Festlegen von Ablaufverfolgungen und Erfassen von Protokollen in CCE

Inhalt

Einleitung

In diesem Dokument wird das Festlegen und Sammeln von Ablaufverfolgungen in Cisco Unified Contact Center Enterprise (CCE) beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Unified Contact Center Enterprise (UCCE)
- Package Contact Center Enterprise (PCCE)

- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco Virtualized Voice Browser (VVB)
- Cisco Unified Border Element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Session Initiation Protocol (SIP) Proxy (CUSP)

Verwendete Komponenten

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

- Cisco Finesse Version 12.5
- CVP Server Version 12.5
- UCCE/PCCE Version 12.5
- Cisco VVB Version 12.5
- CUIC Version 12.5

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 verstehen.

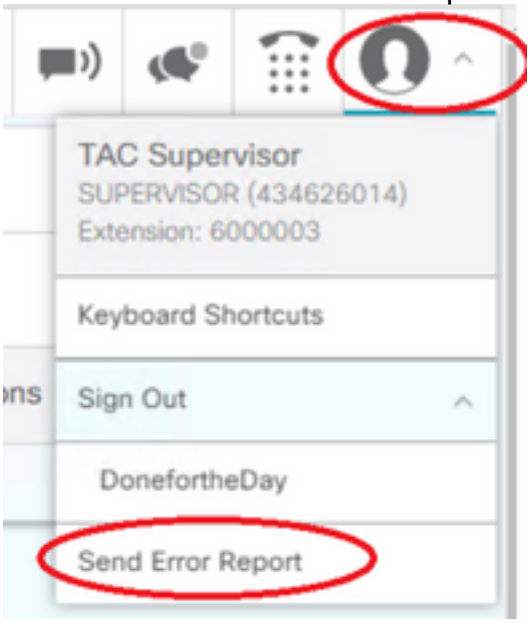
Traces setzen und Finesse-Protokolle sammeln

Finesse-Client

Es gibt mehrere Möglichkeiten, Finesse-Client-Protokolle zu sammeln.

Option 1: Sammeln von Client-Protokollen mithilfe des Berichts zum Senden von Fehlern

1. Melden Sie einen Agenten an.
2. Wenn ein Mitarbeiter während eines Anrufs oder einer Medienveranstaltung ein Problem feststellt, weisen Sie ihn an, auf den Link **Send Error Report (Fehlerbericht senden)** oben rechts auf dem Finesse-Desktop zu klicken.

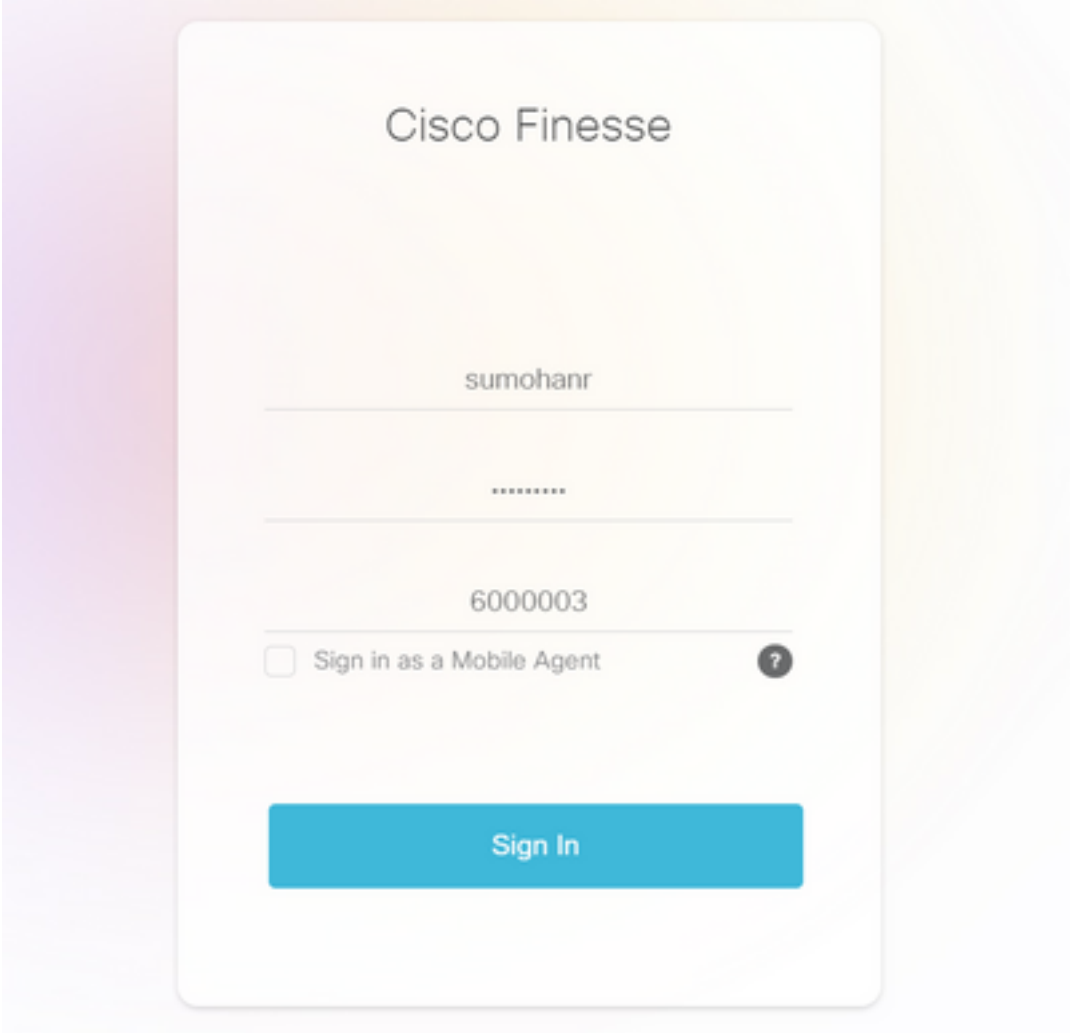


3. Der Agent sieht die **Protokolle erfolgreich gesendet!** Nachricht.
4. Die Client-Protokolle werden an den Finesse-Server gesendet. Navigieren Sie zu https://x.x.x.x/finesse/logs, und melden Sie sich mit einem Administratorkonto an.
5. Sammeln Sie die Protokolle im Verzeichnis **clientlogs/**.

Option 2: Festlegen der permanenten Protokollierung

1. Navigieren Sie zu https://x.x.x.x:8445/desktop/locallog.
2. Klicken Sie auf **Mit permanenter Protokollierung anmelden**.

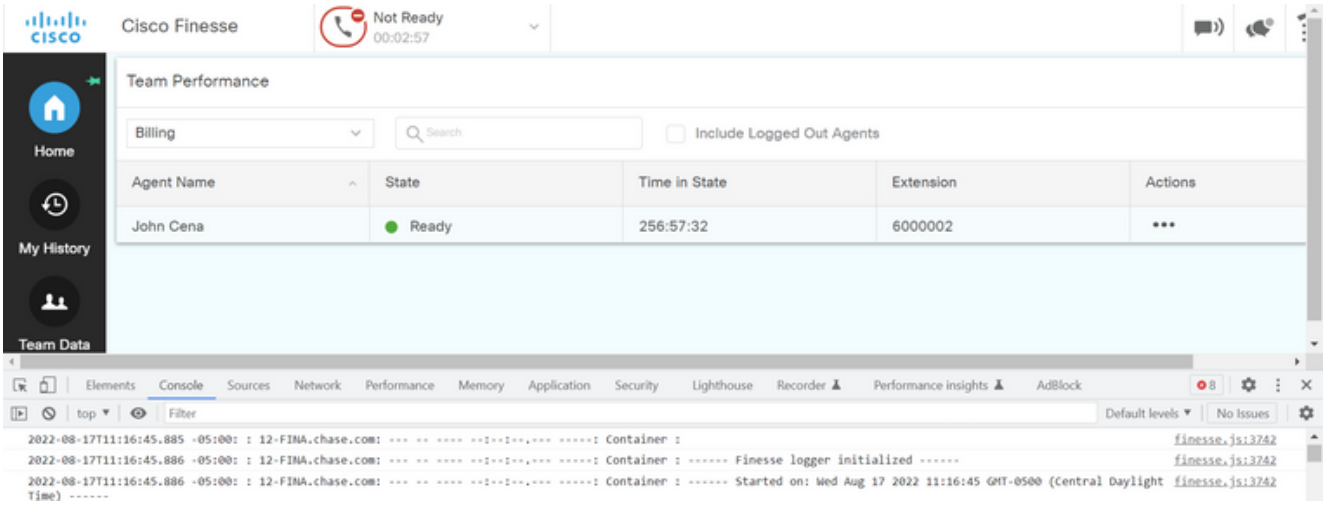
3. Die Anmeldeseite für den Cisco Finesse Agent-Desktop wird geöffnet. Melden Sie den Agenten an.



4. Die gesamte Desktop-Interaktion des Agenten wird registriert und an die lokalen Speicherprotokolle gesendet. Um die Protokolle zu sammeln, navigieren Sie zu https://x.x.x.x:8445/desktop/locallog, und kopieren Sie den Inhalt in eine Textdatei. Save die Datei zur weiteren Analyse.

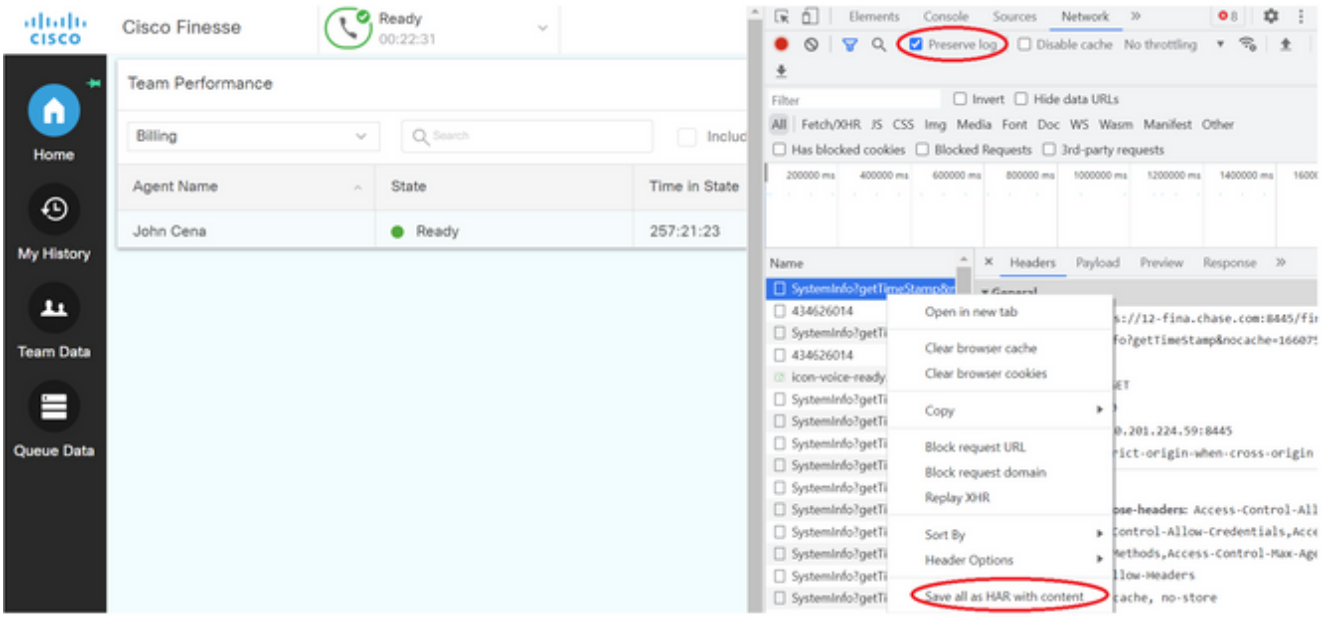
Option 3: Webbrowser-Konsole

1. Wenn sich ein Agent angemeldet hat, drücken Sie **F12**, um die Browserkonsole zu öffnen.
2. Wählen Sie die Registerkarte **Konsole**.
3. Überprüfen Sie die Browserkonsole auf Fehler. Kopieren Sie den Inhalt in eine Textdatei, und save IT.



4. Wählen Sie die Registerkarte **Netzwerk**, und aktivieren Sie die Option Protokoll beibehalten.
5. Klicken Sie mit der rechten Maustaste auf ein Netzwerknamensereignis, und wählen Sie **Save**

als HAR mit Inhalt.



Finesse-Server

Option 1: Über die Benutzeroberfläche - Web-Services (erforderlich) und zusätzliche Protokolle

1. Navigieren Sie zu https://x.x.x.x/finesse/logs, und melden Sie sich mit dem Administrationskonto an.
2. Erweitern Sie das Verzeichnis **webservices/**

3. Erfassen der letzten Webdienstprotokolle Wählen Sie die letzte Unzip-Datei aus. Beispiel: **Desktop-Webservices.201X-..log.zip**. Klicken Sie auf den Datei-Link, um die Option save die Datei.

4. Sammeln Sie die anderen erforderlichen Protokolle (je nach Szenario). Beispielsweise OpenFire für Probleme mit Benachrichtigungsdiensten, Realm-Protokolle für Authentifizierungsprobleme und Tomcatlogs für APIs-Probleme.

Anmerkung: Die empfohlene Methode zum Erfassen der Cisco Finesse-Serverprotokolle erfolgt über Secure Shell (SSH) und Secure File Transfer Protocol (SFTP). Mit dieser Methode können Sie nicht nur die Webdienstprotokolle sammeln, sondern auch alle zusätzlichen Protokolle wie, Fippa, openfire, Realm und Clientlogs.

Option 2: Über SSH und Secure File Transfer Protocol (SFTP) - empfohlene Option

1. Melden Sie sich mit dem SSH beim Finesse-Server an.
2. Geben Sie diesen Befehl ein, um die benötigten Protokolle zu sammeln. Der Befehl sammelt

die Protokolle für 2 Stunden. Sie werden aufgefordert, den SFTP-Server zu identifizieren, auf den die Protokolle hochgeladen werden.

file get activelog desktop recurs compress reltime hours 2

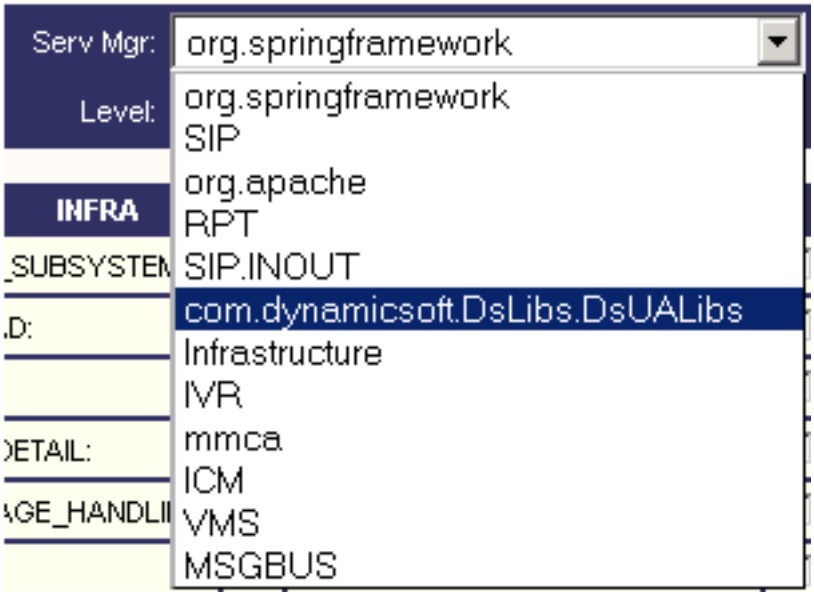
```
Total size in Bytes: 413567
Total size in Kbytes: 403.87402
Would you like to proceed [y/n]? y
SFTP server IP:
```

3. Diese Protokolle werden im SFTP-Serverpfad gespeichert: <IP-Adresse>\<Datums-Zeitstempel>\active_nnn.tgz , wobei nnn ein Zeitstempel im Langformat ist.
4. Weitere Protokolle wie Tomcat, Context Service, Servm und Installationsprotokolle finden Sie im Abschnitt Log Collection im Cisco Finesse Administration Guide Release 12.5(1).

Festlegen von Ablaufverfolgungen und Erfassen von CVP- und CVVB-Protokollen

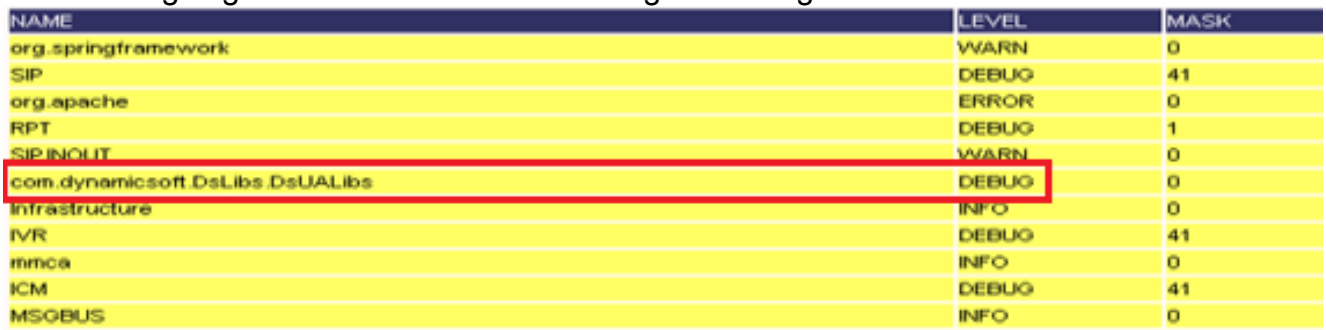
CVP-Anrufserver

1. Die Standardstufe der Ablaufverfolgungen des CVP CallServer reicht für die Fehlerbehebung in den meisten Fällen aus. Wenn Sie jedoch weitere Informationen zu den SIP-Nachrichten (Session Initiation Protocol) benötigen, müssen Sie die SIP-Strack-Traces auf die DEBUG-Ebene festlegen.
2. Rufen Sie die CVP CallServer Diag-Webseite unter http:/localhost:8000/cvp/diag auf. **Anmerkung:** Diese Seite enthält gute Informationen über den CVP-Anrufserver und ist sehr nützlich, um bestimmte Szenarien zu beheben.
3. Wählen Sie **com.dynamicsoft.DsLibs.DsUALibs** aus dem **Serv. Mgr**-Dropdown-Menü oben links



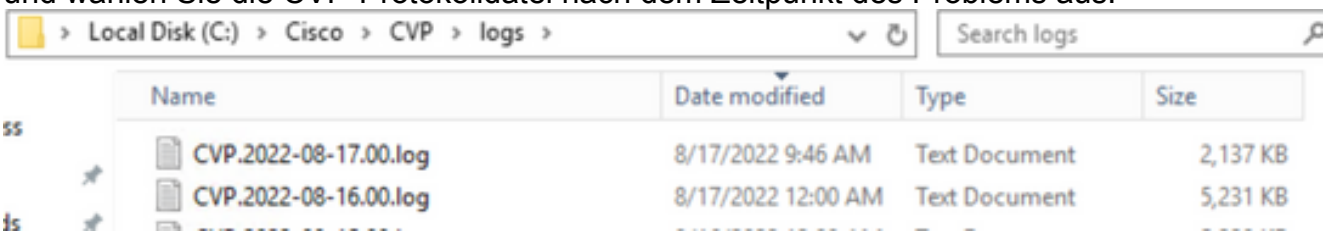
4. Klicken Sie auf die Schaltfläche **Festlegen**.

5. Blättern Sie im Trace-Fenster nach unten, um sicherzustellen, dass die Ebene der Traces korrekt festgelegt wurde. Dies sind Ihre Debugeinstellungen.



NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
SIP.INOUT	WARN	0
com.dynamicsoft.DsLibs.DsUALibs	DEBUG	0
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
MSGBUS	INFO	0

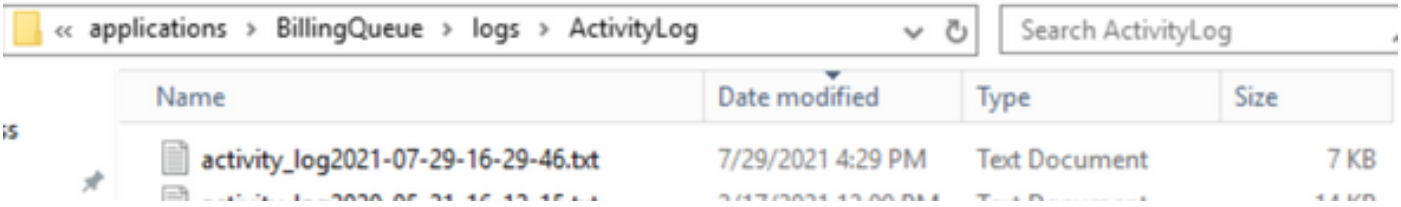
6. Wenn Sie das Problem reproduzieren, sammeln Sie die Protokolle von **C:\Cisco\CVP\logs**, und wählen Sie die CVP-Protokolldatei nach dem Zeitpunkt des Problems aus.



CVP Voice XML (VXML)-Anwendung

In sehr seltenen Fällen müssen Sie die Traces der VXML-Serveranwendungen erhöhen. Andererseits wird eine Erhöhung nur auf Anforderung eines Cisco Technikers empfohlen.

Um die VXML-Server-Anwendungsprotokolle zu sammeln, navigieren Sie zum jeweiligen Anwendungsverzeichnis unter dem VXML-Server. Beispiel: **C:\Cisco\CVP\VXMLServer\applications\{Name der Anwendung}\logs\ActivityLog**, und sammeln Sie die Aktivitätsprotokolle.



CVP Operations and Administration Management Portal (OAMP)

In den meisten Fällen reichen die Standardwerte für die Spuren von OAMP und ORM aus, um die Ursache des Problems zu ermitteln. Wenn jedoch der Pegel von Traces erhöht werden muss, führen Sie diese Aktion wie folgt aus:

1. Backup **%CVP_HOME%\conf\oamp.properties**

2. Bearbeiten **%CVP_HOME%\conf\oamp.properties**

```
omgr.traceMask=-1
omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERROR
net.sf.ehcache.logLevel=ERROR
```

3. Starten Sie OPSConsoleServer nach der Änderung wie dargestellt neu.

Informationen auf Ablaufverfolgungsebene

Ablaufverfolgungsebene	Beschreibung	Protokollstufe	Ablaufverfolgungsmaske
0	Standard-Produktinstallation. Keine oder minimale Auswirkungen auf die Leistung erwartet.	INFORMATIONEN	None
1	Weniger detaillierte Ablaufverfolgungsmeldungen mit geringen Auswirkungen auf die Leistung.	DEBUG	GERÄTEKONFIGURATION + DATENBANK_ÄNDERN + MANAGEMENT=0x0101100 0
2	Detaillierte Ablaufverfolgungsmeldungen mit mittleren Auswirkungen auf die Leistung.	DEBUG	GERÄTEKONFIGURATION + SYSLVL_CONFIGURATION + DATENBANK_ÄNDERN + MANAGEMENT=0x0501100 0
3	Detaillierte Ablaufverfolgungsmeldungen mit Auswirkungen auf die Leistung.	DEBUG	GERÄTEKONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + DATENBANK_ÄNDERN + MANAGEMENT=0x0511100 0
4	Detaillierte Ablaufverfolgungsmeldungen mit sehr starken Auswirkungen auf die Leistung.	DEBUG	MISC + GERÄTEKONFIGURATION + ST_KONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK TRACE + DATENBANK_ÄNDERN + DATABASE_SELECT + DATENBANK_PO_INFO + MANAGEMENT + TRACE_METHOD +

			TRACE_PARAM=0x173710 00
5	Höchste detaillierte Ablaufverfolgungsmeldung.	DEBUG	MISC + GERÄTEKONFIGURATION + ST_KONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK TRACE + DATENBANK_ÄNDERN + DATABASE_SELECT + DATENBANK_PO_INFO + MANAGEMENT + TRACE_METHOD + TRACE_PARAM=0x173710 06

Cisco Virtualized Voice Browser (CVVB)

Im CVVB ist eine Ablaufverfolgungsdatei eine Protokolldatei, die die Aktivitäten der Subsysteme und Schritte der Cisco VVB-Komponenten aufzeichnet.

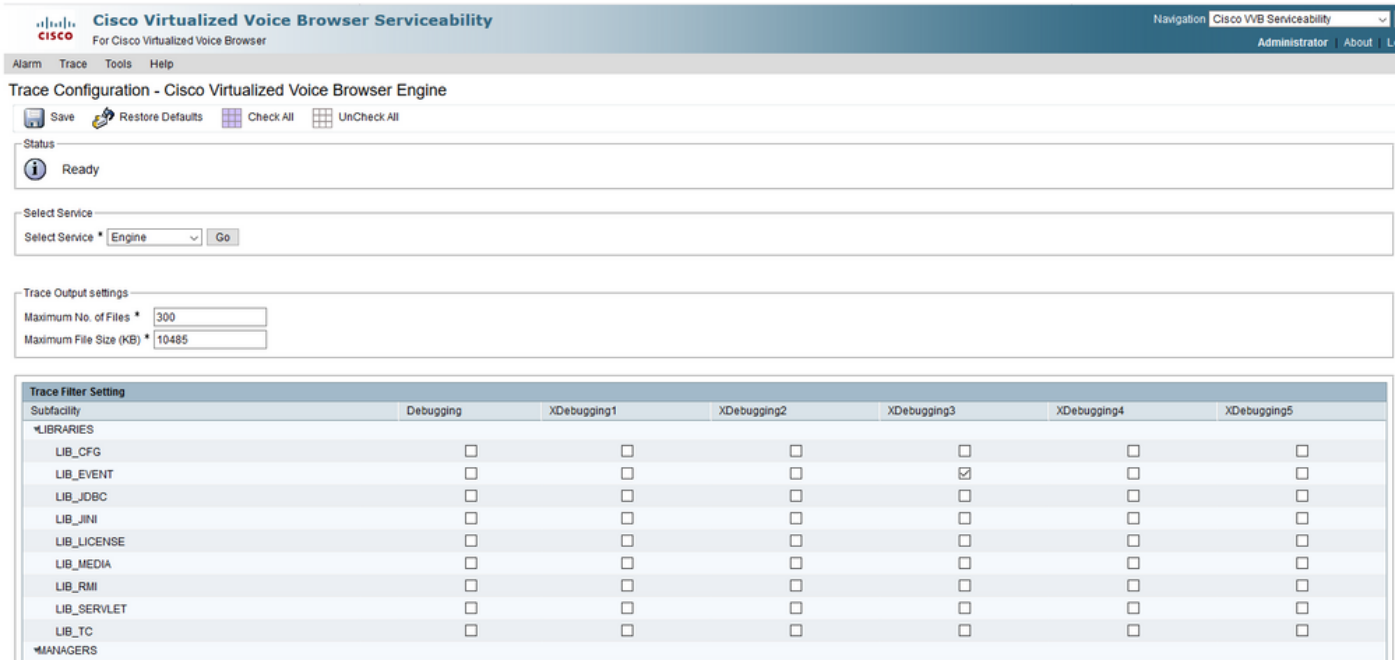
Cisco VVB besteht im Wesentlichen aus zwei Komponenten:

- Cisco VB "Administration"-Traces, auch MADM-Protokolle genannt
- Als MIVR-Protokolle bezeichnete Cisco VB "Engine"-Traces

Sie können die Komponenten angeben, für die Sie Informationen erfassen möchten, sowie die Ebene der Informationen, die Sie erfassen möchten.

Protokollstufen reichen von:

- Debuggen - Grundlegende Flussdetails zum
- XDebugging 5 - Detailed Level mit Stack Trace



Warnung: Xdebugging5 darf auf dem in der Produktion geladenen System nicht aktiviert werden.

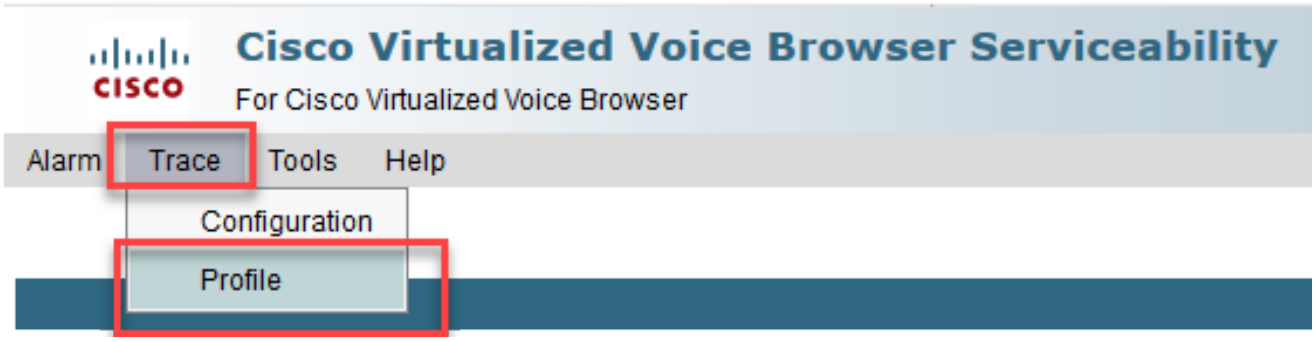
Die gängigsten Protokolle, die Sie sammeln müssen, sind die Engine. Die Standard-Trace-Stufe für die CVVB Engine-Traces reicht aus, um die meisten Probleme zu beheben. Wenn Sie jedoch die Ebene der Ablaufverfolgungen für ein bestimmtes Szenario ändern müssen, empfiehlt Cisco die Verwendung der vordefinierten Systemprotokollprofile.

Systemprotokollprofile

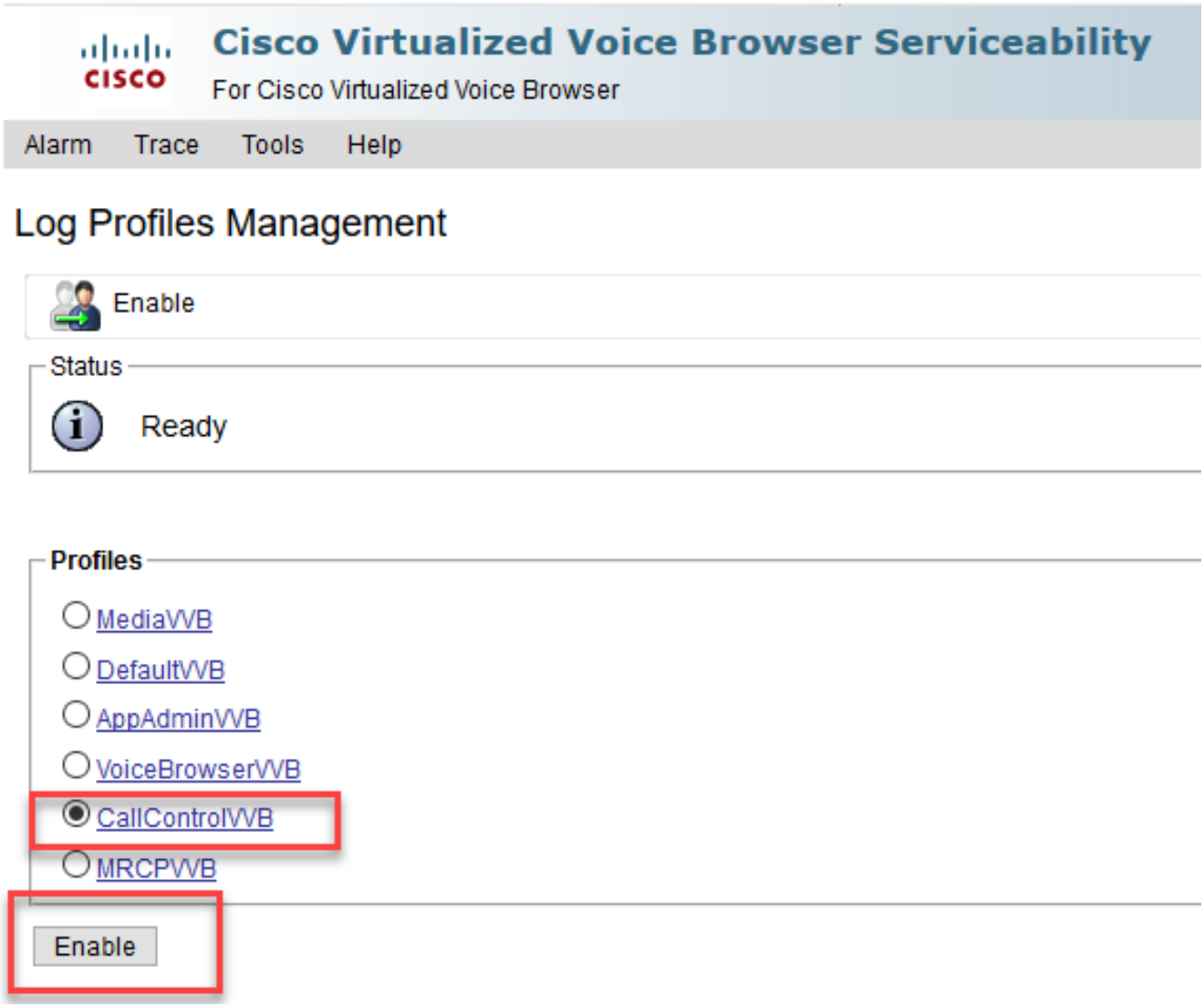
Name	Szenario, in dem dieses Profil aktiviert werden muss
StandardVVB	Generische Protokolle sind aktiviert.
Anwendungs-AdminVB	Bei Problemen mit der Web-Administration über AppAdmin, Cisco VVB Serviceability und andere Webseiten.
MedienVVB	Bei Problemen mit der Medieneinrichtung oder -übertragung.
SprachbrowserVB	Bei Problemen mit der Anrufbearbeitung.
MRCPVB	Bei Problemen mit ASR/TTS und Cisco VVB.
AnrufsteuerungVVB	Bei Problemen mit SIP-Signalen werden diese im Protokoll veröffentlich

1. Öffnen Sie die CVVB-Hauptseite (https://X.X.X.X/uccxservice/main.htm), und navigieren Sie zur Cisco VVB Serviceability-Seite. Melden Sie sich mit dem Administratorkonto an.

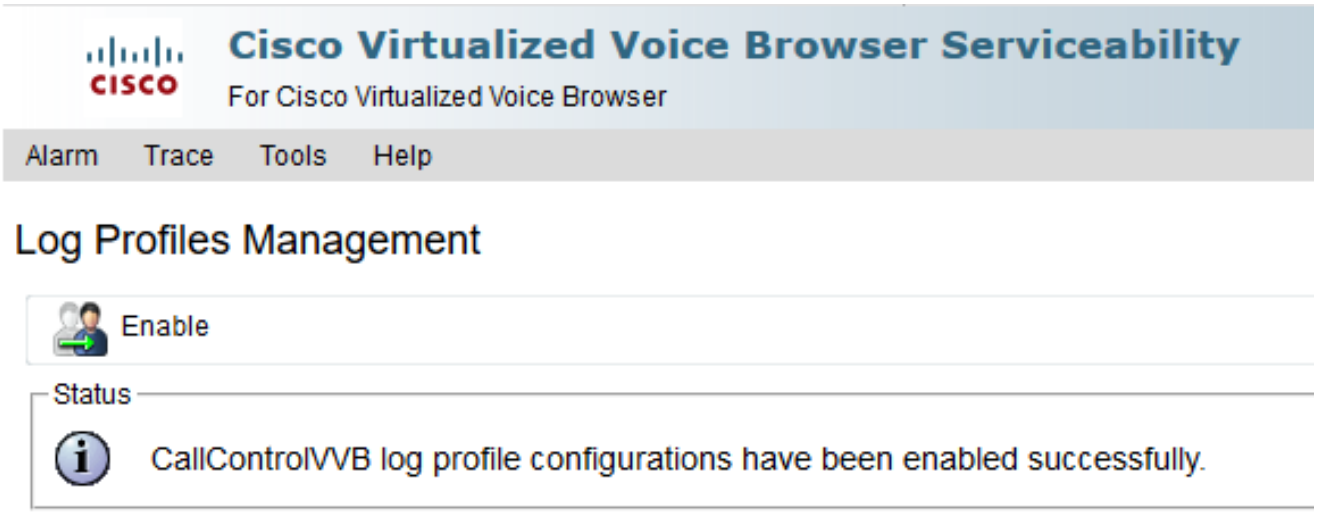
2. Auswählen **Nachverfolgung -> Profil.**



3. Aktivieren Sie das Profil, das Sie für das jeweilige Szenario aktivieren möchten, und klicken Sie auf die Schaltfläche **Aktivieren**. Aktivieren Sie beispielsweise das Profil CallControlVVB für SIP-bezogene Probleme oder MRCPVB für Probleme im Zusammenhang mit der automatischen Spracherkennung und der Text-to-Speech-Interaktion (ASR/TTS).

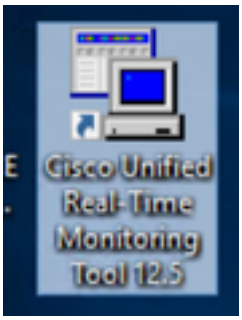


4. Nach dem Klicken auf die Schaltfläche "Aktivieren" wird die Meldung angezeigt.

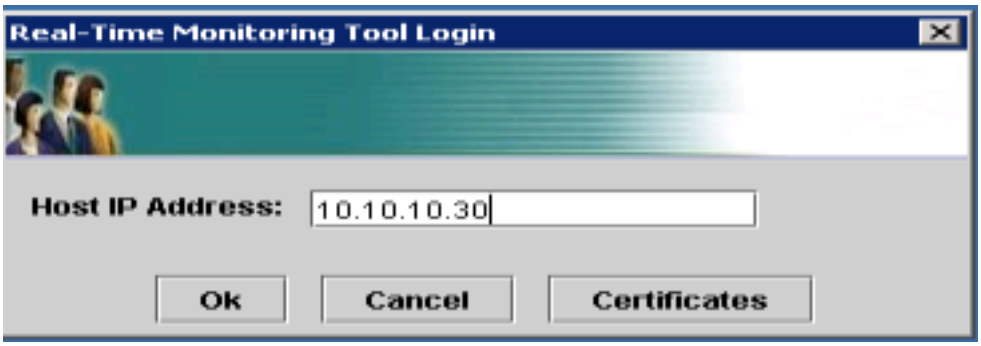


5. Nachdem das Problem reproduziert wurde, sammeln Sie die Protokolle. Verwenden Sie das Real Time Monitor Tool (RTMT), das im Lieferumfang des CVVB enthalten ist, um die Protokolle zu erfassen.

6. Klicken Sie auf Ihrem Desktop auf das Symbol für das Cisco Unified Real-Time Monitoring Tool (bei Bedarf können Sie dieses Tool aus dem CVVB herunterladen).

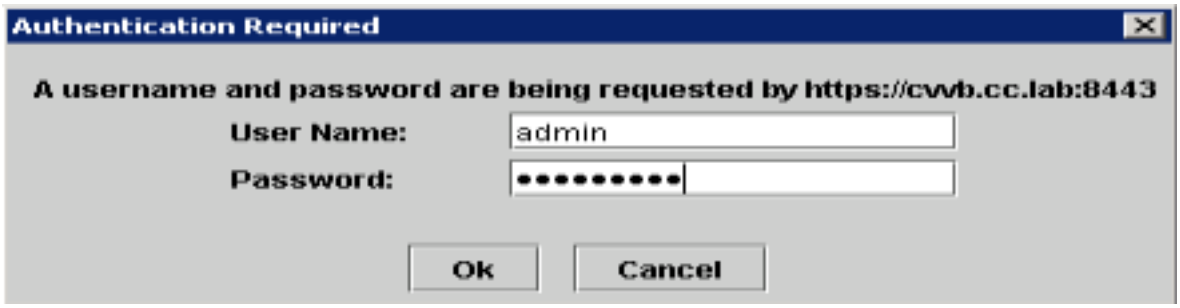


7. Geben Sie die IP-Adresse der VVB an, und klicken Sie auf **OK**.



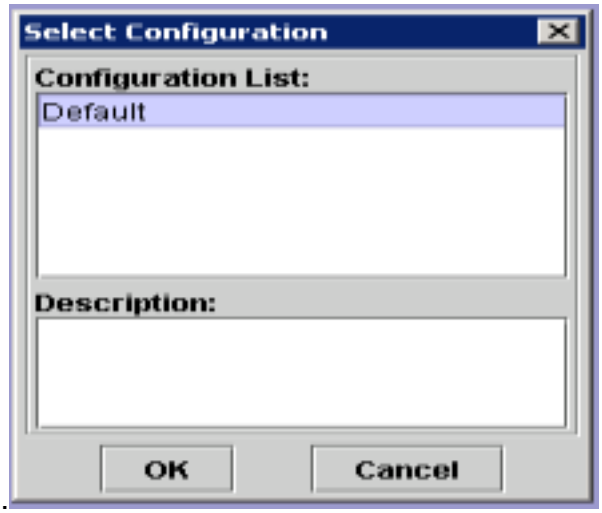
8. Akzeptieren Sie die Zertifikatinformationen, wenn diese angezeigt werden.

9. Geben Sie die Anmeldeinformationen an, und klicken Sie auf **OK**.

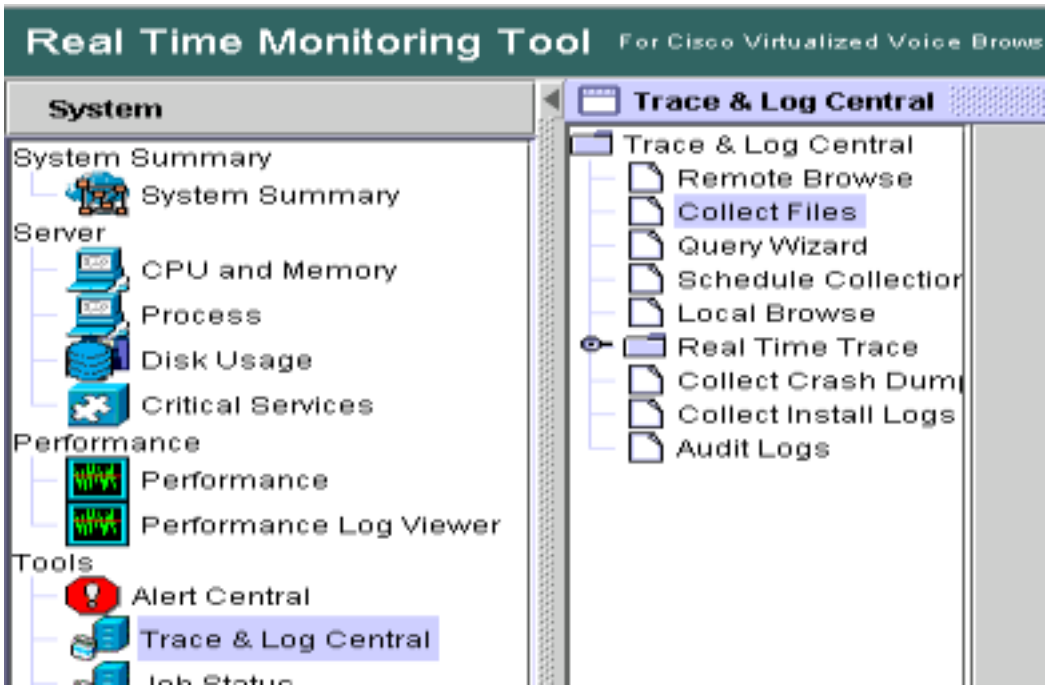


10. Wenn Sie den TimeZone-Fehler erhalten haben, kann RTMT geschlossen werden, nachdem Sie auf die Schaltfläche **Ja** geklickt haben. Starten Sie das RTMT-Tool erneut.

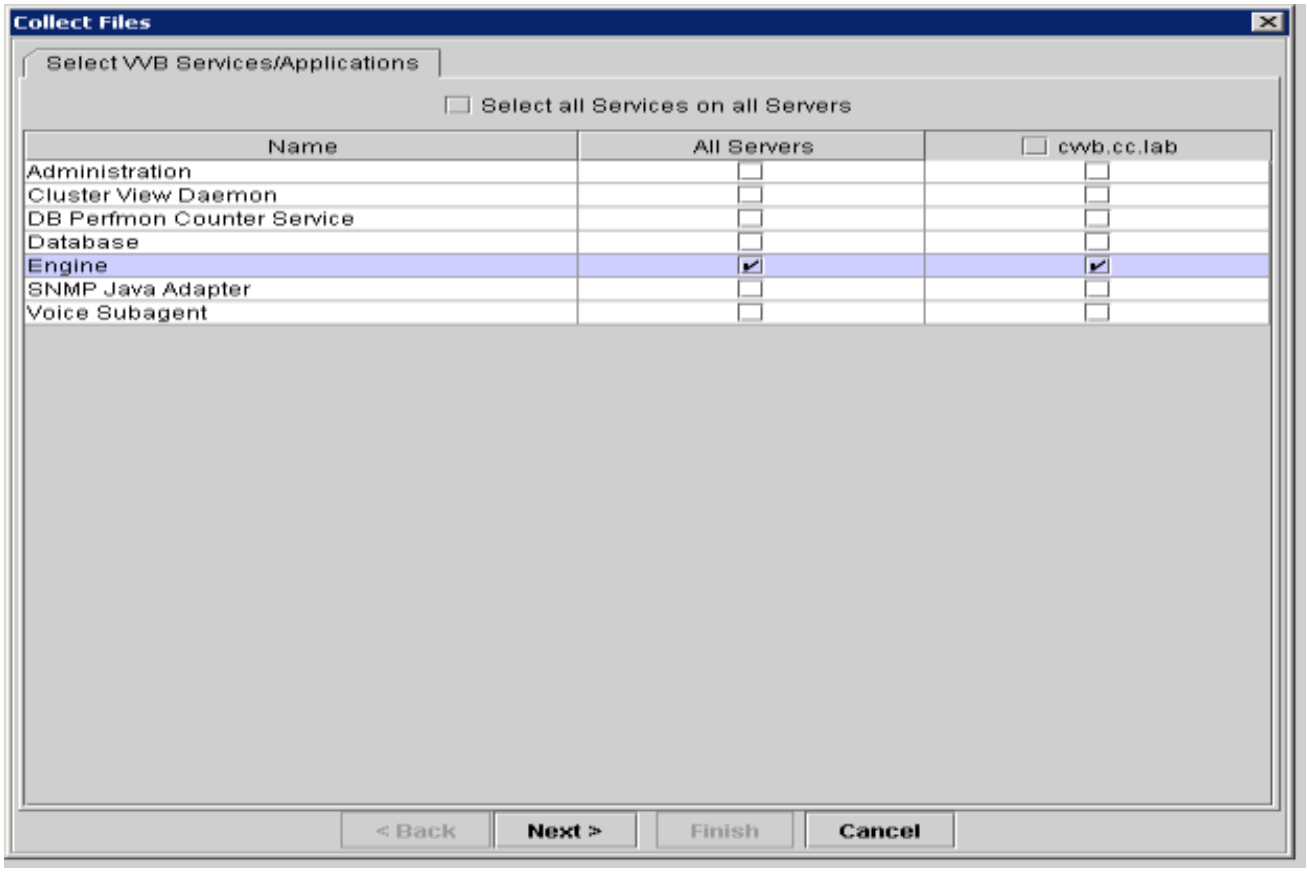
11. Lassen Sie die Standardkonfiguration ausgewählt, und klicken Sie auf **OK**.



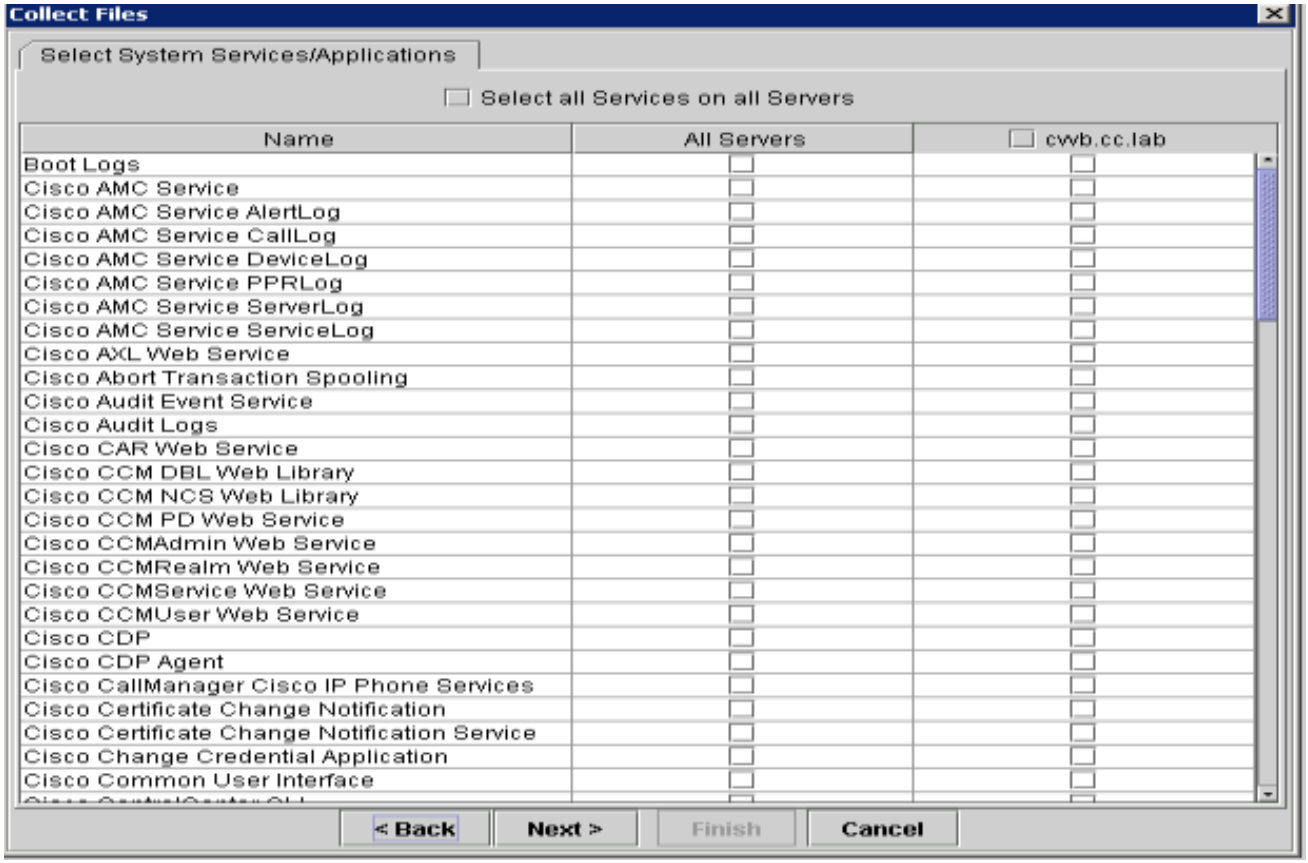
12. Wählen Sie **Trace & Log Central** und doppelklicken Sie dann auf **Dateien sammeln**.



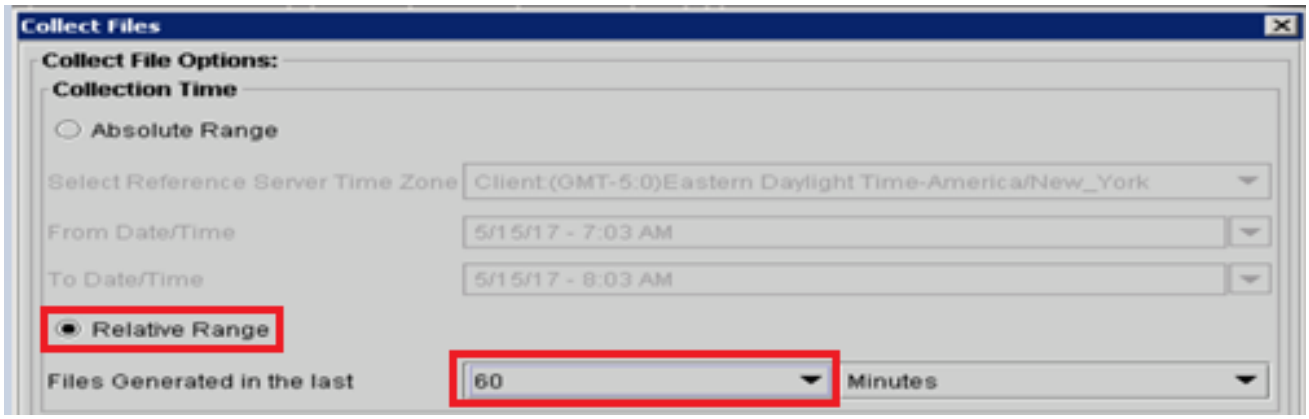
13. Wählen Sie im neu geöffneten Fenster das **Modul aus,** und klicken Sie auf Weiter.



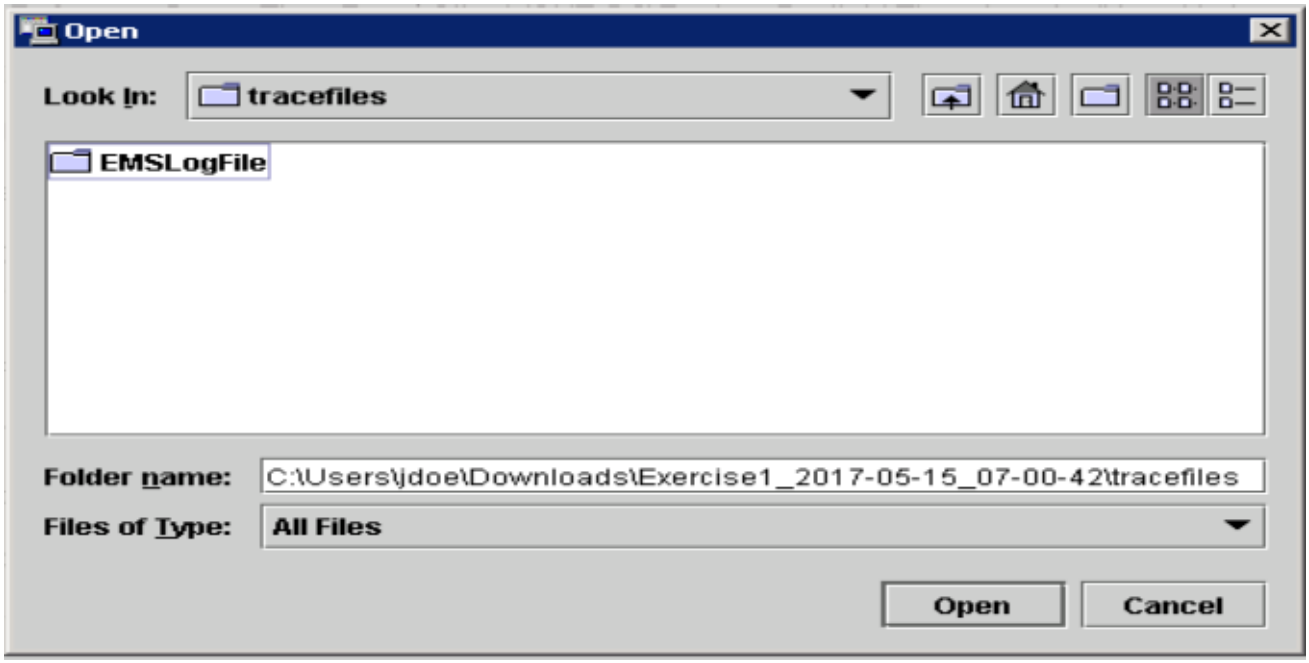
14. Klicken Sie im nächsten Fenster erneut auf **Weiter**.



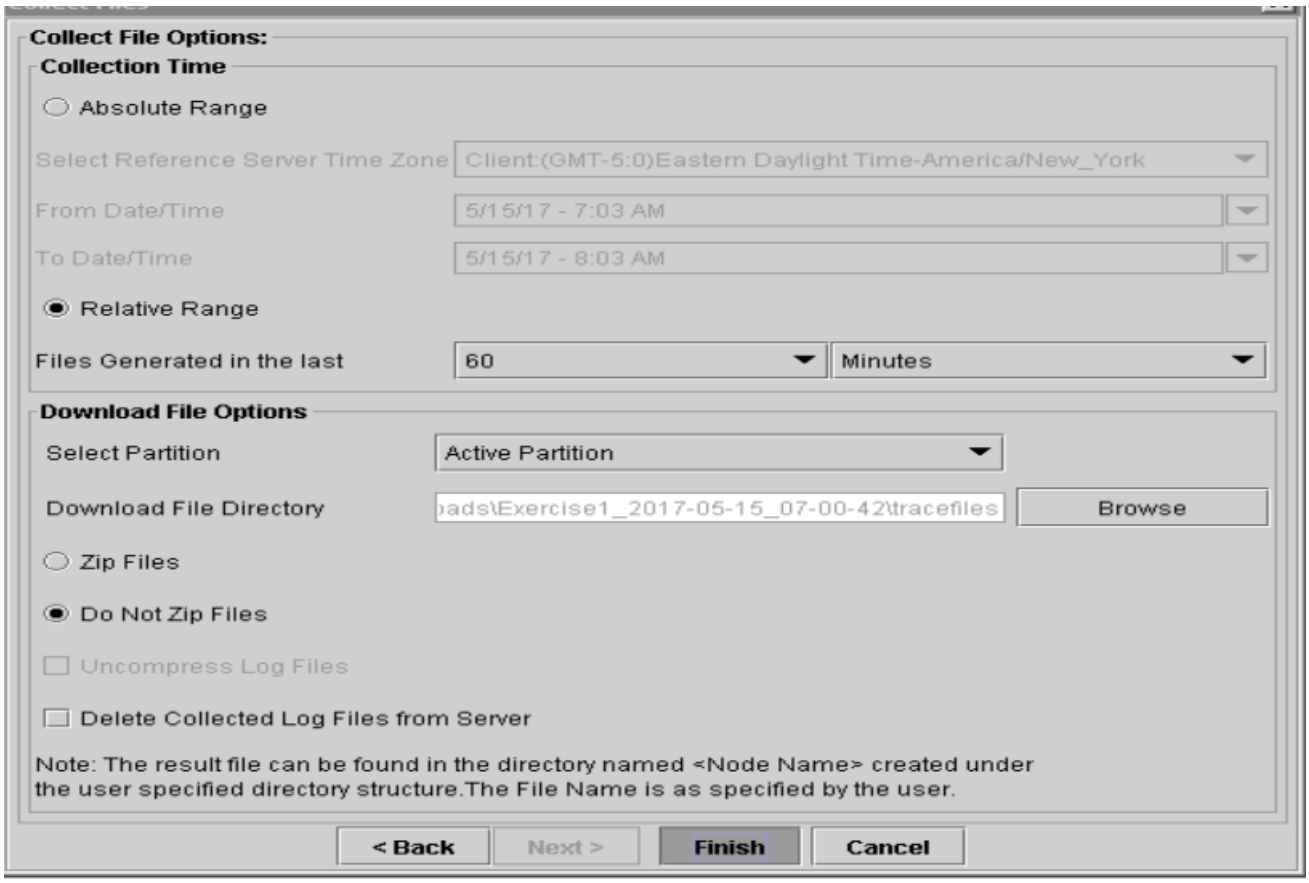
15. Wählen Sie **Relative Range (Relative Reichweite**) aus, und vergewissern Sie sich, dass Sie die Zeit für einen falschen Anruf auswählen.



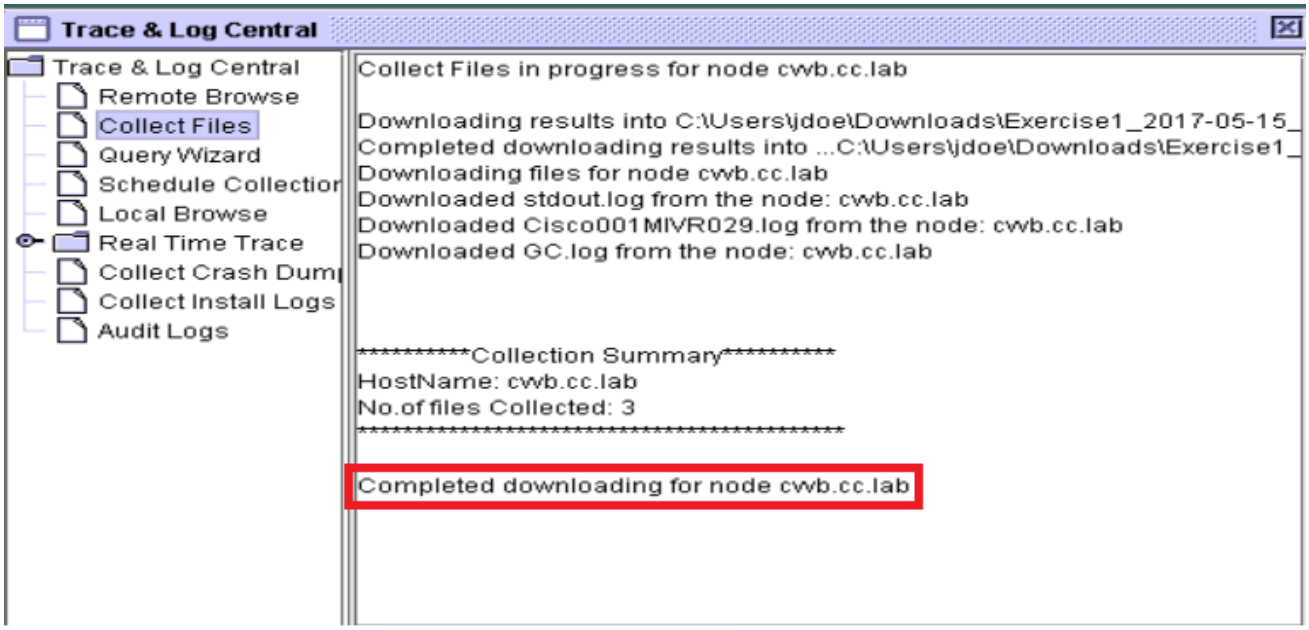
16. Klicken Sie unter Download-Dateioptionen auf **Durchsuchen**, und wählen Sie das gewünschte Verzeichnis aus. save klicken Sie auf **Öffnen**.



17. Wenn alles ausgewählt ist, klicken Sie auf die Schaltfläche **Fertig stellen**.



18. Dadurch werden die Protokolldateien gesammelt. Warten Sie, bis auf RTMT eine Bestätigungsmeldung angezeigt wird.



19. Navigieren Sie zu dem Ordner, in dem die Ablaufverfolgungen gespeichert sind.

20. Die Engine-Protokolle sind alles, was Sie benötigen. Um sie zu finden, navigieren Sie zum Ordner **\<Zeitstempel>\uccx\log\MIVR**.

Option 2: Über SSH und SFTP - Empfohlene Option

1. Melden Sie sich mit der Secure Shell (SSH) beim VVB-Server an.
2. Geben Sie diesen Befehl ein, um die benötigten Protokolle zu sammeln. Die Protokolle werden komprimiert, und Sie werden aufgefordert, den SFTP-Server zu identifizieren, auf den die Protokolle hochgeladen werden. **file get activelog /uccx/log/MIVR/***

```
Total size in Bytes: 413567
Total size in Kbytes: 403.87402
Would you like to proceed [y/n]? y
SFTP server IP:
```

3. Diese Protokolle werden im SFTP-Serverpfad gespeichert: *<IP-Adresse>\<Datums-Zeitstempel>\active_nnn.tgz,* wobei nnn ein Zeitstempel im Langformat ist.

Festlegen von Ablaufverfolgungs- und Erfassungsprotokollen für CUBE und CUSP

CUBE (SIP)

1. Legen Sie den Zeitstempel der Protokolle fest, und aktivieren Sie den Protokollierungspuffer.

```
#conf  t
service timestamps debug datetime msec
service timestamps log datetime msec
service sequence-numbers
no logging console
no logging monitor
logging buffered 5000000 7
end
clear logging
```

Warnung: Jegliche Änderung an einem produktiven Cisco IOS® Software GW kann einen Ausfall verursachen.

2. Dies ist eine sehr robuste Plattform, die die vorgeschlagenen Debug-Vorgänge im bereitgestellten Anrufvolumen problemlos verarbeiten kann. Cisco empfiehlt jedoch Folgendes: Alle Protokolle an einen Syslog-Server anstatt an den Protokollierungspuffer senden.

```
logging <syslog server ip>
logging trap debugs
```

Wenden Sie die Debug-Befehle nacheinander an, und überprüfen Sie anschließend die CPU-Auslastung.

```
show proc cpu hist
```

Warnung: Erhält die CPU eine CPU-Auslastung von bis zu 70-80 %, erhöht sich das Risiko einer leistungsbezogenen Beeinträchtigung des Service erheblich. Aktivieren Sie daher keine zusätzlichen Debugs, wenn das GW 60 % erreicht.

3. Aktivieren Sie diese Debug-Optionen:

```
debug voip ccapi inout
debug ccsip mess
After you make the call and simulate the issue, stop the debugging:
```

4. Reproduzieren Sie das Problem.
5. Deaktivieren Sie die Ablaufverfolgungen.
   ```
   #undebug all
   ```
6. Sammeln Sie die Protokolle.

```
term len 0
show ver
show run
show log
```

CUSP

1. Aktivieren Sie SIP-Ablaufverfolgungen für CUSP.
   ```
   (cusp)> config
   (cusp-config)> sip logging
   (cusp)> trace enable
   (cusp)> trace level debug component sip-wire
   ```
2. Reproduzieren Sie das Problem.
3. Deaktivieren Sie die Protokollierung, sobald Sie fertig sind.

Protokolle sammeln

1. Konfigurieren Sie einen Benutzer für den CUSP (z. B.: Test).
2. Fügen Sie diese Konfiguration an der CUSP-Eingabeaufforderung hinzu.
   ```
   username <userid> create
   username <userid> password <password>
   username <userid> group pfs-privusers
   ```
3. FTP an die CUSP-IP-Adresse Verwenden Sie den Benutzernamen (Test) und das Kennwort wie im vorherigen Schritt definiert.
4. Ändern Sie die Verzeichnisse in /cusp/log/trace.
5. Rufen Sie log_<Dateiname> ab.

Festlegen von Trace und Sammeln von UCCE-Protokollen

Cisco empfiehlt, Ablaufverfolgungsebenen festzulegen und Ablaufverfolgungen mithilfe des Diagnostik-Framework-Portfolios oder der System-CLI-Tools zu erfassen.

> **Anmerkung:** Weitere Informationen zum Diagnostic Framework-Portfolio und zur System-CLI finden Sie im Kapitel Diagnosetools im Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1).

Wenn Sie bei den meisten UCCE-Szenarien eine Fehlerbehebung durchführen und die Standardstufe der Ablaufverfolgungen nicht genügend Informationen liefert, setzen Sie die Stufe der Ablaufverfolgungen in den erforderlichen Komponenten (mit einigen Ausnahmen) auf 3.

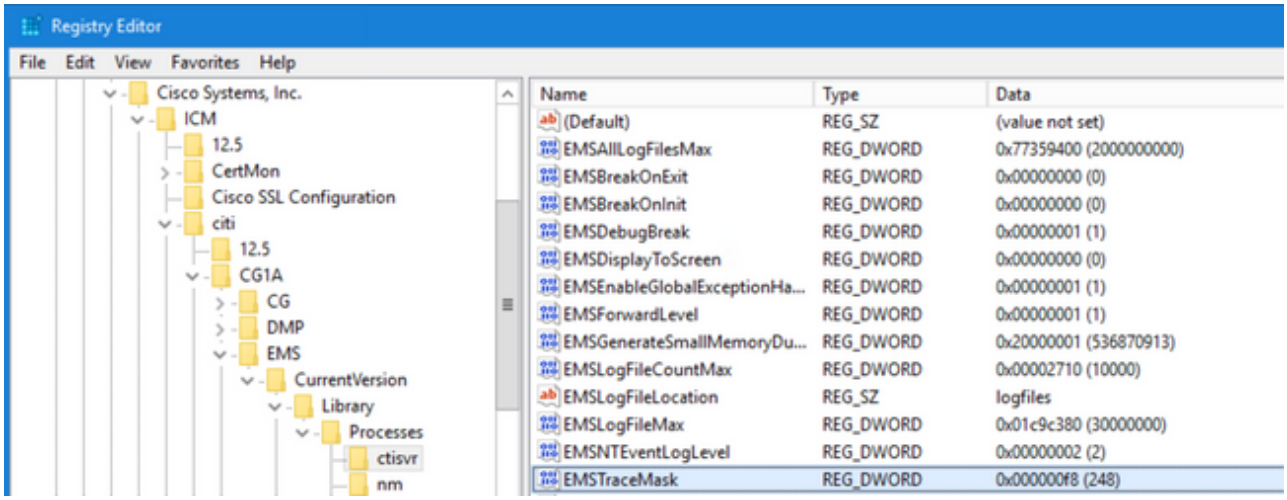
> **Anmerkung: Weitere Informationen finden Sie** im Abschnitt Ablaufverfolgungsebene im Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1).

Wenn Sie beispielsweise Probleme mit Outbound Dialer beheben, muss die Ablaufverfolgungsebene auf Ebene 2 festgelegt werden, wenn der Dialer beschäftigt ist.

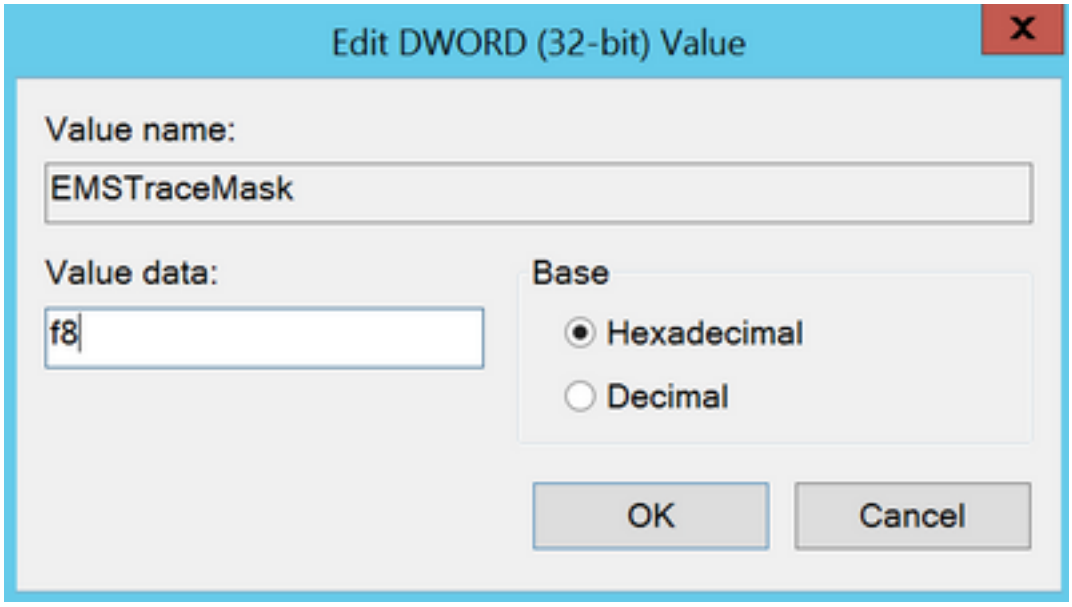
Für CTISVR (CTISVR) wird in Stufe 2 und Stufe 3 nicht die von Cisco empfohlene Registrierungsebene festgelegt. Die empfohlene Ablaufverfolgungsregistrierung für CTISVR ist 0XF8.

1. Öffnen Sie auf dem UCCE Agent PG den Registrierungs-Editor (Regedit).

2. Navigieren Sie zu HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a und b)\EMS\CurrentVersion\library\Processes\ctisvr.



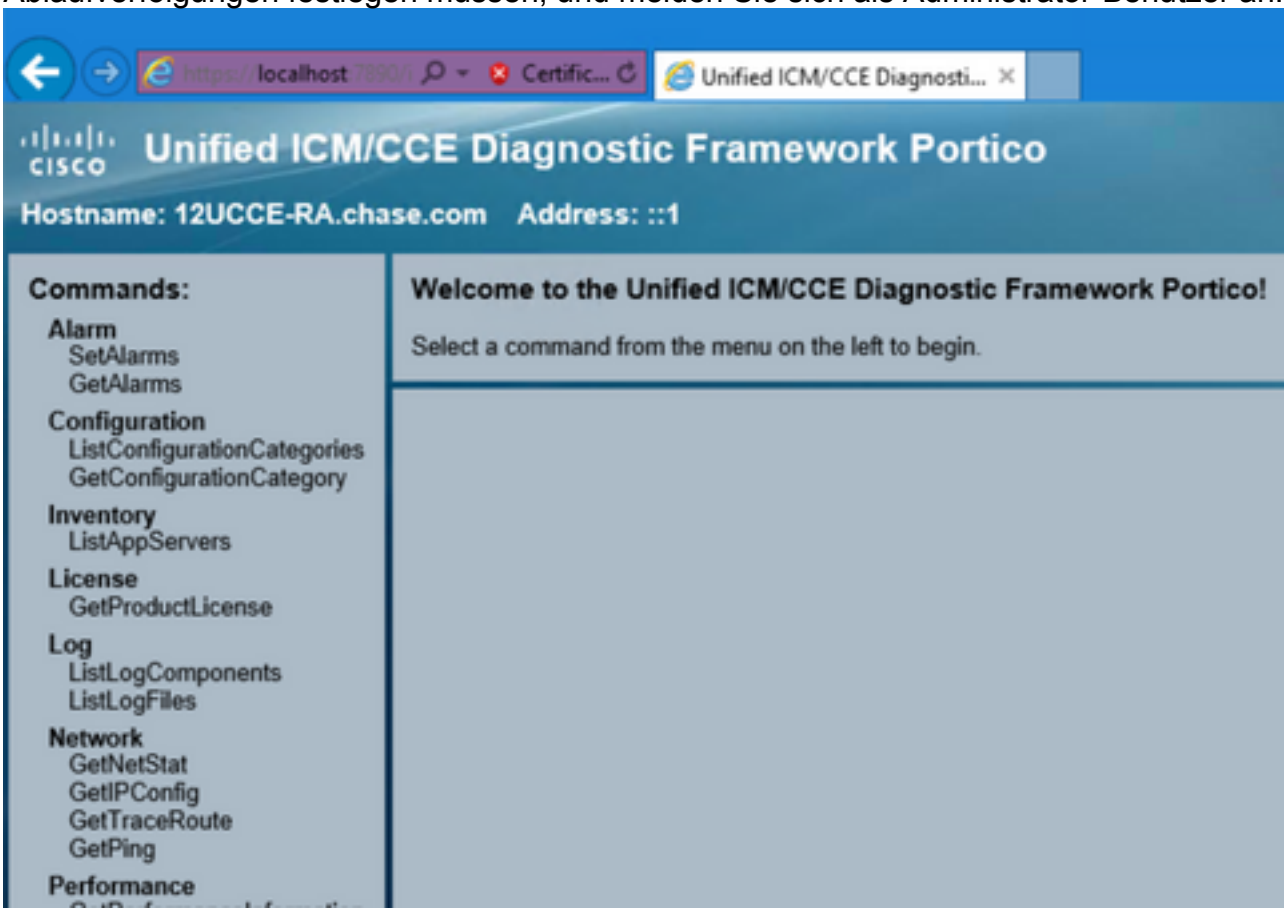
3. Doppelklicken Sie auf **EMSTraceMask**, und legen Sie den Wert auf **f8 fest**.



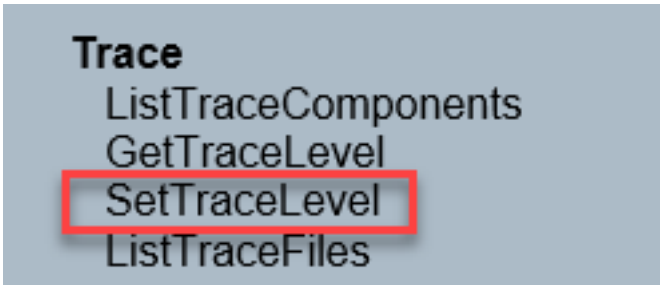
4. Klicken Sie auf **OK**, und schließen Sie den Registrierungs-Editor. Dies sind die Schritte zum Festlegen der UCCE-Komponentenspuren (der RTR-Prozess wird als Beispiel verwendet).

SetTrace-Ebene

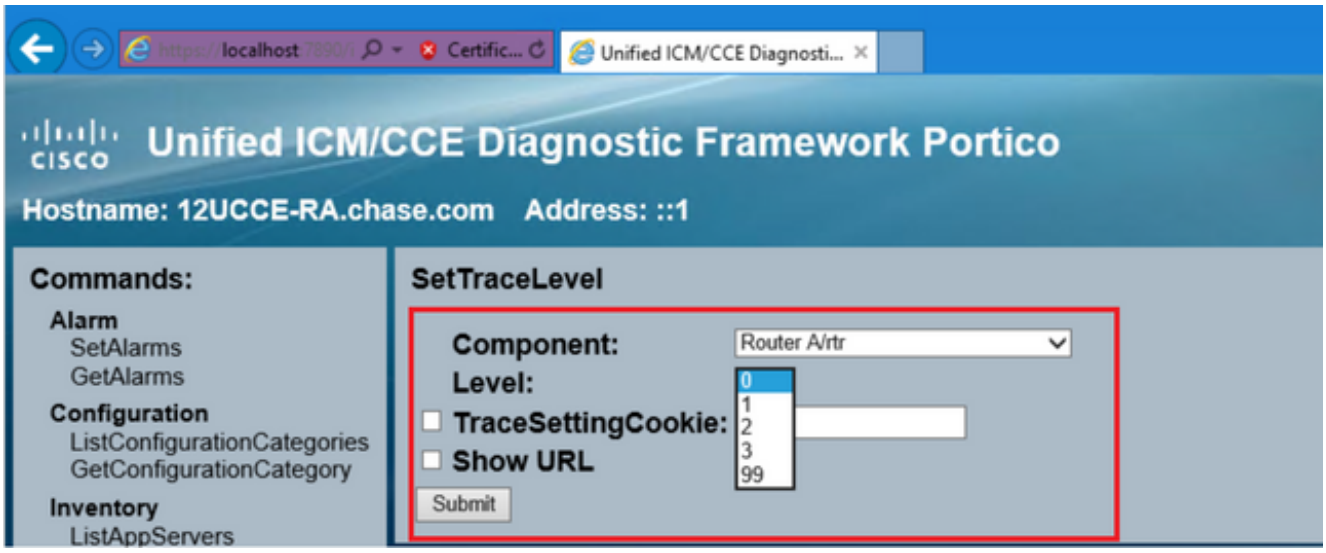
1. Öffnen Sie das Diagnose-Framework-Portfolio auf dem Server, auf dem Sie die Ablaufverfolgungen festlegen müssen, und melden Sie sich als Administrator-Benutzer an.



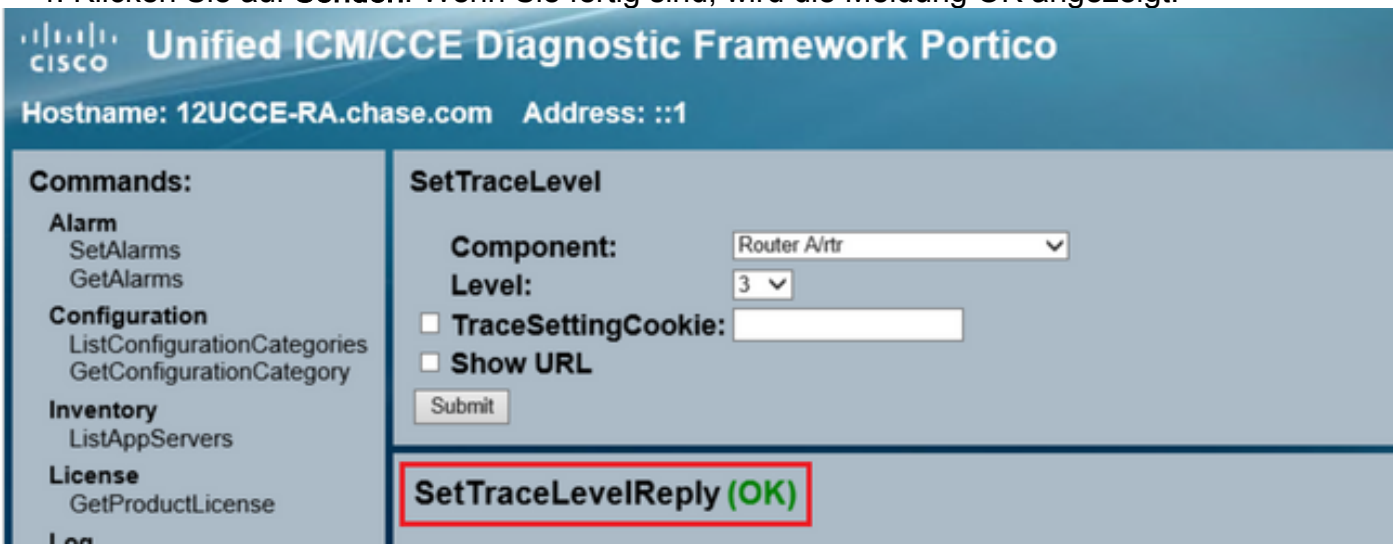
2. Navigieren Sie im Abschnitt "Befehle" zu **Nachverfolgung,** und wählen Sie **SetTraceLevel**



3. Wählen Sie im Fenster **SetTraceLevel** die Komponente und die Ebene aus.



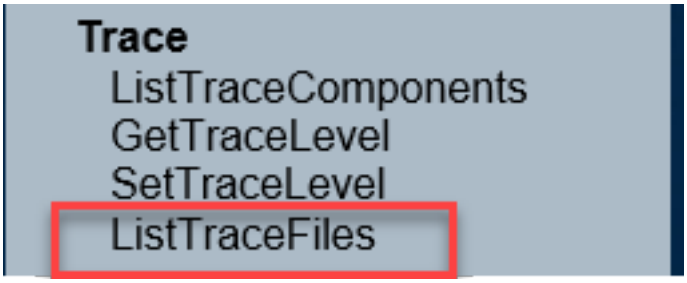
4. Klicken Sie auf **Senden**. Wenn Sie fertig sind, wird die Meldung OK angezeigt.



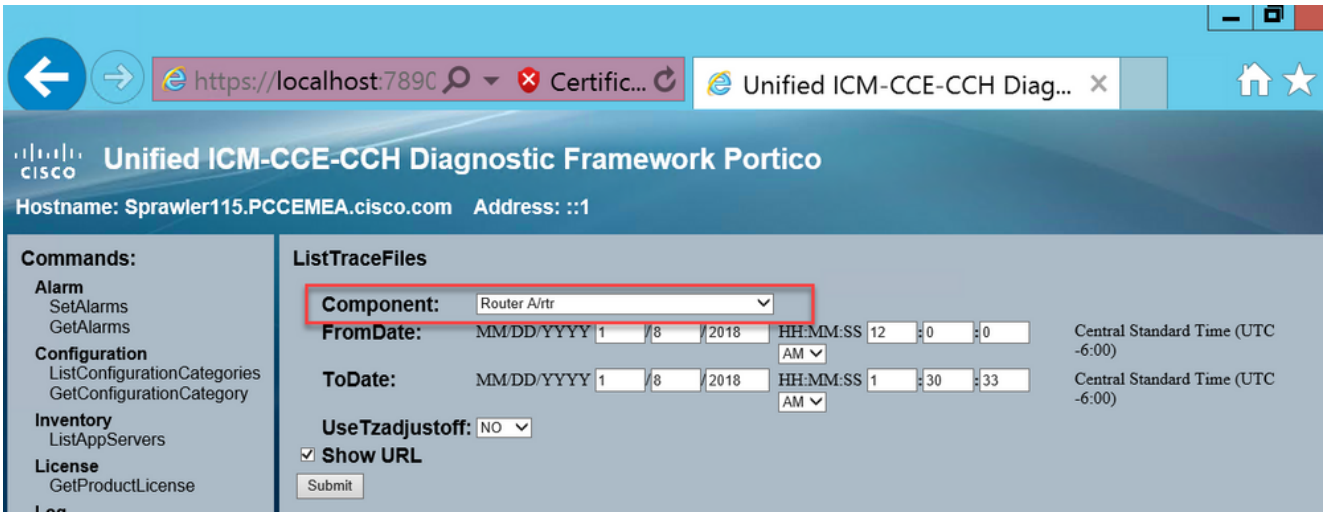
Warnung: Legen Sie die Ebene der Ablaufverfolgungen auf Ebene 3 fest, während Sie versuchen, das Problem zu reproduzieren. Nachdem das Problem reproduziert wurde, setzen Sie die Ablaufverfolgungsebene auf den Standardwert. Seien Sie besonders vorsichtig, wenn Sie die JTAPIGW-Ablaufverfolgungen festlegen, da Level 2 und Level 3 die Ablaufverfolgungen auf niedriger Ebene festlegen. Dies kann die Leistung beeinträchtigen. Stellen Sie Ebene 2 oder Ebene 3 im JTAPIGW ein, wenn Sie sich nicht in der Produktionsumgebung befinden, oder in einer Laborumgebung.

Protokollsammlung

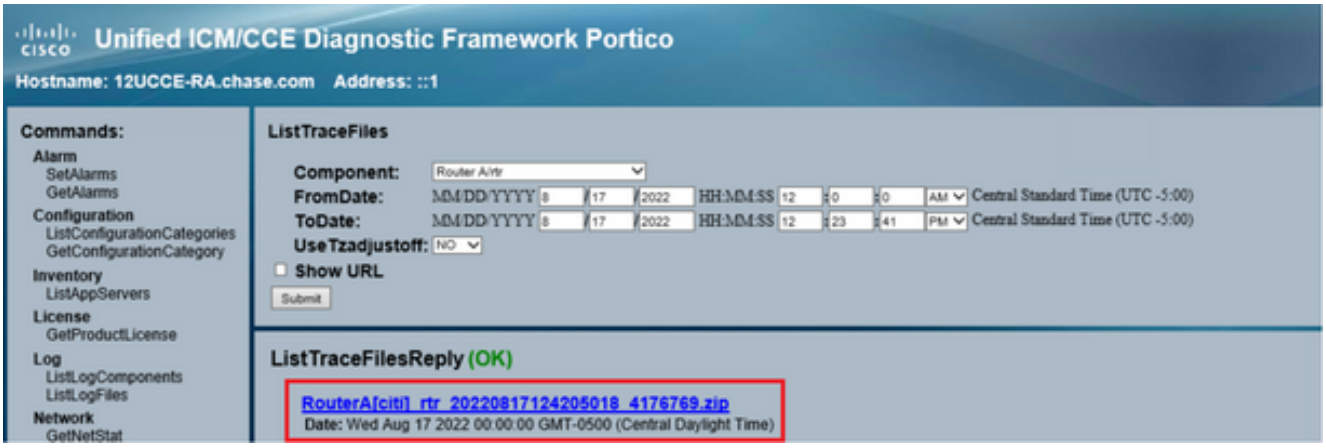
1. Navigieren Sie im Diagnostic Framework-Portfolio im Abschnitt **Commands** zu **Trace,** und wählen Sie **ListTraceFile aus**.



2. Wählen Sie im Fenster **ListTraceFile** die **Komponenten**, **FromDate** und **ToDate aus**. Aktivieren Sie das **Feld "URL anzeigen",** und klicken Sie dann auf **Senden**.



3. Wenn die Anforderung beendet ist, wird die Meldung OK mit dem Link zur ZIP-Protokolldatei angezeigt.



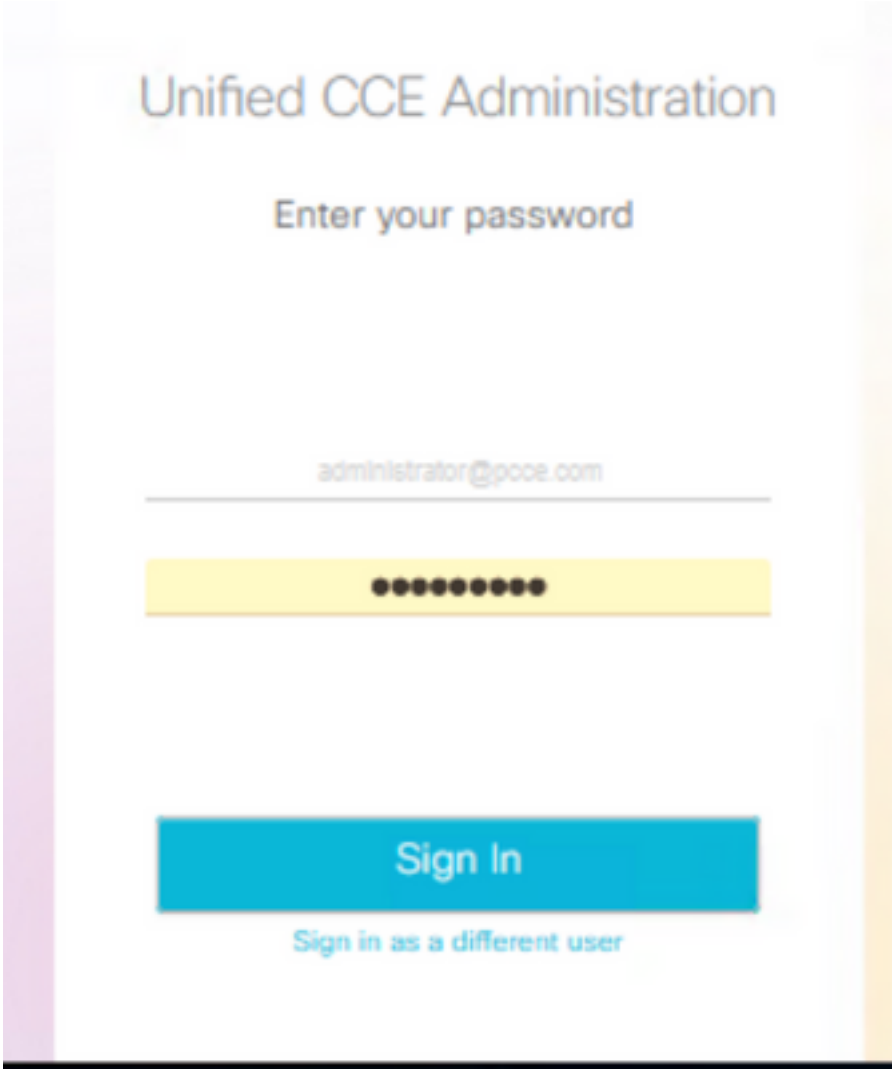
4. Klicken Sie auf den ZIP-Datei-Link und save die Datei an dem von Ihnen gewählten Speicherort.

Festlegen von Ablaufverfolgung und Erfassen von PCCE-Protokollen

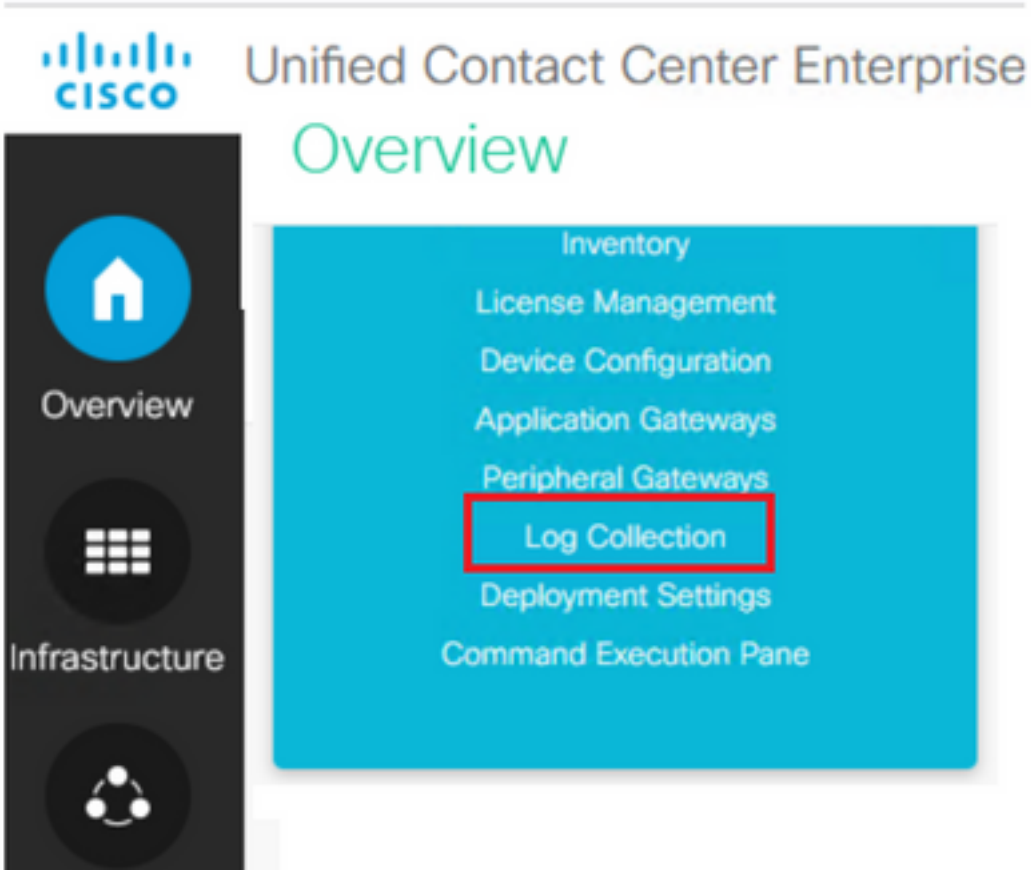
PCCE verfügt über ein eigenes Tool zum Einrichten von Ablaufverfolgungsebenen. Dies gilt nicht

für UCCE-Umgebungen, in denen das Diagnose-Framework-Portal oder die System-CLI die bevorzugten Methoden zum Aktivieren und Erfassen von Protokollen darstellen.

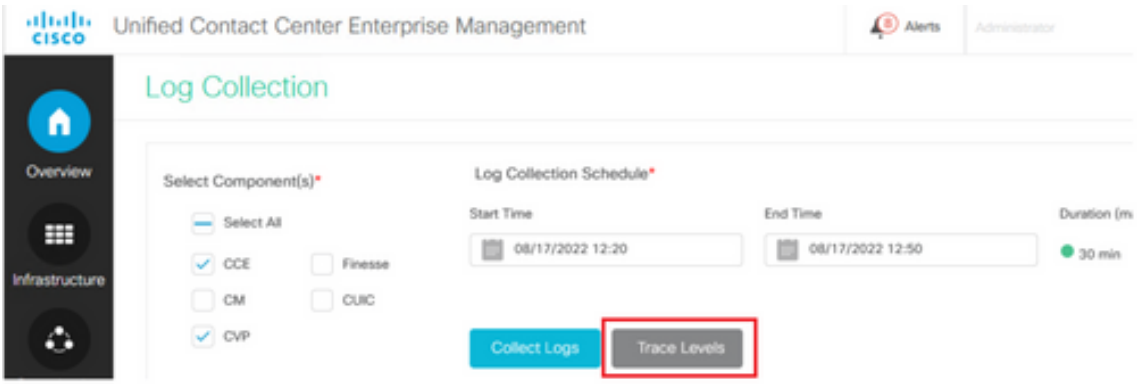
1. Öffnen Sie auf dem PCCE AW-Server das Unified CCE-Webverwaltungstool, und melden Sie sich beim Administratorkonto an.



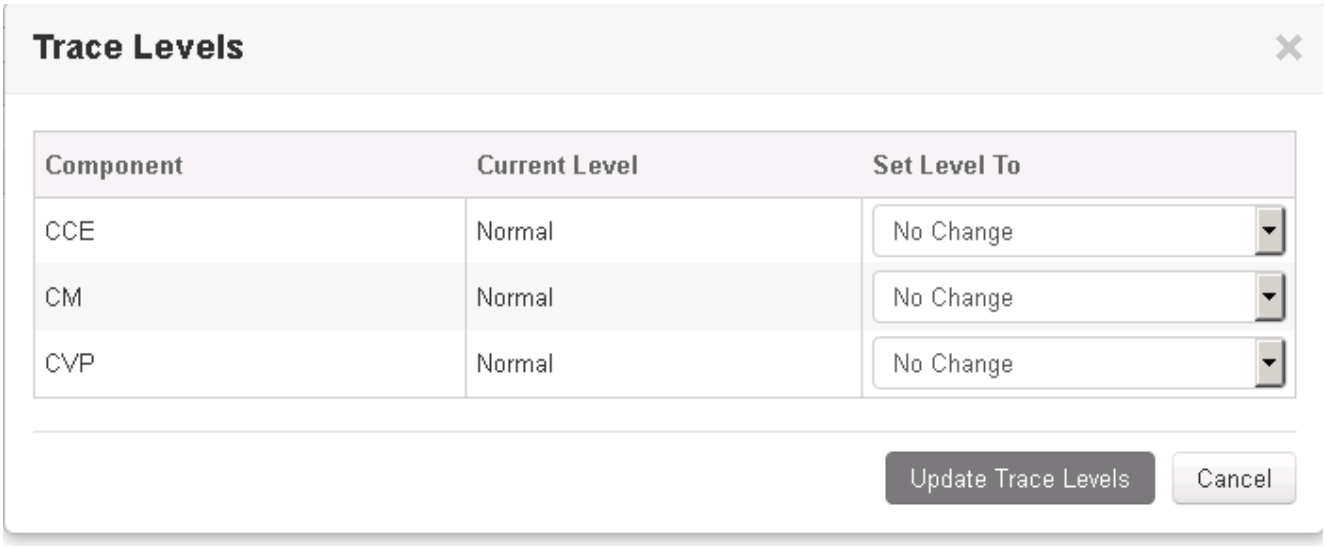
2. Navigieren Sie zu **Overview->Infrastructure Settings->Log Collection**, um die Seite Log Collection zu öffnen.



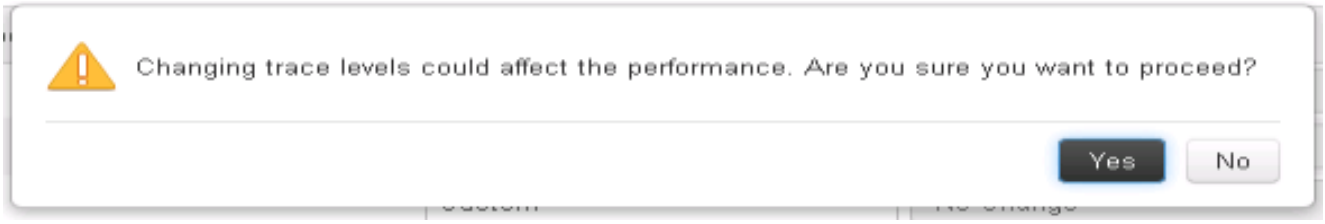
3. Klicken Sie auf der Seite Protokollsammlung auf **Ablaufverfolgungsebenen,** wodurch das Dialogfeld **Ablaufverfolgungsebenen** geöffnet wird.



4. Legen Sie die Nachverfolgungsebene für CCE auf "**Detailed**" fest, und belassen Sie sie bei "**No Change** for CM and CVP". Klicken Sie dann auf **Trace-Ebenen aktualisieren**



5. Klicken Sie auf **Ja**, um die Warnung zu bestätigen.



6. Wenn das Problem reproduziert wurde, öffnen Sie die **Unified CCE-Verwaltung,** und navigieren Sie zurück zum **System > Protokollsammlung.**
7. Wählen Sie im Bereich "Komponenten" die Optionen **CCE** und **CVP aus**.
8. Wählen Sie die entsprechende Protokollerfassungszeit aus (standardmäßig die letzten 30 Minuten).
9. Klicken Sie auf **Collect Logs** (**Protokolle sammeln**) und auf **Yes** (Ja), um die Dialogwarnung auszugeben. Die Protokollsammlung wird gestartet. Warten Sie einige Minuten, bevor es fertig ist.

10. Klicken Sie abschließend auf die Schaltfläche **Download** in der Spalte **Aktionen**, um eine gezippte Datei mit allen Protokollen herunterzuladen. Save die **ZIP**-Datei an einem beliebigen Speicherort ablegen, den Sie benötigen.

Nachverfolgung einrichten und CUIC-/Live-Daten-/IDS-Protokolle sammeln

Protokolle mit SSH herunterladen

1. Melden Sie sich bei der SSH-Befehlszeile von CUIC, LD und IDS an.

2. Führen Sie den Befehl aus, um CUIC-bezogene Protokolle zu erfassen.

file get activelog /cuic/logs/cuic/*.* recurs compress reltime hours 1

file get activelog /cuic/logs/cuicsrvr/*.* recurs compress reltime hours 1
file get activelog tomcat/logs/*.* recurs compress

3. Führen Sie den Befehl aus, um LD-bezogene Protokolle zu erfassen.

   file get activelog livedata/logs/*.*

4. Führen Sie den Befehl aus, um IDs-bezogene Protokolle zu sammeln.

   file get activelog ids/log/*.* recurs compress reltime days 1

5. Diese Protokolle werden im SFTP-Serverpfad gespeichert: <IP-Adresse>\<Datums-Zeitstempel>\active_nnn.tgz , wobei nnn ein Zeitstempel im Langformat ist.

Protokolle mit RTMT herunterladen

1. Laden Sie RTMT von der OAMP-Seite herunter. Melden Sie sich bei https://<HOST-ADRESSE>/oamp an, wobei HOST-ADRESSE die IP-Adresse des Servers ist.

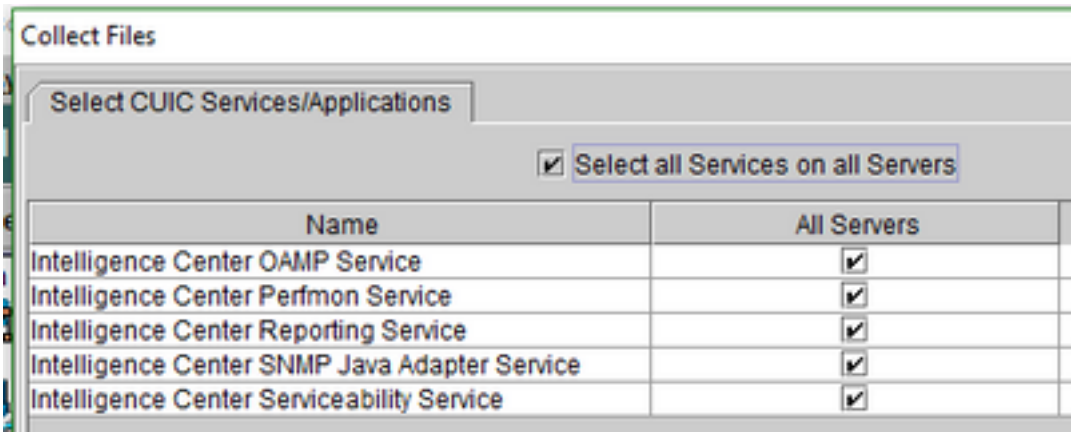
2. Navigieren Sie zu **Extras > RTMT-Plugin herunterladen.** Laden Sie das Plugin herunter und installieren Sie es.

3. Starten Sie RTMT, und melden Sie sich mit Administratorrechten beim Server an.

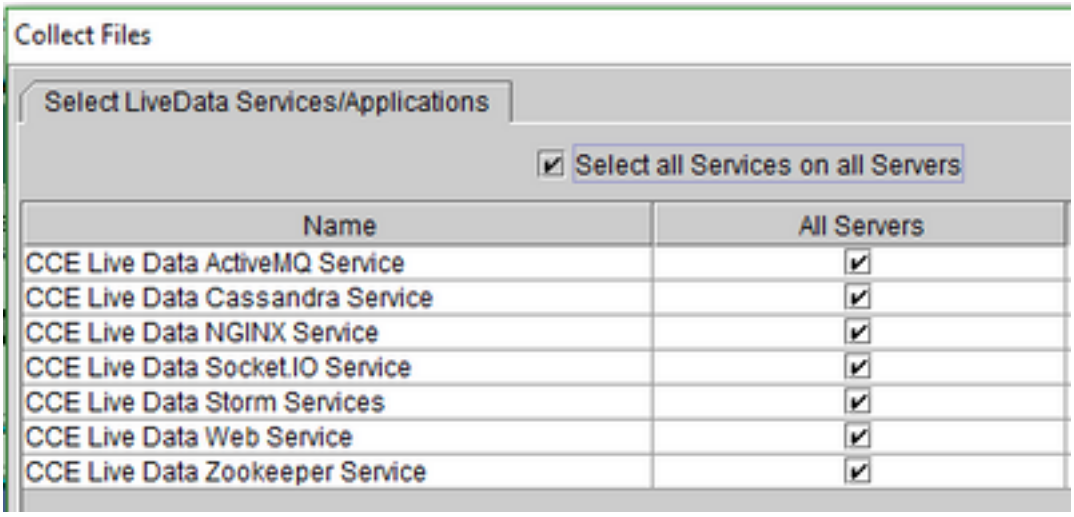
4. Doppelklicken Sie auf **Trace and Log Central** und doppelklicken Sie dann auf **Collect Files**.

5. Sie können diese Registerkarten für die jeweiligen Services sehen. Sie müssen alle Services/Server für CUIC, LD und IDS auswählen.

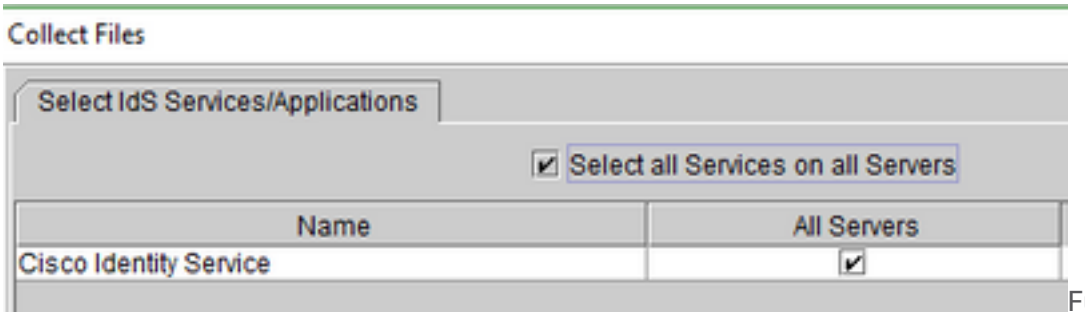
   Für CUIC:



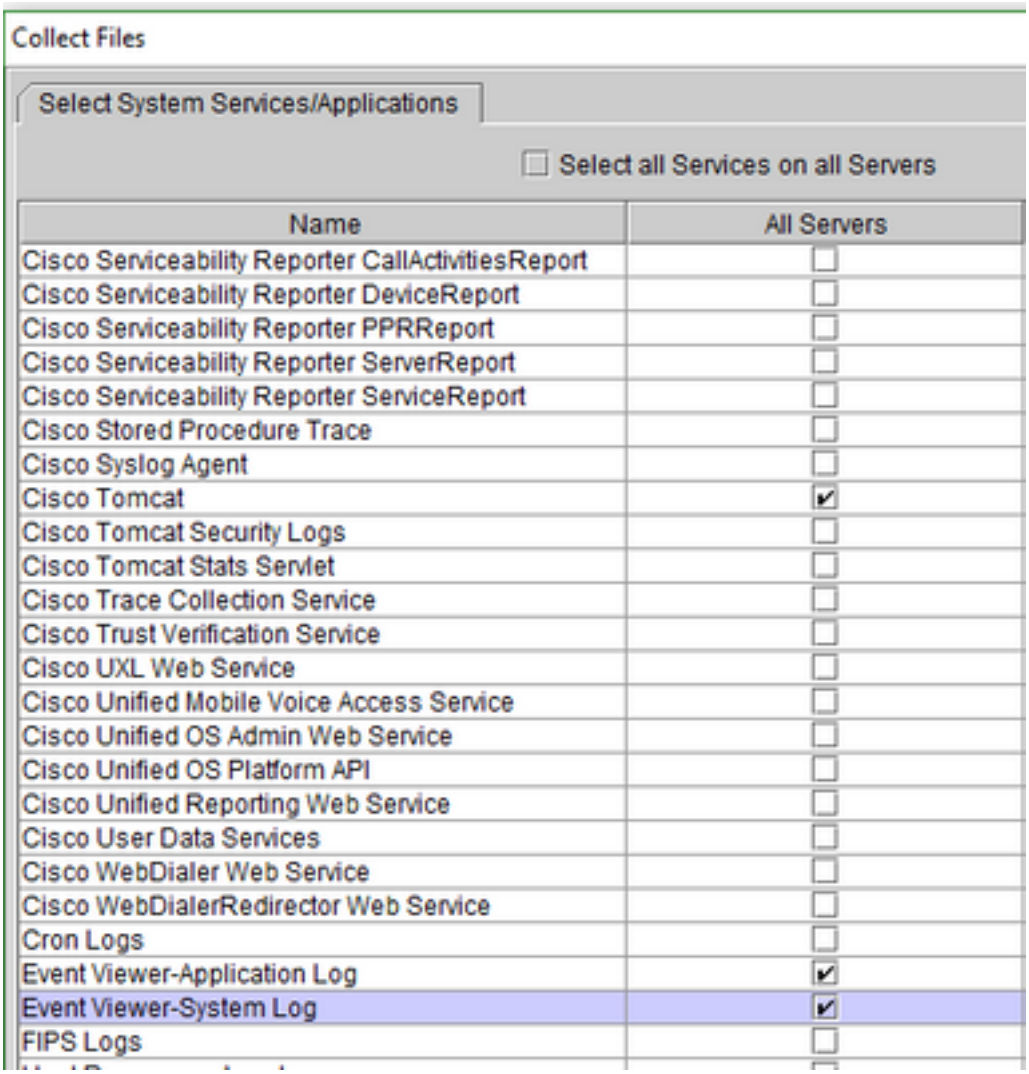
   Für LD:



Für IDS:

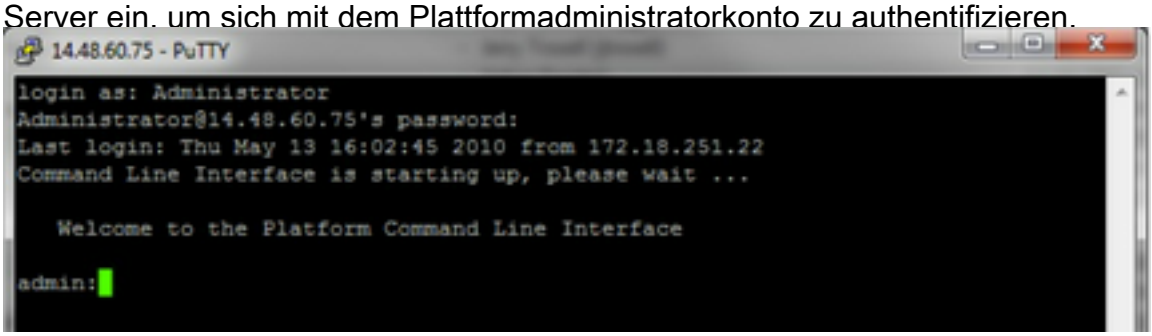


Für Plattformdienste ist es generell empfehlenswert, Tomcat und Ereignisanzeige-Protokolle auszuwählen:



6. Wählen Sie das **Datum und die Uhrzeit** zusammen mit dem Zielordner aus, um save die Protokolle.

Paketerfassung über VoS (Finesse, CUIC, VVB)

1. Erfassung starten Richten Sie zum Starten der Erfassung eine SSH-Sitzung mit dem VOS-Server ein, um sich mit dem Plattformadministratorkonto zu authentifizieren.
2. 

1a) Befehlssyntax

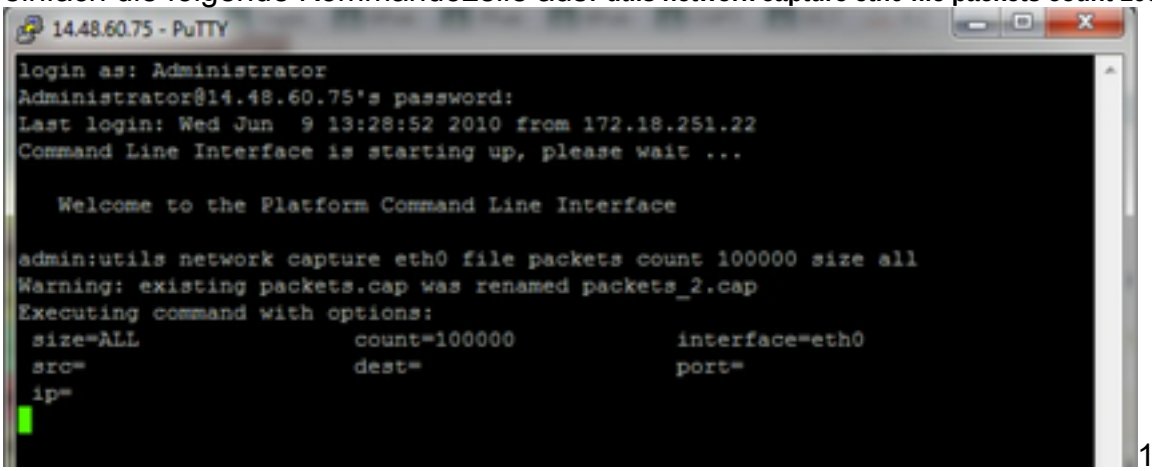
Der Befehl lautet **utils network capture**und die Syntax lautet wie folgt:

```
Syntax:
utils network capture [options]
options  optional
```

```
page,numeric,file fname,count num,size bytes,src addr,dest addr,port
num,host protocol addr
options are:
page
- pause output
numeric               - show hosts as dotted IP
addresses
file fname            - output the information to a file

Note: The file is saved in platform/cli/fname.cap

fname should not contain the "." character
count num             - a
count of the number of packets to capture
   Note: The maximum count
for the screen is 1000, for a file is 100000
size bytes            -
the number of bytes of the packet to capture
   Note: The maximum
number of bytes for the screen is 128
         For a file it can be
any number or ALL
src addr              - the source address of the
packet as a host name or IPV4 address
dest addr             - the
destination address of the packet as a host name or IPV4 address
port
num              - the port number of the packet (either src or dest)
host
protocol addr    - the protocol should be one of the following:
ip/arp/rarp/all. The host address of the packet as a host name or IPV4
address. This option  will display all packets to and from that address.

Note: If "host" is provided, do not provide "src" or "dest"
```

1b) Gesamten Datenverkehr erfassen

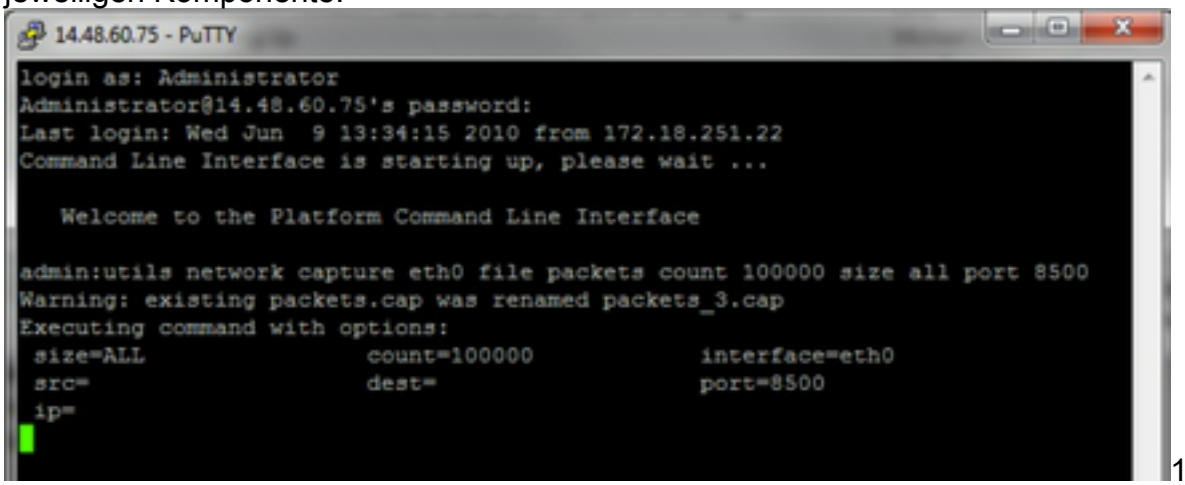
Für eine typische Erfassung kann man ALLE Pakete ALLER Größen von und bis ALLE Adressen in einer Erfassungsdatei namens packages.cap sammeln. Führen Sie dazu einfach die folgende Kommandozeile aus: **utils network capture eth0 file packets count 100000 size all**



1c) Erfassung basierend auf Portnummer

Um ein Kommunikationsproblem mit dem Cluster Manager zu beheben, kann es wünschenswert sein, die Port-Option zu verwenden, um die Daten basierend auf einem bestimmten Port (8500) zu erfassen.

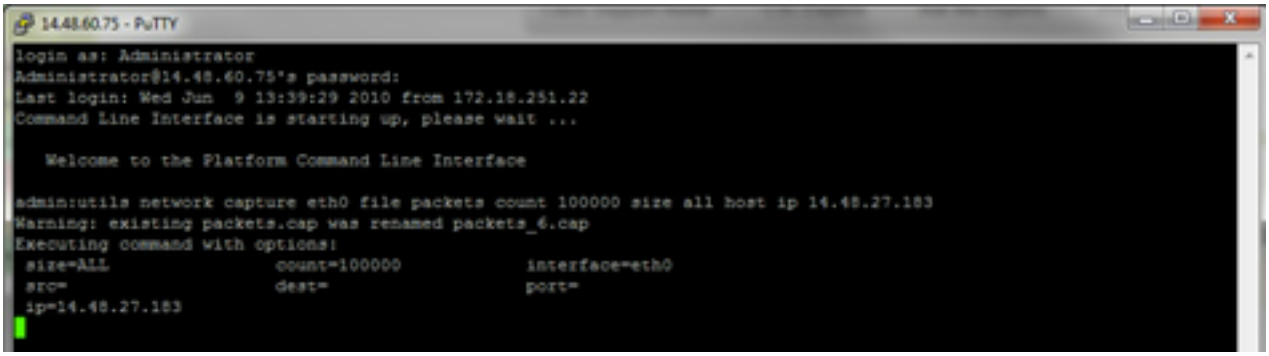
Weitere Informationen darüber, welche Dienste an jedem Port kommunizieren müssen, finden Sie in der TCP- und UDP-Port-Nutzungsanleitung für die jeweilige Version der jeweiligen Komponente.



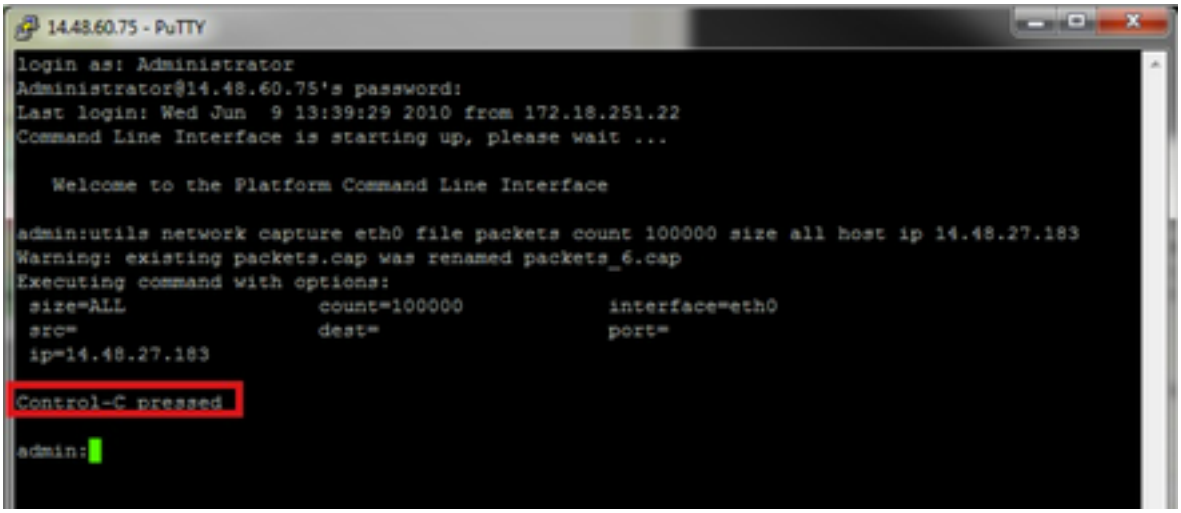
1d) Erfassung nach Host

Um ein Problem mit VOS und einem bestimmten Host zu beheben, kann es erforderlich sein, die Option "host" zu verwenden, um nach Datenverkehr zu und von einem bestimmten Host zu filtern.

Es kann auch notwendig sein, einen bestimmten Host auszuschließen, in diesem Fall ein "!" vor dem IP. Ein Beispiel dafür wäre **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

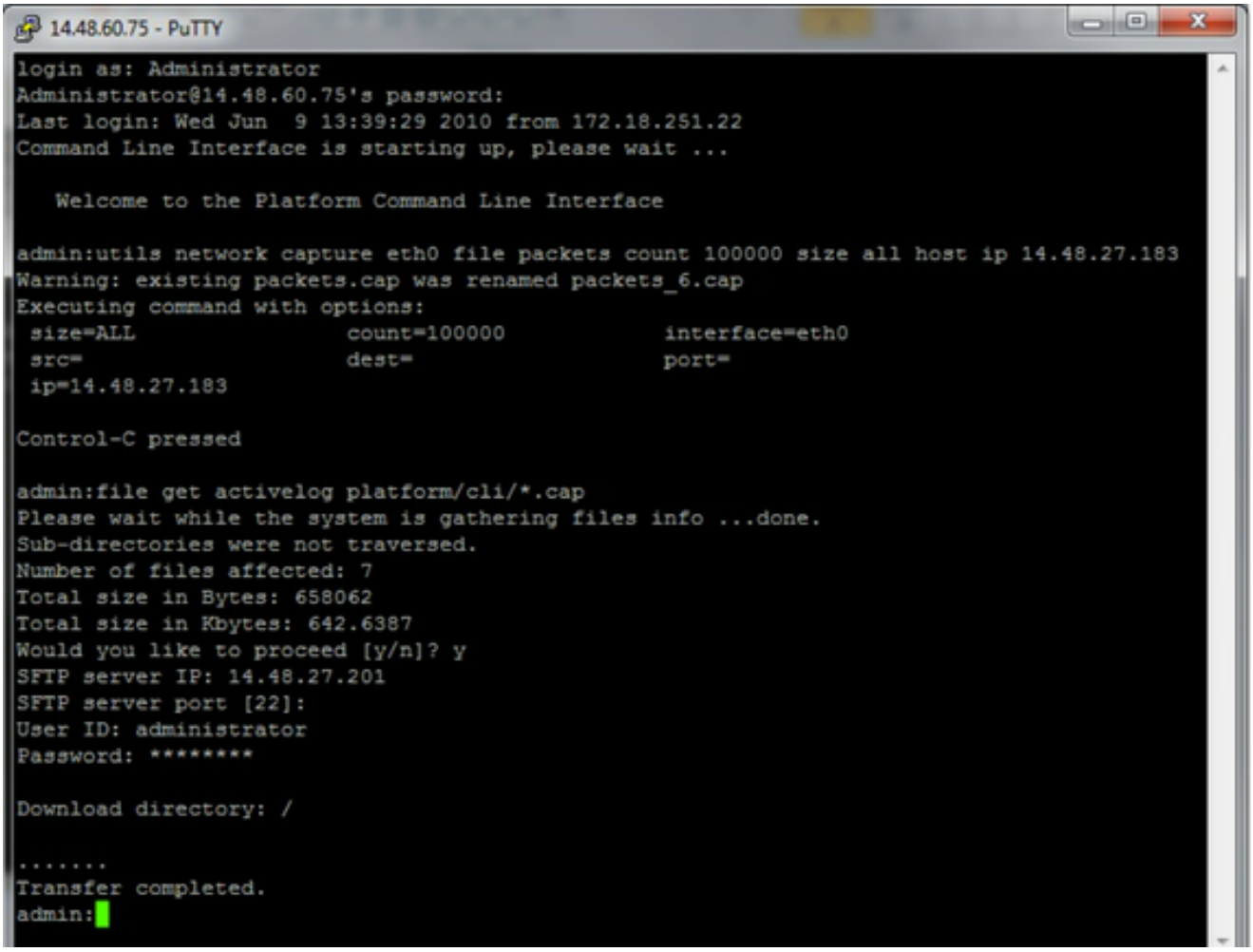


3. Reproduzieren des Symptoms des Problems Während der Erfassung wird damit begonnen, das Symptom oder den Zustand des Problems zu reproduzieren, sodass die erforderlichen Pakete in die Erfassung einbezogen werden. Wenn das Problem zeitweilig auftritt, kann es erforderlich sein, die Erfassung für einen längeren Zeitraum auszuführen. Wenn die Erfassung beendet wird, ist der Puffer gefüllt, starten Sie die Erfassung neu, und die vorherige Erfassung wird automatisch umbenannt, damit die vorherige Erfassung nicht verloren geht. Wenn eine Datenerfassung über einen längeren Zeitraum erforderlich ist, verwenden Sie eine Überwachungssitzung auf einem Switch, um die Datenerfassung auf Netzwerkebene durchzuführen.
4. Erfassung beenden Um die Erfassung zu stoppen, halten Sie die **Strg**-Taste gedrückt und drücken **C** auf der Tastatur. Dadurch wird der Erfassungsprozess beendet, und dem Erfassungs-Dump werden keine neuen Pakete hinzugefügt.
5.



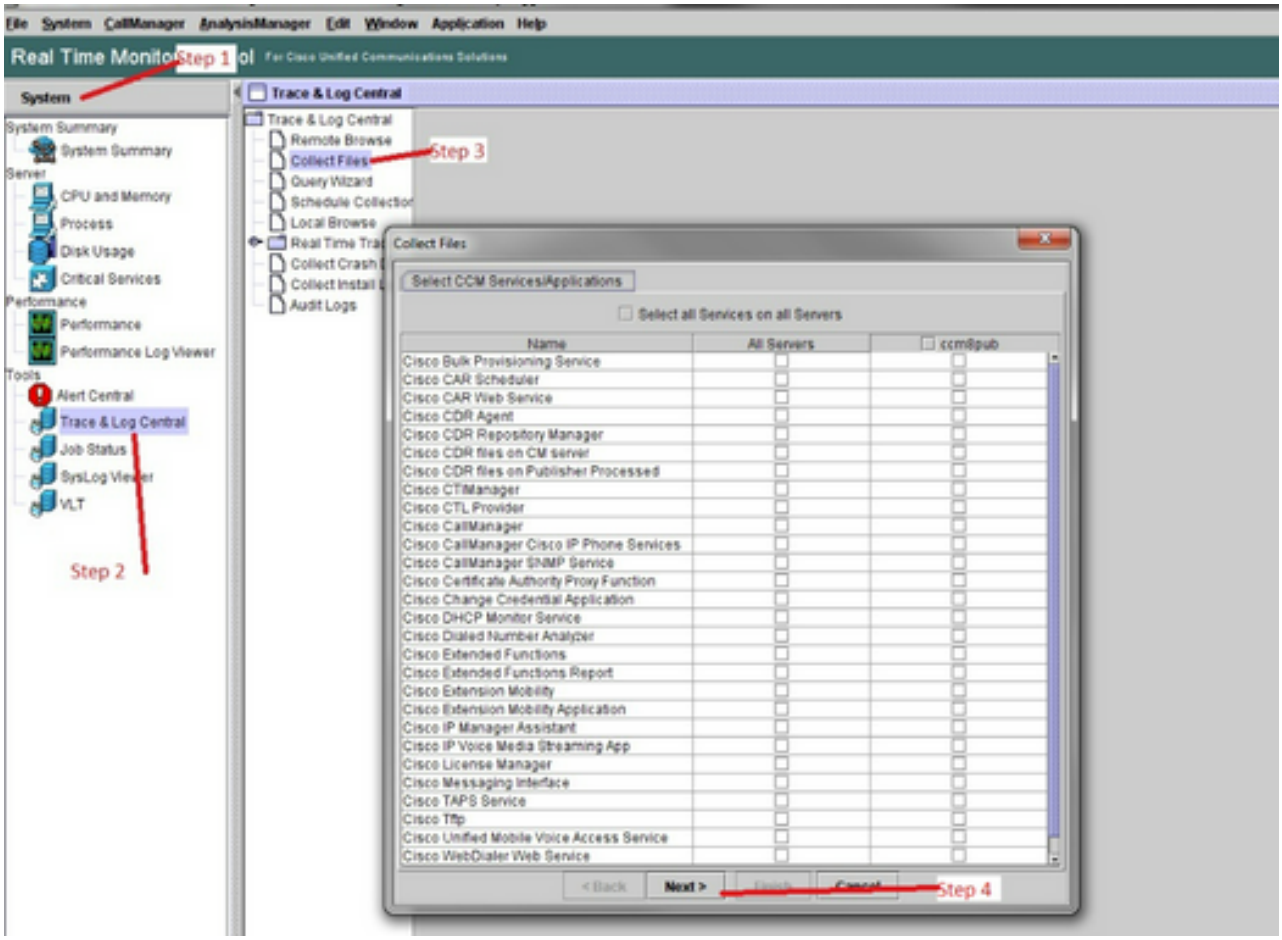
Sobald dies abgeschlossen ist, wird eine Erfassungsdatei auf dem Server im Verzeichnis 'activelog platform/cli/' gespeichert.

6. Erfassung vom Server erfassen
   Die Erfassungsdateien werden im Verzeichnis "activelog platform/cli/" auf dem Server gespeichert. Sie können die Dateien über CLI auf einen SFTP-Server oder mit dem RTMT auf den lokalen PC übertragen. 4a) Übertragen der Erfassungsdatei über die CLI an einen SFTP-Server
   Verwenden Sie den Befehl **file get activelog platform/cli/packets.cap** , um die Datei packages.cap auf dem SFTP-Server zu sammeln.
   Alternativ können Sie alle auf dem Server gespeicherten .cap-Dateien sammeln: 'file get activelog platform/cli/*.cap'
   Geben Sie abschließend die IP/FQDN des SFTP-Servers, den Port, den Benutzernamen, das Kennwort und die Verzeichnisinformationen ein:

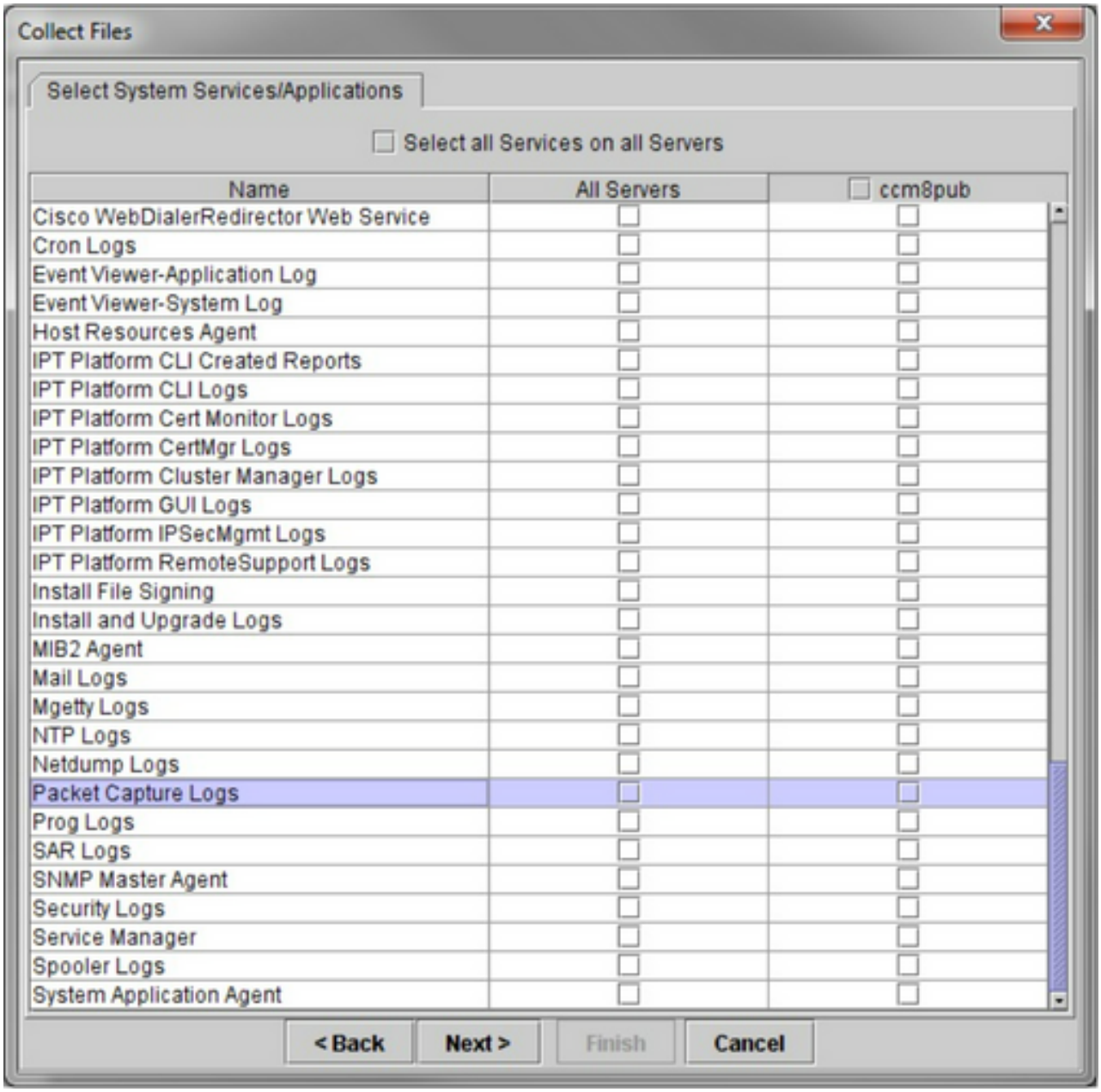


Die CLI zeigt an, dass die Dateiübertragung zum SFTP-Server erfolgreich war oder fehlgeschlagen ist.

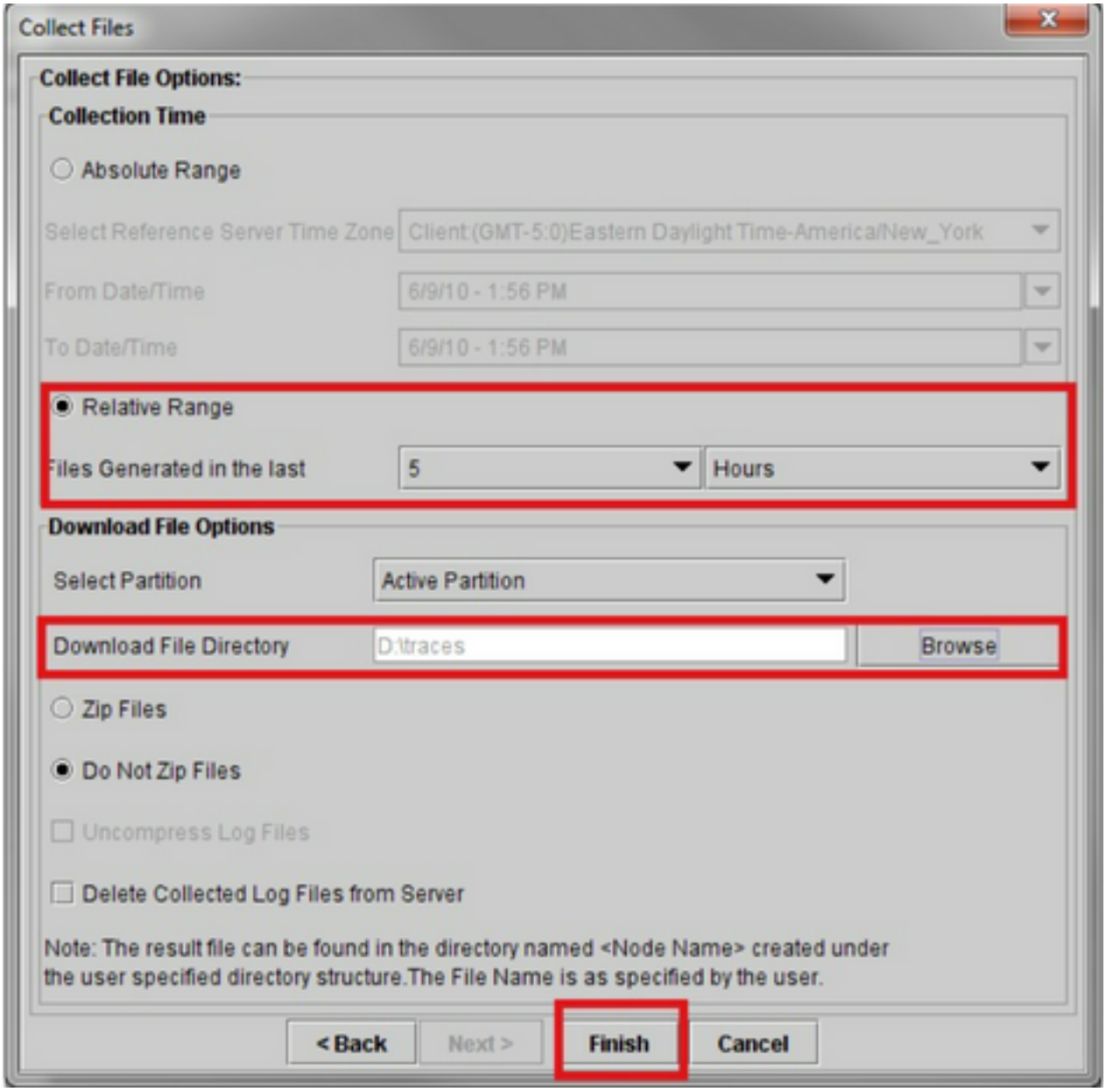
4b) Verwenden Sie RTMT, um eine Erfassungsdatei auf einen lokalen PC zu übertragen. Starten Sie das RTMT. Wenn es nicht auf dem lokalen PC installiert ist, installieren Sie die entsprechende Version von der VOS-Administration-Seite und gehen Sie zum Menü **Applications->Plugins**.
Klicken Sie auf **System**, **Trace & Log Central**, und doppelklicken Sie dann auf **Dateien sammeln.** Klicken Sie im ersten Menü auf **Weiter**.



Aktivieren Sie im zweiten Menü das Kontrollkästchen **Paketerfassungsprotokolle** auf dem Server, auf dem die Erfassung durchgeführt wurde, und klicken Sie dann auf **Weiter**.



Wählen Sie auf dem letzten Bildschirm einen Zeitbereich für die Erfassung und ein Downloadverzeichnis auf dem lokalen PC aus.



RTMT schließt dieses Fenster und fährt fort, die Datei zu sammeln und sie auf dem lokalen PC am angegebenen Speicherort zu speichern.

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.