Sporen instellen en logbestanden verzamelen in CCE

Inhoud

Inleiding

Dit document beschrijft hoe u sporen kunt instellen en verzamelen in Cisco Unified Contact Center Enterprise (CCE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Enterprise (UCS)
- Package Contact Center Enterprise (PCE)

- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco gevirtualiseerde spraakbrowser (VVB)
- Cisco Unified border-element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Session Initiation Protocol (SIP) proxy (CUSP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco FineReader-softwarerelease 12.5
- CVP-serverrelease 12.5
- UCS/PCE-release 12.5
- Cisco VVB release 12.5
- CUC-release 12.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

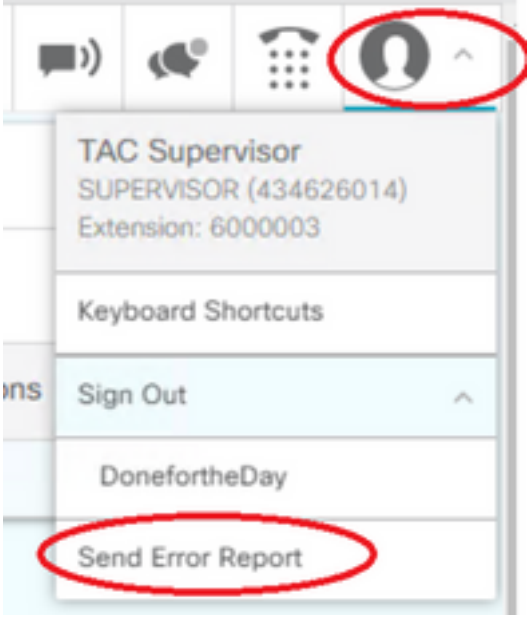
Traces instellen en finesse-logbestanden verzamelen

Finesse-client

Er zijn verschillende opties voor het verzamelen van Finesse client logs.

Optie 1: Verzamel clientlogbestanden via het Send Error Report.

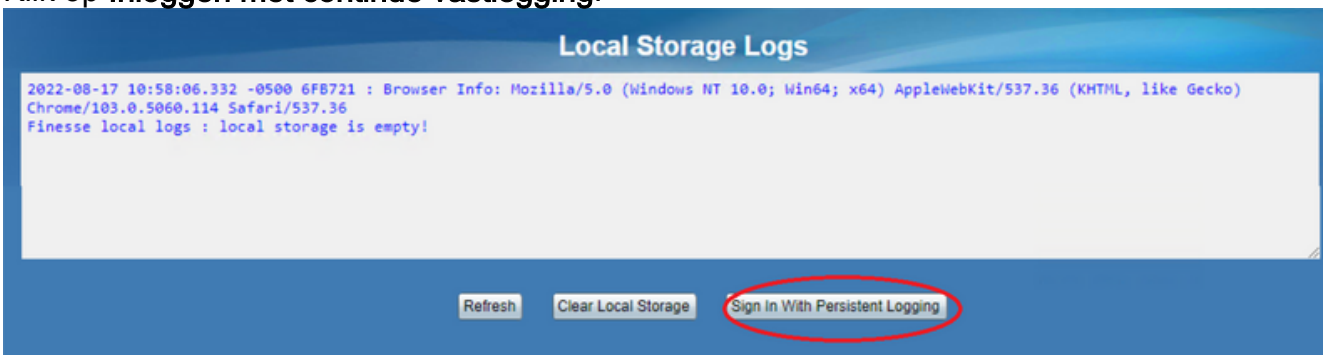
1. Log een agent in.
2. Als een agent een probleem ondervindt tijdens een oproep of media-event, instrueer de agent om te klikken op de koppeling **Send Error Report** in de rechterbovenhoek van het fijne bureaublad.



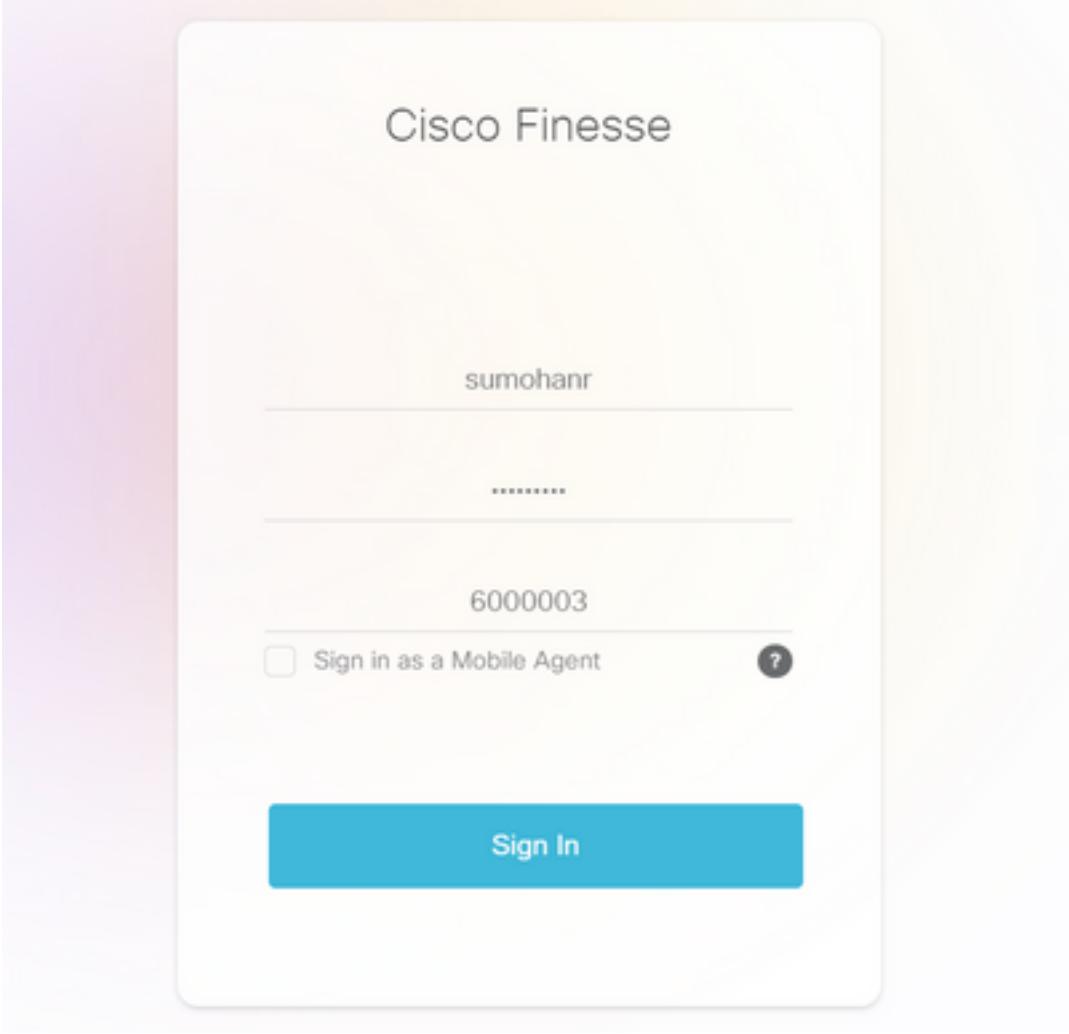
3. De agent ziet de **Logs met succes verzonden!** bericht.
4. De logbestanden van de client worden naar de Finesse-server verzonden. Navigeer naar https://x.x.x.x/finesse/logs en log in met een beheeraccount.
5. Verzamel de logbestanden onder de **clientlogs/** directory.

Optie 2: Vastlegging persistentie

1. Navigeer naar https://x.x.x.x:8445/desktop/locallog.
2. Klik op **Inloggen met continue vastlegging**.



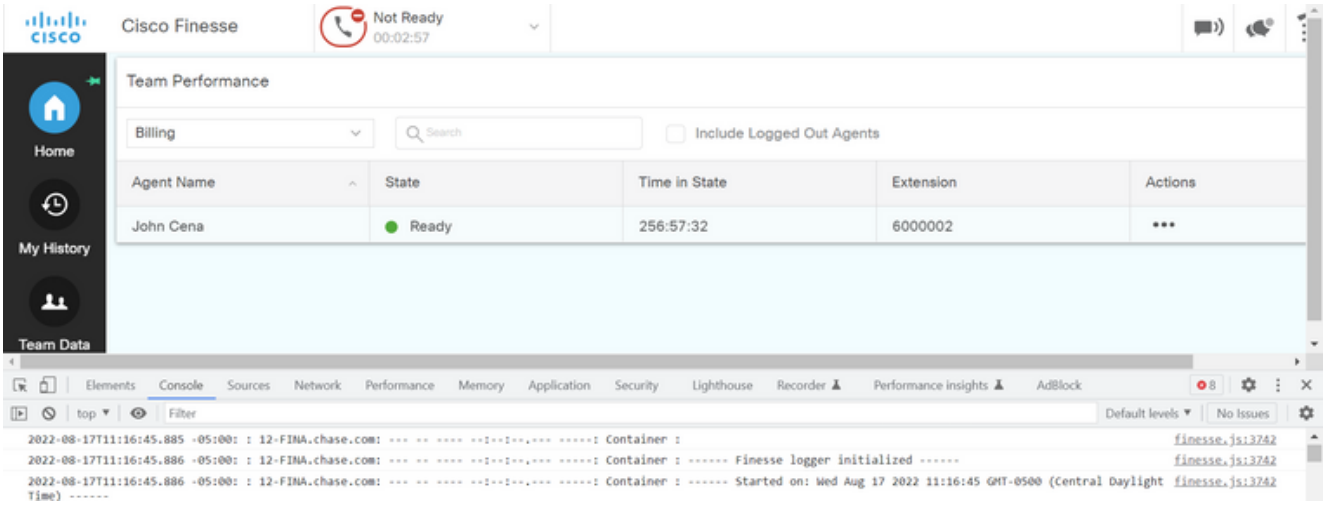
3. De inlogpagina voor Cisco Finesse Agent-bureaublad wordt geopend. Log de agent in.



4. Alle desktopinteractie van de agent wordt geregistreerd en naar de lokale opslaglogs verzonden. Om de logboeken te verzamelen, navigeer aan https://x.x.x.x:8445/desktop/locallog en kopieer de inhoud in een tekstbestand. Save het dossier voor verdere analyse.

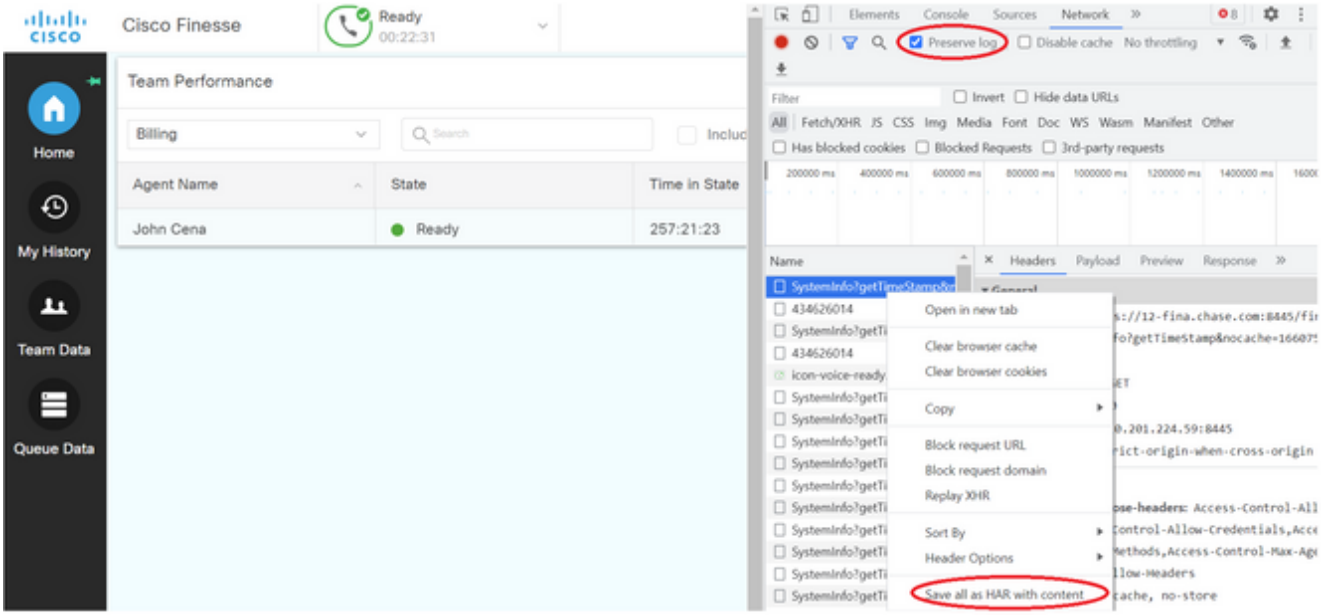
Optie 3: Webbrowser-console

1. Nadat een agent inlogt, drukt u op **F12** om de browserconsole te openen.
2. Selecteer het tabblad **Console**.
3. Controleer de browserconsole op fouten. Kopieert de inhoud naar een tekstbestand en save het.



4. Selecteer het tabblad **Netwerk** en controleer de optie Logbestand behouden.
5. Klik met de rechtermuisknop op een van de netwerknaamgebeurtenissen en selecteer **Save**

als HAR met inhoud.



Finesse-server

Optie 1: Via de gebruikersinterface (UI) - Web Services (vereist) en extra logbestanden

1. Navigeer naar https://x.x.x.x/finesse/logs en log in met de beheeraccount.
2. De directory **webservices/**

3. Verzamel de laatste web service logs. Selecteer het laatste unzip-bestand. Bijvoorbeeld **Desktop-Webservices.201X-..log.zip**. Klik op de bestandslink en u ziet de optie om save het bestand.

4. Verzamel de andere vereiste logbestanden (afhankelijk van het scenario). Bijvoorbeeld, openfire voor meldingen, realm logs voor authenticatie probleem en tomcatlogs voor API problemen.

Opmerking: De aanbevolen methode om de Cisco Finesse-serverlogbestanden te verzamelen is via Secure Shell (SSH) en Secure File Transfer Protocol (SFTP). Deze methode staat u niet alleen toe om de webservices logs te verzamelen, maar alle extra logs zoals, Fippa, openfire, Realm, en Clientlogs.

Optie 2: Via SSH en Secure File Transfer Protocol (SFTP) - aanbevolen optie

1. Log in op de Finesse-server met de SSH.
2. Voer deze opdracht in om de logbestanden te verzamelen die u nodig hebt. De opdracht verzamelt de logbestanden gedurende 2 uur. U wordt gevraagd om SFTP-server te

identificeren waarop de logbestanden zijn geüpload.

file get activelog desktop recurs compress reltime hours 2

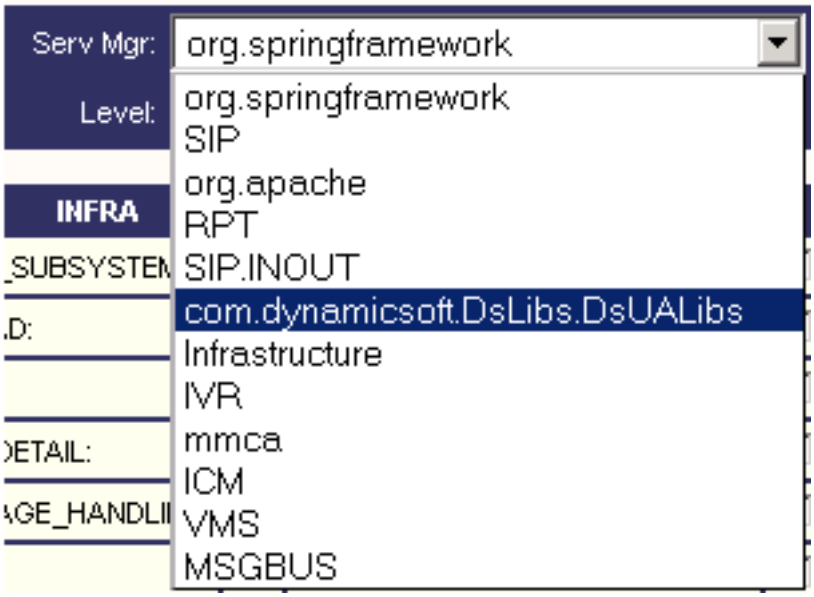
```
Total size in Bytes: 413567
Total size in Kbytes: 403.87402
Would you like to proceed [y/n]? y
SFTP server IP:
```

3. Deze logbestanden worden opgeslagen op het SFTP-serverpad: <IP-adres>\<date time stamp>\active_nnn.tgz, waar nnn tijdstempel in lang formaat is.
4. Als u extra logbestanden wilt verzamelen, zoals logbestanden voor tomcat, Context Service en Server- en installatiebestanden, kijkt u naar het gedeelte Log Collection van Cisco Finesse Administration Guide release 12.5(1).

Traces instellen en CVP- en CVVB-logbestanden verzamelen

CVP-gespreksserver

1. Het CVP CallServer-standaardniveau van overtredingen is voldoende voor probleemoplossing in de meeste gevallen. Wanneer u echter meer informatie wilt over de SIP-berichten (Session Initiation Protocol), moet u de SIP-stracksporen instellen op het DEBUG-niveau.
2. Navigeer naar de CVP CallServer Diag webpagina URL http:/localhost:8000/cvp/diag. **Opmerking:** Deze pagina biedt goede informatie over de CVP CallServer en het is zeer nuttig om bepaalde scenario's problemen op te lossen.
3. Selecteer **com.dynamicsoft.DsLibs.DsUALibs** uit de **Serv. Mgr**-vervolgkeuzemenu in linkerbovenhoek

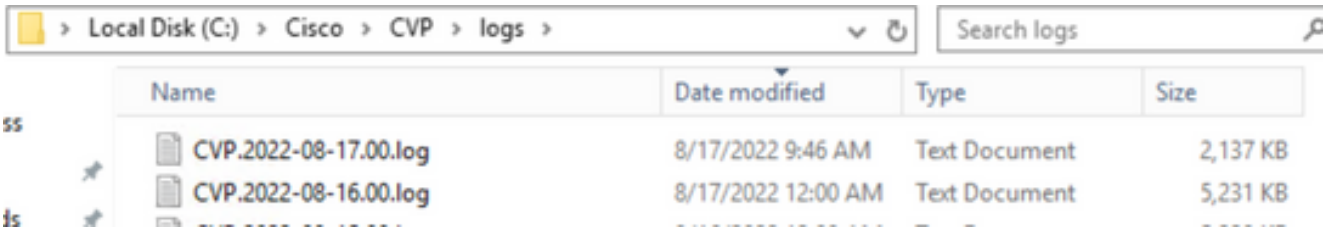


4. Klik op de knop **Instellen**.

5. Blader naar beneden in het overtrek venster om er zeker van te zijn dat het niveau van de sporen juist is ingesteld. Dit zijn uw debug instellingen.

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

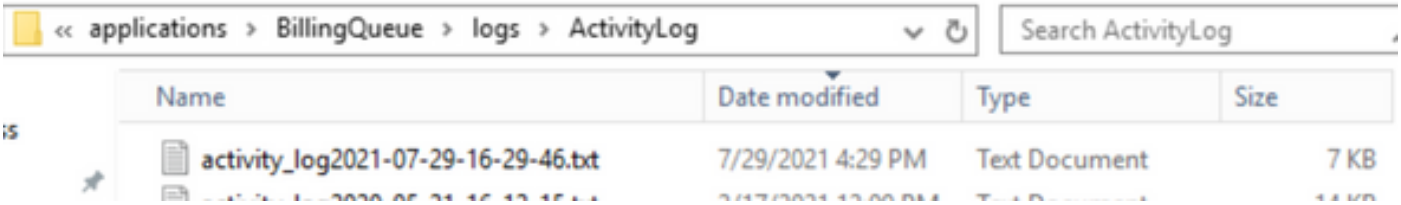
6. Wanneer u het probleem reproduceert, verzamelt u de logbestanden van **C:\Cisco\CVP\logs** en selecteert u het CVP-logbestand op basis van het tijdstip waarop het probleem zich voordeed.



CVP Voice XML (VXML) toepassing

In zeer zeldzame omstandigheden moet u het niveau van sporen van de VXML-servertoepassingen verhogen. Anderzijds wordt het niet aangeraden om de grenswaarde te verhogen, tenzij een Cisco-engineer hierom vraagt.

Om de toepassingslogboeken van de VXML-server te verzamelen, navigeer naar de specifieke toepassingsmap onder de VXML-server, bijvoorbeeld: **C:\Cisco\CVP\VXMLServer\applications\{name of application}\logs\ActivityLog** en verzamel de activiteitenlogboeken.



CVP Operations and Administration Management Portal (OAMP)

In de meeste gevallen is het standaardniveau van sporen van OAMP en ORM voldoende om de grondoorzaak van het probleem te bepalen. Als echter het niveau van sporen moet worden verhoogd, zijn hier de stappen om deze actie uit te voeren:

1. Reserve **%CVP_HOME%\conf\oamp.eigenschappen**

2. Bewerken **%CVP_HOME%\conf\oamp.eigenschappen**

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

3. Start OPSConsoleServer na de wijziging opnieuw zoals aangegeven.

Informatie over traceringsniveau

Overtrek	Beschrijving	Lognivea u	Trace-masker
0	Standaard productinstallatie. Geen of minimale impact op de prestaties verwacht.	INFORM ATIE	None
1	Minder gedetailleerde sporenberichten met een klein effect op de prestaties.	DEBUG GEN	APPARAAT_CONFIGURAT E + DATABASE_WIJZIGEN + BEHEER=0x01011000
2	Gedetailleerde sporenberichten met een gemiddelde prestatie-impact.	DEBUG GEN	APPARAAT_CONFIGURAT E + SYSLVL_CONFIGURATIE + DATABASE_WIJZIGEN + BEHEER=0x05011000
3	Gedetailleerde sporenbericht met een hoog prestatieseffect.	DEBUG GEN	APPARAAT_CONFIGURAT E + SYSLVL_CONFIGURATIE + BULK_OPERATIES + DATABASE_WIJZIGEN + BEHEER=0x05111000
4	Gedetailleerde sporenboodschap met een zeer hoge prestatie impact.	DEBUG GEN	MISC + APPARAAT_CONFIGURAT E + ST_CONFIGURATIE + SYSLVL_CONFIGURATIE + BULK_OPERATIES + BULK_EXCEPTION_STACK TRACE + DATABASE_WIJZIGEN + DATABASE_SELECTIE + DATABASE_PO_INFO + BEHEER + TRACE_METHODE + TRACE_PARAM=0x173710 00
5	Hoogste gedetailleerde spoorbericht.	DEBUG GEN	MISC + APPARAAT_CONFIGURAT E + ST_CONFIGURATIE + SYSLVL_CONFIGURATIE +

BULK_OPERATIES +
BULK_EXCEPTION_STACK
TRACE +
DATABASE_WIJZIGEN +
DATABASE_SELECTIE +
DATABASE_PO_INFO +
BEHEER +
TRACE_METHODE +
TRACE_PARAM=0x17371006

Cisco gevirtualiseerde spraakbrowser (CVVB)

In CVVB, is een spoordossier een logboekdossier dat activiteit van de de componentsubsystemen van Cisco VVB en stappen registreert.

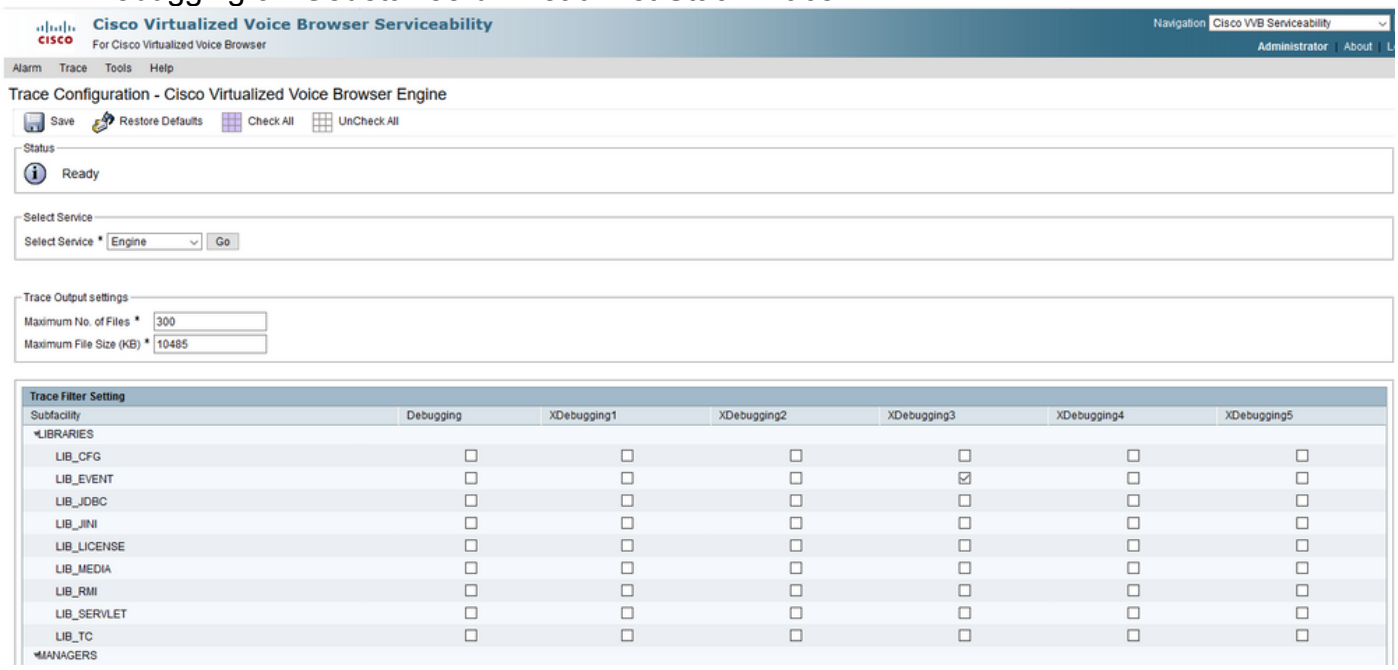
Cisco VVB heeft twee hoofdcomponenten:

- Cisco VVB "Administratie"-sporen aangeduid als MADM-logs
- Cisco VVB "Engine"-sporen als MIVR-logs

U kunt de componenten specificeren waarvoor u informatie wilt verzamelen en het niveau van informatie dat u wilt verzamelen.

Logniveaus variëren van:

- Debuggen - Basisgegevens over doorstroming naar
- XDebugging 5 - Gedetailleerd niveau met Stack Trace



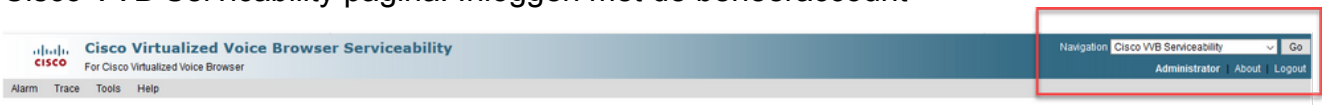
Waarschuwing: Xdebugging5 mag niet worden ingeschakeld op een systeem met productie-lading.

De meest voorkomende logs die u moet verzamelen zijn de Engine. Het standaardniveau van sporen voor de CVVB Engine sporen is genoeg om de meeste problemen op te lossen. Als u echter het niveau van overtredingen voor een specifiek scenario moet wijzigen, raadt Cisco u aan de vooraf gedefinieerde profielen voor systeemlogbestanden te gebruiken.

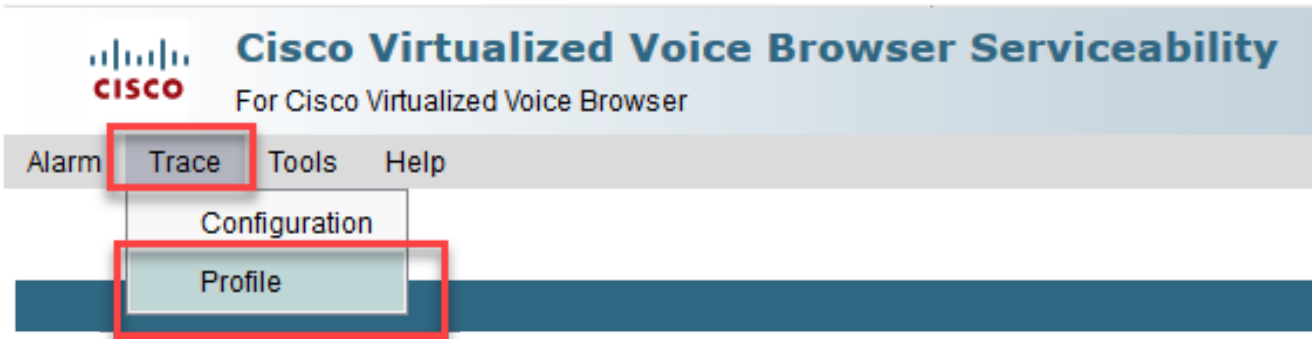
Systeemlogprofielen

Name	Scenario waarin dit profiel moet worden geactiveerd
StandaardVVB	Generic logs zijn ingeschakeld.
AppAdminVVB	Voor problemen met webbeheer via AppAdmin, Cisco VVB Servicability andere webpagina's.
MediaVVB	Voor problemen met de installatie van media of de transmissie van mec
VoiceBrowser VVB	Voor kwesties met vraaghandvat.
MRCPVVB	Voor problemen met ASR/TTS met Cisco VVB interactie.
CallControlVVB	Voor problemen met SIP-signaal worden in het logbestand gepubliceerc

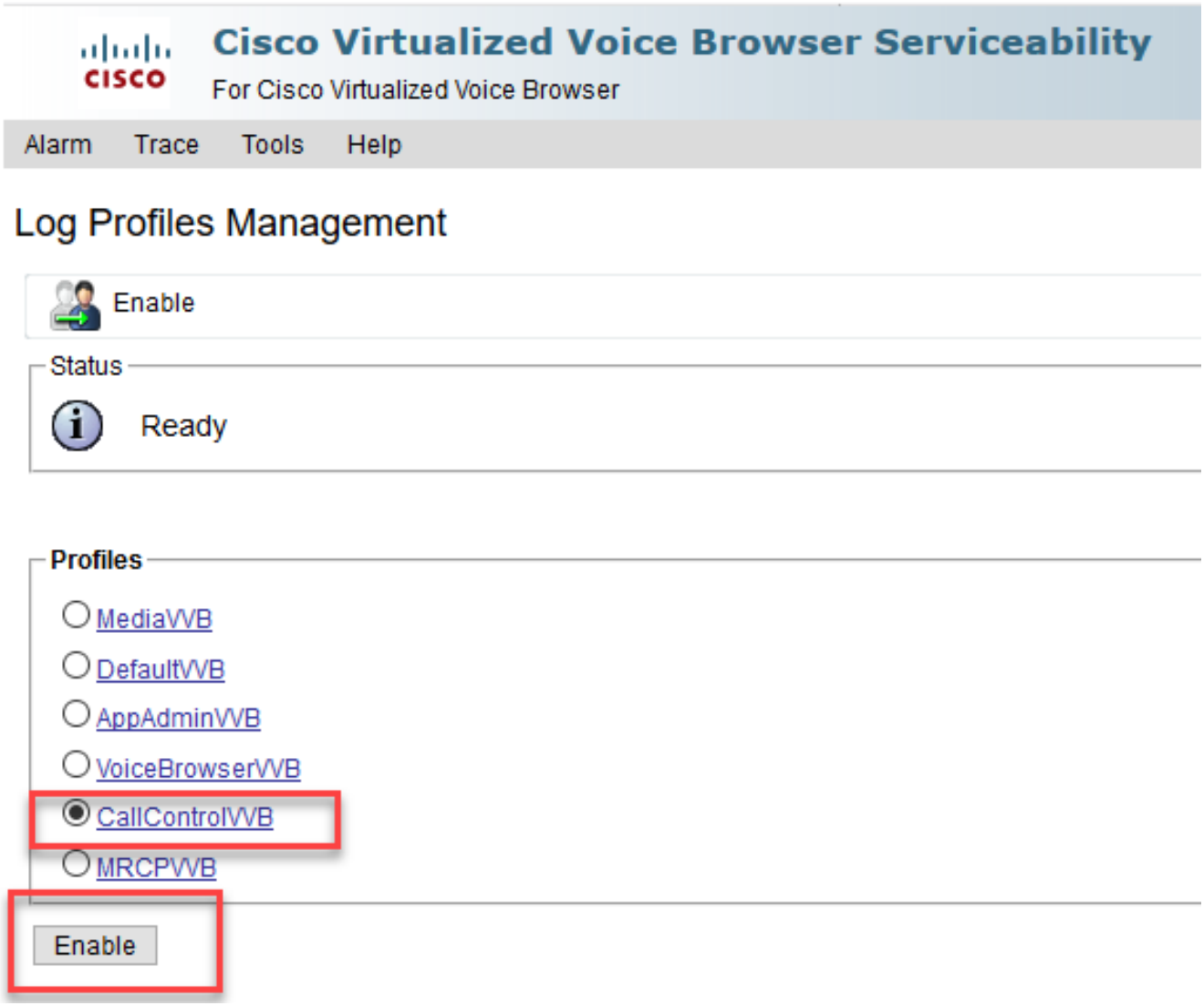
1. Open de CVVB hoofdpagina (https://X.X.X/uccxservice/main.htm) en navigeer naar de Cisco VVB Servicability pagina. Inloggen met de beheeraccount



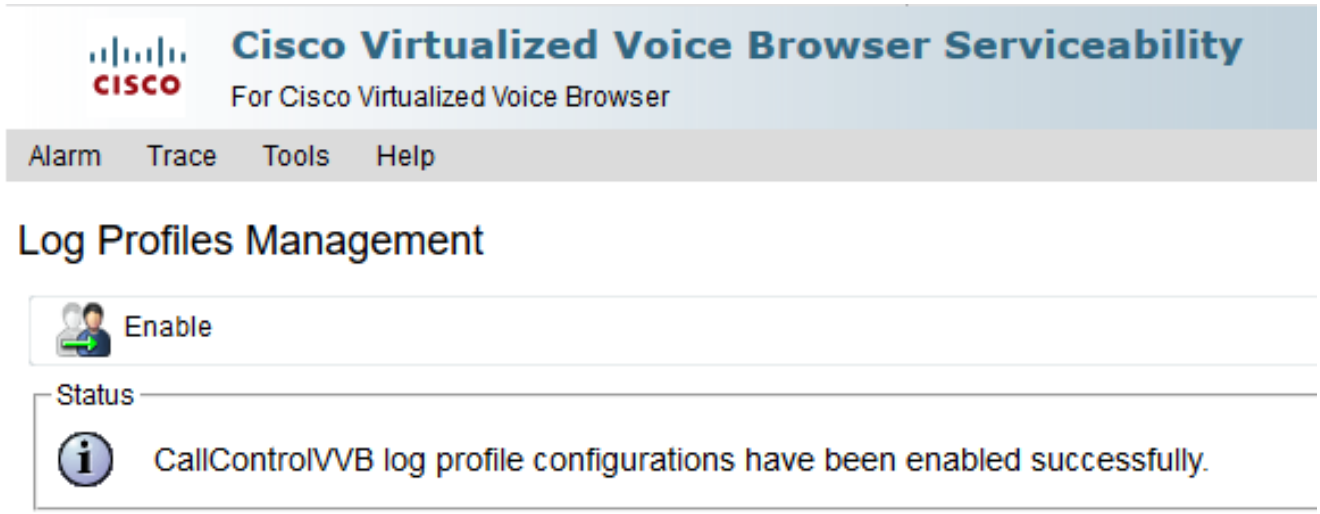
2. Kiezen **Overtrekken -> Profiel.**



3. Controleer het profiel dat u voor het specifieke scenario wilt inschakelen en klik op de knop **Inschakelen**. Schakel bijvoorbeeld het profiel CallControlVVB voor SIP-gerelateerde problemen in of MRCPVVB voor kwesties die verband houden met automatische spraakherkenning en de interactie Text to Speech (ASR/TTS).

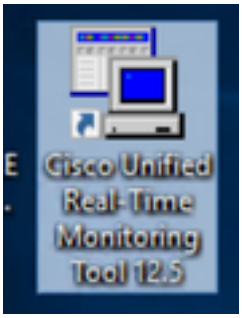


4. U ziet het bericht nadat u op de knop Inschakelen hebt geklikt.

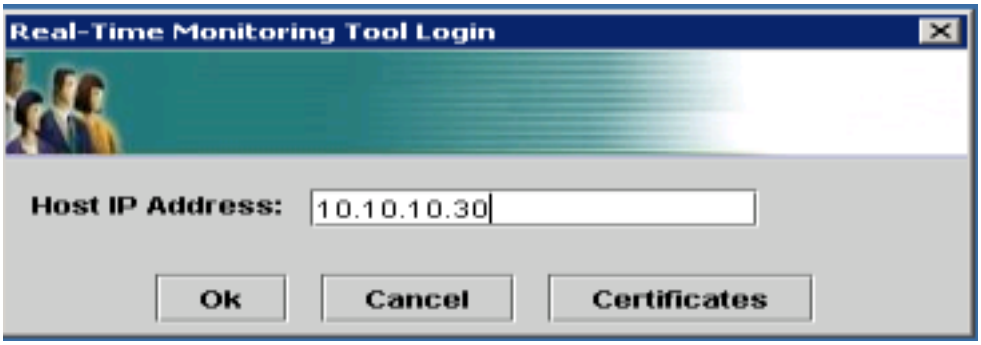


5. Nadat het probleem is gereproduceerd, verzamelt u de logbestanden. Gebruik de Real Time Monitor Tool (RTMT) die bij de CVVB wordt geleverd om de logbestanden te verzamelen.

6. Klik op het pictogram Cisco Unified Real-Time Monitoring Tool op uw bureaublad (indien nodig, download deze tool van de CVVB).

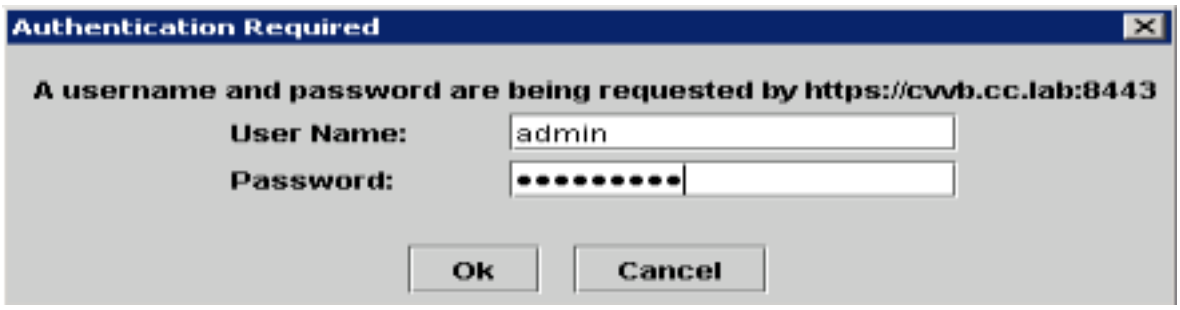


7. Vermeld het IP-adres van de VVB en klik op **OK**.



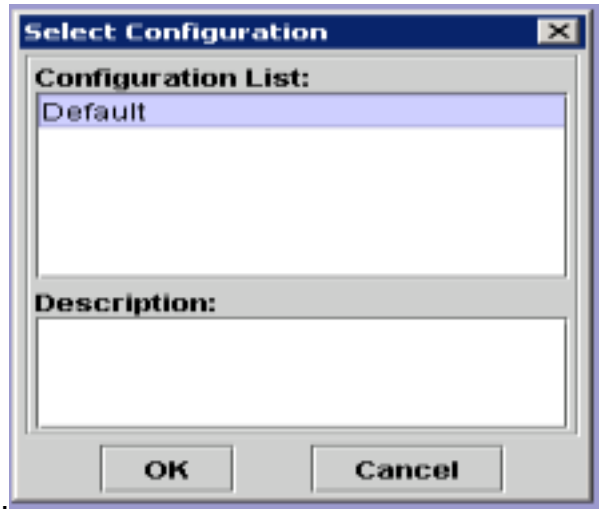
8. De certificaatinformatie accepteren indien deze wordt weergegeven

9. Geef de referenties op en klik op **OK**.

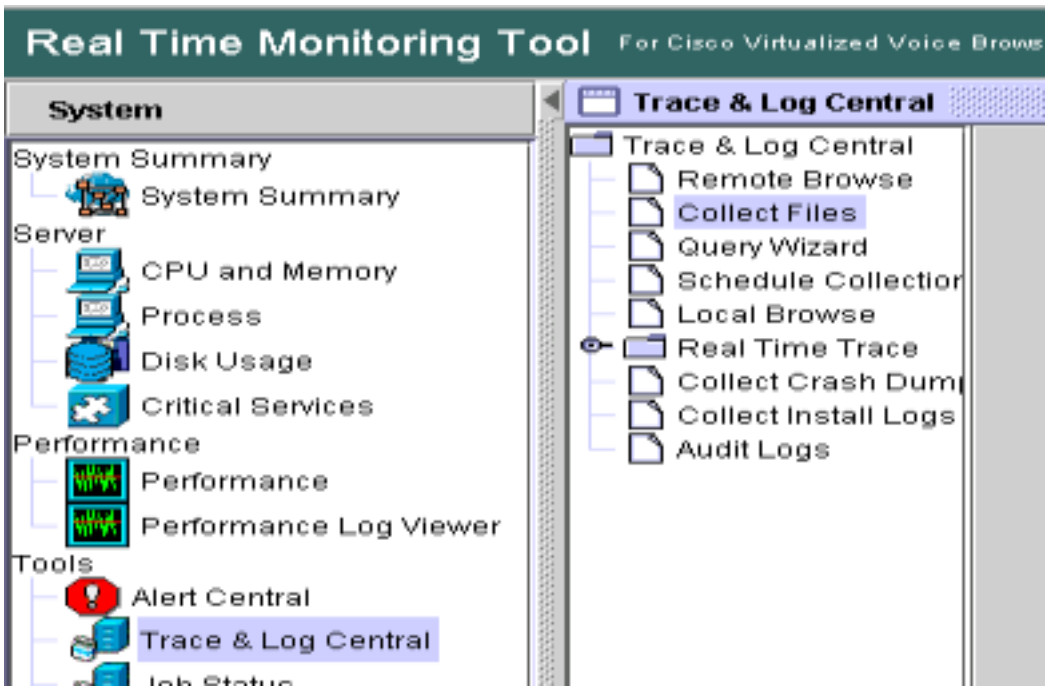


10. Als u de TimeZone-fout hebt ontvangen, kan RTMT worden gesloten nadat u op de knop **Ja** hebt geklikt. Start de RTMT-tool opnieuw.

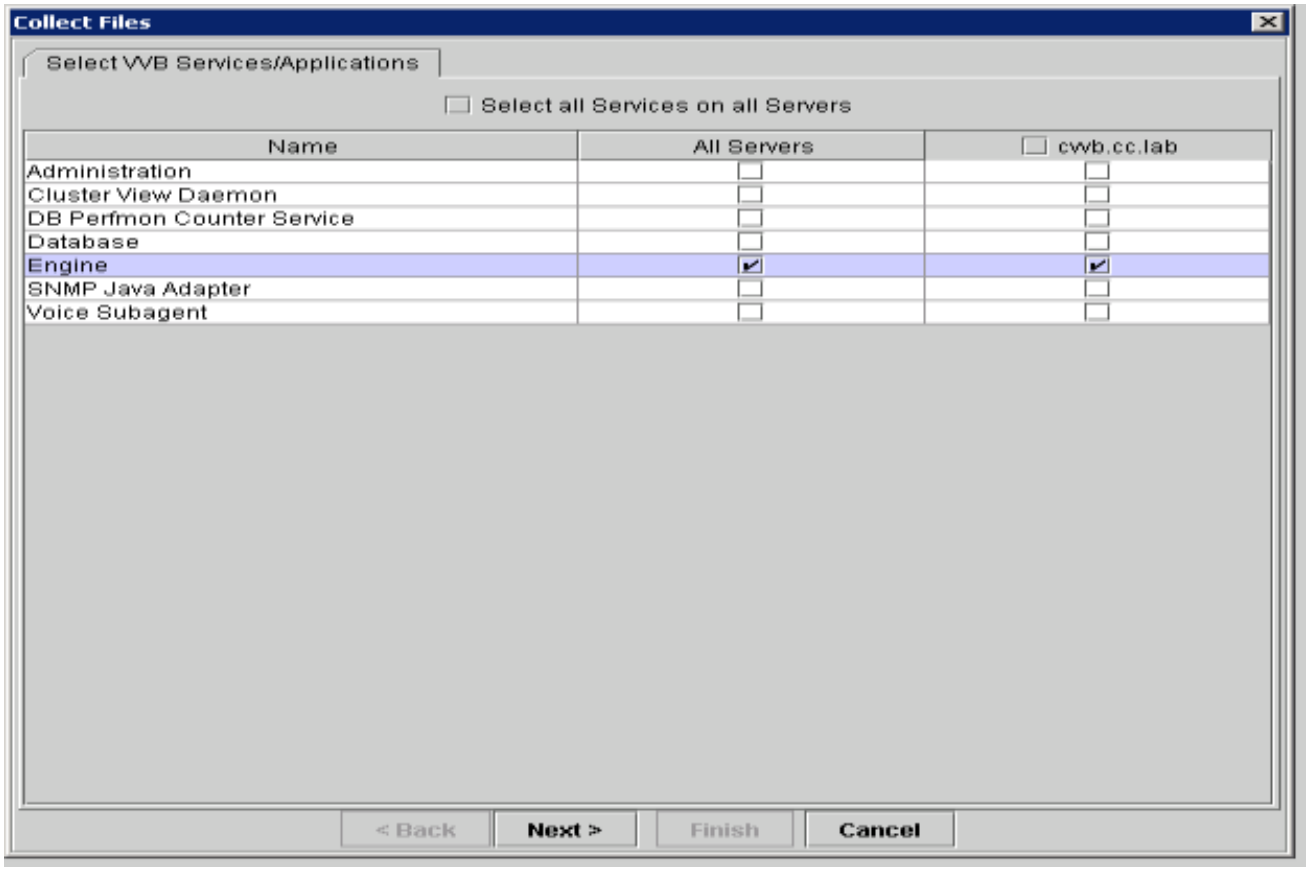
11. Laat de standaardconfiguratie geselecteerd en klik op **OK**.



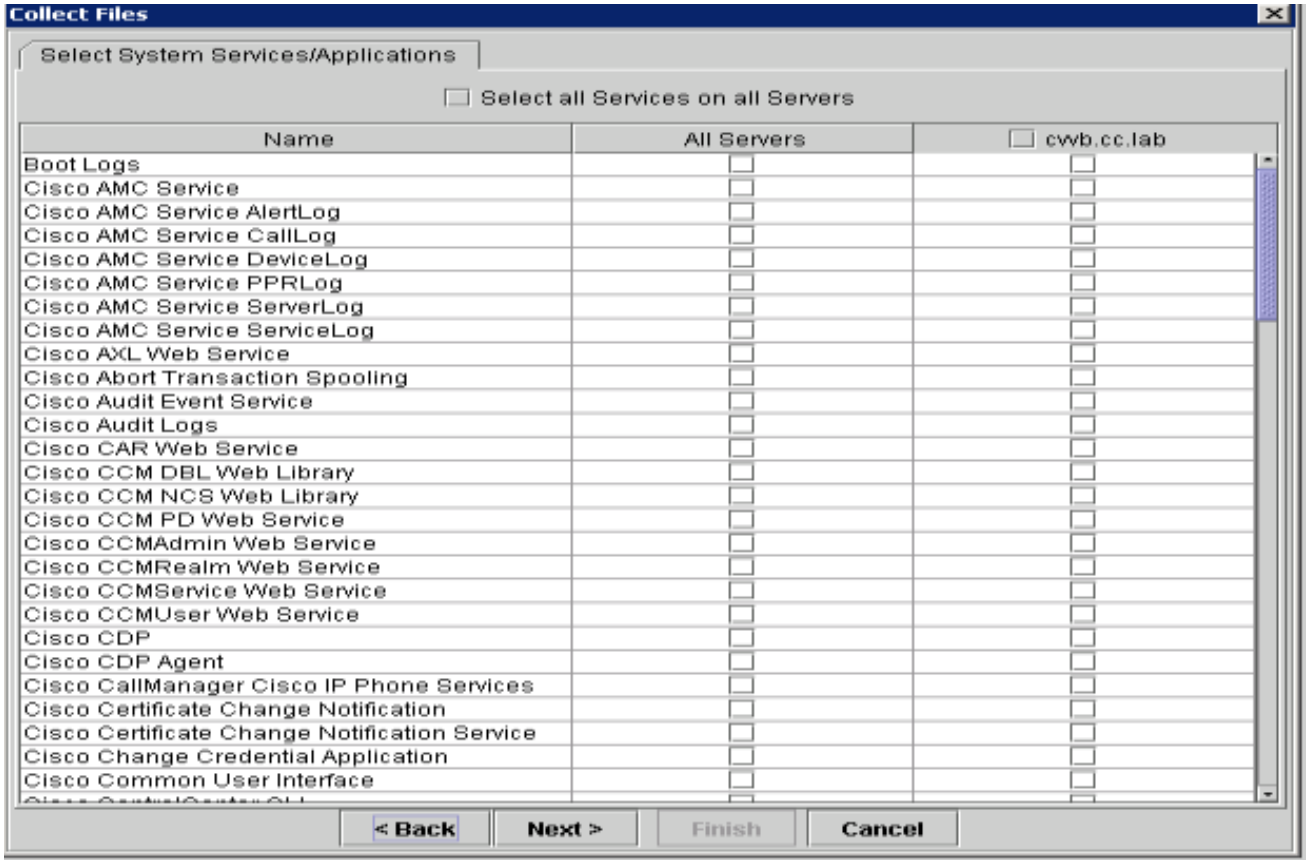
12. Selecteer **Trace & Log Central** en dubbelklik op **Collect Files**.



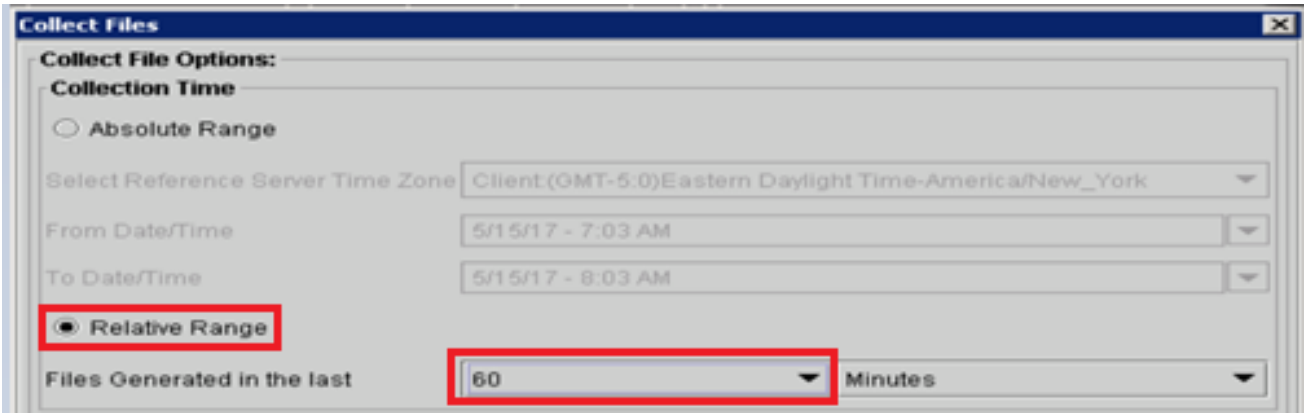
13. Selecteer in het nieuwe geopende venster de **Engine** en klik op Volgende.



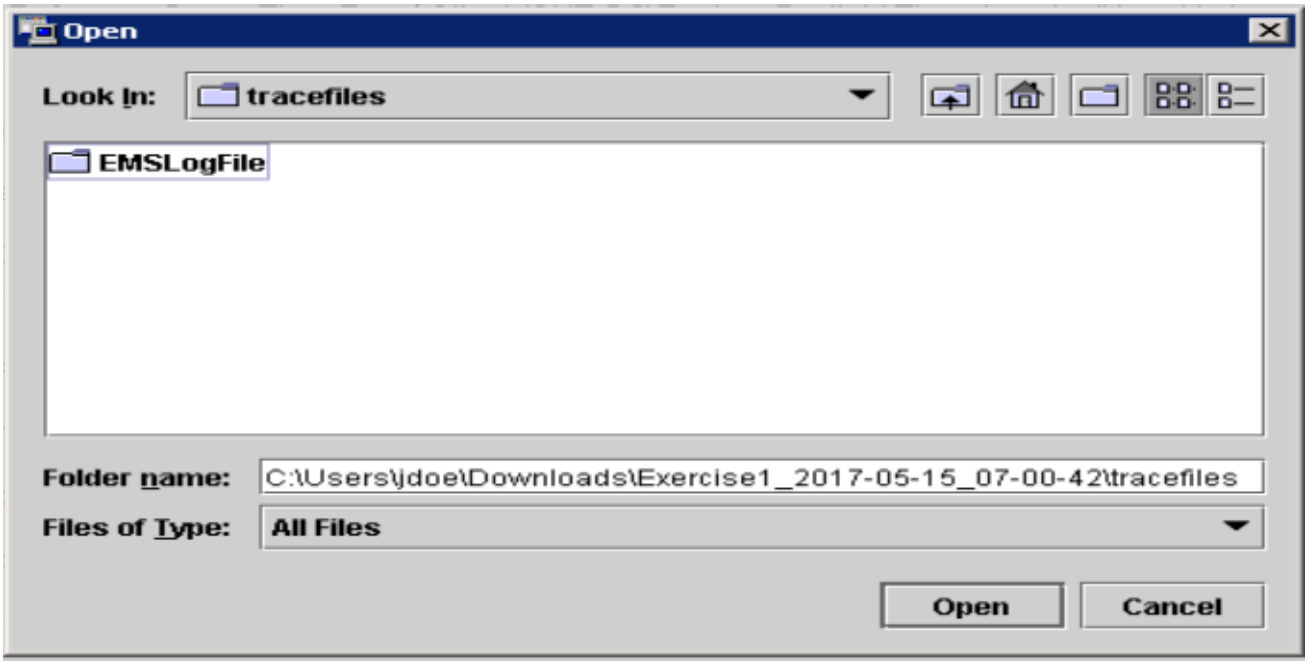
14. Klik nogmaals op **Volgende** in het volgende venster.



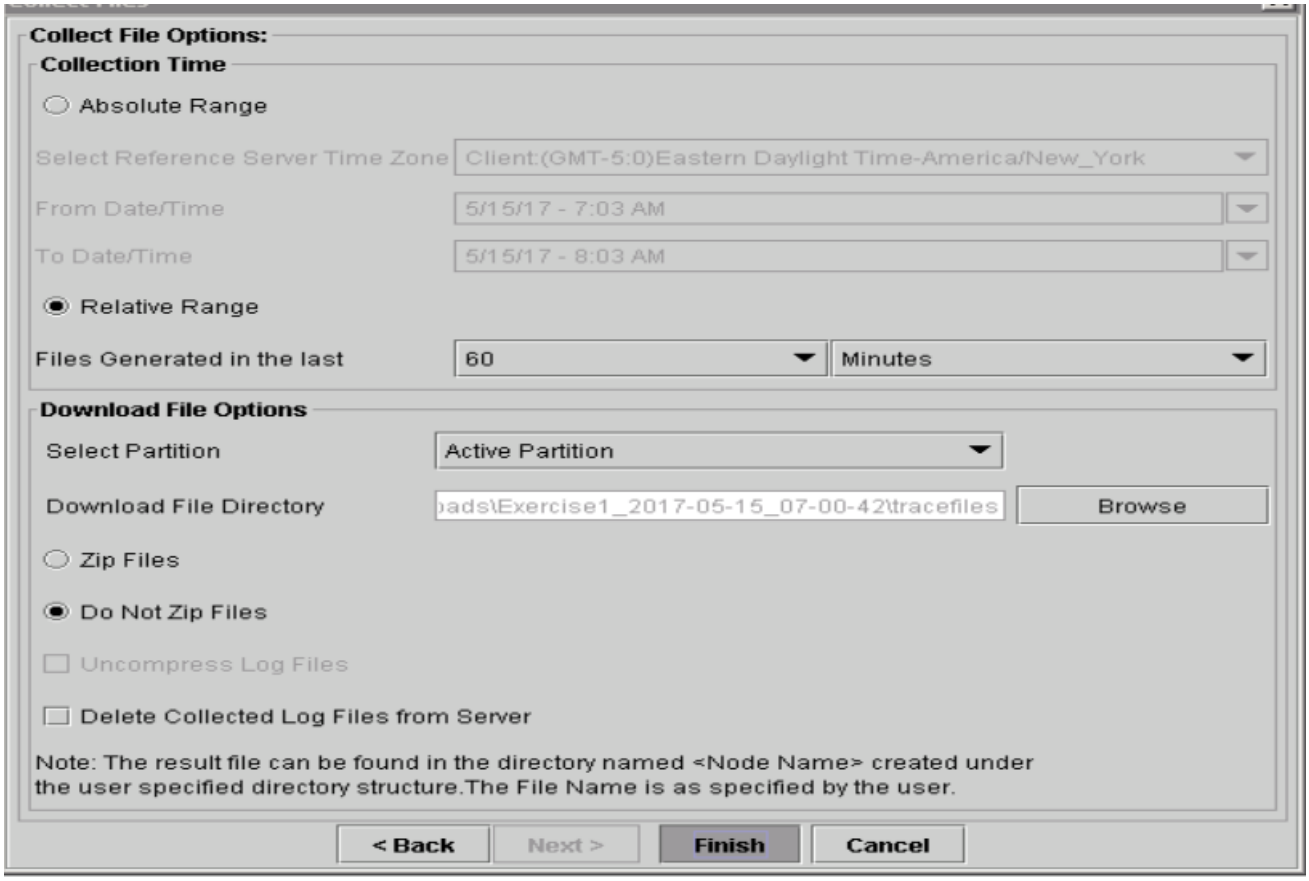
15. Selecteer **Relatief bereik** en zorg ervoor dat u de tijd van uw slechte oproep selecteert.



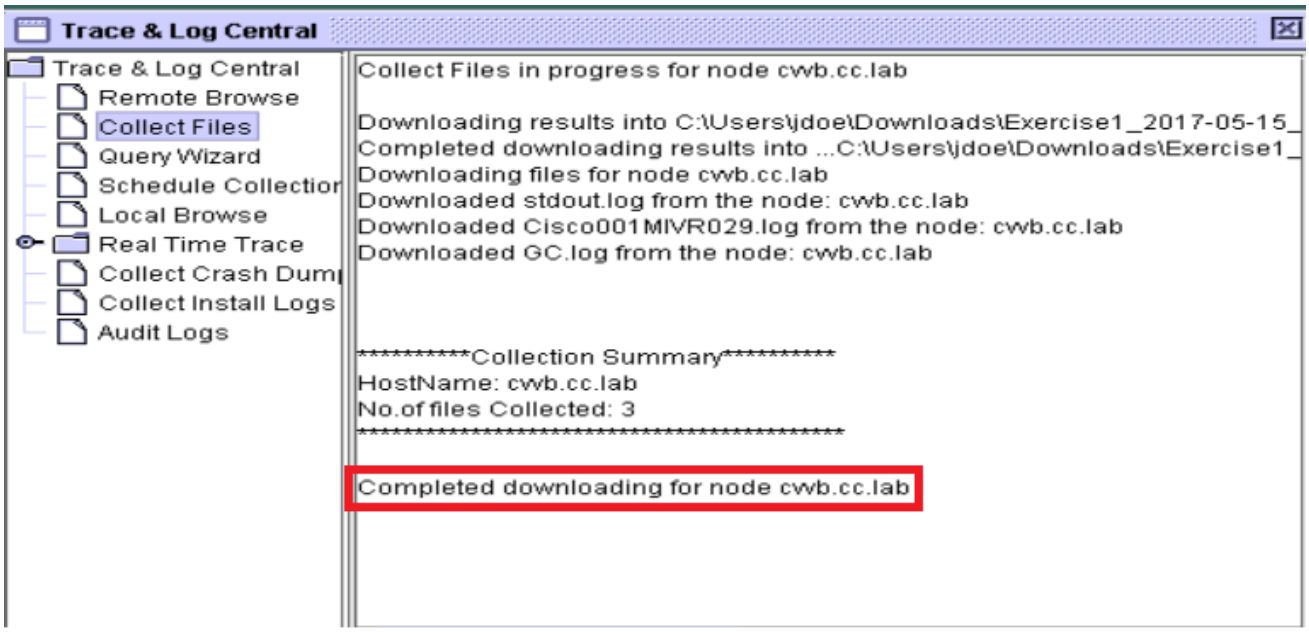
16. Klik in de opties Bestand downloaden op **Bladeren** en selecteer de map waarin u wilt werken save Klik op **Openen** in het bestand.



17. Klik op **Finish** als alles is geselecteerd.



18. Hiermee worden de logbestanden verzameld. Wacht tot je een bevestigingsbericht ziet op RTMT.



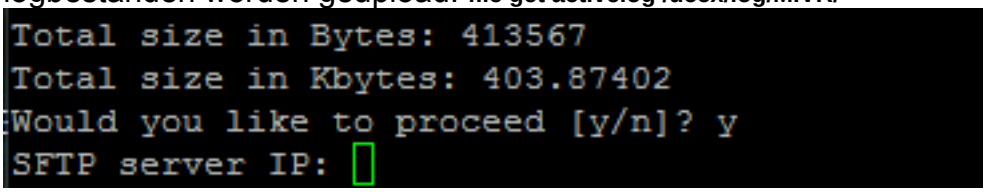
19. Navigeer naar de map waarin de sporen zijn opgeslagen.

20. De Engine logs zijn alles wat je nodig hebt. Om ze te vinden, navigeer je naar **\<tijdstempel>\uccx\log\MIVR** map.

Optie 2: Via SSH en SFTP - aanbevolen optie

1. Log in op de VVB server met de Secure Shell (SSH).

2. Voer deze opdracht in om de logbestanden te verzamelen die u nodig hebt. De logbestanden worden gecomprimeerd en u wordt gevraagd om SFTP-server te identificeren waarop de logbestanden worden geüpload. **file get activelog /uccx/log/MIVR/***



3. Deze logbestanden worden opgeslagen op het SFTP-serverpad: *<IP-adres>**<datum-tijdstempel>**active_nnn.tgz* , waar nnn tijdstempel in lange indeling is.

Logboeken instellen voor overtrekken en verzamelen van CUBE en CUSP

CUBE (SIP)

1. Stel de logtijdstempel in en schakel de logboekbuffer in.

```
#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
```

Waarschuwing: Elke wijziging in een productie van Cisco IOS® software GW kan een stroomonderbreking veroorzaken.

2. Dit is een zeer robuust platform dat de voorgestelde debugs bij het verstrekte vraagvolume zonder kwestie kan behandelen. Cisco raadt u echter aan: Verzend alle logbestanden naar een syslogserver in plaats van naar de logboekbuffer.

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

Pas de debug-opdrachten één voor één toe en controleer het CPU-gebruik na elke opdracht.

```
show proc cpu hist
```

Waarschuwing: Als de CPU tot 70-80% CPU-gebruik toeneemt, is het risico van een prestatiegerelateerde impact op de service enorm toegenomen. Schakel dus geen extra debugs in als de GW 60% bereikt.

3. Schakel deze debugs in:

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

4. Reproduceert het probleem.
5. Schakel de sporen uit.

```
#undebug all
```

6. Verzamel de logboeken.

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

KUSSEN

1. Schakel SIP-sporen in op CUSP.
   ```
   (cusp)> config
   (cusp-config)> sip logging
   (cusp)> trace enable
   (cusp)> trace level debug component sip-wire
   ```
2. Reproduceert het probleem.
3. Schakel de logboekregistratie uit als u klaar bent.

De logbestanden verzamelen

1. Configureer een gebruiker op de CUSP (bijvoorbeeld: test).
2. Voeg deze configuratie toe aan de CUSP-prompt.
   ```
   username <userid> create
   username <userid> password <password>
   username <userid> group pfs-privusers
   ```
3. FTP naar het CUSP IP-adres. Gebruik de gebruikersnaam (test) en het wachtwoord zoals gedefinieerd in de vorige stap.
4. Wijzing de directory's naar /cusp/log/trace.
5. Verkrijg het log_<filename>.

Logboeken voor overtrekken en verzamelen instellen

Cisco raadt aan overtrek-niveaus in te stellen en sporen te verzamelen via Diagnostis Framework Portico of System CLI tools.

> **Opmerking:** Ga voor meer informatie over Diagnostic Framework Portico en System CLI naar het hoofdstuk Diagnostische tools op de Servicehandleiding voor Cisco Unified ICM/Contact Center Enterprise, release 12.5(1).

Wanneer u de meeste scenario's van UCCE problemen oplost, als het standaardniveau van sporen niet genoeg informatie verstrekt, stel het niveau van sporen in op 3 in de vereiste componenten (met sommige uitzonderingen).

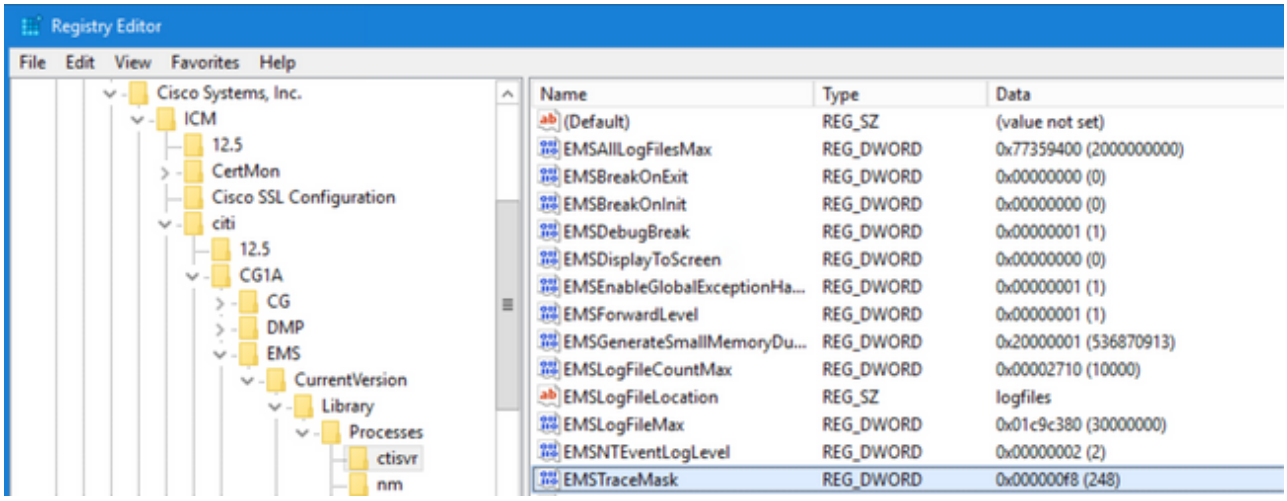
> **Opmerking:** Ga naar de sectie Trace Level op de servicesgids voor Cisco Unified ICM/Contact Center Enterprise, release 12.5(1) voor meer informatie.

Als u bijvoorbeeld problemen met uitgaande snelkiezer oplost, moet het niveau van de sporen worden ingesteld op niveau 2 als de snelkiezer bezig is.

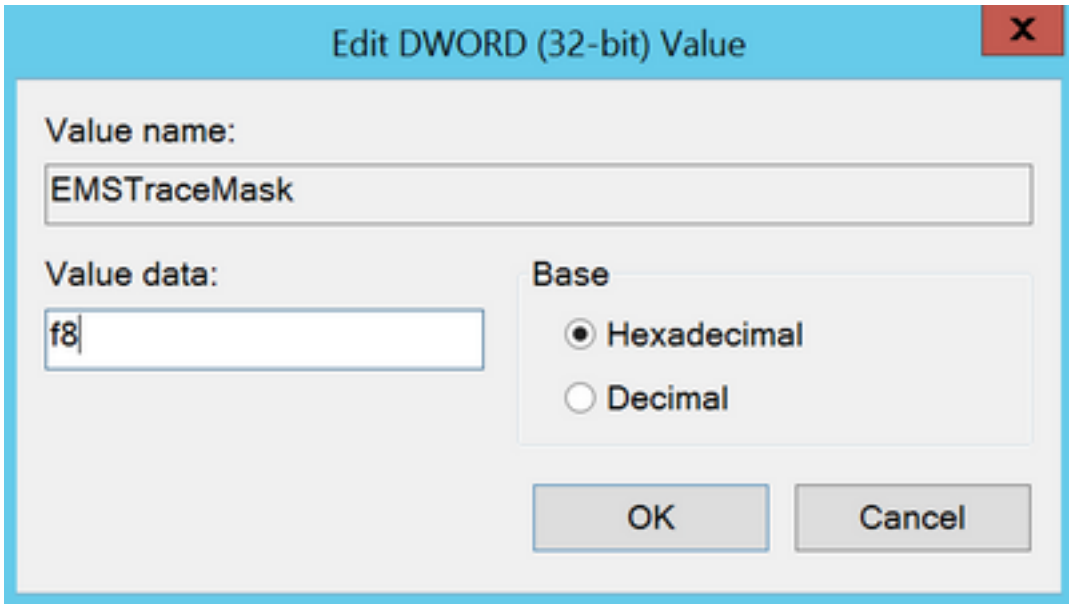
Voor CTISVR (CTISVR) stelt niveau 2 en 3 niet het exacte registerniveau in dat door Cisco wordt aanbevolen. Het aanbevolen sporenregister voor CTISVR is 0XF8.

1. Open de Register-editor (Regedit) op de PG van UCCE Agent.

2. Ga naar HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a en b)\EMS\CurrentVersion\library\Processes\ctisvr.



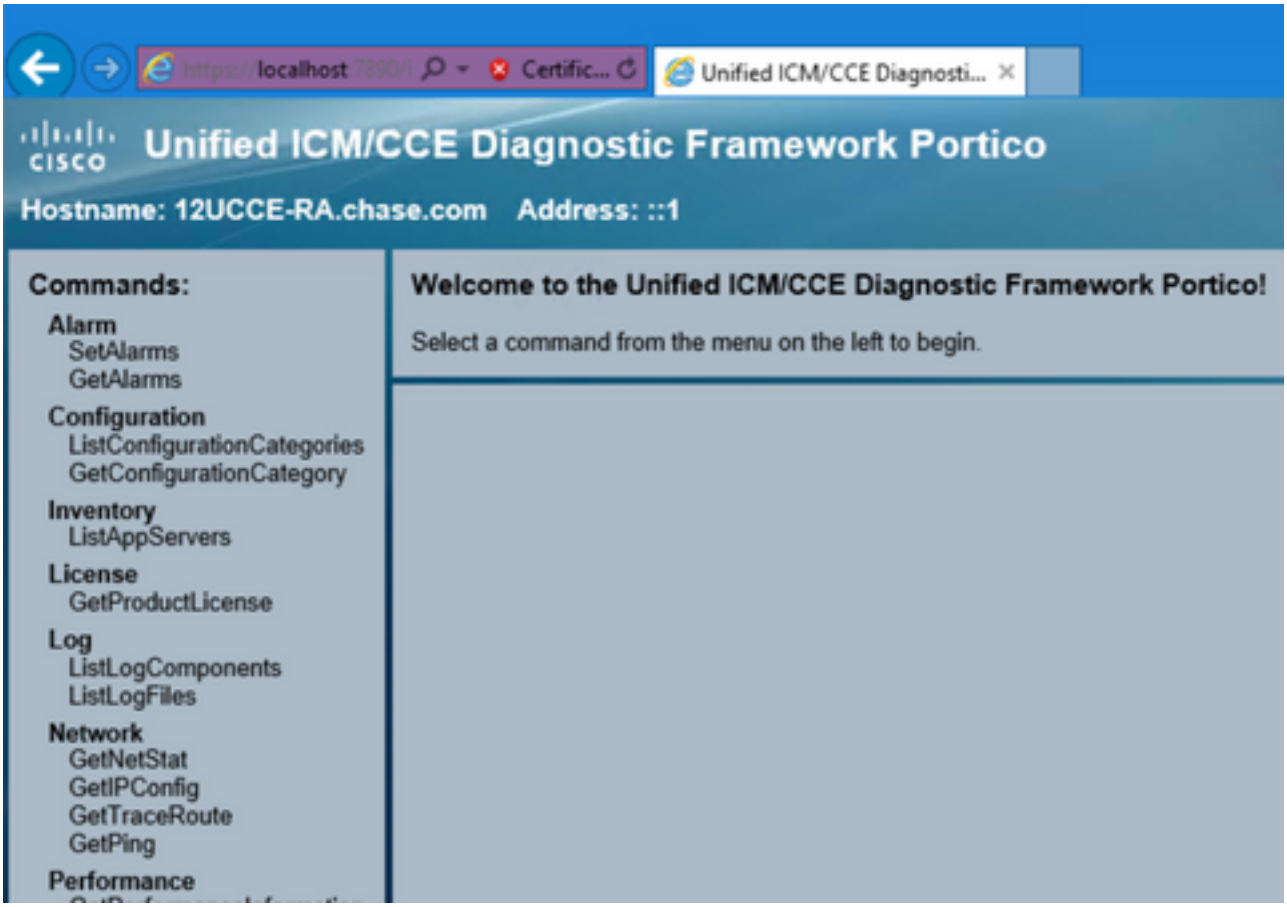
3. Dubbelklik op het **EMSTraceMask** en stel de waarde in op **f8**.



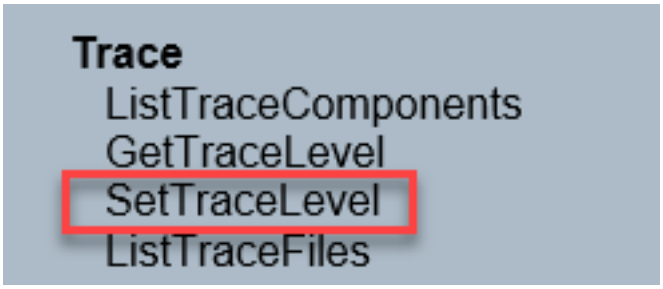
4. Klik op **OK** en sluit de Register-editor. Dit zijn de stappen voor het instellen van een van de sporen van de UCCE-component (het RTR-proces wordt als voorbeeld gebruikt).

Overtrek instellen

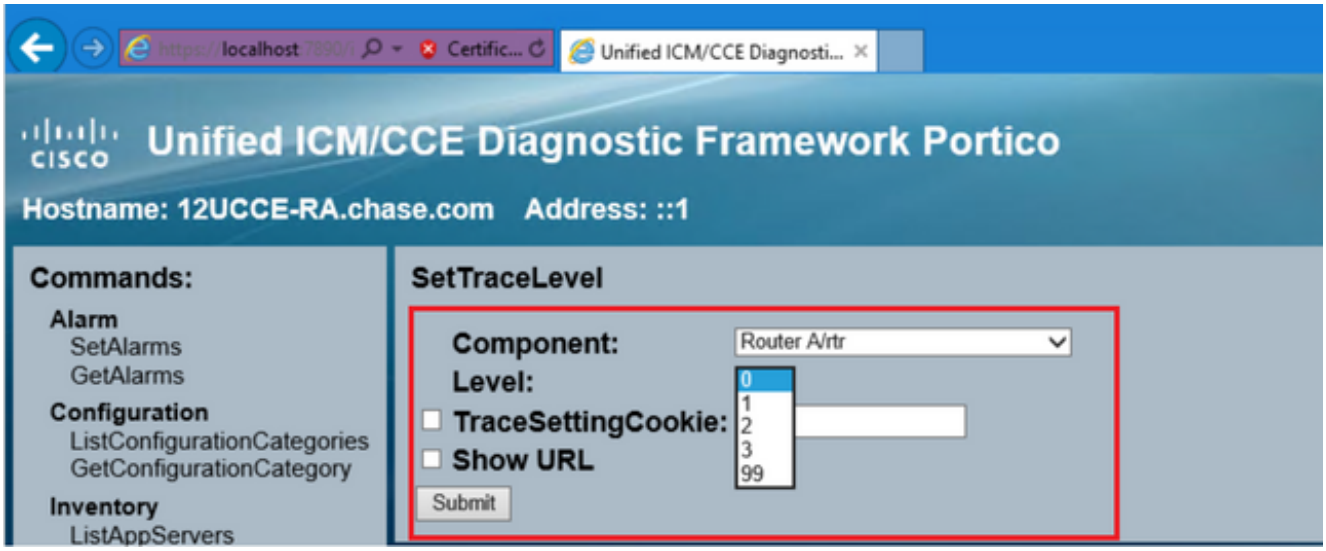
1. Open het Diagnostic Framework Portico vanaf de server die u nodig hebt om de overtrekken in te stellen, en log in als beheerder gebruiker



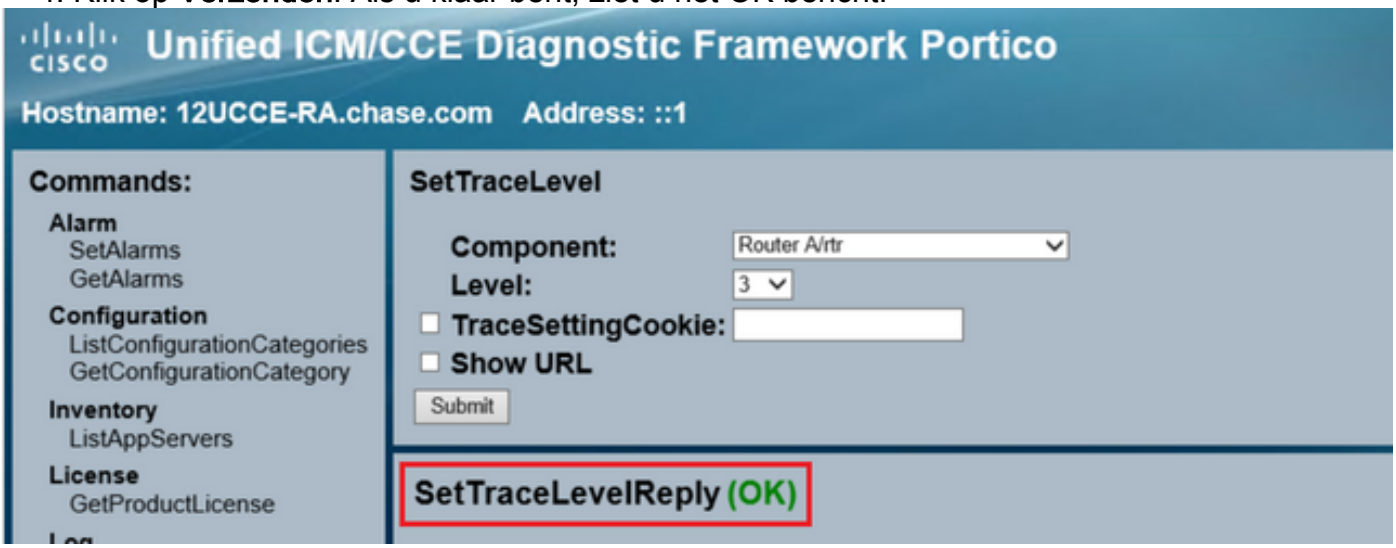
2. Navigeer in het gedeelte Opdrachten naar **Overtrekken** en selecteer **Overtrek instellen.**



3. Selecteer in het venster **SetTraceLevel** het onderdeel en het niveau.



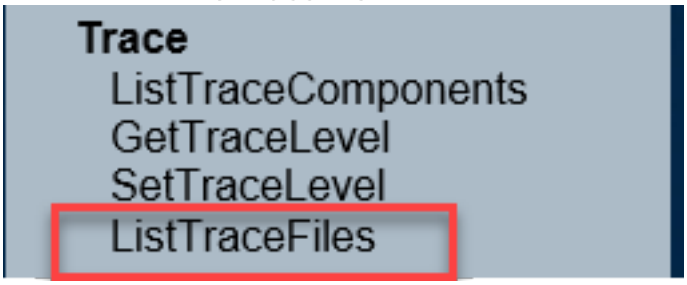
4. Klik op **Verzenden**. Als u klaar bent, ziet u het OK bericht.



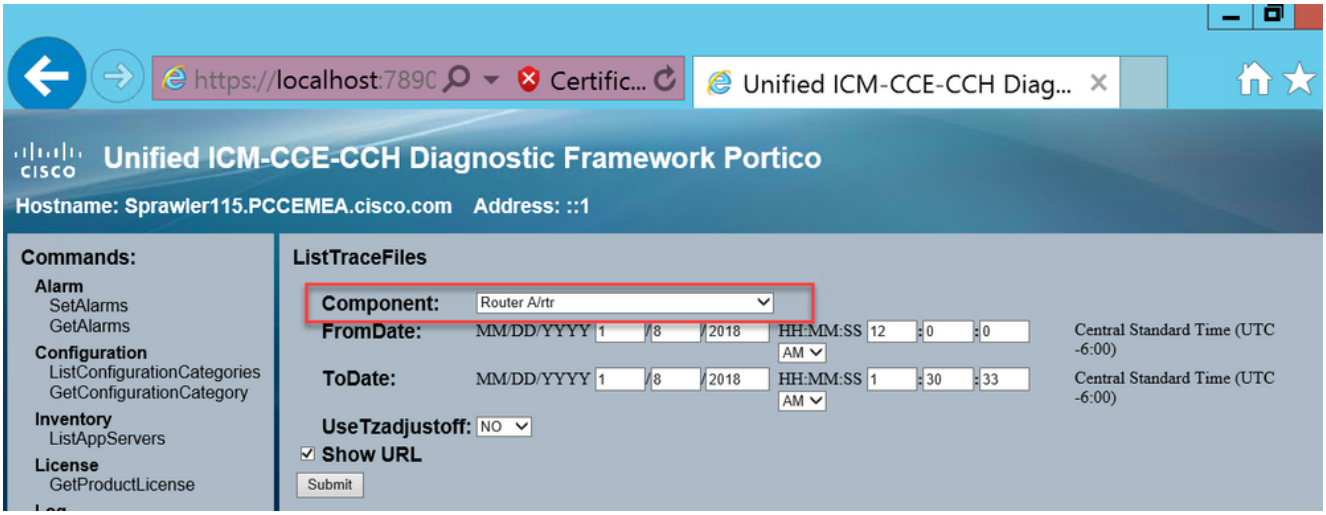
Waarschuwing: Stel het niveau van de sporen in op niveau 3 terwijl u probeert het probleem te reproduceren. Nadat het probleem wordt gereproduceerd, stelt u het standaardniveau voor overtrekken in. Gebruik speciaal voorzichtig wanneer u de JTAPIGW-sporen instelt, aangezien niveau 2 en niveau 3 de Lage-niveau-sporen instellen en dit een impact kan hebben op de prestaties. Stel niveau 2 of niveau 3 in in de JTAPIGW tijdens niet-productietijd of in een laboratoriumomgeving.

Logbestanden verzamelen

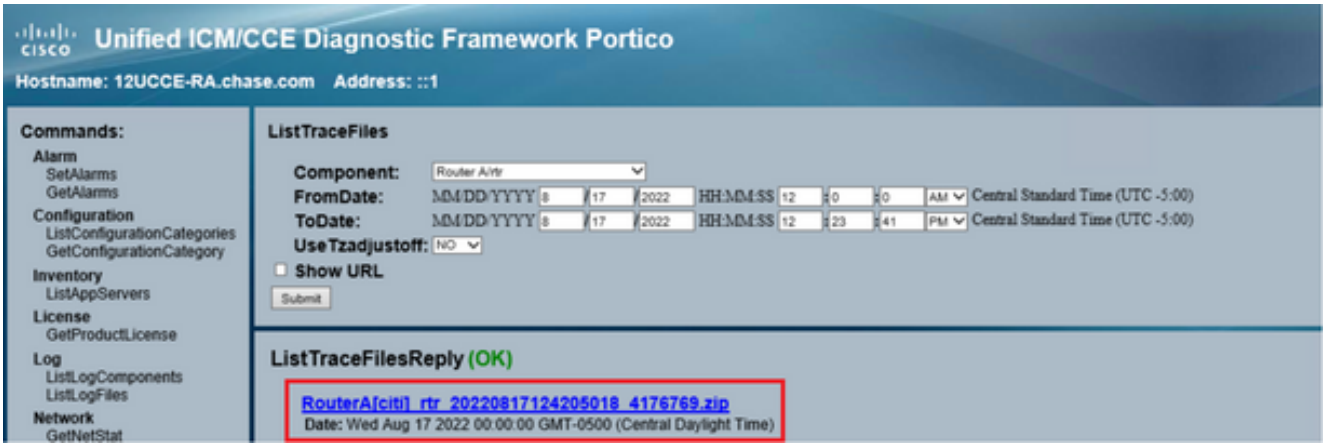
1. Van het Kenmerkende Portico van het Kader, op de sectie **Opdrachten**, navigeer aan **Spoor** en selecteer **ListTraceFile**.



2. Selecteer in het venster **ListTraceFile** de opties **Component**, **FromDate** en **ToDate**. Controleer het **vak URL tonen** en klik vervolgens op **Verzenden**.



3. Wanneer het verzoek is voltooid, ziet u het OK-bericht met de koppeling van het ZIP-logbestand.

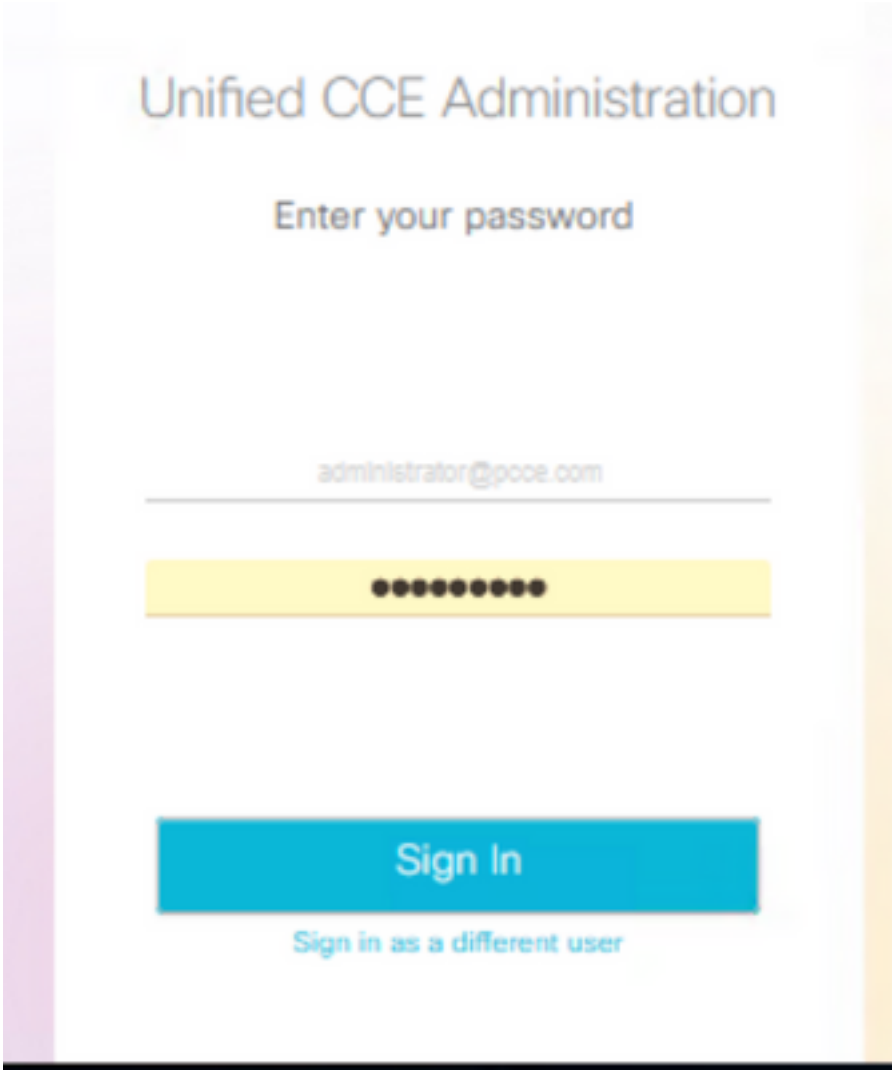


4. Klik op de koppeling ZIP-bestand en save het bestand op de door u gekozen locatie.

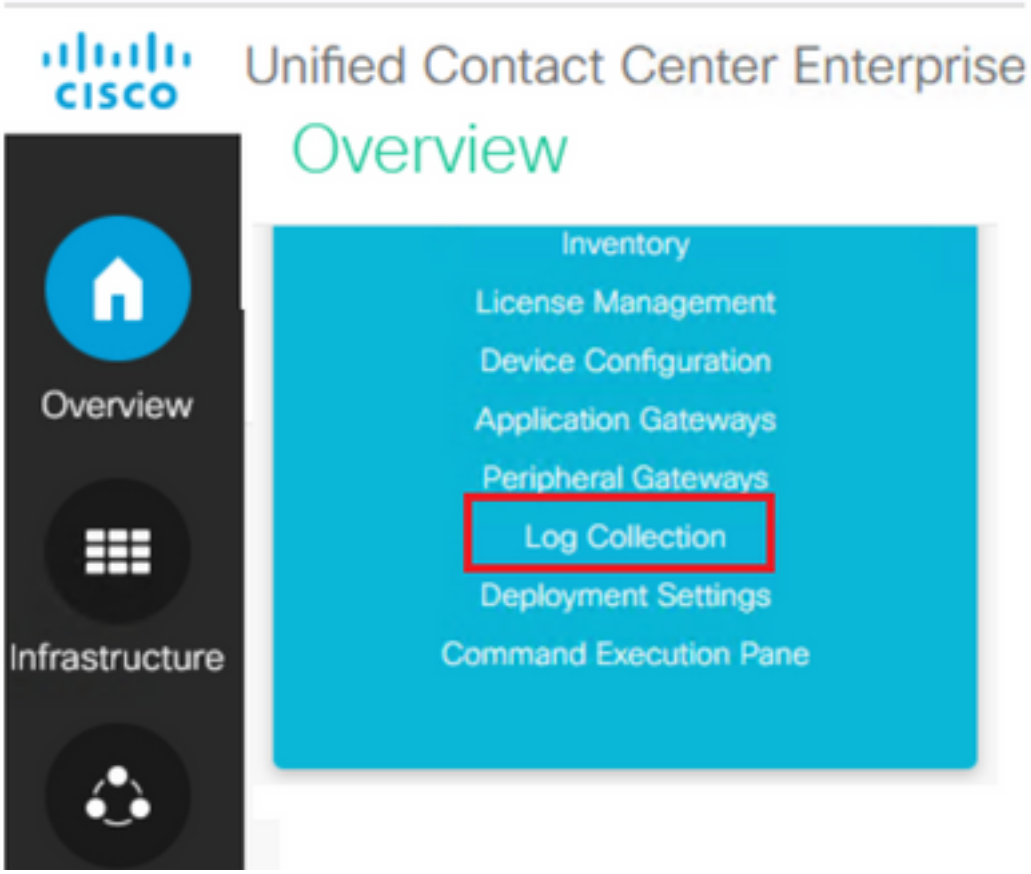
PCCE-logs overtrekken en verzamelen

PCCE heeft een eigen tool om overtrek niveaus in te stellen. Het is niet van toepassing op de UCS-omgeving waar Diagnostic Framework Portico of het systeem CLI de voorkeursmanieren zijn om logbestanden in te schakelen en te verzamelen.

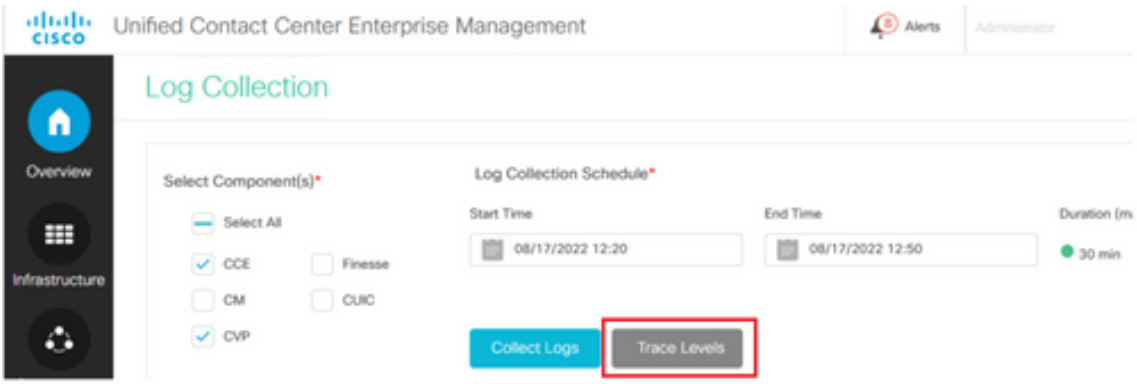
1. Open vanuit de PCE AW-server het Unified CCE Web Administration Tool en log in bij de Administrator-account.



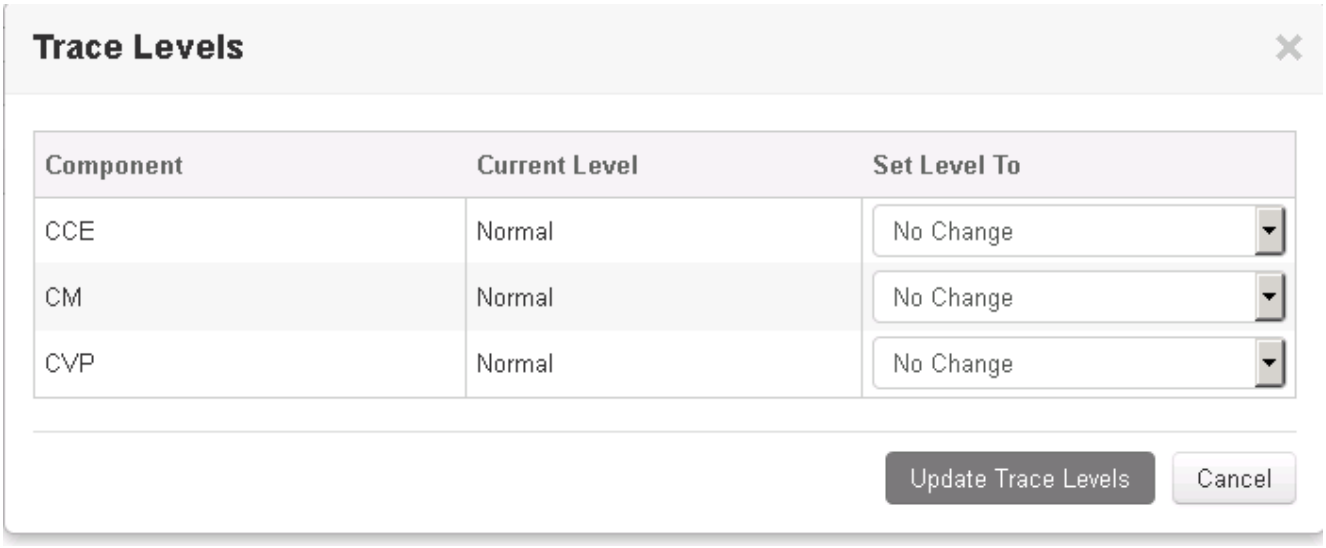
2. Blader naar **Overzicht->Infrastructuurinstellingen->Log** in om de pagina Log Collection te openen.



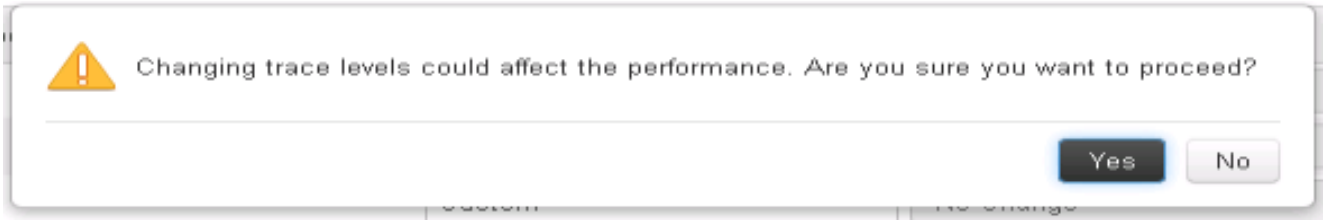
3. Klik op de pagina Logbestanden verzamelen op **Niveaus overtrekken** waarmee het dialoogvenster **Niveaus overtrekken** wordt geopend.



4. Stel het overtrek-niveau in op **Gedetailleerd** op CCE en laat het als **Geen wijziging** staan voor CM en CVP, en klik vervolgens op **Overtrek-niveaus bijwerken.**



5. Klik op **Ja** om de waarschuwing te bevestigen.



6. Nadat het probleem is gereproduceerd, opent u de **Unified CCE-beheerder** en gaat u terug naar **System > Logbestanden verzamelen.**
7. Selecteer **CCE** en **CVP** in het deelvenster Componenten.
8. Selecteer de gewenste tijd voor logverzameling (de standaardinstelling is de laatste 30 minuten).
9. Klik op **Logbestanden verzamelen** en **op Ja** om de waarschuwing te bevestigen. De logboekinzameling begint. Wacht een paar minuten voordat het klaar is.

10. Als u klaar bent, klikt u op de knop **Downloaden** in de kolom **Acties** om een zipped bestand met alle inlogbestanden te downloaden. Save het **zip**-bestand op elke gewenste locatie.

Vaststellen van tracering en verzamelen van CUIC/Live Data/IDS-logbestanden

Logboeken met SSH downloaden

1. Log in op de SSH Command Line (CLI) van CUIC, LD en IDS.

2. Voer de opdracht uit om CUIC-gerelateerde logbestanden te verzamelen.

```
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. Voer de opdracht uit om LD-gerelateerde logs te verzamelen.

file get activelog livedata/logs/*.*

4. Voer de opdracht uit om met ID's verband houdende logbestanden te verzamelen.

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

5. Deze logbestanden worden opgeslagen op het SFTP-serverpad: <IP-adres>\<date time stamp>\active_nnn.tgz, waar nnn tijdstempel in lang formaat is.

Logs downloaden met RTMT

1. Download RTMT van OAMP pagina. Log in op https://<HOST ADDRESS>/oamp waar HOST ADDRESS het IP-adres van de server is.

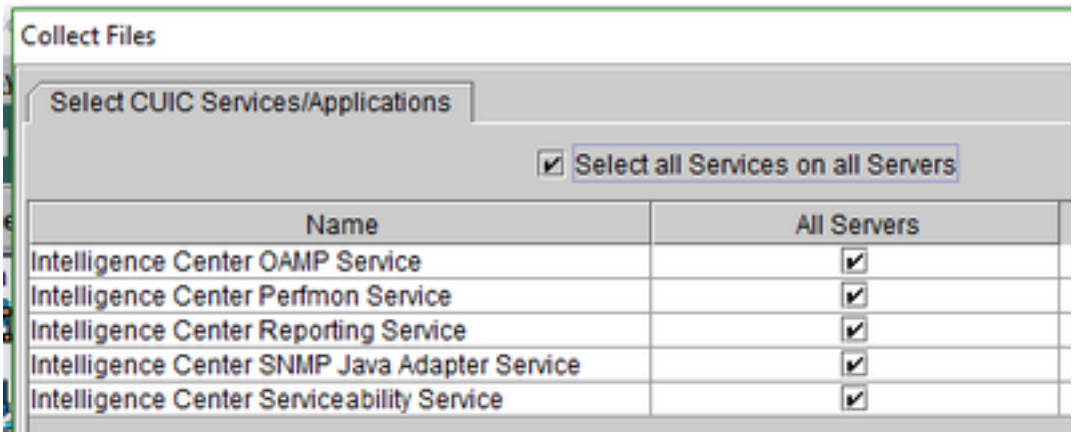
2. Ga naar **Tools > RTMT plugin downloaden.** Download en installeer de plug-in.

3. Start RTMT en log in bij de server met beheerdersreferenties.

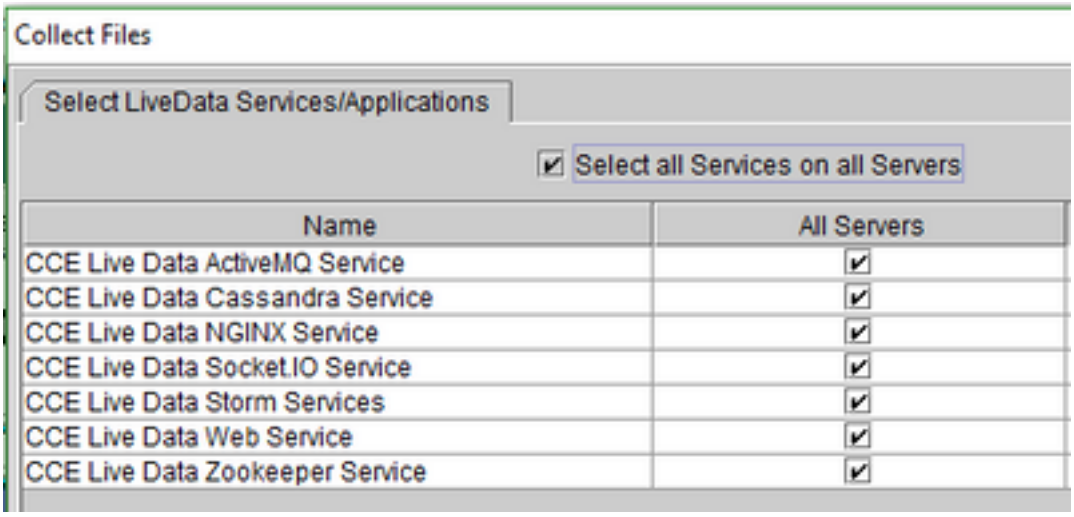
4. Dubbelklik op **Trace en Log Central** en dubbelklik op **Collect Files**.

5. U kunt deze tabbladen zien voor de specifieke services. U moet alle services/servers selecteren voor CUIC, LD en IDS.

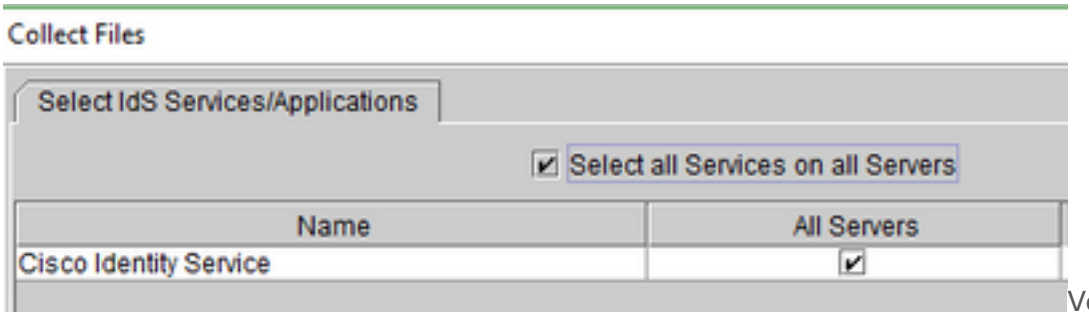
   voor CUIC:



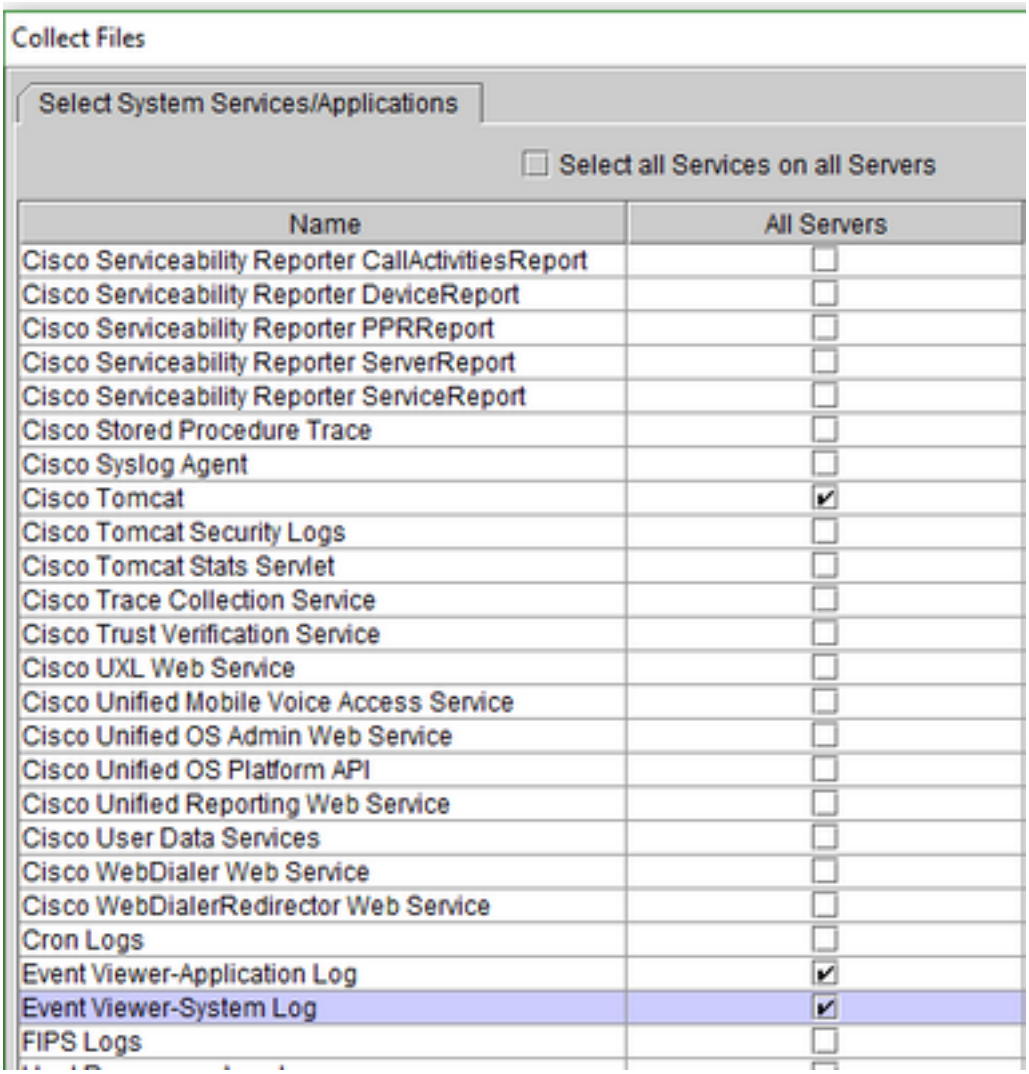
   Voor LD:



Voor IDS:

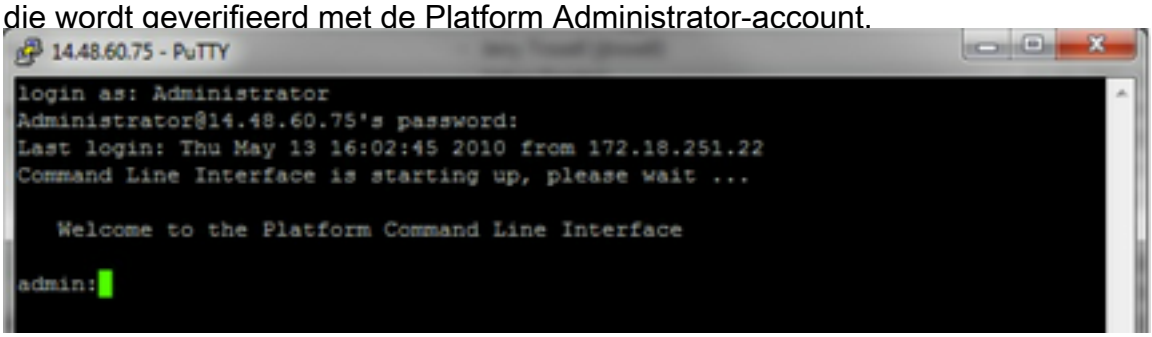


Voor platformdiensten is het over het algemeen een goed idee om de kijkerslogboeken van Tomcat en Event te selecteren:



6. Selecteer de **datum en tijd** samen met de doelmap om save de logbestanden.

Packet Capture op VoS (Finesse, CUIC, VVB)

1. Start de vastlegging Om de opname te starten, zet u een SSH-sessie op naar de VOS-server die wordt geverifieerd met de Platform Administrator-account.
2. 

1 bis. Opdrachtsyntaxis

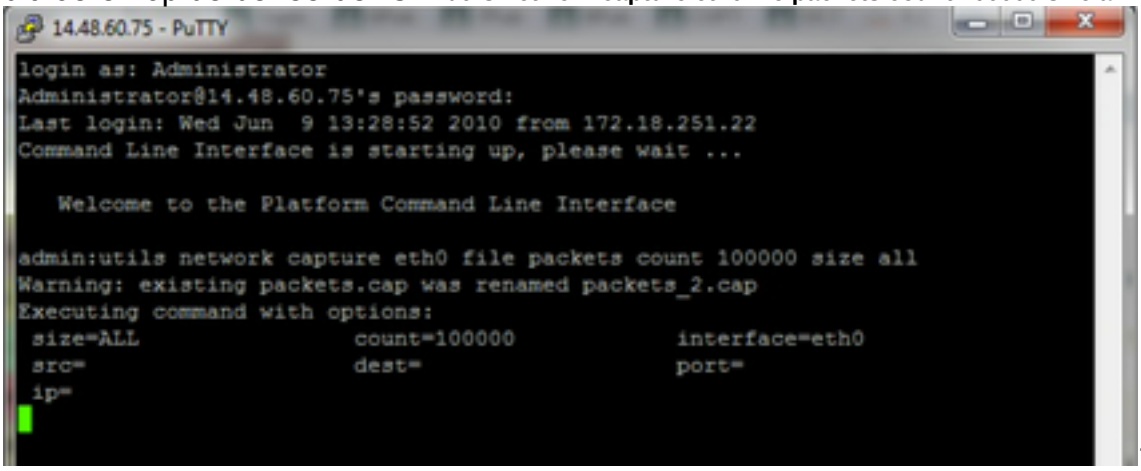
De opdracht is **utils network capture**en de syntaxis is als volgt:

```
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"
```

1 ter. Alle verkeer opnemen

Voor een typische opname, kan men ALLE pakketten van ALLE grootten van en aan ALLE adres in een opnamebestand verzamelen genoemd **packets.cap**. Om dit te doen gewoon uitvoeren op de beheerder CLI **utils network capture eth0 file packets count 100000 size all**

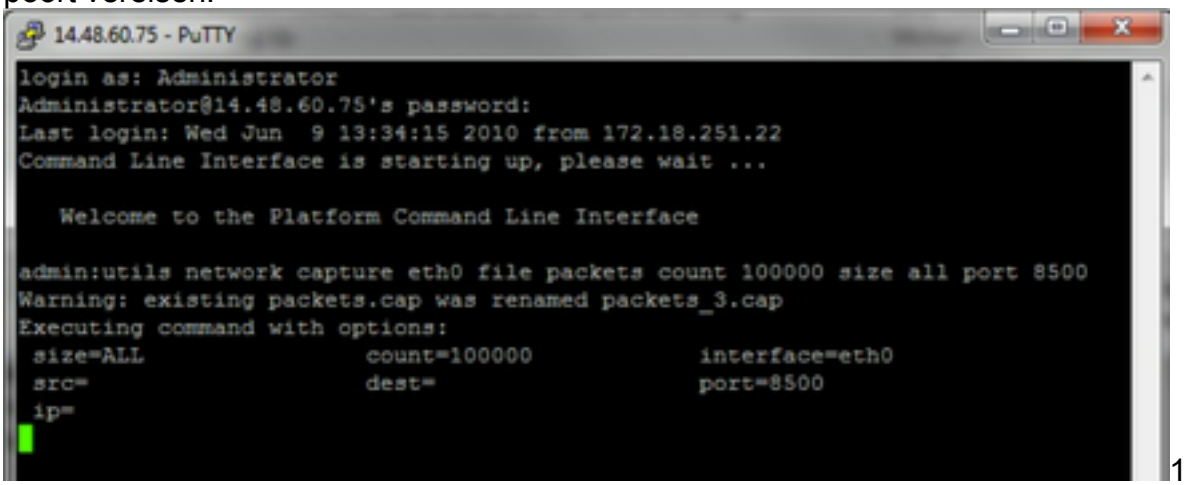


1 quater. Opname op basis van poortnummer

Om een communicatieprobleem met de Cluster Manager op te lossen, kan het handig zijn om de poortoptie te gebruiken om op basis van een specifieke poort op te nemen (8500).

Raadpleeg de handleiding voor TCP- en UDP-poortgebruik voor de toepasselijke versie van de betreffende component voor meer informatie over welke services communicatie op elke

poort vereisen.

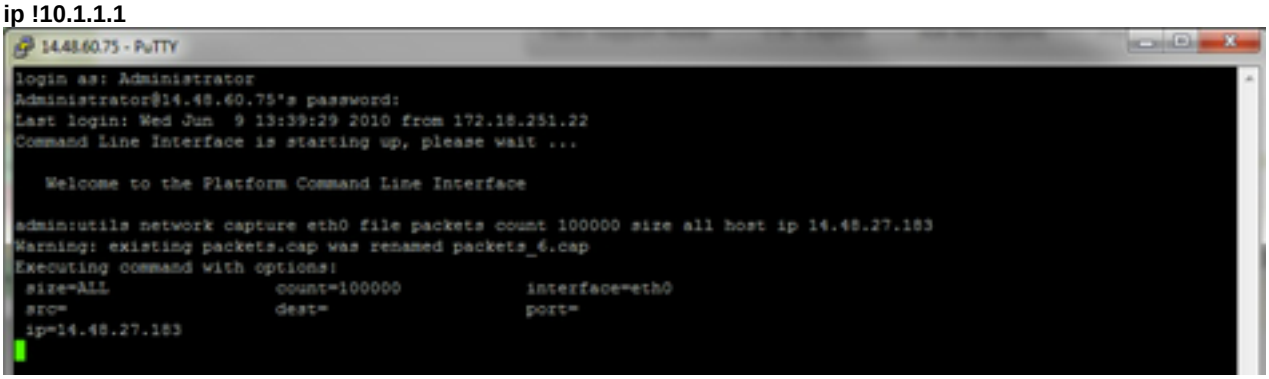


1

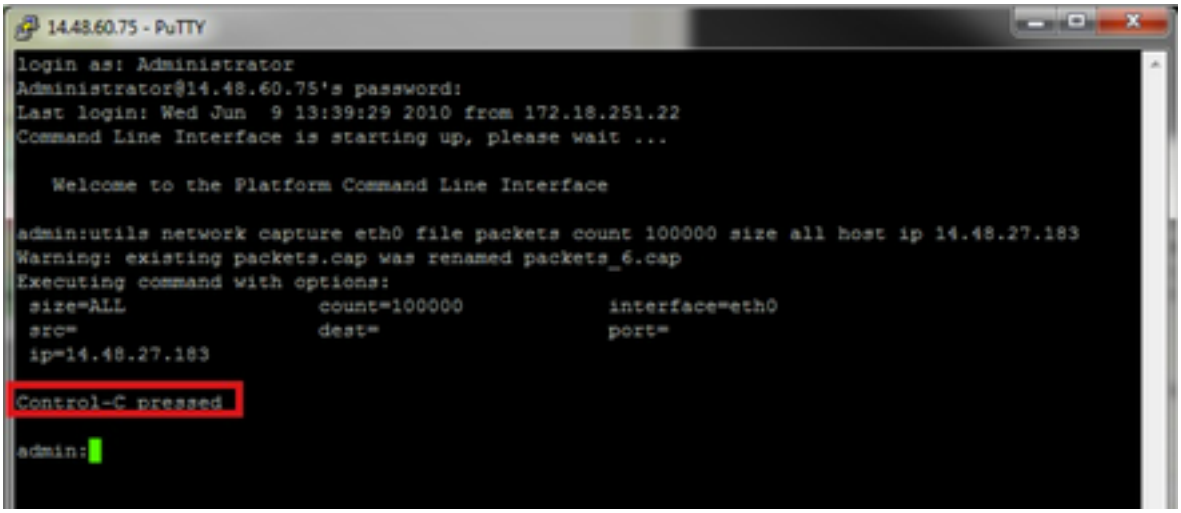
quinquies. Opname op basis van host

Om een probleem met VOS en een bepaalde host op te lossen, kan het nodig zijn om de 'host' optie te gebruiken om voor verkeer van en naar een bepaalde host te filteren.

Het kan ook noodzakelijk zijn om een bepaalde host uit te sluiten, in dit geval gebruik een "!" vóór het OT. Een voorbeeld hiervan is **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

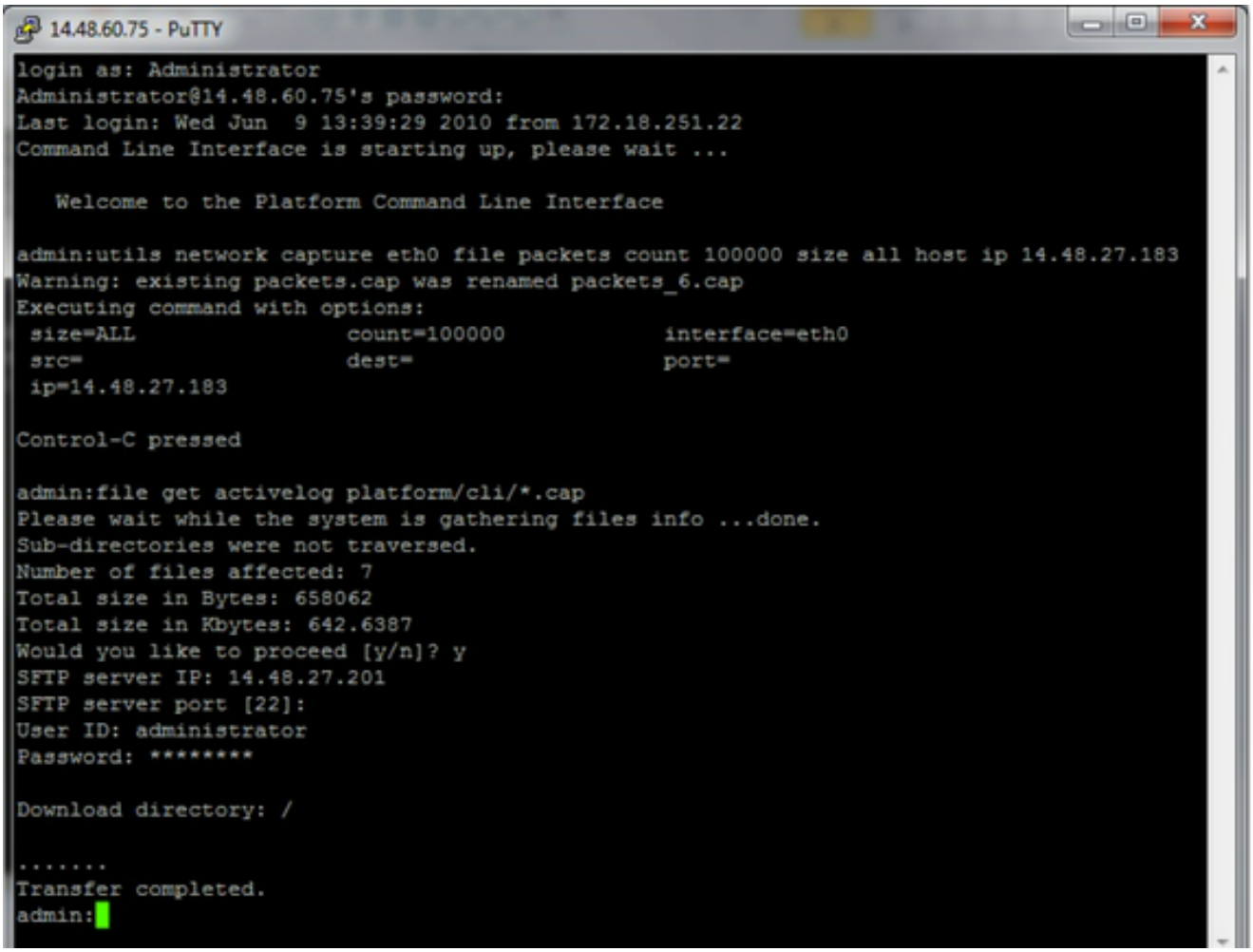


3. Het probleemsymptoom reproduceren Terwijl de opname is begonnen het probleemsymptoom of de toestand te reproduceren zodat de benodigde pakketten in de opname zijn opgenomen. Als het probleem intermitterend is, kan het nodig zijn om de opname voor een langere periode uit te voeren. Als de opname eindigt, is dit omdat de buffer gevuld is, de opname opnieuw opstarten en de vorige opname automatisch wordt hernoemd zodat de vorige opname niet verloren gaat. Als een opname voor een langere periode nodig is, gebruikt u een monitorsessie op een switch om op netwerkniveau op te nemen.
4. Stop de vastlegging Om het opnemen te stoppen, houdt u de **Control-**toets ingedrukt en drukt u op **C** op het toetsenbord. Dit veroorzaakt het opnameproces om te beëindigen en er worden geen nieuwe pakketten toegevoegd aan de opnamedump.
5.



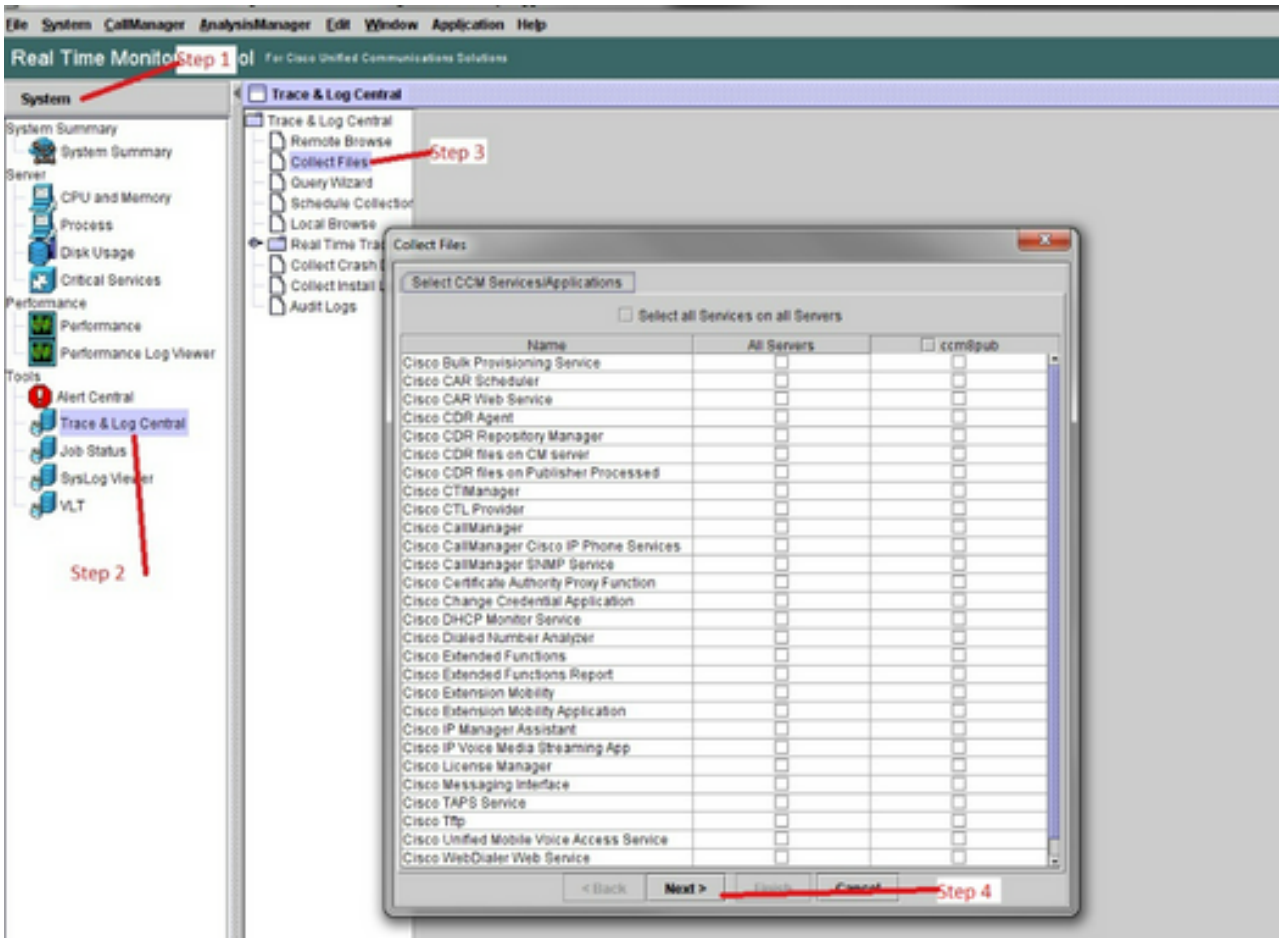
Zodra dit is voltooid, wordt een opnamebestand opgeslagen op de server op de locatie 'activelog platform/cli/'

6. Verzamel de opname van de server
   De opnamebestanden worden opgeslagen op een "activelog platform/cli/" locatie op de server. U kunt de bestanden via CLI overzetten naar een SFTP-server of naar de lokale pc met de RTMT. 4 bis. Opnamebestand via de CLI naar een SFTP-server overbrengen
   Gebruik de opdracht **file get activelog platform/cli/packets.cap** om het bestand packets.cap op de SFTP-server te verzamelen.
   Als alternatief voor het verzamelen van alle .cap bestanden die zijn opgeslagen op de server, gebruik 'file get activelog platform/cli/*.cap
   Tot slot vul de SFTP server IP/FQDN, poort, gebruikersnaam, wachtwoord en directory informatie in:

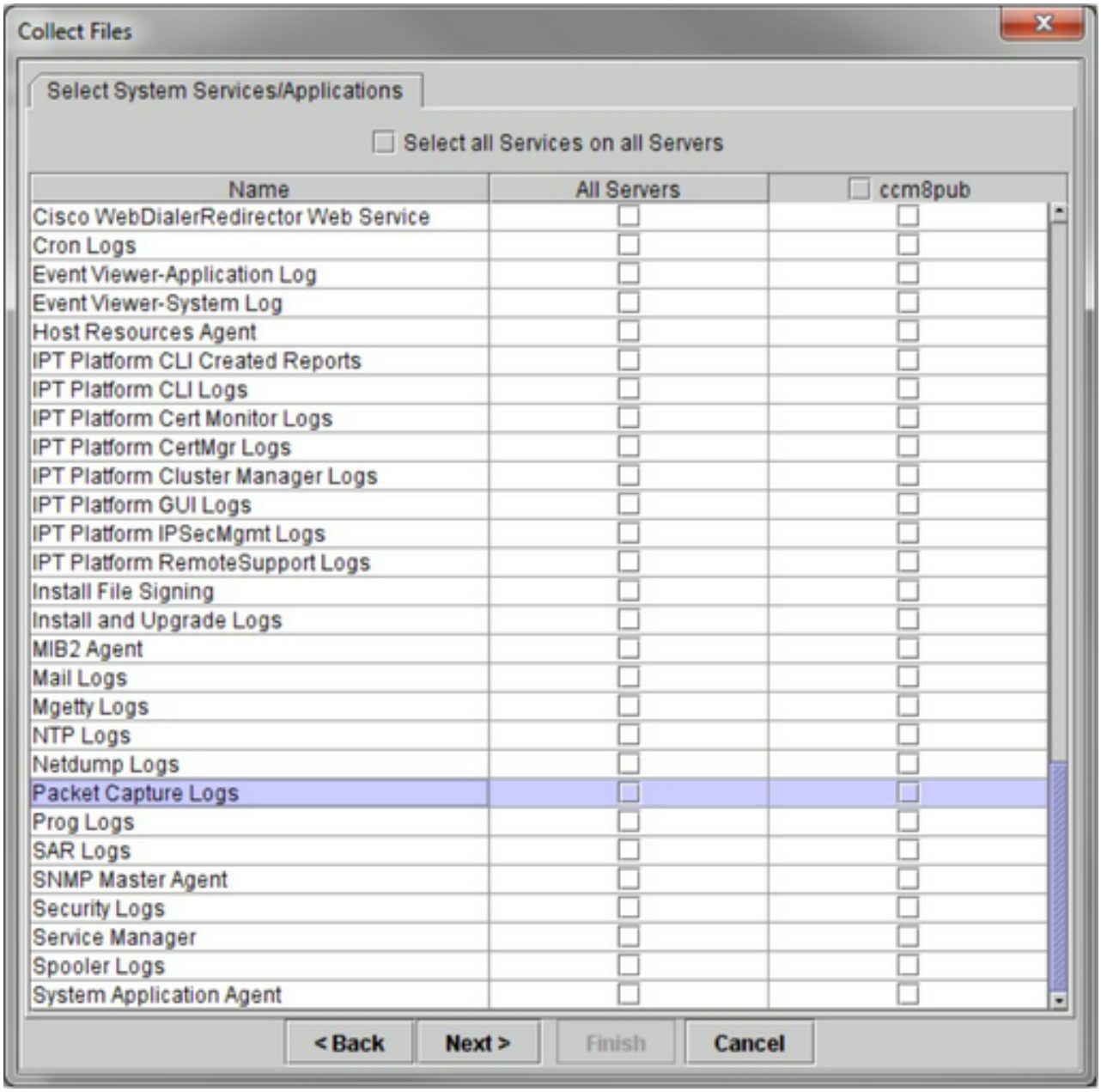


De CLI geeft aan of de bestandsoverdracht naar de SFTP-server is geslaagd of mislukt.

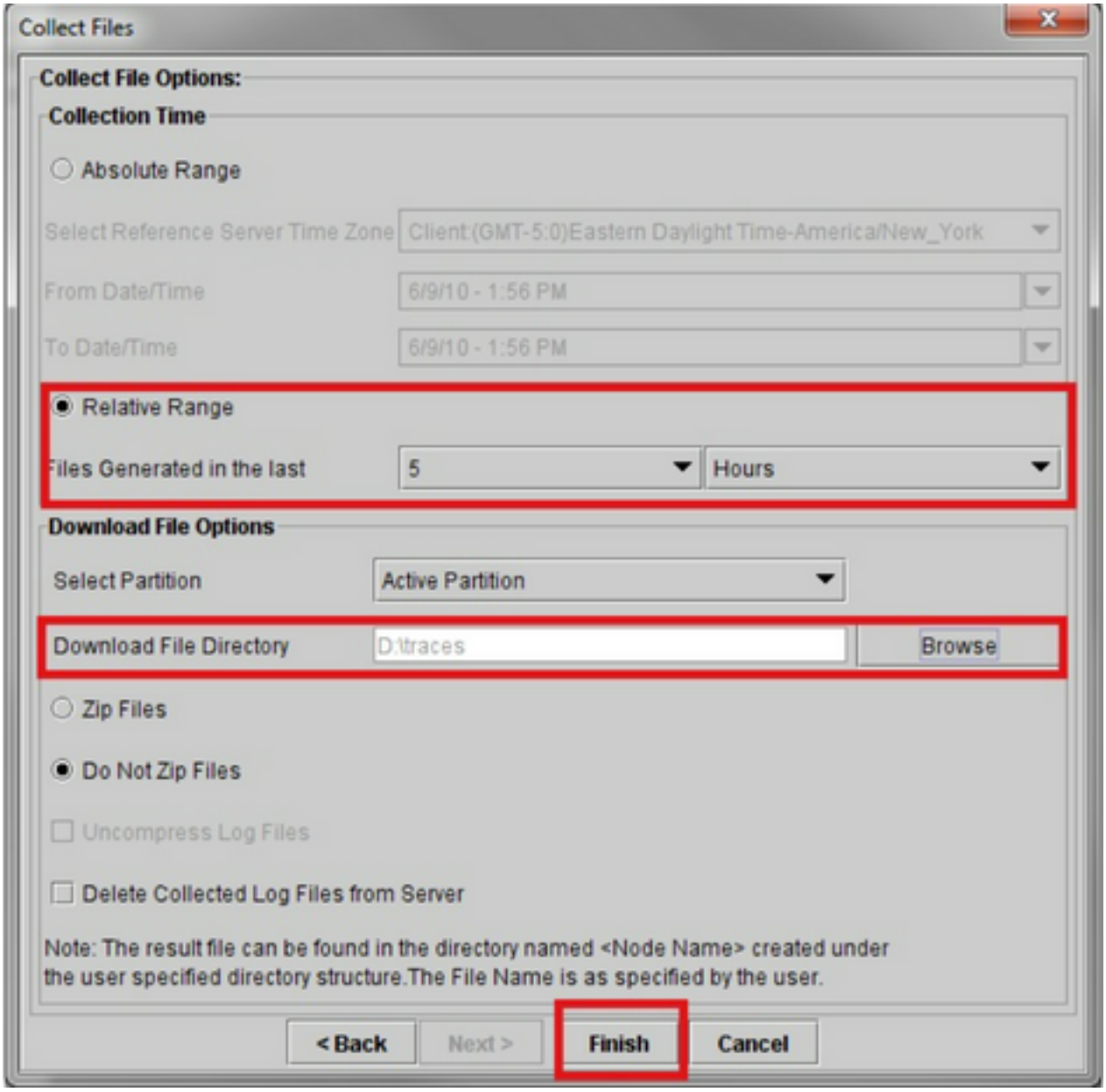
4 ter. Gebruik RTMT om een opnamebestand naar een lokale pc over te brengen.
Start de RTMT. Als het niet op de lokale pc is geïnstalleerd, installeert u de juiste versie van de VOS-beheerpagina en gaat u naar het menu **Toepassingen->Plugins**.
Klik op **System**, dan op **Trace & Log Central**, en dubbelklik op **Collect Files.** Klik op **Volgende** in het eerste menu.



In het tweede menu kies het selectievakje voor **Packet Capture Logs** op de server die de opname is uitgevoerd en klik vervolgens op **Volgende**.



Kies op het laatste scherm een tijdbereik wanneer de opname is uitgevoerd en kies een downloadmap op de lokale pc.



RTMT sluit dit venster en gaat u verder om het bestand te verzamelen en op te slaan op de lokale pc in de opgegeven locatie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.