Konfigurieren von Ablaufverfolgungen und Sammeln von UCCE-Protokollen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Ablaufverfolgungen für Cisco UCCE, Finesse, Customer Voice Portal (CVP), UCCE Outbound Dialer und Cisco Gateways einrichten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Unified Contact Center Enterprise (UCCE)
- Package Contact Center Enterprise (PCCE)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco Virtualized Voice Browser (CVVB)
- Cisco Unified Border Element (CUBE)
- Cisco Unified Session Initiation Protocol (SIP) Proxy (CUSP)

Verwendete Komponenten

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

- Cisco Finesse 11,5
- CVP-Server 11.5
- Unified Contact Center Enterprise (UCCE) 11,5

- Cisco Virtualized Voice Browser 11.5

In diesem Dokument wird beschrieben, wie Sie Ablaufverfolgungen für Cisco Unified Contact Center Enterprise (UCCE), Cisco Finesse, Cisco Customer Voice Portal (CVP), Cisco UCCE Outbound Dialer und Cisco Gateways einrichten.

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.

Ablaufverfolgungseinstellungen und Finesse für die Protokollsammlung

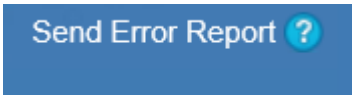
Finesse-Client

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

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

Schritt 1: Melden Sie einen Agenten an.

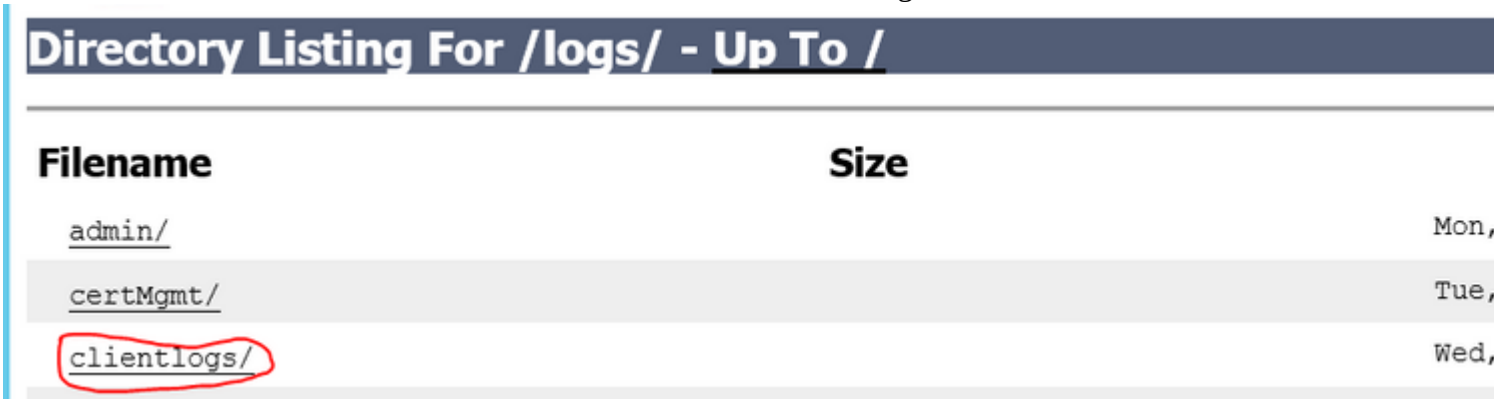
Schritt 2: Wenn ein Mitarbeiter während eines Anrufs oder einer Medienveranstaltung ein Problem feststellt, weisen Sie ihn an, auf den Link Send Error Report (Fehlerbericht senden) unten rechts auf dem Finesse-Desktop zu klicken.



Schritt 3: Der Agent sieht die Nachricht "Protokolle erfolgreich gesendet!".

Schritt 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.

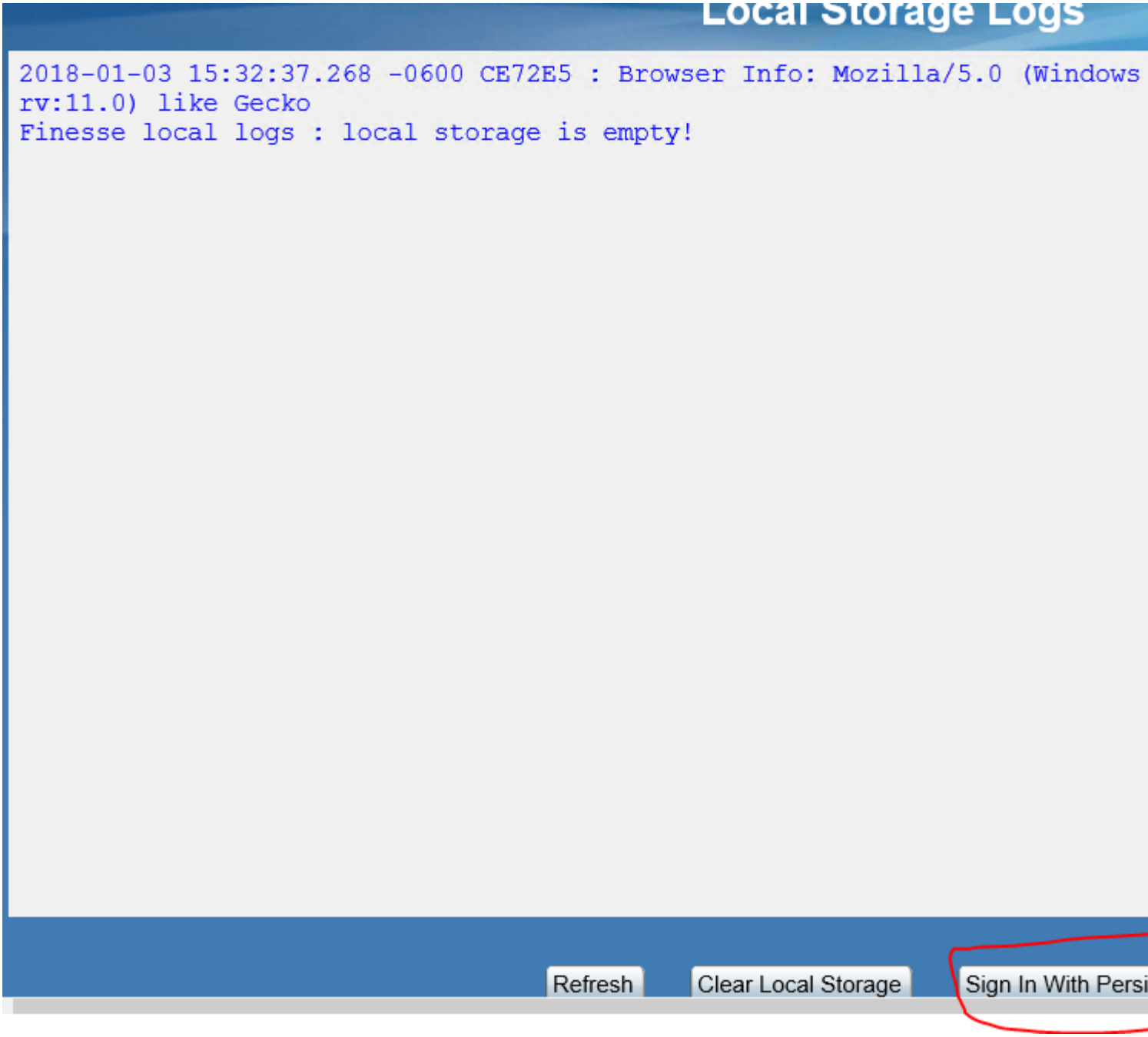
Schritt 5: Sammeln Sie die Protokolle unter dem Verzeichnis clientlogs/.



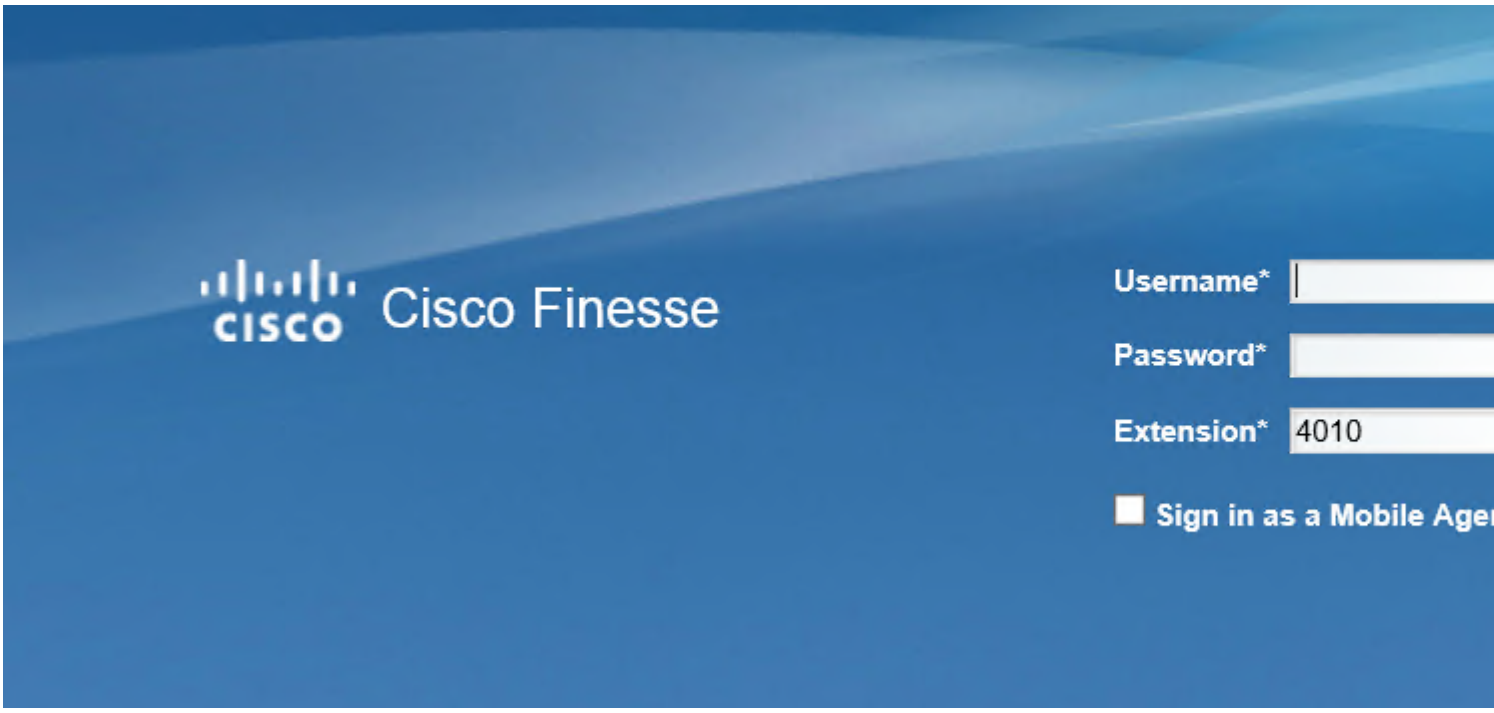
Option 2: Festlegen der permanenten Protokollierung

Schritt 1: Navigieren Sie zu https://x.x.x.x:8445/desktop/locallog.

Schritt 2: Klicken Sie auf Mit permanenter Protokollierung anmelden.



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



Schritt 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. Speichern Sie die Datei zur weiteren Analyse.

.

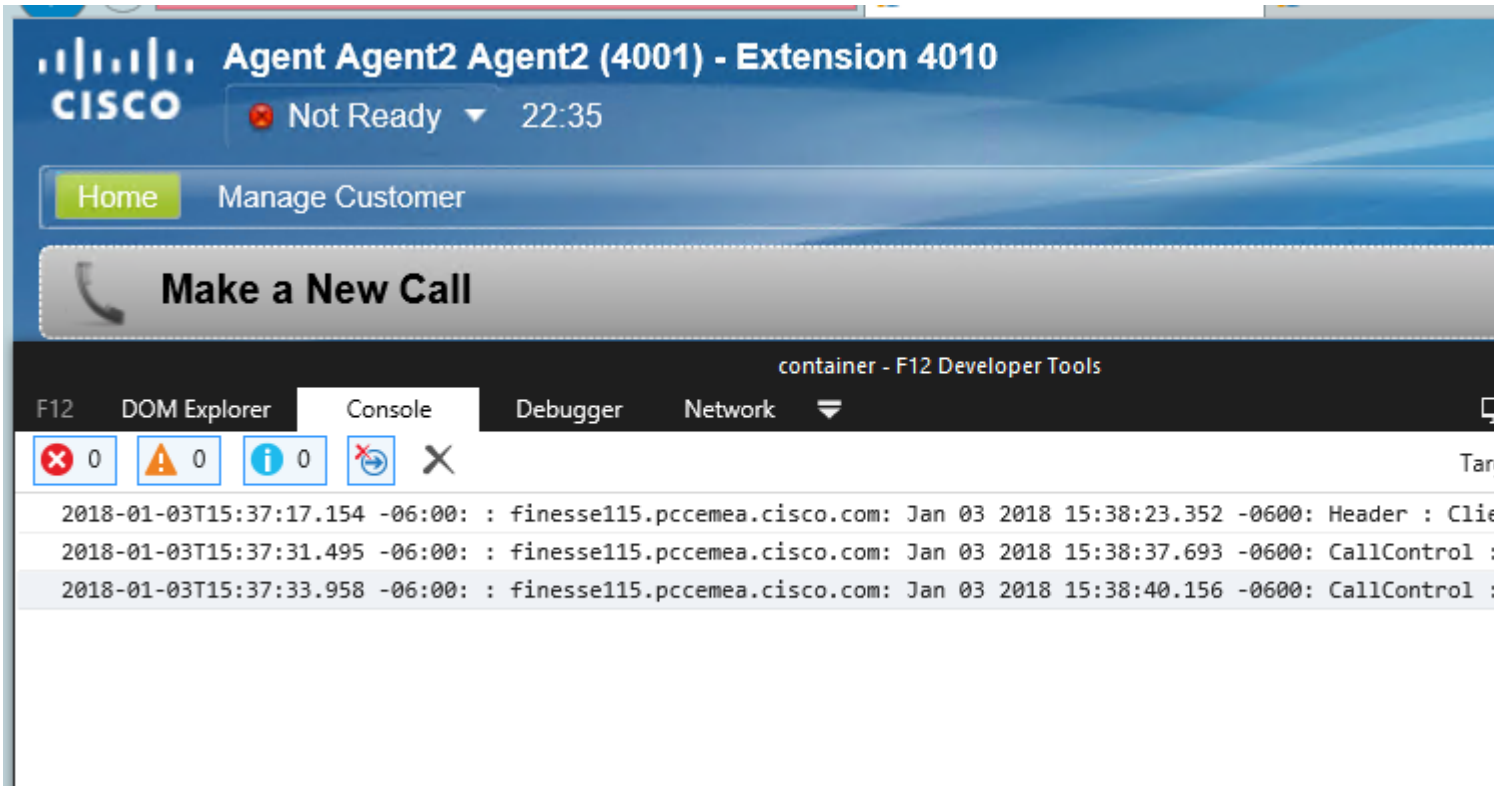
Hinweis: Es gibt einen Vorbehalt bezüglich der permanenten Protokollierung. Nachdem die persistente Protokollierung aktiviert wurde, werden die Informationen nicht mehr an die lokalen Speicherprotokolle gesendet. Cisco Bug-ID CSCvf93030 - Bei der permanenten Protokollierung können keine Protokolle erfasst werden. Finesse 11.5(1) ES-2 weiter Weitere Informationen zu diesem Vorbehalt und den erforderlichen Schritten zur Behebung finden Sie unter

Option 3: Webbrowser-Konsole

Schritt 1: Wenn sich ein Agent angemeldet hat, drücken Sie F12, um die Browserkonsole zu öffnen.

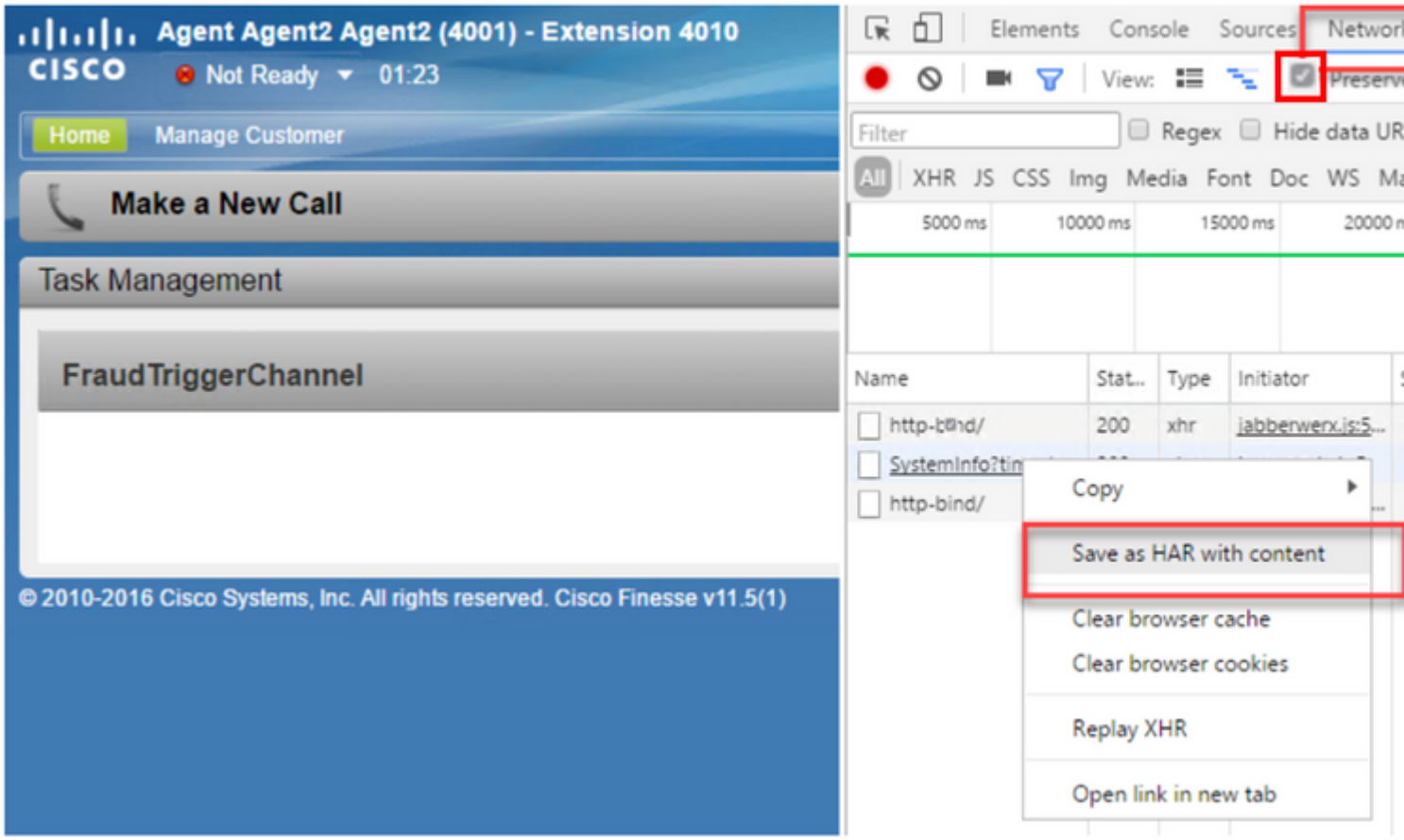
Schritt 2: Wählen Sie die Registerkarte Konsole aus.

Schritt 3:Überprüfen Sie die Browserkonsole auf Fehler. Kopieren Sie den Inhalt in eine Textdatei, und speichern Sie diese.



Schritt 4: Wählen Sie die Registerkarte Netzwerk aus, und aktivieren Sie die Option Protokoll beibehalten.

Schritt 5: Klicken Sie mit der rechten Maustaste auf ein Netzwerknamensereignis, und wählen Sie Save as HAR with content (Als HAR mit Inhalt speichern) aus.



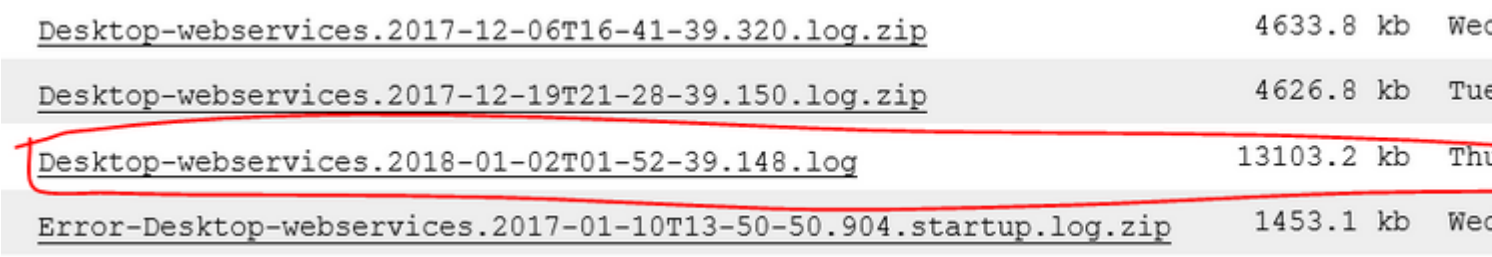
Finesse-Server

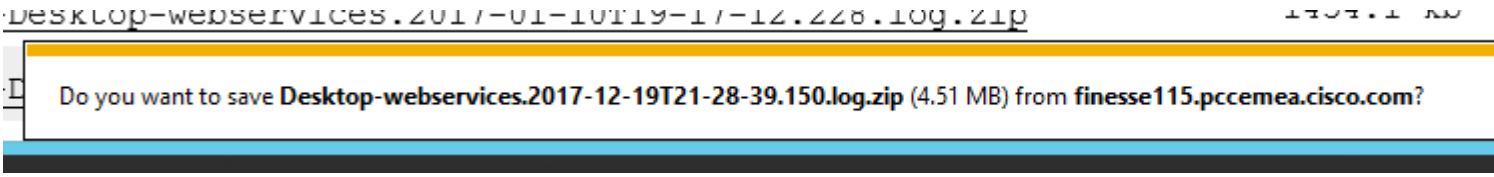
Option 1: Über die Benutzeroberfläche - Web-Services (erforderlich) und zusätzliche Protokolle

Schritt 1: Navigieren Sie zu https://x.x.x.x/finesse/logs, und melden Sie sich mit dem Administratorkonto an.

Schritt 2: Erweitern Sie das Verzeichnis webservices/

Schritt 3: Erfassen der letzten Webdienstprotokolle Wählen Sie die letzte Unzip-Datei aus. Beispiel: Desktop-Webservices.201X-..log.zip Klicken Sie auf den Datei-Link, und es wird die Option zum Speichern der Datei angezeigt.





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

Hinweis: Die empfohlene Methode zum Erfassen der Cisco Finesse-Serverprotokolle erfolgt über Secure Shell (SSH) und Secure File Transfer Protocol (SFTP). Diese Methode erlaubt es Ihnen nicht nur, die Webservice-Protokolle zu sammeln, sondern auch alle zusätzlichen Protokolle wie, Fippa, openfire, Realm und Clientlogs.

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

Schritt 1: Melden Sie sich mit der Secure Shell (SSH) beim Finesse-Server an.

Schritt 2: Geben Sie diesen Befehl ein, um die benötigten Protokolle zu sammeln. Die Protokolle werden komprimiert und haben eine relative Zeit von 2 Stunden. Sie werden aufgefordert, den SFTP-Server zu identifizieren, auf den die Protokolle hochgeladen werden.

Datei erhalten activelog desktop recurs komprimieren reltime Stunden 2.

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

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

Schritt 4: Weitere Protokolle wie Tomcat, Context Service, Server und Installationsprotokolle finden Sie im Abschnitt Log Collection im Cisco Finesse Administration Guide.

Cisco Finesse Administrationsleitfaden, Version 11.5(1)

Hinweis: Weitere Informationen zu SFTP für Finesse-Übertragungsdateien finden Sie in diesem Dokument: Finesse Backup and Upgrade Configuration with SFTP

Ablaufverfolgungseinstellungen und Protokollerfassung CVP und CVVB

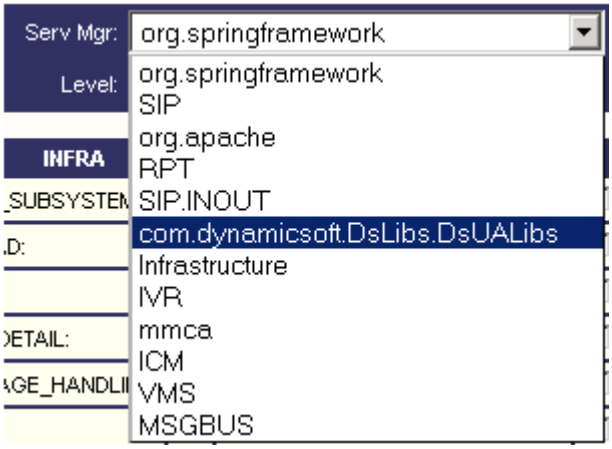
CVP-Anrufserver

Die Standardstufe der Ablaufverfolgungen des CVP CallServer reicht aus, um die meisten Probleme zu beheben. Wenn Sie jedoch weitere Informationen zu den SIP-Nachrichten (Session Initiation Protocol) benötigen, müssen Sie die SIP-Strack-Traces auf die DEBUG-Ebene festlegen.

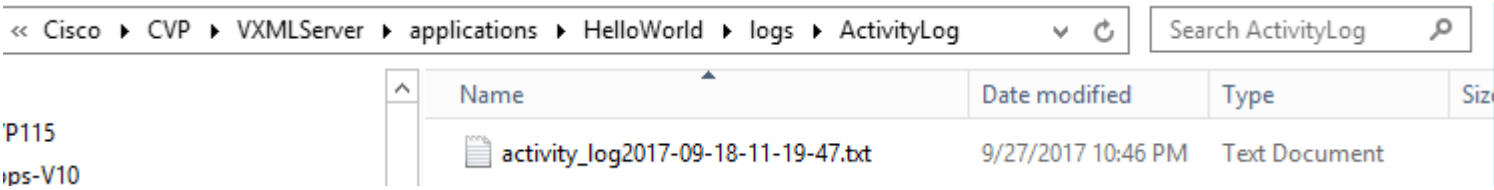
Schritt 1: Rufen Sie die CVP CallServer Diag-Webseite unter http://cvp.cc.lab:8000/cvp/diag auf.

Hinweis: Diese Seite enthält gute Informationen über den CVP-Anrufserver. Sie ist sehr nützlich, um in bestimmten Szenarien eine Fehlerbehebung durchzuführen.

Schritt 2: Wählen Sie com.dynamicsoft.DsLibs.DsUALibs vom Serv aus. Dropdown-Menü "Mgr" oben links



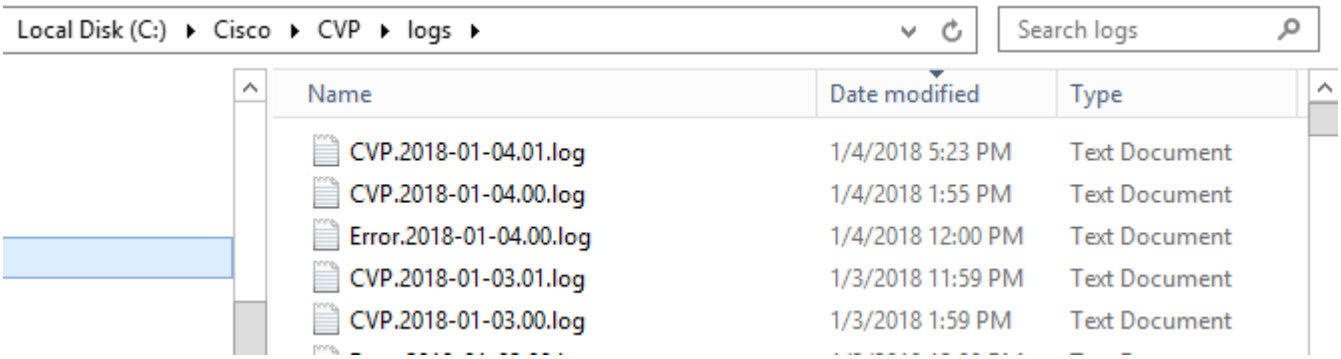
Schritt 3: Klicken Sie auf die Schaltfläche Festlegen.



Schritt 4: Blättern Sie im Trace-Fenster nach unten, um sicherzustellen, dass die Ebene der Traces korrekt festgelegt wurde. Dies sind Ihre Debug-Einstellungen.

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

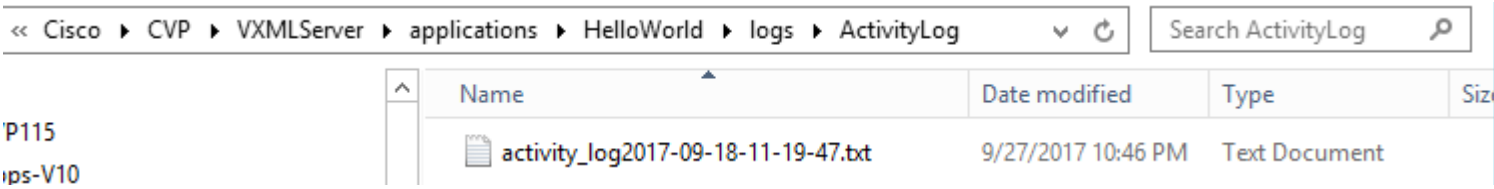
Schritt 5: Wenn Sie das Problem reproduzieren, sammeln Sie die Protokolle von C:\Cisco\CVP\logs, und wählen Sie die CVP-Protokolldatei nach dem Zeitpunkt des Problems aus.



CVP Voice XML (VXML)-Anwendung

In sehr seltenen Fällen müssen Sie die Traces der VXML-Serveranwendungen erhöhen. Es wird jedoch nicht empfohlen, den Wert zu erhöhen, es sei denn, ein Cisco Techniker hat darum gebeten.

Um die VXML-Server-Anwendungsprotokolle zu sammeln, navigieren Sie zum jeweiligen Anwendungsverzeichnis unter dem VXML-Server, z. B.: C:\Cisco\CVP\VXMLServer\applications\{name of application}\logs\ActivityLog\, und erfassen 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:

Schritt 1: Sichern Sie %CVP_HOME%\conf\oamp.properties .

Schritt 2: %CVP_HOME%\conf\oamp.properties bearbeiten

omgr.traceMask=-1

omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERROR
net.sf.ehcache.logLevel=ERROR

Schritt 3: Starten Sie OPSConsoleServer neu.

Informationen auf Ablaufverfolgungsebene

Ablaufverfolgungsebene	Beschreibung	Protokollstufe	Ablaufverfolgungsmaske
0	Standard für die Produktinstallation. Keine/minimale Beeinträchtigung der Leistung	INFORMATIONEN	None
1	Weniger detaillierte Ablaufverfolgungsmeldungen mit geringen Auswirkungen auf die Leistung.	DEBUG	GERÄTEKONFIGURATION + DATENBANK_ÄNDERN + MANAGEMENT=0x01011000

Ablaufverfolgungsebene	Beschreibung	Protokollstufe	Ablaufverfolgungsmaske
2	Detaillierte Ablaufverfolgungsmeldungen mit mittleren Auswirkungen auf die Leistung.	DEBUG	GERÄTEKONFIGURATION + SYSLVL_CONFIGURATION + DATENBANK_ÄNDERN + MANAGEMENT=0x05011000
3	Detaillierte Ablaufverfolgungsmeldungen mit Auswirkungen auf die Leistung.	DEBUG	GERÄTEKONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + DATENBANK_ÄNDERN + MANAGEMENT=0x05111000
4	Detaillierte Ablaufverfolgungsmeldungen mit sehr starken Auswirkungen auf die Leistung.	DEBUG	MISC + GERÄTEKONFIGURATION + ST_KONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACKTRAC + DATENBANK_ÄNDERN + DATENBANK_AUSWAHL + DATENBANK_PO_INFO + MANAGEMENT + TRACE_METHODE + TRACE_PARAM=0x17371000
5	Höchste detaillierte Ablaufverfolgungsmeldung.	DEBUG	MISC + GERÄTEKONFIGURATION + ST_KONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACKTRAC + DATENBANK_ÄNDERN + DATENBANK_AUSWAHL + DATENBANK_PO_INFO + MANAGEMENT + TRACE_METHODE + TRACE_PARAM=0x17371006

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:

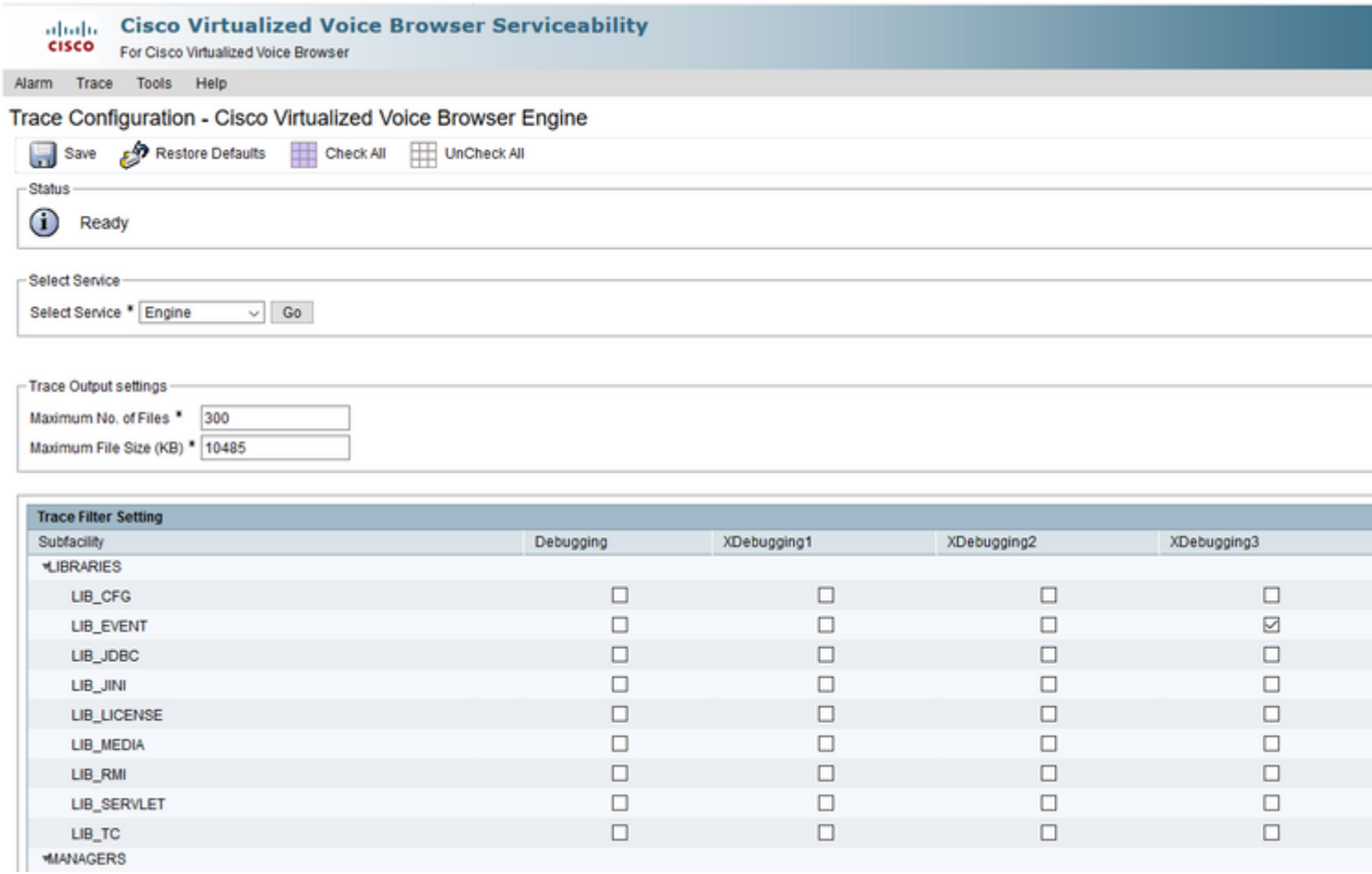
- Cisco VB "Administration"-Traces, auch MADM-Protokolle genannt
- Als MIVR-Protokolle bezeichnete Cisco VB "Engine"-Traces

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 - Detailliertes Level mit Stack Trace



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

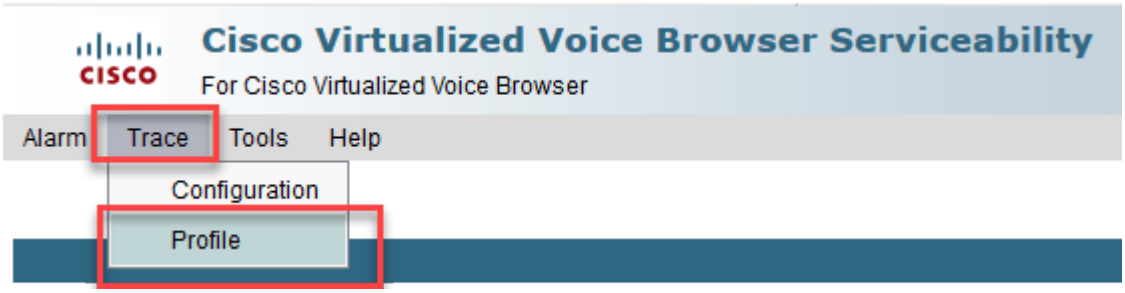
Die gängigsten Protokolle, die Sie sammeln müssen, sind die Engine. Die Standardstufe der Ablaufverfolgungen für die CVVB-Engine-Ablaufverfolgungen reicht aus, um die meisten Probleme zu beheben. Wenn Sie jedoch die Ablaufverfolgungsebene für ein bestimmtes Szenario ändern müssen, empfiehlt Cisco die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

Systemprotokollprofile	
Name	Szenario, in dem dieses Profil aktiviert werden muss
StandardVVB	Generische Protokolle sind aktiviert.

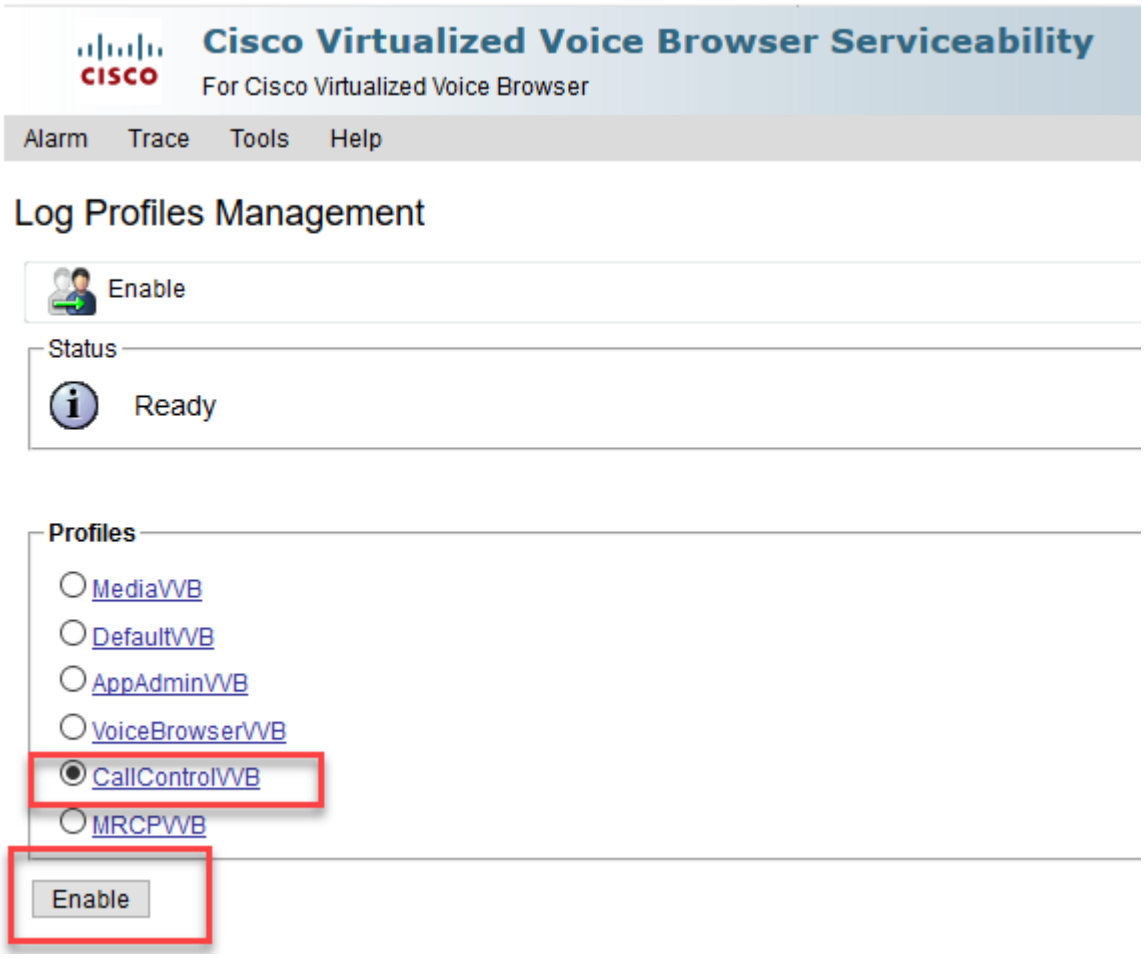
Anwendungs-AdminVB	Bei Problemen mit der Web-Administration über AppAdmin, Cisco VVB Serviceability und andere Webseiten.
MedienVVB	Bei Problemen mit der Medieneinrichtung oder -übertragung.
SprachbrowserVB	Bei Problemen mit der Anrufbearbeitung.
MRCPVB	Bei Problemen mit ASR/TTS und Cisco VVB.
AnrufsteuerungVVB	Bei Problemen mit der SIP-Signalisierung werden diese im Protokoll veröffentlicht.

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

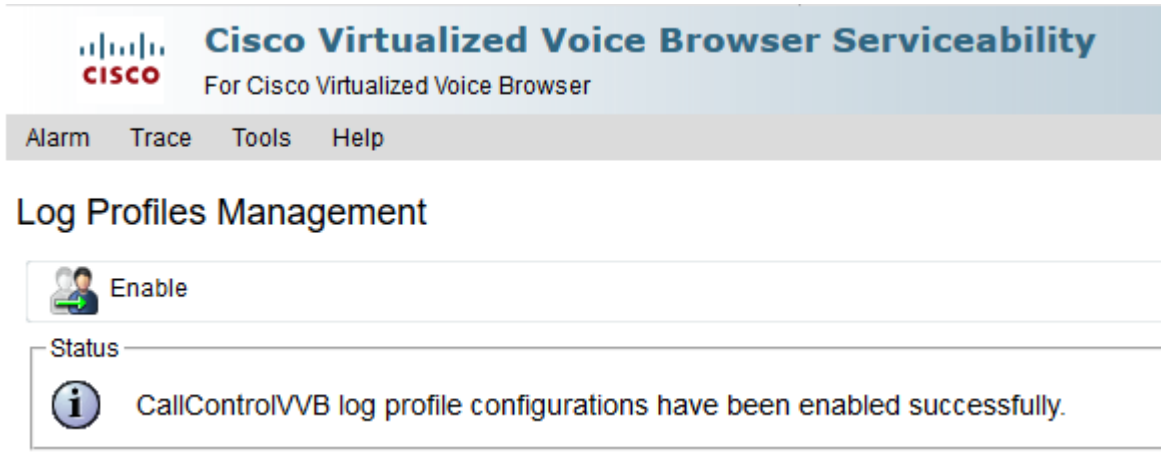
Schritt 2: Trace auswählen -> Profil



Schritt 3: Aktivieren Sie das Profil, das Sie für das jeweilige Szenario aktivieren möchten, und klicken Sie auf die Schaltfläche Enable (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).



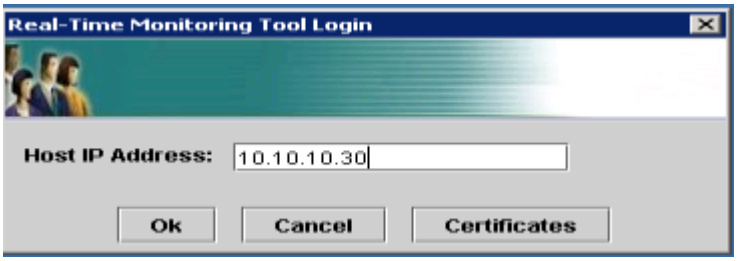
Nach dem Klicken auf die Schaltfläche "Aktivieren" wird die Meldung angezeigt.



Schritt 4: Nachdem das Problem erneut aufgetreten ist, sammeln Sie die Protokolle. Verwenden Sie das Real Time Monotor Tool (RTMT), das im Lieferumfang des CVVB enthalten ist, um die Protokolle zu erfassen.

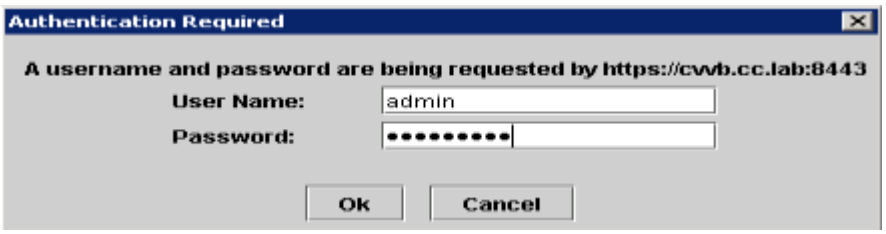
Schritt 5: Klicken Sie auf dem Desktop auf das Symbol für das Cisco Unified Real-Time Monitoring Tool (falls Sie dieses Tool bereits vom CVVB heruntergeladen haben).

Schritt 6: Geben Sie die IP-Adresse der VVB an, und klicken Sie auf OK.



Schritt 7. Akzeptieren Sie die Zertifikatinformationen, wenn diese angezeigt werden.

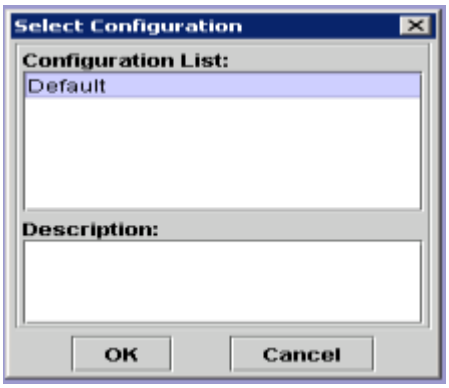
Schritt 8: Geben Sie die Anmeldeinformationen an, und klicken Sie auf OK.



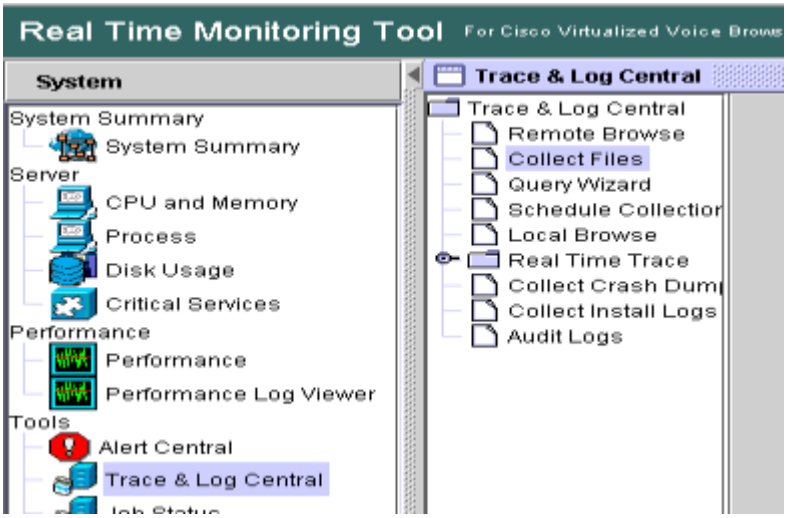
Schritt 9. Wenn Sie eine Warnung vor Zeitzonenkonflikten erhalten, klicken Sie auf JA, und fahren Sie fort.

Schritt 10. Wenn Sie den TimeZone-Fehler erhalten haben, wird RTMT möglicherweise geschlossen, nachdem Sie auf die Schaltfläche Yes (Ja) geklickt haben. Starten Sie das RTMT-Tool erneut.

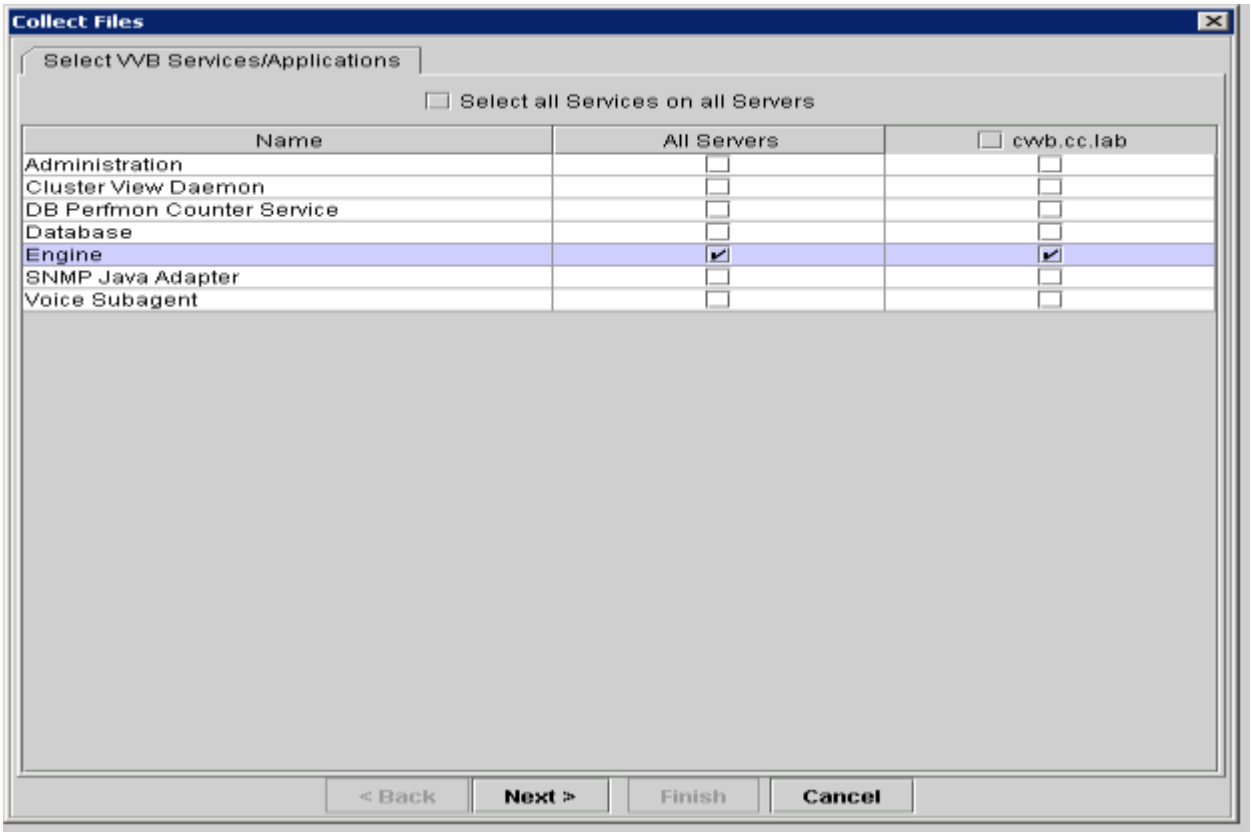
Schritt 11. Lassen Sie die Standardkonfiguration ausgewählt, und klicken Sie auf OK.



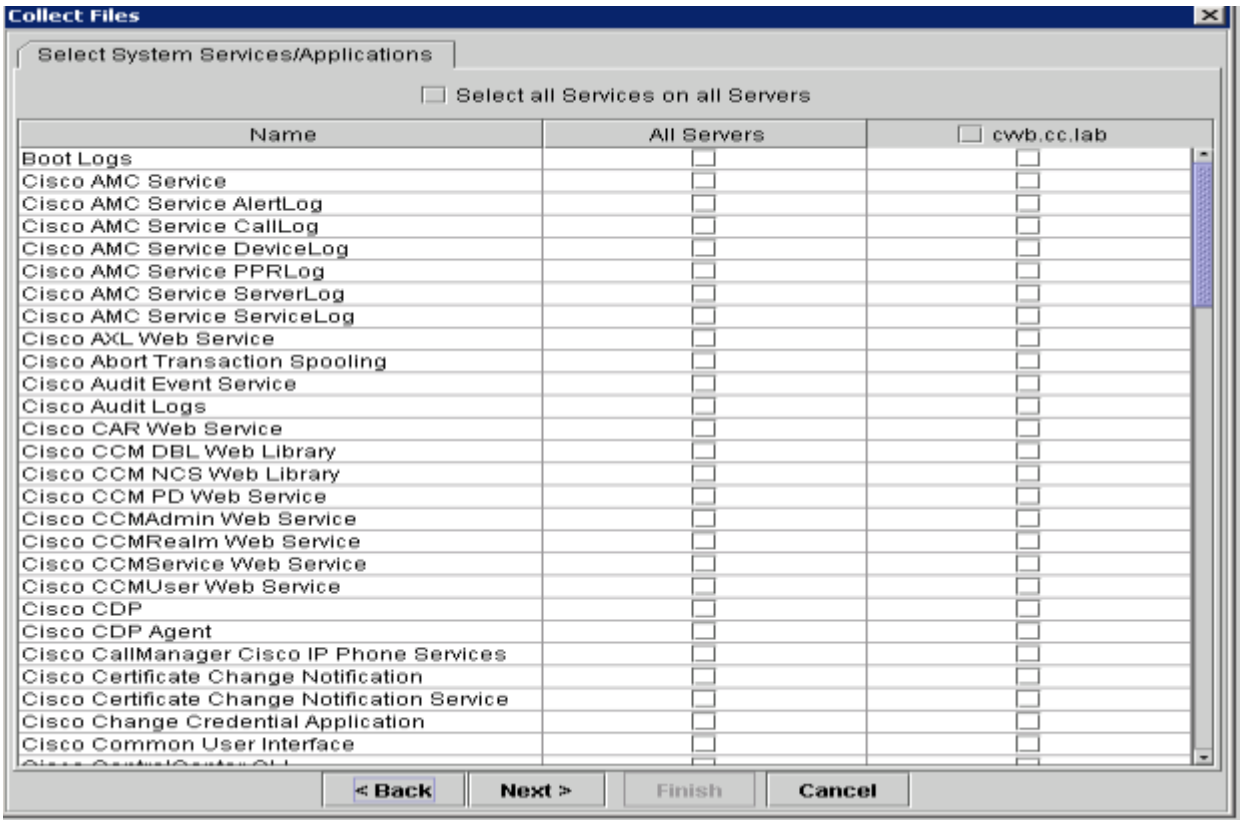
Schritt 12: Wählen Sie Trace & Log Central aus, und doppelklicken Sie dann auf Collect Files



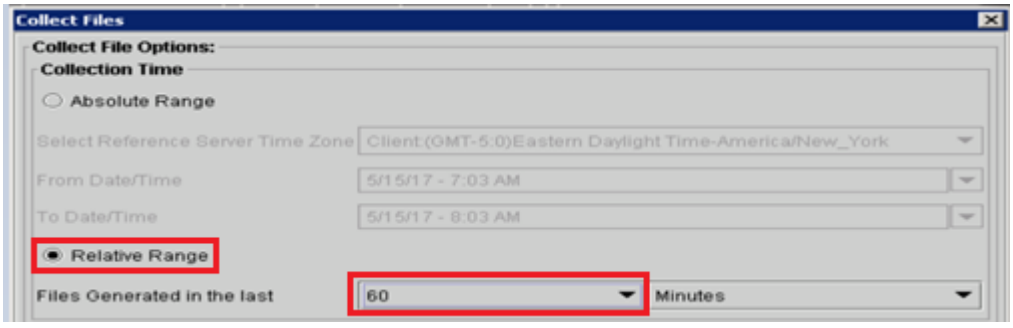
Schritt 13: Wählen Sie im neu geöffneten Fenster Engine aus, und klicken Sie auf Next (Weiter).



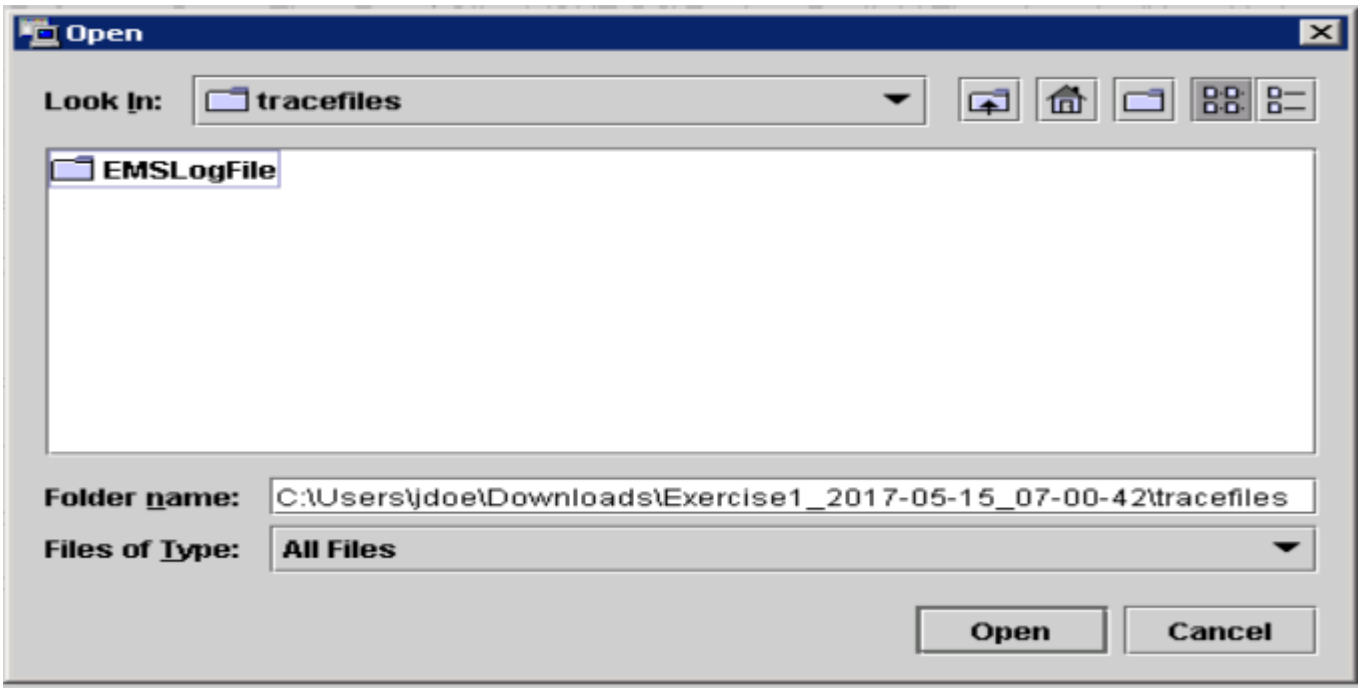
Schritt 14: Klicken Sie im nächsten Fenster erneut auf Weiter



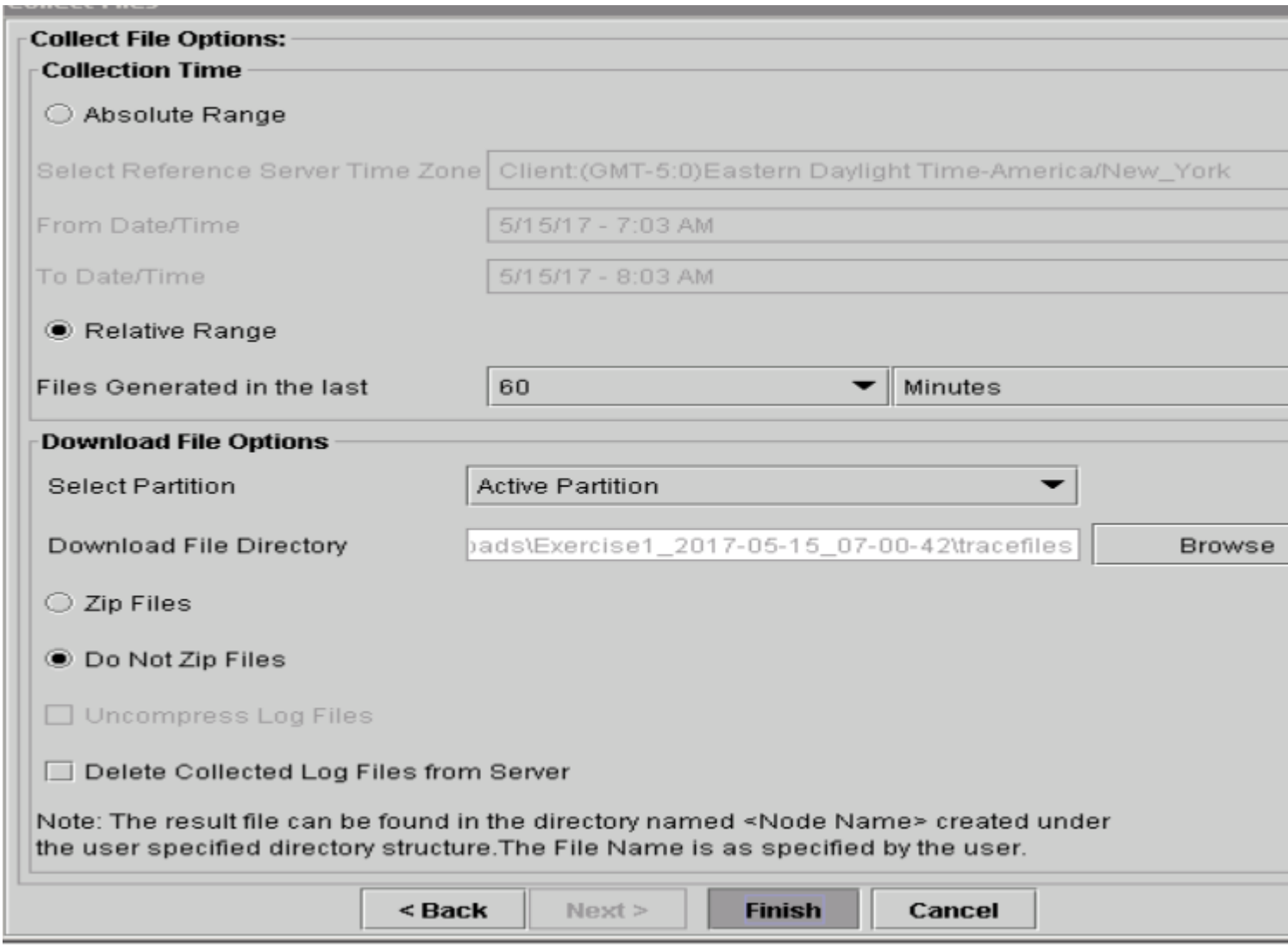
Schritt 15: Wählen Sie Relative Range (Relative Reichweite) aus, und vergewissern Sie sich, dass Sie die Zeit für einen falschen Anruf auswählen.



Schritt 16: Klicken Sie unter Download-Dateioptionen auf Durchsuchen, wählen Sie das Verzeichnis aus, in dem die Datei gespeichert werden soll, und klicken Sie auf Öffnen.

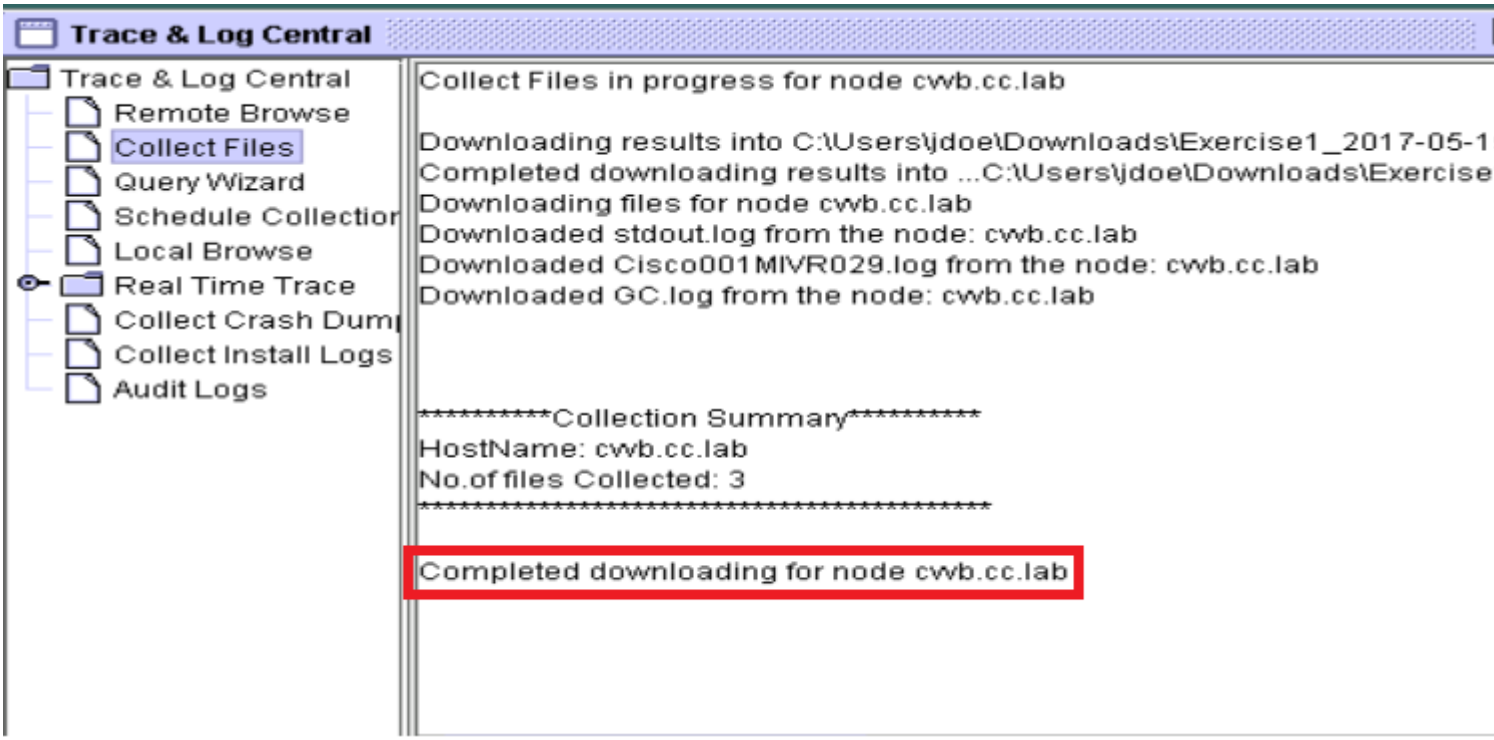


Schritt 14: Wenn alles ausgewählt ist, klicken Sie auf die Schaltfläche Fertig stellen.



Schritt 15: Dadurch werden die Protokolldateien gesammelt. Warten Sie, bis die Bestätigungsmeldung auf

RTMT angezeigt wird.



Schritt 16: Navigieren Sie zu dem Ordner, in dem die Ablaufverfolgungen gespeichert sind.

Schritt 17: Die Engine-Protokolle sind alle erforderlich. Um sie zu finden, navigieren Sie zum Ordner \<Zeitstempel>\uccx\log\MIVR.

Trace-Einstellungen und Protokollsammlung für CUBE und CUSP

CUBE (SIP)

Schritt 1: Zeitstempel der Protokolle festlegen und Protokollierungspuffer aktivieren

```
#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: Jede Änderung an einem produktiven Cisco IOS® Software-GW kann zu einem Ausfall führen.

Dies ist eine sehr robuste Plattform, die die vorgeschlagenen Debug-Vorgänge im bereitgestellten Anrufvolumen problemlos verarbeiten kann. Cisco empfiehlt jedoch Folgendes:

- Senden Sie alle Protokolle an einen Syslog-Server anstatt an den Protokollierungspuffer:

```
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: Wenn die CPU bis zu 70-80 % CPU-Auslastung erhält, erhöht sich das Risiko von leistungsbezogenen Servicebeeinträchtigungen erheblich. Aktivieren Sie daher keine zusätzlichen Debugs, wenn das GW 60 % erreicht.

Schritt 2: Aktivieren Sie diese Debug-Optionen:

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

Schritt 3: Reproduzieren des Problems
Schritt 4: Deaktivieren Sie die Spuren.

```
#undebug all
```

Schritt 5: Sammeln Sie die Protokolle.

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

CUSP

Schritt 1: Aktivieren Sie SIP-Ablaufverfolgungen für CUSP.

```
(cusp)> config
(cusp-config)> sip logging
(cusp)> trace enable
(cusp)> trace level debug component sip-wire
```

Schritt 2: Reproduzieren des Problems

Schritt 3: Deaktivieren Sie die Protokollierung, sobald Sie fertig sind.

Sammeln Sie die Protokolle.

Schritt 1: Konfigurieren Sie einen Benutzer auf dem CUSP (z. B. Test).

Schritt 2: Fügen Sie diese Konfiguration an der CUSP-Eingabeaufforderung hinzu.

```
username <userid> create
username <userid> password <password>
username <userid> group pfs-privusers
```

Schritt 3: FTP an die CUSP-IP-Adresse Verwenden Sie den Benutzernamen (Test) und das Kennwort wie im vorherigen Schritt definiert.

Schritt 4: Ändern Sie die Verzeichnisse in /cusp/log/trace.

Schritt 5: Rufen Sie log_<Dateiname> ab.

Ablaufverfolgungseinstellungen und Protokollerfassung - UCCE

Cisco empfiehlt, Ablaufverfolgungsebenen festzulegen und Ablaufverfolgungen mit den Diagnose-Framework-Portico- oder System-CLI-Tools zu erfassen.

Hinweis: Weitere Informationen zum Diagnose-Framework-Portfolio und zur System-CLI finden Sie im Kapitel Diagnosetools im Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 11.5(1).

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

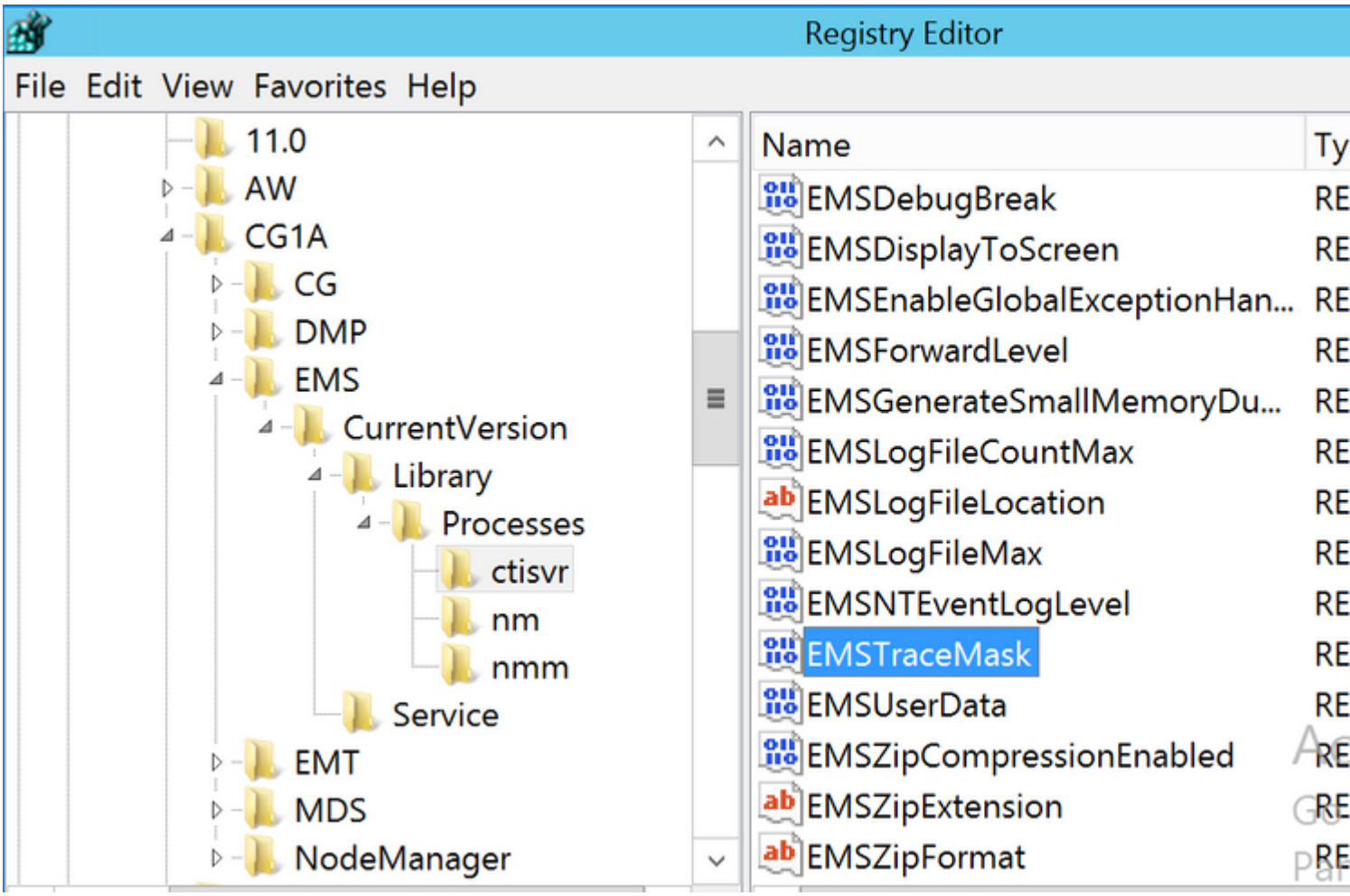
Hinweis: Weitere Informationen finden Sie im Abschnitt Ablaufverfolgungsebene im Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 11.5(1).

Wenn Sie beispielsweise Probleme mit der Wählhilfe für ausgehende Anrufe beheben, legen Sie die Ebene der Ablaufverfolgungen auf Ebene 2 fest, wenn die Wählhilfe beschäftigt ist.

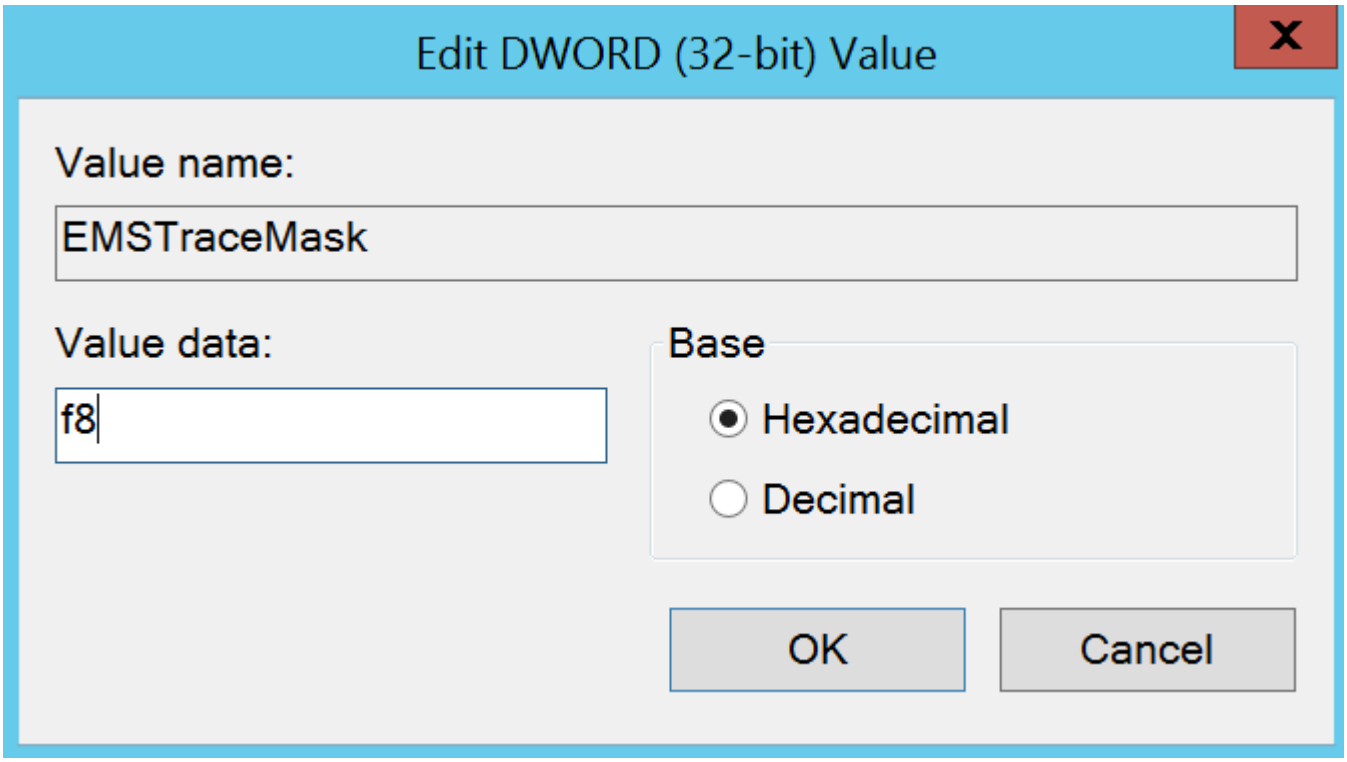
Für CTISVR (CTISVR) wird in Stufe 2 und Stufe 3 nicht die von Cisco empfohlene Registrierungsebene festgelegt. Die empfohlene Ablaufverfolgungsregistrierung für CTISVR ist 0XF8.

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

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



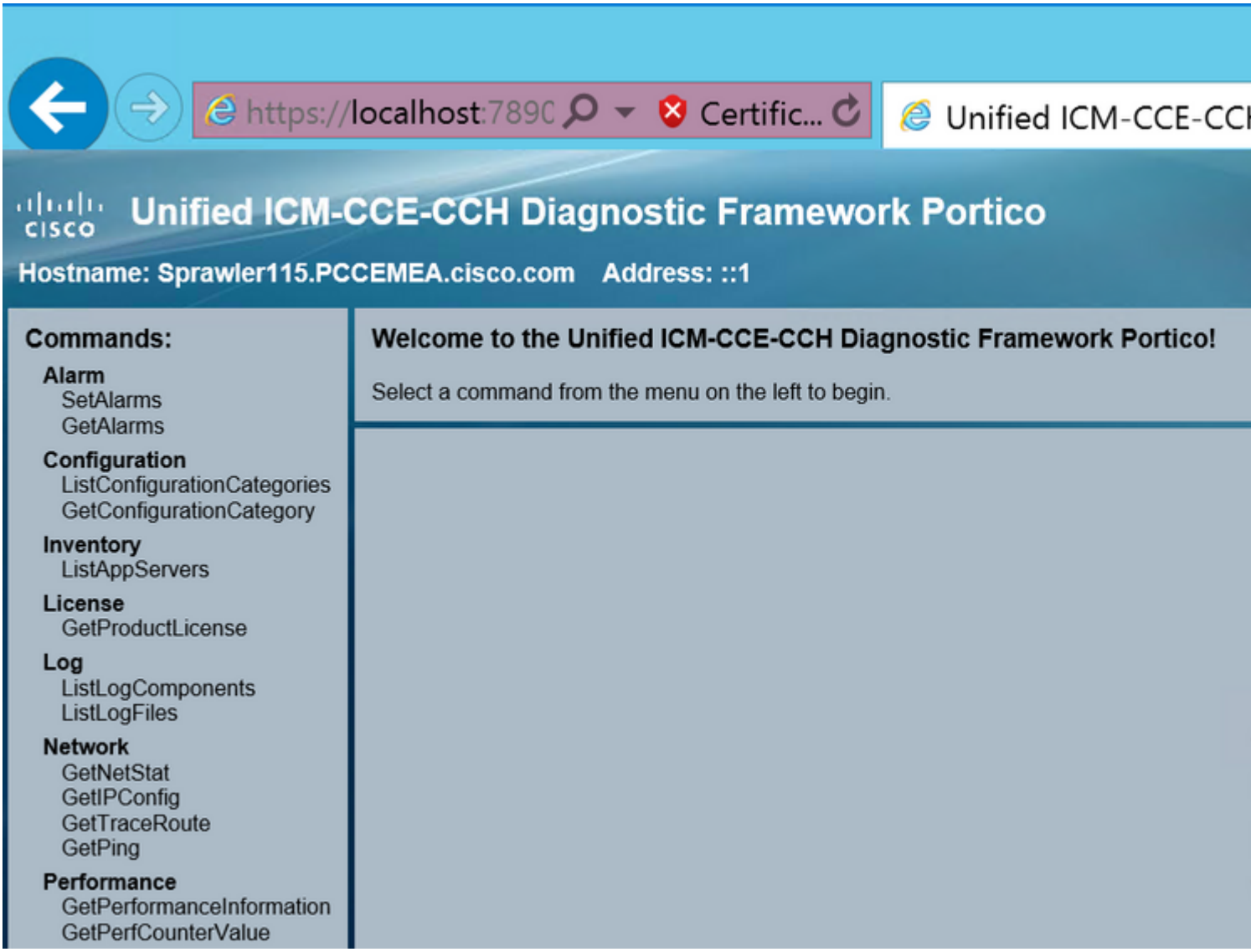
Schritt 3.Doppelklicken Sie auf EMSTraceMask, und legen Sie den Wert auf f8 fest.



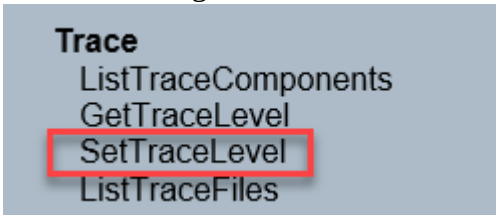
Schritt 4: Klicken Sie auf OK, und schließen Sie den Registrierungs-Editor.

Dies sind die Schritte zum Festlegen von UCCE-Komponentenspuren (als Beispiel wird der RTR-Prozess

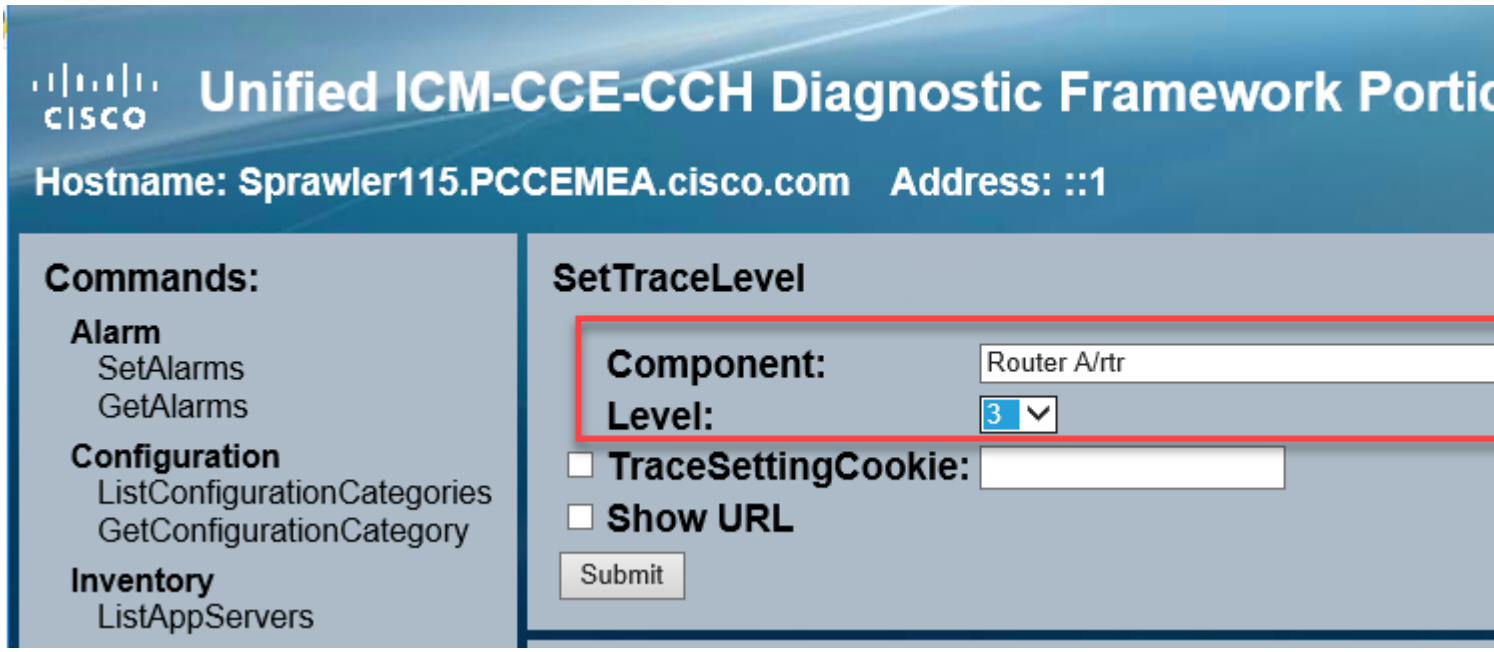
verwendet).
Schritt 1: Öffnen Sie das Diagnose-Framework-Portfolio auf dem Server, auf dem Sie die Traces einrichten müssen. Melden Sie sich mit dem Administrator-Benutzer an.



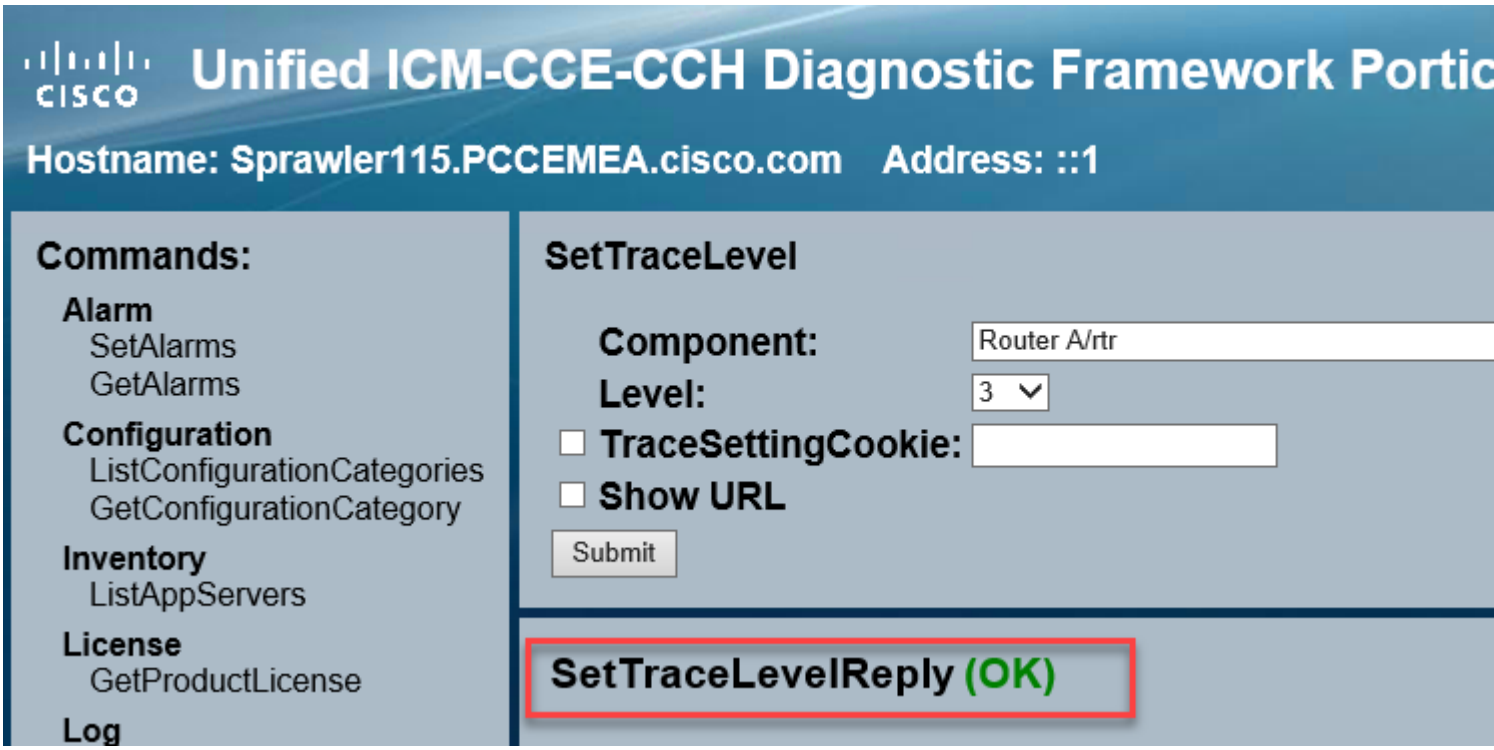
Schritt 2: Navigieren Sie im Abschnitt Befehle zu Ablaufverfolgung, und wählen Sie SetTraceLevel aus.



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

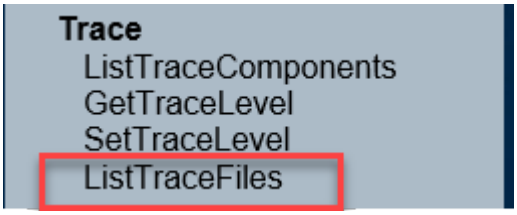


Schritt 4: Klicken Sie auf Senden. Wenn Sie fertig sind, wird die Meldung OK angezeigt.

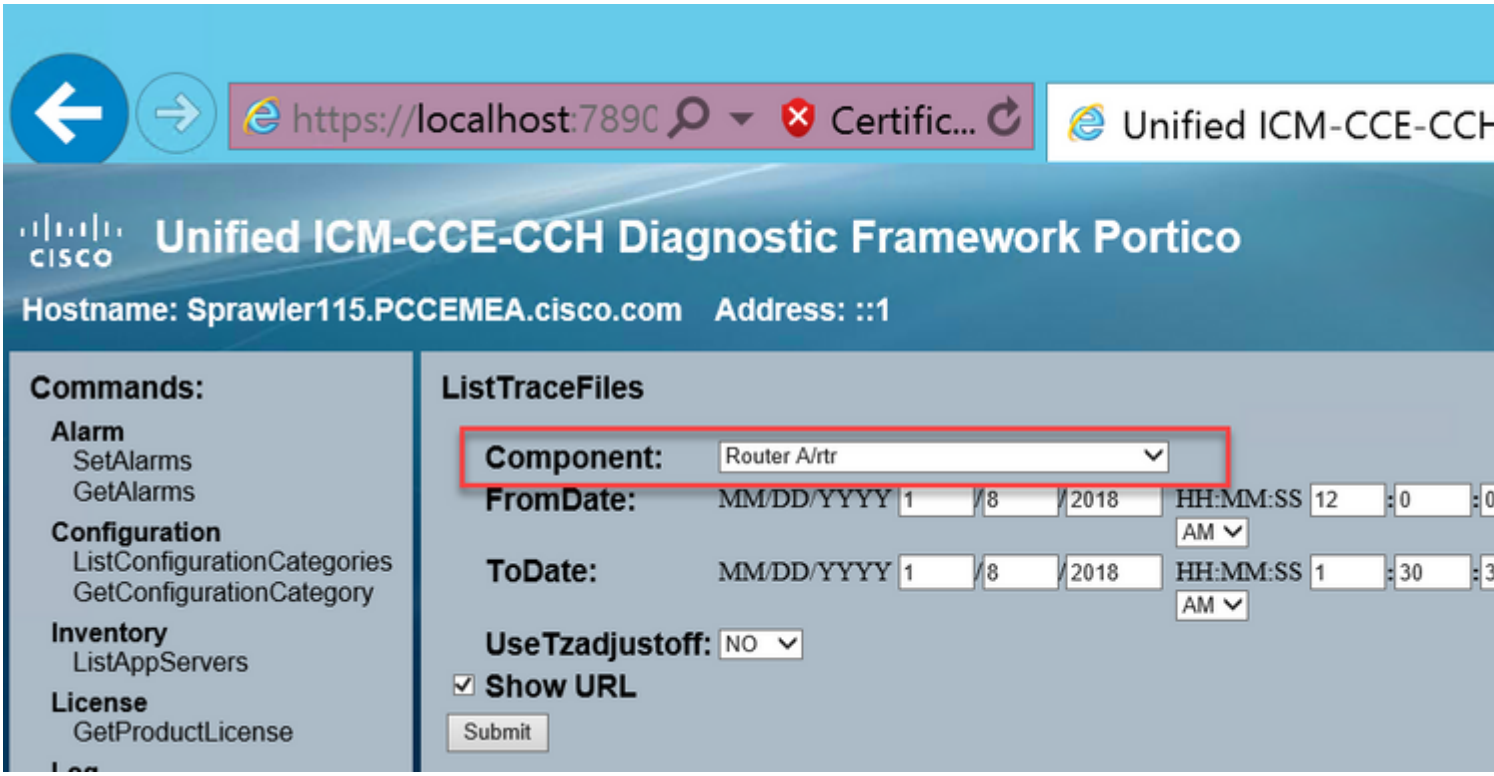


Warnung: Setzen Sie die Ebene der Spuren auf Ebene 3, während Sie mit der Reproduktion des Problems beginnen. Nachdem das Problem reproduziert wurde, setzen Sie die Ablaufverfolgungsebene auf die Standardeinstellung. Seien Sie besonders vorsichtig, wenn Sie die JTAPIGW-Ablaufverfolgungen festlegen, da 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 sich in einer Laborumgebung befinden.

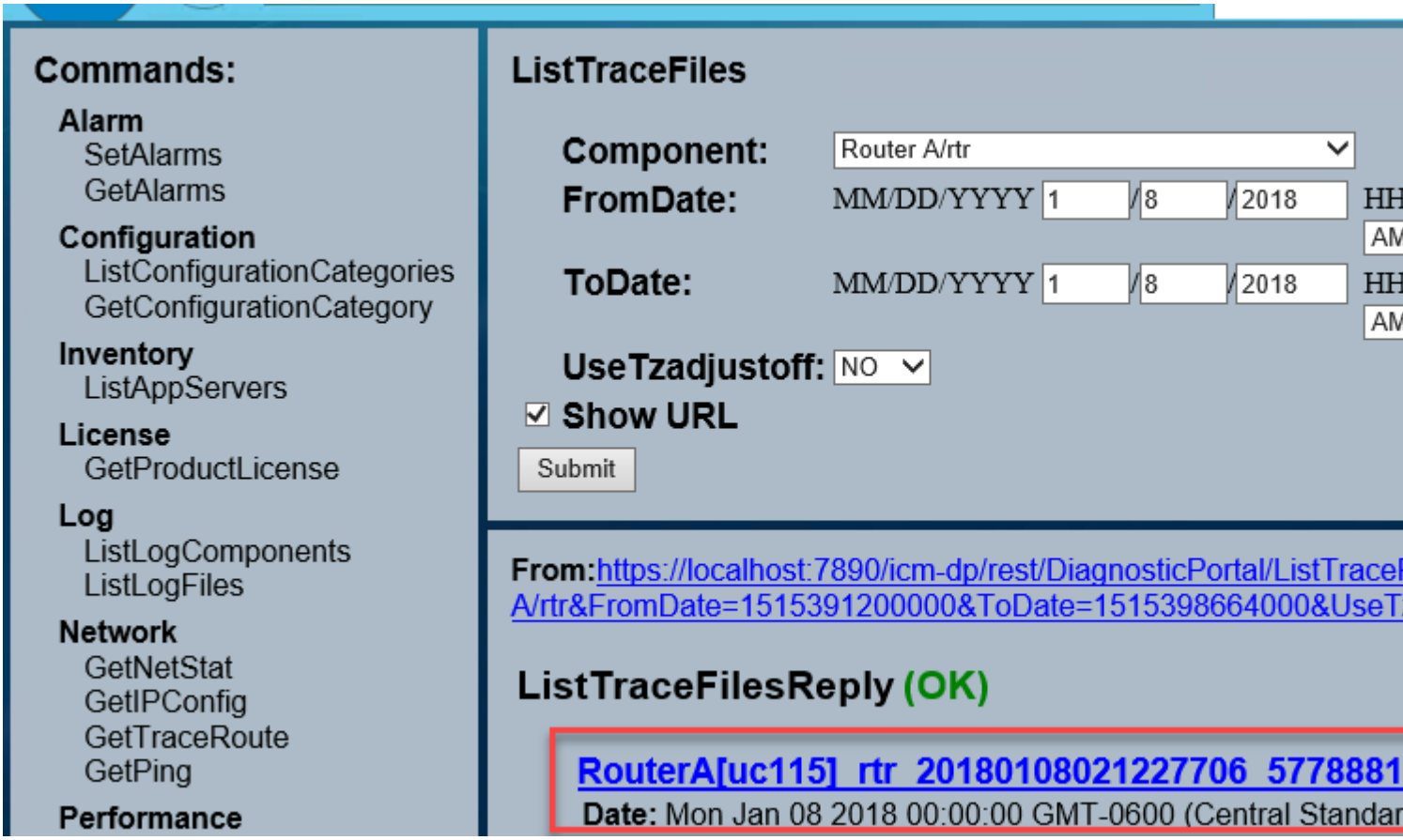
Protokollsammlung
Schritt 1: Navigieren Sie im Abschnitt "Befehle" des Portlets "Diagnoseframework" zu Trace, und wählen Sie ListTraceFile aus.



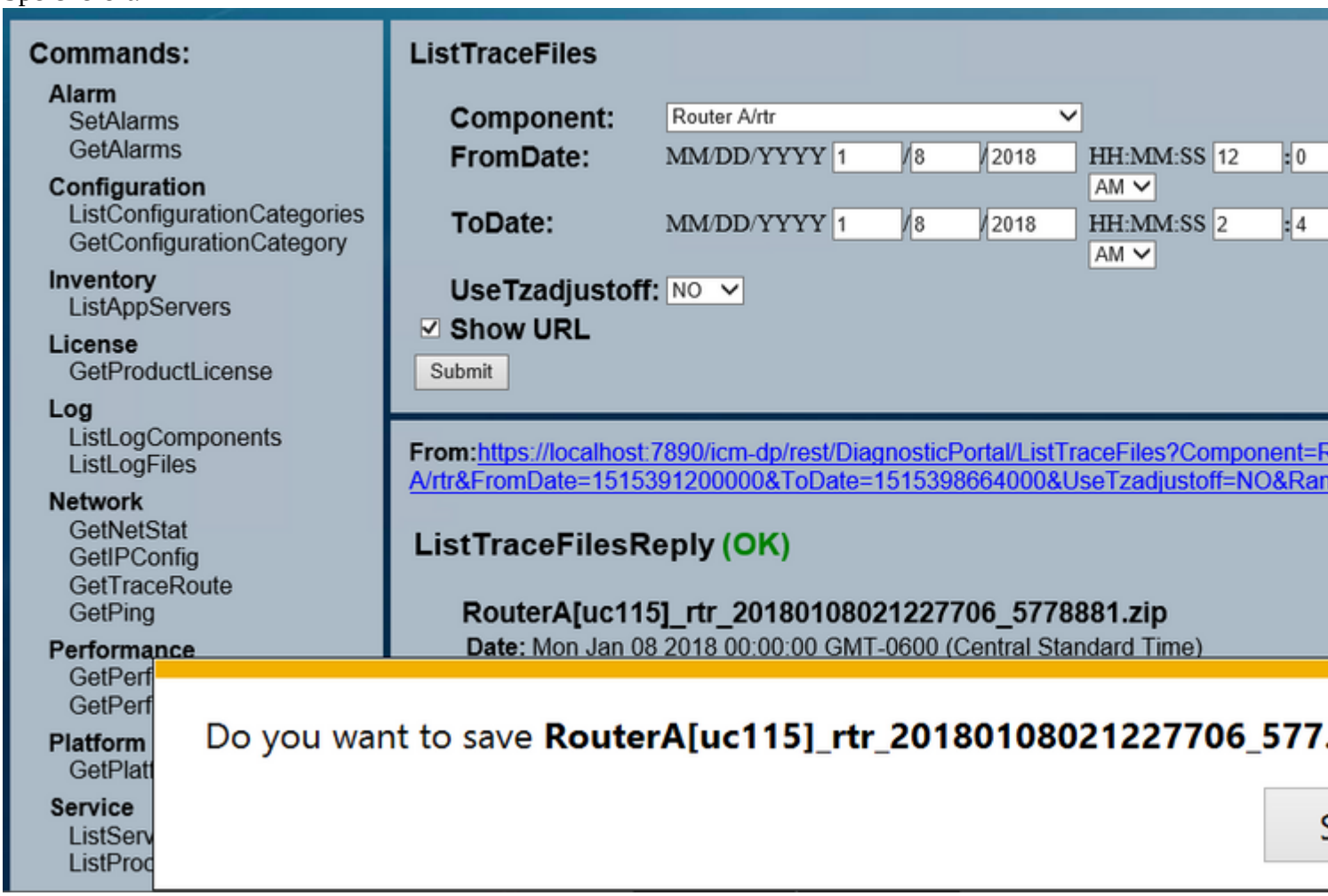
Schritt 2: Wählen Sie im ListTraceFile-Fenster Component, FromDate und ToDate aus. Aktivieren Sie das Kontrollkästchen Show URL (URL anzeigen), und klicken Sie dann auf Submit (Senden).



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



Schritt 4: Klicken Sie auf den Link Zip-Datei und speichern Sie die Datei an dem von Ihnen gewählten Speicherort.

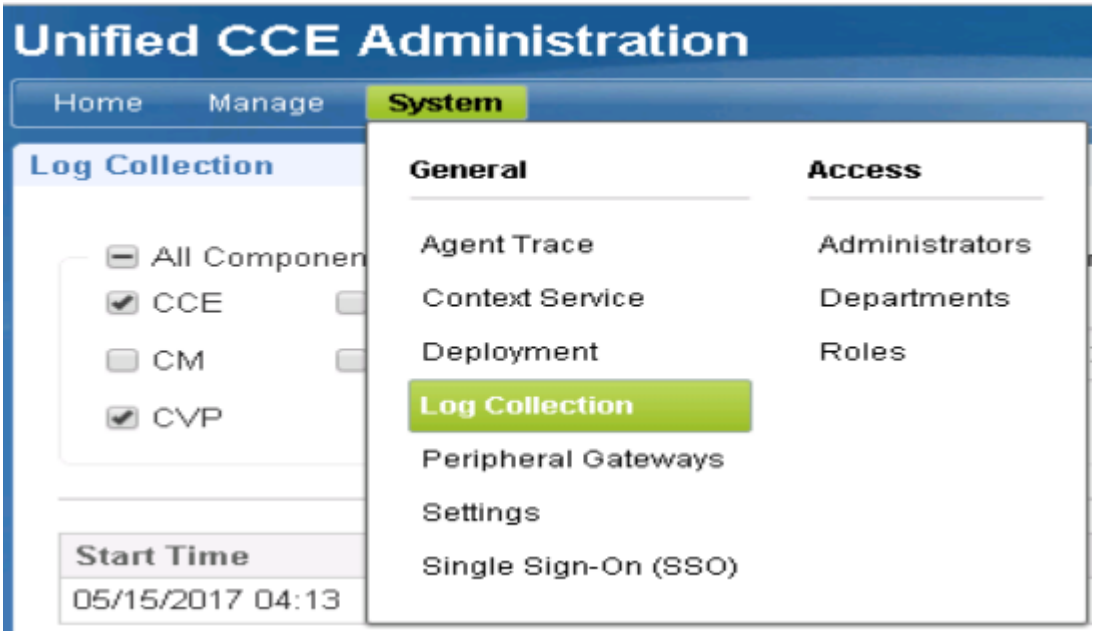


Ablaufverfolgungseinstellungen und Protokollsammlung - PCCE

PCCE verfügt über ein eigenes Tool zum Einrichten von Ablaufverfolgungsebenen. Sie ist nicht auf UCCE-Umgebungen anwendbar, in denen das Diagnose-Framework-Portal oder die System-CLI die bevorzugten Möglichkeiten zum Aktivieren und Erfassen von Protokollen darstellen.

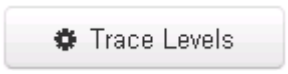
Schritt 1: Öffnen Sie auf dem PCCE AW-Server das Unified CCE-Webverwaltungstool, und melden Sie sich mit dem Administratorkonto an.

Schritt 2: Navigieren Sie zu System ->Log Collection.

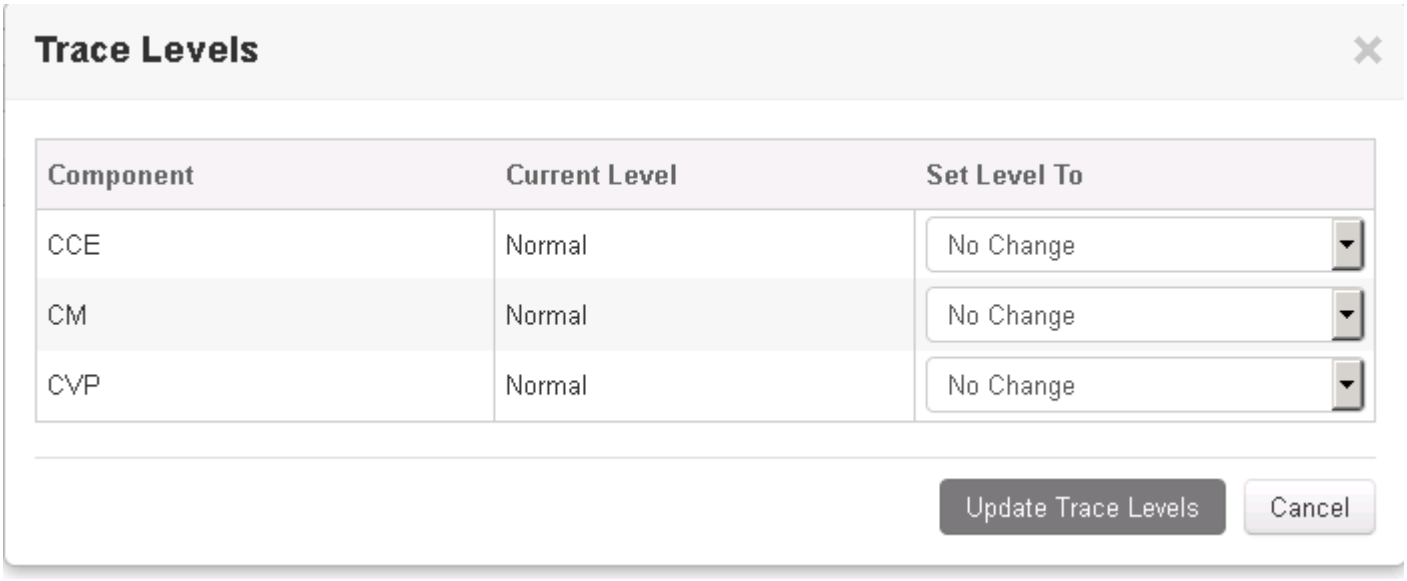


Schritt 3: Die Seite "Log Collection" wird geöffnet.

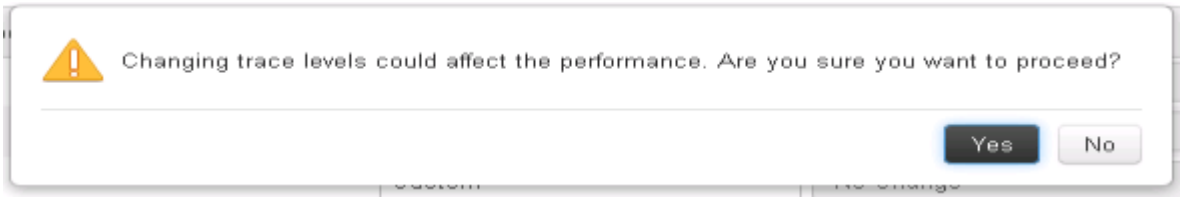
Schritt 4: Klicken Sie auf , Trace Levels, ein Popup-Dialog wird geladen



Schritt 5: Setzen Sie die Ablaufverfolgungsebene in CCE auf "Detailed", und belassen Sie sie bei "No Change for CM, CVP". und klicke auf "Trace-Ebenen aktualisieren".



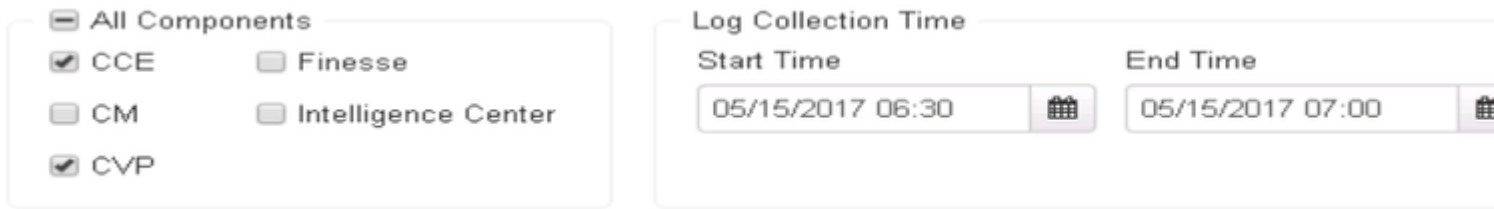
Schritt 6: Klicken Sie auf Ja, um die Warnung zu bestätigen.



Schritt 7. Wenn das Problem reproduziert wurde, öffnen Sie die Unified CCE-Verwaltung, und navigieren Sie zurück zu System -> Log Collection.

Schritt 8: Wählen Sie im Bereich "Komponenten" die Optionen CCE und CVP aus.

Schritt 9. Wählen Sie die entsprechende Protokollerfassungszeit aus (standardmäßig die letzten 30 Minuten).



Hinweis: Aktualisieren Sie die Seite für die Endzeit, damit sie mit der aktuellen Zeit aktualisiert wird.

Schritt 10. Klicken Sie auf Collect Logs (Protokolle sammeln) und Yes (Ja), um die Dialogwarnung anzuzeigen. Die Protokollsammlung wird gestartet. Warten Sie einige Minuten, bevor es fertig ist.

Schritt 11. Klicken Sie abschließend in der Spalte "Aktionen" auf die Schaltfläche Download, um eine gezippte Datei mit allen darin enthaltenen Protokollen herunterzuladen. Speichern Sie die ZIP-Datei an einem beliebigen Speicherort.

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.