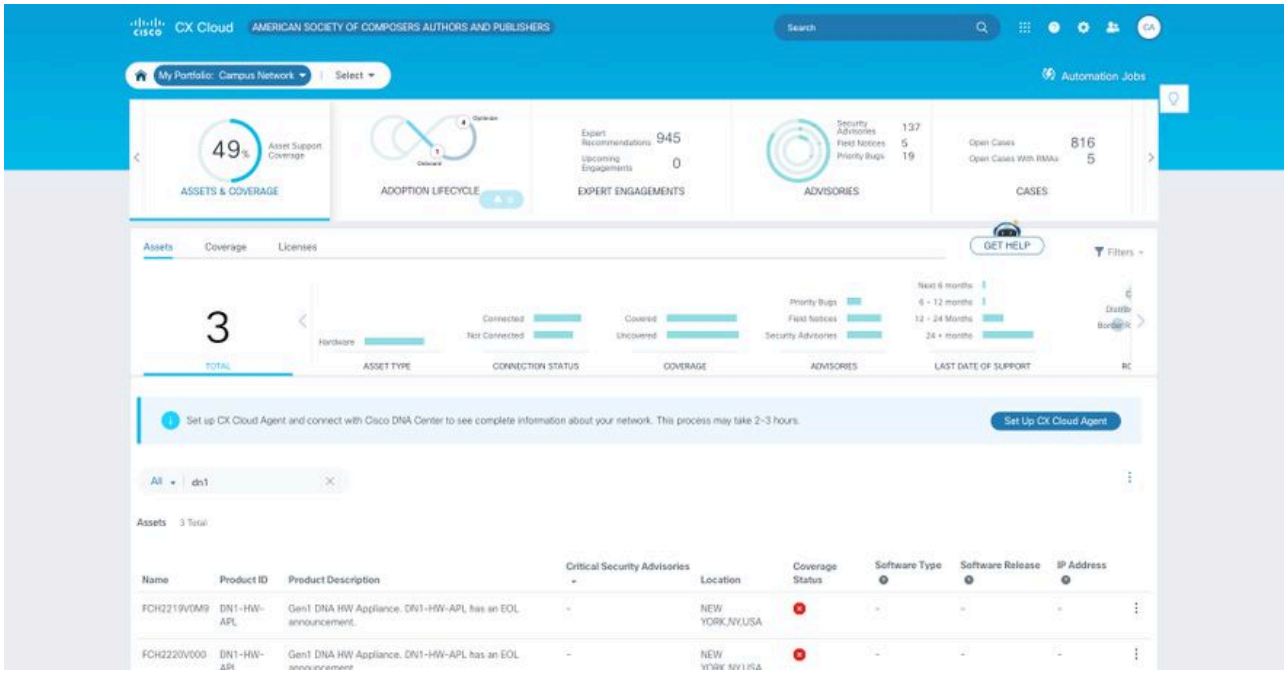
Für eine optimale Nutzung auf Cisco.com empfehlen wir die neueste offizielle Version dieser Browser:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Bereitstellung von CX Cloud Agent

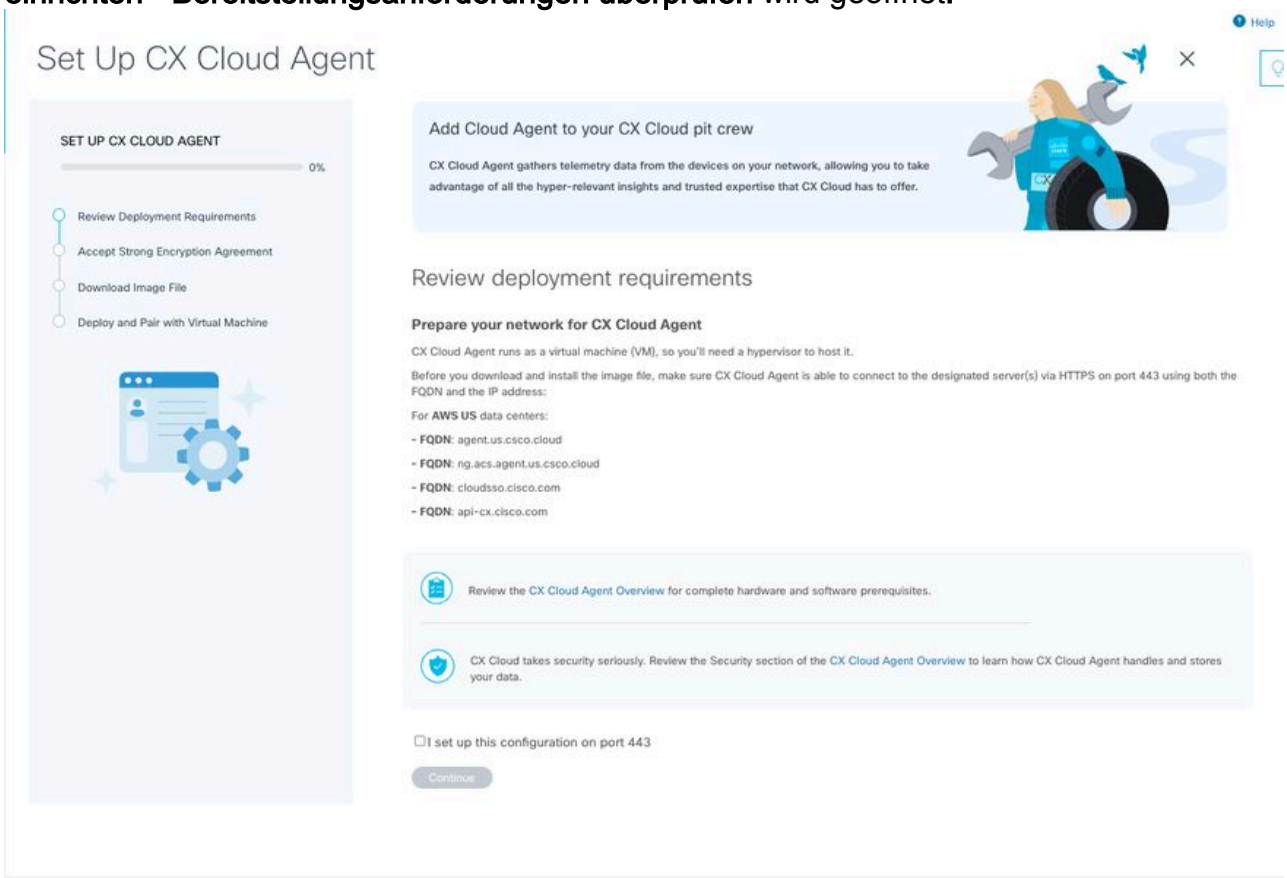
So stellen Sie CX Cloud Agent bereit:

1. Klicken Sie auf cx.cisco.com, um sich bei CX Cloud anzumelden.
2. Auswählen Campus Network und navigieren Sie zu ASSETS & COVERAGE Kachel.



Startseite

3. Klicken Sie im Banner auf **CX Cloud Agent einrichten**. Das Fenster **CX Cloud Agent einrichten - Bereitstellungsanforderungen überprüfen** wird geöffnet.



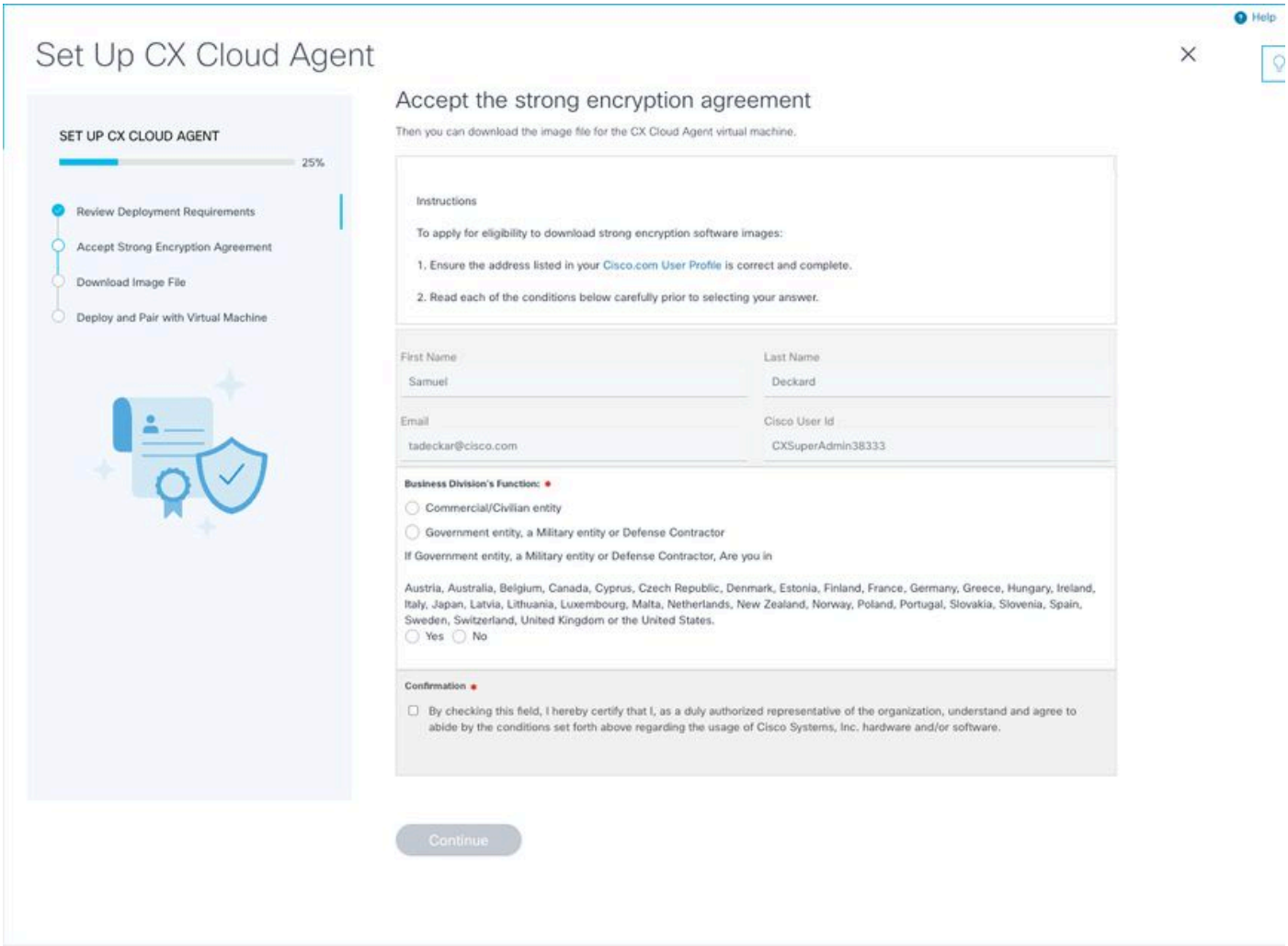
Prüfung der Bereitstellungsanforderungen

4. Lesen Sie die Voraussetzungen unter **Prüfen der Bereitstellungsanforderungen**, und aktivieren Sie das Kontrollkästchen, damit **ich diese Konfiguration auf Port 443 eingerichtet habe**.

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

5. Klicken Sie auf **Weiter**. Das Fenster **CX Cloud Agent einrichten - Starke**

Verschlüsselungsvereinbarung akzeptieren wird geöffnet.



Verschlüsselungsvereinbarung

6. Überprüfen Sie die bereits eingegebenen Informationen in den Feldern **Vorname, Nachname, E-Mail** und **CCO-Benutzer-ID**.

7. Wählen Sie die entsprechende Business division's function.

8. Wählen Sie Confirmation um den Nutzungsbedingungen zuzustimmen.

9. Klicken Sie auf **Weiter**. Das Fenster **CX Cloud Agent einrichten - Bilddatei herunterladen** wird geöffnet.

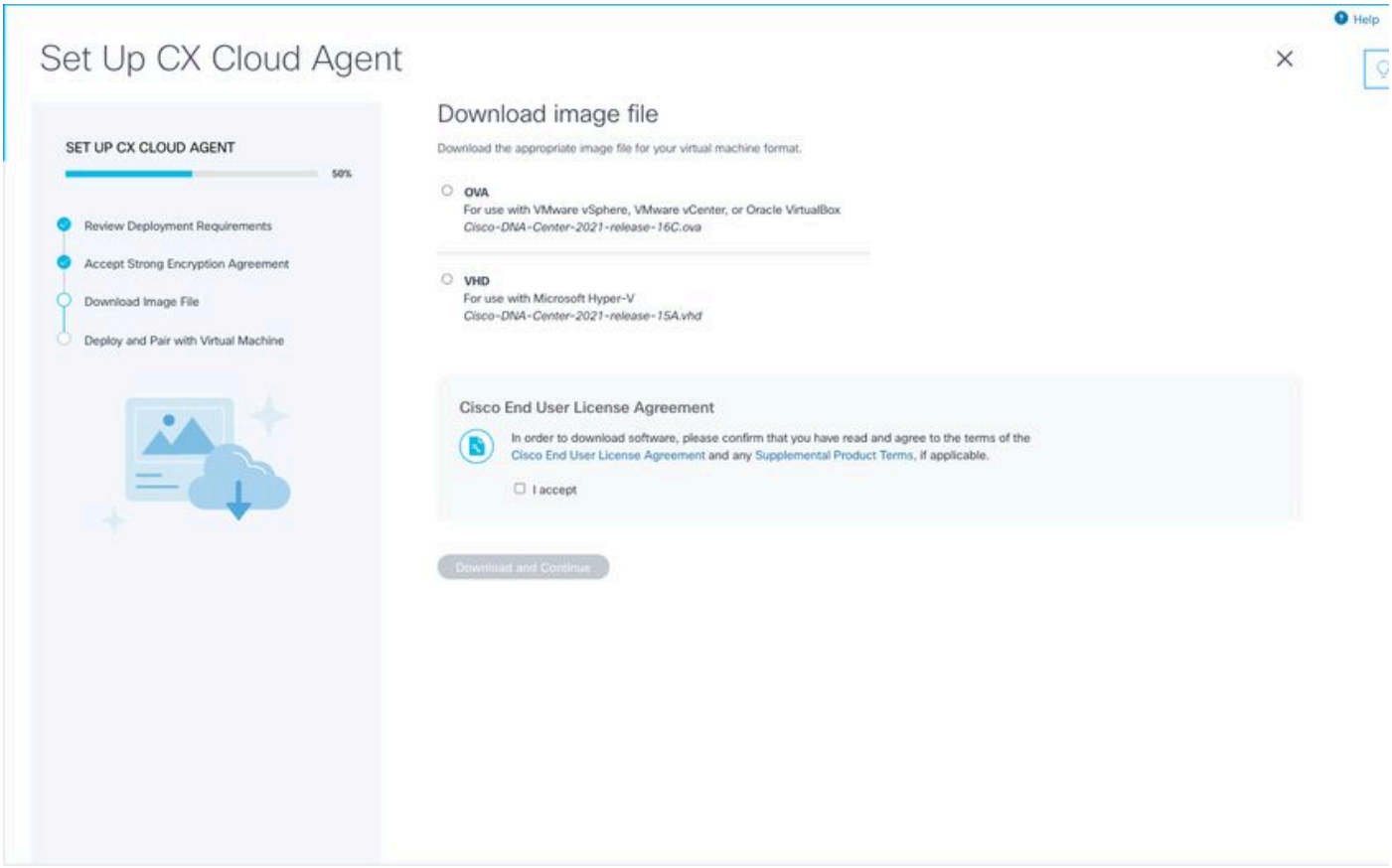


Image herunterladen

10. Wählen Sie das entsprechende Dateiformat aus, um die für die Installation erforderliche Image-Datei herunterzuladen.

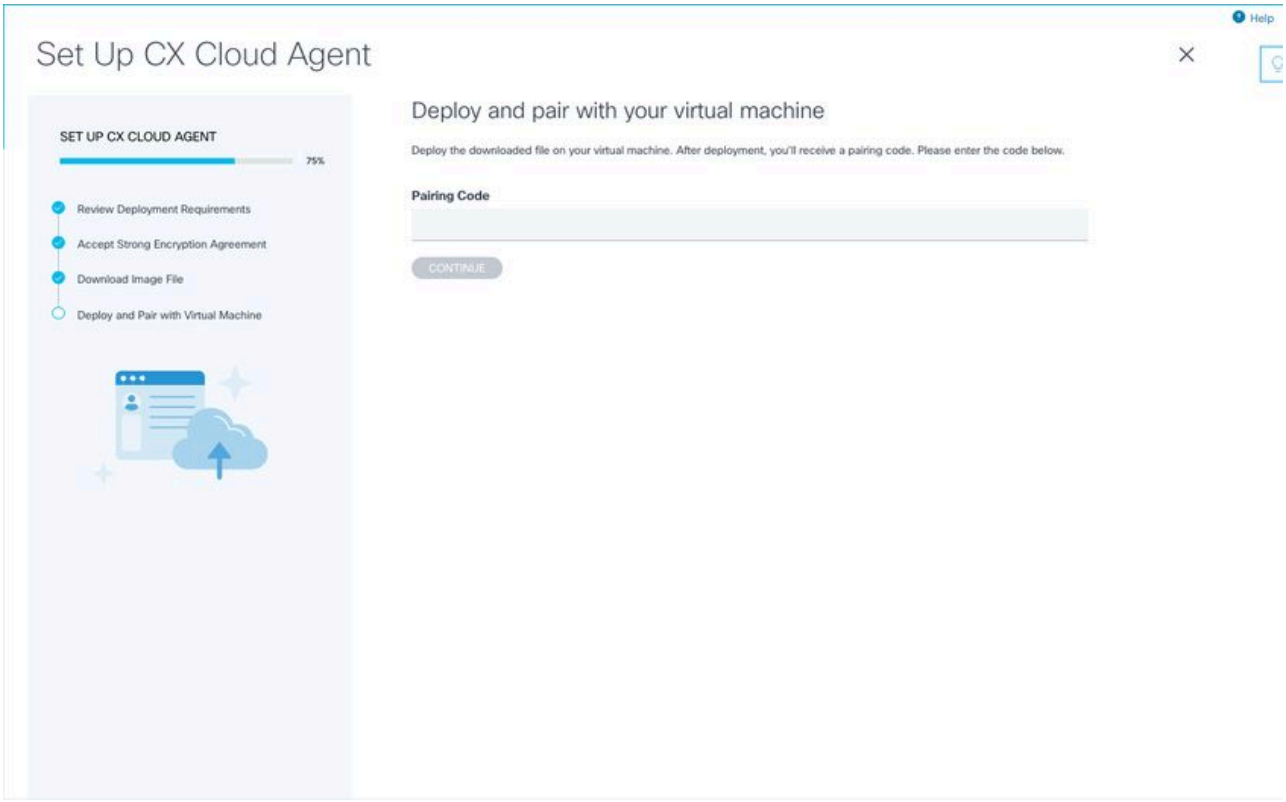
11. Aktivieren Sie das Kontrollkästchen **Ich akzeptiere**, um der Cisco Endbenutzer-Lizenzvereinbarung zuzustimmen.

12. Klicken Sie auf **Herunterladen und fortfahren**. Das Fenster **CX Cloud Agent einrichten - Bereitstellen und mit dem virtuellen System koppeln** wird geöffnet.

13. Weitere Informationen zur Installation von CX Cloud Agent finden Sie unter Netzwerkkonfiguration für die OVA-Installation. Fahren Sie dann mit dem nächsten Abschnitt fort.

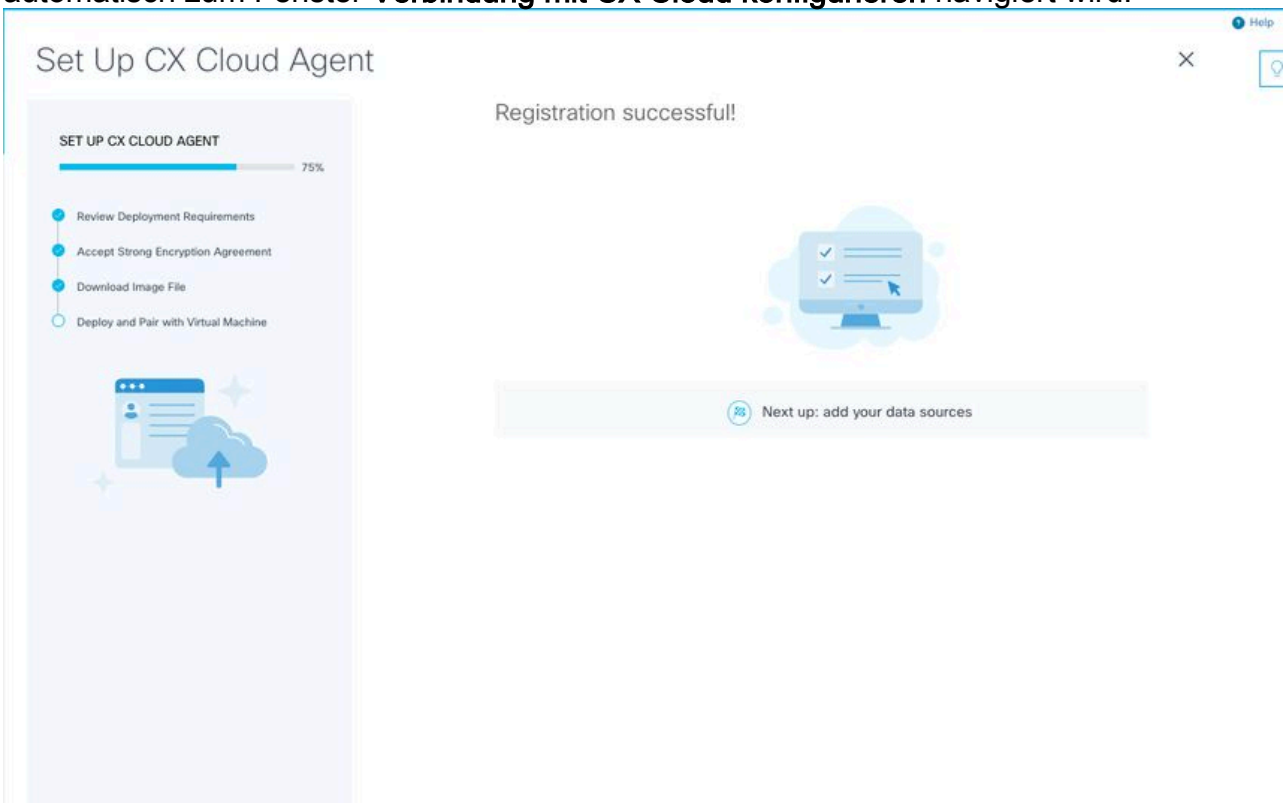
Verbindung zwischen CX Cloud Agent und CX Cloud

1. Geben Sie den **Kopplungscode** im Konsolendialog oder in der Befehlszeilenschnittstelle (CLI) ein.

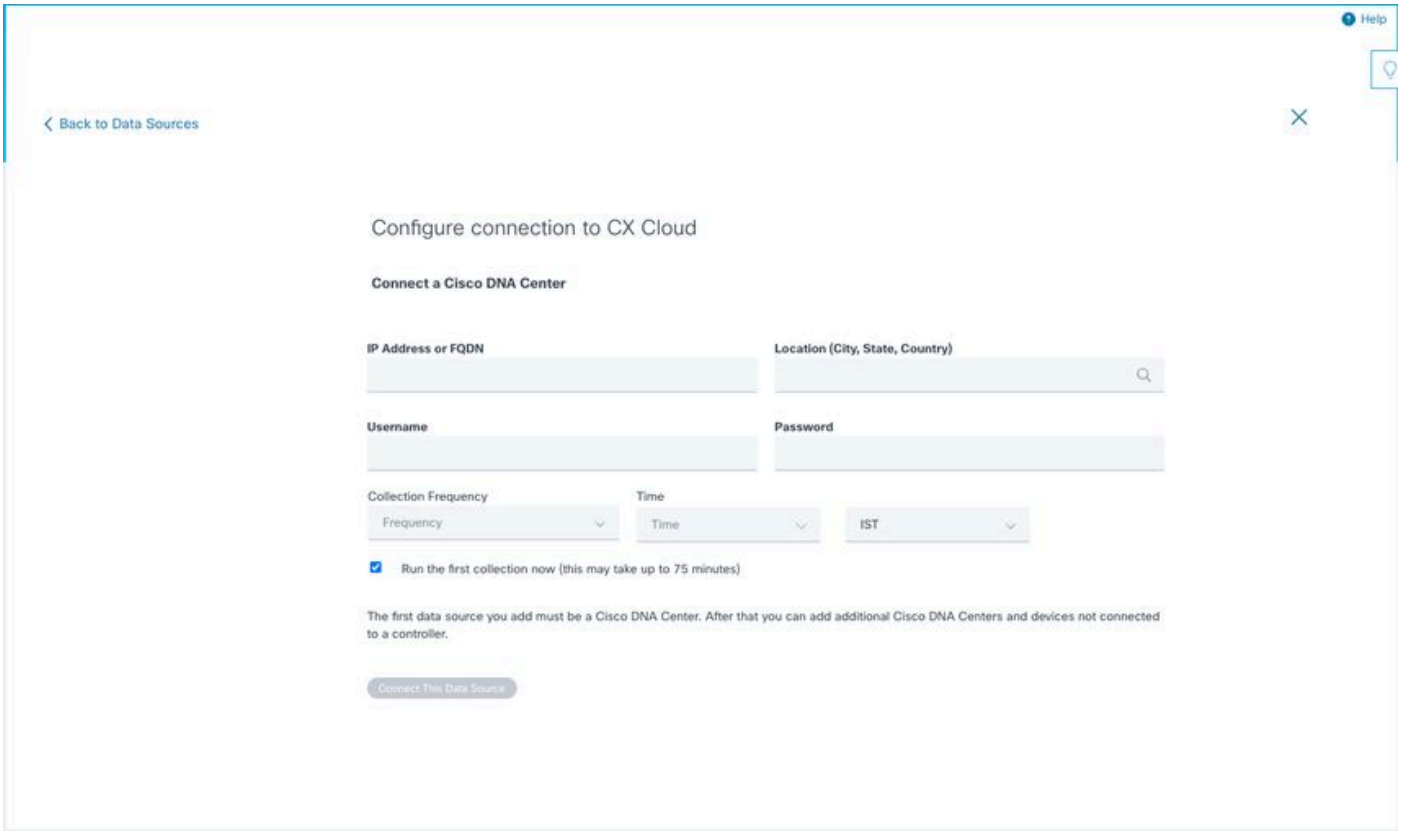


Kopplungscode

2. Klicken Sie auf **Weiter**, um den CX Cloud Agent zu registrieren. Das Fenster **CX Cloud Agent einrichten - Registrierung erfolgreich** wird einige Sekunden lang angezeigt, bevor automatisch zum Fenster **Verbindung mit CX Cloud konfigurieren** navigiert wird.

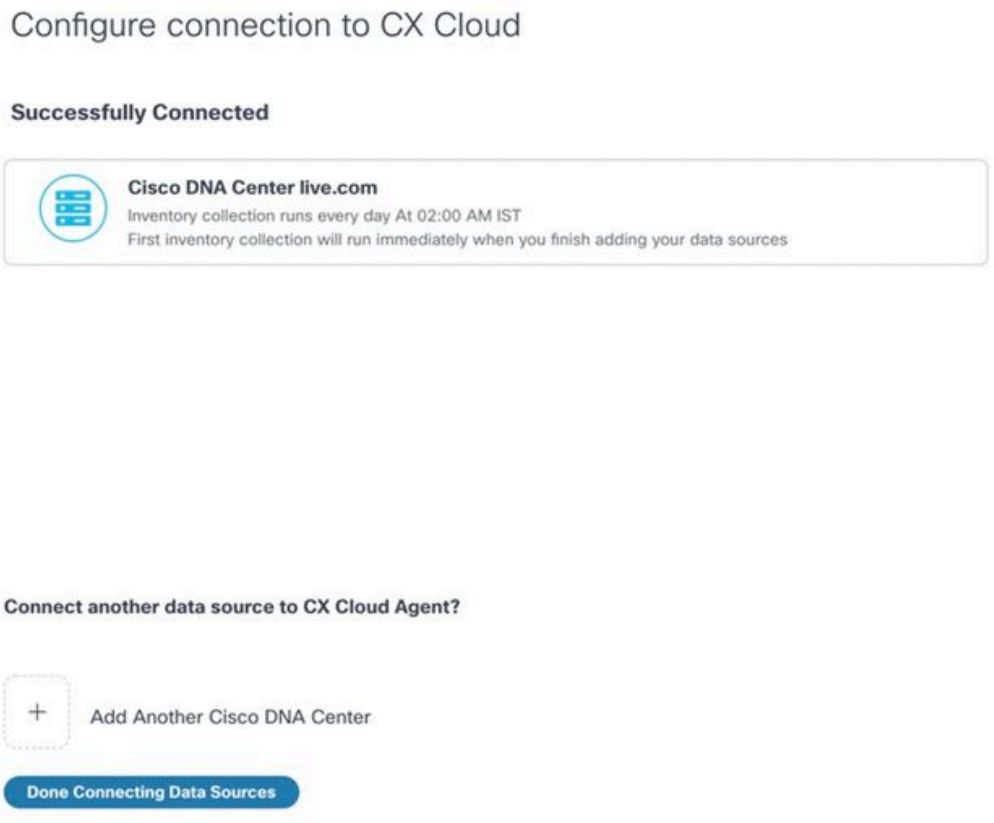


Registrierung erfolgreich



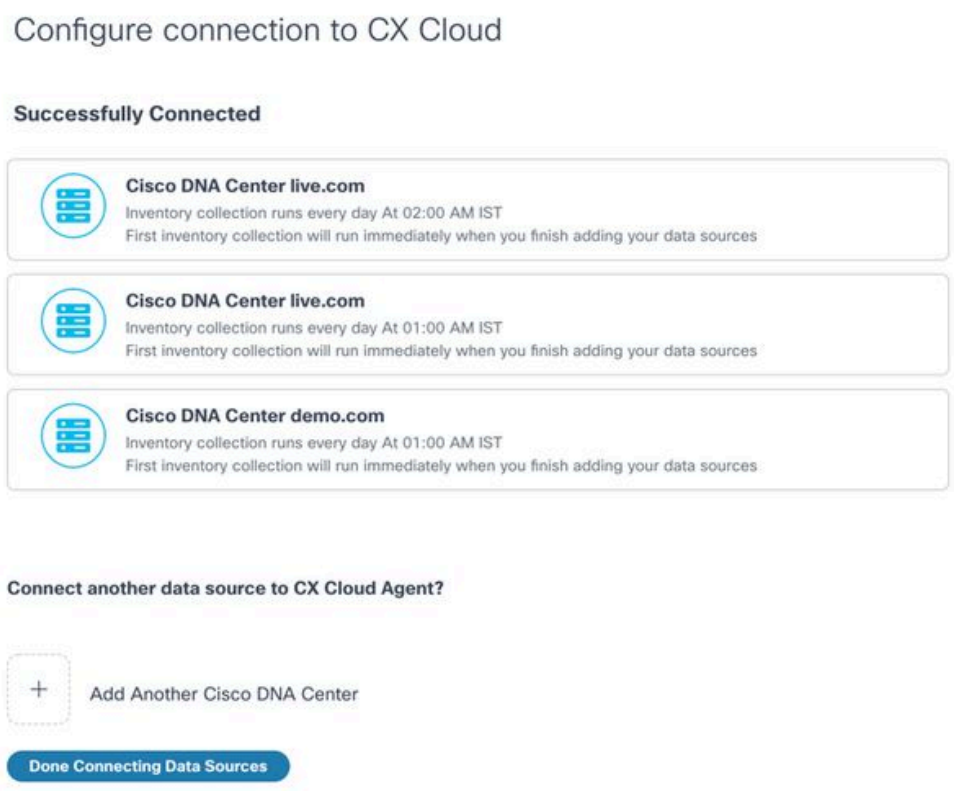
Verbindung konfigurieren

3. Geben Sie Daten ein, und klicken Sie auf **Diese Datenquelle verbinden**. Die Bestätigungsmeldung "Successfully Connected" wird angezeigt.



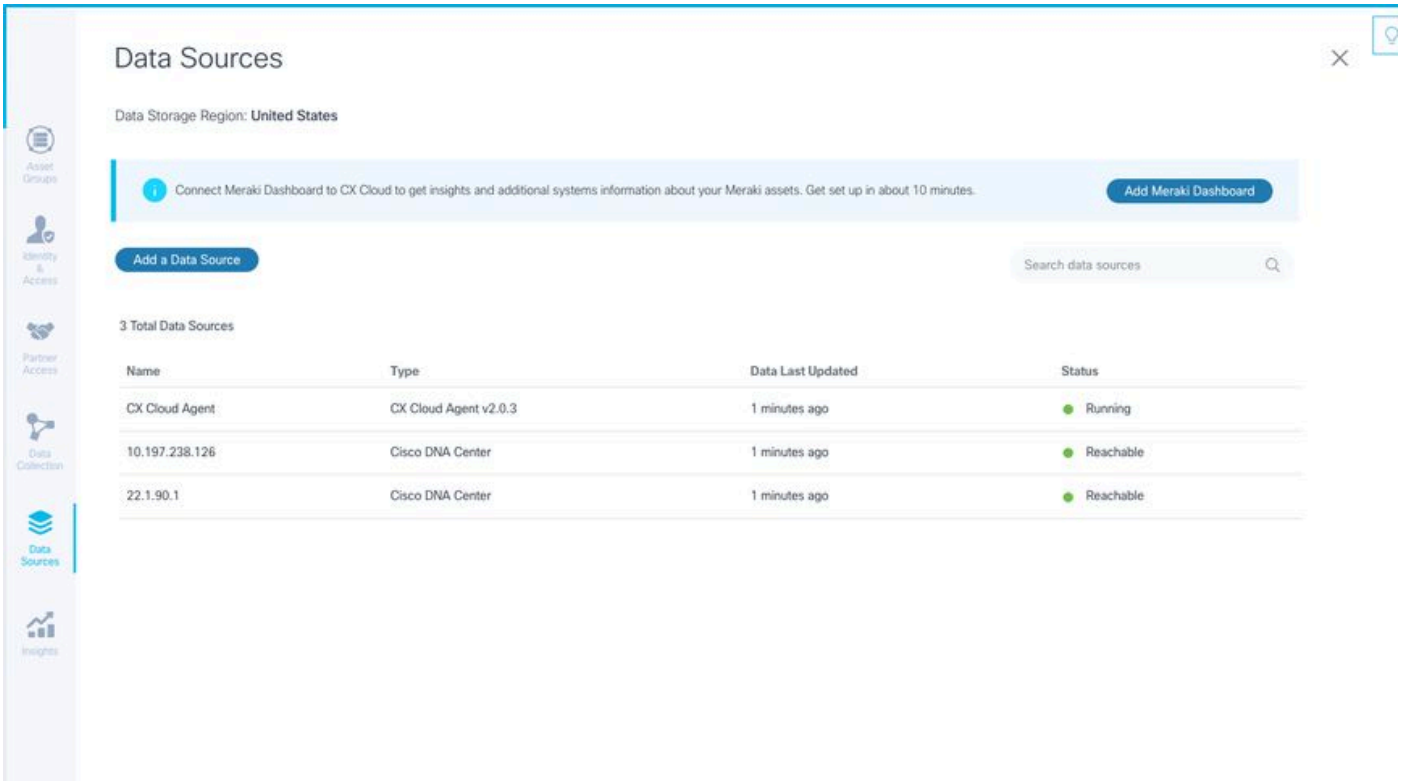
DNAC erfolgreich hinzugefügt

Anmerkung: Klicken Sie auf Add Another Cisco DNA Centerum mehrere DNACs hinzuzufügen.



Mehrere DNACs hinzugefügt

4. Klicken Sie auf **Fertig Verbinden von Datenquellen**. Das Fenster **Datenquellen** wird geöffnet.



Datenquellen

Bereitstellung und Netzwerkkonfiguration

Für die Bereitstellung von CX Cloud Agent können folgende Optionen ausgewählt werden:

- Wenn Sie VMware vSphere/vCenter Thick Client ESXi 5.5/6.0 auswählen, wechseln Sie zu Thick Client
- Wenn Sie VMware vSphere/vCenter Web Client ESXi 6.0 auswählen, wechseln Sie zu Web Client vSphere oder Center
- Wenn Sie Oracle VirtualBox 5.2.30 auswählen, wechseln Sie zu Oracle VM
- Wenn Sie Microsoft Hyper-V auswählen, wechseln Sie zu Hyper-V

OVA-Bereitstellung

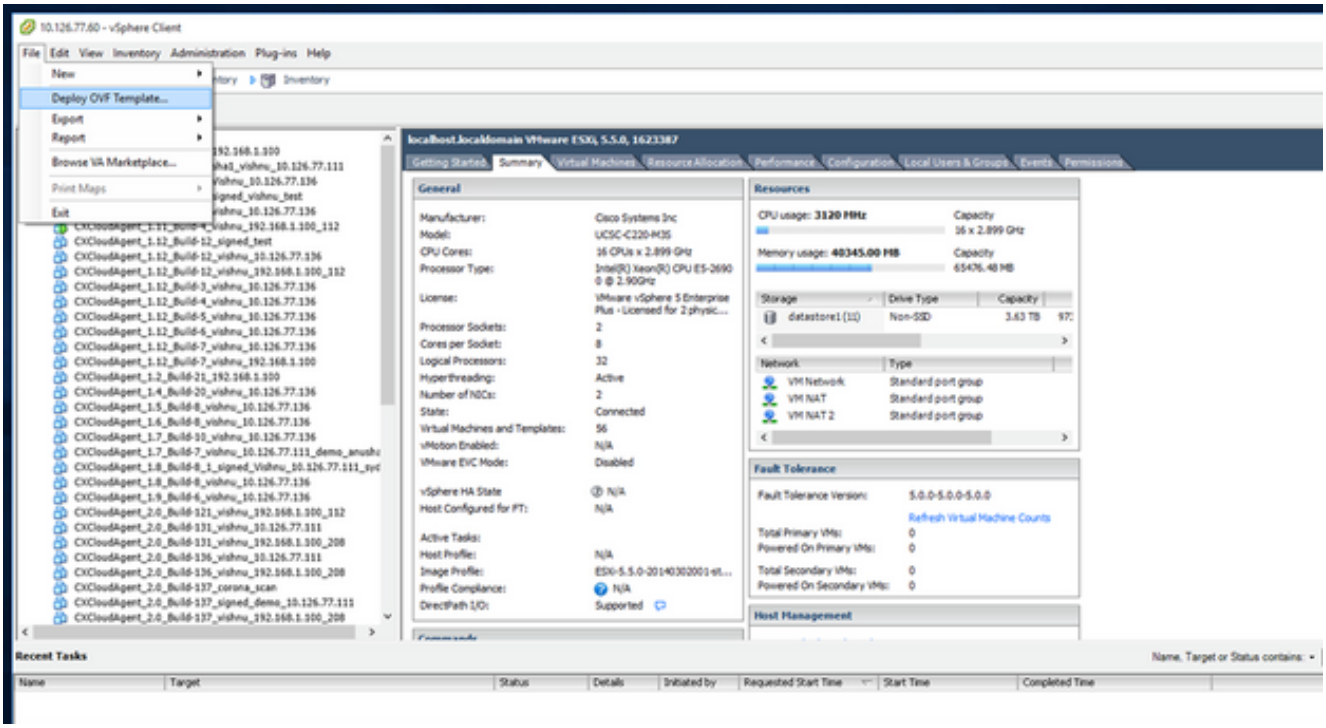
Installation von Thick Client ESXi 5.5/6.0

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.

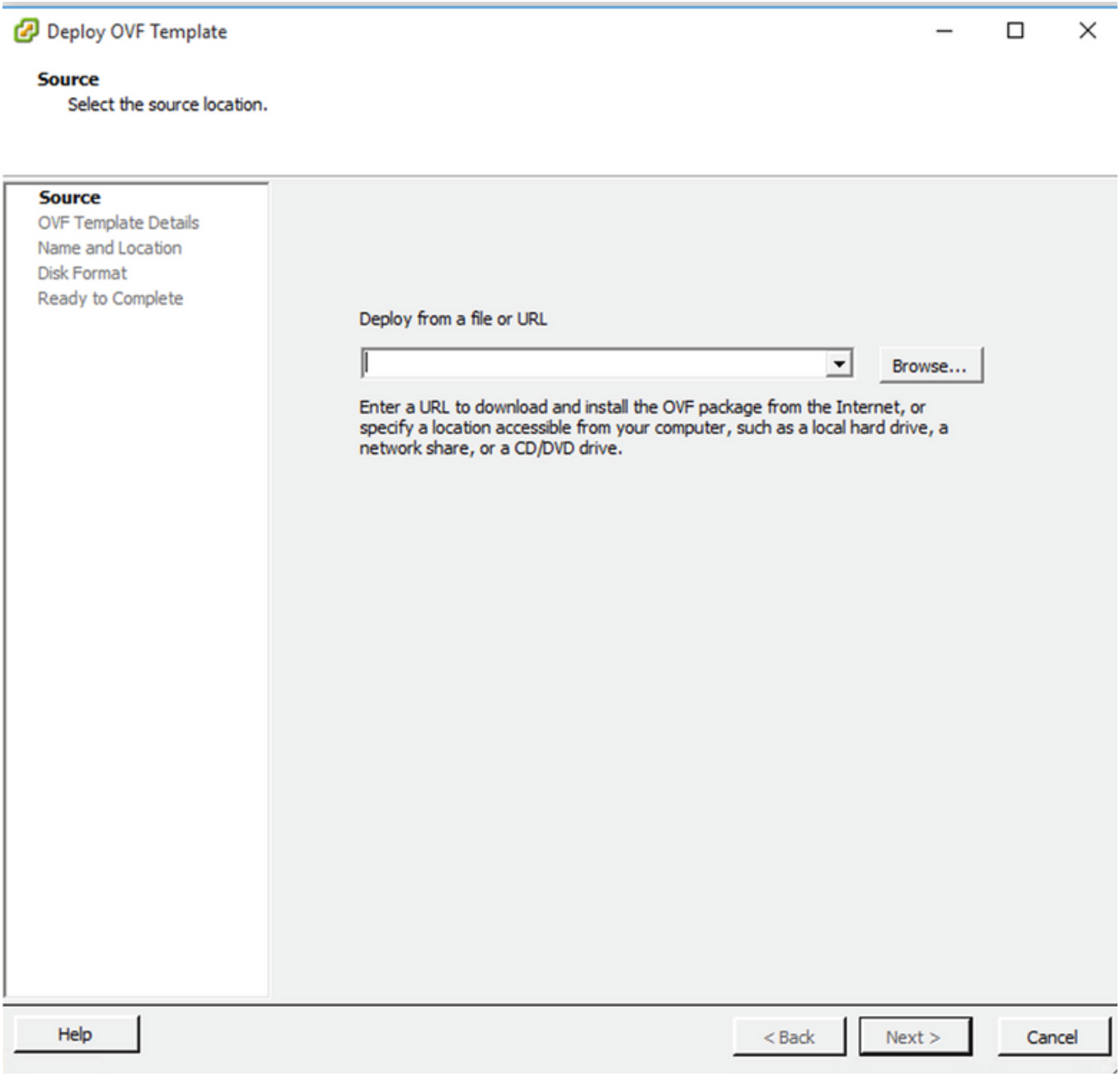
Anmelden

2. Navigieren Sie zu File > Deploy OVF Template.



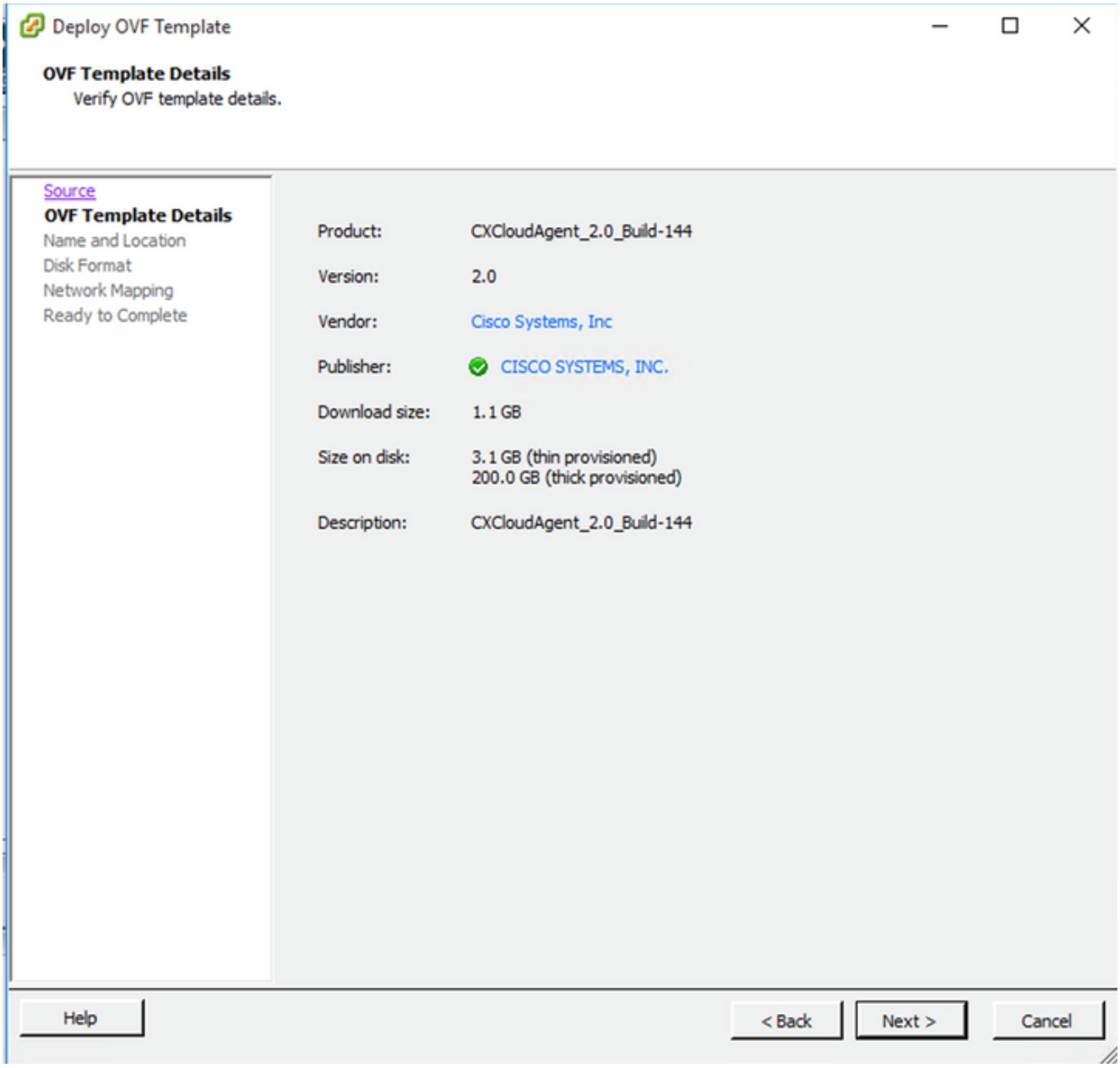
vSphere-Client

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



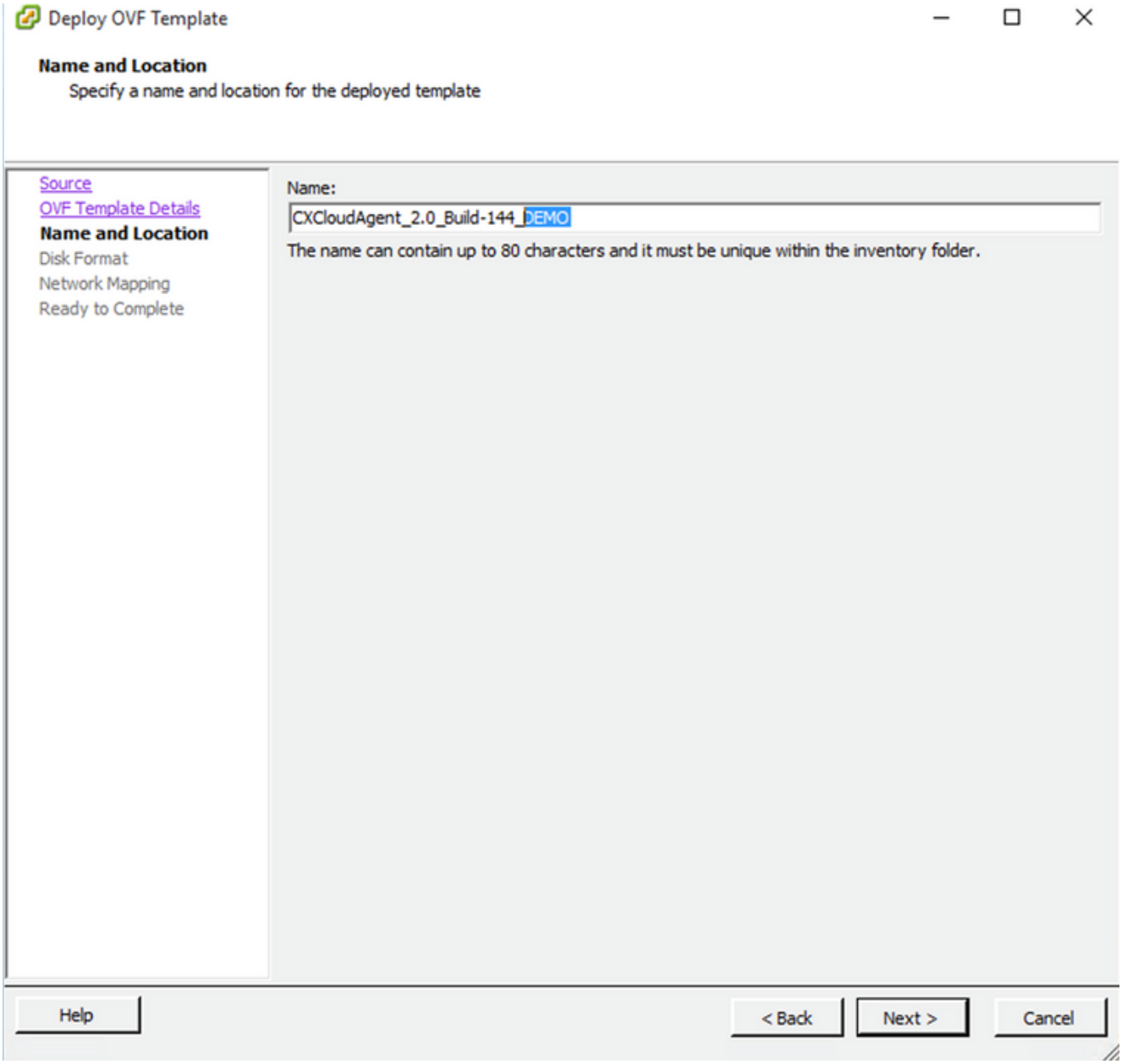
OVA-Pfad

4. Überprüfen Sie OVF Details und klicke auf Next.



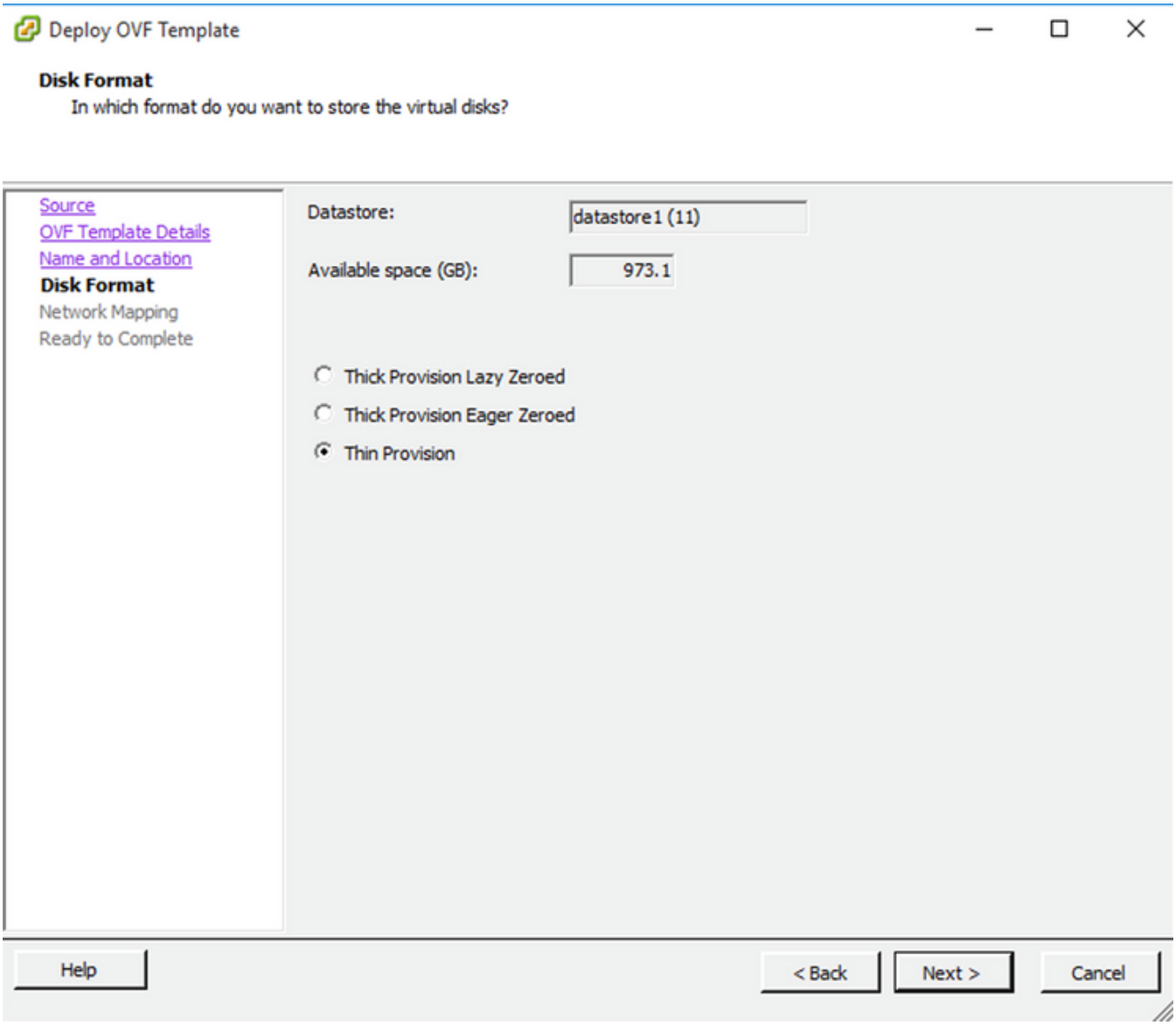
Vorlagendetails

5. Geben Sie Unique Name und klicke auf Next.



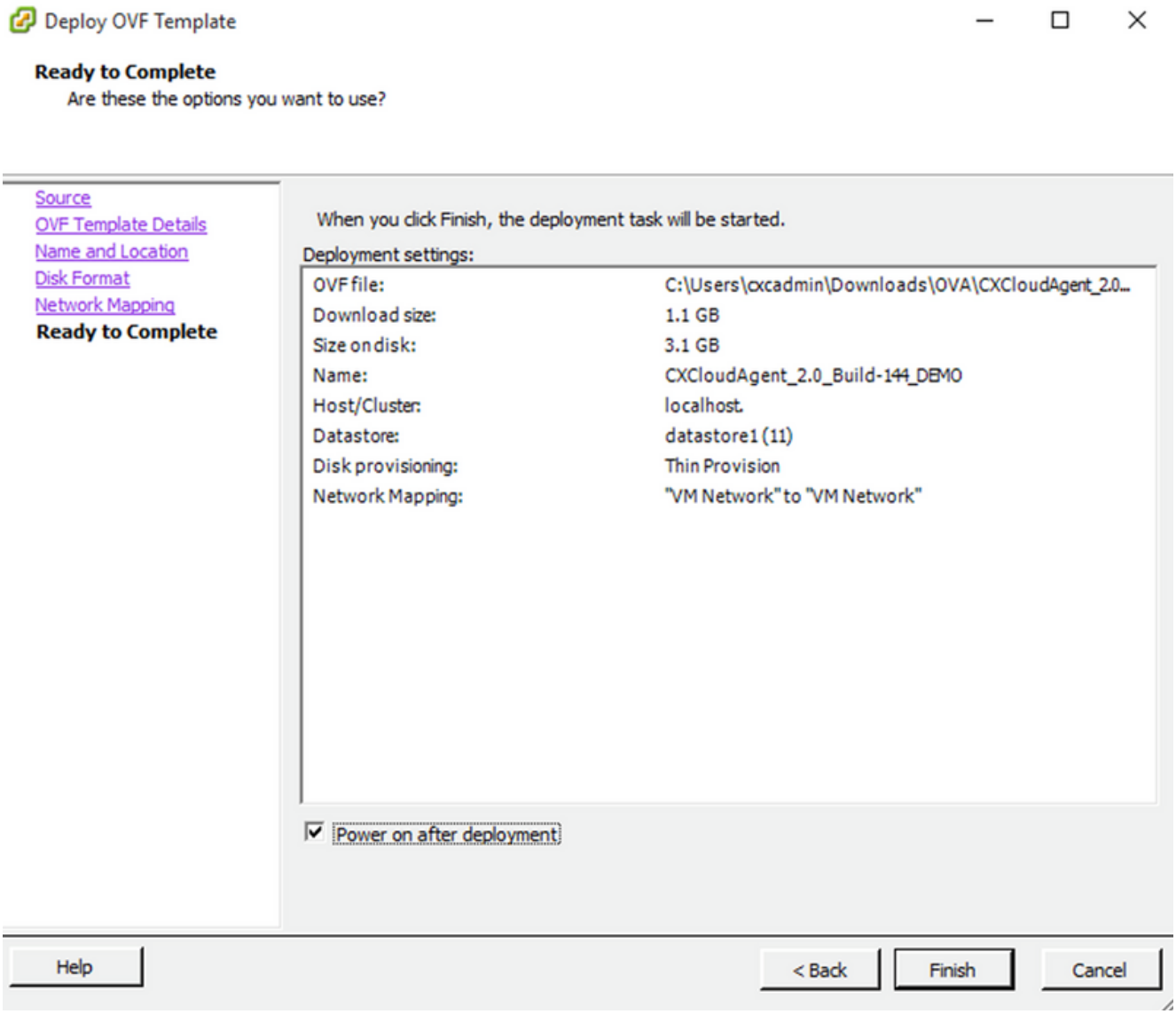
Name und Standort

6. Wählen Sie Disk Format und klicke auf Next (Thin Provision wird empfohlen).



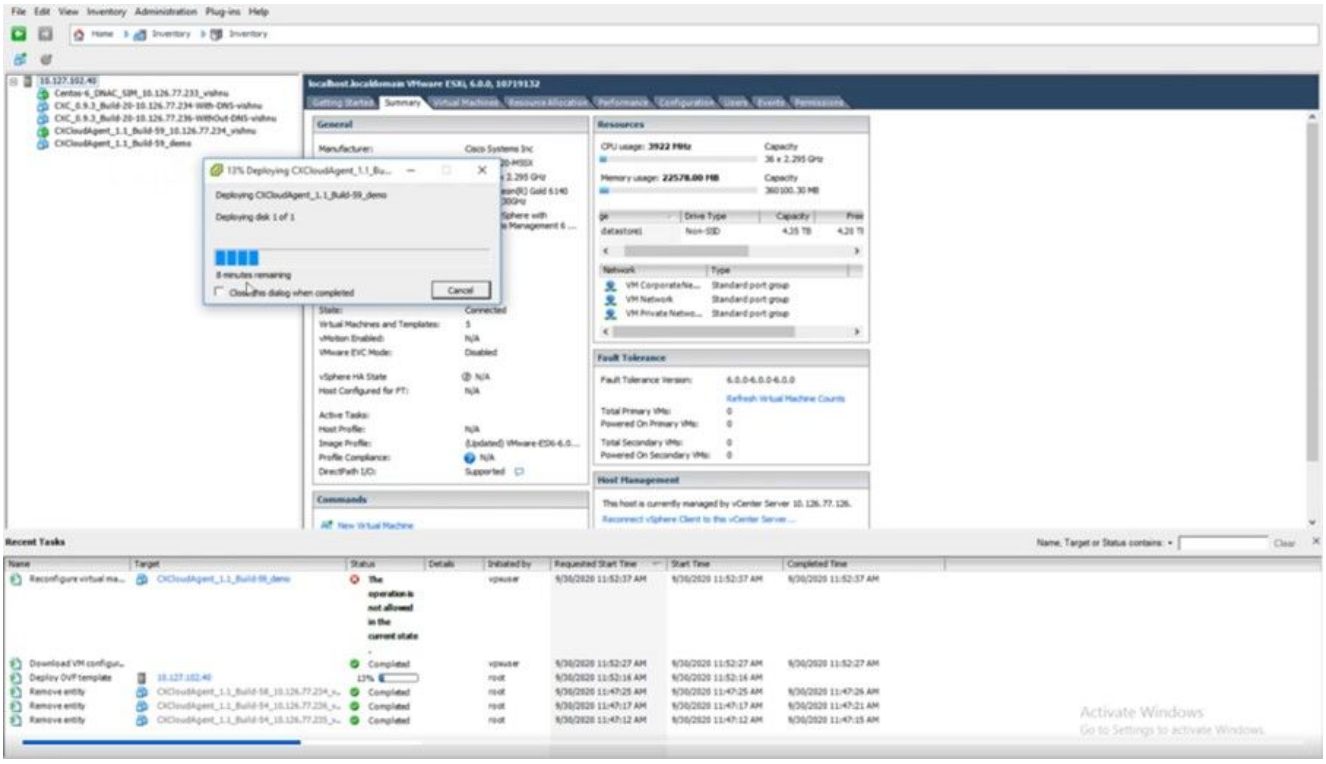
Datenträgerformatierung

7. Wählen Sie Power on after deployment und klicke auf Finish.

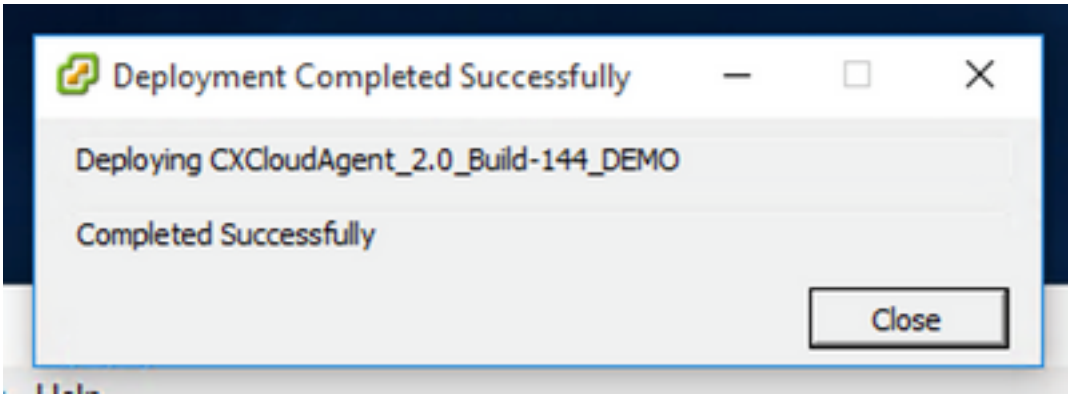


Bereit zur Fertigstellung

Die Bereitstellung kann einige Minuten dauern. Warten Sie, bis eine Erfolgsmeldung angezeigt wird.



Bereitstellung wird ausgeführt



Bereitstellung abgeschlossen

8. Wählen Sie die gerade bereitgestellte VM aus, öffnen Sie die Konsole, und wechseln Sie zu Network Configuration.

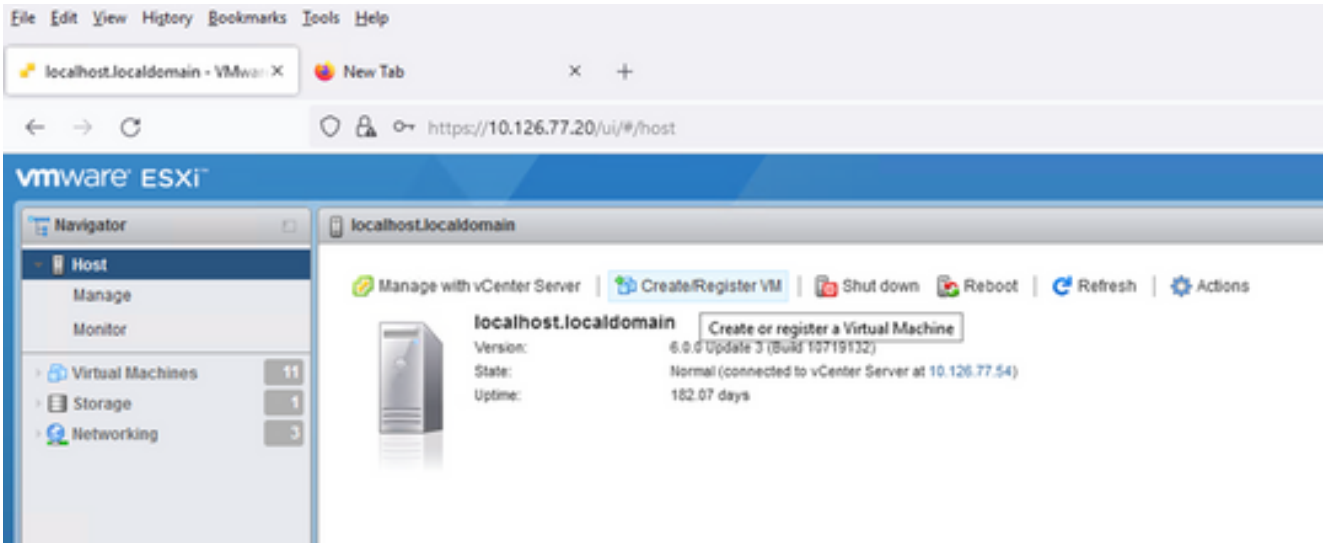
Installation von Web Client ESXi 6.0

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

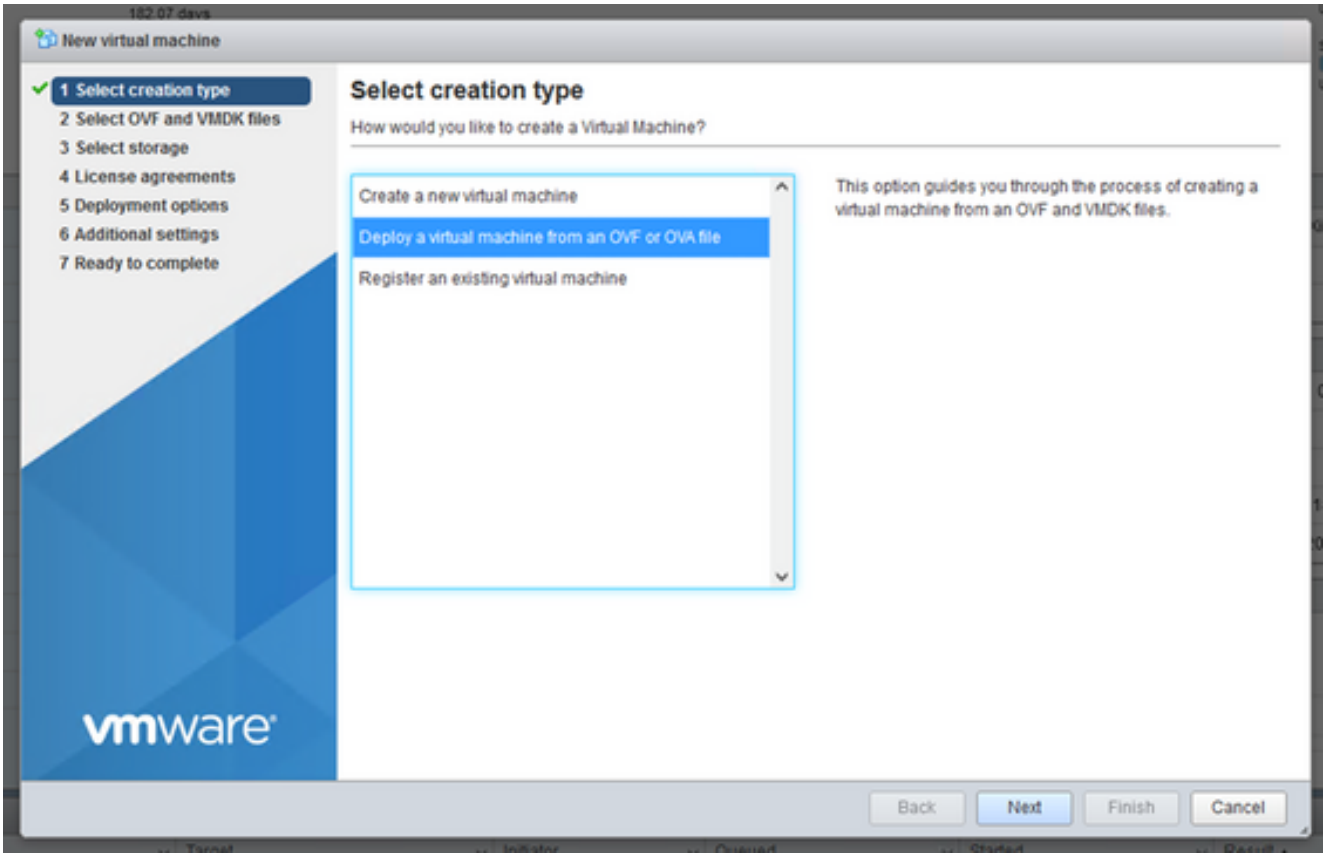
1. Melden Sie sich bei der VMWare-Benutzeroberfläche mit den ESXi/Hypervisor-Anmeldeinformationen an, die für die Bereitstellung von VM verwendet werden.

VMware ESXi-Anmeldung

2. Auswählen Virtual Machine > Create / Register VM.

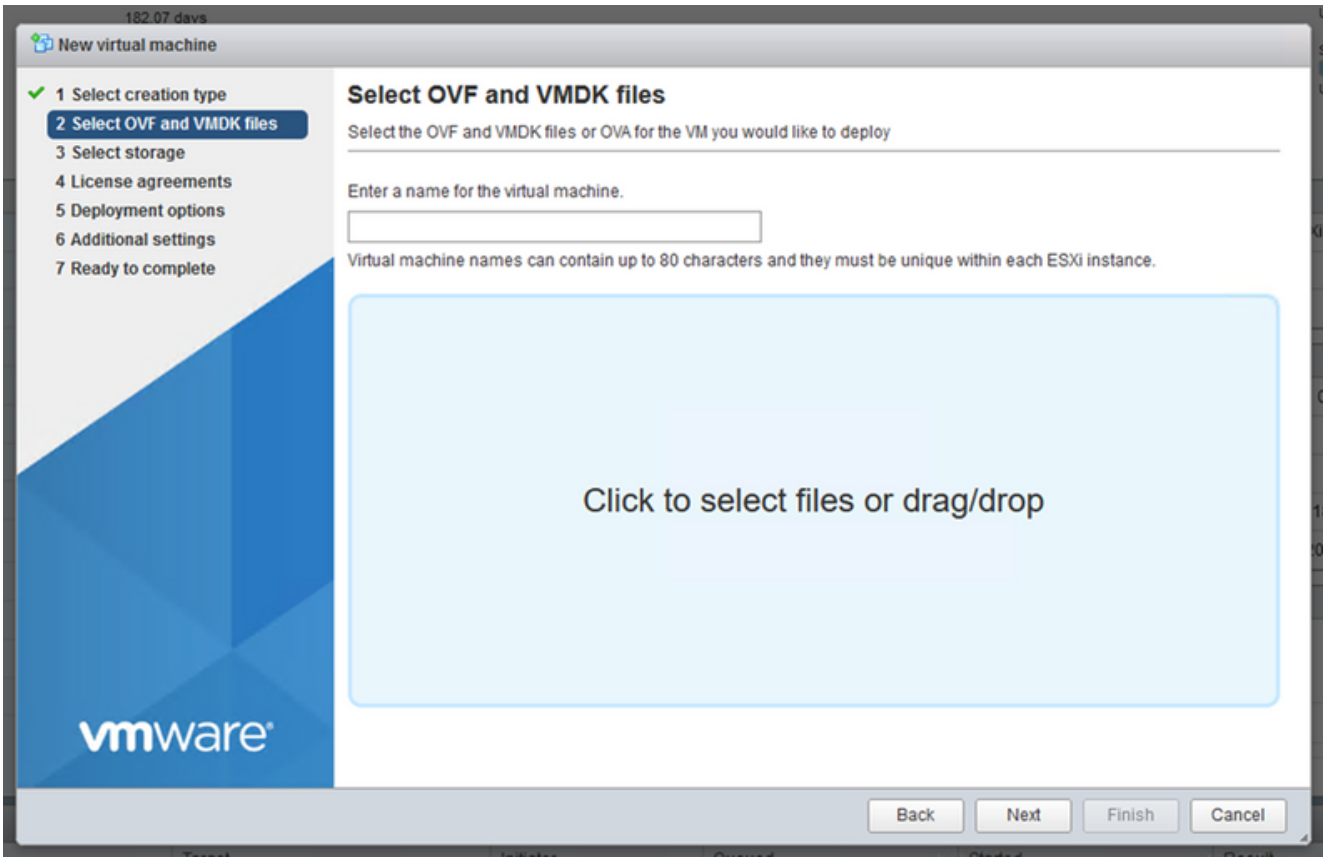


VM erstellen



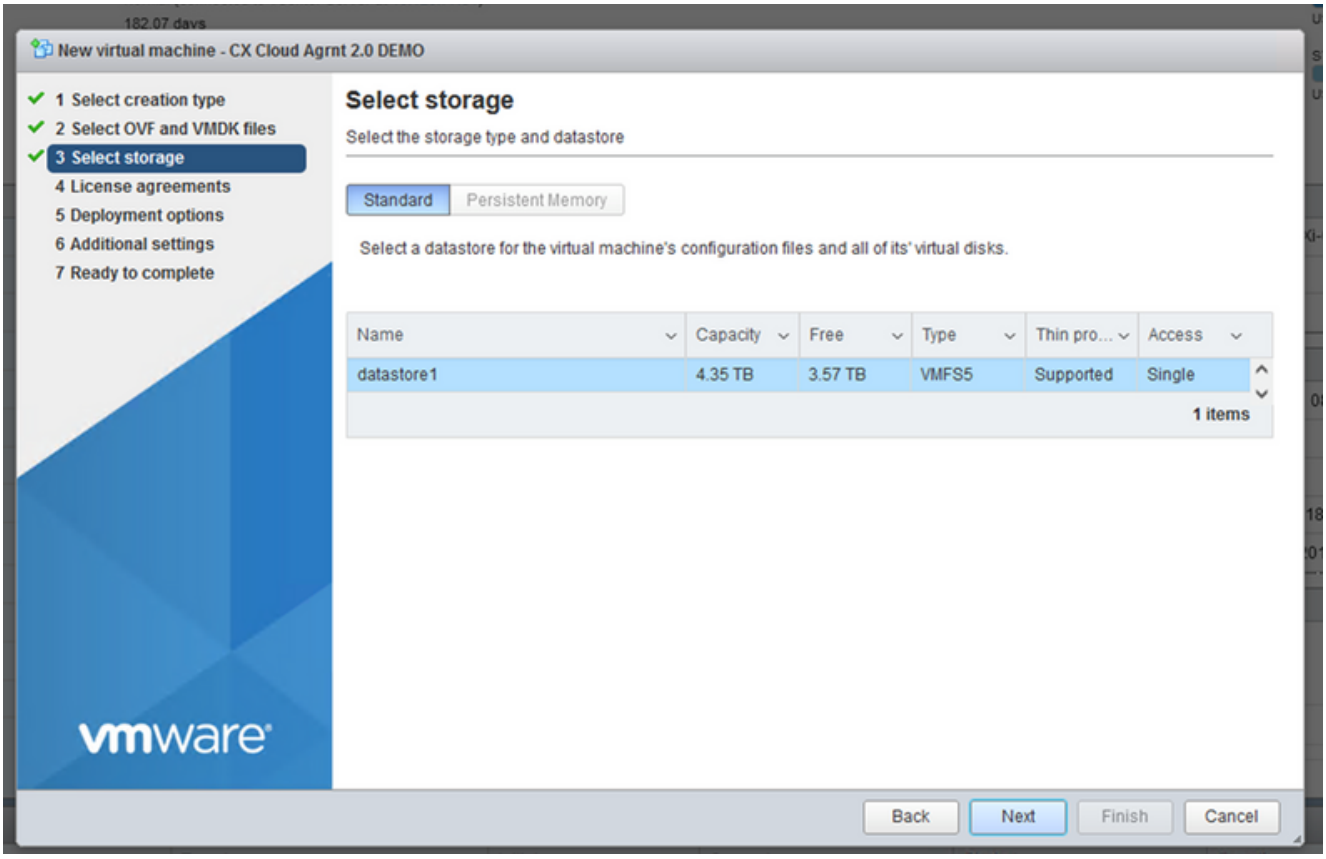
OVA-Bereitstellung

3. Auswählen Deploy a virtual machine from an OVF or OVA file und klicke auf Next.
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.

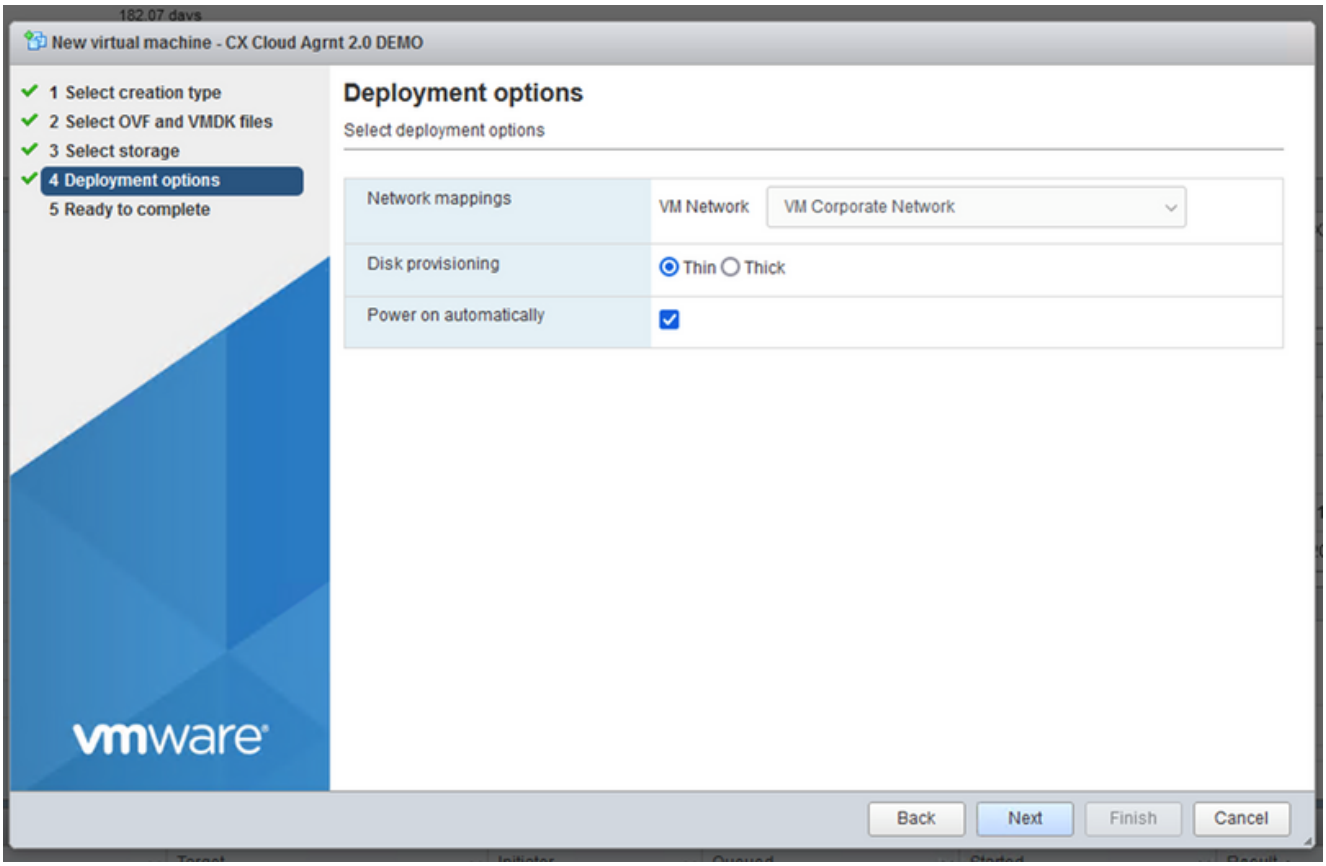


OVA-Auswahl

6. Auswählen Standard Storage und klicke auf Next.

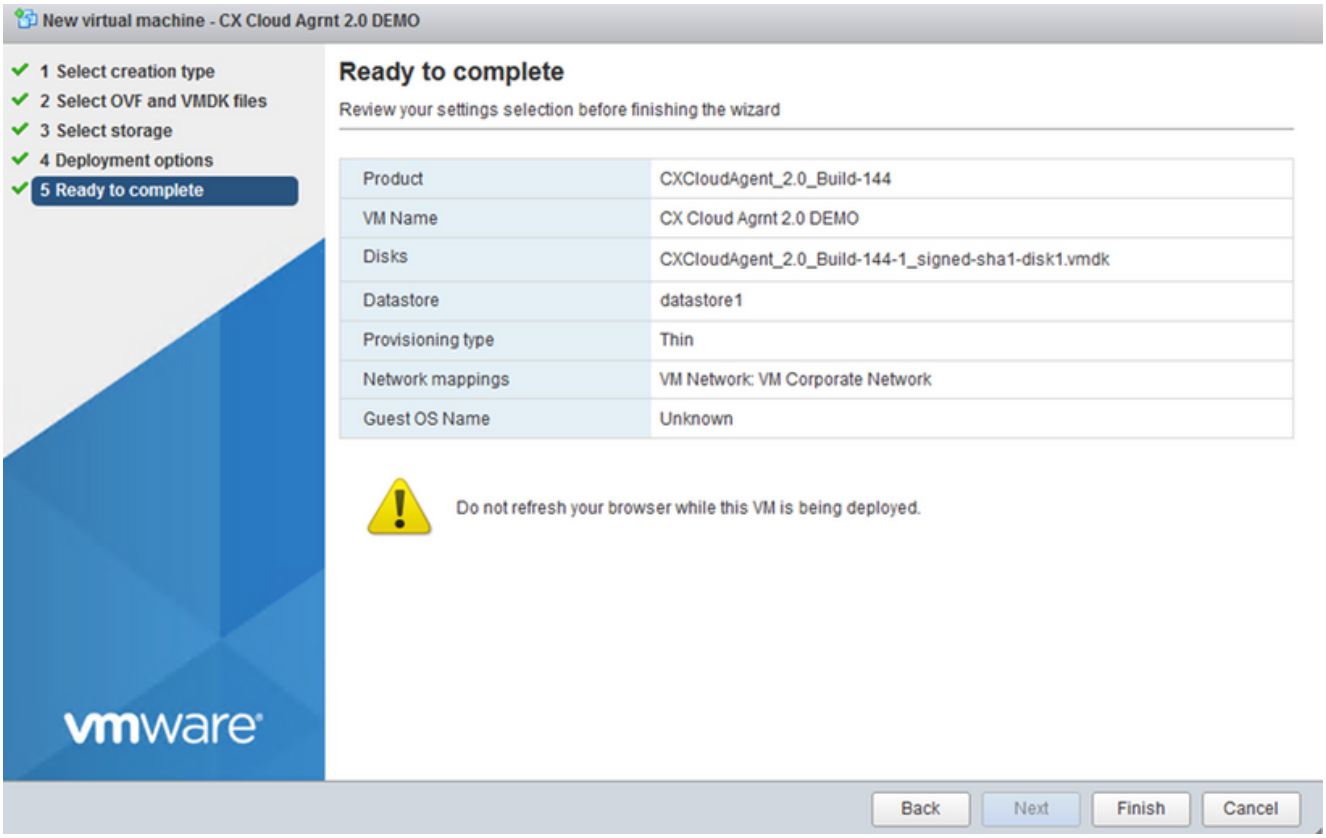


Auswahl von externem Speicher

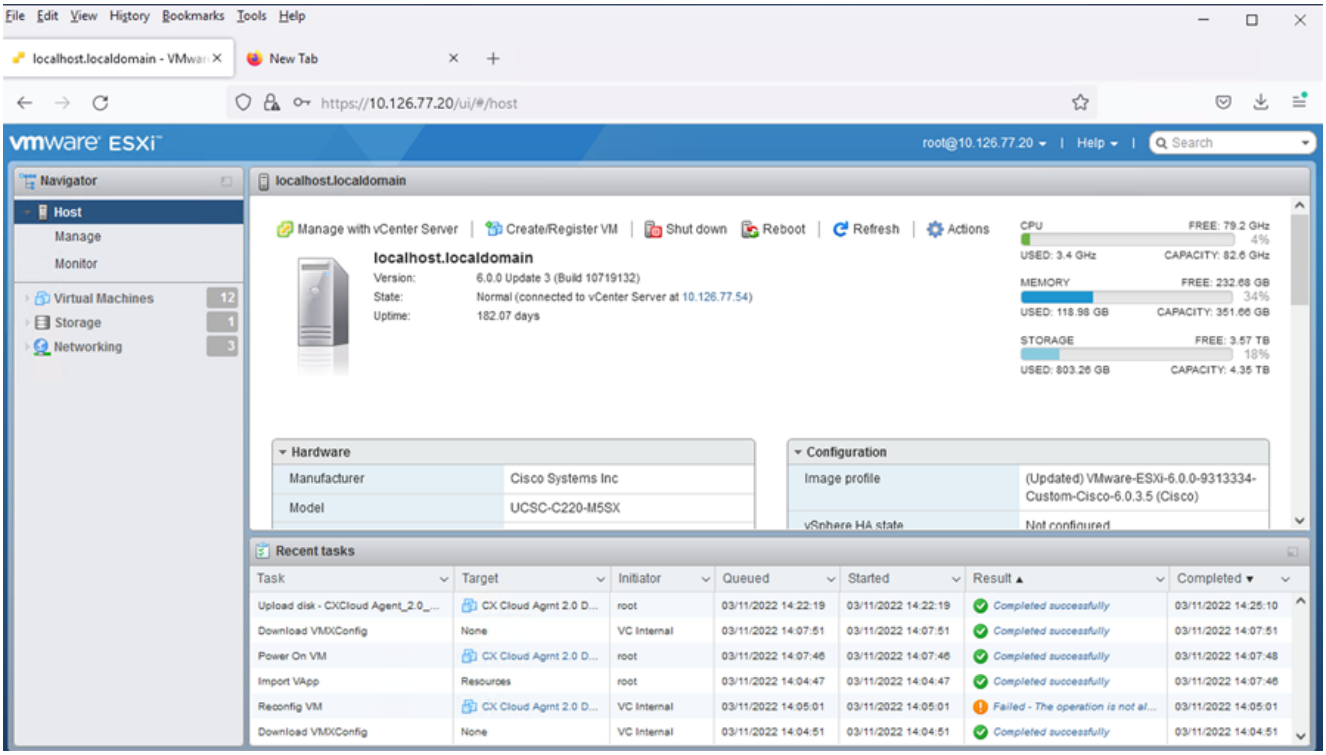


Bereitstellungsoptionen

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

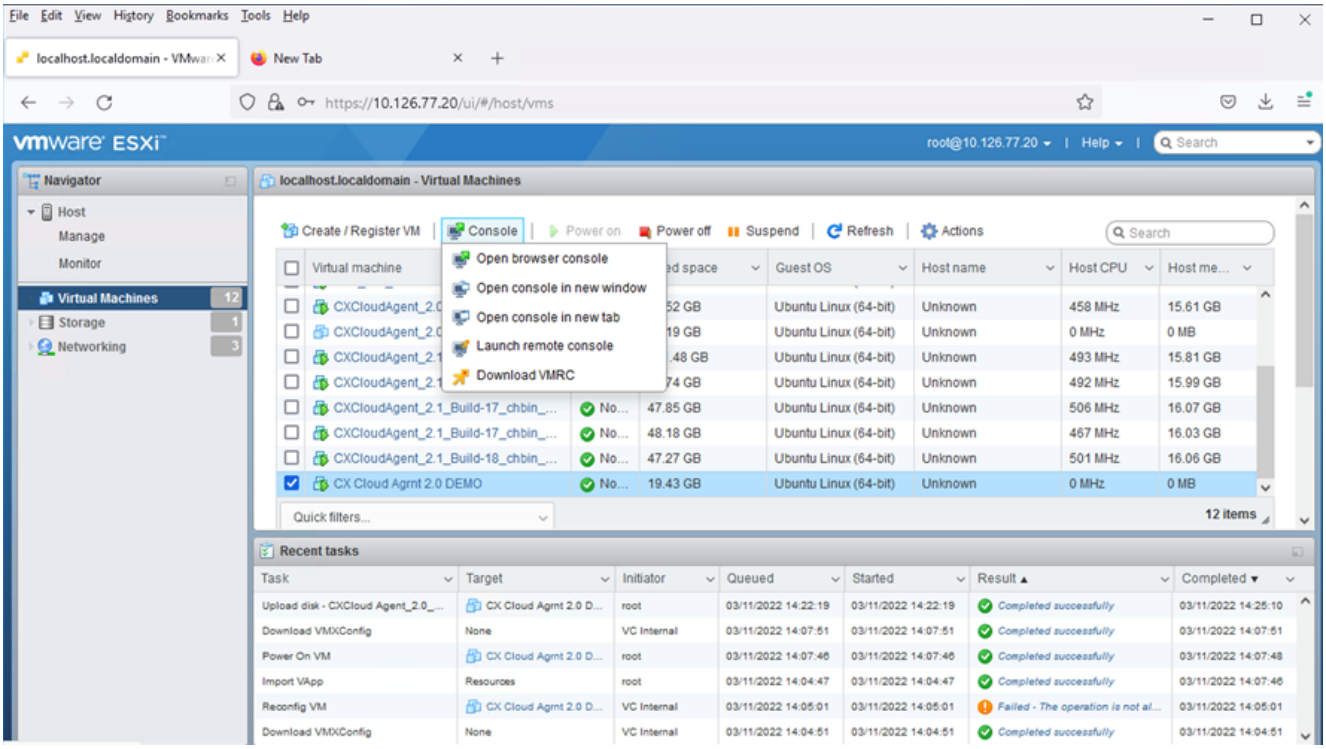


Bereit zur Fertigstellung



Abschluss erfolgreich

8. Überprüfen Sie die Einstellungen, und klicken Sie auf Finish.
9. Wählen Sie die gerade bereitgestellte VM aus, und wählen Sie Console > Open browser console.



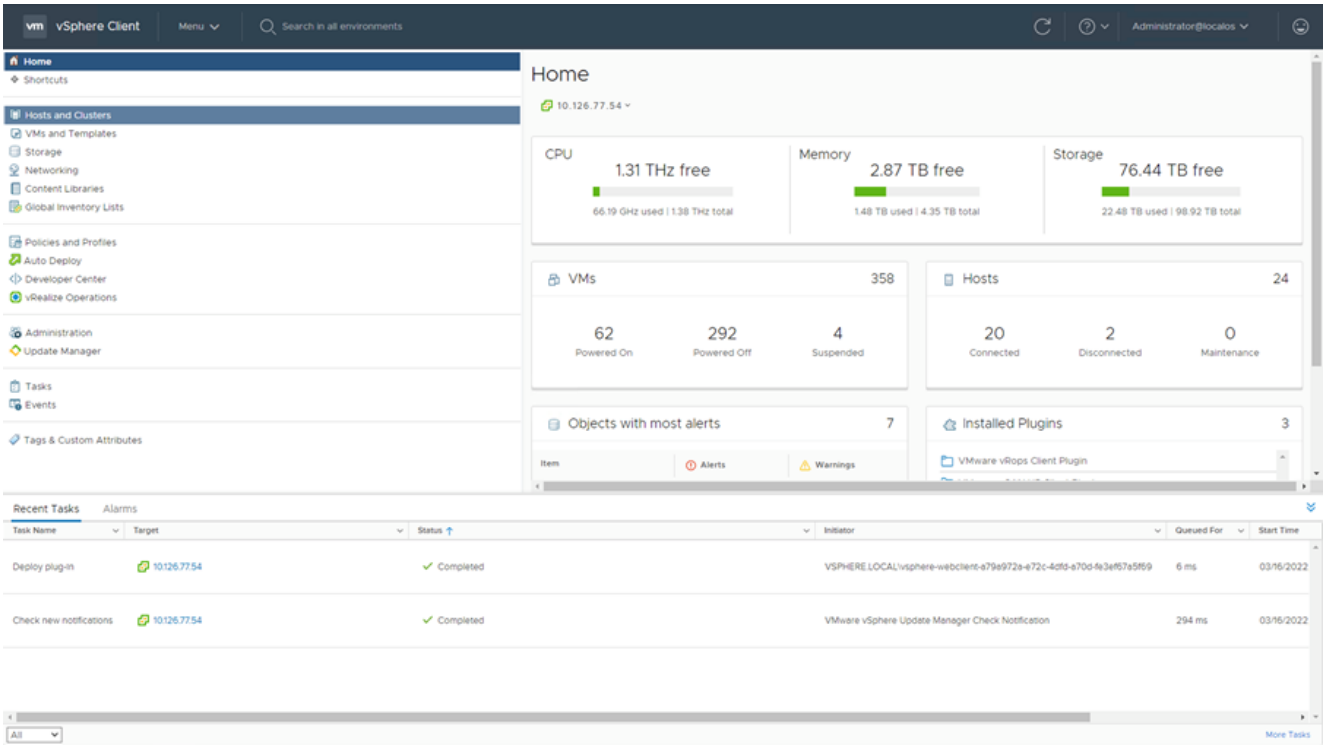
Konsole öffnen

10. Navigieren Sie zu Netzwerkkonfiguration.

Installation von Web Client vCenter

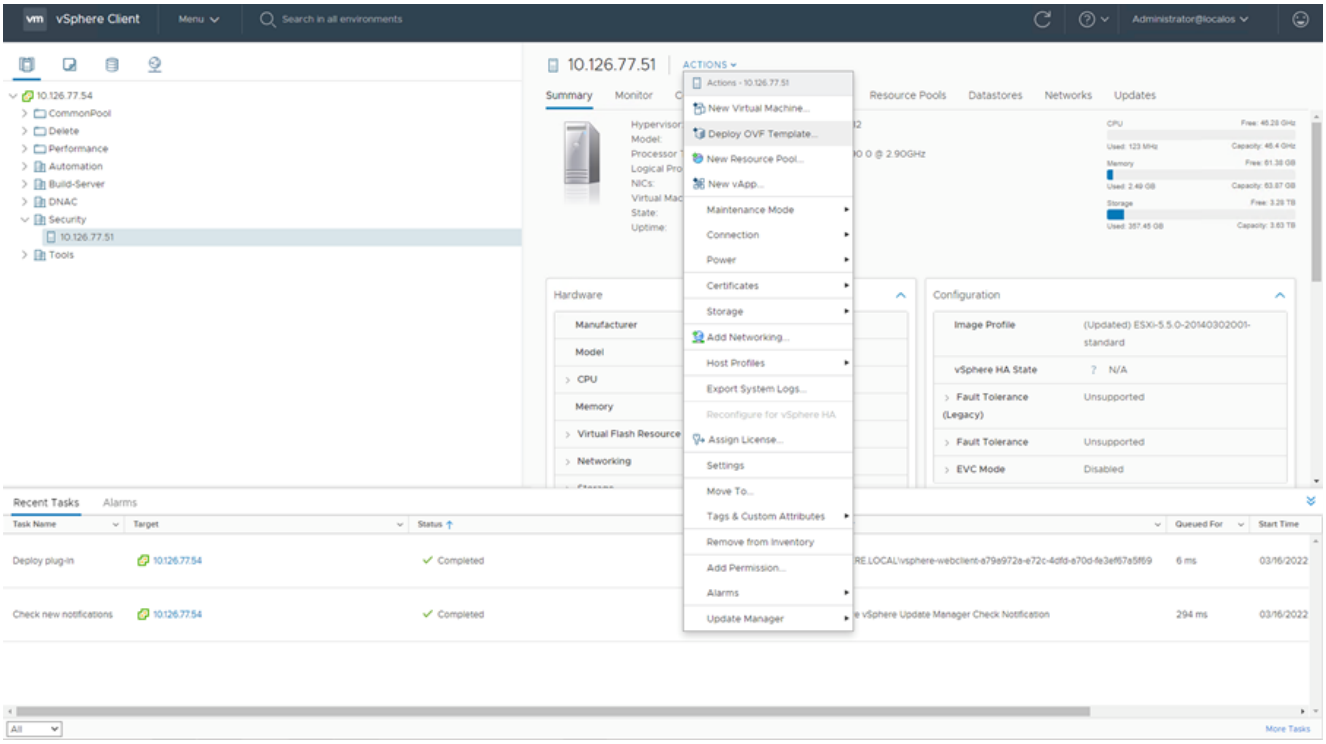
1. Melden Sie sich mit den ESXi/Hypervisor-Anmeldeinformationen beim vCenter-Client an.

Anmelden

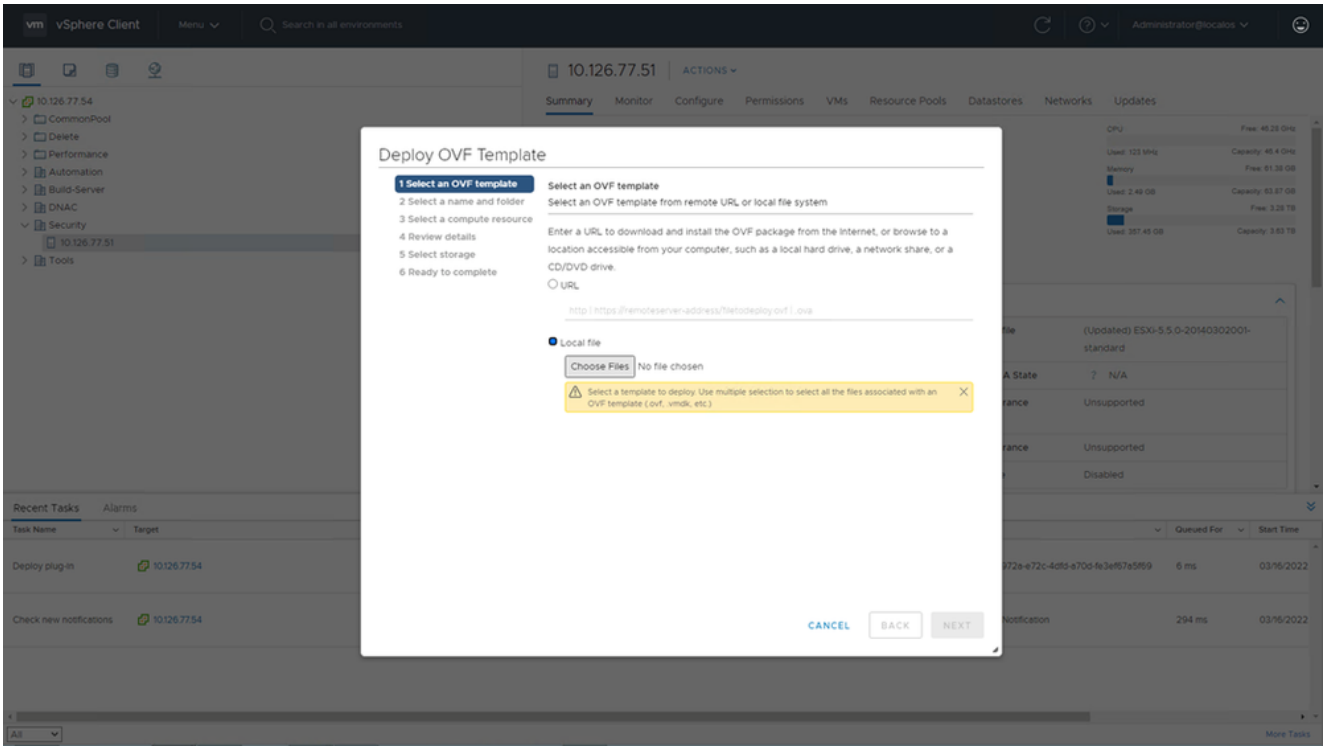


Startbildschirm

2. Klicken Sie auf der Startseite auf Hosts and Clusters.
3. Wählen Sie die VM aus, und klicken Sie auf Action > Deploy OVF Template.

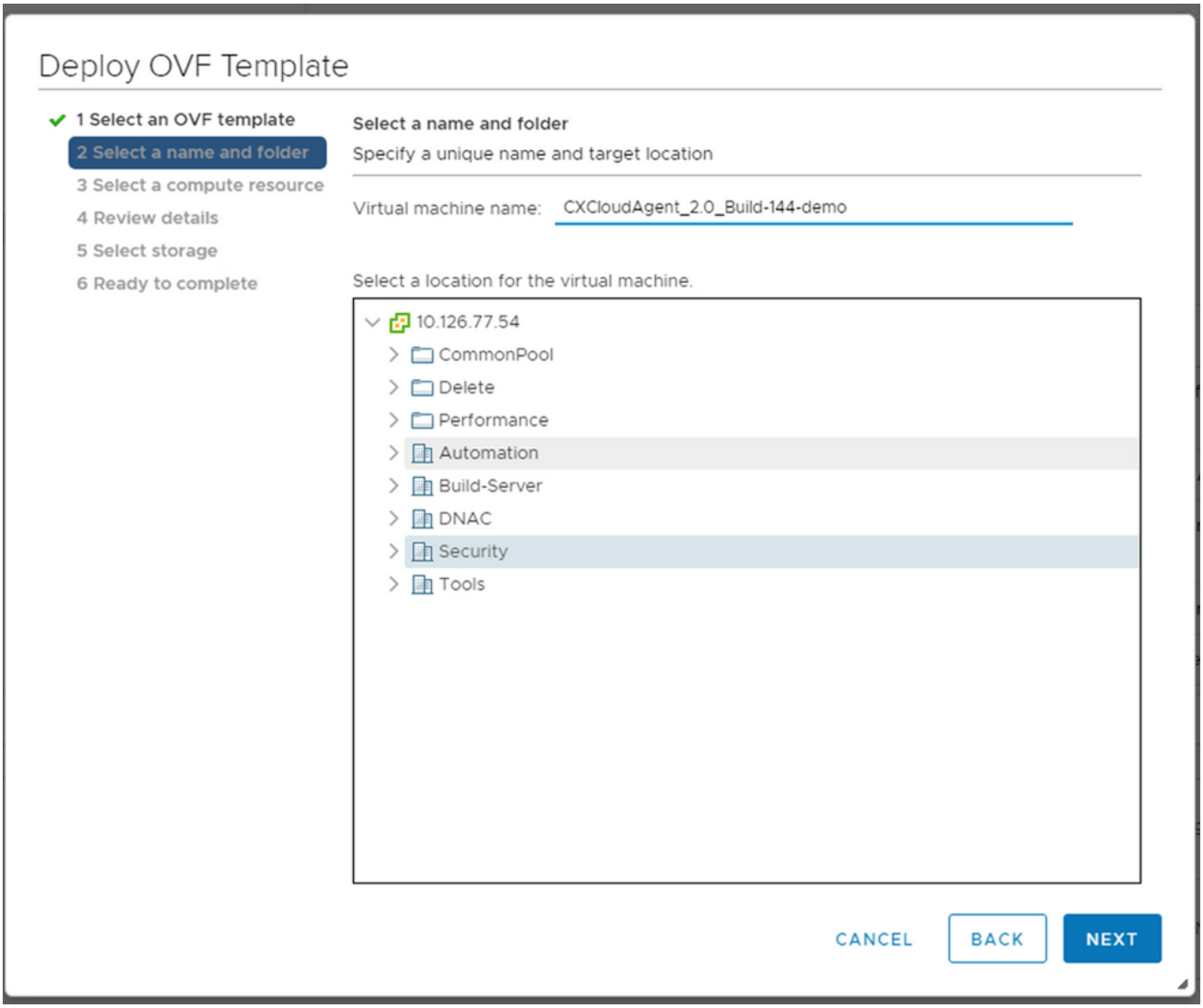


Aktionen



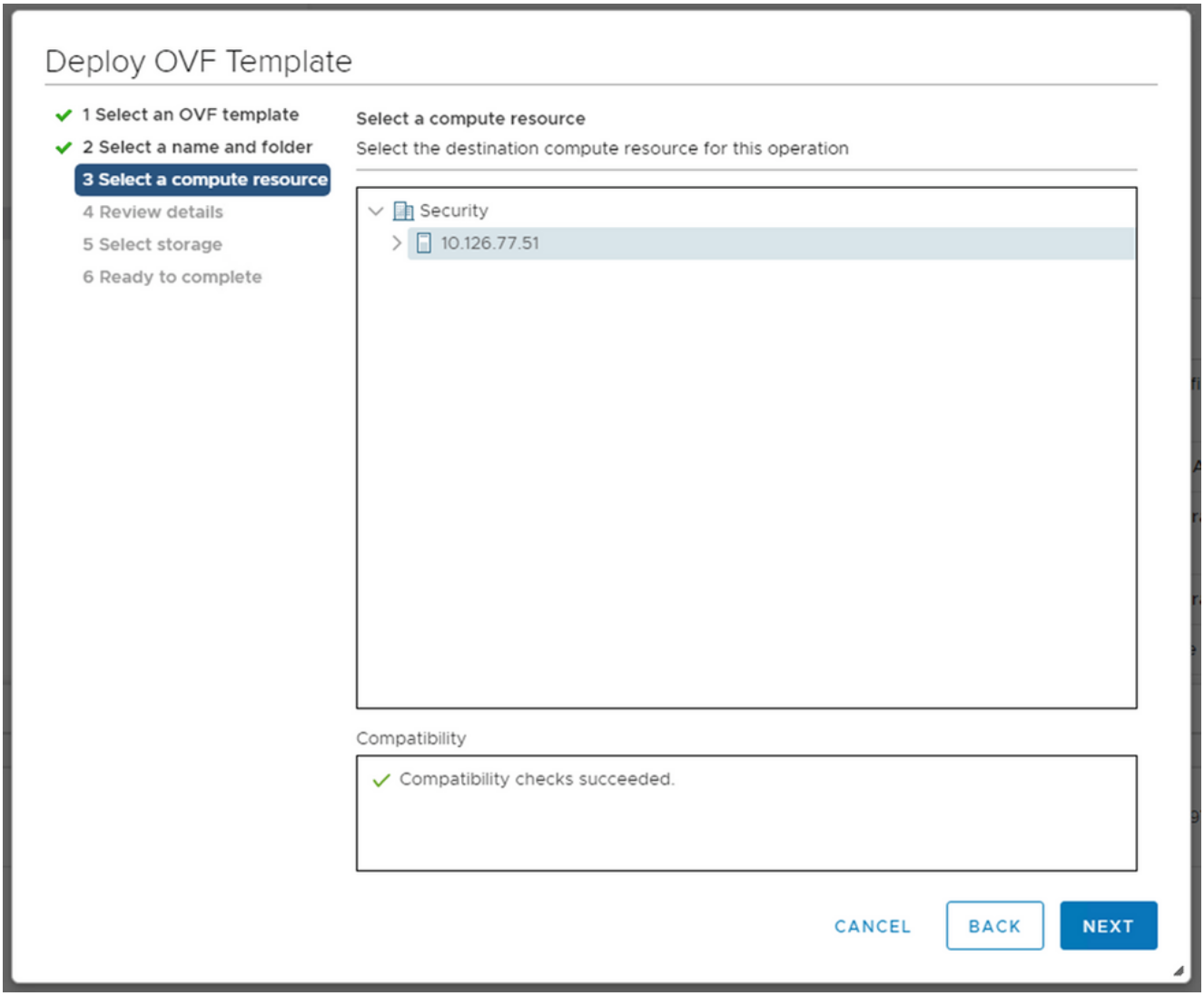
Vorlage auswählen

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



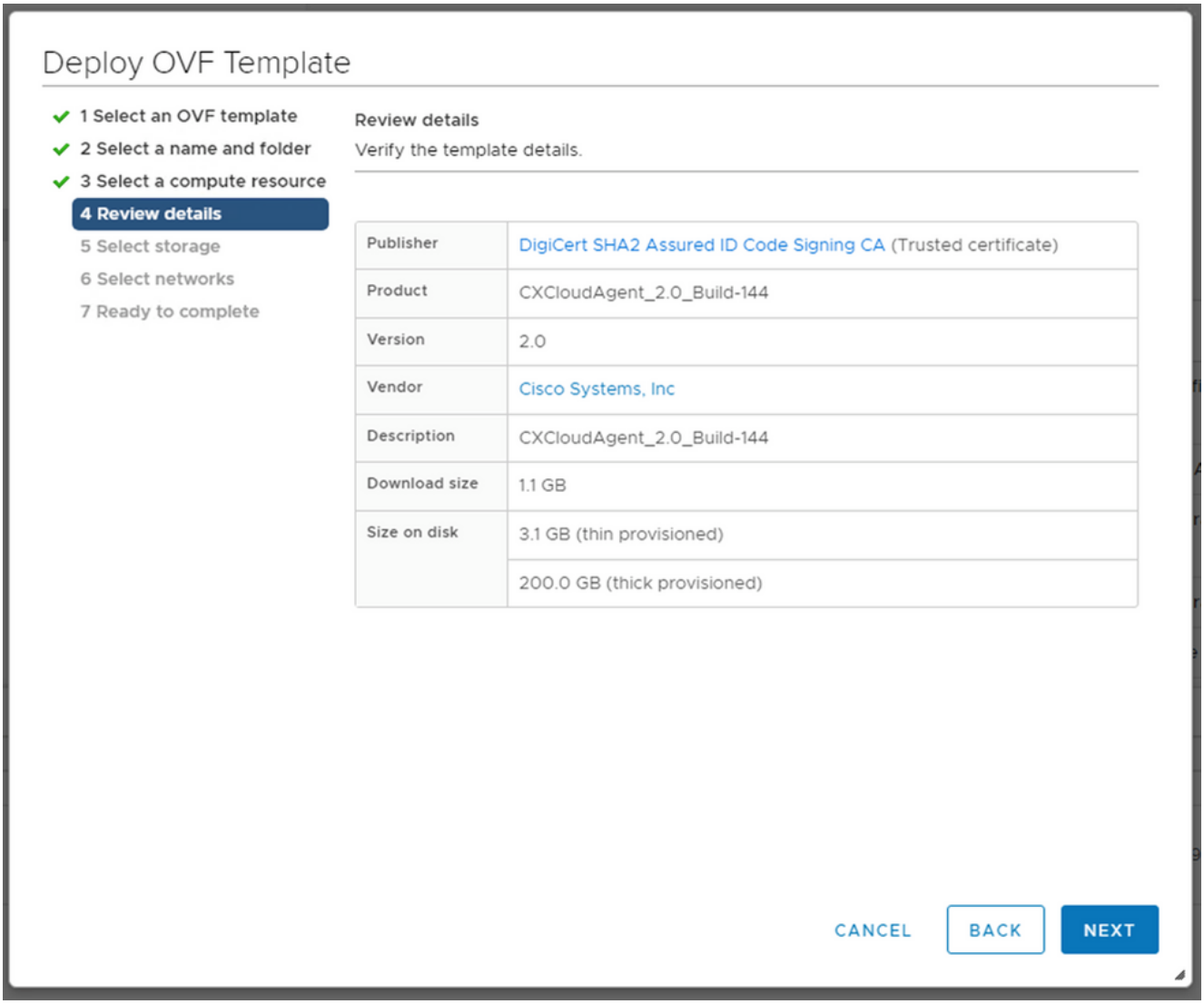
Name und Ordner

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



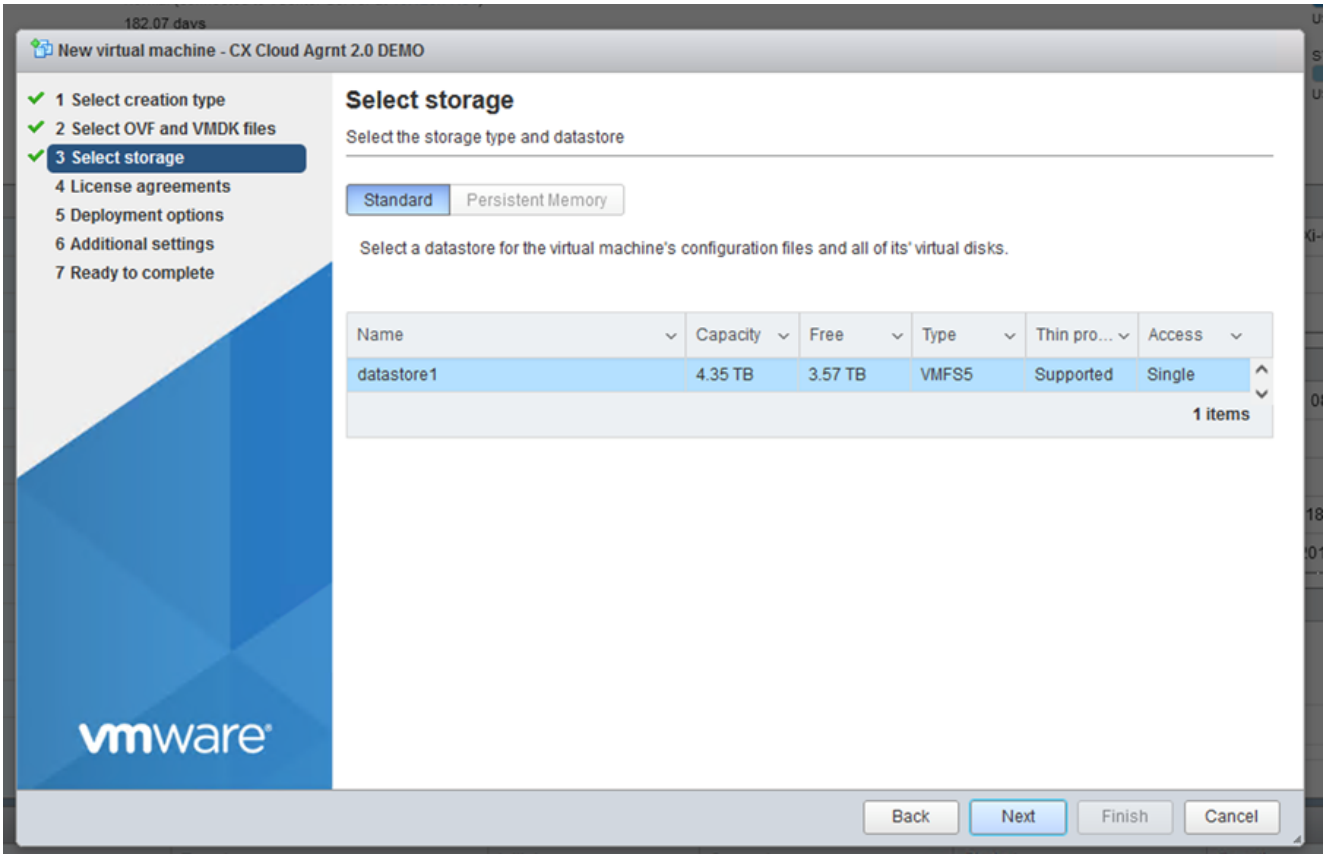
Rechenressource auswählen

8. Überprüfen Sie die Details, und klicken Sie auf Next.



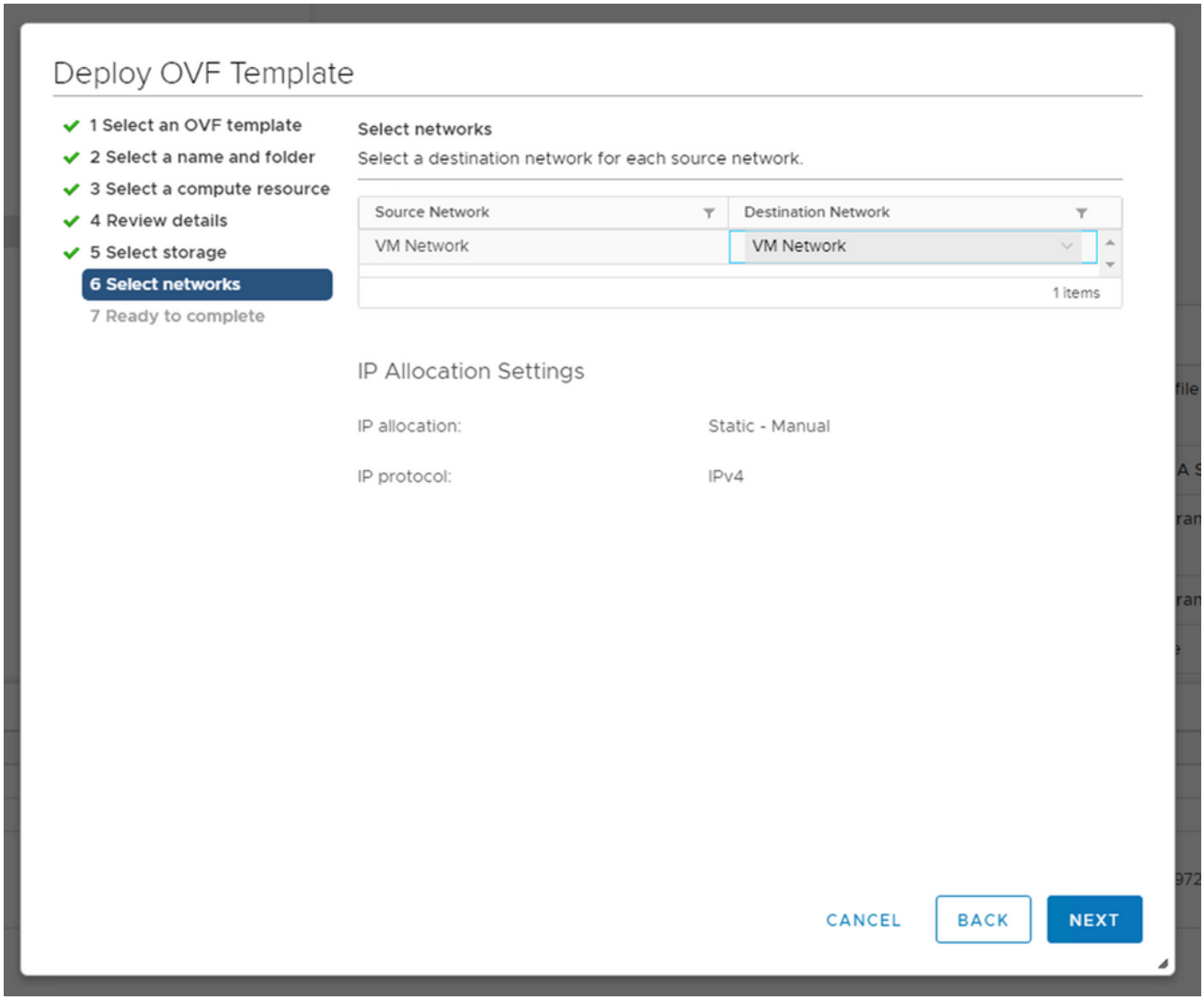
Details überprüfen

9. Wählen Sie das Format der virtuellen Festplatte aus, und klicken Sie auf Next.



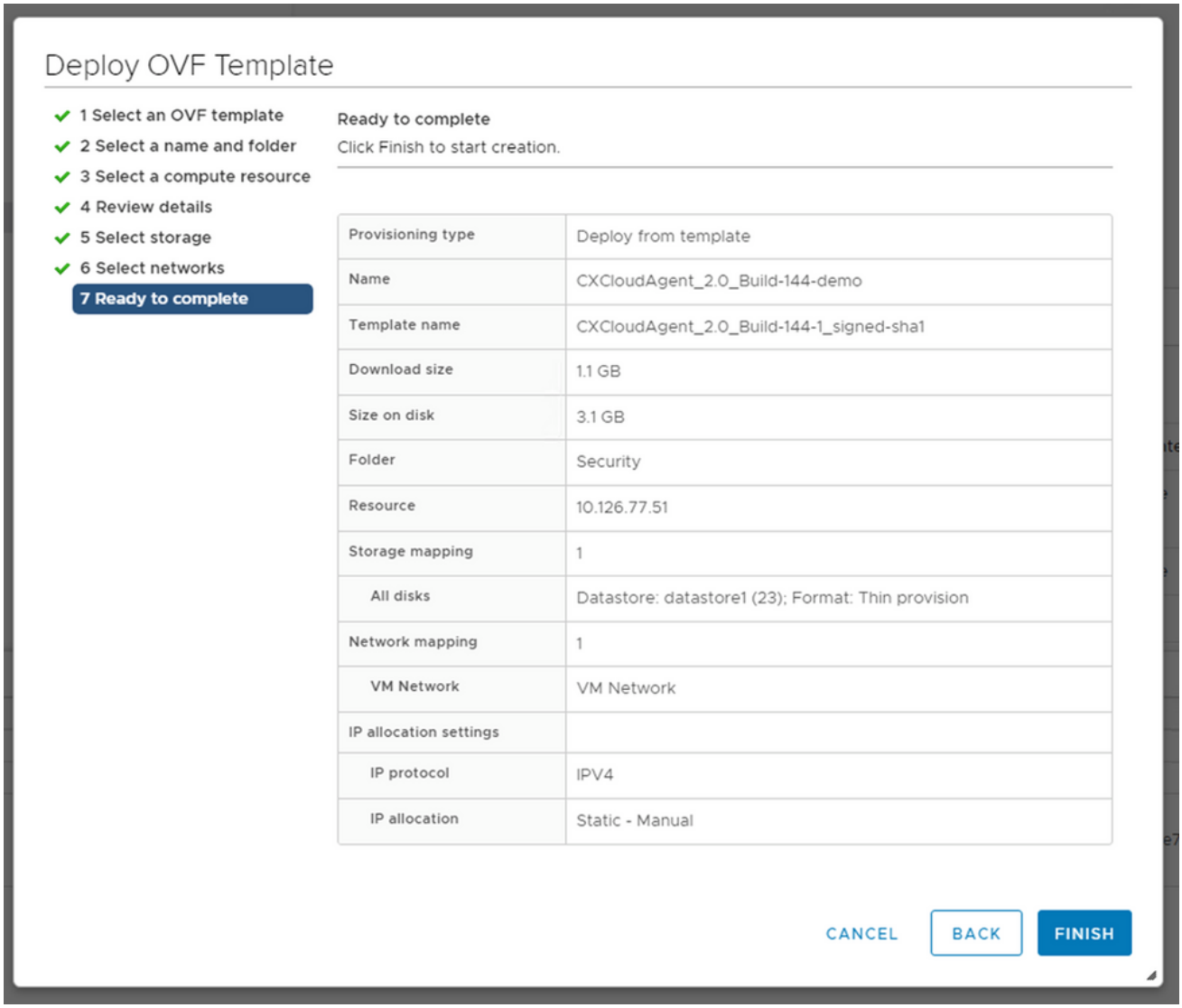
Auswahl von externem Speicher

10. Klicken Sie auf Next.



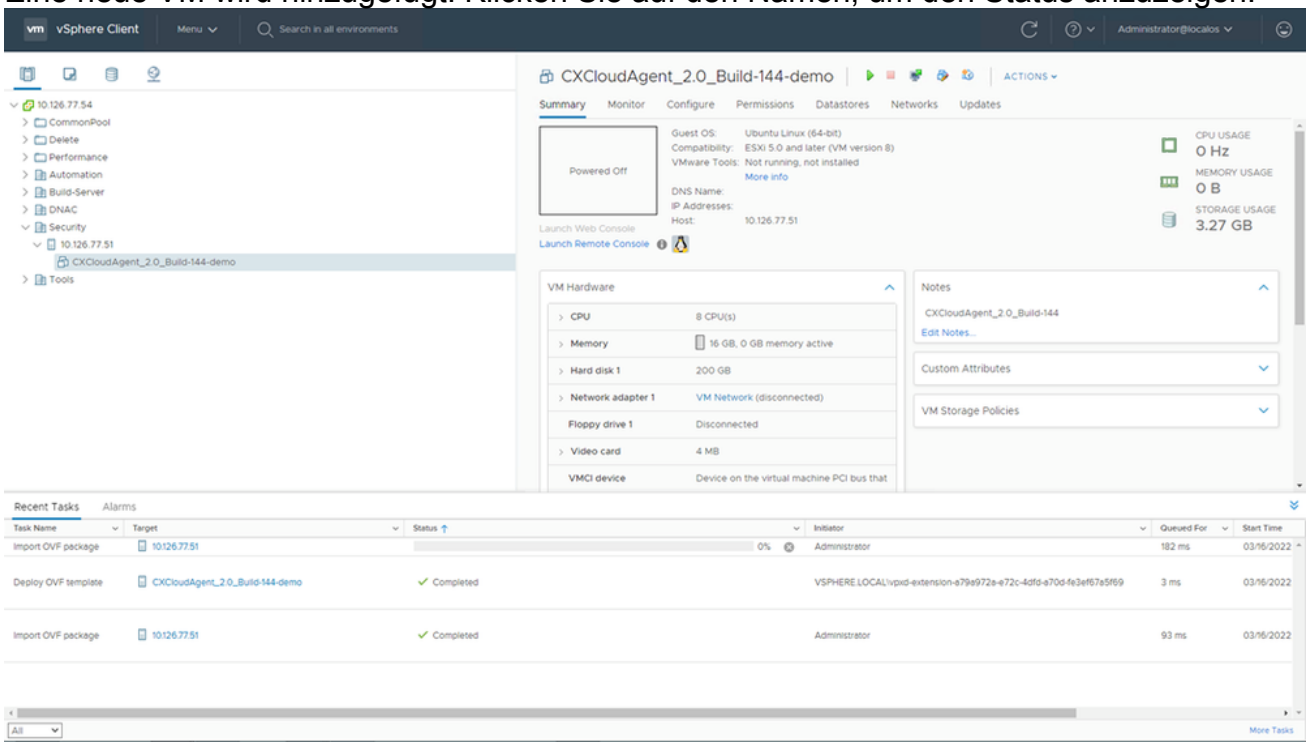
Netzwerke auswählen

11. Klicken Sie auf Finish.



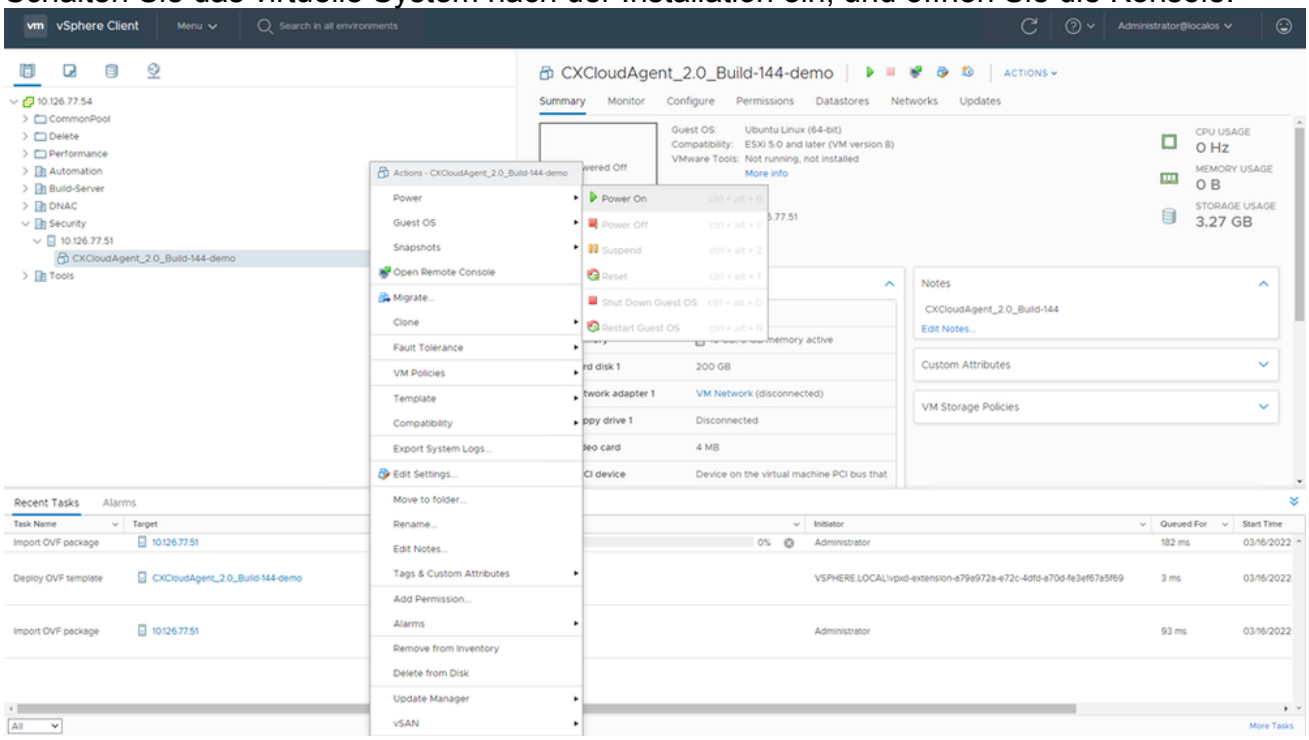
Bereit zur Fertigstellung

12. Eine neue VM wird hinzugefügt. Klicken Sie auf den Namen, um den Status anzuzeigen.



VM hinzugefügt

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



Konsole öffnen

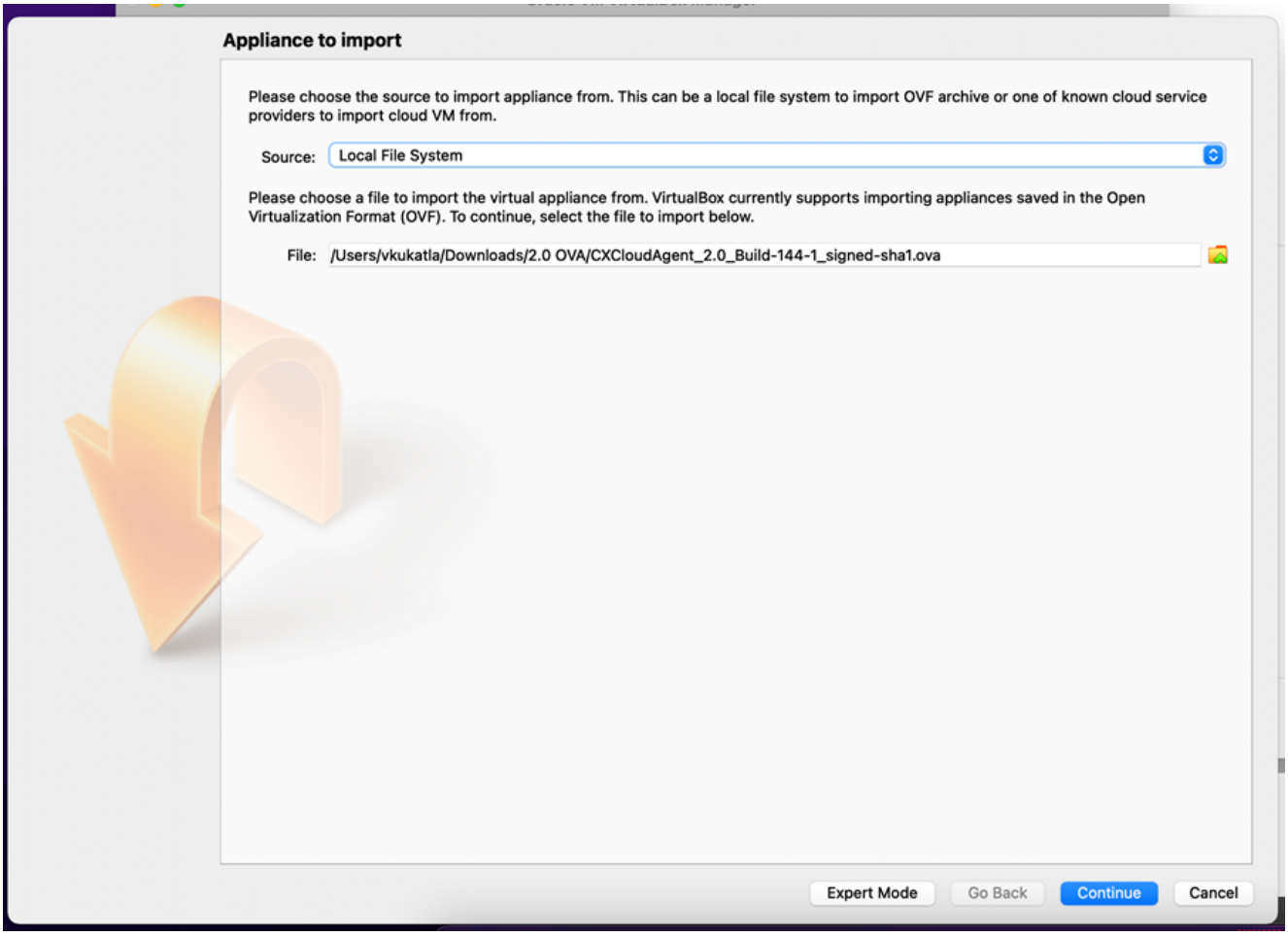
14. Navigieren Sie zu Netzwerkkonfiguration.

Installation von Oracle VirtualBox 5.2.30

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

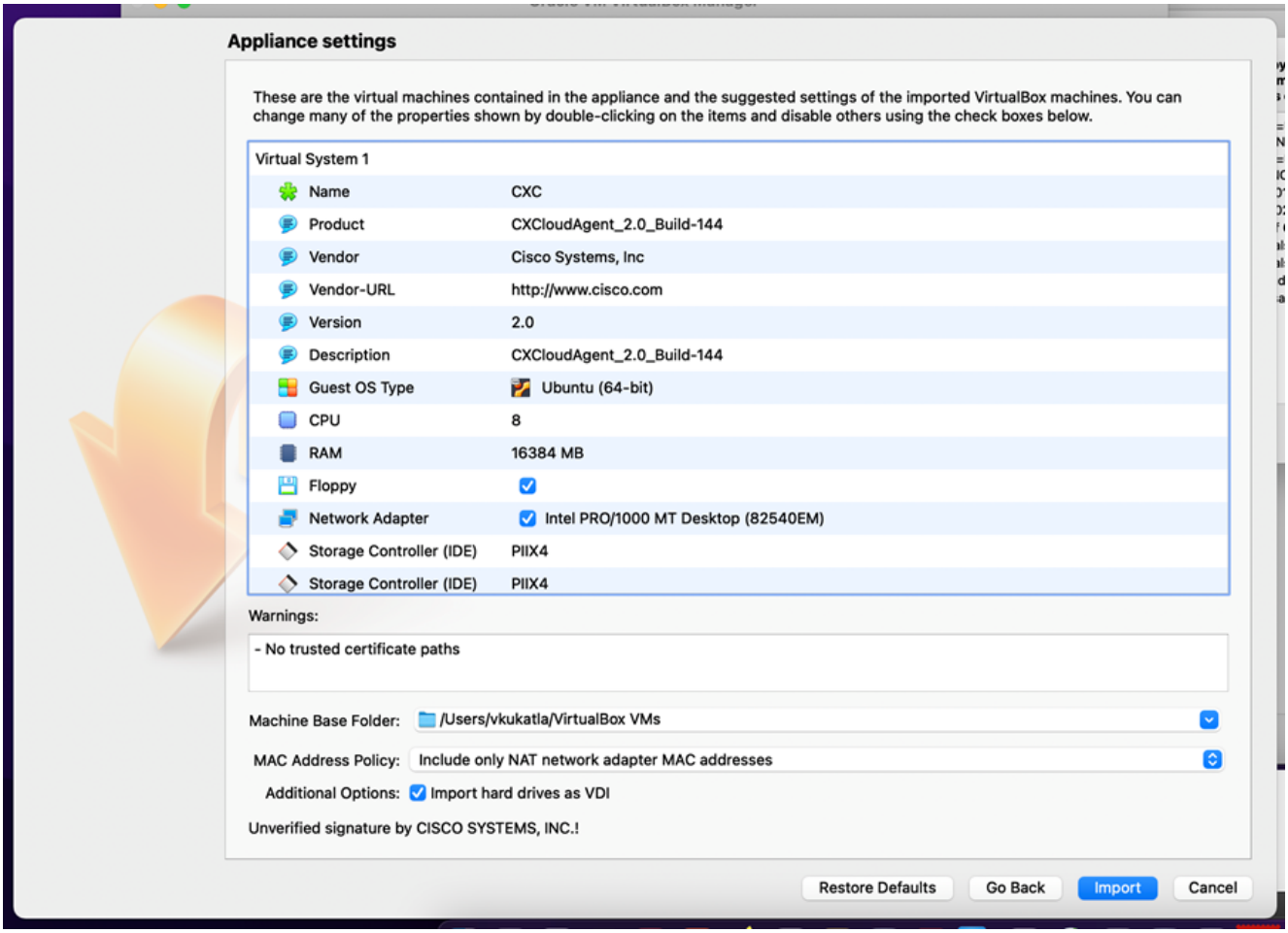
Oracle VM

1. Öffnen Sie die Oracle VM-Benutzeroberfläche, und wählen Sie File > Import Appliance.
2. Klicken Sie auf "Durchsuchen", um die OVA-Datei zu importieren.



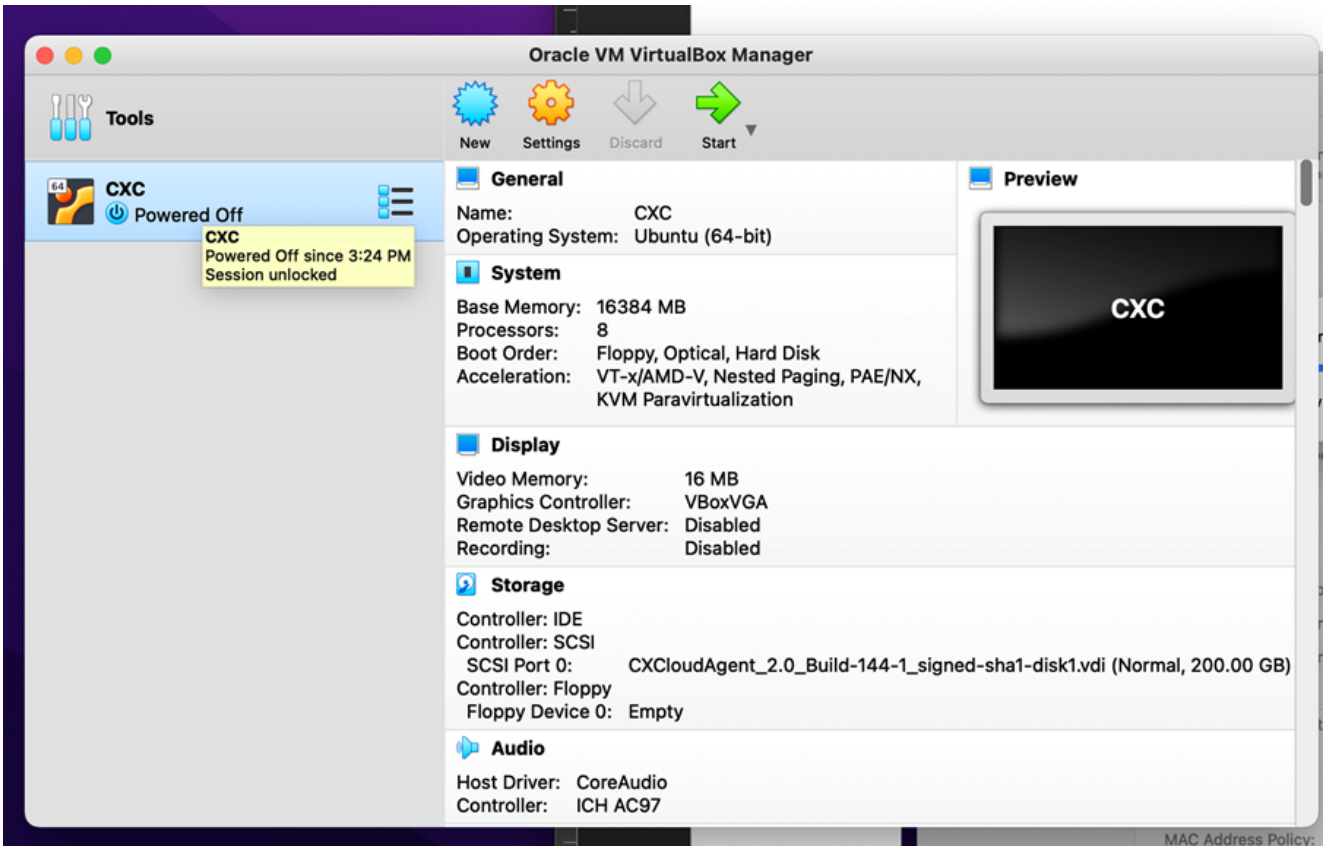
Datei auswählen

3. Klicken Sie auf Import.

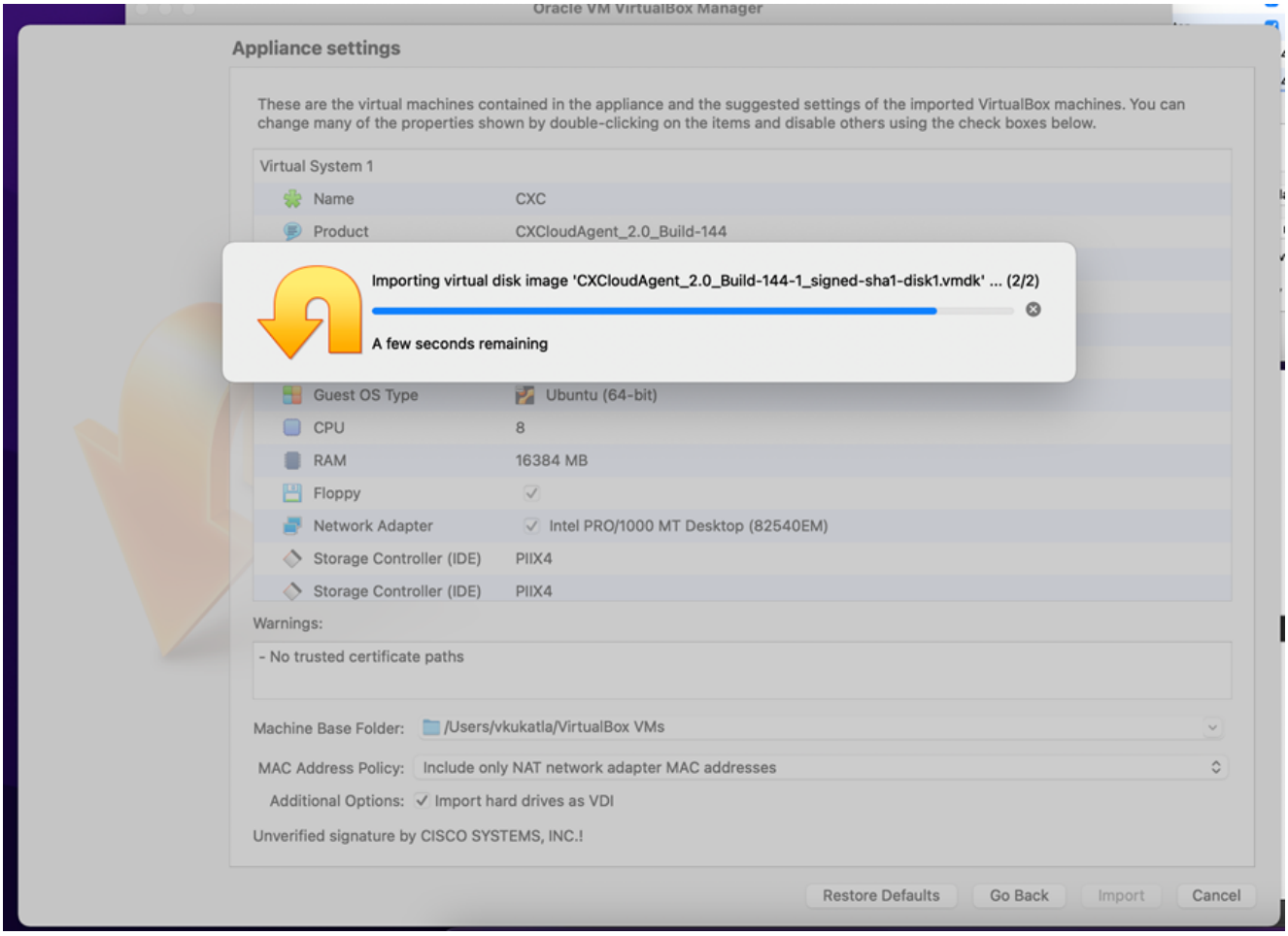


Datei importieren

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

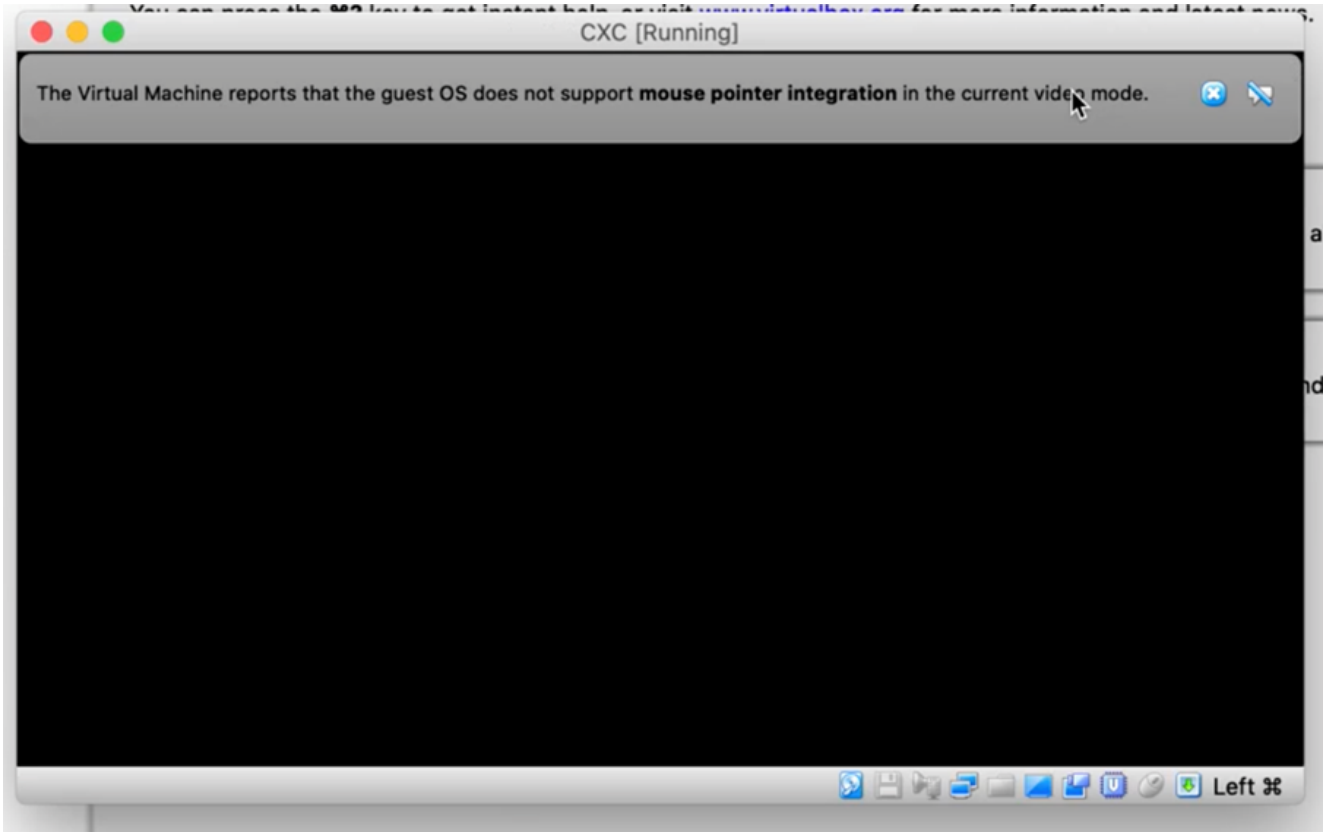


Start der VM-Konsole



Import in Bearbeitung

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

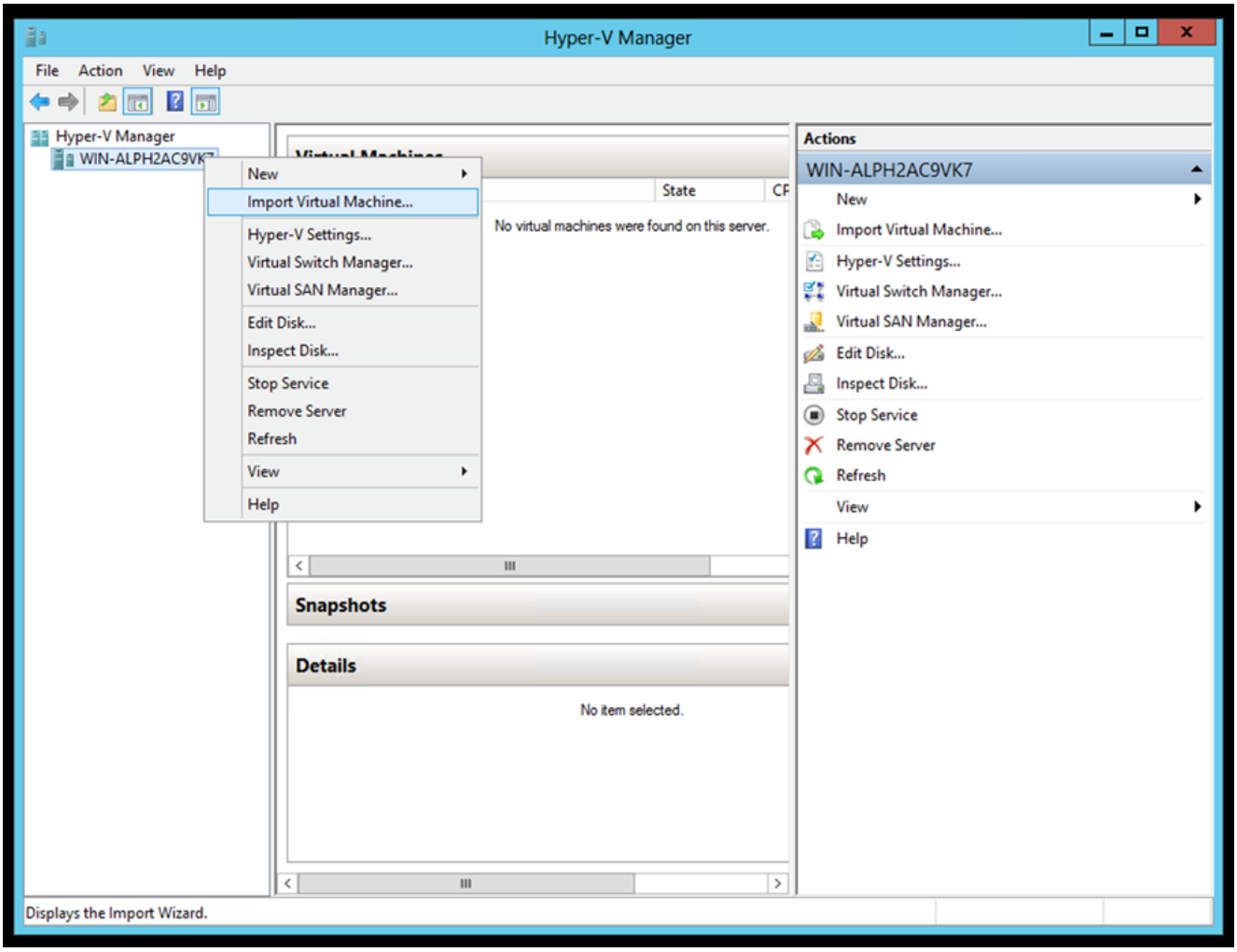


Konsole öffnen

6. Navigieren Sie zu Netzwerkkonfiguration.

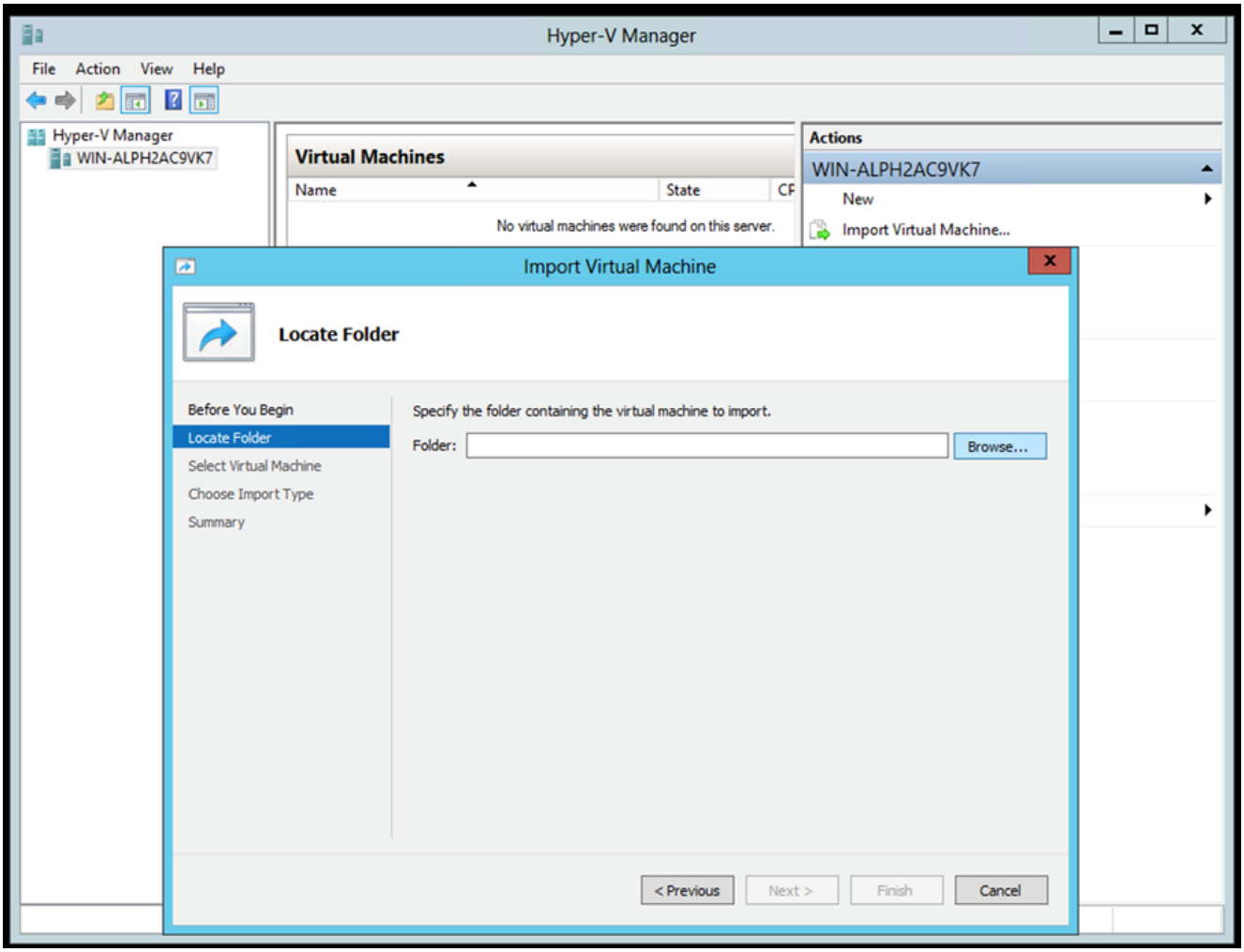
Installation von Microsoft Hyper-V

1. Auswählen Import Virtual Machine.



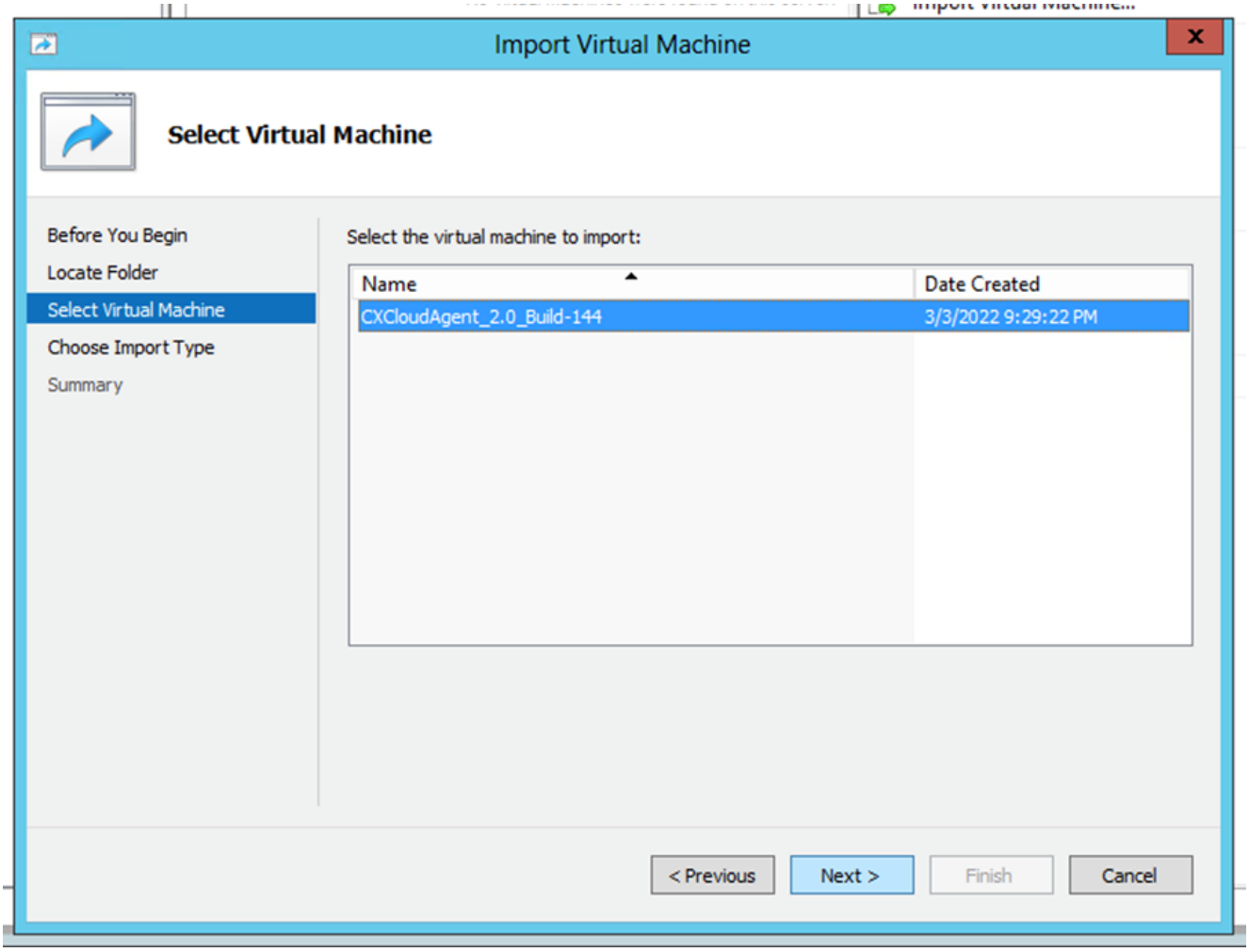
Hyper-V-Manager

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



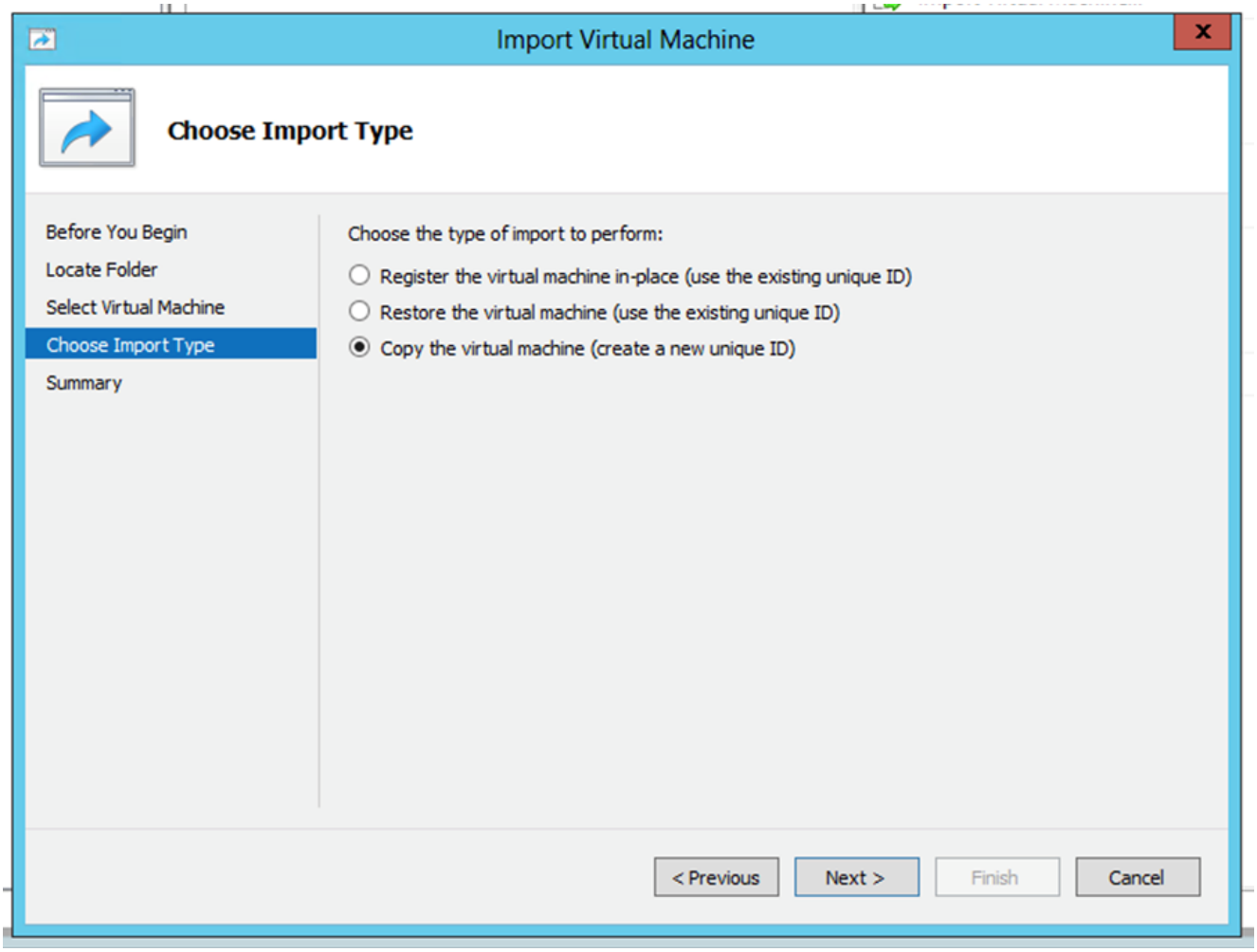
Zu importierender Ordner

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



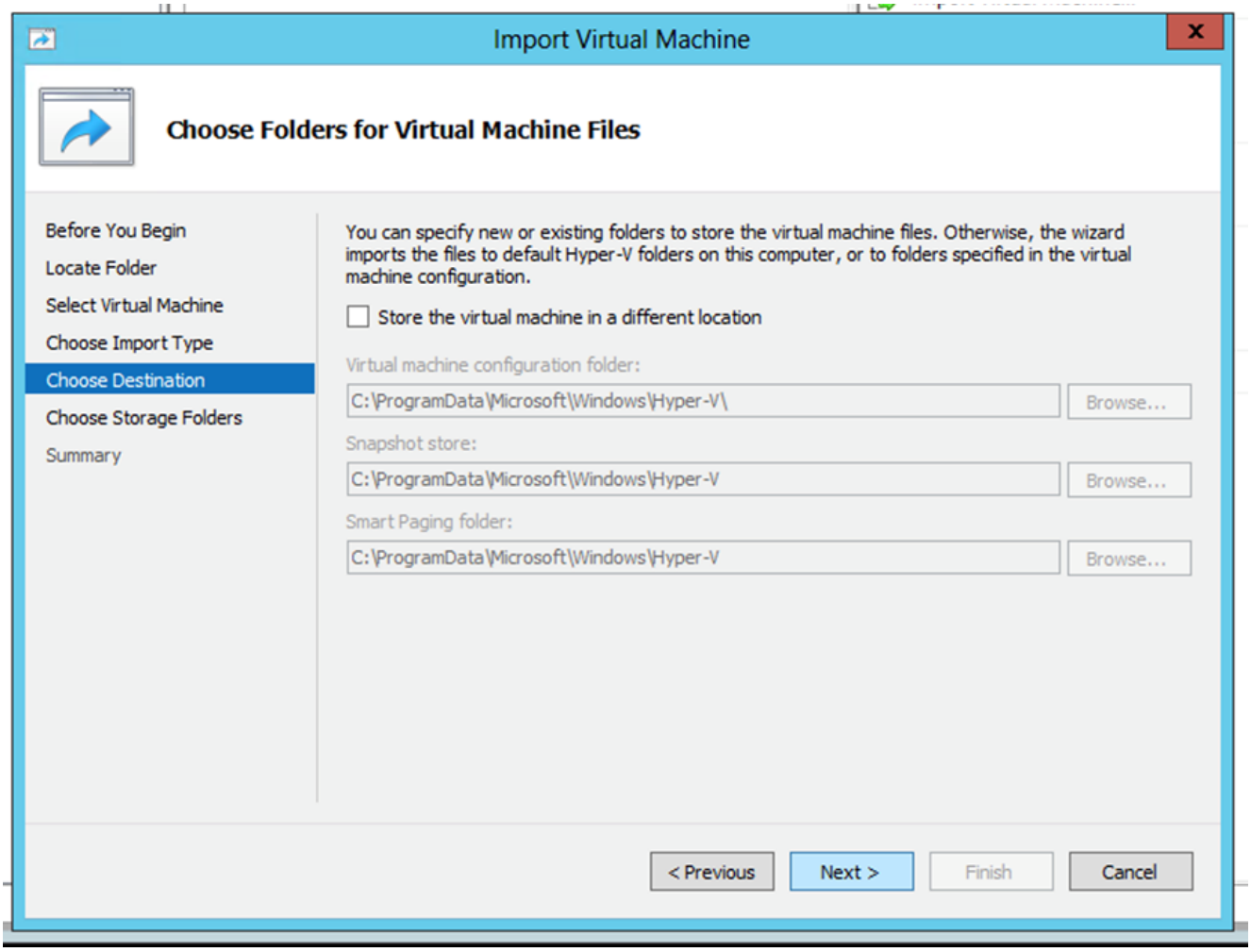
VM auswählen

5. Wählen Sie Copy the virtual machine (create a new unique ID) Optionsfeld und klicken Next.



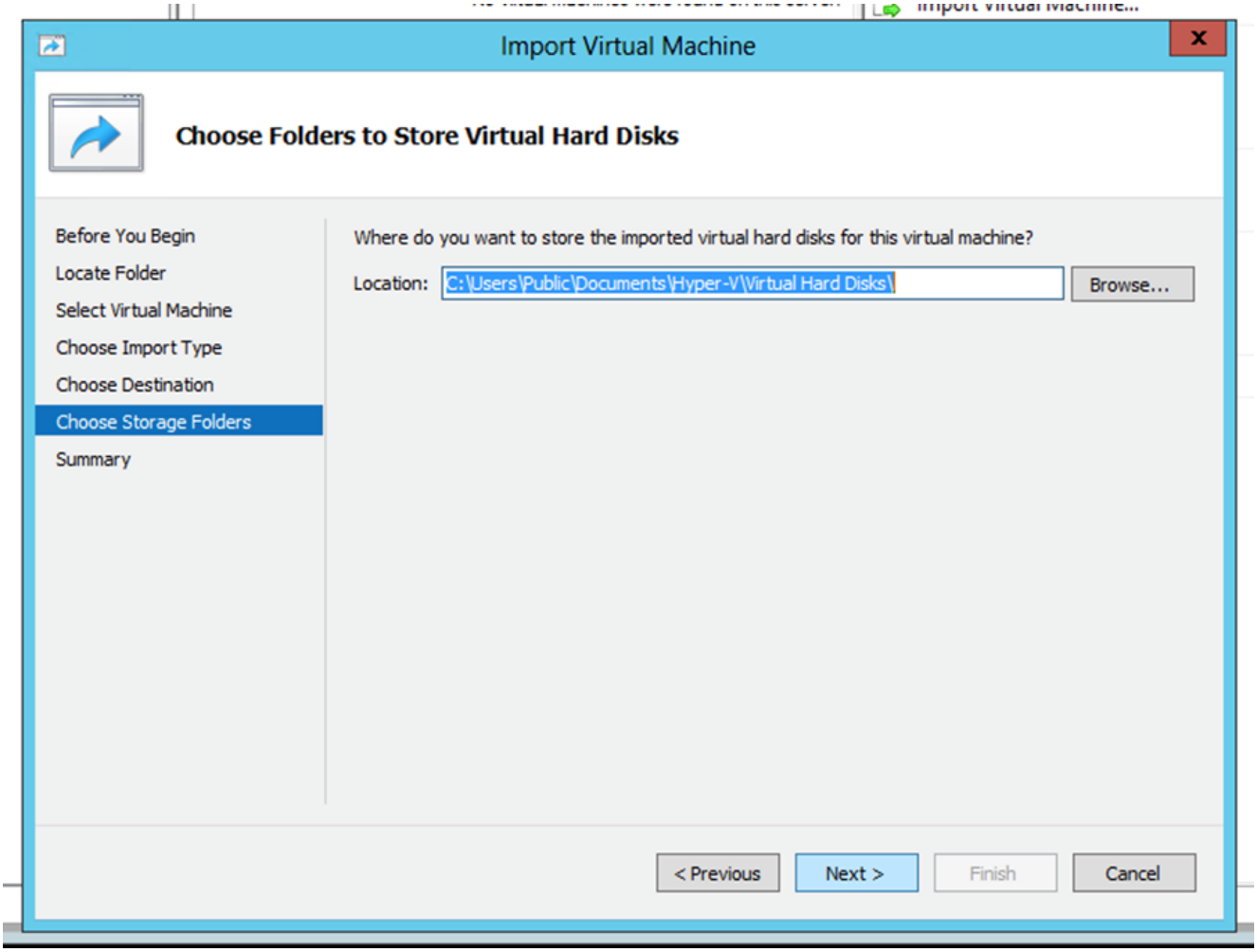
Importtyp

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



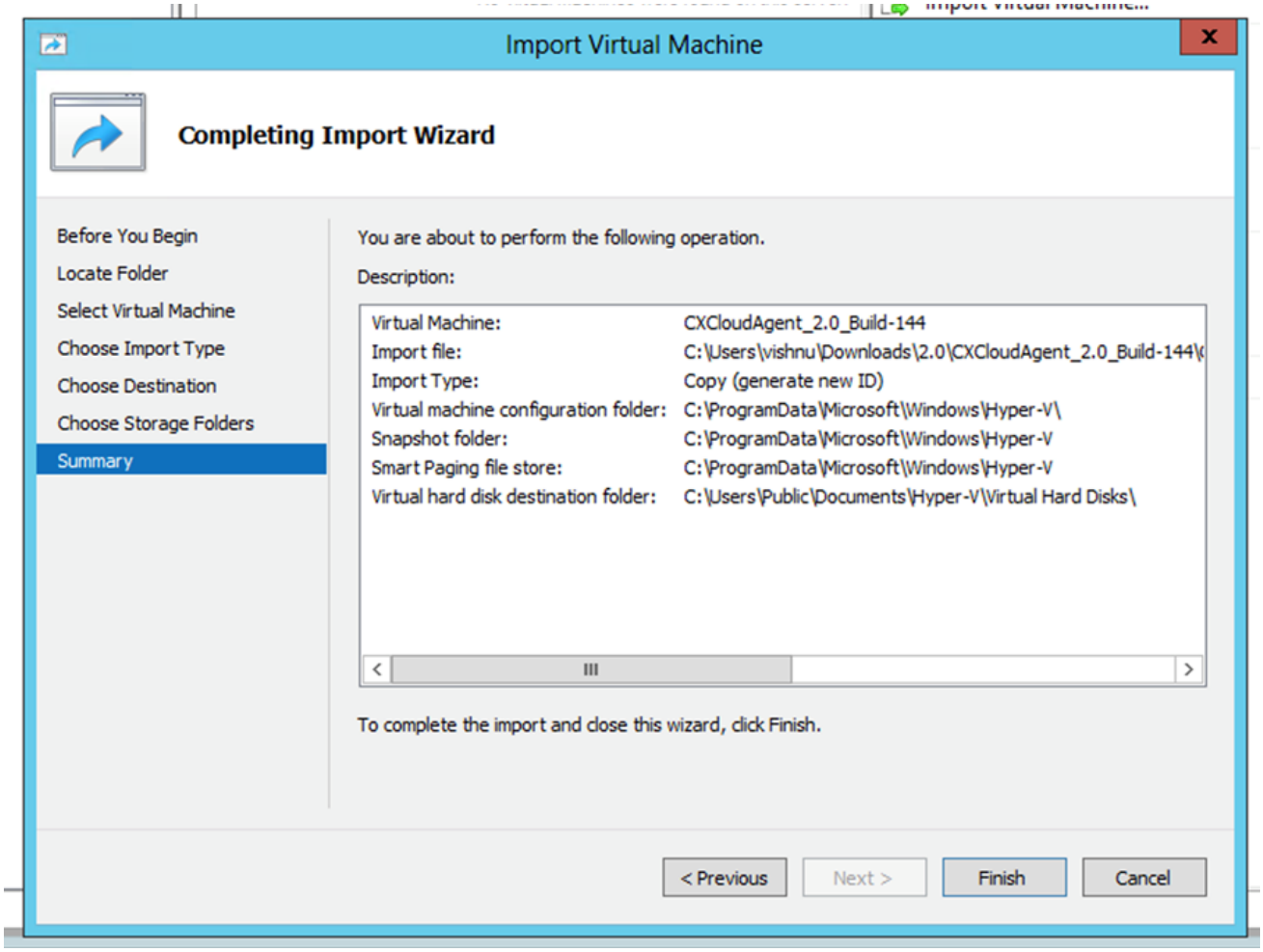
Ordner auswählen

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.



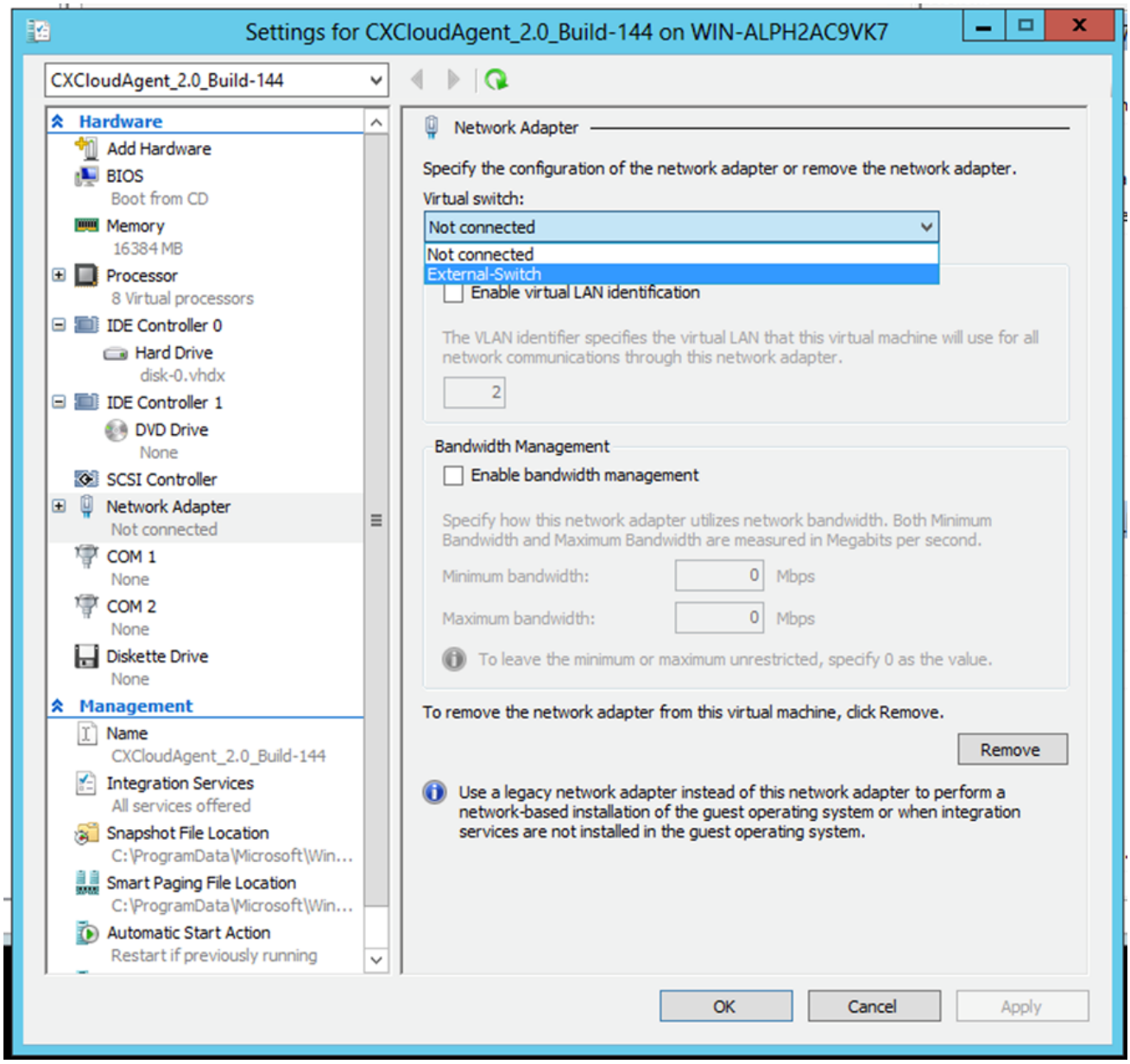
Ordner zum Speichern virtueller Festplatten

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



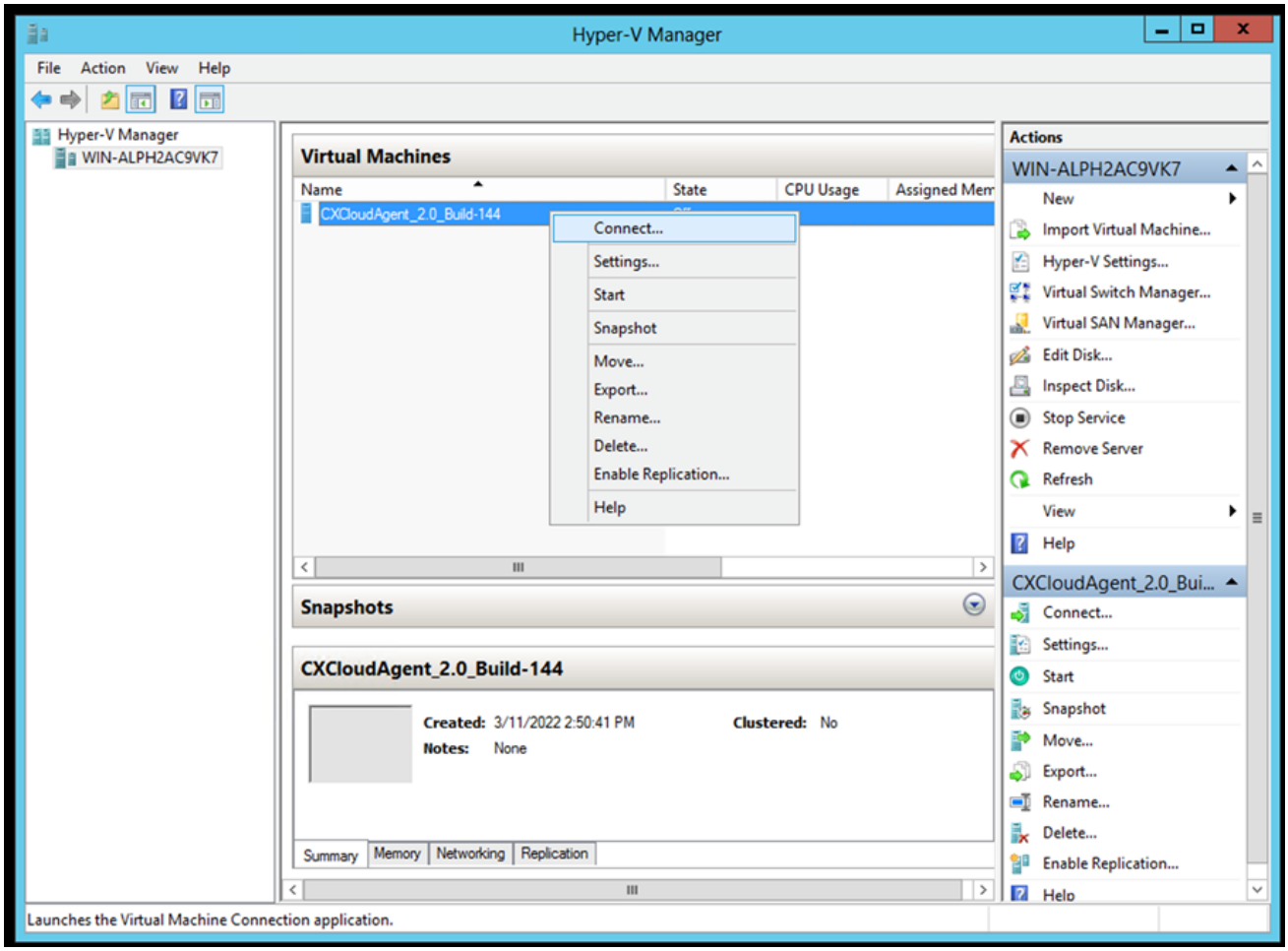
Zusammenfassung

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 aus, und wählen Sie den verfügbaren Virtual Switch aus dem Dropdown-Menü aus.



Virtueller Switch

13. Auswählen Connect um das virtuelle System zu starten.



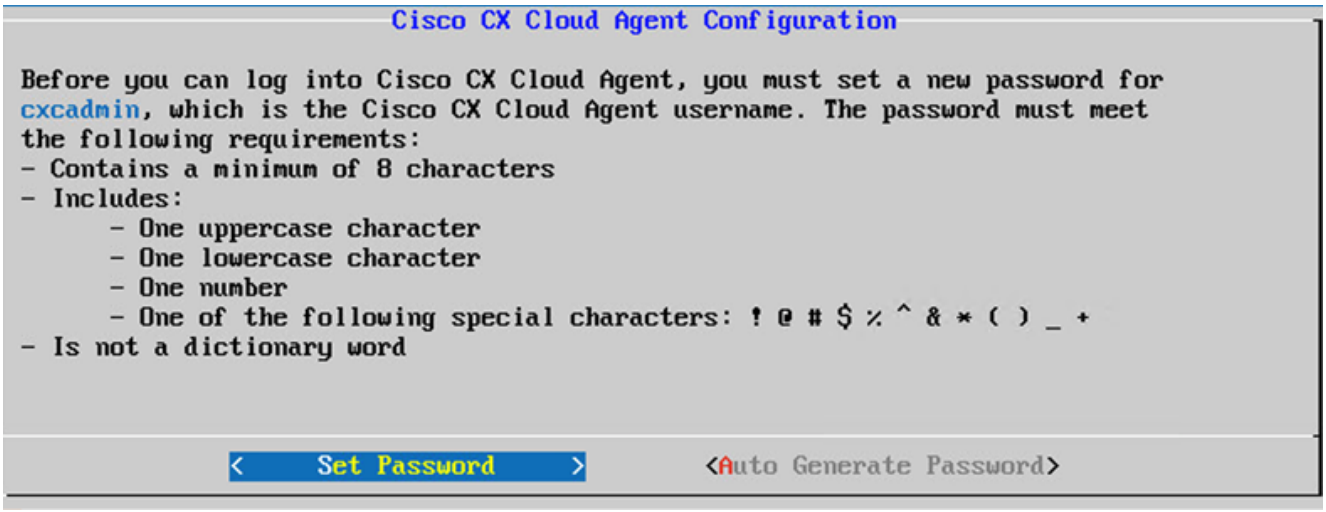
VM wird gestartet

14. Navigieren Sie zu Netzwerkkonfiguration.

Netzwerkkonfiguration

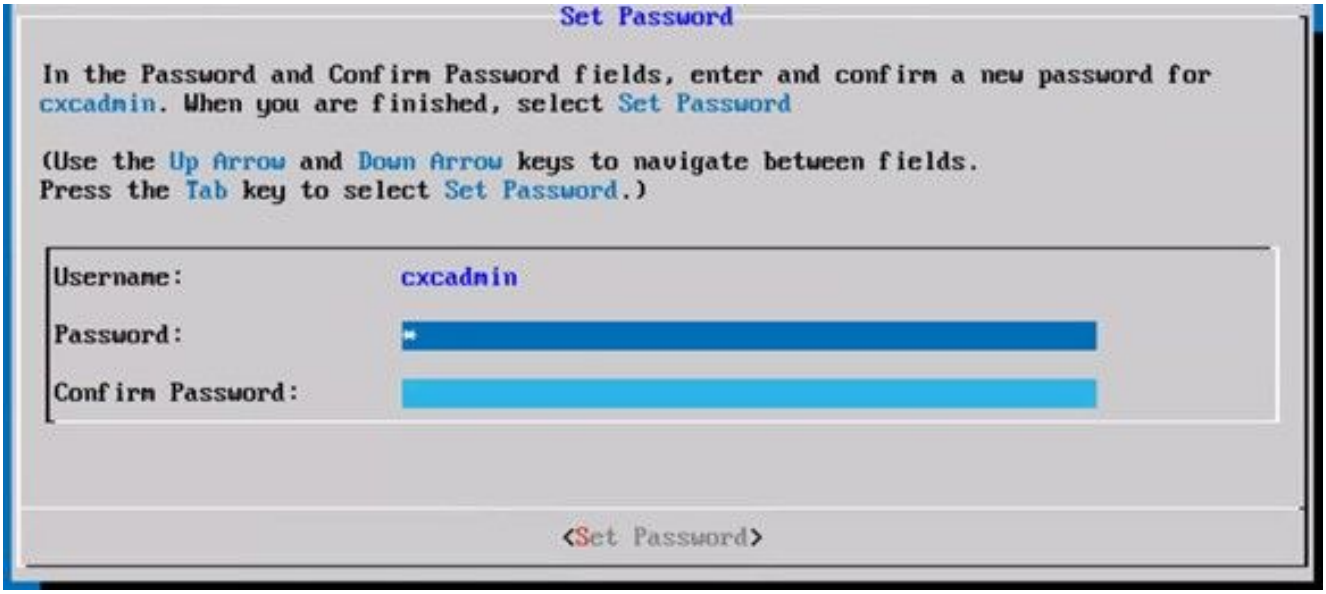
VM-Konsole

1. Klicken Sie auf Set Password um ein neues Kennwort für cxcadmin hinzuzufügen, ODER klicken Sie auf Auto Generate Password um ein neues Passwort zu erhalten.



Passwort festlegen

2. Wenn Set Password ausgewählt ist, geben Sie das Kennwort für cxcadmin ein, und bestätigen Sie es. Klicken Sie auf Set Password und gehe zu Schritt 3.



Neues Kennwort

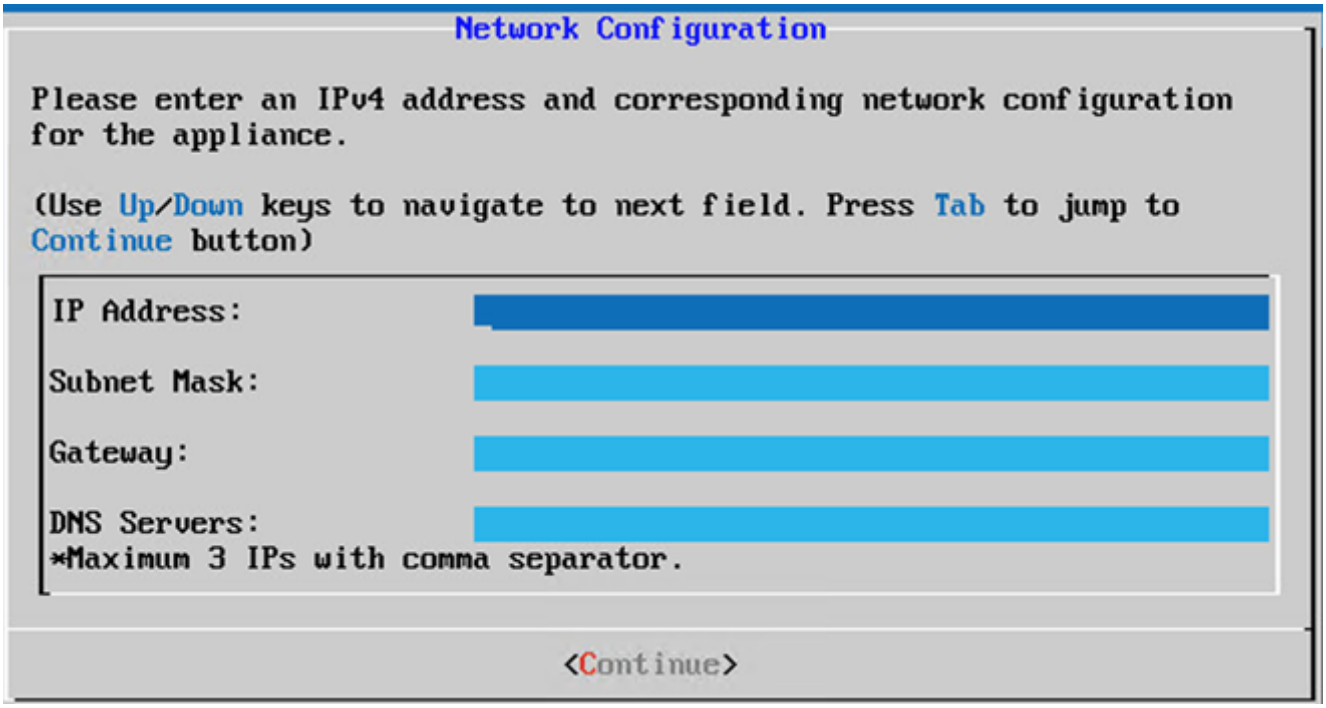
ODER Auto Generate Password ausgewählt ist, kopieren Sie das generierte Kennwort, und speichern Sie es zur späteren Verwendung. Klicken Sie auf Save Password und gehe zu Schritt 4
über.

Auto Generated Password (Automatisch generiertes Kennwort)

3. Klicken Sie auf Save Password um es für die Authentifizierung zu verwenden.

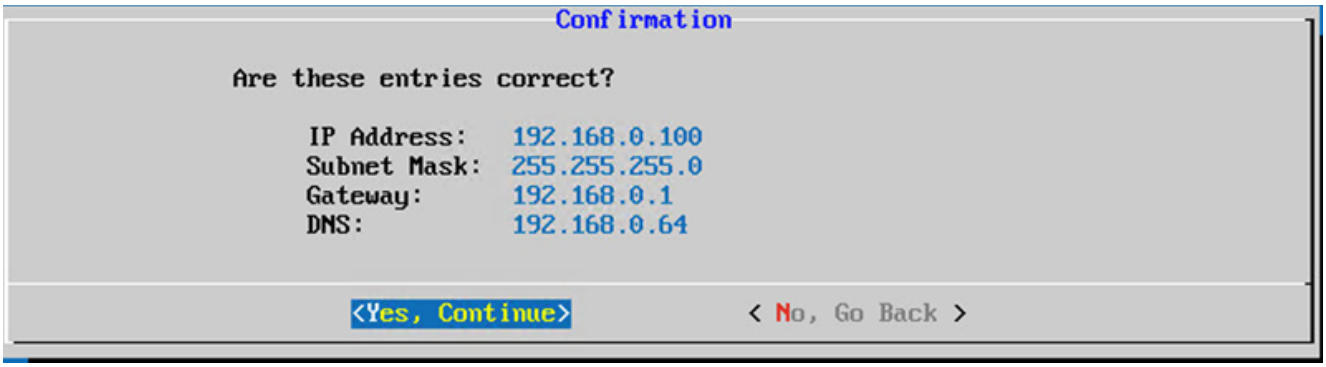
Passwort speichern

4. Geben Sie IP Address, Subnet Mask, Gatewayund DNS Server und klicke auf Continue.



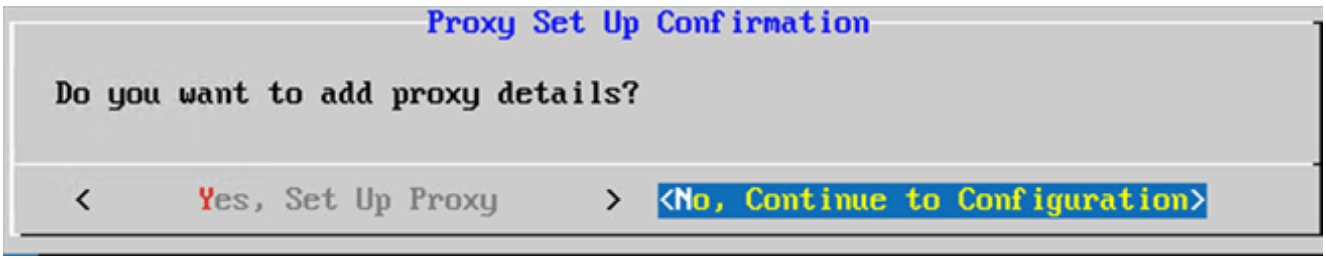
Netzwerkkonfiguration

5. Bestätigen Sie die Einträge, und klicken Sie auf Yes, Continue.



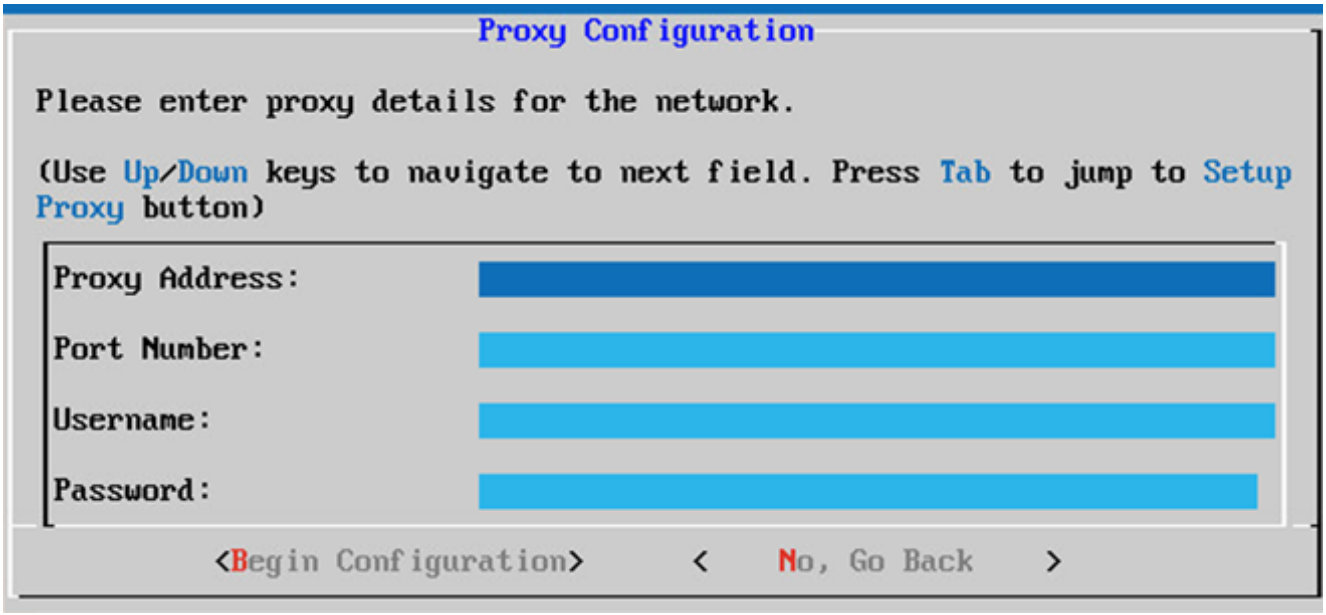
Bestätigung

6. Klicken Sie auf Yes, Set Up Proxy oder klicken Sie auf No, Continue to Configuration um die Konfiguration abzuschließen und mit Schritt 8 fortzufahren.



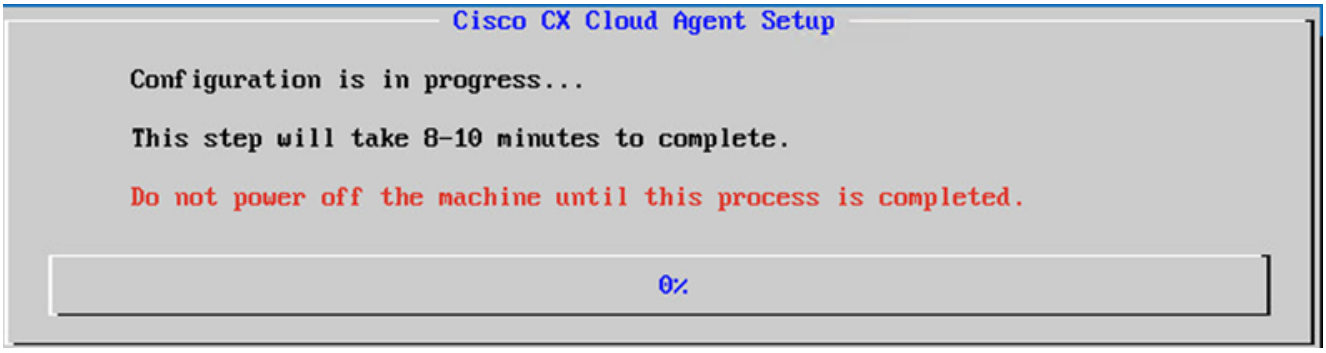
Proxy-Einrichtung

7. Geben Sie Proxy Address, Port Number, Usernameund Password.



Proxy-Konfiguration

8. Klicken Sie auf Begin Configuration. Die Konfiguration kann einige Minuten in Anspruch nehmen.



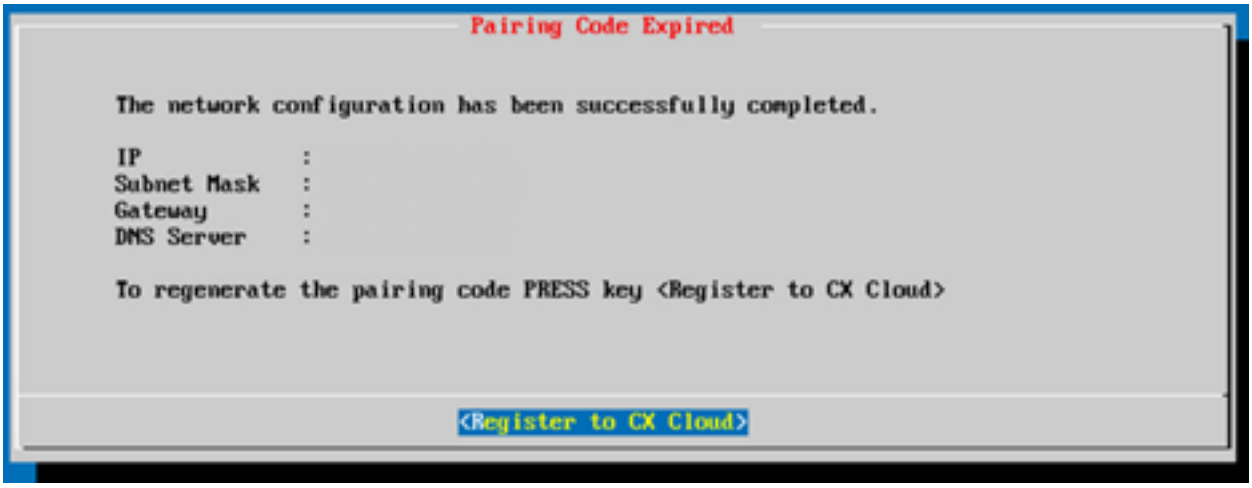
Konfiguration in Bearbeitung

9. Kopieren Sie Pairing Code und kehren Sie zur CX Cloud zurück, um die Einrichtung fortzusetzen.

Kopplungscode

10. Wenn der Kopplungscode abläuft, klicken Sie auf Register to CX Cloud um den Code erneut

abzurufen.



Code abgelaufen

11. Klicken Sie auf OK.

Registrierung erfolgreich

12. Kehren Sie zum Abschnitt Verbinden von CX Cloud Agent mit CX Cloud zurück, und führen Sie die aufgeführten Schritte aus.

Alternativer Ansatz zum Generieren von Kopplungscode mit CLI

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

So generieren Sie mithilfe der CLI einen Kopplungscode:

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 Pairing Code und kehren Sie zur CX Cloud zurück, um die Einrichtung fortzusetzen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Kundenportal.

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

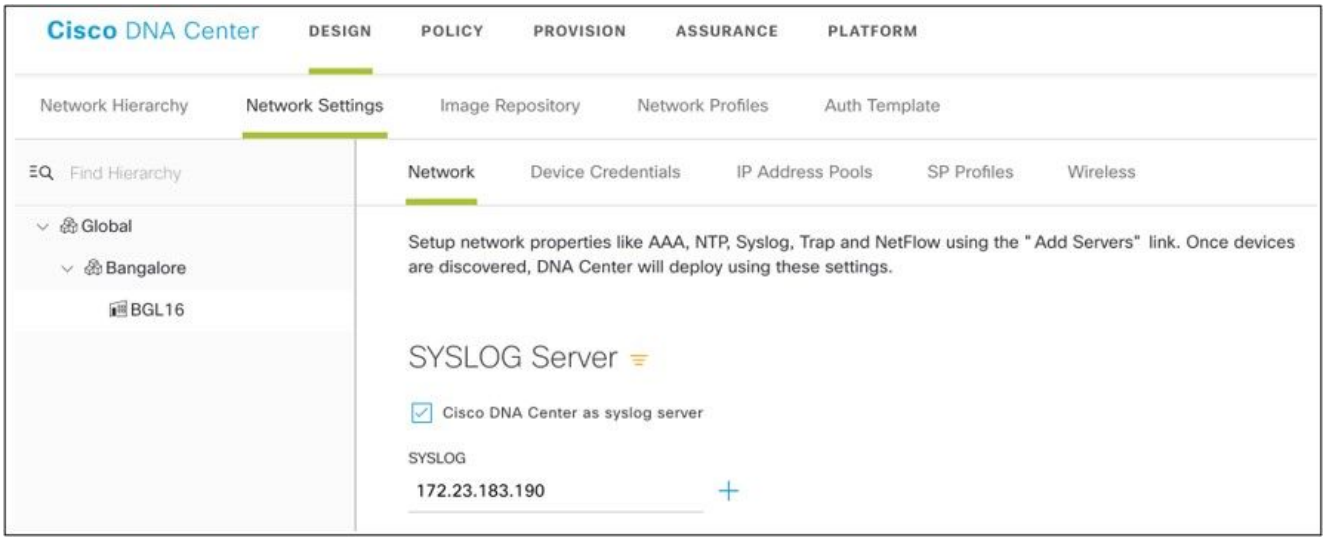
Voraussetzung

Die unterstützten Cisco DNA Center-Versionen reichen von 1.2.8 bis 1.3.3.9 und von 2.1.2.0 bis 2.2.3.5.

Syslog-Weiterleitungseinstellung konfigurieren

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

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



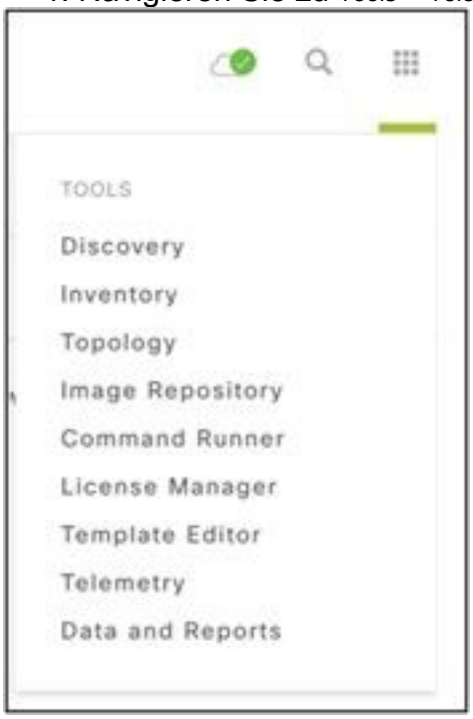
Syslog-Server

Hinweise:
- Nach der Konfiguration werden alle Geräte für diesen Standort so konfiguriert, dass Syslog mit der für CX Cloud Agent kritischen Stufe gesendet wird.
- Geräte müssen einem Standort zugeordnet werden, um die Syslog-Weiterleitung vom Gerät an 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.

Syslog-Einstellungen auf Informationsebene aktivieren

So machen Sie die Syslog-Informationen sichtbar:

1. Navigieren Sie zu Tools > Telemetry.



Menü Extras

2. Wählen und erweitern Sie das Site View und eine Site aus der Standorthierarchie auswählen.

Standortansicht

3. Wählen Sie den gewünschten Standort und alle Geräte aus, die den Device name Kontrollkästchen.

4. Aus dem Actions Dropdown-Liste auswählen Optimal Visibility.

Aktionen

Sicherheit

CX Cloud Agent gewährleistet dem Kunden umfassende Sicherheit. Die Verbindung zwischen CX Cloud und CX Cloud Agent ist verschlüsselt. Die Secure Socket Shell (SSH) von CX Cloud Agent unterstützt 11 verschiedene Chiffren.

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 die häufig gestellten Fragen lesen, um dieses Bootloader-Kennwort (Einzelbenutzermodus) festzulegen.

Benutzerzugriff

CX Cloud-Benutzer können nur eine Authentifizierung erhalten und auf die Cloud Agent-APIs zugreifen.

Kontosicherheit

Bei der Bereitstellung wird das cxcadmin-Benutzerkonto erstellt. Die Benutzer müssen während der Erstkonfiguration ein Kennwort festlegen. Der Benutzer cxcadmin/Die Anmeldeinformationen für Benutzer cxcadmin werden verwendet, um auf die CX Cloud Agent-APIs zuzugreifen und die Appliance über SSH zu verbinden.

Der Benutzer "cxcadmin" hat den Zugriff mit den geringsten Rechten eingeschränkt. Das Kennwort "cxcadmin" folgt der Sicherheitsrichtlinie und wird einseitig gehasht. Die Gültigkeitsdauer beträgt 90 Tage. Der Benutzer cxcadmin kann mithilfe des Dienstprogramms remote-account einen Benutzer mit dem Namen cxcroot erstellen. Der Benutzer cxcroot kann Root-Berechtigungen erhalten. Die Passphrase läuft in zwei Tagen ab.

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

Kennwortbasierte Authentifizierung: Die Appliance verwaltet einen einzelnen Benutzer – „cxcadmin“ . Dies ermöglicht es dem Benutzer, sich beim CX Cloud Agent zu authentifizieren und mit ihm zu kommunizieren.

- Privilegierte Aktionen auf der Appliance mit SSH rooten cxcadmin Benutzer kann cxcroot Benutzer erstellen, mit einem Dienstprogramm namens remote-account. Dieses Dienstprogramm zeigt ein verschlüsseltes RSA/ECB/PKCS1v1_5-Kennwort an, das nur vom SWIM-Portal (https://swims.cisco.com/abraxas/decrypt) entschlüsselt werden kann. Nur autorisiertes Personal hat Zugriff auf dieses Portal. Der Benutzer cxcroot kann mit diesem entschlüsselten Kennwort Root-Berechtigungen erhalten. Die Passphrase ist nur zwei Tage lang gültig. Der Benutzer cxcadmin muss das Konto neu erstellen und das Kennwort nach Ablauf des Kennworts aus dem SWIM-Portal abrufen.

Härtung

Die CX Cloud Agent-Appliance folgt den CIS-Härtungsstandards.

Datensicherheit

Die CX Cloud Agent-Appliance speichert keine persönlichen Kundeninformationen.

Die Anwendung für Geräteanmeldeinformationen (die als einer der Pods ausgeführt wird) speichert verschlüsselte Anmeldeinformationen für den Cisco DNA Center-Server in einer sicheren Datenbank. Die von Cisco DNA Center erfassten Daten werden in keiner Form in der Appliance gespeichert. Die erfassten Daten werden kurz nach Abschluss der Erfassung in die gesicherte Datei hochgeladen. Die Daten werden vom Agenten gelöscht.

Datenübertragung

Das Registrierungspaket enthält die erforderlichen eindeutigen X.509 Gerätezertifikat und Schlüssel, um eine sichere Verbindung mit dem Iot Core herzustellen. Mit diesem Agent wird eine sichere Verbindung mit MQTT über TLS v1.2 hergestellt.

Protokolle und Überwachung

Protokolle enthalten keinerlei vertrauliche Informationen. Überwachungsprotokolle erfassen alle sicherheitsrelevanten Aktionen, die auf der CX Cloud Agent-Appliance ausgeführt werden.

Sicherheitszusammenfassung

Sicherheitsfunktionen	Beschreibung
Bootloader-Kennwort	Für das Bootloader-Kennwort (Einzelbenutzermodus) wird ein zufälliges, eindeutiges Kennwort festgelegt. Der Benutzer muss die häufig gestellten Fragen lesen, um sein Bootloader-Kennwort (Einzelbenutzermodus) festzulegen.
Benutzerzugriff	SSH: • Für den Zugriff auf die Appliance mit dem Benutzer cxcadmin sind die Anmeldeinformationen erforderlich, die während der Installation erstellt wurden.

Benutzerkonten	• Der Zugriff auf die Appliance über den Benutzer "cxcroot" erfordert, dass die Anmeldeinformationen von autorisierten Mitarbeitern über das SWIM Portal entschlüsselt werden. • cxcadmin: Dies ist ein erstelltes Standardbenutzerkonto. Der Benutzer kann über cxcli Anwendungsbefehle für CX Cloud Agent ausführen und hat nur die notwendigsten Berechtigungen für die Appliance. Benutzer cxcroot und das zugehörige verschlüsselte Kennwort werden über den Benutzer cxcadmin generiert • cxcroot: cxcadmin kann diesen Benutzer mit dem Dienstprogramm "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, Ziffern 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 zugehörige Kennwort sind maximal zwei Tage lang gültig und können mit dem Benutzer cxcadmin neu generiert werden.
Richtlinie für das SSH-Anmeldekennwort	• Mindestens acht (8) Zeichen mit drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen • 5 fehlgeschlagene Anmeldeversuche blockieren das System für 30 Minuten. Das Kennwort läuft nach 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.

Häufig gestellte Fragen

CX Cloud Agent

Bereitstellung

F - Kann der Benutzer über die Option "Neu installieren" den neuen Cloud Agent mit neuer IP-Adresse bereitstellen?

A - Ja

F - Welche Dateiformate stehen für die Installation zur Verfügung?

A - OVA und VHD

F - In welcher Umgebung kann die installierbare Einheit bereitgestellt werden?

A - OVA

VMWare ESXi Version 5.5 oder höher

Oracle Virtual Box 5.2.30 oder höher

VHD

Windows Hypervisor 2012 bis 2016

F - Kann CX Cloud Agent IP-Adressen in einer DHCP-Umgebung erkennen?

A - Ja, im Falle einer DHCP-Umgebung erfolgt die IP-Adresszuweisung während der IP-Konfiguration. Die für den CX Cloud Agent erwartete IP-Adressänderung wird jedoch in Zukunft nicht unterstützt. Zudem wird dem Kunden empfohlen, die IP für den Cloud Agent in seiner DHCP-Umgebung zu reservieren.

F - Unterstützt CX Cloud Agent sowohl die IPv4- als auch die IPv6-Konfiguration?

A - Nein, nur IPv4 wird unterstützt.

F - Wird die IP-Adresse während der IP-Konfiguration validiert?

A - Ja, IP-Adressensyntax und doppelte IP-Adresszuweisung werden validiert.

F - Wie viel Zeit nehmen die Bereitstellung der OVA und die IP-Konfiguration ungefähr in Anspruch?

A - Die OVA-Bereitstellung ist im Hinblick auf das Kopieren der Daten von der Geschwindigkeit des Netzwerks abhängig. Die IP-Konfiguration dauert etwa 8 bis 10 Minuten und umfasst Kubernetes und Containererstellungen.

F - Gibt es Einschränkungen bezüglich der Hardware?

A - Der Host-Rechner, auf dem OVA bereitgestellt wird, muss die im Rahmen der CX-Portal-Konfiguration gestellten Anforderungen erfüllen. Der CX Cloud Agent wird mit VMware/Virtual Box getestet, die auf einer Hardware mit Intel Xeon E5 Prozessoren mit einem vCPU/CPU-Verhältnis von 2:1 ausgeführt wird. Wenn eine weniger leistungsstarke Prozessor-CPU oder ein größeres Verhältnis verwendet wird, kann sich die Leistung verschlechtern.

F - Können wir den Kopplungscode jederzeit generieren?

A - Nein, der Kopplungscode kann nur generiert werden, wenn der Cloud Agent nicht registriert ist.

F - Welche Bandbreitenanforderungen bestehen zwischen DNACs (für bis zu 10 Cluster oder 20 Nicht-Cluster) und Agent?

A - Die Bandbreite stellt keine Einschränkung dar, wenn sich Agent und DNAC in der Kundenumgebung im selben LAN/WAN-Netzwerk befinden. Die mindestens erforderliche Netzwerkbandbreite beträgt 2,7 Mbit/s für Bestandssammlungen von 5.000 Geräten +13000 Access Points für eine Verbindung zwischen Agent und DNAC. Wenn Syslogs für L2-Einblicke erfasst werden, beträgt die erforderliche Mindestbandbreite 3,5 Mbit/s für die Abdeckung von 5.000 Geräten +13000 Access Points für Bestand, 5.000 Geräte Syslogs und 2.000 Geräten für Scans - alle parallel von Agent ausgeführt.

Versionen und Patches

F - Welche Arten von Versionen sind für das Upgrade von CX Cloud Agent aufgeführt?

A - Hier sind die veröffentlichten Versionen von CX Cloud Agent aufgeführt:

- Ax0 (x steht für die aktuelle Produktionsversion mit ihren Hauptfunktionen, Beispiel: 1.3.0)
- A.x.y (wobei A.x.0 obligatorisch ist und ein inkrementelles Upgrade initiiert werden muss, x die neueste Version der Hauptfunktionen für die Produktion und y der neueste aktive Upgrade-Patch ist, Beispiel: 1.3.1).
- A.x.y-z (wobei A.x.0 obligatorisch ist und ein inkrementelles Upgrade initiiert werden muss, x die neueste Version der Hauptfunktionen für die Produktion ist und y der neueste aktive Upgrade-Patch ist, und z der Spot-Patch ist, der eine sofortige Korrektur für einen sehr kurzen Zeitraum darstellt, z. B.: 1.3.1-1)

wobei A eine langfristige Veröffentlichung ist, die sich über einen Zeitraum von 3-5 Jahren erstreckt.

F - Wo finden Sie die neueste Version von CX Cloud Agent und wie aktualisieren Sie den vorhandenen CX Cloud Agent?

A - Gehe zu Admin Settings > Data Sources. Klicken Sie auf View Update und die auf dem Bildschirm freigegebenen Anweisungen ausführen.

Authentifizierung und Proxy-Konfiguration

F - Wie lautet der Standardbenutzer der CX Cloud Agent-Anwendung?

A - cxcadmin

F - Wie wird das Kennwort für den Standardbenutzer festgelegt?

A - Das Kennwort wird während der Netzwerkkonfiguration festgelegt.

F - Gibt es eine Möglichkeit, das Kennwort nach dessen Ablauf zurückzusetzen?

A - Der Agent bietet keine spezielle Option zum Zurücksetzen des Kennworts, aber Sie können die Linux-Befehle verwenden, um das Kennwort für cxcadmin zurückzusetzen.

F - Wie lauten die Kennwortrichtlinien für die Konfiguration des CX Cloud Agent?

A - Die Kennwortrichtlinien lauten wie folgt:

- Das maximale Kennwortalter (Länge) ist auf 90 Tage festgelegt
- Das minimale Kennwortalter (Länge) ist auf 8 festgelegt
- Die maximale Kennwortlänge beträgt 127 Zeichen.
- Es muss mindestens ein Ober- und ein Unterfall vorgesehen sein.
- Muss mindestens ein Sonderzeichen enthalten (z. B. !$%^&*()_+|~-=\`{}[]:";'<>?,/).
- Diese Zeichen sind nicht zulässig. 8-Bit-Sonderzeichen (Beispiel: ¬£, √Å √´, √¥, √ë, ¬ø, √ü)Leerzeichen
- Das Kennwort darf nicht die zuletzt verwendeten 10 Kennwörter sein.

- Darf keinen regulären Ausdruck enthalten, d. h.
- Darf folgende Wörter oder Derivate nicht enthalten: cisco, sanjose und sanfran

F - Wie wird das GRUB-Kennwort festgelegt?

A - So legen Sie das Grub-Kennwort fest:

1. Führen Sie den Befehl "ssh als cxcroot" aus und stellen Sie das Token bereit. [Wenden Sie sich an das Support-Team, um das cxcroot-Token zu erhalten.]
2. Führen Sie den Befehl "sudo su" aus und geben Sie das gleiche Token an.
3. Führen Sie den Befehl "grub-mkpasswd-pbkdf2" aus und legen Sie das GRUB-Kennwort fest. Der Hash des angegebenen Kennworts wird gedruckt. Kopieren Sie den Inhalt.
4. vi in Datei /etc/grub.d/00_header. Navigieren Sie zum Ende der Datei und ersetzen Sie die Hash-Ausgabe, gefolgt vom Inhalt password_pbkdf2 root *****, durch den erhaltenen Hash für das Kennwort aus Schritt 3.
5. Speichern Sie die Datei mit dem Befehl ":wq!".
6. Führen Sie den Befehl "update-grub" aus

Q - Wie lange läuft das Kennwort von ab? cxcadmin?

A - Das Kennwort läuft nach 90 Tagen ab.

F - Wird das Konto nach mehreren aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen deaktiviert?

A - Ja, das Konto wird nach 5 aufeinanderfolgenden fehlgeschlagenen Versuchen deaktiviert. Die Sperrzeit beträgt 30 Minuten.

F - Wie wird eine Passphrase generiert?

A - Führen Sie diese Schritte aus,

1. Führen Sie ssh aus, und melden Sie sich als Benutzer cxcadmin an.
2. Führen Sie den Befehl *remoteaccount cleanup -f aus.*
3. Führen Sie den Befehl *remoteaccount create aus.*

F - Unterstützt der Proxy-Host sowohl Hostname als auch IP?

A - Ja, aber um den Hostnamen zu verwenden, muss der Benutzer die DNS-IP während der Netzwerkkonfiguration angeben.

Secure Shell (SSH)

F - Welche Chiffren werden von der Secure Shell (SSH) unterstützt?

A - chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com , aes256-ctr, aes192-ctr, aes128-ctr

F - Wie kann ich mich bei der Konsole anmelden?

A - Führen Sie die folgenden Schritte aus, um sich anzumelden:

1. Melden Sie sich als Benutzer cxcadmin an.

2. Geben Sie das Kennwort cxcadmin ein.

F - Werden SSH-Anmeldungen protokolliert?

A - Ja, sie werden als Teil von var/logs/audit/audit.log protokolliert.

F - Wie lange dauert die Leerlaufsitzung?

A - Ein Timeout für eine SSH-Sitzung tritt auf, wenn der Cloud-Agent fünf (5) Minuten lang inaktiv ist.

Ports und Services

F - Welche Ports werden im CX Cloud Agent standardmäßig offen gehalten?

A - Diese Ports sind verfügbar:

- Outbound port: Der bereitgestellte CX Cloud Agent kann eine Verbindung zum Cisco Backend herstellen, wie in der Tabelle auf HTTPS-Port 443 angegeben, oder über einen Proxy, um Daten an Cisco zu senden. Der bereitgestellte CX Cloud Agent kann über den HTTPS-Port 443 eine Verbindung zum Cisco DNA Center herstellen.

.

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

Anmerkung: Wenn EMEA- oder APJC-Kunden den Cloud Agent neu installieren, muss zusätzlich zu den aufgeführten Domänen die Domäne agent.us.csco.cloud in der Kunden-Firewall zugelassen sein.

Die Domain agent.us.csco.cloud wird nach erfolgreicher Neuinstallation nicht mehr benötigt.

Anmerkung: Stellen Sie sicher, dass Datenrückverkehr auf Port 443 zugelassen werden muss.

- Inbound port: Für die lokale Verwaltung des CX Cloud Agent müssen 514 (Syslog) und 22 (SSH) zugänglich sein. Der Kunde muss zulassen, dass Port 443 in seiner Firewall Daten von der CX Cloud empfängt.

CX Cloud Agent-Verbindung mit Cisco DNA Center

F - Welchen Zweck haben Cisco DNA Center und CX Cloud Agent und in welcher Beziehung stehen sie zueinander?

A - Cisco DNA Center ist der Cloud Agent, der die Netzwerkgeräte am Kundenstandort verwaltet. CX Cloud Agent sammelt die Bestandsinformationen der Geräte über das konfigurierte Cisco DNA

Center und lädt die Bestandsinformationen hoch, die als "Ressourcenansicht" in CX Cloud verfügbar sind.

F - Wo kann der Benutzer Details zum Cisco DNA Center zum CX Cloud Agent angeben?

A - Während der Einrichtung von Tag 0 - CX Cloud Agent kann der Benutzer die Details zum Cisco DNA Center aus dem CX Cloud-Portal hinzufügen. Zusätzlich können Benutzer während des Day N-Betriebs zusätzliche DNA-Zentren hinzufügen, Admin Settings > Data source.

F - Wie viele Cisco DNA Center können hinzugefügt werden?

A - Entweder 10 Cisco DNAC-Cluster oder 20 DNAC-Nicht-Cluster.

Frage: Welche Rolle kann ein Benutzer von Cisco DNA Center übernehmen?

A - Die Benutzerrolle kann entweder admin Oder observer.

F - Wie kann ich die Änderungen in CX Agent aufgrund von Änderungen bei den Anmeldeinformationen des vernetzten DNA Centers wiedergeben?

A - Führen Sie diesen Befehl von der Konsole des CX Cloud Agent aus:

cxcli agent modifizierenController

Wenden Sie sich bei Problemen während der Aktualisierung der DNAC-Anmeldeinformationen an den Support.

F - Wie werden die Cisco DNA Center-Details in CX Cloud Agent gespeichert?

A - Anmeldeinformationen für Cisco DNA Center werden mit AES-256 verschlüsselt und in der Datenbank des CX Cloud Agent gespeichert. Die Datenbank des CX Cloud Agent ist mit einer sicheren Benutzer-ID und einem Kennwort geschützt.

F - Welche Art von Verschlüsselung wird beim Zugriff auf die Cisco DNA Center-API über den CX Cloud Agent verwendet?

A - Für die Kommunikation zwischen Cisco DNA Center und dem CX Cloud Agent wird HTTPS über TLS 1.2 verwendet.

F - Welche Vorgänge führt der CX Cloud Agent auf dem integrierten Cisco DNA Center Cloud Agent aus?

A - CX Cloud Agent sammelt Daten von Cisco DNA Center zu den Netzwerkgeräten und nutzt die Befehlsrunner-Schnittstelle von Cisco DNA Center, um mit Endgeräten zu kommunizieren und CLI-Befehle auszuführen (Befehl show). Es werden keine Konfigurationsänderungsbefehle ausgeführt

F - Welche Standarddaten werden von Cisco DNA Center erfasst und in das Backend hochgeladen?

A -

- Netzwerkentität

- Module
- Show version
- Konfig.
- Gerätebildinformationen
- Tags

F - Welche zusätzlichen Daten werden von Cisco DNA Center erfasst und in Cisco Backend hochgeladen?

A - Sie erhalten alle Informationen hier.

F - Wie werden die Bestandsdaten in das Backend hochgeladen?

A - CX Cloud Agent lädt die Daten über das TLS 1.2-Protokoll auf den Cisco Backend-Server hoch.

F - Wie oft werden Bestände hochgeladen?

A - Die Erfassung wird gemäß dem benutzerdefinierten Zeitplan ausgelöst und in das Cisco Backend hochgeladen.

F - Kann der Benutzer den Bestand neu planen?

A - Ja, es ist eine Option zum Ändern der Zeitplaninformationen von verfügbar. Admin Settings> Data Sources.

F - Wann tritt das Verbindungs-Timeout zwischen Cisco DNA Center und Cloud Agent auf?

A - Timeouts werden wie folgt kategorisiert:

- Bei der Erstverbindung beträgt das Timeout maximal 300 Sekunden. Wenn innerhalb von maximal 5 Minuten keine Verbindung zwischen Cisco DNA Center und Cloud Agent hergestellt wird, wird die Verbindung beendet.
- Bei wiederkehrenden Verbindungen, typischen Verbindungen oder Aktualisierungen: Das Antwort-Timeout beträgt 1.800 Sekunden. Wenn die Antwort nicht innerhalb von 30 Minuten empfangen wird oder nicht gelesen werden kann, wird die Verbindung beendet.

CX Cloud Agent verwendet Diagnosescan

F - Welche Befehle werden auf dem Gerät für den Scan ausgeführt?

A - Befehle, die für den Scan auf dem Gerät ausgeführt werden müssen, werden während des Scanvorgangs dynamisch bestimmt. Die Befehlssätze können sich im Laufe der Zeit ändern, auch für das gleiche Gerät (und ohne Kontrolle über die Diagnosescans).

F - Wo werden die Scan-Ergebnisse gespeichert und profiliert?

A - Die gescannten Ergebnisse werden im Cisco Backend gespeichert und profiliert.

F - Werden die Duplikate (nach Hostname oder IP) in Cisco DNA Center zum Diagnosescan hinzugefügt, wenn die Cisco DNA Center-Quelle angeschlossen ist?

A - Nein, Duplikate werden gefiltert und nur die eindeutigen Geräte werden extrahiert.

F - Was geschieht, wenn einer der Befehlsscans fehlschlägt?

A - Der Gerätescan wird vollständig beendet und als nicht erfolgreich markiert.

CX Cloud Agent-Systemprotokolle

F - Welche Integritätsinformationen werden an die CX-Cloud gesendet?

A - Anwendungsprotokolle, Pod-Status, Cisco DNA Center-Details, Audit-Protokolle, Systemdetails und Hardwaredetails.

F - Welche System- und Hardwaredetails werden erfasst?

A - Beispielausgabe:

Systemdetails":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
"Betriebssystem":"Linux",
"osImage":"Ubuntu 20.04.1 LTS",
"systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
},
"Hardware_Details":{
"total_cpu":"8",
"cpu_usage":"12,5 %",
"Speicher gesamt":"16007 MB",
"freier Speicher":"9994 MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}

F - Wie werden die Integritätsdaten an das Backend gesendet?

A - Mit CX Cloud Agent überträgt der Integritätsdienst (Betriebsfähigkeit) die Daten an das Cisco Backend.

F - Wie lautet die Aufbewahrungsrichtlinie für Integritätsdatenprotokolle des CX Cloud Agent im Backend?

A - Die Aufbewahrungsrichtlinie für Integritätsdatenprotokolle des CX Cloud Agent im Backend beträgt 120 Tage.

F - Welche Arten von Uploads sind verfügbar?

A - Drei Arten von Uploads sind verfügbar,

1. Bestands-Upload
2. Syslog-Upload
3. Agenten-Statusupload: 3 Dinge als Teil des Health Uploads Service-Zustand - alle 5 MinutenPodlog - alle 1 StundeAudit-Protokoll - alle 1 Stunde

Fehlerbehebung

Problem: Kein Zugriff auf die konfigurierte IP möglich.

Lösung: Führen Sie SSH mit der konfigurierten IP aus. Bei einer Verbindungsunterbrechung liegt der mögliche Grund in einer falschen IP-Konfiguration. Führen Sie in diesem Fall eine Neuinstallation durch, indem Sie eine gültige IP-Adresse konfigurieren. Dies kann über das Portal mit der im Admin Setting Seite.

Problem: Wie kann überprüft werden, ob die Services nach der Registrierung betriebsbereit sind?

Lösung: Führen Sie den hier gezeigten Befehl aus, und stellen Sie sicher, dass die PODs betriebsbereit sind.

1. SSH auf die konfigurierte IP als cxcadmin.
2. Geben Sie das Kennwort an.
3. Führen Sie den Befehl *kubectl get pods aus*.

Die PODs können sich in einem beliebigen Status befinden, z. B. "Wird ausgeführt", "Initialisiert" oder "Container erstellt". Nach 20 Minuten müssen die PODs jedoch den Status "Wird ausgeführt" aufweisen.

Wenn der Status *nicht ausgeführt wird* oder *Pod nicht initialisiert wird*, überprüfen Sie die POD-Beschreibung mit dem hier gezeigten Befehl.

kubectl description pod <podname>

Die Ausgabe enthält die Informationen zum Podstatus.

Problem: Wie kann ich überprüfen, ob SSL Interceptor im Kundenproxy deaktiviert ist?
Lösung: Führen Sie den hier gezeigten Curl-Befehl aus, um den Abschnitt für das Serverzertifikat zu überprüfen. Die Antwort enthält die Zertifikatdetails des consoweb-Servers.

curl -v —header 'Autorisierung: Basic xxxxxx' https://concsoweb-prd.cisco.com/

* Serverzertifikat:

* Betreff: C=USA; ST=Kalifornien; L=San Jose; O=Cisco Systems, Inc. CN=concsoweb-prd.cisco.com

* Startdatum: 16.02.11 11:55:11 Uhr GMT

* Ablaufdatum: 16.02.12 12:05:00 2022 GMT

* BetreffAltName: Host "concsoweb-prd.cisco.com" entspricht "concsoweb-prd.cisco.com" von CERT

* Emittent: C=USA; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL CA G3

* SSL-Zertifikat überprüft OK.

>GET/HTTP/1.1

Problem: kubectl-Befehle fehlgeschlagen und zeigt den Fehler als "Die Verbindung zum Server wurde verweigert X.X.X.X:6443 - haben Sie den richtigen Host oder Port angegeben"
Lösung:

- sollten Sie die Verfügbarkeit der Ressourcen überprüfen. [beispiel: CPU, Arbeitsspeicher]
- Warten Sie, bis der Kubernetes Service gestartet wird

Problem: Wie erhalte ich Details zu einem Erfassungsfehler für einen Befehl/ein Gerät?

Lösung:

- Durchführung `kubectl get pods` und rufen Sie den Namen des Sammlungspods ab.
- Durchführung `kubectl logs` um bestimmte Details zu dem Befehl/Gerät abzurufen.

Problem: Der Befehl kubectl kann nicht ausgeführt werden. Fehler: "[authentication.go:64] Die Anfrage kann aufgrund eines Fehlers nicht authentifiziert werden: [x509: Zertifikat ist abgelaufen oder ist noch nicht gültig, x509: Zertifikat ist abgelaufen oder noch nicht gültig]"

Lösung: Führen Sie die hier gezeigten Befehle als *cxcroot*-Benutzer aus

rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl —insecure-skip-tls-verify=true delete secret -n kube-system k3s-serving
systemctl restart k3s

Reaktionen auf Erfassungsfehler

Ursache für Erfassungsfehler können Einschränkungen oder Probleme mit dem hinzugefügten Controller oder den im Controller vorhandenen Geräten sein.

Die hier abgebildete Tabelle enthält den Fehlerausschnitt für Anwendungsfälle, der während des Erfassungsprozesses unter dem Collection-Mikrodienst angezeigt wird.

Anwendungsfall	Protokoll-Snippet im Microservice "Erfassung"
Wenn das angeforderte Gerät in Cisco DNA Center nicht gefunden wird	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a " }
Wenn das angeforderte Gerät nicht über Cisco DNA Center erreichbar ist	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error occurred while executing command: show version\r connecting to device [Host: 172.21.137.221:22]No route to host : No route t }
Wenn das angeforderte Gerät nicht über Cisco DNA Center erreichbar ist	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error occured while executing command : show version\r connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connection timed out: /X.X.X.X:22" }
Wenn der angeforderte Befehl im Gerät nicht verfügbar ist	{ "command": "show run-config", "status": "Success", "commandResponse": " Error occured while executing command : show ru config\n\nshow run-config\n ^\n% Invalid input detected at \u0027^\u00 marker.\n\nXXCT5760#", "errorMessage": "" }
Wenn das angeforderte Gerät nicht über SSHv2 verfügt und Cisco DNA Center versucht, das Gerät mit SSHv2 zu verbinden	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error occured while executing command : show version\r channel closed : Remote party uses incompatible protocol, it is not SSH-2 compatible." }
Wenn der Befehl im Microservice "Erfassung" deaktiviert ist	{ "command": "config paging disable", "status": "Command_Disabled", "commandResponse": "Command collection is disabled", "errorMessage": "" }
Wenn die Command Runner-Aufgabe fehlgeschlagen ist und die Aufgaben-URL nicht von Cisco DNA Center zurückgegeben wird	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s. Task UR empty." }
Wenn die Command Runner-Aufgabe in Cisco DNA Center nicht erstellt werden konnte	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, Request %s. No task details." }
Wenn der Microservice "Erfassung" keine Antwort auf eine Command Runner-Anfrage vom Cisco DNA Center empfängt	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, Request

Wenn Cisco DNA Center die Aufgabe nicht innerhalb der konfigurierten Zeitüberschreitung abschließt (5 Minuten pro Befehl im Microservice "Erfassung")	%s."
	}
	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Operation Timedout. The command runner task failed for
	%s, RequestURL: %s. No progress details."
	}

Wenn die Command Runner-Aufgabe fehlgeschlagen ist und die Datei-ID nicht von Cisco DNA Center übermittelt wird	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, Request
	%s. File id is empty."
	}

Wenn die Command Runner-Aufgabe fehlschlägt und das Datei-ID-Tag nicht von Cisco DNA Center zurückgegeben wird	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, Request
	%s. No file id details."
	}

Wenn das Gerät nicht für die Ausführung durch den Command Runner geeignet ist	{
	"command": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Requested devices are not in inventory,try with other de
	available in inventory"
	}

Wenn der Befehl "runner" für den Benutzer deaktiviert ist	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"Role does not have valid permissions to ac
	the API\"}\n"
	}

Reaktionen auf Diagnosescanfehler

Der Scanfehler und die Ursache können auf eine der aufgeführten Komponenten zurückzuführen sein

Wenn der Benutzer einen Scan vom Portal aus initiiert, führt dies gelegentlich zu folgender Fehlermeldung: "Fehlgeschlagen: Interner Serverfehler."

Die Ursache des Problems kann eine der aufgeführten Komponenten sein

- Kontrollpunkt
- Netzwerk-Datengateway
- Anschluss
- Diagnosescan
- CX Cloud Agent Microservice [Gerätemanager, Erfassung]
- Cisco DNA Center
- APIX
- Mashery
- Ping-Zugriff
- IRONBANK

- IRONBANK GW
- Big Data Broker (BDB)

Protokolle anzeigen:

1. Melden Sie sich bei der CX Cloud Agent-Konsole an.
2. Geben Sie das Kennwort an, um sich über SSH mit den Anmeldeinformationen des Benutzers cxcadmin anzumelden.
3. Durchführung kubectl get pods
4. Rufen Sie den PoD-Namen für Sammlung, Anschluss und Betriebsfähigkeit ab.
5. So überprüfen Sie die Microservice-Protokolle für Erfassung, Anschluss und Wartung

- Durchführung kubectl logs
- Durchführung kubectl logs
- Durchführung kubectl logs

In der hier gezeigten Tabelle wird der Fehlerausschnitt angezeigt, der unter den Protokollen des Collection-Microservice und der Service-Microservice zu finden ist und aufgrund von Problemen/Einschränkungen mit den Komponenten auftritt.

Anwendungsfall	Protokoll-Snippet im Microservice "Erfassung"
Das Gerät kann erreichbar sein und wird unterstützt, aber die Befehle, die auf diesem Gerät ausgeführt werden sollen, werden im Collection-Microservice blockiert.	{ "command": "config paging disable", "status": "Command_Disabled", "commandResponse": "Command collection is disabled", }
Wenn das zu scannende Gerät nicht verfügbar ist. Dazu kommt es, wenn ein Synchronisierungsproblem zwischen den Komponenten auftritt, z. B. zwischen Portal, Diagnosescan, CX-Komponente und Cisco DNA Center.	No device found with id 02eb08be-b13f-4d25-9 eaf4e882f71a
Wenn das zu scannende Gerät ausgelastet ist, wenn dasselbe Gerät Teil eines anderen Auftrags war und keine parallelen Anfragen von Cisco DNA Center für das Gerät verarbeitet werden.	All requested devices are already being queried command runner in another session. Please try devices".
Wenn das Gerät den Scanvorgang nicht unterstützt.	Requested devices are not in inventory, try with devices available in inventory
Wenn das Gerät nicht erreichbar ist	"Error occurred while executing command: sho udi\nError connecting to device [Host: x.x.x.x:2 route to host : No route to host { "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task fa device %s, RequestURL: %s." }
Wenn Cisco DNA Center über den Cloud Agent nicht erreichbar ist oder der Microservice "Erfassung" des Cloud Agent keine Antwort auf eine Command Runner-Anfrage vom Cisco DNA Center erhält.	

Anwendungsfall	Protokoll-Snippet im Microservice "Kontrollpunkt Agent"
	Failed to execute request
Wenn bei der Scananfrage Zeitplandetails fehlen.	{"message":"23502: null value in column \"schedule\" violates no constraint"}
Wenn bei der Scananfrage Gerätedetails fehlen.	Failed to create scan policy. No valid devices in the request

Wenn die Verbindung zwischen CPA und Netzwerkverbindungen unterbrochen ist.	Failed to execute request.
Wenn das angeforderte Gerät in den Diagnosescans nicht zum Scannen verfügbar ist.	Failed to submit the request to scan. Reason = {\"message\":\"D with Hostname=x.x.x.x' was not found\"}

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.