

# Veelgestelde vragen over CX Cloud Agent

## Inhoud

[Inleiding](#)

[Implementatie](#)

[Releases en patches](#)

[Verificatie en proxyconfiguratie](#)

[Secure Shell SSH](#)

[Poorten en services](#)

[Diagnostische scan van CX Cloud Agent](#)

[Systeemlogboeken van CX Cloud Agent](#)

[Probleemoplossing](#)

## Inleiding

In dit document worden verschillende veelgestelde vragen en probleemoplossingsscenario's opgesomd die gebruikers kunnen tegenkomen tijdens het werken met CX Cloud Agent.

## Implementatie

### V. Is URL-omleiding naar [cloudfront.net](https://cloudfront.net) een verwacht gedrag bij verbinding met CX Cloud backend-domein?

A. Ja, voor sommige specifieke implementatiescenario's de omleiding naar [cloudfront.net](https://cloudfront.net) wordt verwacht. Oongebonden toegang moet worden toegestaan met omleiding ingeschakeld op poort 443 voor deze FQDN's.

### V. Kan de gebruiker de nieuwe Cloud Agent met nieuw IP-adres implementeren met de optie "opnieuw installeren"?

A. Ja

### V. Wat zijn de beschikbare bestandsindelingen voor de installatie?

A. OVA en VHD

### V. Wat is de omgeving waarin het installatieprogramma kan worden ingezet?

#### A. Voor EICELLEN

- VMWare ESXi versie 5.5 of hoger
- Oracle Virtual Box 5.2.30 of hoger

#### Voor VHD

- Windows Hypervisor 2012 tot 2016

### V. Kan CX Cloud Agent IP-adres detecteren in een DHCP-omgeving?

**A.** Ja, in het geval van DHCP-omgeving wordt de IP-adrestoewijzing tijdens IP-configuratie uitgevoerd. Verwachte wijziging van het IP-adres voor CX Cloud Agent in de toekomst wordt echter niet ondersteund. Bovendien wordt de klant aanbevolen om het IP-adres voor de Cloud Agent in de DHCP-omgeving te reserveren.

## **V. Ondersteunt CX Cloud Agent zowel IPv4- als IPv6-configuratie?**

**A.** Nee, alleen IPV4 wordt ondersteund.

## **V. Is tijdens de IP-configuratie het IP-adres gevalideerd?**

**A.** Ja, IP-adressyntaxis en dubbele IP-adrestoewijzing worden gevalideerd.

## **V. Wat is de geschatte tijd die nodig is voor de OVA-implementatie en IP-configuratie?**

**A.** De OVA-implementatie is afhankelijk van de snelheid van het netwerk om de gegevens te kopiëren. De IP-configuratie duurt ongeveer 8-10 minuten, inclusief Kubernetes en het maken van containers.

## **Q. Zijn er beperkingen met betrekking tot om het even welk hardwaretype?**

**A.** De hostmachine waarop de OVA wordt geïmplementeerd, moet voldoen aan de vereisten die worden geboden als onderdeel van de CX-portal-instelling. De CX Cloud Agent is getest terwijl VMware/Virtual box draait op een hardware met Intel Xeon E5 processors met vCPU/CPU ratio ingesteld op 2:1. Als er een minder krachtige processor CPU of grotere verhouding wordt gebruikt, kunnen de prestaties afnemen.

## **V. Kunnen we de koppelingscode altijd genereren?**

**A.** Nee, de koppelingscode kan alleen worden gegenereerd als de Cloud Agent niet is geregistreerd.

## **V. Wat zijn de bandbreedtevereisten tussen Cisco DNA-centra (voor maximaal 10 clusters of 20 niet-clusters) en Agent?**

**A.** De bandbreedte is geen beperking wanneer de Agent en Cisco DNA Center zich in hetzelfde LAN/WAN-netwerk in de omgeving van de klant bevinden. De minimaal vereiste netwerkbandbreedte is 2,7 Mbits/sec voor inventarisverzamelingen van 5000 apparaten +13000 access points voor een Agent naar Cisco DNA Center-verbinding. Als syslogs worden verzameld voor L2 inzichten, is de minimum vereiste bandbreedte 3.5 Mbits/sec bedekkingen voor 5000 apparaten +13000 access points voor inventaris, 5000 apparaten syslogs en 2000 apparaten voor scans - allen lopen parallel van Agent.

## **V. Hoe worden de Agent-systemen voor de bewaking van de CX Cloud Agent Virtual Machine (VM) en andere doeleinden benaderd?**

**A.** Syslogs voor Agent VM zijn toegankelijk via de lokale VM-login met de volgende twee paden:

*/var/log/syslog.1 (toegankelijk via cxcadmin en cxcroot logins)*

*/var/log/syslog (benaderd met wortel)*

## **Releases en patches**

## **V. Wat zijn de verschillende soorten versies die worden vermeld voor de upgrade van**

## CX Cloud Agent?

A. Hier getoond zijn de set van de vrijgegeven versies van CX Cloud Agent die worden vermeld:

- A.x.0 (waarbij x de meest recente belangrijke functierelease is, bijvoorbeeld: 1.3.0)
- A.x.y (waar A.x.0 verplicht is en de stijgende verbetering om worden geïnitieerd, x is de recentste productie belangrijkste eigenschapversie, en y is de recentste verbeteringsflard die, bijvoorbeeld: 1.3.1) levend is
- A.x.y-z (waar A.x.0 verplicht is en de stijgende verbetering om worden geïnitieerd, x is de recentste productie belangrijkste eigenschapversie, en y is het recentste verbeteringsflard die levend is, en z is de vlek-flard die een onmiddellijke moeilijke situatie voor een zeer korte tijdspanne is, bijvoorbeeld: 1.3.1-1)

waarbij A een over een periode van 3-5 jaar gespreid vrijkomen op lange termijn is.

## V. Waar vindt u de nieuwste versie van de CX Cloud Agent en hoe u de bestaande CX Cloud Agent kunt upgraden?

A. Ga naar **Beheerinstellingen > Gegevensbronnen**. Klik op **Update** bekijken en voer de instructies uit die op het scherm worden gedeeld.

## Verificatie en proxyconfiguratie

### V. Wat is de standaardgebruiker van de CX Cloud Agent-toepassing?

A. cxcadmin.

### V. Hoe wordt het wachtwoord ingesteld voor de standaardgebruiker?

A. Het wachtwoord wordt ingesteld tijdens de netwerkconfiguratie.

### V. Is er een optie om het wachtwoord na Dag-0 opnieuw in te stellen?

A. De agent biedt geen specifieke optie om het wachtwoord opnieuw in te stellen, maar u kunt de linux-opdrachten gebruiken om het wachtwoord voor cxcadmin te herstellen.

### V. Wat is het wachtwoordbeleid om CX Cloud Agent te configureren?

A. Wachtwoordbeleid:

- Maximale wachtwoordduur is 90 dagen.
- Minimale wachtwoordlengte is 8 tekens.
- Maximale wachtwoordlengte is 127 tekens
- Er moet ten minste één hoofdletters en één kleine letters worden verstrekt
- Moet ten minste één speciaal teken bevatten (bijvoorbeeld !\$%^&\*()\_+|~-=\ "{} []: ";' <> ?, /)
- Deze tekens zijn niet toegestaan
  - Speciale 8-bits tekens (bijvoorbeeld ¬£, âˆšÅ âˆš´, âˆš¥, âˆšë, ¬ø, âˆšü)
  - Spaties
- Het wachtwoord mag niet de laatst gebruikte 10 wachtwoorden zijn
- Mag geen reguliere expressie bevatten, d.w.z.
- Mag niet deze woorden of derivaten bevatten: cisco, sanjose, en sanfran

## **V. Hoe het Grub wachtwoord instellen?**

**A.** Voer de volgende stappen uit om het Grub-wachtwoord in te stellen:

1. Start ssh met gebruiker cxcroot en geef het token op [neem contact op met het ondersteuningsteam voor het cxcroot-token].
2. Voer sudo su uit en geef hetzelfde token op.
3. Voer de opdracht grub-mkpasswd-pbkdf2 uit en stel het Grub-wachtwoord in. De hash van het wachtwoord wordt afgedrukt. Kopieer de content
4. Voer vi uit op het bestand /etc/grub.d/00\_header. Ga naar het einde van het bestand en vervang de hash-uitvoer bij de tekst password\_pbkdf2 root \*\*\*\*\* met de hash voor het wachtwoord die u in stap 3 heeft gekregen.
5. Sla het bestand op met de opdracht :wq!
6. Voer de opdracht update-grub uit.

## **V. Wat is de vervalt termijn voor het wachtwoord van cxcadmin?**

**A.** Het wachtwoord verloopt na 90 dagen.

## **V. Schakelt het systeem de account uit na opeenvolgende niet-succesvolle inlogpogingen?**

**A.** Ja, de account wordt uitgeschakeld na 5 opeenvolgende onsuccesvolle pogingen. De wachttijd bedraagt 30 minuten.

## **V. Hoe kunt u een wachtwoord genereren?**

**A.** Voer de volgende stappen uit:

1. Start ssh en log in als gebruiker cxcadmin
2. Voer de opdracht Remote-account schoonmaken uit -f
3. Voer de opdracht Remote-account uit

## **V. Ondersteunt proxy host zowel hostname als IP?**

**A.** Ja, maar om hostname te gebruiken, moet de gebruiker de DNS IP tijdens netwerkconfiguratie verstrekken.

## **Secure Shell SSH**

### **V. Wat worden de algoritmen ondersteund door ssh shell?**

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

### **V. Hoe inloggen op console?**

**A.** Voer de volgende handelingen uit:

1. Log in als gebruiker cxcadmin
2. Het cxcadmin-wachtwoord opgeven

## Q. Zijn SSH-logins geregistreerd?

A. Ja, ze zijn gelogd als deel van de var/logs/audit/audit.log.

## V. Wat is de tijd voor ongebruikte sessies?

A. Time-out van SSH-sessie treedt op als Cloud Agent vijf (5) minuten niet actief is.

## Poorten en services

### V. Wat zijn de poorten die standaard worden geopend op de CX Cloud Agent?

Deze poorten zijn beschikbaar:

- **Uitgaande poort:** de geïmplementeerde CX Cloud Agent kan verbinding maken met een Cisco-backend zoals aangegeven in de tabel op HTTPS-poort 443 of via een proxy om gegevens naar Cisco te verzenden. De geïmplementeerde CX Cloud Agent kan verbinding maken met Cisco DNA Center op HTTPS-poort 443.

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.cisco.cloud	agent.emea. <a href="#">cisco.cloud</a>	agent.apjc. <a href="#">cisco.cloud</a>
ng.acs.agent.us.cisco.cloud	ng.acs.agent.emea. <a href="#">cisco.cloud</a>	ng.acs.agent.apjc.cisco.cloud

---

**Opmerking:** wanneer EMEA- of APJC-kliënten de Cloud Agent opnieuw installeren, moet het domein agent.us.cisco.cloud in de firewall van de klant worden toegestaan.

De domeinnaam agent.us.cisco.cloud is niet langer nodig na een succesvolle herinstallatie.

---

**Opmerking:** Zorg ervoor dat terugkeerverkeer op haven 443 moet worden toegestaan.

---

- Inbound port: Voor lokaal beheer van de CX Cloud Agent moeten 514(Syslog) en 22(ssh) toegankelijk zijn. De klant moet poort 443 in zijn firewall toestaan om gegevens van CX Cloud te ontvangen.

## Verbinding van CX Cloud Agent met Cisco DNA Center

### V. Wat is het doel en de relatie van Cisco DNA Center met CX Cloud Agent?

A. Cisco DNA Center is de Cloud Agent die de netwerkapparaten van de klant beheert. CX Cloud Agent verzamelt de inventarisgegevens van de apparaten via het geconfigureerde Cisco DNA Center en uploadt de inventarisgegevens die in CX Cloud beschikbaar zijn als *Asset View*™ (Weergave van middelen).

## **V. Waar kan de gebruiker Cisco DNA Center-gegevens over de CX Cloud-agent verstrekken?**

A. Tijdens de installatie van Day 0 - CX Cloud Agent kan de gebruiker de gegevens van Cisco DNA Center toevoegen via het CX Cloud-portal. Daarnaast kunnen gebruikers tijdens dag N operaties extra DNA-centra toevoegen van Admin Settings > Data source.

## **V. Hoeveel Cisco DNA-centra kunnen er worden toegevoegd?**

A. 10 Cisco DNA Center-clusters of 20 Cisco DNA Center-non-clusters.

## **V. Welke rol kan de Cisco DNA Center-gebruiker hebben?**

A. De gebruikersrol kan of **admin** of **waarnemer** zijn.

## **V. Hoe de wijzigingen in CX Agent weer te geven als gevolg van wijzigingen in de verbonden DNA Center-referenties?**

A. Voer de opdracht *cxcli agent modifcatorController uit* vanaf de CX Cloud Agent-console:

Neem contact op met ondersteuning voor eventuele problemen tijdens de update van de referenties voor Cisco DNA Center.

## **V. Hoe worden de gegevens over Cisco DNA Center en seed-bestanden opgeslagen in CX Cloud Agent?**

A. Alle gegevens, inclusief referenties van CX Cloud Agent-verbonden controllers (bijv. Cisco DNA Center) en rechtstreeks verbonden activa (bijv. via seed-bestand, IP-bereik) worden versleuteld met AES-256 en opgeslagen in CX Cloud Agent-database. De CX Cloud Agent-database wordt beschermd met een beveiligde gebruikers-ID en wachtwoord.

## **V. Wat voor soort codering wordt gebruikt bij toegang tot Cisco DNA Center API via CX Cloud Agent?**

A. HTTPS via TLS 1.2 wordt gebruikt voor de communicatie tussen Cisco DNA Center en CX Cloud Agent.

## **V. Welke bewerkingen worden door CX Cloud Agent uitgevoerd op de geïntegreerde Cisco DNA Center Cloud Agent?**

A. CX Cloud Agent verzamelt gegevens die Cisco DNA Center over de netwerkapparaten heeft en gebruikt de opdrachtrunner-interface van Cisco DNA Center om te praten met eindapparaten en CLI-opdrachten uit te voeren (opdracht tonen). Er worden geen opdrachten voor configuratiewijzigingen uitgevoerd.

## **V. Wat zijn de standaardgegevens die van Cisco DNA Center worden verzameld en naar het backend worden geüpload?**

A.

- Netwerkentiteit
- Modules

- show version
- Config
- Informatie over apparaat-image
- Tags

## **V. Wat zijn de extra gegevens die van Cisco DNA Center worden verzameld en naar de Cisco-backend worden geüpload?**

A. Je krijgt [hier](#) alle informatie.

## **V. Hoe worden de inventarisgegevens geüpload naar backend?**

A. CX Cloud Agent uploadt de gegevens via het TLS 1.2-protocol naar een Cisco-back-endserver.

## **V. Wat is de frequentie van het uploaden van de inventaris?**

A. Collection wordt geactiveerd volgens het door de gebruiker ingestelde schema en wordt geüpload naar de Cisco-backend.

## **V. Kan de gebruiker de inventaris opnieuw plannen?**

A. Ja, er is een optie beschikbaar om de planningsinformatie aan te passen via **Beheerinstellingen > Gegevensbronnen**.

## **V. Wanneer vindt de verbindingstime-out plaats tussen Cisco DNA Center en Cloud Agent?**

A. Time-outs zijn als volgt gecategoriseerd:

- Bij eerste verbinding is de time-out maximaal 300 seconden. Als niet binnen maximaal 5 minuten verbinding wordt gemaakt tussen Cisco DNA Center en de Cloud Agent wordt de verbinding beëindigd.
- Voor terugkerende, typische, of updates: de reactieonderbreking is 1800 seconden. Als de respons niet binnen 30 minuten wordt ontvangen of niet kan worden gelezen, wordt de verbinding beëindigd.

## **Diagnostische scan van CX Cloud Agent**

### **V. Welke opdrachten worden op het apparaat uitgevoerd om te worden gescand?**

A. Opdrachten die voor de scan op het apparaat moeten worden uitgevoerd, worden tijdens het scanproces dynamisch bepaald. De reeks opdrachten kan in de loop van de tijd veranderen, zelfs voor hetzelfde apparaat (en niet voor de controle over Diagnostic Scan).

### **V. Waar worden de scanresultaten opgeslagen en geprofileerd?**

A. De gescande resultaten worden opgeslagen en geprofileerd in een Cisco-backend.

### **V. Worden de duplicaten (door hostnaam of IP) in Cisco DNA Center toegevoegd aan de diagnostische scan wanneer de bron van Cisco DNA Center is aangesloten?**

A. Nee, duplicaten worden gefilterd en alleen de unieke apparaten worden geëxtraheerd.

## **V. Wat gebeurt er als een van de opdrachtscans mislukt?**

A. De apparaatscan wordt volledig gestopt en wordt gemarkeerd als niet succesvol.

## **Stysteemlogboeken van CX Cloud Agent**

### **V. Welke gezondheidsinformatie wordt naar de CX Cloud verzonden?**

A. Toepassingslogboeken, podstatus, Cisco DNA Center-gegevens, controlelogboeken, systeemgegevens en hardwaregegevens.

### **V. Welke systeemgegevens en hardwaregegevens worden verzameld?**

A. Uitvoer voorbeeld:

```
system_details":{
  "os_details":{
    "containerRuntimeVersion":"docker://19.3.12",
    "kernelVersion":"5.4.0-47-generiek",
    "kubeProxyVersion":"v1.15.12",
    "kubeletVersion":"v1.15.12",
    "machine-ID":"81edd7df1c1145e7bcc1ab4fe778615f",
    "besturingssysteem":"linux",
    "Beeld":"Ubuntu 20.04.1 LTS",
    "systemUID":"42002151-4131-2ad8-4443-8682911bdadb"
  },
  "hardware_details":{
    "total_cpu":"8",
    "cpu_use":"12,5%",
    "total_memory":"16007MB",
    "free_memory":"994MB",
    "hdd_size":"214G",
    "free_hdd_size":"202G"
  }
}
```

### **V. Hoe worden de gezondheidsgegevens naar backend verzonden?**

A. Met CX Cloud Agent streamt de gezondheidsdienst (servicability) de gegevens naar de Cisco-backend.

### **V. Wat is het beleid van CX Cloud Agent voor het bewaren van gezondheidsgegevens in de backend?**

A. Het beleid van de CX Cloud Agent voor het bewaren van gezondheidsgegevens in de backend is 120 dagen.

### **V. Wat zijn de soorten uploads die beschikbaar zijn?**

A. Er zijn drie soorten uploads beschikbaar:

1. Inventaris uploaden



2. Syslog-uploadtoken
3. Agent Health Upload: 3 dingen als deel van gezondheid upload
  1. Diensten gezondheid - elke 5 minuten
  2. Podlog - elke 1 uur
  3. Auditlogboek - om de 1 uur

## Probleemoplossing

**Probleem:** geen toegang tot het geconfigureerde IP.

**Oplossing:** Voer SSH uit met behulp van geconfigureerd IP. Als de verbindingstijden uitvallen, is de mogelijke oorzaak IP misconfiguratie. Installeer in dit geval opnieuw door een geldig IP-adres te configureren. Dit kan worden gedaan via het portal met de herinstallatieoptie in de Admin Settingspagina.

**Probleem:** Hoe kan ik controleren of de diensten na de registratie actief zijn?

**Oplossing:** Voer de volgende opdrachten uit om te controleren of de peulen actief zijn:

1. ssh naar het geconfigureerde IP-adres als cxcadmin
2. Geef het wachtwoord op
3. Voer deze opdracht uit: *kubectl get pods*

De peulen kunnen in elke toestand zijn zoals draaien, initialiseren of Container maken, maar na 20 minuten moeten de peulen in actieve staat zijn.

Als de staat *niet loopt* of *Peul initialiseert*, controleer de peulbeschrijving met het volgende bevel:

```
kubectl beschrijf pod <podname>
```

De uitvoer bevat informatie over de status van de pod.

**Probleem:** Hoe te verifiëren of SSL-onderschepping is uitgeschakeld bij de klant Proxy?

**Oplossing:** Voer de curl-opdracht uit die hier wordt getoond om de sectie van het servercertificaat te verifiëren. Het antwoord heeft de certificaatgegevens van concsoweb server.

```
curl -v -H "header 'Autorisatie: Basic xxxxxx'https://concsoweb-prd.cisco.com/
```

\* Servercertificaat:

\* onderwerp: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

\* begindatum: 16 feb 11:55:11 2021 GMT

\* Vervaldatum: 16 feb 12:05:00 2022 GMT

\* subjectAltName: host "concsoweb-prd.cisco.com" kwam overeen met cert "concsoweb-prd.cisco.com"

\* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL CA G3

\* SSL-certificaat verifiëren ok.

```
> OPHALEN / HTTP/1.1
```

**Probleem:** kubectl-opdrachten zijn mislukt en toont de fout als "De verbinding met de server X.X.X.X:6443

is geweigerd - heeft u de juiste host of poort opgegeven"

**Oplossing:**

- Controleer op beschikbaarheid van middelen. [voorbeeld: CPU, geheugen].
- Wacht tot de Kubernetes-service start.

**Probleem:** Hoe krijg je de details van de inzamelingsfout voor een commando/apparaat?

**Oplossing:**

- Voer deze opdracht uit: `kubectl get pods` om de naam van de verzamelpod op te halen.
- Voer deze opdracht uit: `kubectl logs` om de opdracht-/apparaatspecifieke gegevens op te halen.

**Probleem:** `kubectl` opdracht werkt niet met fout "[authenticatie.go:64] Kan het verzoek niet authenticeren vanwege een fout: [x509: certificaat is verlopen of is nog niet geldig, x509: certificaat is verlopen of is nog niet geldig]"

**Oplossing:** Start de opdrachten die hier als *Microsoft*-gebruiker worden getoond

```
rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systematisch opnieuw opstarten k3s
kubectl --insecure-skip-tls-verify=true delete geheim -n kube-system k3s-serve
systematisch opnieuw opstarten k3s
```

### Antwoorden bij fouten bij verzameling

De oorzaak van fouten bij verzameling kan een beperking van/probleem met de toegevoegde controller of apparaten in de controller zijn.

In de hier getoonde tabel staat het foutfragment voor gebruikscases die tijdens het inzamelingsproces onder de Collection microservice te zien zijn.

Use case	Logboekfragment in verzamelmicroservice
Het gevraagde apparaat is niet vindbaar in Cisco DNA Center	<pre>{   "commando": "show version",   "status": "Mislukt",   "CommandResponse": "",   "errorMessage": " Geen apparaat gevonden met id 02eb08be- b13f-4d25-9d63-eaf4e882f71a " }</pre>
Het gevraagde apparaat is niet bereikbaar via Cisco DNA Center	<pre>{   "commando": "show version",   "status": "Mislukt",   "CommandResponse": "",   "errorMessage": "Fout opgetreden tijdens het uitvoeren van de opdracht: toon versie\nFout die met apparaat verbindt [Host: 172.21.137.221:22]Geen route naar host: Geen route naar host " }</pre>

Use case	Logboekfragment in verzamelmicroservice
Het gevraagde apparaat is niet bereikbaar via Cisco DNA Center	<pre>{   "commando": "show version",   "status": "Mislukt",   "CommandResponse": "",   "errorMessage": "Fout opgetreden tijdens het uitvoeren van de opdracht: toon versie\nFout bij verbinding met apparaat [Host: X.X.X.X]Verbinding met time-out: /X.X.X.X:22: Time out verbinding: /X.X.X.X:22" }</pre>
De gevraagde opdracht is niet beschikbaar in het apparaat	<pre>{   "commando": "show run-config",   "status": "succes",   "commandoResponse": " Fout tijdens uitvoeren van opdracht: toon run-config\n\nshow run-config\n ^\n% Ongeldige invoer gedetecteerd bij \u0027^\u0027 markering.\n\nXXCT5760#",   "foutbericht": "" }</pre>
Als het gevraagde apparaat geen SSHv2 heeft en Cisco DNA Center probeert het apparaat met SSHv2 te verbinden	<pre>{   "commando": "show version",   "status": "Mislukt",   "CommandResponse": "",   "errorMessage": "Fout opgetreden tijdens het uitvoeren van de opdracht: toon versie\nSSH2 kanaal gesloten: Remote party gebruikt incompatibel protocol, het is niet SSH-2 compatibel." }</pre>
De opdracht is uitgeschakeld in de verzamelmicroservice	<pre>{   "commando": "config paging deactiveren",   "status": "Command_Disabled",   "commandoResponse": "Opdrachtverzameling is uitgeschakeld",   "foutbericht": "" }</pre>
De Command Runner-taak is mislukt en de taak-URL wordt niet door Cisco DNA Center geretourneerd	<pre>{   "commando": "show version",   "status": "Mislukt",   "CommandResponse": "",   "errorMessage": "De taak van de opdrachtuitvoerder is mislukt voor apparaat %s. Taak-URL is leeg." }</pre>
De Command Runner-taak wordt niet gemaakt in Cisco DNA Center	<pre>{   "commando": "show version",</pre>

Use case	Logboekfragment in verzamelmicroservice
	<pre> "status": "Mislukt", "CommandResponse": "", "errorMessage": "De taak van de opdrachtuitvoerder is mislukt voor apparaat %s, aanvraag-URL: %s. Geen taakdetails." } </pre>
<p>De verzamelmicroservice ontvangt geen respons op een Command Runner-aanvraag van Cisco DNA Center</p>	<pre> { "commando": "show version", "status": "Mislukt", "CommandResponse": "", "errorMessage": "De taak van de opdrachtrunner is mislukt voor apparaat %s, aanvraagURL: %s." } </pre>
<p>Cisco DNA Center heeft de taak niet binnen de opgegeven time-out voltooid (5 minuten per opdracht in de verzamelmicroservice)</p>	<pre> { "commando": "show version", "status": "Mislukt", "CommandResponse": "", "errorMessage": "Bedieningstimer. De taak van de opdrachtrunner is mislukt voor apparaat %s, VerzoekURL: %s. Geen voortgangsdetails." } </pre>
<p>De Command Runner-taak mislukt en de bestands-ID voor de door Cisco DNA Center verzonden taak is leeg</p>	<pre> { "commando": "show version", "status": "Mislukt", "CommandResponse": "", "errorMessage": "De taak van de opdrachtuitvoerder is mislukt voor apparaat %s, aanvraag-URL: %s. Bestandsnaam is leeg." } </pre>
<p>De Command Runner-taak mislukt en de tag van de bestands-ID wordt niet door Cisco DNA Center geretourneerd</p>	<pre> { "commando": "show version", "status": "Mislukt", "CommandResponse": "", "errorMessage": "De taak van de opdrachtuitvoerder is mislukt voor apparaat %s, aanvraag-URL: %s. Geen details van bestand-id." } </pre>
<p>Het apparaat komt niet in aanmerking voor uitvoering van een Command Runner-taak</p>	<pre> { "commando": "config paging deactiveren", "status": "Mislukt", "CommandResponse": "", "errorMessage": "Aangevraagde apparaten zijn niet in voorraad, probeer met andere apparaten die in voorraad </pre>

Use case	Logboekfragment in verzamelmicroservice
	<pre>beschikbaar zijn" }</pre>
<p>Command Runner is uitgeschakeld voor de gebruiker</p>	<pre>{ "commando": "show version", "status": "Mislukt", "CommandResponse": "", "foutbericht": "{ \"bericht\": \"Rol heeft geen geldige rechten voor toegang tot API\" }\n" }</pre>

## Antwoorden bij fouten in diagnostische scan

De fout en de oorzaak ervan kunnen worden achterhaald via een van de vermelde componenten.

Wanneer de gebruiker een scan start vanuit de portal, komt dit soms als "mislukt: interne serverfout".

De oorzaak van het probleem kan een van de vermelde onderdelen zijn

- Controlepunt
- Gateway voor netwerkdata
- Aansluiting
- Diagnostische scan
- CX Cloud Agent-microservice [apparaatbeheer, verzameling]
- Cisco DNA Center
- APIX
- Mashery
- PingAccess
- IRONBANK
- IRONBANK GW
- Big Data Broker (BDB)

U kunt de logbestanden als volgt zien:

1. Log in op de CX Cloud Agent-console
  2. ssh met gebruiker cxcadmin en voer het wachtwoord in
  3. Voer deze opdracht uit: `kubectl get pods`
  4. Verkrijg de peulnaam van inzamelings, schakelaar, en servicability.
  5. Om de inzamelings, de schakelaar, en de servicability microservice logboeken te verifiëren
- Voer deze opdracht uit: `kubectl logs`
  - Voer deze opdracht uit: `kubectl logs`
  - Voer deze opdracht uit: `kubectl logs`

De hier getoonde tabel toont het foutfragment dat wordt gezien onder Collectie microservice- en servicability microservice-logbestanden die optreden als gevolg van de problemen/beperkingen met de

componenten.

Use case	Logboekfragment in verzamelmicroservice
<p>Het apparaat kan bereikbaar en ondersteund worden, maar de opdrachten die op dat apparaat uitgevoerd moeten worden, staan in een blok op de Collection microservice vermeld</p>	<pre>{   "commando": "config paging deactiveren",   "status": "Command_Disabled",   "commandoResponse": "Opdrachtverzameling is uitgeschakeld", }</pre>
<p>Het te scannen apparaat is niet beschikbaar.</p> <p>Dit kan gebeuren wanneer er een synchronisatieprobleem is tussen de componenten, zoals portal, diagnostische scan, CX-component en Cisco DNA Center.</p>	<p>Geen apparaat gevonden met id 02eb08be-b13f-4d25-9d63-eaf4e882f71a</p>
<p>Het te scannen apparaat is bezet (in een scenario), waarbij hetzelfde apparaat deel uitmaakt van een andere taak en er geen parallele aanvragen van Cisco DNA Center voor het apparaat worden verwerkt</p>	<p>Alle gevraagde apparaten worden al door een opdrachtrunner in een andere sessie opgezocht. Probeer andere apparaten</p>
<p>Het apparaat wordt niet ondersteund voor scans.</p>	<p>De gevraagde apparaten zijn niet in voorraad, probeer met andere apparaten beschikbaar in inventaris</p>
<p>Als het apparaat heeft geprobeerd om te scannen onbereikbaar is</p>	<p>"Fout bij uitvoeren van opdracht: toon udi\nFout bij verbinding met apparaat [Host: x.x.x.x:22] Geen route naar host: Geen route naar host</p>
<p>Cisco DNA Center is niet bereikbaar via de Cloud Agent, of de verzamelmicroservice van de Cloud Agent ontvangt geen respons op een Command Runner-verzoek van Cisco DNA Center.</p>	<pre>{   "commando": "show version",   "status": "Mislukt",   "CommandResponse": "",   "errorMessage": "De taak van de opdrachtrunner is mislukt voor apparaat %s, aanvraagURL: %s." }</pre>

Use case	Logboekfragment Control Point Agent-microservice
<p>In de scanaanvraag ontbreken planningsgegevens.</p>	<p>Uitvoeren aanvraag mislukt</p> <pre>{"message":"23502: null value in kolom \ "schema\" overtreedt niet-null beperking"}</pre>

Use case	Logboekfragment Control Point Agent-microservice
In de scanaanvraag ontbreken apparaatgegevens.	Scanbeleid is niet gemaakt. Geen geldige apparaten in het verzoek
De verbinding tussen de Control Point Agent en connectiviteit is verbroken.	Uitvoeren aanvraag mislukt
Het gevraagde scanapparaat is niet beschikbaar in diagnostische scans	Verzenden van aanvraag voor scan mislukt. Reden = {"bericht": "Apparaat met Hostname=x.x.x" is niet gevonden"}

## 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.