Orchestrierung für UCCE konfigurieren

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren der Contact Center Enterprise-Orchestrierung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Unified Contact Center Enterprise (UCCE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x
- Cisco Voice Portal (CVP) 12.x
- Finesse 12.x
- Cisco Unified Intelligence Center (CUIC) 12.x
- Virtual Voice Browser (VVB) 12.x

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cloud Connect 12.6(1) ES3
- UCCE 12.5(1)
- Finesse 12,5 (1)
- CUIC 12.5(1)
- CVP 12.5(1)
- VVB 12,5 (1)

Hinweis: CUIC bezieht sich im gesamten Dokument auf gleichzeitig ausgeführte Installationen sowie auf eigenständige Installationen von CUIC, Live Data (LD) und Identity Server (IDS). Nur wenn eine

---

Anweisung für eine Unterkomponente spezifisch ist, wird auf diese Komponente verwiesen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Versionsanforderungen

UCCE/PCCE 12.5(1) (entweder)

- ES66 (ES55 ist eine obligatorische Installation vor der Installation von ES66)
- UCCE 12.5(2) MR

UCCE/PCCE 12.6(1)

- Keine zusätzlichen Anforderungen

Cloud Connect-Version: 12.6(1)

- ES3

Finesse, CUIC, VVB: 12.5(1)

- ucos.orchestration.enable-12.5.1.cop.sgn
- ucos.keymanagement.cop.sgn

Finesse, CUIC, VVB: 12.6(1)

- ucos.keymanagement.cop.sgn

CVP 12.5(1)

- ES23

CVP 12.6(1)

- Keine zusätzlichen Anforderungen

Besondere Hinweise für Cloud Connect-Upgrades:

Hinweis: Wenn Sie ein Upgrade von Cloud Connect von 12.5 auf 12.6 durchführen, müssen Sie zunächst ucos.keymanagement.cop.sgn installieren. Das Upgrade schlägt fehl, wenn dies nicht durchgeführt wird.

Hinweis: Wenn Sie ein Upgrade von Cloud Connect von 12.5 auf 12.6 durchführen, müssen Sie den Festplattenspeicher von 146 GB auf 246 GB erhöhen. Wenn dieser Schritt vor dem Upgrade verpasst wurde, gehen Sie wie folgt vor:
Schritt 1: Beenden Sie den Cloud Connect-Server.
Schritt 2: Erweitern Sie die Festplatte in vSphere auf 246 GB.
Schritt 3: Starten des Cloud Connect-Servers
VOS erweitert die Partitionen automatisch. Dadurch wird sichergestellt, dass die heruntergeladenen Updates nicht den Speicherplatzmangel auf der gemeinsamen Partition verursachen.

Überblick

CCE-Orchestrierung wird ab Cloud Connect 12.6(1) unterstützt.

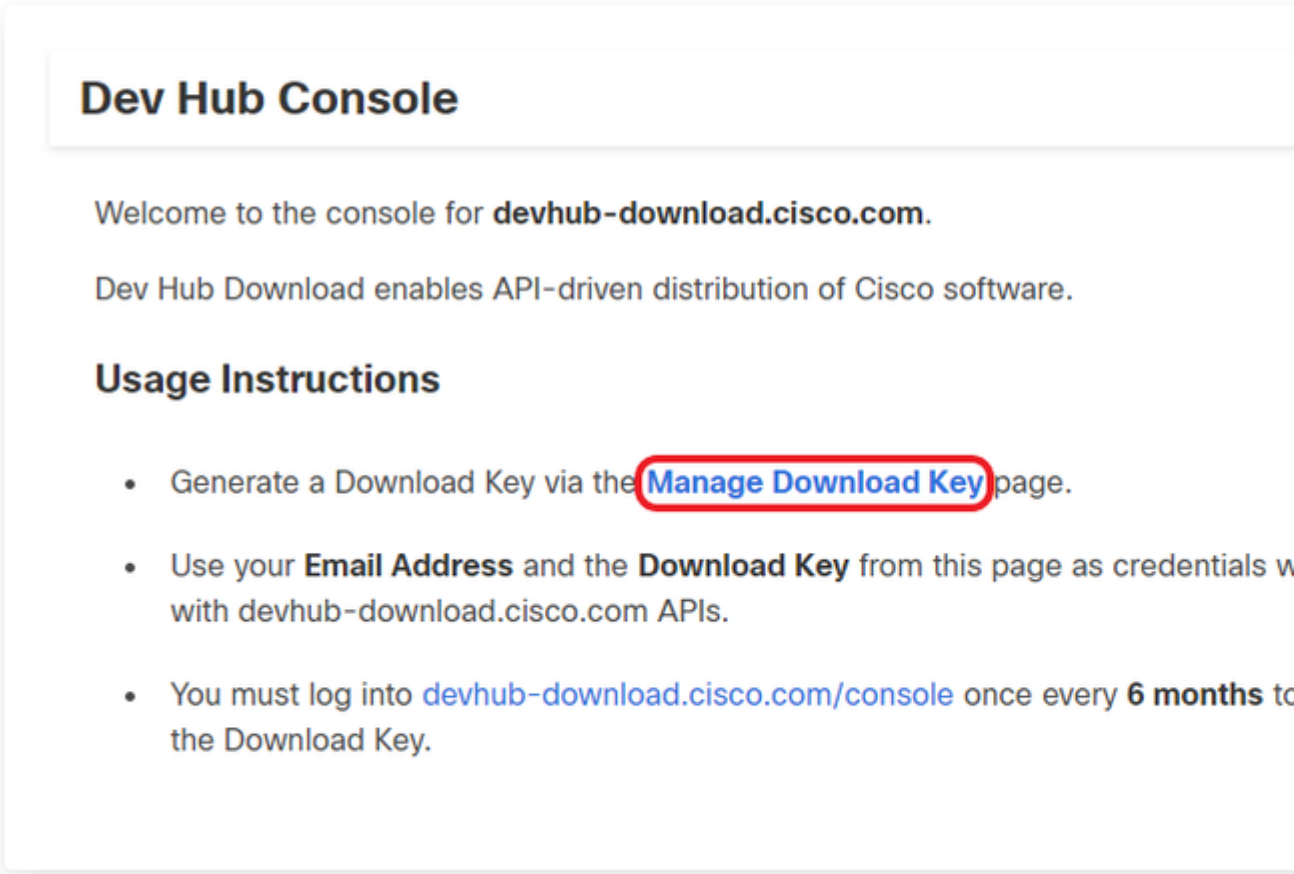
Cloud Connect-Server Version 12.6 (1) unterstützt die Orchestrierung in den folgenden Szenarien:

- CCE 12.5 ES/COP und Windows Updates können über 12.6 Cloud Connect-Server orchestriert werden
- CCE 12.5- bis 12.6-Software-Upgrades können über 12.6 Cloud Connect-Server orchestriert werden

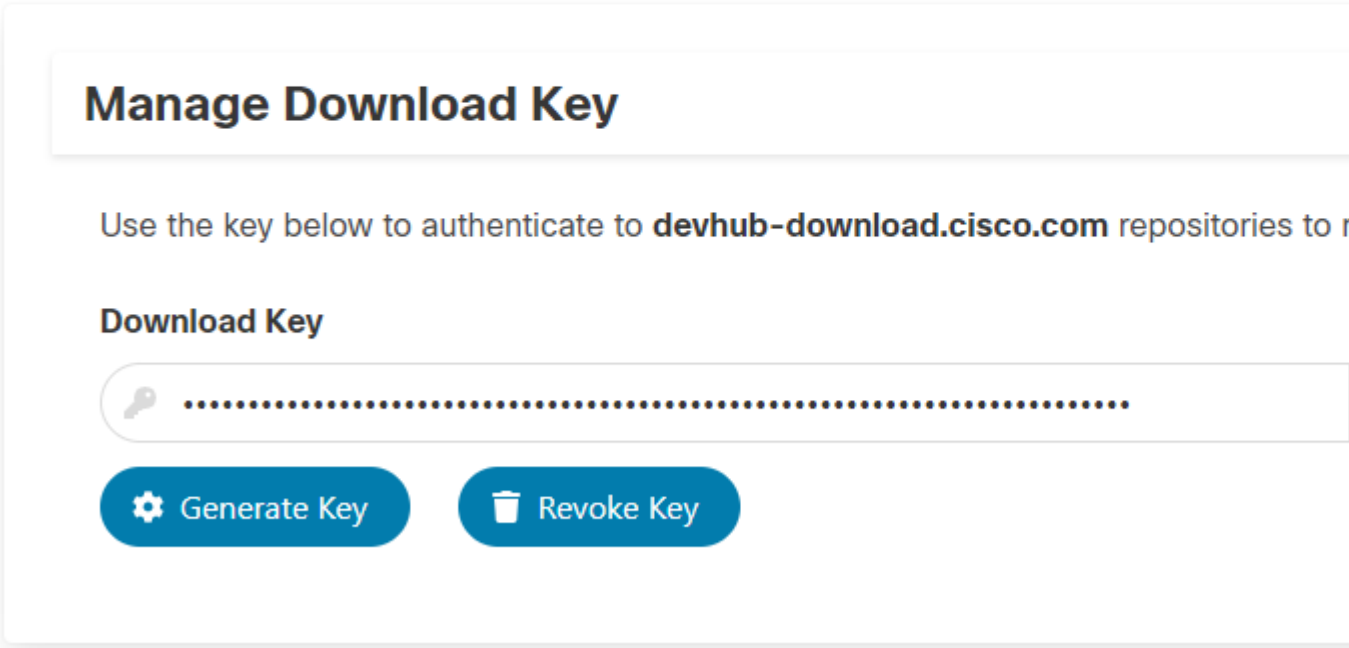
Setup- und Konfigurationsschritte

Schritt 1: Generieren des Artifactory-API-Schlüssels

1. Melden Sie sich mit Ihrem CCO-Benutzernamen und -Kennwort unter https://devhub-download.cisco.com/console/ an.
2. Wählen Sie Download-Schlüssel verwalten auf der Konsolenseite aus, wie im Bild dargestellt.



3. Klicken Sie auf Generate Key-Option, um den API-Schlüssel zu generieren. Die Option zum Anzeigen und Widerrufen des Schlüssels finden Sie auf der Seite "Download-Schlüssel verwalten".



4. Wählen Sie die Schaltfläche Kopieren, um den API-Schlüssel in die Zwischenablage zu kopieren.

Hinweis: Es ist zwingend erforderlich, dass die zur Generierung der API-Schlüssel verwendete CCO-ID über die erforderlichen Berechtigungen für Software-Upgrades verfügt. Die von Ihnen verwendete CCO-ID muss über einen gültigen SWSS- (Servicevertrag) oder Flex-Abonnement verfügen, um über die erforderliche Berechtigung zu verfügen.

Hinweis: Sie müssen sich alle sechs Monate bei https://devhub-download.cisco.com/console anmelden, um die Gültigkeit des API-Schlüssels zu verlängern.

Schritt 2: Konfigurieren der Artifactory-URL und des API-Schlüssels auf Cloud Connect

- Cisco hostet alle Softwareartefakte in einer Cloud-basierten Artefaktstruktur, die vom Cloud Connect-Server zum Herunterladen und Benachrichtigen neuer Updates verwendet wird.
- Der Cloud Connect-Server muss mit der von Cisco gehosteten Software Artifactory URL, Repository-Name und API-Schlüssel konfiguriert werden.

1. Führen Sie den Befehl, ***utils image-repository set***, um artifactory download wie im Bild dargestellt zu

konfigurieren.

```
admin:
admin:utils image-repository set
Please Enter Artifactory URL:https://devhub-download.cisco.com/binaries
Please Enter Artifactory Repository Name [ent-platform-release-external]:
Please Enter API Key:**********************************************************************

CCO ID used to generate API key has access to export restricted and unrestricted software, select 'yes' to download export restricted s
ware (yes/no): yes


Configuration settings has been saved and connection to artifactory is successful.
Artifacts required for orchestration will be downloaded locally to the Cloud Connect at 2 AM server time. Cloud connect server can be r
y, download starts 10 minutes post restart. Usage of orchestration related CLI are blocked during download, and this duration depends o

admin:
```

antwort: Geben Sie die künstlerische URL https://devhub-download.cisco.com/binaries an.

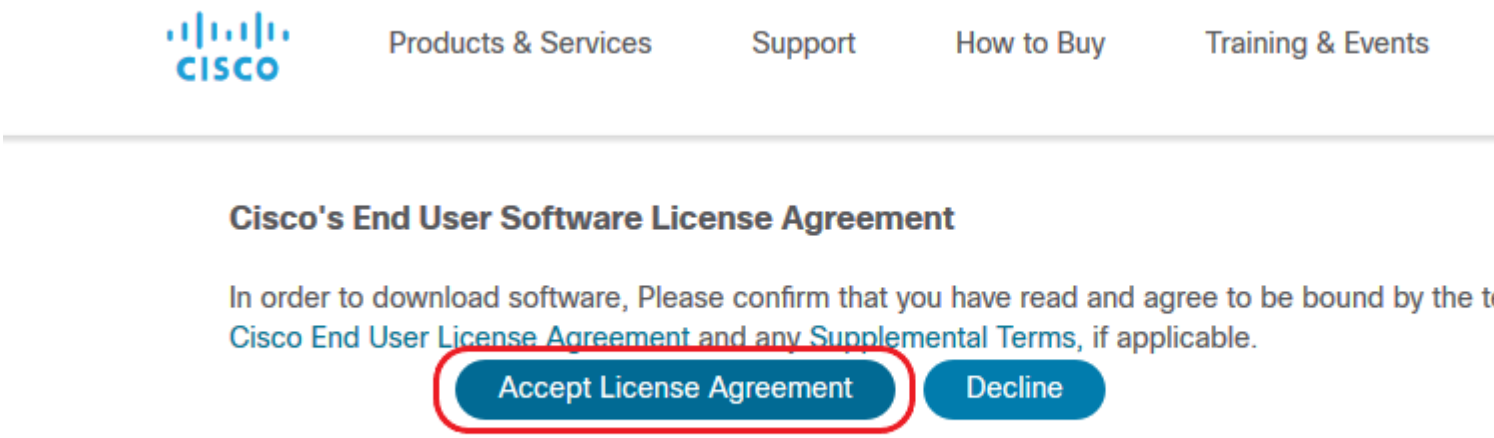
b. Geben Sie den Namen des artifactory-Repositorys ein, ent-platform-release-external.

c. Fügen Sie den generierten API-Schlüssel ein. Der API-Schlüssel wird aus Sicherheitsgründen als Sternchen angezeigt.

2. Führen Sie den Befehl **utils image-repository show aus,** um die konfigurierte Artifactory-URL, den Repository-Namen und den API-Schlüssel auf dem Cloud Connect-Server anzuzeigen, wie im Image dargestellt.

```
admin:
admin:utils image-repository show
Artifactory URL: https://devhub-download.cisco.com/binaries
Artifactory Repository Name: ent-platform-release-external
Artifactory API Key: ****W28W
admin:
```

Hinweis: Bevor der Befehl **utils image-repository set** in der CLI ausgeführt wird, navigieren Sie zur **EULA-URL** (https://software.cisco.com/download/eula), und akzeptieren Sie die EULA. Wenn dies nicht der Fall ist, schlägt der Befehl **utils image-repository set** mit dem Fehler fehl: *Die CCO-ID, die zum Generieren des API-Schlüssels verwendet wird, entspricht nicht der Endbenutzer-Lizenzvereinbarung. Verwenden Sie eine gültige CCO-ID.*
Weitere Informationen finden Sie unter Cisco Bug-ID CSCvy78680.



Hinweis: Beide Befehle können nur über den Publisher-Knoten des Cloud Connect-Servers ausgeführt werden.
Die Replikation der Image-Repository-Konfiguration erfolgt automatisch vom Publisher-Knoten zum Subscriber-Knoten, wenn der Befehl **utils image-repository set** mit erfolgreichen Ergebnissen auf dem Publisher-Knoten ausgeführt wird.

Hinweis: Die CLI des **utils Image-Repository-Sets** kann jederzeit verwendet werden, um die Option "Export eingeschränkt/Unrestricted Software" in der Bereitstellung zu ändern.
Starten Sie den Cloud Connect-Server neu, um die Bereinigung und den Download von eingeschränkter und nicht eingeschränkter Software durchzusetzen. Der Download beginnt 10 Minuten nach dem Neustart.

Hinweis: Hinweise zu künstlerischen Vorgängen:
Nach der erfolgreichen Konfiguration der Artefaktdetails werden die Artefakte um 02:00 Uhr Serverzeit lokal auf den Cloud Connect-Server heruntergeladen.
Orchestrierungsvorgänge wie Patch-Installation, Rollback oder Upgrade können nur ausgeführt werden, nachdem die Artefakte heruntergeladen wurden.
Wenn die Artefakte unmittelbar nach den Konfigurationsschritten heruntergeladen werden müssen, kann der Cloud Connect-Server neu gestartet werden, und der Download beginnt 10 Minuten nach dem Neustart.
Die Verwendung von CLI-Befehlen, die sich auf die Orchestrierung beziehen, wird beim Start des Downloads blockiert, und diese Dauer hängt von der Anzahl der herunterzuladenden Artefakte ab.

Hinweis: Wenn der Cloud Connect-Server einen Proxy für den Zugriff auf das Internet benötigt, muss ES3 oder höher installiert sein. Weitere Informationen zur Proxy-Konfiguration finden Sie im UCCE-Installations- und Upgrade-Handbuch.

Schritt 3: Integration von VOS-Knoten in einen Orchestrierungssteuerungsknoten

Voraussetzungen:

- Stellen Sie sicher, dass alle Systemversionsanforderungen erfüllt sind.
- Importieren Sie die Zertifikate aus dem Cloud Connect-Cluster (Pub und Sub) in das Tomcat-Trust auf allen Ziel-VOS-Servern (Tomcat für selbstsignierte und Root/Intermediate für CA-signierte Server).

Um jedes Finesse-, CUIC-, VVB-, IDS-, LD-System an einen Cloud Connect-Server anzubinden, führen Sie den Befehl aus, **verwendet das System an Bord** vom Publisher-Knoten des jeweiligen VOS-Clusters aus, wie im Bild dargestellt.

```
admin:
admin:utils system onboard initiate
You can onboard a cluster to a Cloud Connect node. Enter the details of the Cloud Connect noc
Cloud Connect FQDN:cloudconnect1.dcloud.cisco.com
Cloud Connect Application User:appadmin
Cloud Connect Application User's Password:*********
The cluster has been successfully onboarded.
admin:
```

1. Geben Sie den FQDN des Cloud Connect Publisher-Knotens an.

2. Geben Sie den Anwendungsbenutzernamen für den Cloud Connect-Server an.

3. Geben Sie das Benutzerkennwort der Anwendung für den Cloud Connect-Server an.

- Der Publisher-Knoten des Cloud Connect-Servers muss online sein, wenn der Onboard-Initiator vom VOS-Knoten ausgeführt wird.
- Wenn der integrierte Initiator vom VOS-Knoten ausgeführt wird, muss der FQDN des Cloud Connect Publisher-Servers verwendet werden.
- **Der** Befehl **utils system onboard trigger** muss auf allen VOS Publishern (Finesse, CUIC, LD, IdS, alle VVBs) ausgeführt werden.

Hinweis: Wenn das System (Cluster) teilweise mit einem Fehler auf den Cloud Connect-Server umgeschaltet wird, überprüfen Sie die Ursache des Fehlers und korrigieren Sie sie. Führen Sie dann den Befehl **utils system onboard update** anstelle des Befehls **utils system onboard trigger** aus.

Hinweis: Onboard ist nur zulässig, wenn sowohl der Publisher- als auch der Subscriber-Knoten auf dem Cloud Connect-Server erreichbar sind.

Hinweis: Wenn der Cloud Connect-Server beschädigt ist und mit einer neuen Installation neu bereitgestellt wird, muss der Administrator **utils system onboard remove** vom VOS-Knoten ausführen und dann **utils system onboard restart** erneut ausführen, um die VOS-Knoten zu integrieren.

Hinweis: Um den Anwendungsbenutzernamen des Cloud Connect Servers zu überprüfen/zu finden, führen Sie den Befehl **run sql select * from applicationUser** on the Cloud Connect Servers' CLI aus.

Schritt 4: Einbinden von Windows-Knoten in einen Orchestrierungssteuerungsknoten

Der integrierte Prozess unterstützt den Aufbau einer kennwortlosen Verbindung zwischen dem Cloud Connect-Knoten und den Windows-Knoten. So integrieren Sie die Windows-basierten Knoten in den Orchestrierungssteuerungsknoten:

Konfigurieren Sie den öffentlichen SSH-Schlüssel auf den Windows-Knoten:

antwort: Navigieren Sie zu ***%Users%\<logonUser>\.ssh\,*** und erstellen Sie eine Datei mit ***autorisierten Schlüsseln***, falls diese nicht vorhanden ist. *(Der Erweiterungstyp "authorized_keys" ist "Datei" und kann nicht geändert werden.)*

Hinweis: Der Benutzer darf nicht aus dem System entfernt werden und muss ein Domänenbenutzer mit Domänenadministratorrechten oder mit Berechtigungen für die lokale Verwaltung sein.

---

b. Öffnen Sie den Browser, und geben Sie die **Cloud Connect Publisher-URL ein:** https://<CloudConnectIP>:8445/inventar/controlNode/key

c. Geben Sie Ihre Anmeldeinformationen für die Cloud Connect-Anwendung ein. Bei erfolgreicher Authentifizierung wird der öffentliche Cloud Connect SSH-Schlüssel über eine REST-API-Antwort abgerufen.

d. Kopieren Sie diesen öffentlichen Schlüsselwert in die Datei authorized_keys in ***%Users%\<logonUser>\.ssh***.

Ein Beispiel für die Ausgabe der URL wird angezeigt. Kopieren Sie in der Ausgabe nur den Teil, der mit **ssh-rsa** beginnt und mit **root@localhost** endet, in die Datei authorized_keys.

```
{"category":"PUBLISHER","hostName":"cc125clouda.uclabservices.com","publicKey":"ssh-rsa AAAAB3NzaC1y
```

Die Datei authorized_keys für das Beispiel wird angezeigt.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDfJDl7RUZ/Umdflp5r3IqMaoV8WSrr7iLBOWindC0lGeGPYkprVW2xq6H6I8Fu
```

e. Wiederholen Sie die Schritte b, c und d, um den öffentlichen Schlüssel des Cloud Connect-Abonnenten abzurufen (sofern es sich bei Cloud Connect um eine hoch verfügbare Einrichtung handelt).

Hinweis: Öffentliche Schlüssel von Cloud Connect-Herausgebern und -Abonnenten müssen in eine Datei mit autorisierten Schlüsseln kopiert werden. Die Publisher- und Subscriber-Einträge müssen auf separaten Leitungen stehen und dürfen am Ende der Leitung kein zusätzliches Leerzeichen, Komma oder Sonderzeichen verwenden.

---

f. Starten Sie die OpenSSH-Dienste neu:
- **OpenSSH SSH-Server**
- **OpenSSH-Authentifizierungs-Agent**

Gehen Sie zur Fehlerbehebung bei der SSH-Anmeldung wie folgt vor:

antwort: Navigieren Sie zu **C:\ProgramData\ssh**, und öffnen Sie die Datei **sshd_config** in einem Texteditor.

b. Suchen Sie den Abschnitt dieser Datei, der mit der **#-Protokollierung** beginnt.

c. Heben Sie die Auskommentierung der SyslogFacility-Zeile und der LogLevel-Zeile auf.

d. Ändern Sie SyslogFacility in LOCAL0 und LogLevel in DEBUG, wie im Beispiel gezeigt

```
# Logging
SyslogFacility LOCAL0
LogLevel DEBUG
```

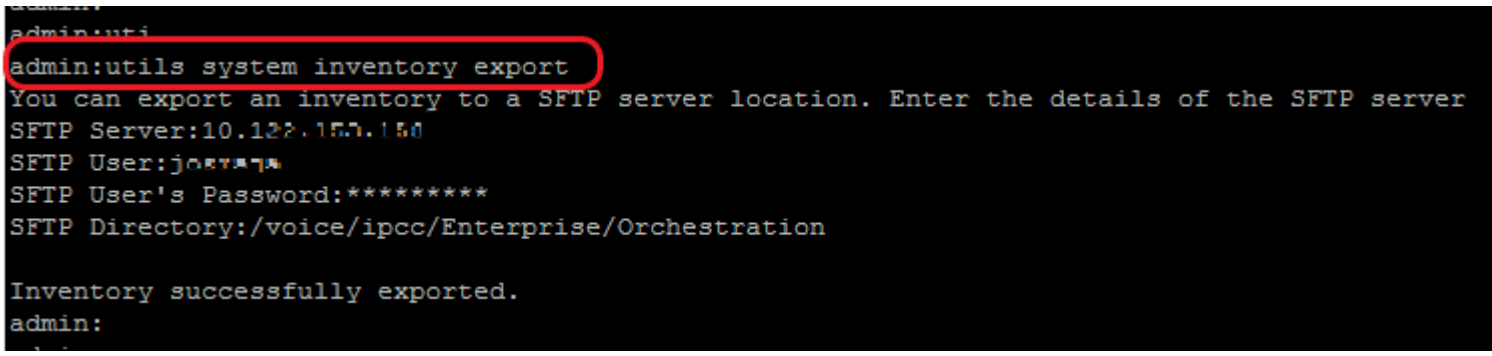
e. Speichern Sie die Datei sshd_config, und starten Sie dann den **OpenSSH SSH Server**-Dienst neu.

f. Die Protokolldatei wird in **C:\ProgramData\ssh\logs\sshd.log** geschrieben.

Schritt 5: Aktualisieren Sie die Datei Inventory.conf.

1. Führen Sie den Befehl **utils system Inventory export** aus, um das Inventar auf einen SFTP-Server

hochzuladen, wie im Bild gezeigt.



antwort: Geben Sie die IP-Adresse oder den FQDN eines SFTP-Servers an.

b. Geben Sie den Benutzernamen mit Lese-/Schreibzugriff auf den SFTP-Server an.

c. Geben Sie das Kennwort für den Benutzer ein.

d. Geben Sie das Verzeichnis an, in das die Inventardatei im UNIX/Linux-Format geschrieben werden soll.

Beispiel: /voice/ipcc/Enterprise/Orchestrierung

2. Bearbeiten Sie das Inventar, um die VOS- und Windows-Komponenten aufzunehmen.

- Syntax, Ausrichtung und Einrückung müssen genau mit der in der Inventardatei übereinstimmen.
- CRLF-Zeilenenden müssen im UNIX-Stil enden. Daher kann ein Linux-basierter oder ein Mac OS-basierter Editor verwendet werden, um die Windows-Inventardatei zu erstellen. Ein Programm wie Notepad++ kann ebenfalls verwendet werden.
- Die Komponentennamen, z. B. CVPREPORTING, ROGGER, PG usw., müssen in Großbuchstaben geschrieben werden.

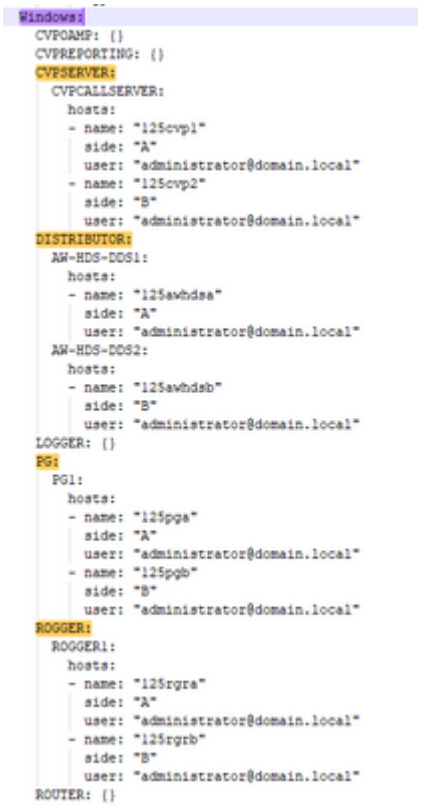
Hinweis: Die Datei Inventory.conf reagiert auf Einrückungen. Weitere Informationen finden Sie in den Beispielkonfigurationsdateien.

Beispieldateien mit dem richtigen Format können hier heruntergeladen werden:
https://github.com/CXCCSummit/Repository

Das Beispiel des VOS-Servers wird im Bild angezeigt:

```
CUIC: {}
CUIC_LiveData_IdS:
  CUIC_LiveData_IdS-Cluster-1:
    hosts:
    - name: "125cuicpub"
      side: "A"
      type: "Publisher"
    - name: "125cuicsub"
      side: "B"
      type: "Subscriber"
Finesse:
  Finesse-Cluster-1:
    hosts:
    - name: "125finpub"
      side: "A"
      type: "Publisher"
    - name: "125finsub"
      side: "B"
      type: "Subscriber"
IdS: {}
LiveData: {}
VVB:
  VVB-Cluster-1:
    hosts:
    - name: "125vvb1"
      side: "A"
      type: "Publisher"
  VVB-Cluster-2:
    hosts:
    - name: "125vvb2"
      side: "B"
      type: "Publisher"
```

Das Beispiel für Windows Server wird im Bild angezeigt:



```
Windows:
  CVPOAMP: {}
  CVPREPORTING: {}
  CVPSERVER:
    CVPCALLSERVER:
      hosts:
      - name: "125cvp1"
        side: "A"
        user: "administrator@domain.local"
      - name: "125cvp2"
        side: "B"
        user: "administrator@domain.local"
  DISTRIBUTOR:
    AW-HDS-DDS1:
      hosts:
      - name: "125awhdsa"
        side: "A"
        user: "administrator@domain.local"
    AW-HDS-DDS2:
      hosts:
      - name: "125awhdsb"
        side: "B"
        user: "administrator@domain.local"
  LOGGER: {}
  PG:
    PG1:
      hosts:
      - name: "125pga"
        side: "A"
        user: "administrator@domain.local"
      - name: "125pgb"
        side: "B"
        user: "administrator@domain.local"
  ROGGER:
    ROGGER1:
      hosts:
      - name: "125rgra"
        side: "A"
        user: "administrator@domain.local"
      - name: "125rgrb"
        side: "B"
        user: "administrator@domain.local"
  ROUTER: {}
```

3. Bearbeiten Sie die Zeichenfolgen in der Inventardatei nach Bedarf.

deploymentName: Geben Sie einen eindeutigen Namen für die Bereitstellung an.

- Dieser Name wird in der Betreffzeile der E-Mail-Benachrichtigung angezeigt. Wenn sie nicht konfiguriert ist, enthält die Betreffzeile der E-Mail-Benachrichtigung nur die Art des Vorgangs und

den Gesamtstatus.

deploymentType: Dieses Feld wird für die Kompatibilitätsprüfung in den Upgrade-, Rollback- oder Switchforward-Prozeduren verwendet.

```
deploymentName: "UnifiedCCE"
deploymentType: "UCCE-2000-Agents"
```

Folgende Bereitstellungstypen werden unterstützt:

- UCCE-2000-Agenten
- UCCE-4000-Agenten

- PCCE-2000-Agenten
- PCCE-4000-Agenten

- HCS-CC-2000-Agenten
- HCS-CC-4000-Agenten

Hinweis: Lesen Sie die folgenden Hinweise zu den unterstützten Bereitstellungsarten.
Die Orchestrierung wird für die Bereitstellungsmodelle 12000, 24000 und 26000 der Agenten nicht unterstützt.
Das HCS-SCC-Bereitstellungsmodell (Small Contact Center) wird für die Orchestrierung derzeit nicht unterstützt.
Stellen Sie sicher, dass die in dieses Feld eingegebenen Werte dem unterstützten Listenformat für Bereitstellungstypen entsprechen. Beim Bereitstellungstyp wird die Groß- und Kleinschreibung unterschieden.

Hinweis: Der Administrator kann die Standardwerte bei Bedarf je nach Bereitstellungstyp und bevorzugtem Bereitstellungsnamen aktualisieren oder bearbeiten.

---

4. Führen Sie den Befehl "**utils system Inventory import** on the Cloud Connect publisher node" aus, um das aktualisierte Inventar vom SFTP-Server wie im Bild dargestellt zu importieren.

```
admin:
admin:utils system inventory import
You can import an inventory from SFTP server location. Enter the details of the SFTP server
SFTP Server:10.122.1[illegible]
SFTP User:jo[illegible]
SFTP User's Password:*********
SFTP Directory:/voice/ipcc/Enterprise/Orchestration

Import will replace the existing inventory config. Do you want to continue(yes/no): yes
Inventory successfully imported. Components in the deployment will be validated as part of l
Please use "file get activelog ansible/component_cache_update.log" command to check the log
admin:
```

antwort: Geben Sie die IP-Adresse oder den FQDN eines SFTP-Servers an.

b. Geben Sie den Benutzernamen mit Lese-/Schreibzugriff auf den SFTP-Server an.

c. Geben Sie das Kennwort für den Benutzer ein.

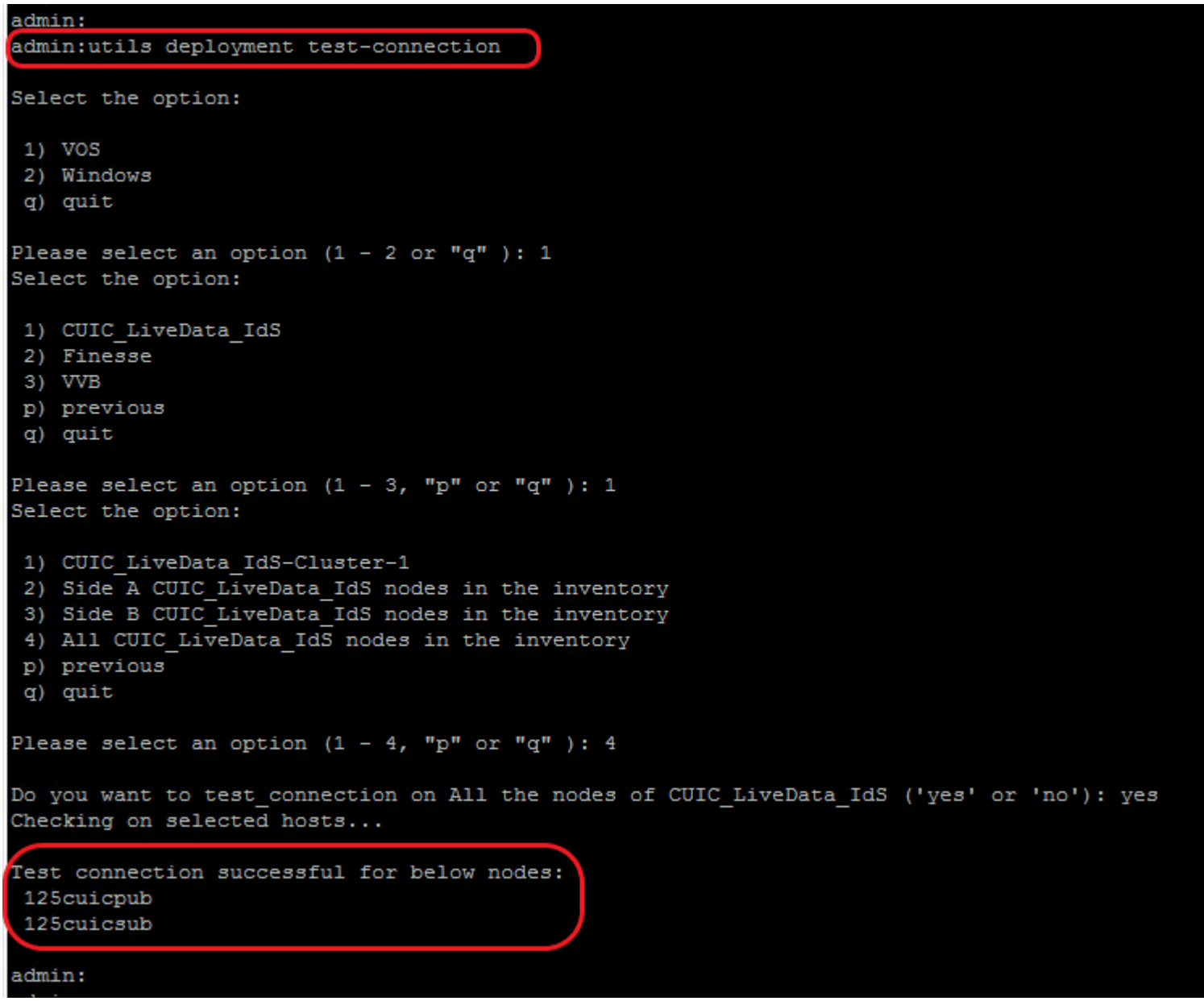
d. Geben Sie das Verzeichnis an, in das die Inventardatei im UNIX/Linux-Format geschrieben werden soll.

Beispiel: /voice/ipcc/Enterprise/Orchestrierung

e. Beantworten Sie die Frage mit "Ja", damit die neue Bestandsdatei den aktuellen Bestand ersetzen kann.

Schritt 6: Validierung integrierter Knoten für Orchestrierung

Um zu überprüfen, ob die VOS- und Windows-Knoten erfolgreich integriert wurden, und um zu überprüfen, ob die Orchestrierungsfunktion für die Verwendung bereit ist, führen Sie den Befehl aus, **verwendet die Bereitstellungstestverbindung,** wie im Abbild dargestellt.



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.