

# CX Cloud Agent - Overzicht v2.2

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Toegang tot kritieke domeinen](#)

[Door Cisco DNA Center ondersteunde versie](#)

[Ondersteunde browsers](#)

[Ondersteunde productlijst](#)

[Gegevensbronnen aansluiten](#)

[CX Cloud Agent instellen](#)

[CX Cloud Agent verbinden met CX Cloud](#)

[Cisco DNA Center als gegevensbron toevoegen](#)

[Toevoeging van andere activa als gegevensbronnen](#)

[Overzicht](#)

[Detectieprotocollen](#)

[Connectiviteitsprotocollen](#)

[Apparaten toevoegen met een zaadbestand](#)

[Beperkingen in telemetrieverwerking voor apparaten](#)

[Apparaten toevoegen met een nieuw zaadbestand](#)

[Apparaten toevoegen met een gewijzigd zaadbestand](#)

[Apparaten toevoegen met IP-bereiken](#)

[IP-bereiken bewerken](#)

[Diagnostische scans voor planning](#)

[Implementatie en netwerkconfiguratie](#)

[OVA-implementatie](#)

[Installatie van ThickClient ESXi 5.5/6.0](#)

[WebClient ESXi 6.0 installeren](#)

[Installatie van WebClient vCenter](#)

[Installatie van Oracle Virtual Box 5.2.30](#)

[Microsoft Hyper-V installatie](#)

[Netwerkconfiguratie](#)

[Alternatieve benadering voor het genereren van paarcode met CLI](#)

[Cisco DNA Center configureren om syslog door te sturen naar CX Cloud Agent](#)

[Voorwaarden](#)

[Voorwaartse instelling van Syslog configureren](#)

[Andere middelen configureren om Syslog door te sturen naar CX Cloud Agent](#)

[Bestaande systeemserver met voorwaartse mogelijkheid](#)

[Bestaande Syslog-server zonder voorwaartse mogelijkheid OF zonder Syslog-server](#)

[Instellingen voor syslogweergave op informatieniveau inschakelen](#)

[Back-up en herstel van de CX Cloud VM](#)

[Back-up](#)

[Terugzetten](#)

[Security](#)

[Fysieke security](#)

[Account security](#)

[Netwerk security](#)

[Verificatie](#)

[Versterking](#)

[Data security](#)

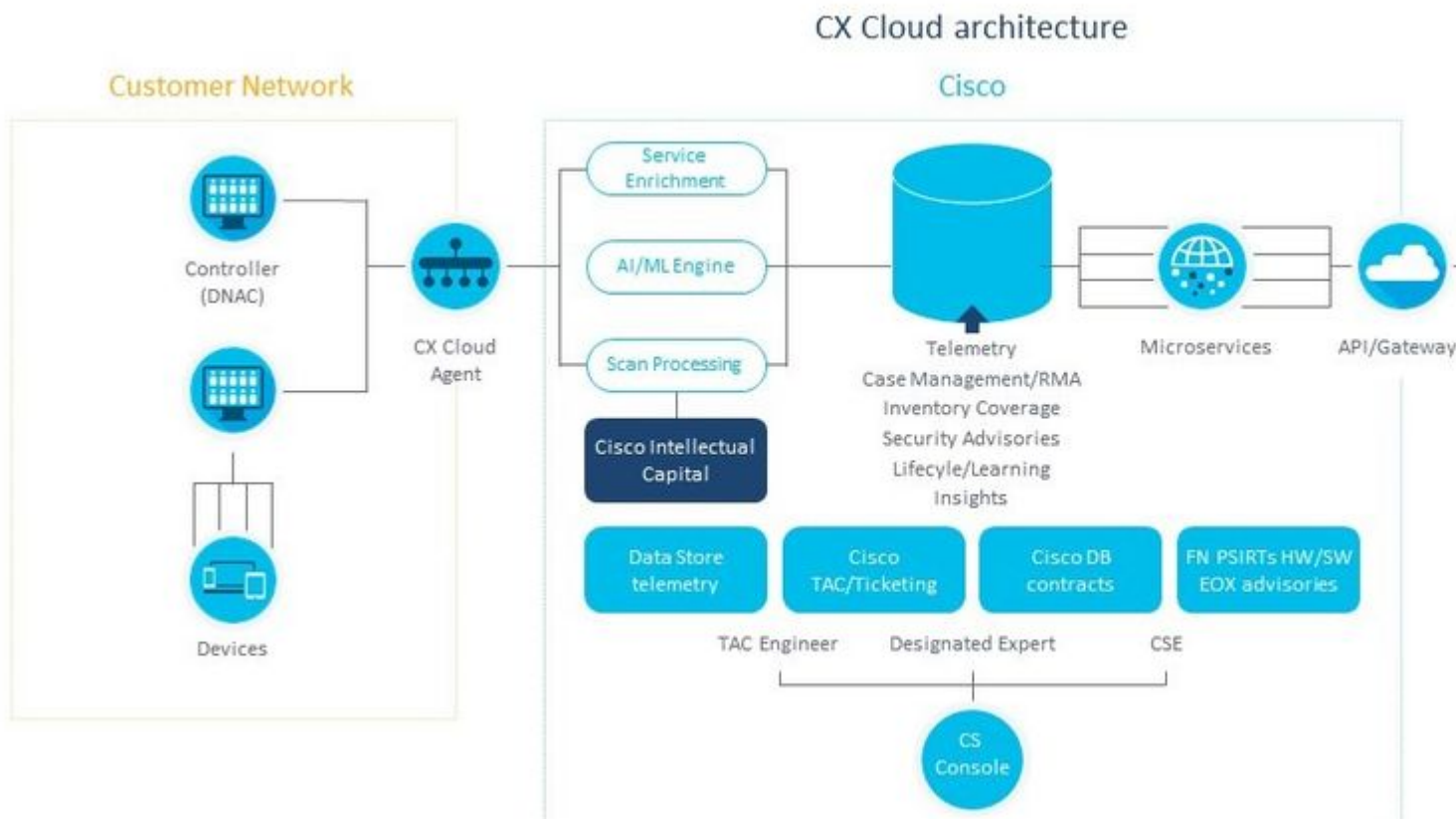
[Gegevensoverdracht](#)

[Logboeken en monitoring](#)  
[Cisco-telemetrieopdrachten](#)  
[Security overzicht](#)

## Inleiding

Dit document beschrijft de Cisco Customer Experience (CX) Cloud Agent. Cisco's (CX) Cloud Agent is een zeer schaalbaar platform dat telemetriegegevens van netwerkapparaten van klanten verzamelt om bruikbare inzichten voor klanten te leveren. CX Cloud Agent maakt de omzetting van Artificial Intelligence (AI)/Machine Learning (ML) van actieve lopende configuratiegegevens in proactieve en voorspellende inzichten weergegeven in CX Cloud mogelijk.

Deze handleiding is specifiek voor CX Cloud Agent v2.2 en verder. Raadpleeg de pagina [Cisco CX Cloud Agent](#) voor toegang tot eerdere versies.



Architectuur van CX Cloud Agent

**Opmerking:** Afbeeldingen (en de inhoud ervan) in deze handleiding zijn alleen voor referentiedoeleinden bestemd. De werkelijke inhoud kan afwijken.

## Voorwaarden

CX Cloud Agent werkt als een Virtual Machine (VM) en kan worden gedownload als een Open Virtual Appliance (OVA) of een virtuele harde schijf (VHD).

Te gebruiken vereisten:

- Een van deze hypervisors:
  - VMware ESXi versie 5.5 of hoger
  - Oracle Virtual Box 5.2.30 of hoger
  - Windows Hypervisor versie 2012 tot 2016
- De hypervisor kan een VM hosten die vereist:
  - CPU met 8 cores
  - 16 GB geheugen/RAM
  - 200 GB schijfruimte
- Voor klanten die aangewezen datacenters in de VS gebruiken als het primaire gegevensgebied om CX Cloud-gegevens op te slaan, moet de CX Cloud Agent verbinding kunnen maken met de hieronder getoonde servers met behulp van de Fully Qualified Domain Name (FQDN) en met behulp van HTTPS op TCP-poort 443:
  - FQDN: agent.us.cisco.cloud
  - FQDN: ng.acs.agent.us.cisco.cloud
  - FQDN: cloudssso.cisco.com
  - FQDN: api-cx.cisco.com
- Voor klanten die aangewezen Europe-datacenters gebruiken als het primaire gegevensgebied om CX

Cloud-gegevens op te slaan: de CX Cloud Agent moet verbinding kunnen maken met beide servers die hier worden getoond, met behulp van de FQDN en met behulp van HTTPS op TCP-poort 443:

- FQDN: agent.us.cisco.cloud
- FQDN: agent.emea.cisco.cloud
- FQDN: ng.acs.agent.emea.cisco.cloud
- FQDN: cloudsso.cisco.com
- FQDN: api-cx.cisco.com
- Voor klanten die aangewezen Asia Pacific-datacenters gebruiken als het primaire gegevensgebied om CX Cloud-gegevens op te slaan: de CX Cloud Agent moet verbinding kunnen maken met beide hier getoonde servers met behulp van de FQDN en met behulp van HTTPS op TCP-poort 443:
  - FQDN: agent.us.cisco.cloud
  - FQDN: agent.apic.cisco.cloud
  - FQDN: ng.acs.agent.apic.cisco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- Voor klanten die aangewezen datacenters in Europa en Azië-Pacific als hun primaire gegevensregio gebruiken, is connectiviteit met FQDN: agent.us.cisco.cloud alleen vereist voor het registreren van de CX Cloud Agent met CX Cloud tijdens de eerste configuratie. Nadat de CX Cloud Agent met succes is geregistreerd bij CX Cloud, is deze verbinding niet langer nodig.
- Voor lokaal beheer van de CX Cloud Agent moet poort 22 toegankelijk zijn.
- De volgende tabel bevat een samenvatting van de poorten en protocollen die moeten worden geopend en ingeschakeld voor een correcte werking van CX Cloud Agent:

<b>CX Cloud Agent Traffic</b>				
Source	Destination		Protocol	Port
	IP Address	Hostname		
<b>Data Collection and Transfer</b>				
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.cisco.cloud DNAC Servers  Additionally, For Americas region, FQDN: ng.acs.agent.us.cisco.cloud For EMEA region, FQDN: agent.emea.cisco.cloud, and FQDN: ng.acs.agent.emea.cisco.cloud For APJC region, FQDN: agent.apjc.cisco.cloud, and FQDN: ng.acs.agent.apjc.cisco.cloud	HTTPS	TCP/ 443
Agent IP		Customer Device	SNMP	UDP/161
Devices		Agent IP	SYSLOG	UDP/514
Agent IP		Customer Device	SSH	TCP/22
Agent IP		Customer Device	Echo	TCP/7
Agent IP		Customer Device	Telnet	TCP/23
<b>Agent Administration Access</b>				
Support VM		Agent IP	SSH	TCP/22

### Andere opmerkingen:

- Een IP wordt automatisch gedetecteerd als het Dynamic Host Configuration Protocol (DHCP) is ingeschakeld in de VM-omgeving; anders moeten een gratis IPv4-adres, subnetmasker, IP-adres met standaardgateway en DNS-serveradres (Domain Name Service) beschikbaar zijn
- Alleen IPv4 wordt ondersteund
- De gecertificeerde single node en High Availability (HA) Cluster Cisco DNA Center-versies zijn 2.1.2.0 tot en met 2.2.3.5, 2.3.3.4 tot en met 2.3.3.6, 2.3.5.0 en de virtuele applicatie Cisco DNA Center

- Als het netwerk SSL-onderschepping heeft, laat u het IP-adres van CX Cloud Agent toe.
- Gebruik alleen de meegeleverde hostnamen; statische IP-adressen mogen niet worden gebruikt

## Toegang tot kritieke domeinen

Om het CX Cloud-traject te starten, hebben gebruikers toegang tot de volgende domeinen nodig. Gebruik alleen de opgegeven hostnamen; gebruik geen statische IP-adressen.

### Specifieke domeinen voor de CX Cloud Agent Portal

Belangrijkste domeinen	Andere domeinen
cisco.com	mixpanel.com
cscs.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

### Voor CX Cloud Agent specifieke domeinen

AMERIKANEN	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.cscs.cloud	agent.us.cscs.cloud	agent.us.cscs.cloud
ng.acs.agent.us.cscs.cloud	agent.emea.cscs.cloud	agent.apjc.cscs.cloud
	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

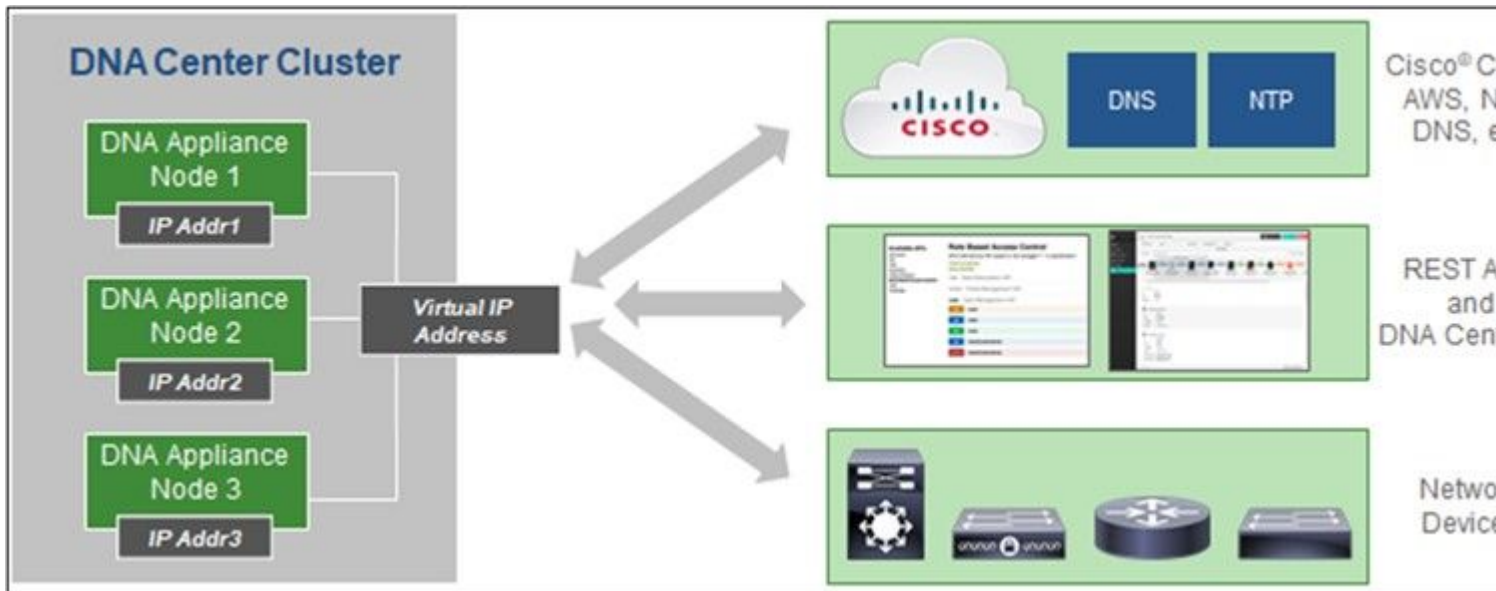
---

**Opmerking:** de uitgaande toegang moet worden toegestaan met omleiding ingeschakeld op poort 443 voor de gespecificeerde FQDN's.

---

## **Door Cisco DNA Center ondersteunde versie**

Ondersteunde single node- en HA Cluster Cisco DNA Center-versies zijn 2.1.2.0 tot 2.2.3.5, 2.3.3.4 tot 2.3.3.6, 2.3.5.0 en virtuele applicatie voor Cisco DNA Center.



Multi-Node HA Cluster Cisco DNA Center

## Ondersteunde browsers

Voor een optimale ervaring op Cisco.com, wordt de meest recente officiële release van deze browsers aanbevolen:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

## Ondersteunde productlijst

Raadpleeg de [lijst met ondersteunde producten](#) voor een overzicht van de producten die door CX Cloud Agent worden ondersteund.

## Gegevensbronnen aansluiten

Gegevensbronnen verbinden:




1. Klik op [ex.cisco.com](#) om in te loggen bij CX Cloud.
2. Selecteer **Campus Network** en navigeer naar de tegel **ASSET & COVERAGE**.

vanuit de banner die wordt weergegeven voordat de gegevensbronnen voor de eerste keer worden ingesteld. Het venster voor het aansluiten van gegevensbronnen wordt geopend. De weergegeven opties kunnen afwijken, afhankelijk van de abonnementen van de klant.



[← Back To Data Sources](#)

Which data source would you like to connect?

	<b>Cisco DNA Center</b> Uses CX Cloud Agent to support Campus Network	<a href="#">Connect</a>
	<b>Intersight</b> Supports Data Center Compute and Cloud Network	<a href="#">Connect</a>
	<b>Other Assets</b> Uses CX Cloud Agent to support Campus Network	<a href="#">Connect</a>

*Gegevensbronnen verbinden*

4. Klik op **Verbinden** om de juiste gegevensbron te selecteren. Als de CX Cloud Agent nog niet eerder is ingesteld, wordt het venster [CX Cloud Agent instellen](#) geopend, waar de installatie moet worden voltooid. Als de configuratie is voltooid, wordt de verbinding voortgezet. Raadpleeg een van de volgende paragrafen om door te gaan:

[CX Cloud Agent instellen](#)

[Cisco DNA Center als gegevensbron toevoegen](#)

[Toevoeging van andere activa als gegevensbronnen](#)

---

**Opmerking:** de optie **Andere bedrijfsmiddelen** is alleen beschikbaar als de verbinding met het directe apparaat niet eerder is geconfigureerd.

---

## CX Cloud Agent instellen

De CX Cloud Agent-instelling wordt gevraagd bij het verbinden van gegevensbronnen als deze nog niet zijn voltooid.

U stelt CX Cloud Agent als volgt in:



# Set Up CX Cloud Agent



## SET UP CX CLOUD AGENT

0%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine



## Add Cloud Agent to your CX Cloud pit crew

CX Cloud Agent gathers telemetry data from the devices on your network, allowing you to take advantage of all the hyper-relevant insights and trusted expertise that CX Cloud has to offer.

## Review deployment requirements

### Prepare your network for CX Cloud Agent

CX Cloud Agent runs as a virtual machine (VM), so you'll need a hypervisor to host it.

Before you download and install the image file, make sure CX Cloud Agent is able to connect to the designated server(s) via HTTPS on port 443 and the IP address:

For **AWS US** data centers:

- **FQDN:** agent.us.cisco.cloud

- **FQDN:** ng.acs.agent.us.cisco.cloud

- **FQDN:** cloudss0.cisco.com

- **FQDN:** api-cx.cisco.com



Review the [CX Cloud Agent Overview](#) for complete hardware and software prerequisites.



CX Cloud takes security seriously. Review the Security section of the [CX Cloud Agent Overview](#) to learn how CX Cloud Agent protects your data.

I set up this configuration on port 443

Continue

*Implementatievereisten bekijken*

1. Controleer de **implementatievereisten voor Review** en selecteer het aanvinkvakje **I Setup this Configuration on port 443**.
2. Klik op Continue (Doorgaan). De CX Cloud Agent instellen - **Het venster voor de sterke coderingsovereenkomst** openen.

# Set Up CX Cloud Agent

## SET UP CX CLOUD AGENT

25%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine



## Accept the strong encryption agreement

Then you can download the image file for the CX Cloud Agent virtual machine.

### Instructions

To apply for eligibility to download strong encryption software images:

1. Ensure the address listed in your [Cisco.com User Profile](#) is correct and complete.
2. Read each of the conditions below carefully prior to selecting your answer.

First Name

Samuel

Last Name

Deckard

Email

tadeckar@cisco.com

Cisco User Id

CXSuperAdmin38333

**Business Division's Function:** \*

Commercial/Civilian entity

Government entity, a Military entity or Defense Contractor

If Government entity, a Military entity or Defense Contractor, Are you in

## Set Up CX Cloud Agent

**SET UP CX CLOUD AGENT**  
50%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine

**Download image file**  
Download the appropriate image file for your virtual machine format.

- OVA**  
For use with VMware vSphere, VMware vCenter, or Oracle VirtualBox  
Cisco-DNA-Center-2021-release-16C.ova
- VHD**  
For use with Microsoft Hyper-V  
Cisco-DNA-Center-2021-release-15A.vhd

**Cisco End User License Agreement**

I accept

Download and Continue

*Image downloaden*

7. Selecteer de juiste bestandsindeling om het afbeeldingsbestand te downloaden dat nodig is voor de installatie.
8. Selecteer het aanvinkvakje **Ik accepteer** om akkoord te gaan met de Gebruiksrechtovereenkomst van Cisco.
9. Klik op **Downloaden en ga verder**. De CX Cloud Agent instellen - **implementeren en koppelen met uw** venster voor **virtuele machines** wordt geopend.
10. Raadpleeg [Netwerkconfiguratie](#) om de koppelcode te verkrijgen die in de volgende sectie is vereist.

### CX Cloud Agent verbinden met CX Cloud

Het verbinden van CX Cloud Agent met CX Cloud is vereist voor telemetrieverzameling om te beginnen zodat informatie in de UI kan worden bijgewerkt om de huidige activa en inzichten weer te geven. Deze sectie verschaft informatie om de richtlijnen voor verbindingen en probleemoplossing te voltooien.

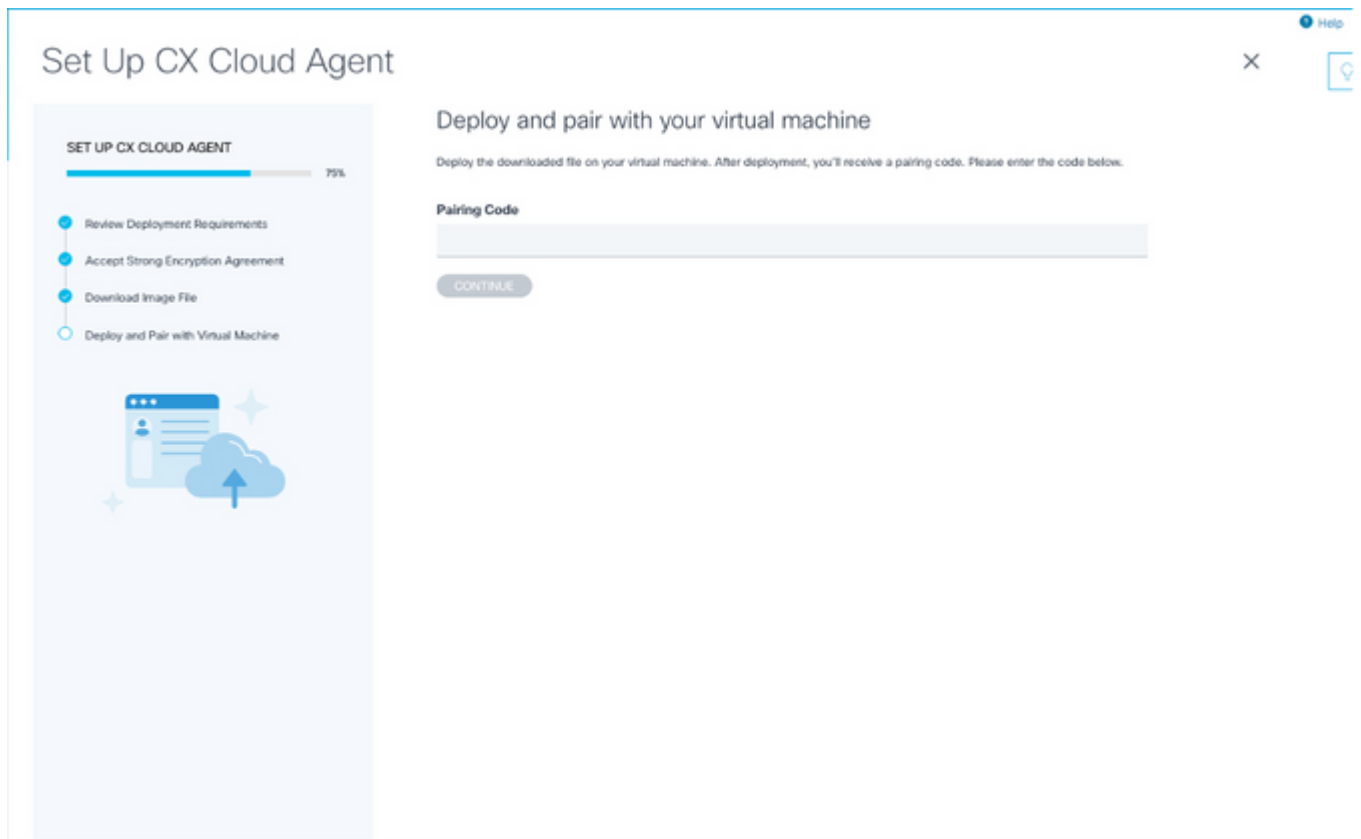
U sluit CX Cloud Agent als volgt aan op CX Cloud:

1. Voer de **paarcode** in die is opgegeven in het console dialoogvenster of de Command Line Interface (CLI) van de virtuele machine die via Agent is verbonden.

---

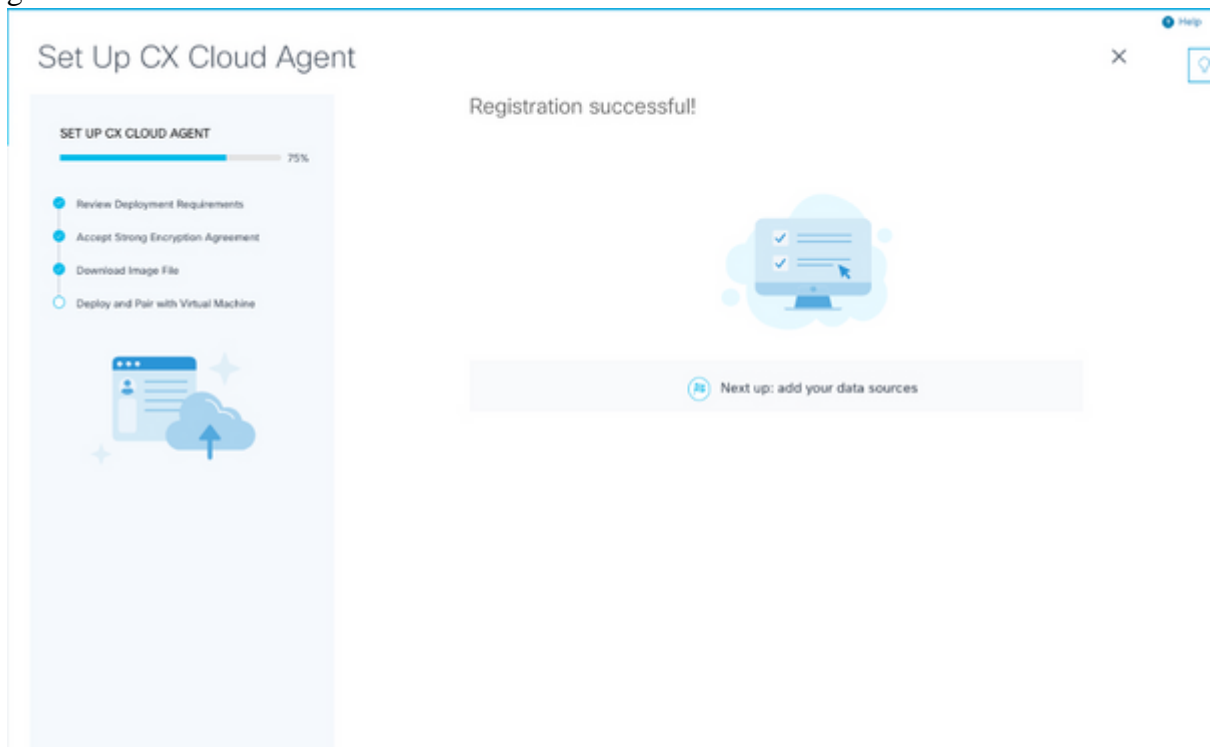
**Opmerking:** de koppelingcode wordt ontvangen na het inzetten van het gedownloadde OVA-bestand.

---



*Koppelingscode*

2. Klik op **Doorgaan** om de CX Cloud Agent te registreren. Het venster **CX Cloud Agent instellen - Registratie geslaagd** wordt kort geopend voordat u automatisch naar de pagina **Add Data Sources** gaat.



*Registratie geslaagd*

## Cisco DNA Center als gegevensbron toevoegen

Wanneer **Cisco DNA Center** is geselecteerd in het venster voor de verbinding met gegevensbronnen (raadpleeg de afbeelding **Gegevensbronnen verbinden** in de sectie Gegevensbronnen verbinden), wordt het volgende venster geopend:

[← Back To Data Sources](#)

## Connect to CX Cloud

### Connect a Cisco DNA Center

IP Address or FQDN

City

Username

Password

### Schedule inventory collection

Frequency

Time

IST

 Run the first collection now (this may take up to 75 minutes)

Connect met CX Cloud

U kunt als volgt Cisco DNA Center als gegevensbron toevoegen:

1. Voer het IP-adres van Cisco DNA Center of het virtuele **IP-adres of FQDN**, **stad** (locatie van Cisco DNA Center), **gebruikersnaam** en **wachtwoord in**.

---

**Opmerking:** gebruik geen afzonderlijke IP-clusterknooppunten.

---

2. Plan een inventarisverzameling door een **frequentie en tijd in** te voeren om aan te geven hoe vaak de CX Cloud Agent netwerkscans moet uitvoeren en informatie over verbonden apparaten moet bijwerken.

---

**Opmerking:** de eerste inventarisatie kan 75 minuten duren.

---

3. Klik op **Verbinden**. Er wordt een bevestiging weergegeven met het IP-adres van Cisco DNA Center.

[← Back To Data Sources](#)

Help

×



## Connect to CX Cloud

Connected



Cisco DNA Center 10.122.58.165  
Inventory collection runs every day At 03:00 AM IST  
First collection will run immediately after data sources are added

---

U kunt het zaadbestand of het IP-bereik gebruiken. Het is niet mogelijk deze selectie na de eerste configuratie te wijzigen. Terwijl de zaadbestanden op elk moment na de eerste configuratie kunnen worden geüpload, kan het IP-bereik van het apparaat na de configuratie niet worden aangepast, gewijzigd, gecorrigeerd of gewijzigd. Gebruikersnamen en wachtwoorden die aan SNMP en/of SSH en/of Telnet zijn gekoppeld, kunnen niet worden gewijzigd.

---

Wanneer **Andere activa** worden geselecteerd in het venster voor de verbinding met gegevensbronnen, wordt het volgende venster geopend:



## Connect to CX Cloud

How would you like to connect these assets?

Upload a seed file (recommended)

Add your devices to a [Seed File Template](#). You can reupload this file later if you need to make changes.

Provide an IP Address range

Select any connection method(s). At least one SNMP and SSH are required.

SNMP v3

SNMP v2c

SSH v2

[More](#)

These options support legacy products

SSH v1

Telnet

[Continue](#)



### Verbinding met CX Cloud configureren

Andere activa als gegevensbronnen toevoegen:

- Upload een zaadbestand met een zaadbestandssjabloon.
- Een IP-adresbereik opgeven

## Detectieprotocollen

Zowel de zaadbestandgebaseerde directe apparaatdetectie als de op IP-bereik gebaseerde detectie vertrouwen op SNMP als het detectieprotocol. Er bestaan verschillende versies van SNMP, maar CX Cloud Agent ondersteunt SNMPV2c en SNMP V3 en een van beide of beide versies kunnen worden geconfigureerd. De gebruiker moet dezelfde informatie, die hieronder in detail wordt beschreven, verstrekken om de configuratie te voltooien en de verbinding tussen het door SNMP beheerde apparaat en de SNMP-servicemanager mogelijk te maken.

SNMPV2c en SNMPV3 verschillen op het gebied van beveiliging en configuratie op afstand. SNMPV3 maakt gebruik van een verbeterd cryptografisch beveiligingssysteem dat SHA-encryptie ondersteunt om berichten te verifiëren en hun privacy te garanderen. Het wordt aanbevolen om SNMPv3 te gebruiken op alle openbare en internet-gerichte netwerken om te beschermen tegen beveiligingsrisico's en bedreigingen. Voor CX Cloud heeft het de voorkeur dat SNMPv3 wordt geconfigureerd en niet SNMPv2c, behalve voor oudere oudere oudere apparaten die geen ingebouwde ondersteuning voor SNMPv3 hebben. Als beide versies van SNMP door de gebruiker zijn geconfigureerd, zal CX Cloud Agent standaard proberen met elk apparaat te communiceren via SNMPv3 en terugkeren naar SNMPv2c als de communicatie niet met succes kan worden onderhandeld.

## Connectiviteitsprotocollen

Als deel van de directe configuratie van de apparaatconnectiviteit moeten gebruikers de details van het protocol voor de apparaatconnectiviteit specificeren: SSH (of, als alternatief, telnet). Er moet gebruik worden gemaakt van SSHv2, behalve in het geval van individuele activa die niet over de juiste ingebouwde ondersteuning beschikken. Houd in acht dat het SSHv1-protocol fundamentele kwetsbaarheden bevat. Door deze kwetsbaarheden kan het ontbreken van extra beveiliging, telemetriegegevens en de onderliggende

activa in het gedrang komen als op SSHv1 wordt vertrouwd. Telnet is ook onveilig. Credentiële informatie (gebruikersnamen en wachtwoorden) die via telnet is verzonden, is niet versleuteld en is daardoor kwetsbaar voor compromittering, afwezigheid van extra beveiliging.

## Apparaten toevoegen met een zaadbestand

### Over zaadbestand

Een seed-bestand is een csv-bestand (komma-gescheiden waarden) waarin elke regel een systeemgegevensrecord vertegenwoordigt. In een zaadbestand komt elke zaadbestandopname overeen met een uniek apparaat waaruit telemetrie moet worden verzameld door CX Cloud Agent. Alle fout- of informatieberichten voor elk apparaat dat wordt geïmporteerd uit het zaadbestand worden opgenomen als onderdeel van de loggegevens van het taakvenster. Alle apparaten in een zaadbestand worden beschouwd als beheerde apparaten, zelfs als de apparaten onbereikbaar zijn op het moment van de eerste configuratie. In het geval dat een nieuw zaadbestand wordt geüpload om een vorige te vervangen, wordt de datum van de laatste upload weergegeven in CX Cloud.

CX Cloud Agent zal proberen verbinding te maken met de apparaten, maar is mogelijk niet in staat om elke te tonen in de Assets-pagina's wanneer het niet in staat is om de PID's of serienummers te bepalen. Elke rij in het beginbestand die begint met een puntkomma wordt genegeerd. De veldnamenrij in het zaadbestand begint met een puntkomma en kan worden bewaard zoals is (aanbevolen optie) of verwijderd tijdens het maken van het klantzaadbestand.

Het is belangrijk dat het formaat van het monsterzaadbestand, inclusief de kolomkoppen, op geen enkele manier wordt gewijzigd. Klik op de koppeling die wordt geleverd om een zaadbestand in PDF-indeling te bekijken. Dit PDF-document is alleen ter referentie en kan worden gebruikt om een zaadbestand te maken dat in .csv-indeling moet worden opgeslagen.

Klik op deze [koppeling](#) om een zaadbestand te bekijken dat kan worden gebruikt om een zaadbestand in .csv-indeling te maken.

---

**N.B.:** Dit PDF-document is alleen ter referentie en kan worden gebruikt om een zaadbestand te maken dat in .csv-indeling moet worden opgeslagen.

---

In de volgende tabel worden alle benodigde kolommen van het zaadbestand geïdentificeerd, evenals de gegevens die in elke kolom moeten worden opgenomen.

kolom startbestand	Kop kolom / identificatie	Doel van de kolom
A	IP-adres of hostnaam	Geef een geldig, uniek IP-adres of hostnaam van het apparaat op.
B	SNMP-protocolversie	Het SNMP-protocol is <b>vereist</b> door CX Cloud Agent en wordt gebruikt voor apparaatdetectie in het klantnetwerk. De waarden kunnen snmpv2c of snmpv3 zijn, maar snmpv3 wordt aanbevolen om veiligheidsredenen.



kolom startbestand	Kop kolom / identificatie	Doel van de kolom
C	snmpRo: Verplicht indien col#=3 geselecteerd als 'snmpv2c'	Als de legacy variant van SNMPv2 is geselecteerd voor een specifiek apparaat, dan moeten SNMPRO (alleen lezen) referenties voor de SNMP-verzameling van het apparaat worden gespecificeerd. Anders kan dit leeg zijn.
D	snmpv3UserName: Verplicht indien col#=3 geselecteerd als 'snmpv3'	Als SNMPv3 is geselecteerd om te communiceren met een specifiek apparaat, moet de respectievelijke login gebruikersnaam worden opgegeven.
E	snmpv3AuthAlgorithm: de waarden kunnen MD5 of SHA zijn	SNMPv3-protocol maakt verificatie mogelijk via de MD5 of SHA-algoritme. Als het apparaat is geconfigureerd met beveiligde verificatie, moet het bijbehorende algoritme worden opgegeven. <b>Opmerking:</b> MD5 wordt als onveilig beschouwd en SHA moet worden gebruikt op alle apparaten die deze ondersteunen.
F	snmpv3AuthPassword: wachtwoord	Als op het apparaat een MD5- of SHA-cryptografisch algoritme is geconfigureerd, moet het relevante verificatiewachtwoord worden ingevoerd voor de toegang tot het apparaat.
G	snmpv3PrivAlgorithm: de waarden kunnen worden ingesteld op DES, 3DES	Als het apparaat is geconfigureerd met het SNMPv3-privacy-algoritme (dit algoritme wordt gebruikt om de respons te versleutelen), dan moet het betreffende algoritme worden geleverd. <b>Opmerking:</b> 56-bits sleutels die door DES worden gebruikt, worden als te kort beschouwd om cryptografische beveiliging te bieden en dat 3DES moet worden gebruikt op alle apparaten die het ondersteunen.
H	snmpv3PrivPassword: wachtwoord	Als het SNMPv3 privacy algoritme is geconfigureerd op het apparaat, dan moet het bijbehorende privacy wachtwoord worden voorzien voor de verbinding met het apparaat.
I	snmpv3EngineID: engineID, unieke ID die apparaat vertegenwoordigt, specificeer motor-ID indien handmatig	De SNMPv3 EngineID is een unieke ID die elk apparaat weergeeft. Deze engine-ID wordt als referentie verzonden tijdens het verzamelen van de SNMP-datasets door CX Cloud Agent. Als de

kolom startbestand	Kop kolom / identificatie	Doel van de kolom
	ingesteld op apparaat	klant de EngineID handmatig configureert, moet de betreffende EngineID worden geleverd.
J	cliProtocol: de waarden kunnen 'telnet', 'sshv1', 'sshv2' zijn. Indien leeg staat standaard ingesteld op 'sshv2'	De CLI is bedoeld om rechtstreeks met het apparaat te communiceren. CX Cloud Agent gebruikt dit protocol voor CLI-verzameling voor een specifiek apparaat. Deze CLI-gegevensverzameling wordt gebruikt voor Asset and Other Insights Reporting binnen CX Cloud. SSHv2 wordt aanbevolen; als er geen andere netwerkbeveiligingsmaatregelen zijn, bieden de SSHv1- en Telnet-protocollen op zichzelf geen adequate transportbeveiliging.
K	cliPort: CLI-protocolpoortnummer	Als een CLI-protocol wordt geselecteerd, moet het bijbehorende poortnummer worden opgegeven. Bijvoorbeeld 22 voor SSH en 23 voor telnet.
L	cliUser: CLI-gebruikersnaam (ofwel CLI-gebruikersnaam/wachtwoord of BEIDE kunnen worden opgegeven, MAAR beide kolommen (col#=12 en col#=13) kunnen niet leeg zijn.)	De respectieve CLI-gebruikersnaam van het apparaat moet worden opgegeven. Dit wordt gebruikt door CX Cloud Agent op het moment van verbinding met het apparaat tijdens CLI-verzameling.
M	cliPassword: CLI-gebruikerswachtwoord (ofwel CLI-gebruikersnaam/wachtwoord of BEIDE kunnen worden opgegeven, MAAR beide kolommen (col#=12 en col#=13) kunnen niet leeg zijn.)	Het respectieve CLI-wachtwoord van het apparaat moet worden opgegeven. Dit wordt gebruikt door CX Cloud Agent op het moment van verbinding met het apparaat tijdens CLI-verzameling.
N	client-gebruiker inschakelen	Als "Enable" is geconfigureerd op het apparaat, moet de EnableUser-waarde van het apparaat worden opgegeven.
O	Wachtwoord inschakelen	Als "Enable" is geconfigureerd op het apparaat, moet de waarde van enablePassword van het apparaat worden geleverd.

<b>kolom startbestand</b>	<b>Kop kolom / identificatie</b>	<b>Doel van de kolom</b>
P	Toekomstige ondersteuning (geen ingangen vereist)	Gereserveerd voor toekomstig gebruik
Q	Toekomstige ondersteuning (geen ingangen vereist)	Gereserveerd voor toekomstig gebruik
R	Toekomstige ondersteuning (geen ingangen vereist)	Gereserveerd voor toekomstig gebruik
S	Toekomstige ondersteuning (geen ingangen vereist)	Gereserveerd voor toekomstig gebruik

### **Beperkingen in telemetrieverwerking voor apparaten**

Bij de verwerking van telemetriegegevens voor apparatuur gelden de volgende beperkingen:

- Sommige apparaten worden weergegeven als bereikbaar in de **Samenvatting** van de **verzameling** maar zijn niet zichtbaar op de pagina **CX Cloud Assets**. Beperkingen van de instrumentatie van de voorziening verhinderen de verwerking van dergelijke apparatentelemetrie.
- Telemetriekenmerken kunnen onjuist zijn of ontbreken in de **CX Cloud Assets** pagina voor apparaten die geen deel uitmaken van de Campus Success Track.
- Als een apparaat uit de verzameling van het zaadbestand of het IP-bereik ook deel uitmaakt van de inventaris van Cisco DNA Center, wordt het apparaat slechts één keer gerapporteerd voor de vermelding Cisco DNA Center. Het beginbestand/IP-bereik wordt niet verzameld of verwerkt om duplicatie te voorkomen.

### **Apparaten toevoegen met een nieuw zaadbestand**

U kunt als volgt apparaten toevoegen met een nieuw zaadbestand:

1. Download de sjabloon voor het zaadbestand (PDF) met behulp van de ingesloten link in dit document (raadpleeg **Info over het zaadbestand**) of via een link in het venster **Verbinding configureren voor CX Cloud**.

---

**Opmerking:** de link in het venster **Configure Connection to CX Cloud** is niet meer beschikbaar nadat het eerste seadbestand is gedownload.

---

## Configure connection to CX Cloud

Upload your seed file ×

Download the [seed file template](#) and add your device info. Then attach the file below.

Drag and Drop files or [browse files](#)

Supports CSV files only. Max file size 5 MB.

Collection Frequency:  Time:  VET

Run the first collection now (this may take up to 75 minutes)

[Connect This Data Source](#)

*Verbinding met CX Cloud-venster configureren*

2. Open een Excel-spreadsheet (of een gewenste spreadsheet) en voer de koppen in zoals in de sjabloon.
3. Voer gegevens handmatig in of importeer gegevens in het bestand.
4. Sla de sjabloon na voltooiing op als een .csv-bestand om het bestand te importeren in CX Cloud Agent.

## Configure connection to CX Cloud

Upload your seed file ×

You've reached your file limit.  
To upload a new file, please remove an existing file.

nextgen\_seedfile.csv Completed. [Delete](#)

---

Schedule Inventory Collection

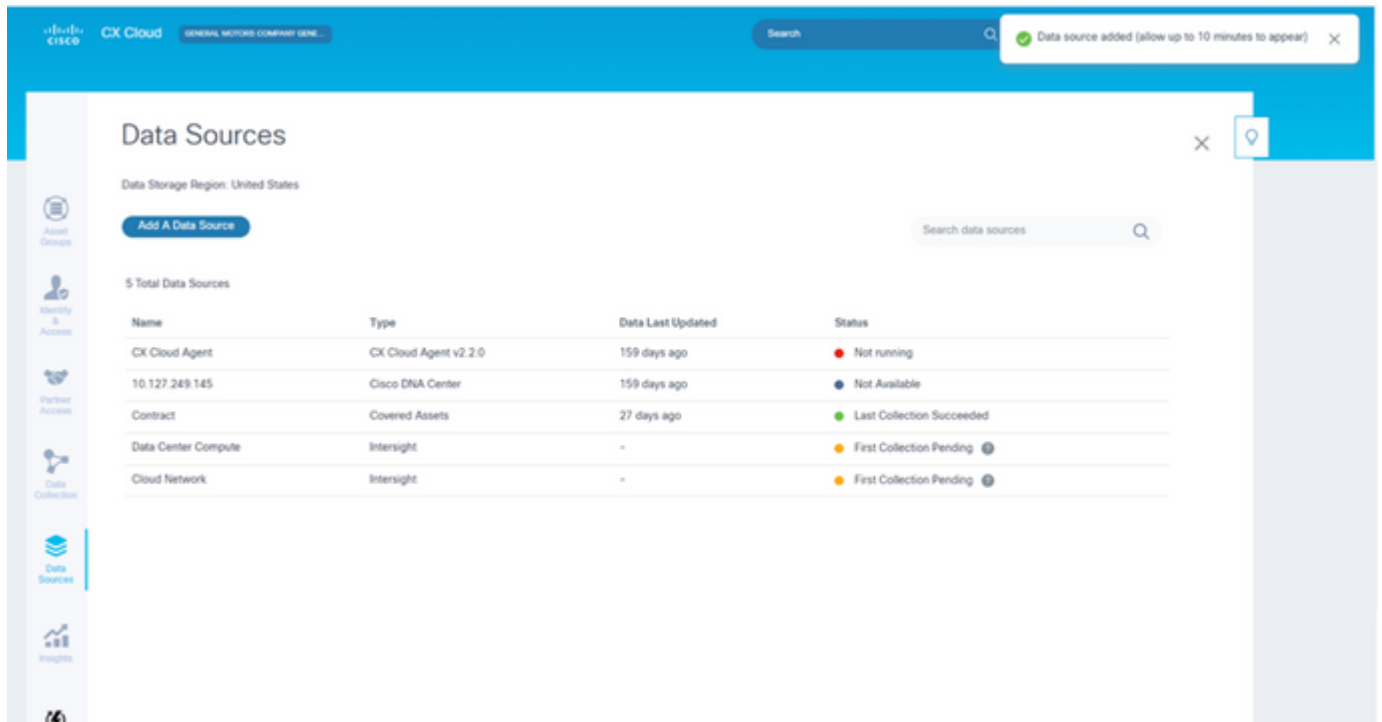
Collection Frequency:  Time:  VET  Day:

Run the first collection now (this may take up to 75 minutes)

[Connect](#)

*Venster zaadbestand uploaden*

5. Sleep in het venster **Zaadbestand uploaden** het nieuwe .csv-bestand of klik op **Bladeren** bestanden en navigeer naar het .csv-bestand.
6. Vul het gedeelte **Schedule Inventory Collection in** en klik op **Connect**. Het venster **Gegevensbronnen** wordt geopend en geeft een bevestigingsbericht weer.
7. Voordat de eerste configuratie van CX Cloud is voltooid, moet CX Cloud Agent de eerste telemetrieverzameling uitvoeren door het zaadbestand te verwerken en verbinding te maken met alle geïdentificeerde apparaten. De inzameling kan op bestelling worden geïnitieerd of volgens een hier bepaald programma lopen. De gebruikers kunnen de eerste telemetrieverbinding uitvoeren door het vakje **Run de eerste inzameling nu** te selecteren. Afhankelijk van het aantal meldingen dat in het zaadbestand is opgegeven en andere factoren, kan dit proces een aanzienlijke hoeveelheid tijd in beslag nemen.



Bevestigingsbericht

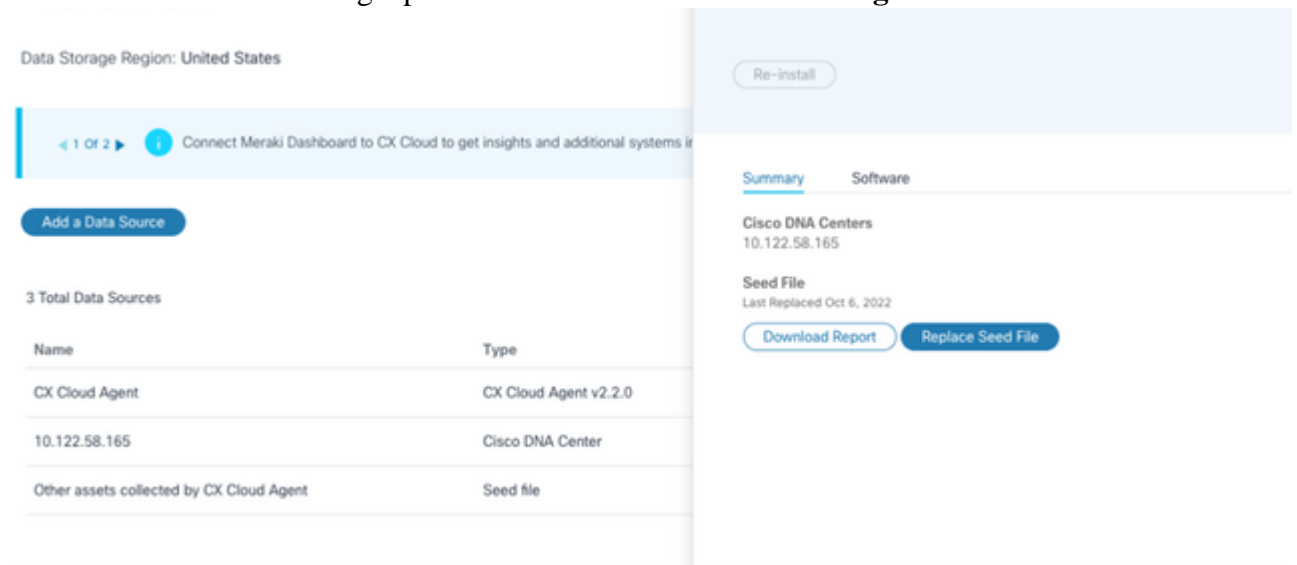
## Apparaten toevoegen met een gewijzigd zaadbestand

U kunt apparaten als volgt toevoegen, wijzigen of verwijderen met het huidige zaadbestand:

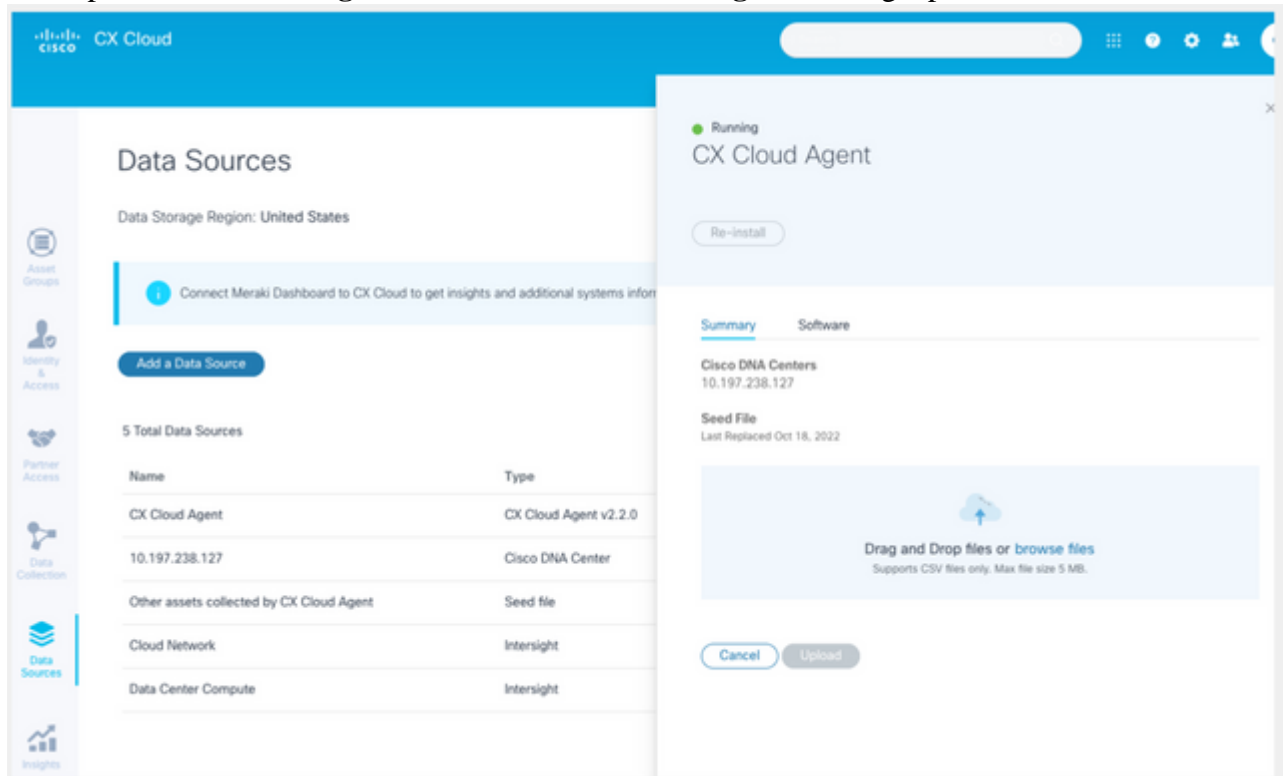
1. Open het eerder gemaakte zaadbestand, breng de gewenste wijzigingen aan en sla het bestand op.

**Opmerking:** als u activa aan het zaadbestand wilt toevoegen, voegt u deze activa toe aan het eerder gemaakte zaadbestand en laadt u het bestand opnieuw. Dit is nodig omdat het uploaden van een nieuw beginbestand het huidige beginbestand vervangt. Alleen het laatste geüploade startbestand wordt gebruikt voor detectie en verzameling.

2. Selecteer op de pagina **Gegevensbronnen** een gegevensbron met een **type** CX Cloud Agent. Er wordt een venster met informatie geopend met de tabbladen **Samenvatting** en **Software**.



3. Klik op **Rapport downloaden** om een rapport te genereren over alle bedrijfsmiddelen voor de geselecteerde gegevensbron. Het rapport bevat informatie over het IP-adres, het serienummer, de bereikbaarheid, het opdrachttype, de opdrachtstatus en de opdrachtfout, indien van toepassing.
4. Klik op **Seed File vervangen**. Het **venster CX Cloud Agent** wordt geopend.



CX Cloud Agent-venster

5. Sleep het gewijzigde zaadbestand naar het venster of blader naar het bestand en voeg het toe in het venster.
6. Klik op **Upload**.

## Apparaten toevoegen met IP-bereiken

IP-bereiken stellen gebruikers in staat om hardware-elementen te identificeren en vervolgens telemetrie te verzamelen van die apparaten op basis van IP-adressen. De apparaten voor telemetrieverzameling kunnen op unieke wijze worden geïdentificeerd door één IP-bereik op netwerkniveau te specificeren, dat met behulp van het SNMP-protocol moet worden gescand door CX Cloud Agent. Als het IP-bereik wordt gekozen om een direct aangesloten apparaat te identificeren, moeten de IP-adressen waarnaar wordt verwezen zo restrictief mogelijk zijn, terwijl dekking voor alle vereiste activa wordt toegestaan.

- Er kunnen specifieke IP's worden geleverd of jokertekens kunnen worden gebruikt om octetten van een IP te vervangen om een bereik te maken
- Als een specifiek IP-adres niet is opgenomen in het IP-bereik dat tijdens de installatie is geïdentificeerd, probeert CX Cloud Agent niet te communiceren met een apparaat met een dergelijk IP-adres en verzamelt het geen telemetrie van een dergelijk apparaat
- Door \*.\*.\* in te voeren, kan CX Cloud Agent de door de gebruiker opgegeven referenties gebruiken bij elke IP. Bijvoorbeeld: 172.16.\*.\* maakt het mogelijk de referenties te gebruiken voor alle apparaten in het 172.16.0.0/16-subnetnummer
- Als er wijzigingen zijn in het netwerk of de geïnstalleerde base (IB), kan het IP-bereik worden gewijzigd. Raadpleeg het gedeelte [IP-bereiken bewerken](#)

CX Cloud Agent zal proberen verbinding te maken met de apparaten, maar kan mogelijk niet elk apparaat verwerken dat wordt weergegeven in de weergave **Assets** wanneer de PID's of serienummers niet kunnen worden bepaald.

---

**Opmerkingen:**

Het specificeren van een IP bereik garandeert niet dat alle apparaten in het bereik zijn opgenomen in de telemetrieverzameling; apparaat bereikbaarheid is gevalideerd op het moment van verbinding en telemetrieverbinding. In CX Cloud worden alleen gegevens weergegeven van een compatibele apparaatklasse die zijn gelicentieerd voor het juiste niveau van Success Tracks.

Als er na de eerste configuratie nieuwe apparaten worden toegevoegd aan het gespecificeerde IP-bereik, zullen die apparaten geen telemetrie rapporteren aan CX Cloud.

---

## Connect to CX Cloud

### Provide IP address range ×

#### Enter IP address range

Starting IP Address \*

198.168.1.10

Ending IP Address \*

198.168.1.20

#### Enter SNMP v2c credentials

Read Community \*

#### Enter SSHv2 credentials

Username \*

Enable Username (Optional)

#### Schedule inventory collection

Frequency

Frequency

Time

Time

IST

Run the first collection now (this may take up to 75 minutes)

Connect

### Eerste IP-adresvenster

Het toevoegen van apparaten met een IP-bereik vereist dat gebruikers alle toepasselijke referenties via de configuratie-gebruikersinterface specificeren. De weergegeven velden zijn afhankelijk van de protocollen die in de vorige vensters zijn geselecteerd. Als er meerdere selecties zijn gemaakt voor hetzelfde protocol, bijvoorbeeld door SNMPv2c en SNMPv3 te selecteren of zowel SSHv2 als SSHv1 te selecteren, onderhandelt CX Cloud Agent automatisch over de protocolselectie op basis van de mogelijkheden van de afzonderlijke apparaten.

Wanneer u apparaten met IP-adressen aansluit, dient de klant ervoor te zorgen dat alle relevante protocollen in het IP-bereik, samen met SSH-versies en Telnet-referenties geldig zijn of dat de verbindingen niet werken.

U kunt als volgt apparaten toevoegen met het IP-bereik:

1. Selecteer in het venster **Verbinding met CX Cloud configureren** de optie **Een IP-adresbereik opgeven**.



## Configure connection to CX Cloud

**Provide IP address range** ×

**Enter IP address range**

Starting IP Address \*

Ending IP Address \*

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

*Voeg apparaten toe met behulp van IP-adressen formulier*

2. Vul het formulier in met de relevante informatie.
3. U kunt meerdere verbindingsopties selecteren. De volgende schermen geven de configuratiereferenties voor de opties weer. Raadpleeg [Over het startbestand](#) voor een beschrijving van de aanmeldingsvelden voor elke verbindingsoptie.

## Configure connection to CX Cloud

**Provide IP address range** ×

**Enter IP address range**

Starting IP Address \*

Ending IP Address \*

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

*SNMP v3-referenties*

Enter SNMP v2c credentials

Read Community \*

Enter SSHV2 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

Enter SSHV1 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

*SNMP v2, SSHV2 en SSHV1 referenties*

### Enter Telnet credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

### Schedule Inventory Collection

Collection Frequency

Time

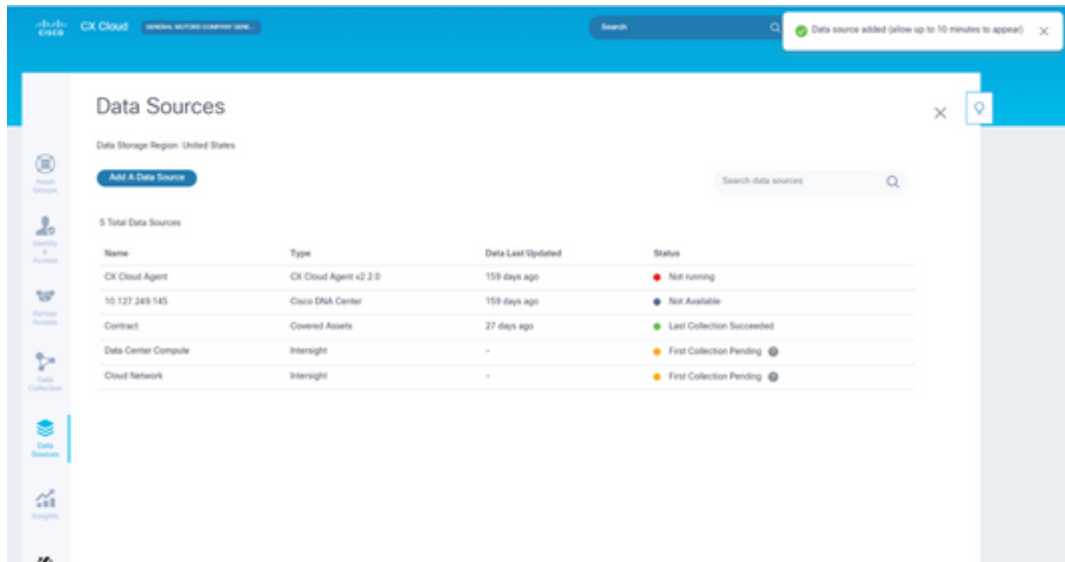
IST

Run the first collection now (this may take up to 75 minutes)

Connect

*Telnet-referenties en netwerkscanschema's*

4. Klik op **Verbinden**. Het venster **Gegevensbronnen** wordt geopend en geeft een bevestigingsbericht weer.

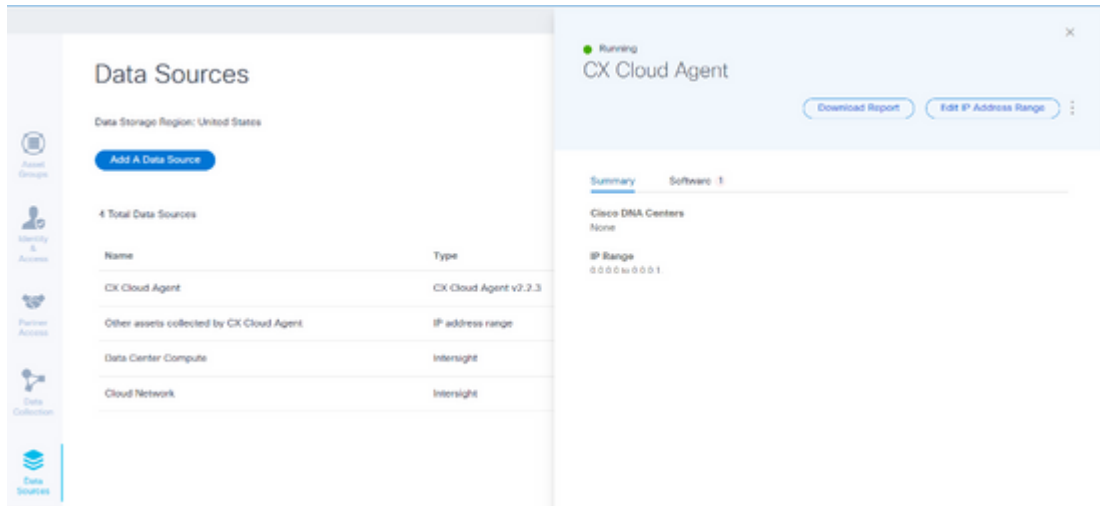


*Bevestiging*

## IP-bereiken bewerken

Om een IP-bereik te bewerken;

1. Navigeer naar het venster **Gegevensbronnen**.



*Databronnen*

2. Klik op de CX Cloud Agent waarvoor IP-bereik moet worden bewerkt in **gegevensbronnen**. Het venster met informatie wordt geopend.
3. Klik op **IP-adresbereik bewerken**. Het venster **Connect to CX Cloud** wordt geopend.

[< Back To Data Sources](#)

### Connect to CX Cloud

Provide an IP address range

[Edit The Protocols](#)

Enter IP address range

Starting IP address \*

0.0.0.0

Ending IP address \*

0.0.0.1

Cancel

Continue

*Een IP-bereik bieden*

4. Werk de nieuwe IP's bij in de velden **Eerste IP-adres** en **Laatste IP-adres**.
5. Klik op de koppeling **Protocollen bewerken**. Het venster **Connect to CX Cloud - Selecteer een protocolvenster** wordt geopend.

## Connect to CX Cloud

### Select a protocol

At least one discovery and collection method are required.

#### Discovery options

- SNMP v3 (recommended)
- SNMP v2c

#### Collection options

- SSH v2 (recommended)
- SSH v1
- Telnet

Cancel

Continue

*Een protocol selecteren*

6. Selecteer de betreffende protocollen door op de juiste selectievakjes te klikken.
7. Klik op **Continue** (Doorgaan). Het venster **IP-adresbereik** bieden wordt geopend.

## Provide an IP address range

[Edit The Protocols](#)

### Enter IP address range

Starting IP address \*

0.0.0.0

Ending IP address \*

0.0.0.2

### Enter SNMP v2c credentials

Read community \*

\_\_\_\_\_

### Enter SSH v1 credentials

Username \*

Enable Username (Optional)

\_\_\_\_\_

Password \*

Enable Password (Optional)

\_\_\_\_\_

Cancel

Connect

*Credentials wachtwoord invoeren*

8. Voer configuratiegegevens in.
9. Klik op **Verbinden**. Het venster **Gegevensbronnen** wordt geopend en geeft een bevestigingsbericht weer.

The screenshot shows the Cisco CX Cloud interface. At the top, there is a blue header with the Cisco logo, 'CX Cloud', and 'PROVIDED UNITED STATES'. A search bar is visible. A notification banner at the top right says 'IP address range updated' with a green checkmark and a close button. The main content area is titled 'Data Sources' and includes a sub-header 'Data Storage Region: United States'. There is a button 'Add A Data Source' and a search bar 'Search data sources'. Below this, it says '4 Total Data Sources'. A table lists the data sources:

Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.2.3	3 minutes ago	Running
Other assets collected by CX Cloud Agent	IP address range	3 minutes ago	1 unreachable
Data Center Compute	Intersight	-	First Collection Pending
Cloud Network	Intersight	-	First Collection Pending

*Bevestiging*

**Opmerking:** het bevestigingsbericht zorgt er niet voor dat de apparaten in het bewerkte bereik bereikbaar zijn en dat de referenties zijn geaccepteerd.

## Informatie over apparaten die worden ontdekt door meerdere controllers

Het is mogelijk dat bepaalde apparaten kunnen worden ontdekt door zowel het Cisco DNA Center als de directe apparaatverbinding met CX Cloud Agent waardoor dubbele gegevens worden verzameld van die apparaten. Om te voorkomen dat dubbele gegevens worden verzameld en dat de apparaten worden beheerd door slechts één controller, moet een prioriteit worden vastgesteld waarvoor CX Cloud Agent de apparaten beheert.

- Als een apparaat eerst wordt ontdekt door Cisco DNA Center en vervolgens wordt herontdekt door een directe apparaatverbinding (met behulp van een zaadbestand of een IP-bereik), heeft Cisco DNA Center voorrang bij het besturen van het apparaat.
- Als een apparaat eerst wordt ontdekt door een directe apparaatverbinding met CX Cloud Agent en vervolgens wordt herontdekt door Cisco DNA Center, krijgt Cisco DNA Center voorrang bij het besturen van het apparaat.

## Diagnostische scans voor planning

Diagnostische scans plannen:

1. Klik op de **Homepagina** op het pictogram **Instellingen** (tandwiel).
2. Selecteer op de pagina **Gegevensbronnen** de optie **Gegevensverzameling** in het linkerdeelvenster.
3. Klik op **Scannen plannen**.

### Data Collection

Diagnostic Scans ⓘ Schedule Scan

< October 2022 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

No Diagnostic Scans Found

Inventory Collection ⓘ  
3 Collections

Source	Schedule	
Other assets collected by CX Cloud Agent	Monthly on the 30th at 05:30 PM EDT	⋮
10.197.238.127	Monthly on the 30th at 05:00 PM EDT	⋮
22.1.90.1	Monthly on the 30th at 09:00 PM EDT	⋮

Rapid Problem Resolution  
Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.

Enable for Campus Network

### Gegevensverzameling

4. Configureer een schema voor deze scan.

## Other assets collected by CX Cloud Agent Inventory Collection Details

### Schedule History

Weekly

on

Sunday

at

12:00 am

EDT

Created: Oct 3, 2022

Save Scheduled Collection

Scanschema configureren

5. Selecteer in de lijst met apparaten alle apparaten voor de scan en klik op **Toevoegen**.

### New Scheduled Scan

#### Data Sources

Other assets collected by CX Cloud Agent

#### Schedule

Frequency

at

Time

IST

Save Changes

#### Description (Optional)

<input type="checkbox"/>	Device	Source IP	IP Address
<input type="checkbox"/>	Device_22_0_2_1	10.127.249.156	22.0.2.1
<input type="checkbox"/>	Device_22_0_32_1	10.127.249.156	22.0.32.1
<input type="checkbox"/>	Device_22_0_36_1	10.127.249.156	22.0.36.1
<input type="checkbox"/>	Device_22_0_41_1	10.127.249.156	22.0.41.1
<input type="checkbox"/>	Device_22_0_51_1	10.127.249.156	22.0.51.1
<input type="checkbox"/>	Device_22_0_55_1	10.127.249.156	22.0.55.1
<input type="checkbox"/>	Device_22_0_61_1	10.127.249.156	22.0.61.1
<input type="checkbox"/>	Device_22_0_63_1	10.127.249.156	22.0.63.1
<input type="checkbox"/>	Device_22_0_64_1	10.127.249.156	22.0.64.1
<input type="checkbox"/>	Device_22_0_70_1	10.127.249.156	22.0.70.1

Add >

< Remove

<input type="checkbox"/>	Device	Source IP	IP Address
Devices are part of selected list			

1 2 Next

Een scan plannen

6. Klik op **Wijzigingen opslaan** wanneer de planning is voltooid.

De **diagnostische scans** en de schema's voor **inventarisverzameling** kunnen worden bewerkt en verwijderd van de pagina **Gegevensverzameling**.



The screenshot displays the 'Data Collection' interface. On the left is a sidebar with icons for Asset Groups, Identity & Access, Partner Access, Data Collection (highlighted), Data Sources, Insights, and Automation. The main content area is divided into two sections: 'Diagnostic Scans' and 'Inventory Collection'.

**Diagnostic Scans** (2 Scans):

Asset Count	Source	Schedule
1	10.127.249.152	Not scannable
10	10.127.249.152	Daily at 07:00 PM IST

A 'Schedule Scan' button is visible above the table. A calendar for October 2022 is shown on the right, with a context menu open over the 10th, offering 'Edit Schedule' and 'Delete Schedule' options.

**Inventory Collection** (8 Collections):

Source	Schedule
Other assets collected by CX Cloud Agent	Daily at 04:00 AM IST
	Daily at 12:30 AM IST
172.20.224.70/five.cisco.com	Monthly on the 9th at 11:30 PM IST
10.127.249.152	Daily at 02:00 AM IST

Below the table, there is a section for 'Rapid Problem Resolution' with a toggle for 'Enable for Campus Network' and a link to 'View detailed instructions'.

Gegevensverzameling met opties voor schema's bewerken en verwijderen

## Implementatie en netwerkconfiguratie

Selecteer een van deze opties om de CX Cloud Agent te implementeren:

- Ga voor het selecteren van VMware vSphere/vCenter Thick Client ESXi 5.5/6.0 naar [Thick Client](#).
- Ga voor het selecteren van VMware vSphere/vCenter Web Client ESXi 6.0 naar [Web Client](#) of [vSphere Center](#)
- Ga voor Oracle Virtual Box 5.2.30 naar [Oracle VM](#)
- Ga voor het selecteren van Microsoft Hyper-V naar [Hyper-V](#)

### OVA-implementatie

#### Installatie van Thick Client ESXi 5.5/6.0

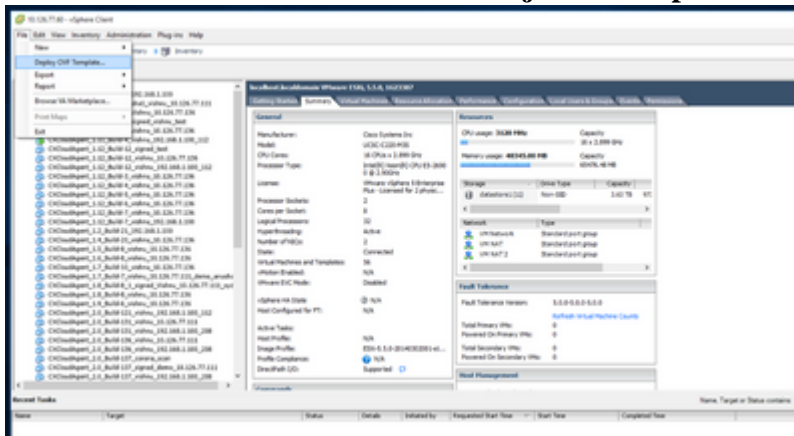
Deze client maakt de implementatie van CX Cloud Agent OVA mogelijk door gebruik te maken van de vSphere dikke client.

1. Start de VMware vSphere-client en log in nadat u de afbeelding hebt gedownload.



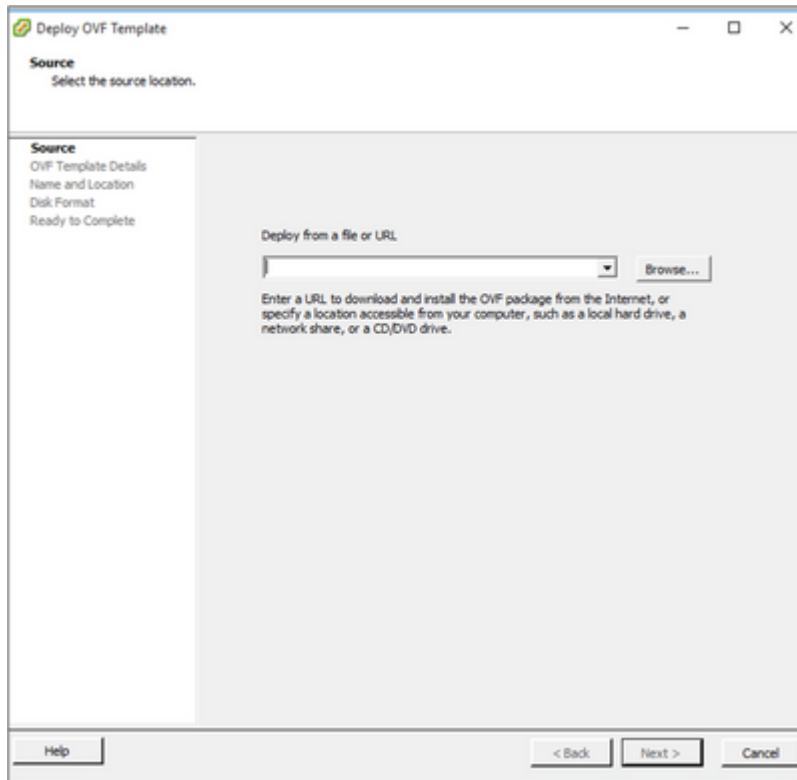
Inloggen

2. Selecteer in het menu **Bestand > OVF-sjabloon implementeren**.



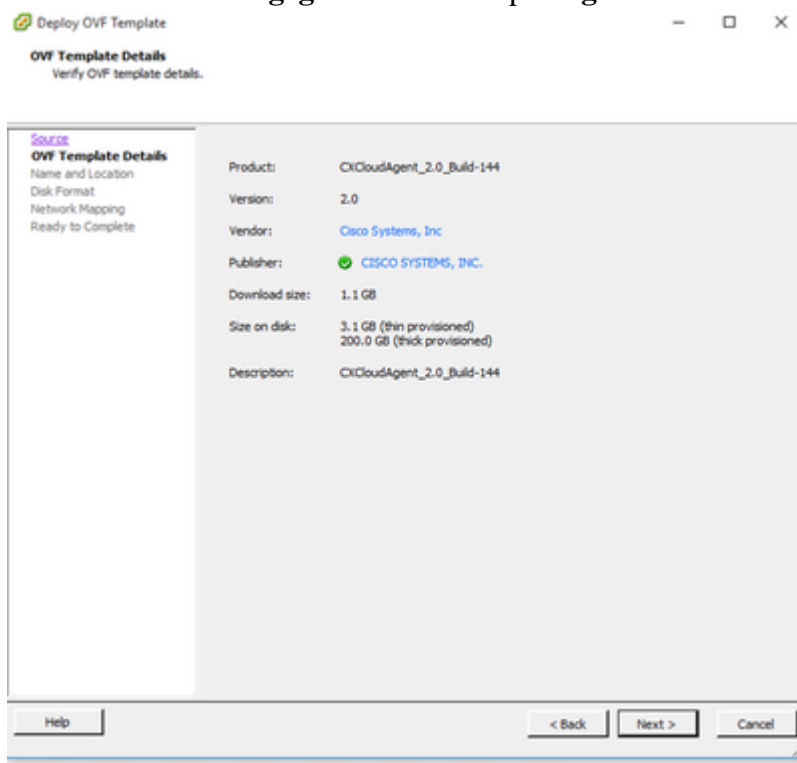
vSphere Client

3. Blader om het OVA-bestand te selecteren en klik op **Volgende**.



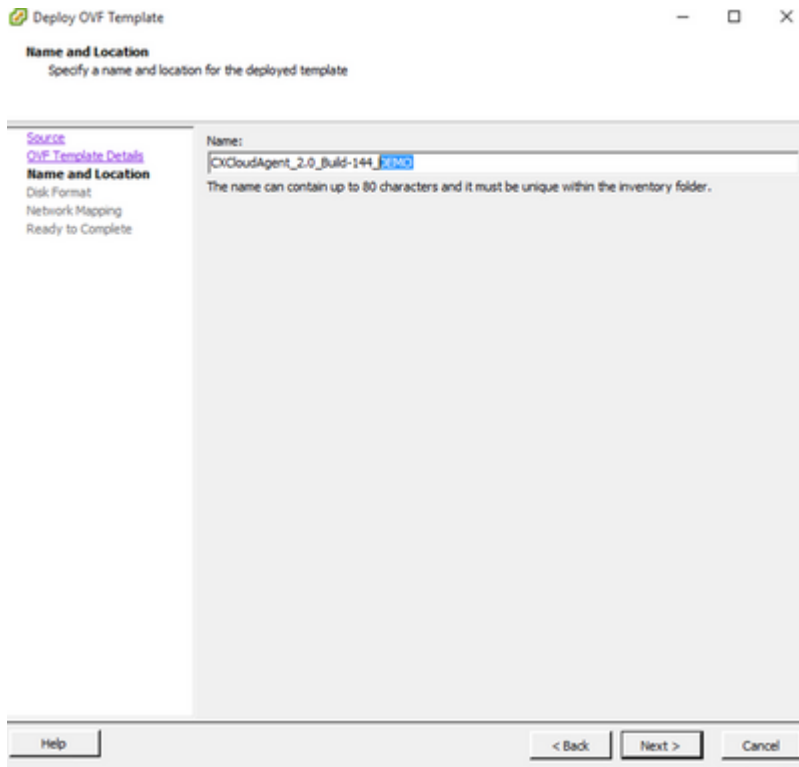
*OVA-pad*

#### 4. Controleer de **OVF-gegevens** en klik op **Volgende**.



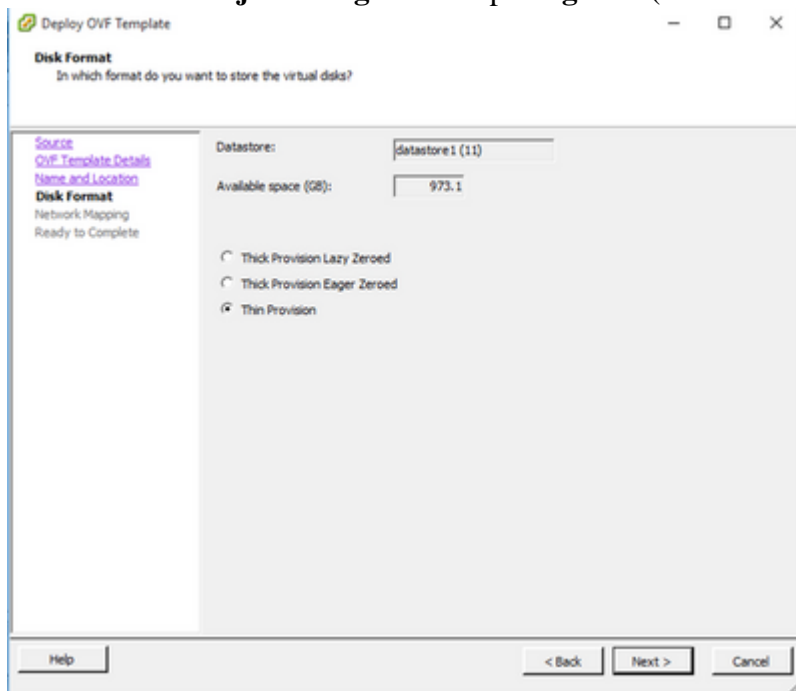
*Gegevens van sjabloon*

#### 5. Voer een **unieke naam in** en klik op **Volgende**.



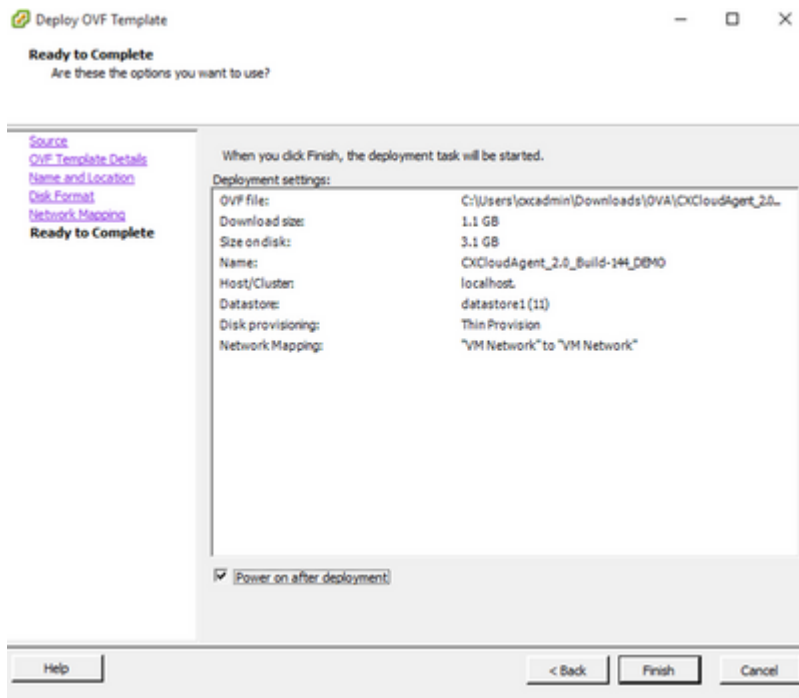
*Naam en locatie*

6. Selecteer een **schijfindeling** en klik op **Volgende** (dunne voorziening wordt aanbevolen).



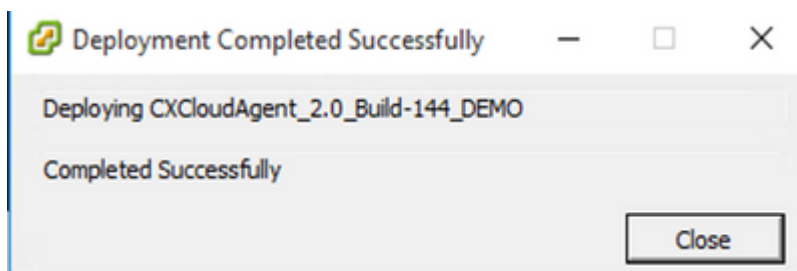
*Schijfindeling*

7. Selecteer het selectievakje **Aan/Uit na implementatie** en klik op **Sluiten**.



*Klaar om te voltooien*

De implementatie kan enkele minuten duren. WC-bevestigingsdisplays bij geslaagde implementatie.



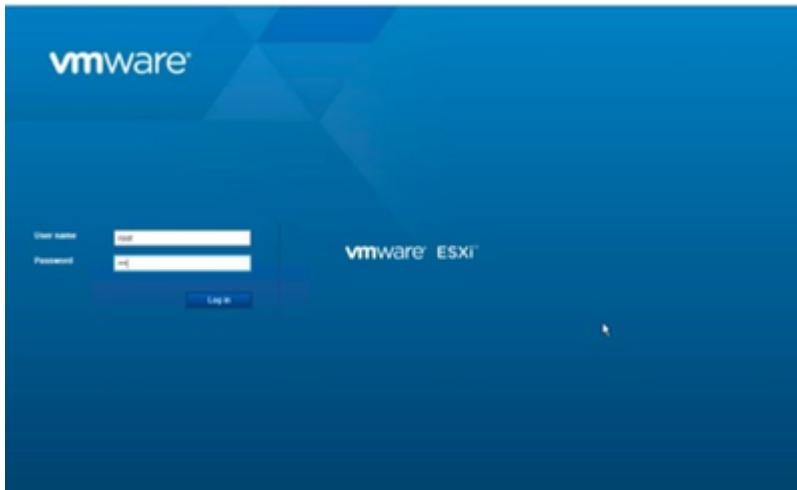
*Implementatie voltooid*

8. Selecteer de geïmplementeerde VM, open de console en ga naar [Network Configuration](#) om verder te gaan met de volgende stappen.

## Installatie van Web Client ESXi 6.0

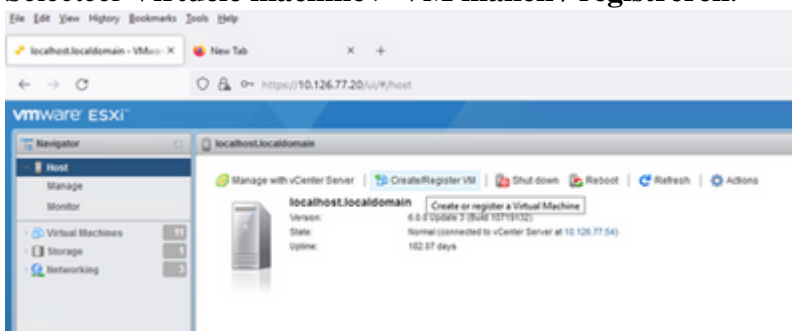
Deze client implementeert CX Cloud Agent OVA met behulp van het vSphere web.

1. Log in op de VMWare UI met de ESXi/hypervisor-referenties die worden gebruikt voor de implementatie van VM.



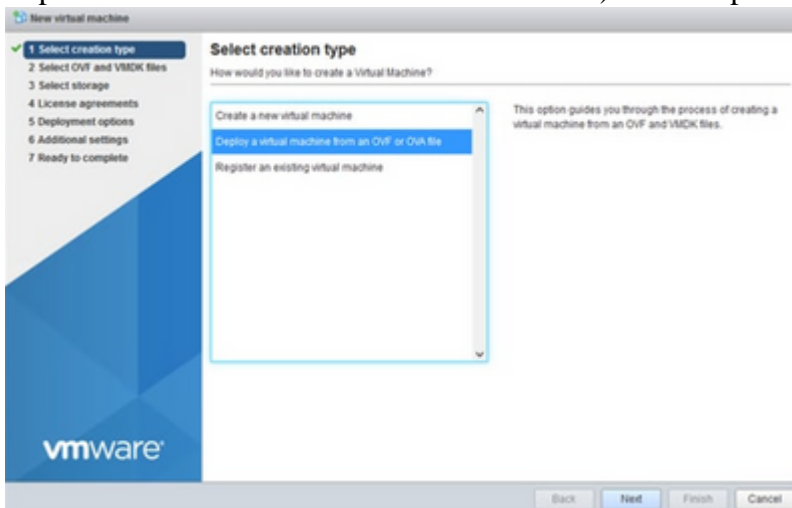
Inloggen bij VMware ESXi

2. Selecteer **Virtuele machine > VM maken / registreren.**



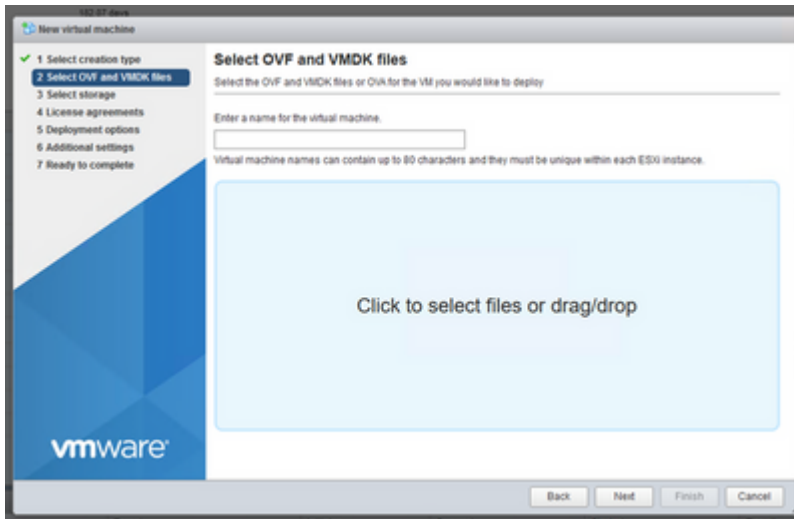
VM maken

3. Selecteer **Deploy a virtual machine from an OVF or OVA file** (Een virtuele machine implementeren via een OVF- of OVA-bestand) en klik op **Next (Volgende).**



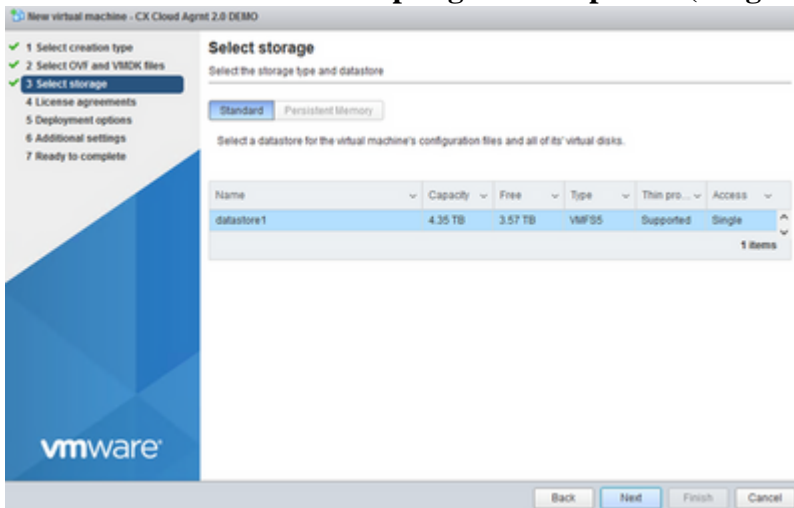
Selecteer Creatietype

4. Voer de naam van de VM in, blader om het bestand te selecteren of sleep het gedownload OVA-bestand.
5. Klik op **Next (Volgende).**



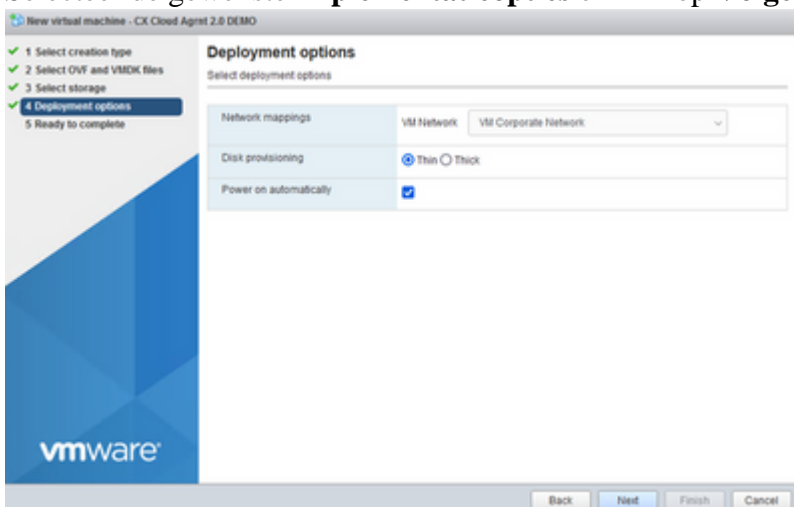
*OVA selecteren*

6. Selecteer **Standard** voor de opslag en klik op **Next (Volgende)**.



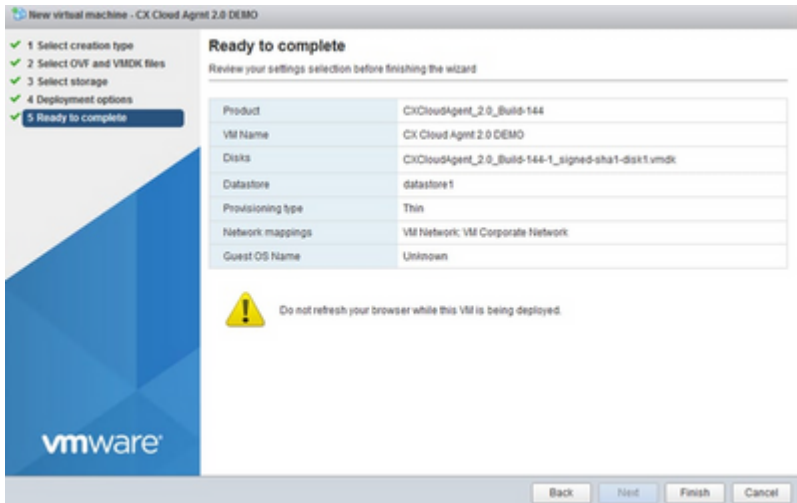
*Opslag selecteren*

7. Selecteer de gewenste **implementatieopties** en klik op **Volgende**.

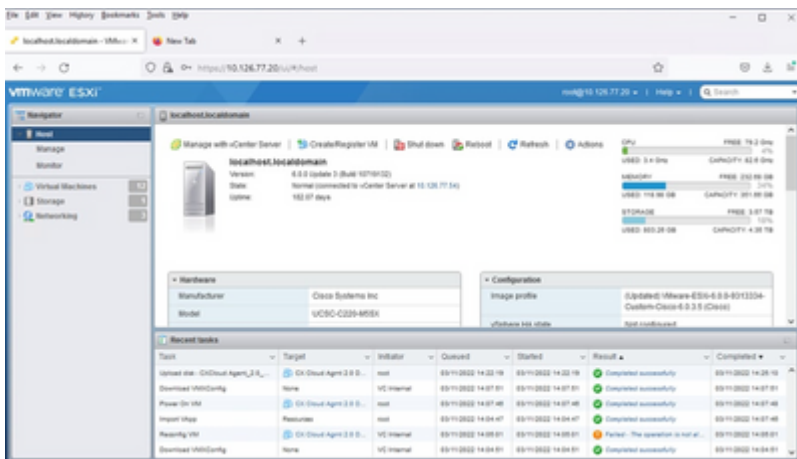


*Implementatieopties*

8. Controleer de instellingen en klik op **Finish (Voltoeien)**.

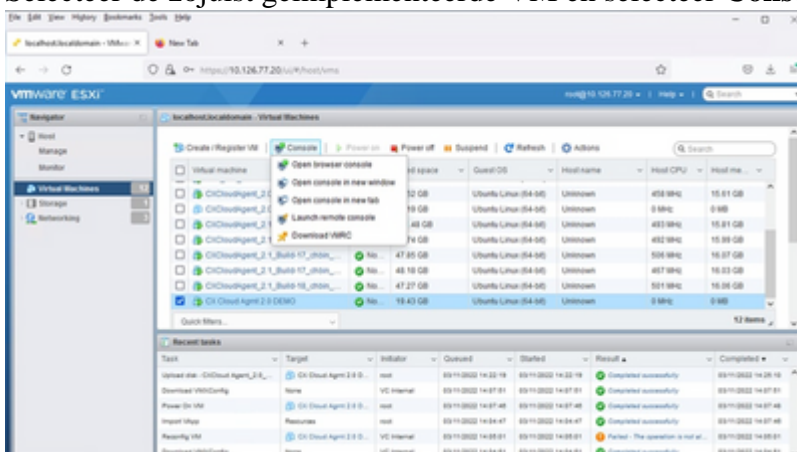


Klaar om te voltooien



Succesvol voltooid

9. Selecteer de zojuist geïmplementeerde VM en selecteer **Console > Open browserconsole**.



console

10. Navigeer naar [Netwerkconfiguratie](#) om met de volgende stappen verder te gaan.

## Installatie van Web Client vCenter



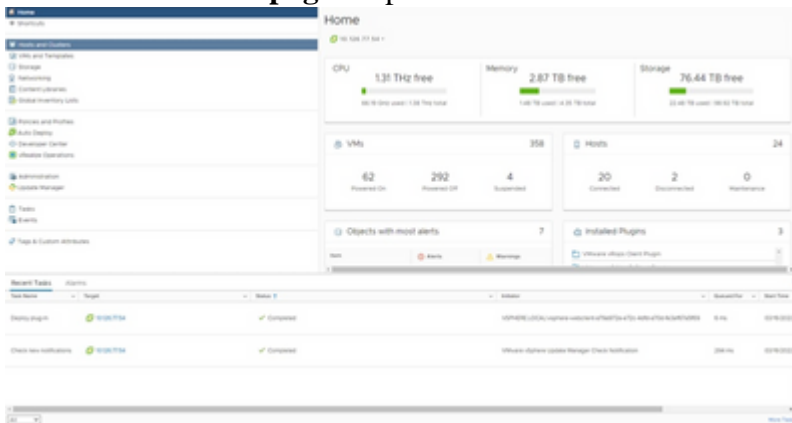
Voer de volgende handelingen uit:

1. Log in op vCenter-client via ESXi/hypervisor-referenties.



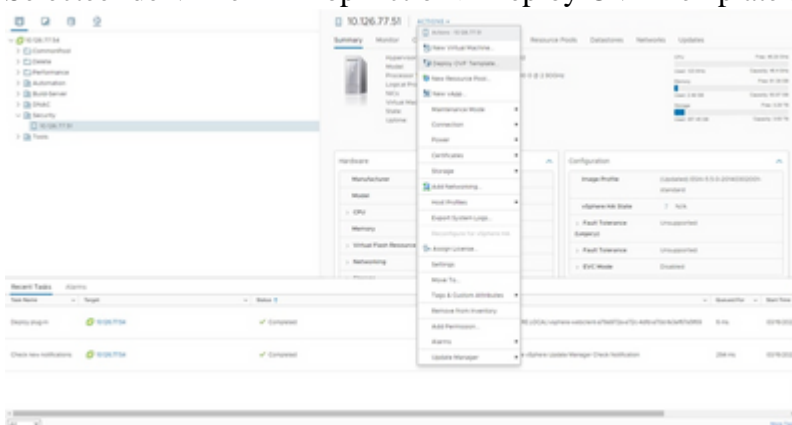
*Inloggen*

2. Klik vanaf de Homepagina op **Hosts en Clusters**.

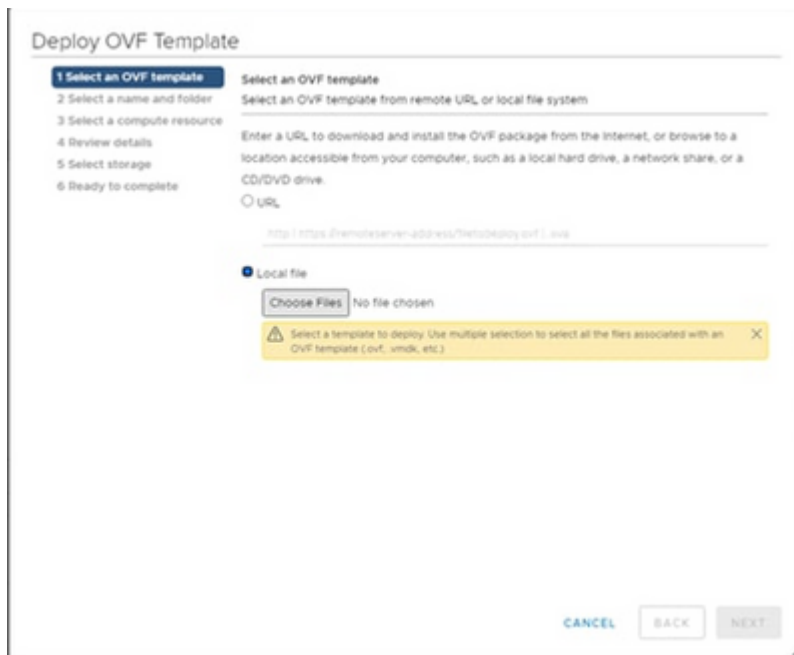


*Startpagina*

3. Selecteer de VM en klik op Action > Deploy OVF Template (Actie > OVF-sjabloon implementeren).

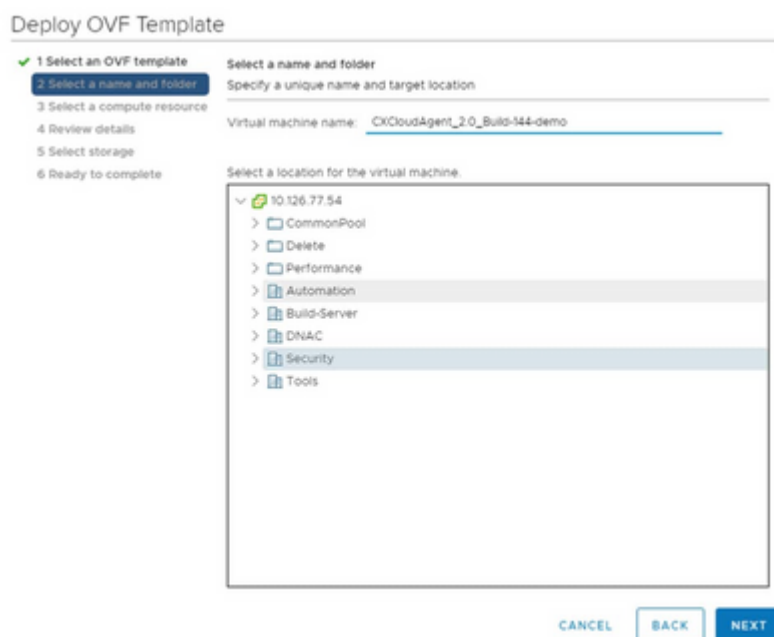


*Acties*



*Sjabloon selecteren*

4. Voeg de URL direct toe of blader om het OVA-bestand te selecteren en klik op **Volgende**.
5. Voer een unieke naam in en blader indien nodig naar de locatie.
6. Klik op Next (Volgende).



*Naam en map*

7. Selecteer een computing resource en klik op **Volgende**.

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource**
- 4 Review details
- 5 Select storage
- 6 Ready to complete

### Select a compute resource

Select the destination compute resource for this operation

Security

- 10.126.77.51

### Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

*Selecteer Computer Resource*

8. Controleer de gegevens en klik op Next (Volgende).

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

### Review details

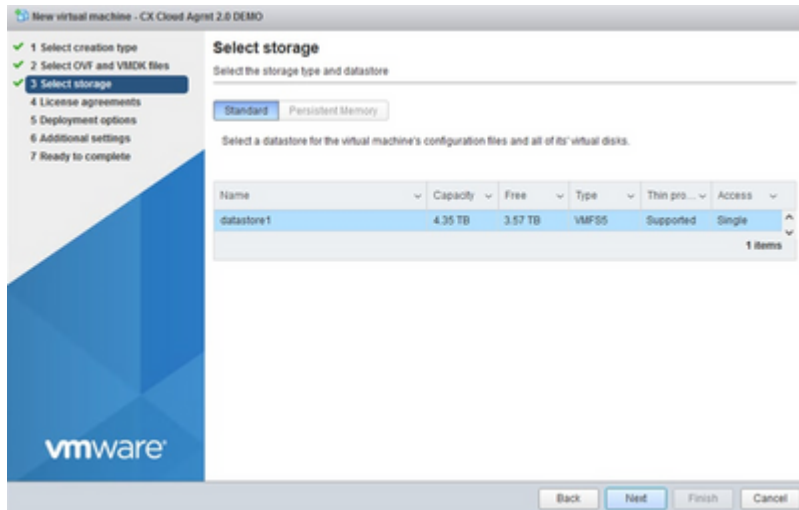
Verify the template details.

Publisher	DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate)
Product	CXCloudAgent_2.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CXCloudAgent_2.0_Build-144
Download size	11 GB
Size on disk	3.1 GB (thin provisioned) 200.0 GB (thick provisioned)

CANCEL BACK NEXT

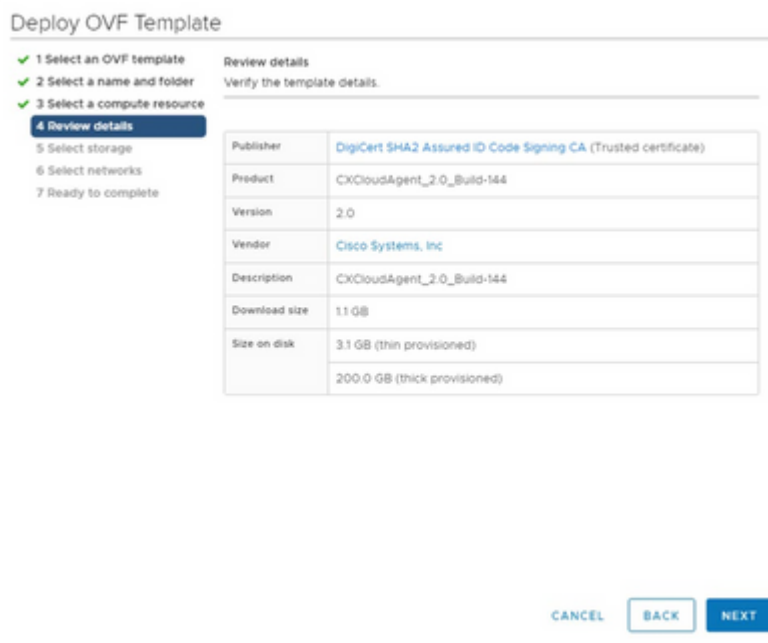
*Gegevens controleren*

9. Selecteer de indeling van de virtuele schijf en klik op Next (Volgende).



*Opslag selecteren*

10. Klik op Next (Volgende).



*Selecteer een netwerk*

11. Klik op Finish (Voltooiën).

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Ready to complete**

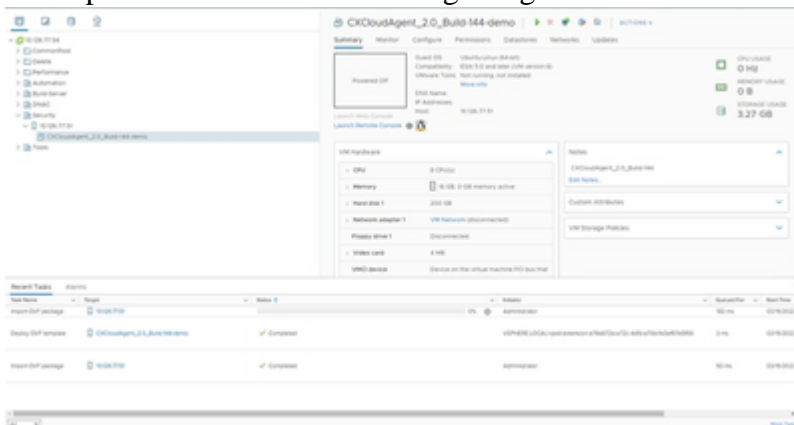
Ready to complete  
Click Finish to start creation.

Provisioning type	Deploy from template
Name	CXCloudAgent_2_0_Build-144-demo
Template name	CXCloudAgent_2_0_Build-144-1_signed-sha1
Download size	11 GB
Size on disk	3.1 GB
Folder	Security
Resource	10.126.77.51
Storage mapping	1
All disks	Datastore: datastore1 (23); Format: Thin provision
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPv4
IP allocation	Static + Manual

CANCEL BACK FINISH

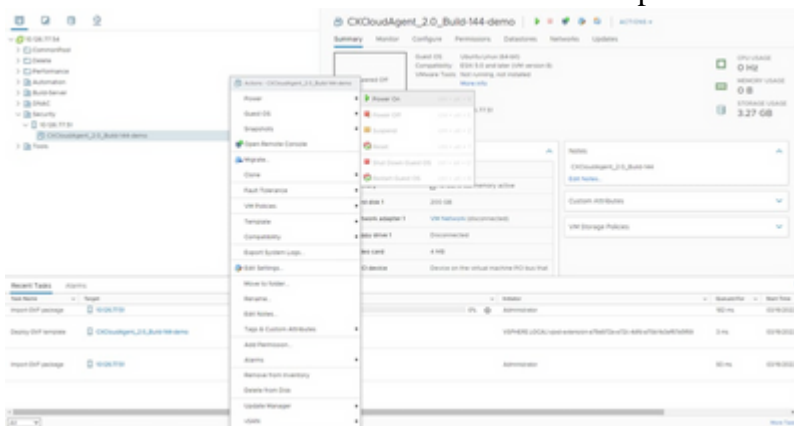
*Klaar om te voltooien*

12. Klik op de naam van de nieuw toegevoegde VM om de status te bekijken.



*Toegevoegd VM*

13. Na installatie de VM inschakelen en de console openen.



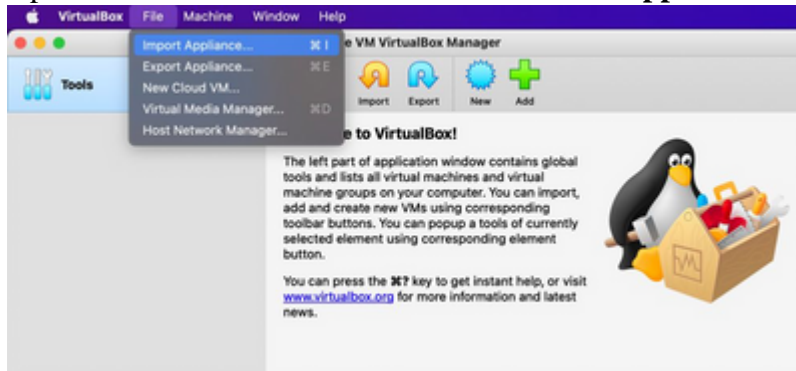
*Console openen*

14. Navigeer naar [Netwerkconfiguratie](#) om met de volgende stappen verder te gaan.

## Installatie van Oracle VirtualBox 5.2.30

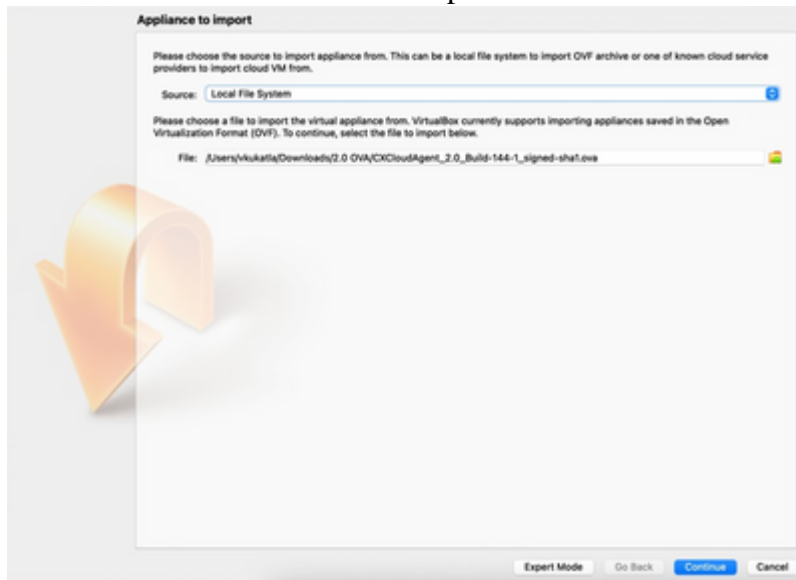
Deze client implementeert CX Cloud Agent OVA via de Oracle Virtual Box.

1. Open de Oracle VM UI en selecteer **Bestand** > **Applicatie importeren**.



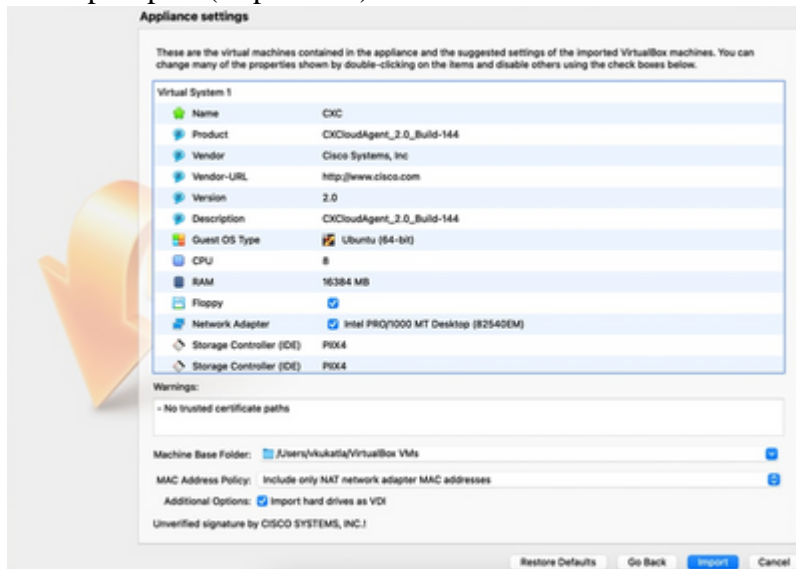
Oracle VM

2. Blader om het OVA-bestand te importeren.

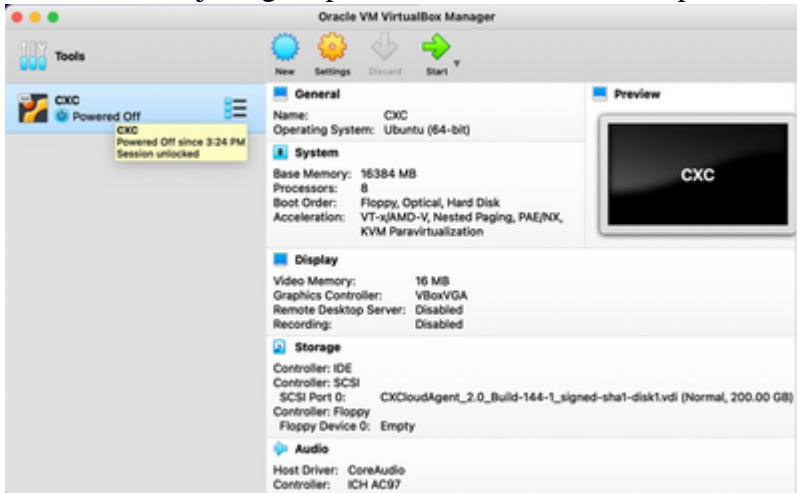


Bestand selecteren

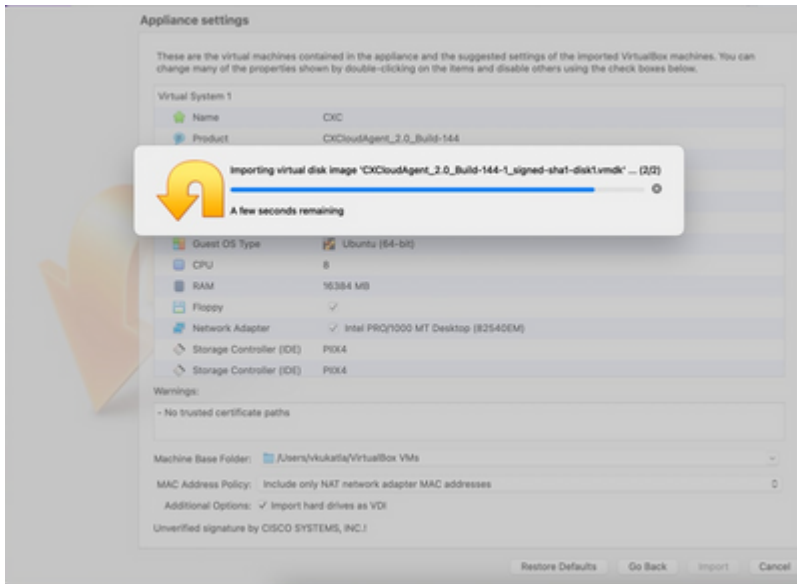
3. Klik op Import (Importeren).



4. Selecteer de zojuist geïmplementeerde VM en klik op **Start**.



VM-console opstarten



Importeren wordt uitgevoerd

5. Schakel de VM in. De console wordt weergegeven.



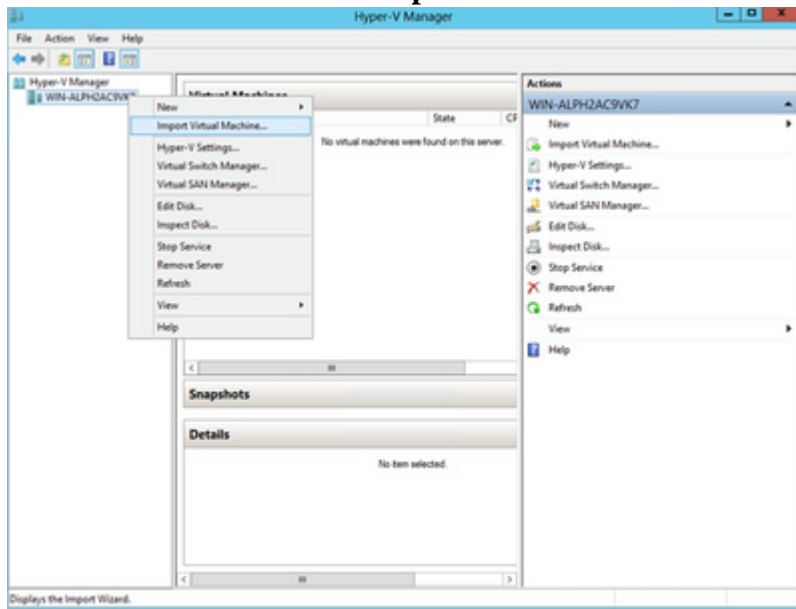
Console openen

6. Navigeer naar [Netwerkconfiguratie](#) om met de volgende stappen verder te gaan.

## Installatie van Microsoft Hyper-V

Voer de volgende handelingen uit:

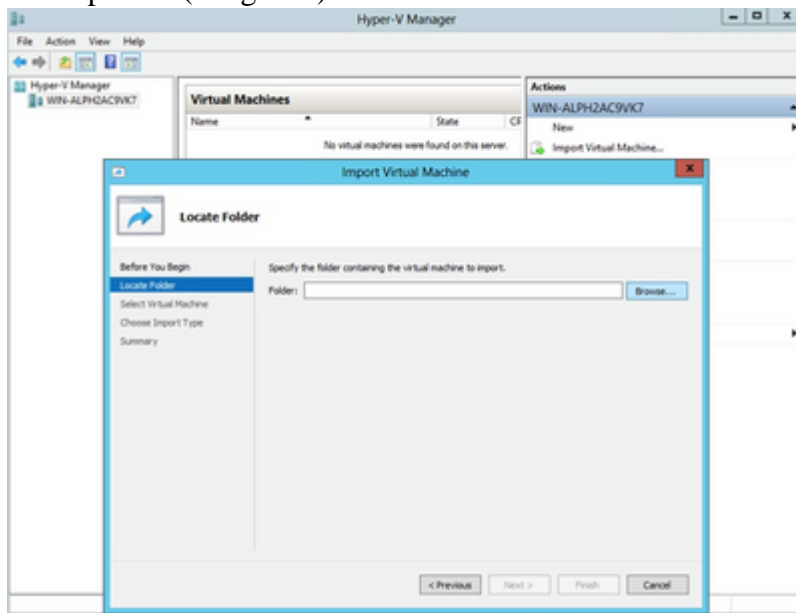
1. Selecteer **Virtuele machine importeren**.



Hyper-V beheer

2. Blader en selecteer de downloadmap.

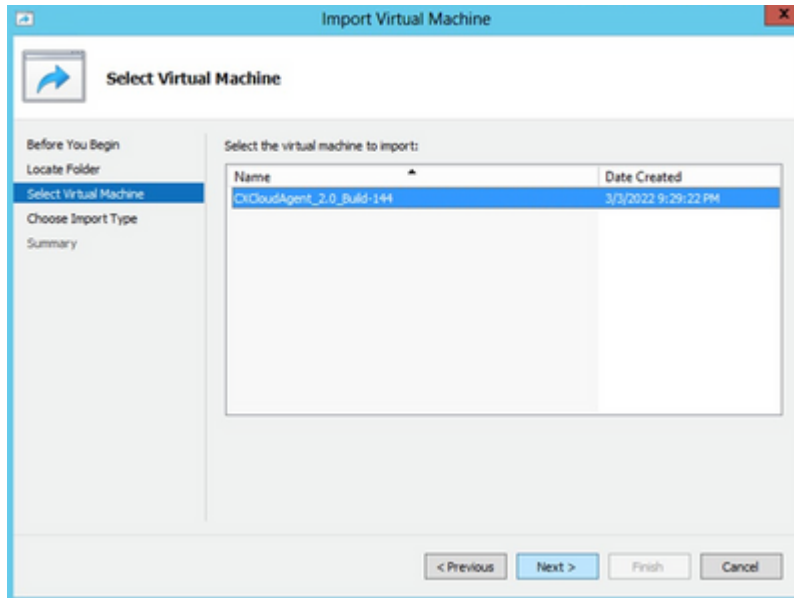
3. Klik op Next (Volgende).



Map om naar te importeren

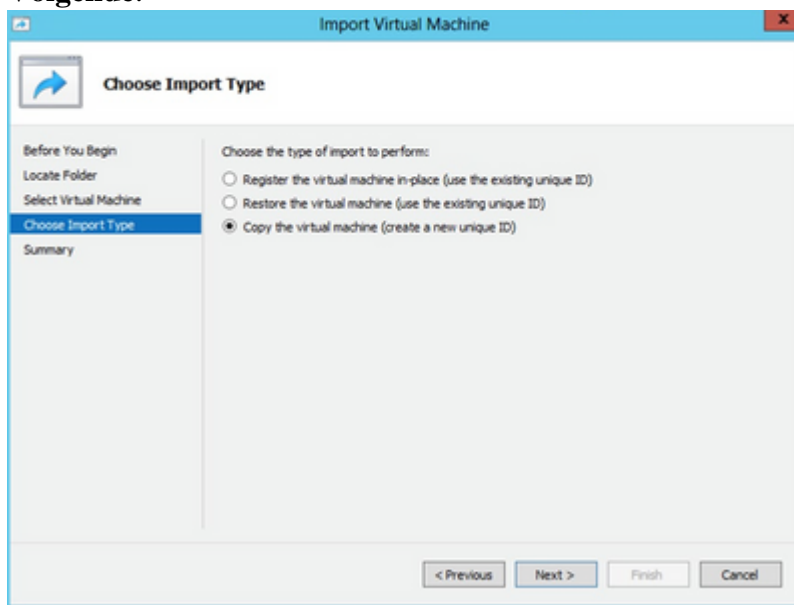
4. Selecteer de VM en klik op **Volgende**.





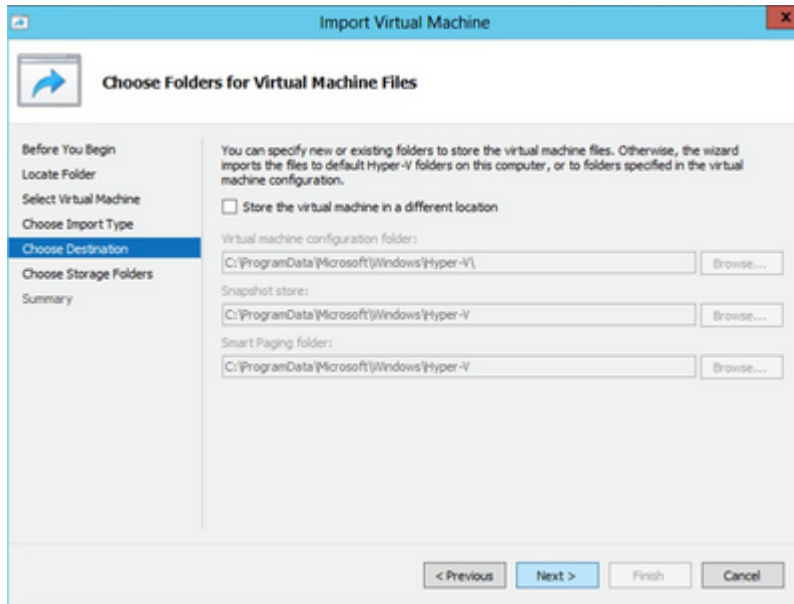
*VM selecteren*

5. Selecteer de radioknop **Kopieer de virtuele machine (maak een nieuwe unieke ID)** en klik op **Volgende**.



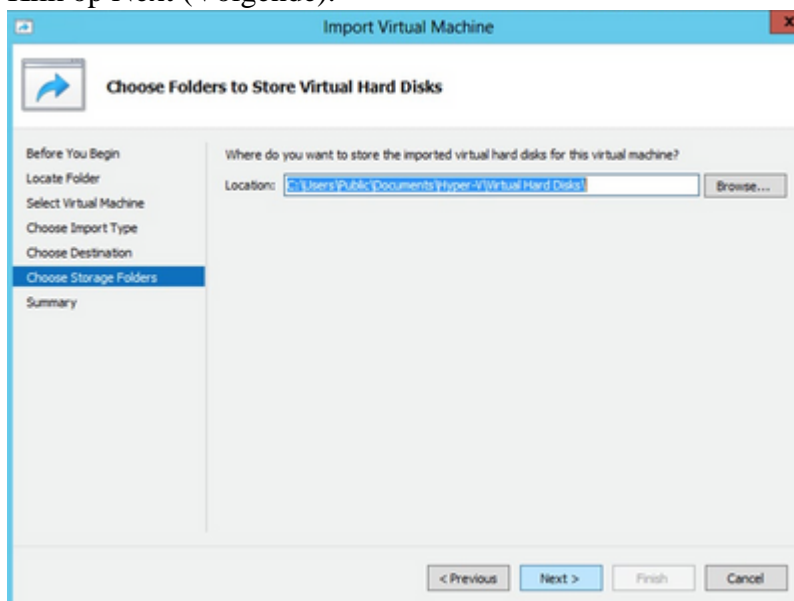
*Importtype*

6. Blader om de map voor VM-bestanden te selecteren. Het wordt aanbevolen om de standaardpaden te gebruiken.
7. Klik op Next (Volgende).



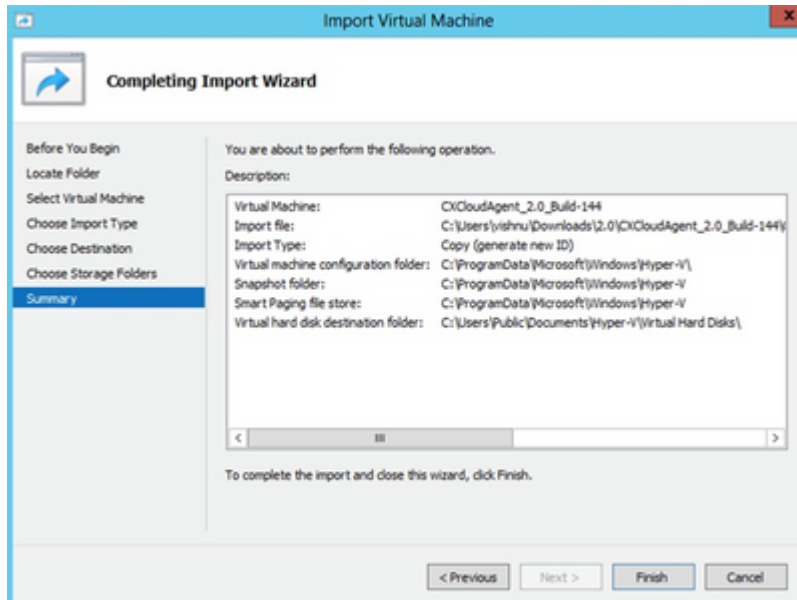
*Mappen voor virtuele machinebestanden kiezen*

8. Blader en selecteer de map om de harde schijf van de VM op te slaan. Aanbevolen wordt om standaardpaden te gebruiken.
9. Klik op Next (Volgende).



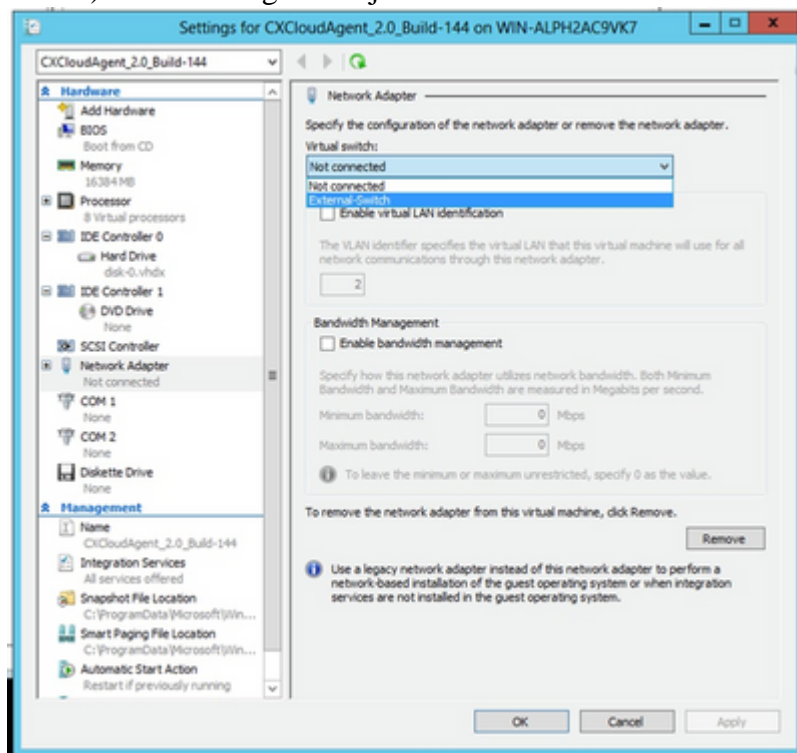
*Map om de virtuele vaste schijven op te slaan*

10. De samenvatting van de VM wordt weergegeven. Controleer alle invoer en klik op **Voltooien**.



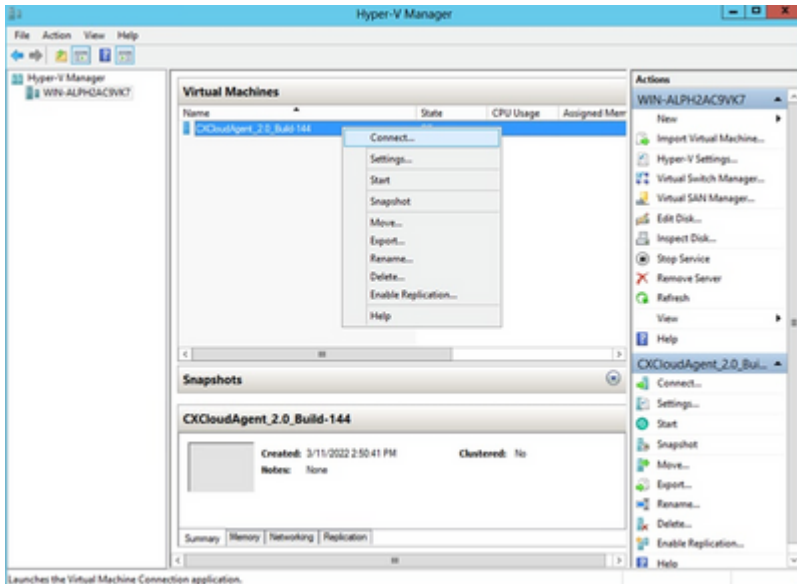
### Samenvatting

11. Wanneer de import succesvol is voltooid, wordt er een nieuwe VM gemaakt op Hyper-V. Open de VM-instelling.
12. Selecteer de netwerkadapter in het linkerdeelvenster en kies de beschikbare Virtual switch (Virtuele switch) in de vervolgkeuzelijst.



### Virtuele switch

13. Selecteer **Verbinden** om de VM te starten.



VM wordt gestart

14. Navigeer naar [Netwerkconfiguratie](#) om met de volgende stappen verder te gaan.

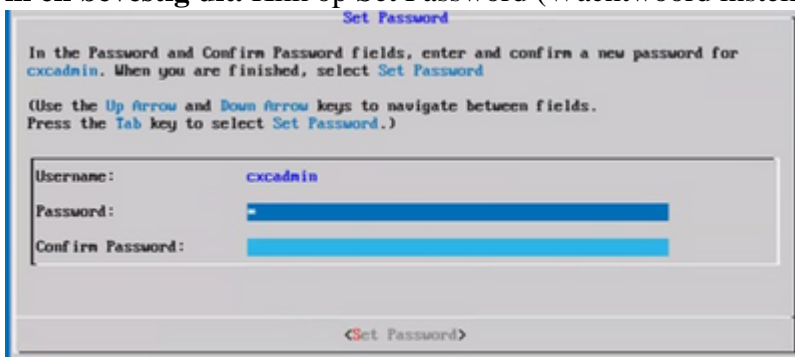
## Netwerkconfiguratie

1. Klik op **Wachtwoord instellen** om een nieuw wachtwoord toe te voegen voor cxcadmin OF klik op **Wachtwoord automatisch genereren** om een nieuw wachtwoord te verkrijgen.



Wachtwoord instellen

2. Als **Set Password** (Wachtwoord instellen) is geselecteerd, voer dan het wachtwoord voor **cxcadmin in en bevestig dit**. Klik op Set Password (Wachtwoord instellen) en ga naar stap 3.



Nieuw wachtwoord

OF

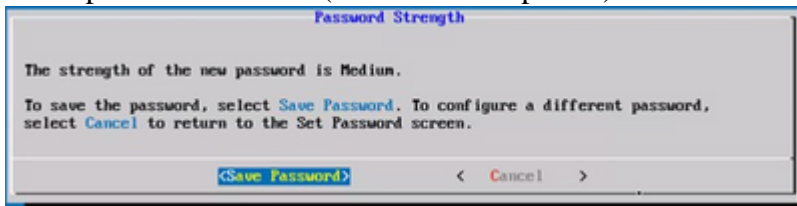
Als **Auto Generate Password** is geselecteerd, kopieert u het gegenereerde wachtwoord en slaat u het

op voor later gebruik. Klik op Save Password (Wachtwoord opslaan) en ga naar stap 4.



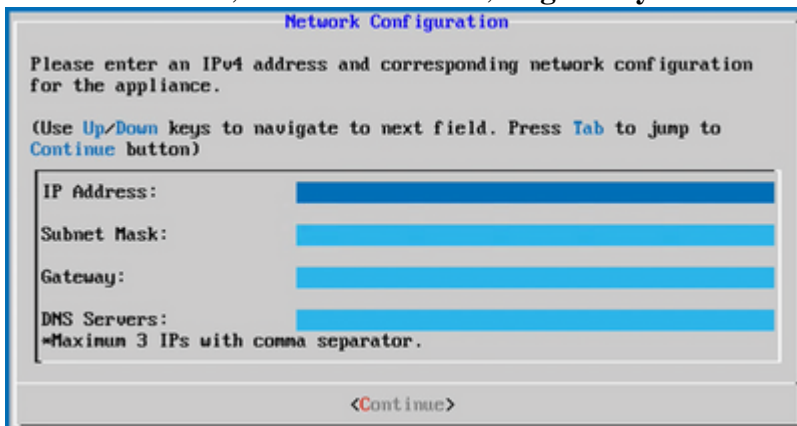
Automatisch gegenereerd wachtwoord

3. Klik op **Save Password** (Wachtwoord opslaan) om het voor verificatie te gebruiken.



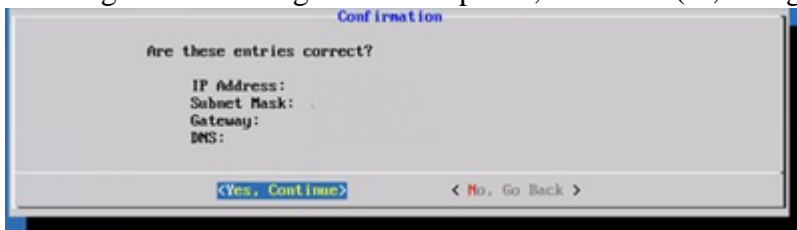
Wachtwoord opslaan

4. Voer het IP-adres, het **subnetmasker**, de **gateway** en de **DNS-server in** en klik op **Doorgaan**.



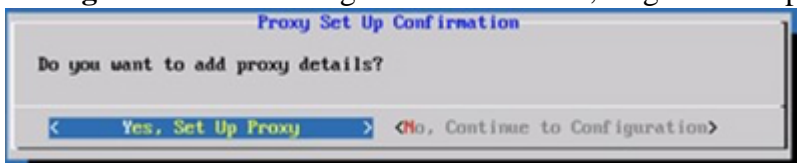
Netwerkconfiguratie

5. Bevestig de vermeldingen en klik op Yes, Continue (Ja, doorgaan).



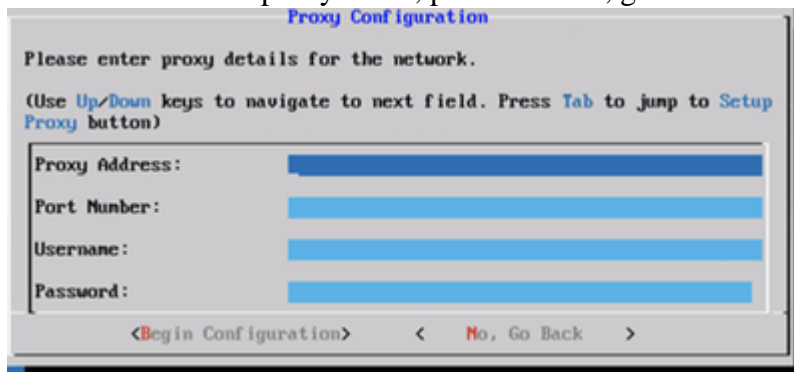
Configuratie

6. Om de volmachtsdetails te plaatsen, klik **ja**, de **Volmacht van de Opstelling** of klik **Nee**, blijf aan **Configuratie** om de configuratie te voltooien, en ga naar Stap 8.



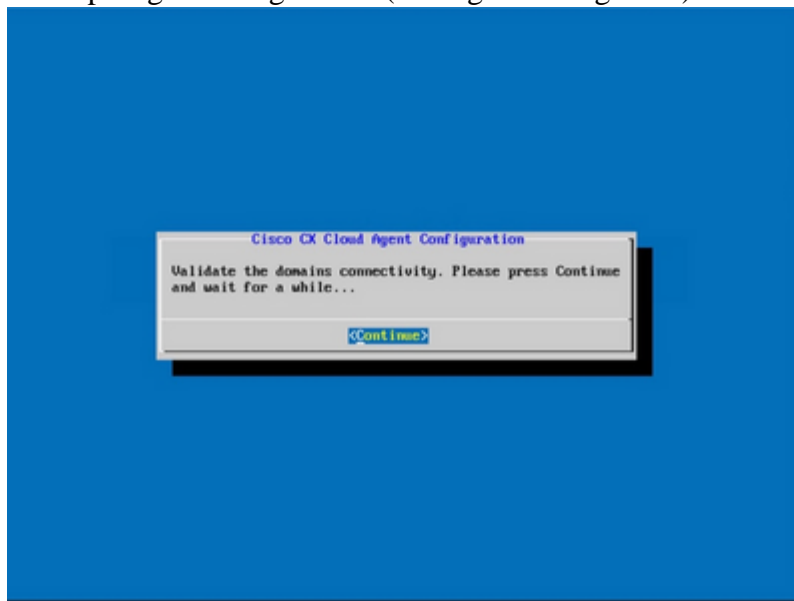
Proxy-instelling

7. Vul de velden voor proxy-adres, poortnummer, gebruikersnaam en wachtwoord in.



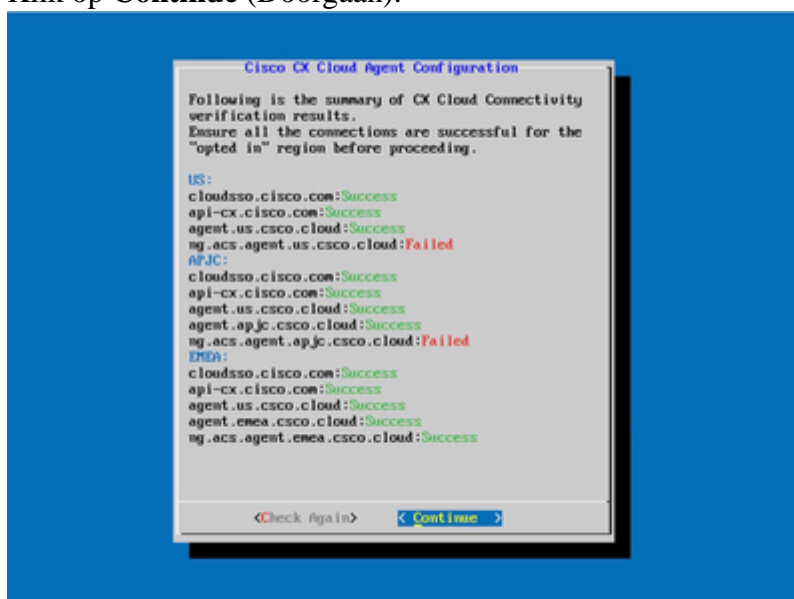
Proxyconfiguratie

8. Klik op Begin Configuration (Configuratie beginnen).



Configuratie starten

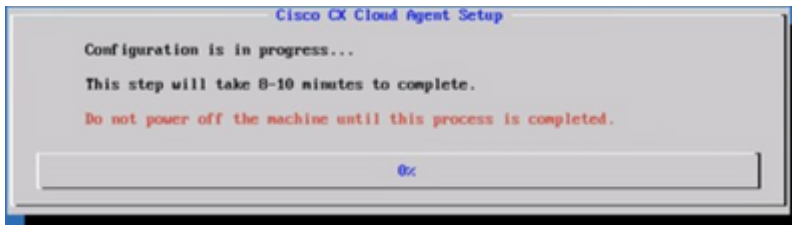
9. Klik op Continue (Doorgaan).



De configuratie gaat verder

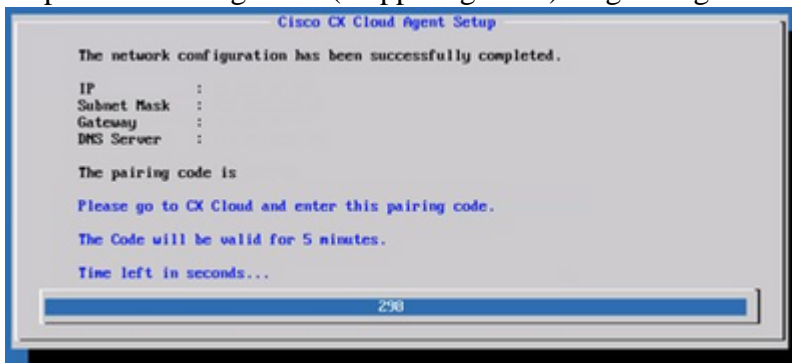
10. Klik op **Doorgaan** om verder te gaan met de configuratie voor een succesvol domeinbereik. De configuratie kan enkele minuten duren.

**Opmerking:** Als de domeinen niet met succes kunnen worden bereikt, moet de klant domeinbereikbaarheid oplossen door wijzigingen aan te brengen in de firewall om ervoor te zorgen dat domeinen bereikbaar zijn. Klik **nogmaals** op **Controle** zodra het probleem met de bereikbaarheid van domeinen is opgelost.



*Configuratie is bezig*

11. Kopieer de Pairing Code (Koppelingscode) en ga terug naar CX Cloud voor verdere instellingen.



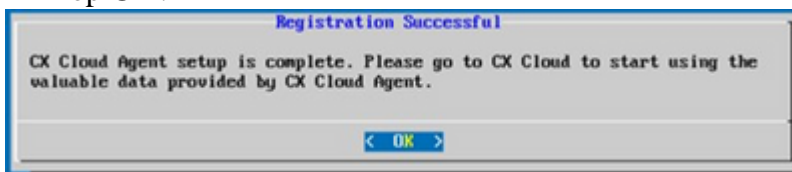
*Koppelingscode*

12. Als de paarcode verloopt, klikt u op **Registreren naar CX Cloud** om de code opnieuw te verkrijgen.



*Code verlopen*

13. Klik op **OK**.



*Registratie geslaagd*

## Alternatieve benadering voor het genereren van paarcode met CLI

Gebruikers kunnen ook een koppelcode genereren met behulp van CLI-opties.

Zo genereert u een koppelcode met CLI:

1. Log in op de Cloud Agent via SSH met behulp van de cxcadmin gebruikersreferenties.
2. Generereert de koppelingscode met de opdracht `cxcli agent generationPairingCode`.

```
cxcadm@cxcloudagent:~$ cxcli agent generatePairingCode

Pairing Code : x3718P
Expires in: 5 minutes
Please use the Pairing Code in the CX Cloud to proceed with CX Cloud Agent registration.

cxcadm@cxcloudagent:~$
```

*Koppelingscode genereren via opdrachtregelinterface*

3. Kopieer de Pairing Code (Koppelingscode) en ga terug naar CX Cloud voor verdere instellingen.

## Cisco DNA Center configureren om Syslog door te sturen naar CX Cloud Agent

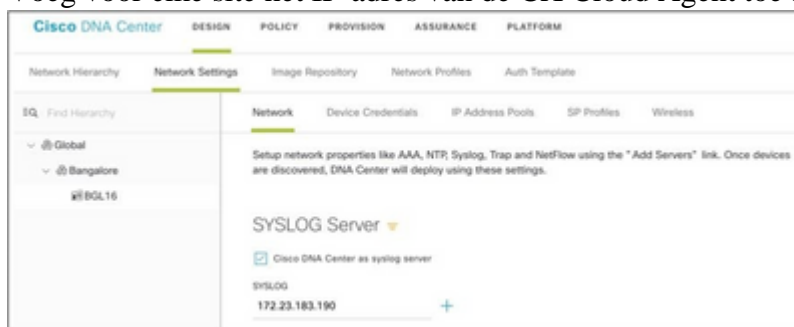
### Voorwaarden

Ondersteunde versies van Cisco DNA Center zijn 2.1.2.0 tot en met 2.2.3.5, 2.3.3.4 tot en met 2.3.3.6, 2.3.5.0 en virtuele applicatie van Cisco DNA Center

### Voorwaartse instelling van Syslog configureren

Voer de volgende stappen uit om Syslog Forwarding naar CX Cloud Agent in het Cisco DNA Center te configureren:

1. Start Cisco DNA Center.
2. Ga naar Design > Network Settings > Network (Ontwerp > Netwerkinstellingen > Netwerk).
3. Voeg voor elke site het IP-adres van de CX Cloud Agent toe als de syslog-server.



*Syslog-server*

---

### Opmerkingen:

Na configuratie worden alle apparaten die zijn gekoppeld aan die site geconfigureerd om syslog met niveau kritische naar CX Cloud Agent te sturen. Apparaten moeten aan een site worden gekoppeld om syslog door te sturen van het apparaat naar CX Cloud Agent mogelijk te maken.

Wanneer een syslogserverinstelling wordt bijgewerkt, worden alle apparaten die aan die site zijn gekoppeld automatisch op een standaard kritisch niveau ingesteld.

---

## Andere middelen configureren om Syslog door te sturen naar CX Cloud Agent

Apparaten moeten zo worden geconfigureerd dat ze Syslog-berichten naar de CX Cloud Agent sturen om de Fault Management-functie van CX Cloud te gebruiken.



---

**Opmerking:** alleen Campus Success Track Level 2-apparaten zijn in aanmerking om andere activa te configureren voor voorwaartse syslog.

---

## Bestaande systeemserver met voorwaartse mogelijkheid

Voer de configuratie-instructies voor de syslogserversoftware uit en voeg het CX Cloud Agent IP-adres als een nieuwe bestemming toe.

---

**Opmerking:** zorg er bij het doorsturen van syslogs voor dat het IP-bronadres van het oorspronkelijke syslogbericht behouden blijft.

---

## Bestaande systeemserver zonder voorwaartse mogelijkheid OF zonder systeemserver

Configureer elk apparaat om syslogs rechtstreeks naar het IP-adres van CX Cloud Agent te verzenden. Raadpleeg de volgende documentatie voor specifieke configuratiestappen.

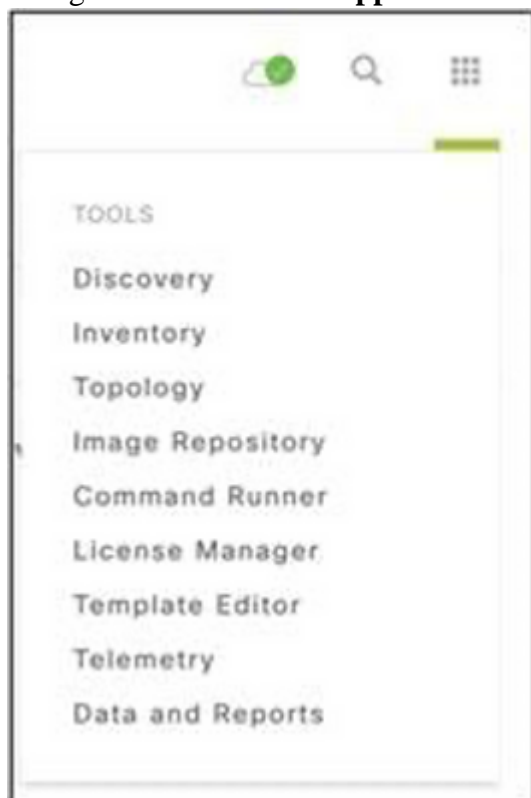
[IOS-XE-configuratiehandleiding](#)

[Configuratiehandleiding voor AireOS draadloze controller](#)

## Systeeminstellingen op informatieniveau inschakelen

Voer de volgende stappen uit om het niveau Syslog-informatie zichtbaar te maken:

1. Navigeer naar **Gereedschappen>Telemetrie**.



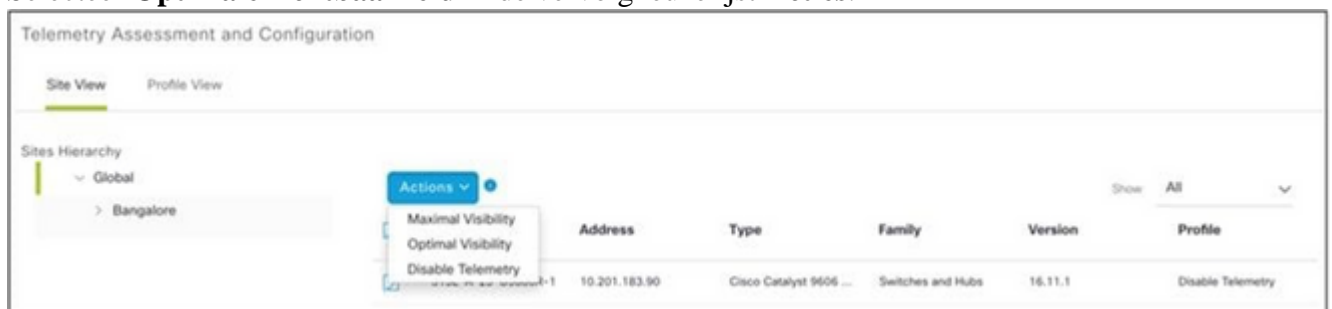
*Het menu Gereedschappen*

2. Selecteer en breid de **siteweergave uit** en selecteer een site uit de sitehiërarchie.



*Siteweergrave*

3. Selecteer de gewenste site en selecteer alle apparaten met behulp van het aanvinkvakje **Apparaatnaam**.
4. Selecteer **Optimale zichtbaarheid** in de vervolgkeuzelijst **Acties**.



*Acties*

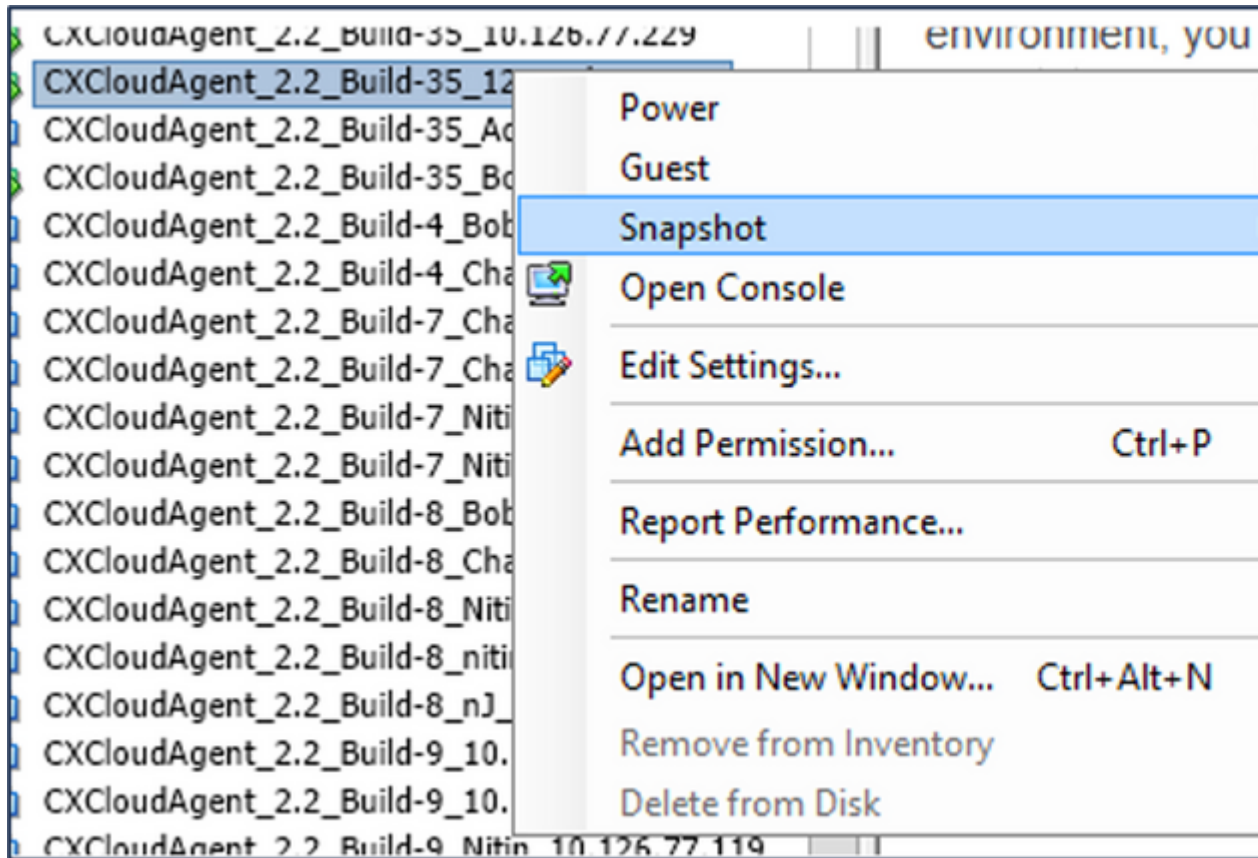
## Back-up en herstel van de CX Cloud VM

Het wordt aanbevolen om de status en gegevens van een CX Cloud Agent VM op een specifiek tijdstip te bewaren met behulp van de snapshot-functie. Deze functie maakt CX Cloud VM-herstel mogelijk op het specifieke tijdstip waarop de snapshot wordt gemaakt.

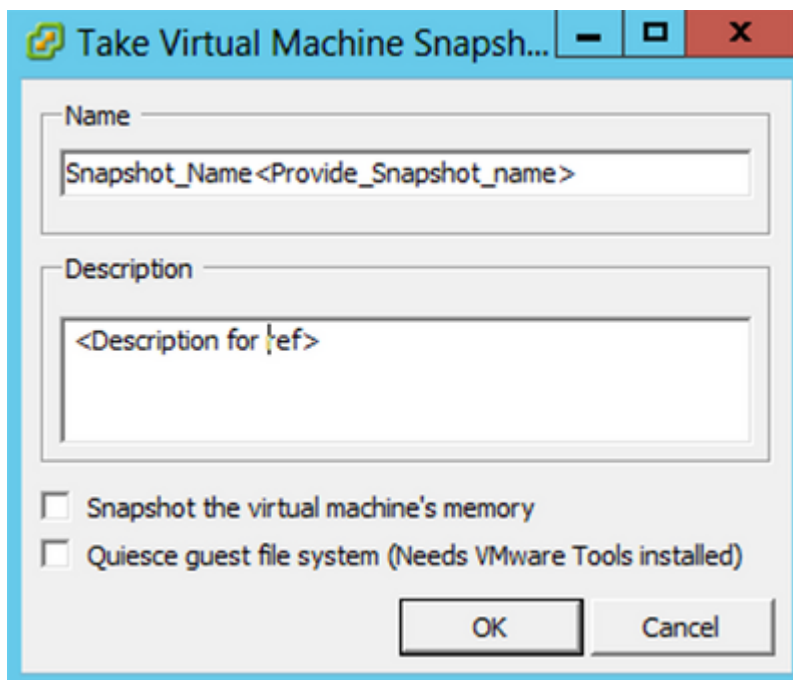
### Back-up

Een back-up maken van de CX Cloud VM:

1. Klik met de rechtermuisknop op de VM en selecteer **Snapshot > Snapshot maken**. Het venster **Take Virtual Machine Snapshot** wordt geopend.



VM selecteren



Snapshot van virtuele machine maken

2. Voer een **naam** en een **beschrijving in**.

---

**Opmerking:** controleer of de snapshot van het aanvinkvakje voor het geheugen van de virtuele machine is gewist.

---

3. Klik op **OK**. De status van de **snapshot van de virtuele machine maken** wordt weergegeven als **voltooid** in de lijst Recente taken.

The screenshot shows the vSphere Client interface. On the left, a list of virtual machines is displayed, with 'CXCloudAgent\_2.2\_Build-35\_10.126.77.227\_Chaitra' selected. The main pane shows the details for this VM, including a 'What is a Virtual Machine?' section, a 'Basic Tasks' section with options like 'Power Off the virtual machine', 'Suspend the virtual machine', and 'Edit virtual machine settings', and a 'Recent Tasks' table at the bottom.

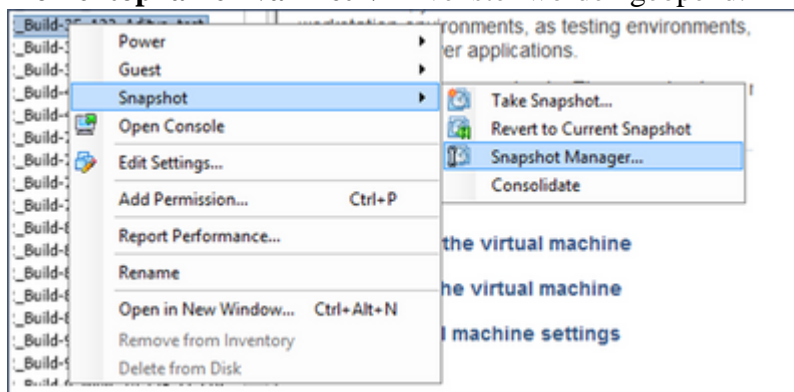
Name	Target	Status	Details
Download VM configuration		Completed	
Revert snapshot	CXCloudAgent_2.2_Build-35_122_Aditya_test	Completed	
Download VM configuration		Completed	
Create virtual machine snapshot	CXCloudAgent_2.2_Build-35_122_Aditya_test	Completed	

Recente taken

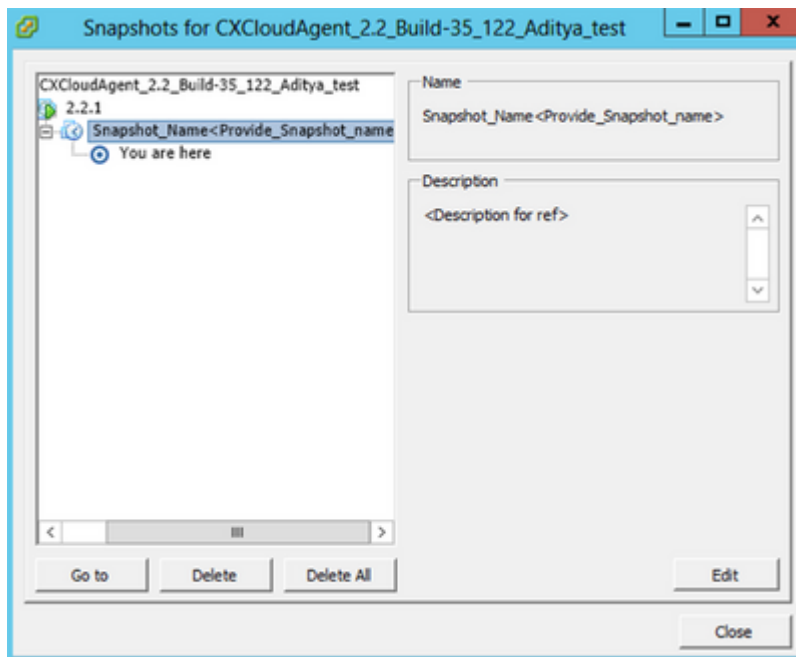
## Terugzetten

U kunt de CX Cloud VM als volgt herstellen:

1. Klik met de rechtermuisknop op de VM en selecteer **Snapshot > Snapshot Manager**. De **momentopnamen van het VM-venster** worden geopend.

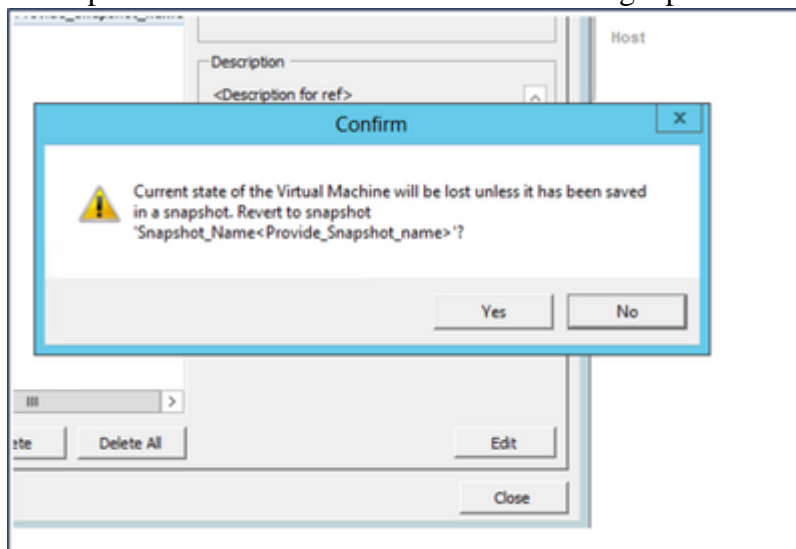


VM-venster selecteren



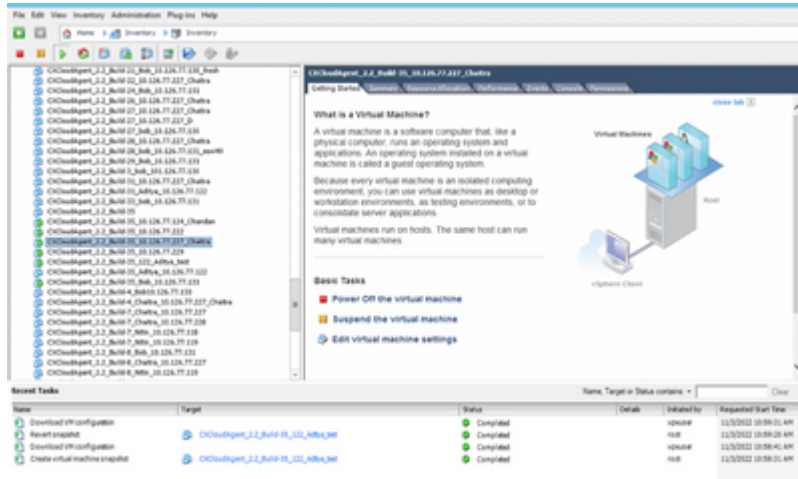
*Snapshots-venster*

2. Klik op **Ga naar**. Het venster **Confirma** wordt geopend.



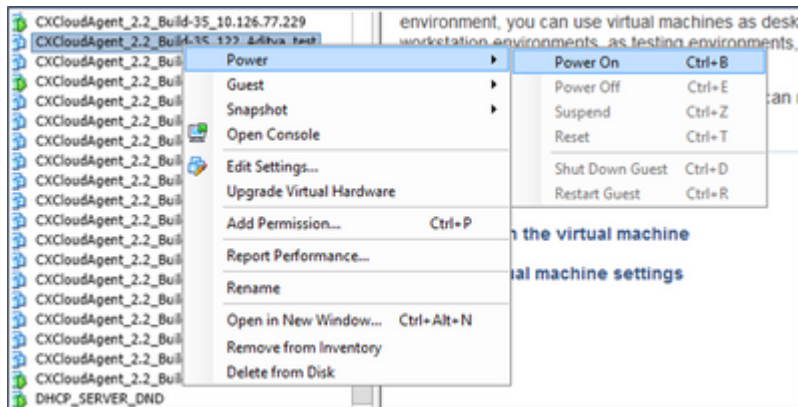
*Venster bevestigen*

3. Klik op **Ja**. De status van de **momentopname omkeren** wordt weergegeven zoals **voltooid** in de lijst Recente taken.



Recente taken

- Klik met de rechtermuisknop op de VM en selecteer **Voeding > Inschakelen** om de VM in te schakelen.



## Security

CX Cloud Agent verzekert de klant van end-to-end beveiliging. De verbinding tussen CX Cloud en CX Cloud Agent is beveiligd met TLS. De standaard SSH-gebruiker van Cloud Agent kan alleen basisbewerkingen uitvoeren.

### Fysieke security

CX Cloud Agent OVA-image implementeren in een beveiligd VMware-serverbedrijf. De OVA wordt veilig gedeeld via het Software Download Center van Cisco. Voor de bootloader (modus met één gebruiker) wordt een willekeurig uniek wachtwoord ingesteld. Gebruikers moeten naar deze [FAQ](#) verwijzen om dit bootloader (single-user mode) wachtwoord in te stellen.

### Account security

Tijdens de implementatie wordt de cxcadmin-gebruikersaccount aangemaakt. Gebruikers worden gedwongen om tijdens de eerste configuratie een wachtwoord in te stellen. CXADMIN-gebruikers/referenties worden gebruikt voor toegang tot zowel de CX Cloud Agent-API's als voor verbinding met het apparaat via SSH.

cxcadmin-gebruikers hebben beperkte toegang met de minste rechten. Het cxcadmin wachtwoord volgt het beveiligingsbeleid en is eenrichtingsgehaakt met een verlooperperiode van 90 dagen. cxcadmin gebruikers kunnen een cxcroot gebruiker maken met behulp van het hulpprogramma genaamd remote account.



cxcadmin gebruikers kunnen wortel voorrechten verkrijgen.

## Netwerk security

De CX Cloud Agent VM is toegankelijk via SSH met cxcadmin-gebruikersreferenties. De inkomende poorten zijn beperkt tot 22 (ssh), 514 (syslog).

## Verificatie

Wachtwoordgebaseerde verificatie: applicatie onderhoudt één gebruiker (cxcadmin) die de gebruiker in staat stelt om te authenticeren en te communiceren met de CX Cloud Agent.

- Acties met root-bevoegdheden op de applicatie via ssh

cxcadmin gebruikers kunnen xcroot gebruiker maken met behulp van een hulpprogramma genaamd Remote account. Dit hulpprogramma toont een versleuteld wachtwoord met RSA/ECB/PKCS1v1\_5 dat alleen kan worden gedecodeerd via het SWIM-portaal (<https://swims.cisco.com/abraxas/decrypt>). Alleen bevoegd personeel heeft toegang tot deze portal. xcroot gebruikers kunnen root privileges verkrijgen met dit gedecrypteerde wachtwoord. Passphrase is slechts twee dagen geldig. cxcadmin gebruikers moeten de account opnieuw aanmaken en het wachtwoord verkrijgen van het SWIM portal na het verstrijken van het wachtwoord.

## Versterking

CX Cloud Agent volgt de normen voor Center of Internet Security hardening.

## Data security

De applicatie CX Cloud Agent slaat geen persoonsgegevens van de klant op.

De credentietoepassing van het apparaat (die als één van de peulen loopt) slaat gecodeerde servergeloofsbriefjes binnen beveiligd gegevensbestand op. De verzamelde gegevens worden in geen enkele vorm binnen het apparaat opgeslagen, behalve tijdelijk wanneer het wordt verwerkt. Telemetriegegevens worden zo snel mogelijk naar CX Cloud geüpload nadat de verzameling is voltooid en worden direct uit de lokale opslag verwijderd nadat is bevestigd dat het uploaden is geslaagd.

## Gegevensoverdracht

Het registratiepakket bevat het vereiste unieke [X.509](#) apparaatcertificaat en de sleutels om een veilige verbinding met Iot Core tot stand te brengen. Met deze agent wordt een beveiligde verbinding tot stand gebracht met Message Queuing Telecommunication Transport (MQT) via Transport Layer Security (TLS) v1.2

## Logboeken en monitoring

Logbestanden bevatten geen enkele vorm van persoonsgegevens (PII). Auditlogboeken bevatten alle beveiligingsgevoelige acties die op het CX Cloud Agent-apparaat worden uitgevoerd.

## Cisco-telemetrieopdrachten

CX Cloud haalt asset telemetry op met behulp van de API's en opdrachten die in de [Cisco Telemetry Commands](#) worden vermeld. Dit document categoriseert opdrachten op basis van hun toepasbaarheid op de



inventaris van Cisco DNA Center, Diagnostic Bridge, Intersight, Compliance Insights, Faults en alle andere telemetriebronnen die door de CX Cloud Agent zijn verzameld.

Gevoelige informatie binnen asset telemetry wordt gemaskeerd voordat ze naar de cloud wordt verzonden. De CX Cloud Agent maskeert gevoelige gegevens voor alle verzamelde activa die telemetry rechtstreeks naar de CX Cloud Agent sturen. Dit omvat wachtwoorden, sleutels, community-strings, gebruikersnamen, enzovoort. Controllers bieden gegevensmaskering voor alle door controller beheerde bedrijfsmiddelen voordat ze deze informatie overdragen aan de CX Cloud Agent. In sommige gevallen kan de door controller beheerde assets telemetry verder worden geanonimiseerd. Raadpleeg de corresponderende [documentatie voor productondersteuning](#) voor meer informatie over het anonimiseren van de telemetry (bijvoorbeeld de sectie [Anonymize Data](#) in de beheerdershandleiding van Cisco DNA Center).

Hoewel de lijst van telemetrieopdrachten niet kan worden aangepast en de gegevensmaskeringsregels niet kunnen worden aangepast, kunnen klanten de toegang van de telemetry CX Cloud van welke activa controleren door gegevensbronnen te specificeren zoals besproken in de [productondersteuningsdocumentatie](#) voor door controllers beheerde apparaten of de sectie Connecting Data Sources van dit document (voor Andere door CX Cloud Agent verzamelde activa).

## Security overzicht

Security functies	Beschrijving
Bootloader-wachtwoord	Voor de bootloader (modus met één gebruiker) wordt een willekeurig uniek wachtwoord ingesteld. Gebruikers moeten <a href="#">FAQ</a> raadplegen om zijn bootloader (single user mode) wachtwoord in te stellen.
Gebruikerstoegang	SSH: <ul style="list-style-type: none"> <li>· Voor toegang tot de applicatie via gebruiker cxcadmin moeten tijdens de installatie inloggegevens worden gemaakt</li> <li>· Toegang tot het apparaat met behulp van xcroot gebruiker vereist dat de aanmeldingsgegevens worden gedecodeerd via het SWIM portal door bevoegd personeel</li> </ul>
Gebruikersaccounts	<ul style="list-style-type: none"> <li>· cxcadmin: standaardgebruikersaccount gemaakt; Gebruiker kan CX Cloud Agent-toepassingsopdrachten uitvoeren met cxcli en heeft de minste rechten op het apparaat; xcroot-gebruiker en het versleutelde wachtwoord worden gegenereerd met cxcadmin-gebruiker</li> <li>· xcroot: cxcadmin kan deze gebruiker creëren met behulp van het hulpprogramma "Remote Account"; Gebruiker kan root-rechten verkrijgen met deze account</li> </ul>
Wachtwoordbeleid voor cxcadmin	<ul style="list-style-type: none"> <li>· Het wachtwoord is een one-way hash met behulp van SHA-256 en wordt veilig opgeslagen</li> <li>· Minimaal acht (8) tekens, die drie van de volgende categorieën bevatten: hoofdletters, kleine letters, getallen en speciale tekens</li> </ul>

<p>Wachtwoordbeleid voor cxcroot</p>	<ul style="list-style-type: none"> <li>· Het wachtwoord van cxcroot is versleuteld met RSA/ECB/PKCS1v1_5</li> <li>· Het gegenereerde wachtwoord moet worden ontsleuteld via de SWIM-portal</li> <li>· De cxcrot-gebruiker en het wachtwoord zijn twee dagen geldig en kunnen worden gegenereerd met cxcadmin-gebruiker</li> </ul>
<p>Wachtwoordbeleid voor inloggen via ssh</p>	<ul style="list-style-type: none"> <li>· Minimaal acht tekens die drie van de volgende categorieën bevatten: hoofdletters, kleine letters, getallen en speciale tekens</li> <li>· Vijf mislukte inlogpogingen vergrendelen de doos voor 30 minuten; Wachtwoord verloopt over 90 dagen</li> </ul>
<p>Poorten</p>	<p>Open inkomende poorten: 514 (syslog) en 22 (ssh)</p>
<p>Data security</p>	<ul style="list-style-type: none"> <li>· Er worden geen klantgegevens opgeslagen</li> <li>· Er worden geen apparaatgegevens opgeslagen</li> <li>· Inloggegevens voor de Cisco DNA Center-server worden versleuteld opgeslagen in de database</li> </ul>

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.