CX Cloud Agent - Häufig gestellte Fragen

Inhalt

[Einleitung](#)
[Bereitstellung](#)
[Versionen und Patches](#)
[Authentifizierung und Proxy-Konfiguration](#)
[Secure Shell (SSH)](#)
[Ports und Services](#)
[CX Cloud Agent verwendet Diagnosescan](#)
[CX Cloud Agent-Systemprotokolle](#)
[Fehlerbehebung](#)

Einleitung

In diesem Dokument sind verschiedene häufig gestellte Fragen und Fehlerbehebungsszenarien aufgeführt, denen Benutzer bei der Arbeit mit CX Cloud Agent begegnen können.

Bereitstellung

Frage: Ist die URL-Umleitung zu cloudfront.net ein erwartetes Verhalten bei der Verbindung mit der CX Cloud-Backend-Domäne?

Antwort: Ja. Bei einigen speziellen Bereitstellungsszenarien wird die Umleitung an cloudfront.net wird erwartet. OUngebundener Zugriff sollte mit aktivierter Umleitung an Port 443 für diese FQDNs zulässig sein.

Frage: Kann der Benutzer mit der Option "Re-install" den neuen Cloud Agent mit neuer IP-Adresse bereitstellen?

Antwort: Ja

F. Welche Dateiformate stehen für die Installation zur Verfügung?

A. OVA und VHD

Frage: In welcher Umgebung kann das Installationsprogramm bereitgestellt werden?

Antwort: für OVA

- VMWare ESXi Version 5.5 oder höher
- Oracle Virtual Box 5.2.30 oder höher

Für VHD

- Windows-Hypervisor 2012 bis 2016

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

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

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

Antwort: Nein, nur IPV4 wird unterstützt.

Frage: Wird die IP-Adresse während der IP-Konfiguration validiert?

Antwort: Ja, die IP-Adresssyntax und die Zuweisung doppelter IP-Adressen werden validiert.

Frage: Wie viel Zeit wird in etwa für die OVA-Bereitstellung und die IP-Konfiguration benötigt?

Antwort: Die OVA-Bereitstellung hängt von der Geschwindigkeit des Netzwerks ab, in das die Daten kopiert werden. Die IP-Konfiguration dauert etwa 8 bis 10 Minuten und umfasst Kubernetes und Containererstellungen.

Frage: Gibt es Einschränkungen in Bezug auf Hardwaretypen?

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

Frage: Können wir den Kopplungscode jederzeit generieren?

Antwort: Nein, der Kopplungscode kann nur generiert werden, wenn der Cloud Agent nicht registriert ist.

Frage: Welche Bandbreitenanforderungen bestehen zwischen Cisco DNA Centern (für bis zu 10 Cluster oder 20 Nicht-Cluster) und Agenten?

Antwort: Die Bandbreite ist nicht eingeschränkt, wenn sich der Agent und das Cisco DNA Center in der Kundenumgebung im selben LAN/WAN-Netzwerk befinden. Die mindestens erforderliche Netzwerkbandbreite beträgt 2,7 Mbit/s für eine Bestandserfassung mit 5.000 Geräten +13000 Access Points für eine Verbindung zwischen Agent und Cisco DNA Center. Wenn Syslogs für L2-Einblicke erfasst werden, beträgt die erforderliche Mindestbandbreite 3,5 Mbit/s für die Abdeckung von 5.000 Geräten +13000 Access Points für Bestand, 5.000 Geräte Syslogs und 2.000 Geräten für Scans - alle parallel von Agent ausgeführt.

Frage: Wie wird auf die Agenten-Syslogs zur Überwachung der CX Cloud Agent Virtual Machine (VM) und anderer Zwecke zugegriffen?

Antwort: Der Zugriff auf Syslogs für Agent VM erfolgt über die lokale VM-Anmeldung über die folgenden beiden Pfade:

/var/log/syslog.1 (Zugriff über cxcadmin- und cxcroot-Anmeldedaten)

/var/log/syslog (Zugriff über Root)

Versionen und Patches

Frage: Welche verschiedenen Versionen werden für das Upgrade von CX Cloud Agent aufgeführt?

Antwort: Hier sehen Sie die veröffentlichten Versionen von CX Cloud Agent, die aufgeführt sind:

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

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

Frage: Wo finden Sie die neueste Version von CX Cloud Agent und wie können Sie ein Upgrade des vorhandenen CX Cloud Agent durchführen?

Antwort: Gehen Sie zu **Admin Settings** > **Data Sources**. Klicken Sie auf **Update anzeigen**, und führen Sie die auf dem Bildschirm freigegebenen Anweisungen aus.

Authentifizierung und Proxy-Konfiguration

Frage: Wie lautet der Standardbenutzer der CX Cloud Agent-Anwendung?

A. cxcadmin

Frage: Wie wird das Kennwort für den Standardbenutzer festgelegt?

Antwort: Das Kennwort wird während der Netzwerkkonfiguration festgelegt.

Frage: Gibt es eine Möglichkeit, das Kennwort nach Tag 0 zurückzusetzen?

Antwort: Der Agent stellt keine spezielle Option zum Zurücksetzen des Kennworts bereit, Sie können jedoch die Linux-Befehle verwenden, um das Kennwort für cxcadmin zurückzusetzen.

Frage: Welche Kennwortrichtlinien werden zum Konfigurieren von CX Cloud Agent verwendet?

Antwort: Kennwortrichtlinien sind:

- Das maximale Kennwortalter (Länge) ist auf 90 Tage festgelegt
- Das minimale Kennwortalter (Länge) ist auf 8 festgelegt
- Die maximale Kennwortlänge beträgt 127 Zeichen
- Mindestens ein Groß- und ein Kleinbuchstabe sind vorzusehen
- Muss mindestens ein Sonderzeichen enthalten (beispielsweise !$%^&*()_+|~-=\`{}[]:";'<>?,/)
- Diese Zeichen sind nicht zulässig.
    - 8-Bit-Sonderzeichen (Beispiel: ¬£, âˆšÅ âˆš´, âˆš¥, âˆšë, ¬ø, âˆšü)

    - Leerzeichen
- Das Kennwort darf nicht die zuletzt verwendeten 10 Kennwörter sein.
- Darf keinen regulären Ausdruck enthalten, d. h.
- Darf folgende Wörter oder Derivate nicht enthalten: cisco, sanjose und sanfran

Frage: Wie setzt man das Grub-Passwort?

Antwort: Um das Grub-Kennwort festzulegen, gehen Sie wie folgt vor:

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

Frage: Wie lange läuft das Kennwort von cxcadmin ab?

Antwort: Das Kennwort läuft nach 90 Tagen ab.

Frage: Deaktiviert das System das Konto nach aufeinander folgenden erfolglosen Anmeldeversuchen?

Antwort: Ja, das Konto wird nach fünf aufeinander folgenden erfolglosen Versuchen deaktiviert. Die Sperrzeit beträgt 30 Minuten.

Frage: Wie wird eine Passphrase generiert?

Antwort: Führen Sie die folgenden Schritte aus:

1. Führen Sie ssh aus, und melden Sie sich als Benutzer cxcadmin an.
2. Führen Sie den Befehl remoteaccount cleanup -f aus.
3. Ausführen des Befehls remoteAccount erstellen

Frage: Unterstützt der Proxy-Host Hostname und IP?

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

Secure Shell (SSH)

Frage: Welche Chiffren werden von der SSH Shell unterstützt?

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

Frage: Wie melde ich mich an der Konsole an?

Antwort: Führen Sie Folgendes aus:

1. Melden Sie sich als Benutzer cxcadmin an
2. Geben Sie das cxcadmin-Kennwort ein.

Frage: Werden SSH-Anmeldungen protokolliert?

Antwort: Ja, sie werden als Teil von var/logs/audit/audit.log protokolliert.

Frage: Wann ist die Sitzung beendet?

Antwort: Ein Timeout für SSH-Sitzungen tritt auf, wenn der Cloud-Agent fünf (5) Minuten lang inaktiv ist.

Ports und Services

Frage: Welche Ports werden standardmäßig auf dem CX Cloud Agent geöffnet?

Diese Ports sind verfügbar:

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

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

---

Hinweis: Wenn EMEA- oder APJC-Kunden den Cloud Agent neu installieren, muss zusätzlich zu den aufgeführten Domänen die Domäne agent.us.csco.cloud in der Kunden-Firewall zugelassen sein. Die Domain agent.us.csco.cloud wird nach erfolgreicher Neuinstallation nicht mehr benötigt.

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

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

CX Cloud Agent-Verbindung mit Cisco DNA Center

F. Welchen Zweck und welche Beziehung hat Cisco DNA Center zu CX Cloud Agent?

Antwort: Cisco DNA Center ist der Cloud Agent, der die Netzwerkgeräte am Kundenstandort verwaltet. CX Cloud Agent sammelt die Bestandsinformationen der Geräte über das konfigurierte Cisco DNA Center und lädt die Bestandsinformationen hoch, die als "Ressourcenansicht" in CX Cloud verfügbar sind.

Frage: Wo kann der Benutzer Cisco DNA Center-Details zum CX Cloud-Agenten angeben?

Antwort: Während der Einrichtung von Day 0 - CX Cloud Agent kann der Benutzer die Details zum Cisco DNA Center über das CX Cloud-Portal hinzufügen. Darüber hinaus können Benutzer während des Day N-Betriebs zusätzliche DNA-Zentren hinzufügen von Admin Settings > Data source.

Frage: Wie viele Cisco DNA Center können hinzugefügt werden?

Antwort: Entweder 10 Cisco DNA Center-Cluster oder 20 Cisco DNA Center-Nicht-Cluster.

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

Antwort: Die Benutzerrolle kann entweder **admin** oder **observer** sein.

F. Wie können die Änderungen in CX Agent aufgrund von Änderungen in den verbundenen DNA Center-Anmeldeinformationen widergespiegelt werden?

A. Führen Sie den Befehl *cxcli agent changeController* von der CX Cloud Agent-Konsole aus:

Wenden Sie sich bei Problemen während der Aktualisierung der Cisco DNA Center-Anmeldeinformationen an den Support.

F. Wie werden die Details zu Cisco DNA Center und Seed-Dateien in CX Cloud Agent gespeichert?

Antwort: Alle Daten, einschließlich der Anmeldedaten der mit CX Cloud Agent verbundenen Controller (z. B. Cisco DNA Center) und der direkt verbundenen Ressourcen (z. B. über Seed-Datei, IP-Bereich) werden mit AES-256 verschlüsselt und in der CX Cloud Agent-Datenbank gespeichert. Die Datenbank des CX Cloud Agent ist mit einer sicheren Benutzer-ID und einem Kennwort geschützt.

Frage: Welche Art von Verschlüsselung wird beim Zugriff auf die Cisco DNA Center-API von CX Cloud Agent verwendet?

Antwort: HTTPS über TLS 1.2 wird für die Kommunikation zwischen Cisco DNA Center und CX Cloud Agent verwendet.

Frage: Welche Vorgänge führt CX Cloud Agent auf dem integrierten Cisco DNA Center Cloud Agent aus?

Antwort: CX Cloud Agent sammelt Daten, die Cisco DNA Center über die Netzwerkgeräte hat, und verwendet die Befehlsrunner-Schnittstelle von Cisco DNA Center, um mit Endgeräten zu kommunizieren und CLI-Befehle auszuführen (Befehl show). Es werden keine Konfigurationsänderungsbefehle ausgeführt.

Frage: Welche Standarddaten werden vom Cisco DNA Center gesammelt und an das

Backend hochgeladen?

Antwort:

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

Frage: Welche zusätzlichen Daten werden vom Cisco DNA Center gesammelt und an das Cisco Backend übertragen?

Antwort: Alle Informationen erhalten Sie hier.

Frage: Wie werden die Bestandsdaten in das Backend hochgeladen?

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

Frage: Wie oft wird ein Inventar hochgeladen?

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

Frage: Kann der Benutzer den Bestand neu planen?

Antwort: Ja, es ist eine Option zum Ändern der Zeitplaninformationen unter **Admin Settings > Data Sources (Admin-Einstellungen > Datenquellen) verfügbar**.

Frage: Wann tritt die Verbindungs-Zeitüberschreitung zwischen Cisco DNA Center und Cloud Agent auf?

Antwort: Timeouts werden wie folgt kategorisiert:

- Bei der Erstverbindung beträgt das Timeout maximal 300 Sekunden. Wenn innerhalb von maximal 5 Minuten keine Verbindung zwischen Cisco DNA Center und Cloud Agent hergestellt wird, wird die Verbindung beendet.
- Bei wiederkehrenden, typischen oder Aktualisierungen beträgt das Zeitlimit für Antworten 1800 Sekunden. Wenn die Antwort nicht innerhalb von 30 Minuten empfangen wird oder nicht gelesen werden kann, wird die Verbindung beendet.

CX Cloud Agent verwendet Diagnosescan

F. Welche Befehle werden auf dem Gerät zum Scannen ausgeführt?

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

Frage: Wo werden die Scan-Ergebnisse gespeichert und in einem Profil festgehalten?

Antwort: Die gescannten Ergebnisse werden im Cisco Backend gespeichert und in einem Profil festgehalten.

Frage: Werden die Duplikate (nach Hostname oder IP) im Cisco DNA Center dem Diagnosescan hinzugefügt, wenn die Cisco DNA Center-Quelle angeschlossen ist?

Antwort: Nein, Duplikate werden gefiltert und nur die einzelnen Geräte werden extrahiert.

F. Was passiert, wenn einer der Befehlsscans fehlschlägt?

Antwort: Der Gerätescan wird vollständig gestoppt und als nicht erfolgreich markiert.

CX Cloud Agent-Systemprotokolle

Frage: Welche Integritätsinformationen werden an die CX-Cloud gesendet?

Antwort: Anwendungsprotokolle, Pod-Status, Details zum Cisco DNA Center, Audit-Protokolle, System- und Hardwaredetails.

F. Welche System- und Hardwaredetails werden erfasst?

Antwort: Beispiel für das Ergebnis:

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

F. Wie werden die Gesundheitsdaten an das Backend gesendet?

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

Frage: Welche Aufbewahrungsrichtlinie für das Integritätsdatenprotokoll des CX

Cloud Agent befindet sich im Backend?

Antwort: Die Aufbewahrungsrichtlinie für das Integritätsdatenprotokoll des CX Cloud Agent im Backend beträgt 120 Tage.

Frage: Welche Arten von Uploads sind verfügbar?

Antwort: Es stehen drei Upload-Typen zur Verfügung.

1. Bestands-Upload
2. Syslog-Upload
3. Agent Health-Upload: 3 Dinge als Teil des Health-Uploads
    1. Service-Zustand - alle 5 Minuten
    2. Podlog - alle 1 Stunde
    3. Audit-Protokoll - alle 1 Stunde

Fehlerbehebung

Problem: Kein Zugriff auf die konfigurierte IP-Adresse.

Lösung: SSH mit konfigurierter IP ausführen. Bei einer Verbindungsunterbrechung liegt der mögliche Grund in einer falschen IP-Konfiguration. Führen Sie in diesem Fall eine Neuinstallation durch, indem Sie eine gültige IP-Adresse konfigurieren. Dies kann über das Portal mit der im bereitgestellten Option zur Neuinstallation Admin SettingsSeite.

Problem: Wie kann überprüft werden, ob die Services nach der Registrierung verfügbar sind und ausgeführt werden?

Lösung: Führen Sie die folgenden Befehle aus, um zu überprüfen, ob die PODs betriebsbereit sind:

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

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

Wenn der Status *nicht ausgeführt wird* oder *kein Pod initialisiert wird*, überprüfen Sie die POD-Beschreibung mit dem folgenden Befehl:

kubectl description pod <podname>

Die Ausgabe enthält die Informationen zum Podstatus.

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

curl -v â€”header 'Authorization: Basic xxxxxx' https://concsoweb-prd.cisco.com/

* Serverzertifikat:

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

* Startdatum: 16. Februar 11:55:11 Uhr GMT

* Gültig bis: 16.02.2022 12:05:00 GMT

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

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

* SSL-Zertifikat überprüft OK.

> GET/HTTP/1.1

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

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

Problem: Wie erhalte ich die Details eines Erfassungsfehlers für einen Befehl/ein Gerät?

Lösung:

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

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

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

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

Reaktionen auf Erfassungsfehler

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

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

Anwendungsfall	**Protokoll-Snippet im Microservice "Erfassung"**
Wenn das angeforderte Gerät in Cisco DNA Center nicht gefunden wird	{ "Befehl": "Version anzeigen", "status": "Failed", "commandResponse": "", "errorMessage": " Kein Gerät mit der ID 02eb08be-b13f-4d25-

Anwendungsfall	**Protokoll-Snippet im Microservice "Erfassung"**
	9d63-eaf4e882f71a gefunden " }

Wenn das angeforderte Gerät nicht über Cisco DNA Center erreichbar ist	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler beim Ausführen des Befehls: show version\nFehler beim Herstellen der Verbindung mit dem Gerät [Host: 172.21.137.221:22]No route to host: No route to host "
	}

Wenn das angeforderte Gerät nicht über Cisco DNA Center erreichbar ist	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler beim Ausführen des Befehls: show version\nFehler beim Herstellen der Verbindung mit dem Gerät [Host: X.X.X.X.X]Zeitüberschreitung der Verbindung: /X.X.X.X:22 : Zeitüberschreitung der Verbindung: /X.X.X.X:22"
	}

Wenn der angeforderte Befehl im Gerät nicht verfügbar ist	{
	"Befehl": "show run-config",
	"Status": "Erfolg",
	"commandResponse": " Fehler beim Ausführen des Befehls: show run-config\n\nshow run-config\n ^\n% Ungültige Eingabe bei Marker \u0027^\u0027 erkannt.\n\nXXCT5760#",
	"errorMessage": ""
	}

Wenn das angeforderte Gerät nicht über SSHv2 verfügt und Cisco DNA Center versucht, das Gerät mit SSHv2 zu verbinden	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler beim Ausführen des Befehls : show version\nSSH2 channel closed : Remote-Teilnehmer verwendet inkompatibles Protokoll, nicht SSH-2-kompatibel."
	}

Wenn der Befehl im Microservice "Erfassung" deaktiviert ist	{
	"command": "config paging disable",
	"Status": "Command_Disabled",
	"commandResponse": "Befehlssammlung ist deaktiviert",
	"errorMessage": ""
	}

Anwendungsfall	**Protokoll-Snippet im Microservice "Erfassung"**

Wenn die Command Runner-Aufgabe fehlgeschlagen ist und die Aufgaben-URL nicht von Cisco DNA Center zurückgegeben wird	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler beim Befehlsrunner-Task für Gerät %s. Task-URL ist leer."
	}

Wenn die Command Runner-Aufgabe in Cisco DNA Center nicht erstellt werden konnte	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler bei der Befehlsausführeraufgabe für Gerät %s, RequestURL: %s. Keine Aufgabendetails."
	}

Wenn der Microservice "Erfassung" keine Antwort auf eine Command Runner-Anfrage vom Cisco DNA Center empfängt	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler bei der Befehlsausführeraufgabe für Gerät %s, RequestURL: %s."
	}

Wenn Cisco DNA Center die Aufgabe nicht innerhalb der konfigurierten Zeitüberschreitung abschließt
(5 Minuten pro Befehl im Microservice "Erfassung")
	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage" (Fehlermeldung): "Operation Timeout. Fehler bei der Befehlsausführeraufgabe für Gerät %s, Anforderungs-URL: %s. Keine Fortschrittsdetails."
	}

Wenn die Command Runner-Aufgabe fehlgeschlagen ist und die Datei-ID nicht von Cisco DNA Center übermittelt wird	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Fehler bei der Befehlsausführeraufgabe für Gerät %s, RequestURL: %s. Datei-ID ist leer."
	}

Wenn die Command Runner-Aufgabe fehlschlägt und das Datei-ID-Tag nicht von Cisco DNA Center zurückgegeben wird	{ "Befehl": "Version anzeigen", "status": "Failed", "commandResponse": "", "errorMessage": "Fehler bei der Befehlsausführeraufgabe für

Anwendungsfall	**Protokoll-Snippet im Microservice "Erfassung"**
	Gerät %s, RequestURL: %s. Keine Datei-ID-Details." }

Wenn das Gerät nicht für die Ausführung durch den Command Runner geeignet ist	{
	"command": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage" (Fehlermeldung): "Angeforderte Geräte befinden sich nicht im Bestand. Versuchen Sie es mit anderen im Bestand verfügbaren Geräten."
	}

Wenn der Befehl "runner" für den Benutzer deaktiviert ist	{
	"Befehl": "Version anzeigen",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"Die Rolle verfügt nicht über gültige Berechtigungen für den Zugriff auf die API\"}\n"
	}

Reaktionen auf Diagnosescanfehler

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

Wenn der Benutzer eine Suche vom Portal aus startet, wird sie gelegentlich als "fehlgeschlagen: Interner Serverfehler" angezeigt.

Die Ursache des Problems kann eine der aufgeführten Komponenten sein

- Kontrollpunkt
- Netzwerk-Datengateway
- Anschluss
- Diagnosescan
- CX Cloud Agent Microservice [Gerätemanager, Erfassung]
- Cisco DNA Center
- APIX
- Mashery
- Ping-Zugriff
- IRONBANK
- IRONBANK GW
- Big Data Broker (BDB)

Protokolle anzeigen:

1. Melden Sie sich bei der CX Cloud Agent-Konsole an.
2. Geben Sie das Kennwort an, um sich über SSH mit den Anmeldeinformationen des Benutzers cxcadmin anzumelden.
3. Durchführung kubectl get pods

4. Rufen Sie den PoD-Namen für Sammlung, Anschluss und Betriebsfähigkeit ab.
5. So überprüfen Sie die Microservice-Protokolle für Erfassung, Anschluss und Wartung

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

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

Anwendungsfall	**Protokoll-Snippet im Microservice "Erfassung"**

Das Gerät kann erreichbar sein und wird unterstützt, aber die Befehle, die auf diesem Gerät ausgeführt werden sollen, werden im Collection-Microservice blockiert.	{
	"command": "config paging disable",
	"Status": "Command_Disabled",
	"commandResponse": "Befehlssammlung ist deaktiviert",
	}

Wenn das zu scannende Gerät nicht verfügbar ist. Dazu kommt es, wenn ein Synchronisierungsproblem zwischen den Komponenten auftritt, z. B. zwischen Portal, Diagnosescan, CX-Komponente und Cisco DNA Center.	Kein Gerät mit der ID 02eb08be-b13f-4d25-9d63-eaf4e882f71a gefunden
Wenn das zu scannende Gerät ausgelastet ist, wenn dasselbe Gerät Teil eines anderen Auftrags war und keine parallelen Anfragen von Cisco DNA Center für das Gerät verarbeitet werden	Alle angeforderten Geräte werden bereits in einer anderen Sitzung vom Befehlsrunner abgefragt. Versuchen Sie es mit anderen Geräten.
Wenn das Gerät den Scanvorgang nicht unterstützt.	Die angeforderten Geräte befinden sich nicht im Bestand. Versuchen Sie es mit anderen im Bestand verfügbaren Geräten.
Wenn das Gerät nicht erreichbar ist	"Fehler beim Ausführen des Befehls: show udi\nFehler beim Herstellen der Verbindung mit dem Gerät [Host: x.x.x.x:22] Keine Route zum Host: Keine Route zum Host
Wenn Cisco DNA Center über den Cloud Agent nicht erreichbar ist oder der Microservice "Erfassung" des Cloud Agent	{ "Befehl": "Version anzeigen", "status": "Failed",

Anwendungsfall	**Protokoll-Snippet im Microservice "Erfassung"**
keine Antwort auf eine Command Runner-Anfrage vom Cisco DNA Center erhält.	"commandResponse": "", "errorMessage": "Fehler bei der Befehlsausführeraufgabe für Gerät %s, RequestURL: %s." }

Anwendungsfall	**Protokoll-Snippet im Microservice "Kontrollpunkt-Agent"**
Wenn bei der Scananfrage Zeitplandetails fehlen.	Anfrage konnte nicht ausgeführt werden {"message":"23502: NULL-Wert in Spalte \"schedule\" verletzt Nicht-Null-Einschränkung"}
Wenn bei der Scananfrage Gerätedetails fehlen.	Fehler beim Erstellen der Scanrichtlinie. Keine gültigen Geräte in der Anforderung
Wenn die Verbindung zwischen CPA und Netzwerkverbindungen unterbrochen ist.	Anfrage konnte nicht ausgeführt werden
Wenn das angeforderte Gerät in den Diagnosescans nicht zum Scannen verfügbar ist.	Fehler beim Übermitteln der Scananforderung. Ursache = {\"Nachricht\":\"Gerät mit Hostname=x.x.x.x' wurde nicht gefunden\"}

Informationen zu dieser Übersetzung

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