Configurazione delle tracce e raccolta dei log UCCE

Sommario

Introduzione

In questo documento viene descritto come impostare le tracce in Cisco UCCE, Finesse, Customer Voice Portal (CVP), UCCE Outbound Dialer e Cisco Gateway.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

- Cisco Virtualized Voice Browser 11.5

In questo documento viene descritto come impostare le tracce in Cisco Unified Contact Center Enterprise (UCCE), Cisco Finesse, Cisco Customer Voice Portal (CVP), Cisco UCCE Outbound Dialer e Cisco Gateway.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Impostazioni traccia e Finesse raccolta log

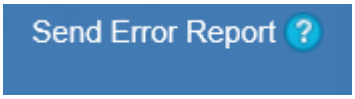
Finesse Client

Sono disponibili diverse opzioni per raccogliere i log del client Finesse.

Opzione 1: raccogliere i log dei client con Invia segnalazione errori.

Passaggio 1. Accedere a un agente.

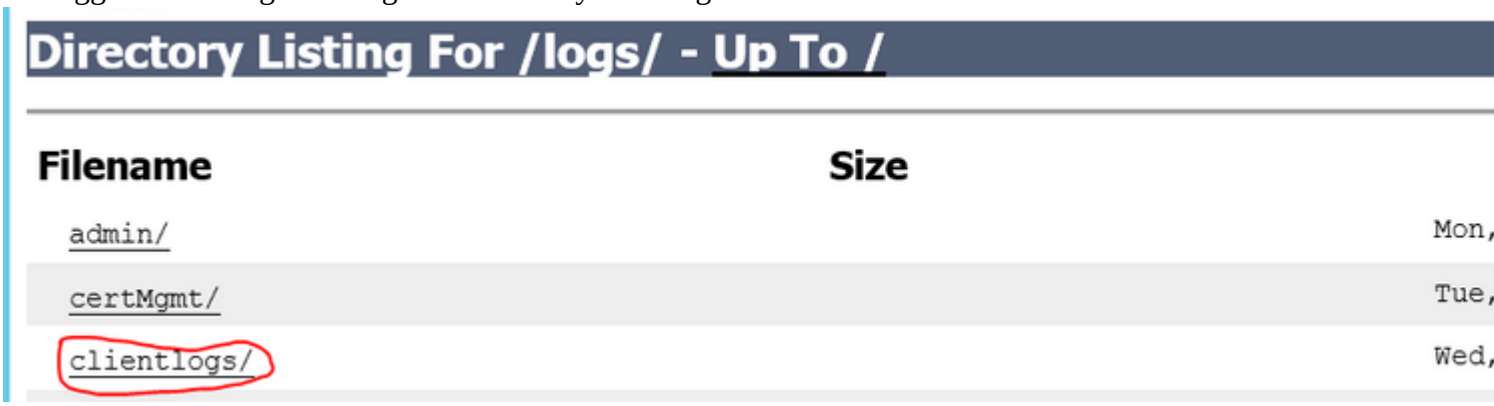
Passaggio 2. Se si verificano problemi durante una chiamata o un evento multimediale, indicare all'agente di fare clic sul collegamento Invia segnalazione errori nell'angolo inferiore destro del desktop di finesse.



Passaggio 3. L'agente visualizza il messaggio Log inviati correttamente.

Passaggio 4. I log del client vengono inviati al server Finesse. Passare a https://x.x.x.x/finesse/logs e accedere con un account di amministrazione.

Passaggio 5. Raccogliere i log nella directory clientlogs/.

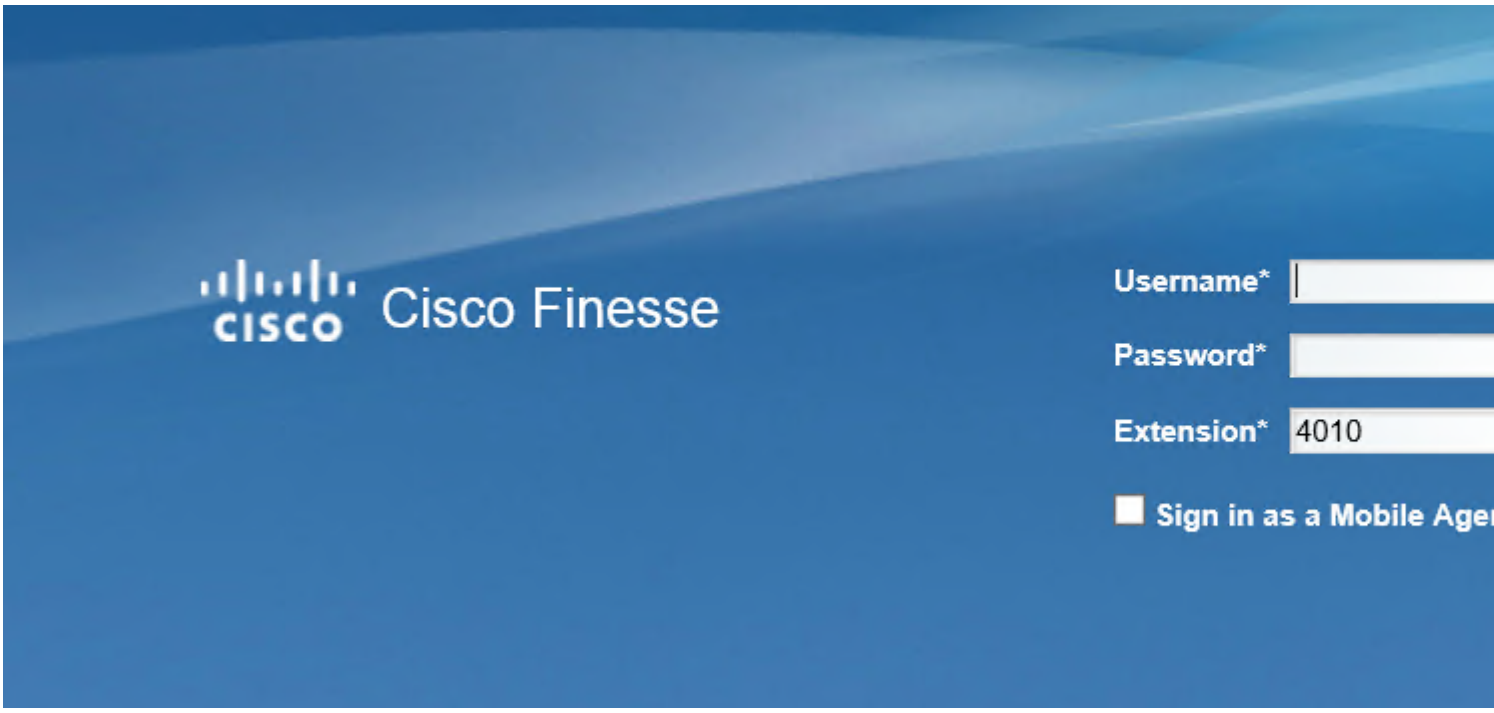


Opzione 2: Impostare la registrazione permanente

Passaggio 1. Passare a https://x.x.x.x:8445/desktop/locallog.

Passaggio 2. Fare Clic Su Accedi Con Registrazione Persistente.

Passaggio 3. Viene visualizzata la pagina di accesso al desktop dell'agente Cisco Finesse. Accedere all'agente.



Passaggio 4. Tutta l'interazione desktop dell'agente viene registrata e inviata ai log di archiviazione locali. Per raccogliere i log, passare a https://x.x.x.x:8445/desktop/locallog e copiare il contenuto in un file di testo. Salvate il file per ulteriori analisi.

.

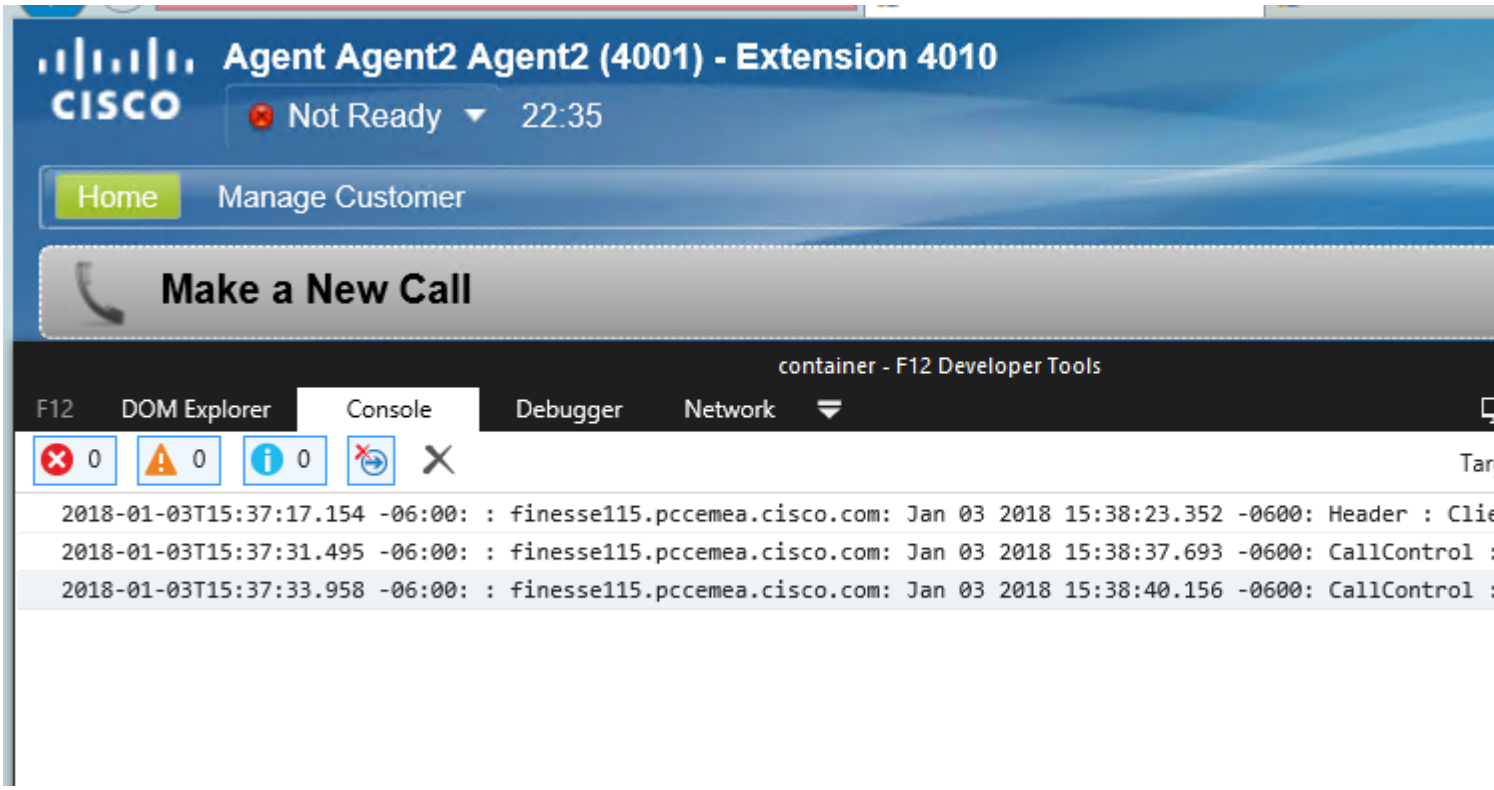
Nota: esiste un avvertimento relativo alla registrazione persistente. Dopo l'attivazione della registrazione permanente, le informazioni non vengono inviate ai log di archiviazione locali. ID bug Cisco CSCvf93030 - La registrazione persistente non consente di acquisire i log. Finesse 11.5(1) ES-2 in avanti. Per ulteriori informazioni su questa avvertenza e sui passaggi per risolverla, visitare il sito Web all'indirizzo

Opzione 3: Console del browser Web

Passaggio 1. Una volta effettuato l'accesso, premere F12 per aprire la console del browser.

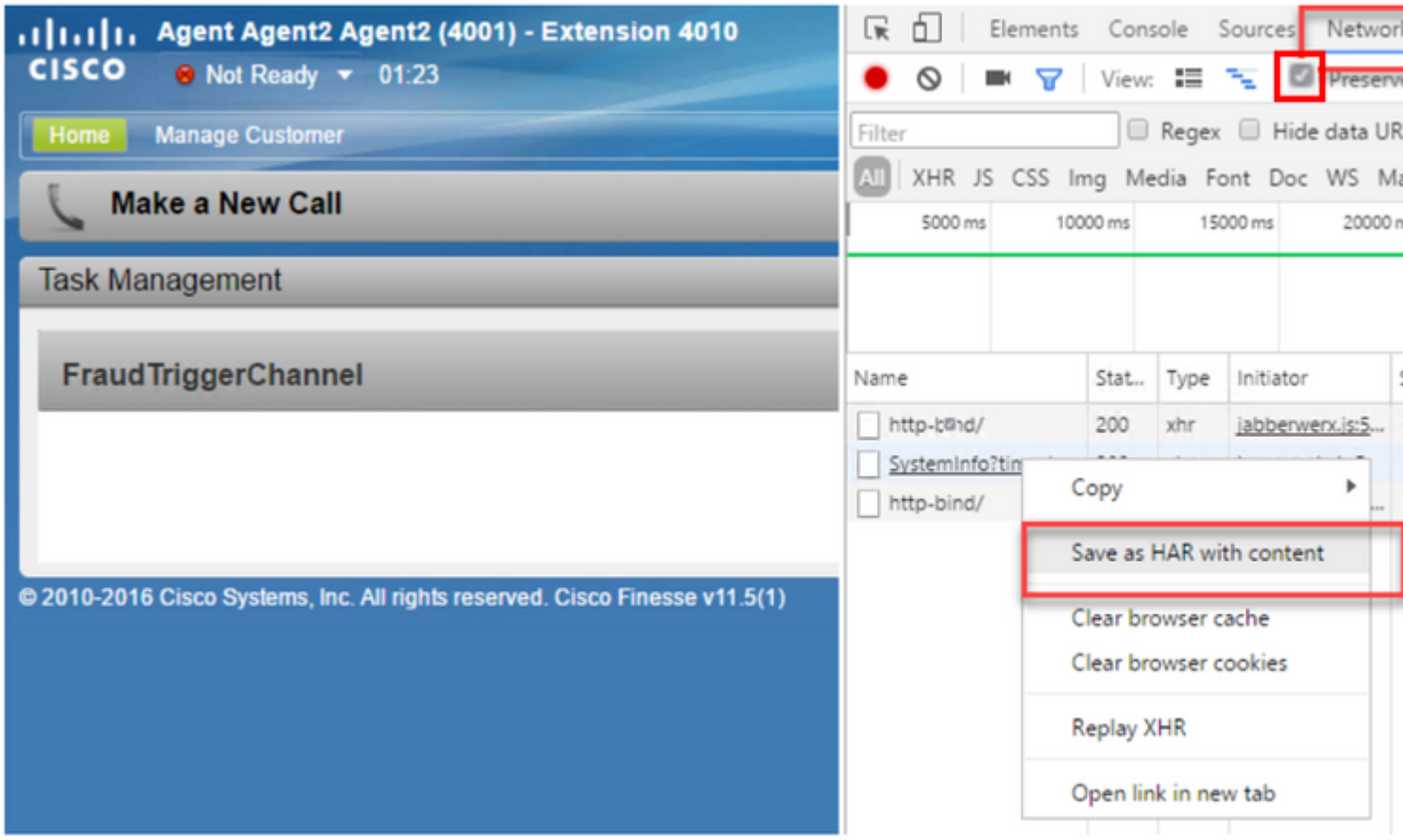
Passaggio 2. Selezionare la scheda Console.

Passaggio 3. Verificare la presenza di errori nella console del browser. Copiare il contenuto in un file di testo e salvarlo.



Passaggio 4. Selezionare la scheda Rete e selezionare l'opzione Mantieni registro.

Passaggio 5. Fare clic con il pulsante destro del mouse su uno degli eventi relativi ai nomi di rete e selezionare Salva come HAR con contenuto.



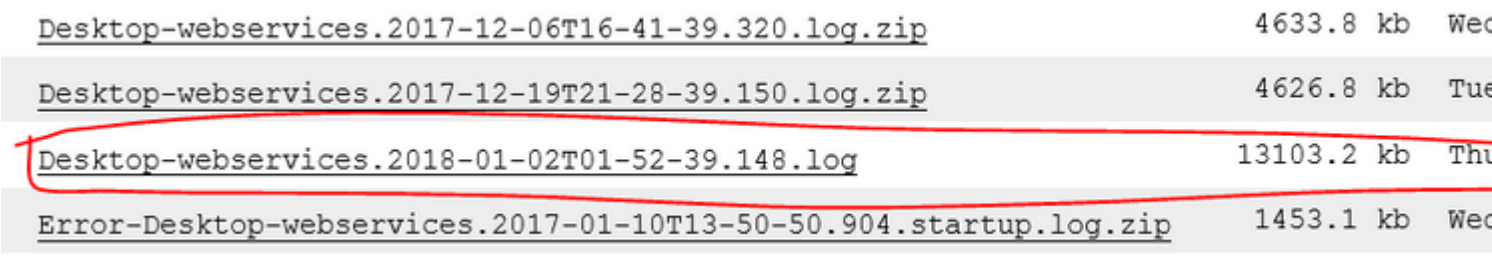
Finesse Server

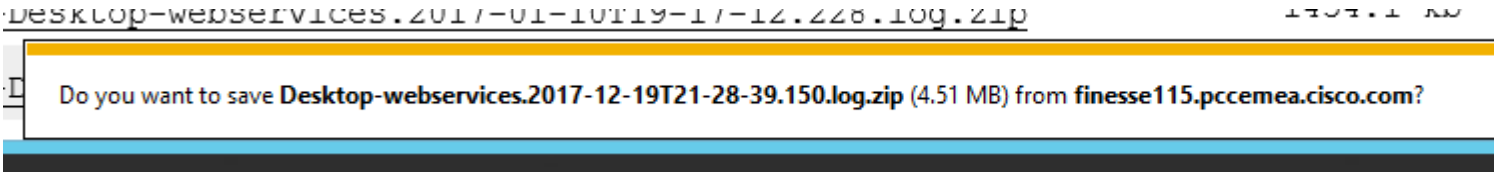
Opzione 1: Tramite interfaccia utente - Servizi Web (richiesti) e registri aggiuntivi

Passaggio 1. Passare a https://x.x.x.x/finesse/logs e accedere con l'account di amministrazione.

Passaggio 2. Espandere la directory webservices/

Passaggio 3. Raccoglie gli ultimi log del servizio Web. Selezionare l'ultimo file di decompressione. Ad esempio, Desktop-Webservices.201X-.log.zip. Fare clic sul collegamento al file e verrà visualizzata l'opzione per il salvataggio del file.





Passaggio 4. Raccogliere gli altri registri necessari (a seconda dello scenario). Ad esempio, openfire per i problemi relativi al servizio di notifica, log del realm per i problemi di autenticazione e tomcatlogs per i problemi relativi alle API.

Nota: il metodo consigliato per raccogliere i log del server Cisco Finesse è tramite Secure Shell (SSH) e Secure File Transfer Protocol (SFTP). Questo metodo non consente solo di raccogliere i log dei servizi Web, ma anche tutti i log aggiuntivi come Fippa, openfire, Realm e Clientlogs.

Opzione 2: Tramite SSH e SFTP (Secure File Transfer Protocol) - Opzione consigliata

Passaggio 1. Accedere al server Finesse con Secure Shell (SSH).

Passaggio 2. Immettere questo comando per raccogliere i log necessari. I registri vengono compressi e hanno un tempo relativo di 2 ore. Viene richiesto di identificare il server SFTP in cui vengono caricati i log.

file get activelog desktop recurs compress reltime ore 2.

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

Passaggio 3. Questi registri sono memorizzati nel percorso del server SFTP: <indirizzo IP>\<data e ora>\active_nnn.tgz , dove nnn è l'indicatore orario in formato esteso.

Passaggio 4. Per raccogliere ulteriori log come tomcat, Context service, Servm e install logs, vedere la sezione Log Collection del manuale Cisco Finesse Administration Guide

Guida all'amministrazione di Cisco Finesse versione 11.5(1)

Nota: per ulteriori informazioni su SFTP per i file di trasferimento Finesse, consultate questo documento Configurazione di backup e aggiornamento Finesse con SFTP

Impostazioni di traccia e CVP e CVB raccolta log

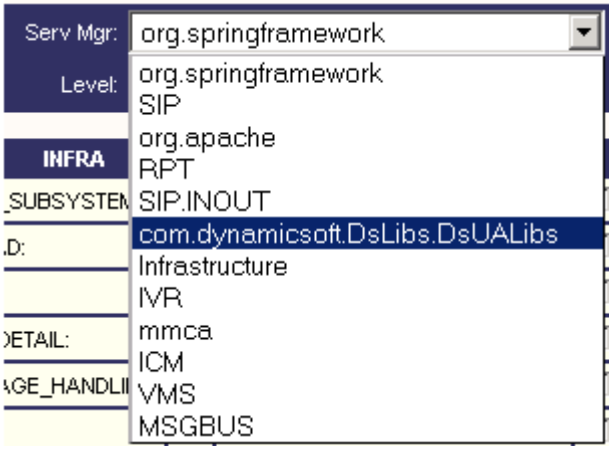
CVP Call Server

Il livello predefinito di tracce di CVP CallServer è sufficiente per risolvere la maggior parte dei casi. Tuttavia, quando si devono ottenere maggiori dettagli sui messaggi SIP (Session Initiation Protocol), è necessario impostare le tracce dello stack SIP sul livello DEBUG

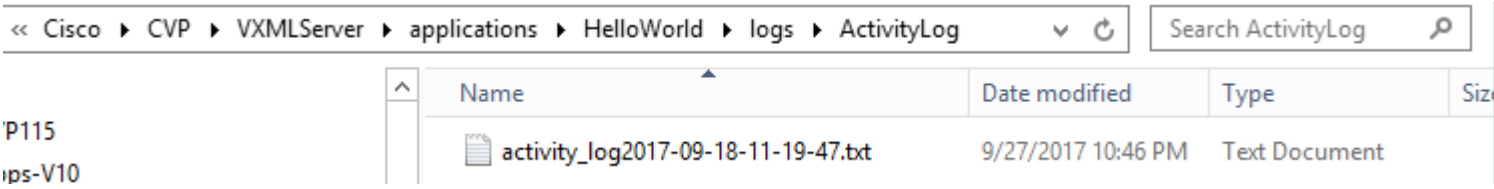
Passaggio 1. Accedere alla pagina Web CVP CallServer Diag all'URL http://cvp.cc.lab:8000/cvp/diag.

Nota: questa pagina fornisce buone informazioni su CVP CallServer ed è molto utile per risolvere alcuni scenari.

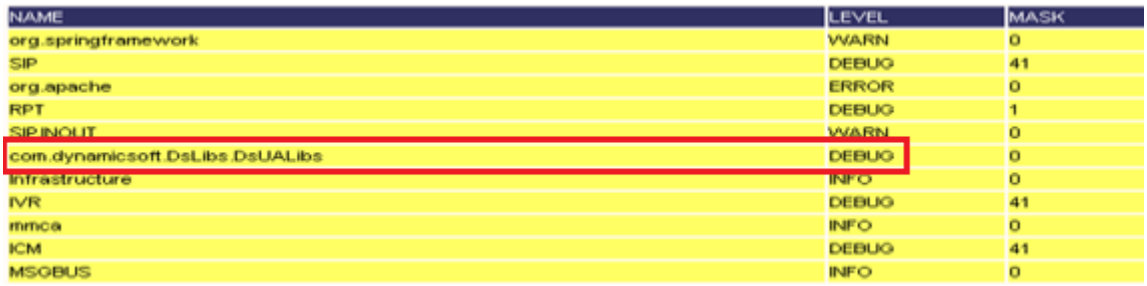
Passaggio 2. Selezionare com.dynamicsoft.DsLibs.DsUALibs dal Serv. Menu a discesa di Mgr nell'angolo superiore sinistro



Passaggio 3. Fare clic sul pulsante Imposta.

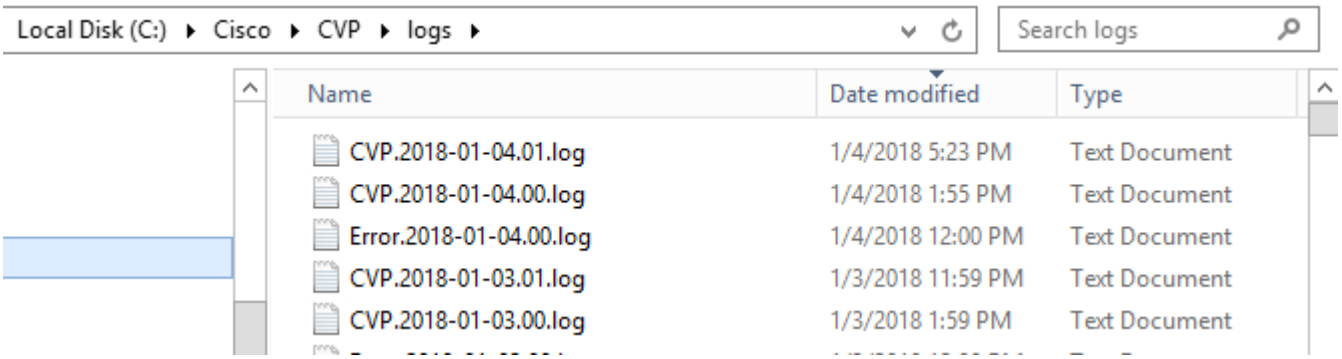


Passaggio 4. Scorrere verso il basso nella finestra di traccia per verificare che il livello delle tracce sia stato impostato correttamente. Queste sono le impostazioni di debug.



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

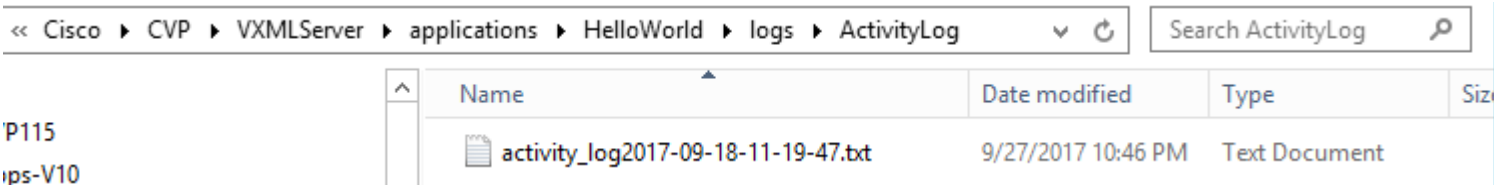
Passaggio 5. Quando si riproduce il problema, raccogliere i log da C:\Cisco\CVP\logs e selezionare il file di log CVP in base all'ora in cui si è verificato il problema.



Applicazione CVP Voice XML (VXML)

In casi molto rari è necessario aumentare il livello delle tracce delle applicazioni server VXML. D'altra parte, si consiglia di non aumentarlo a meno che non sia richiesto da un tecnico Cisco.

Per raccogliere i log dell'applicazione del server VXML, passare alla directory dell'applicazione specifica nel server VXML, ad esempio: C:\Cisco\CVP\VXMLServer\applications\{nome dell'applicazione}\logs\ActivityLog\ e raccogliere i log attività



OAMP (CVP Operations and Administration Management Portal)

Nella maggior parte dei casi, il livello predefinito delle tracce di OAMP e ORM è sufficiente per determinare la causa principale del problema. Tuttavia, se è necessario aumentare il livello delle tracce, eseguire questa azione nei passaggi seguenti:

Passaggio 1. Eseguire il backup di %CVP_HOME%\conf\oamp.properties.

Passaggio 2. Modifica %CVP_HOME%\conf\oamp.properties

omgr.traceMask=-1

omgr.logLevel=Debug
org.hibernate.logLevel=Debug
org.apache.logLevel=ERRORE
net.sf.ehcache.logLevel=ERRORE

Passaggio 3. Riavviare OPSConsoleServer.

Informazioni sui livelli di traccia

Livello traccia	Descrizione	Livello log	Maschera di traccia
0	Installazione predefinita del prodotto. Nessun impatto sulle prestazioni o impatto minimo.	INFORMAZIONI	Nessuna
1	Messaggi di analisi meno dettagliati con un impatto ridotto sulle prestazioni.	DEBUG	CONFIGURAZIONE_PERIFERICA + DATABASE_MODIFY + MANAGEMENT=0x01011000
2	Messaggi di analisi dettagliati con un impatto medio sulle prestazioni.	DEBUG	CONFIGURAZIONE_PERIFERICA + SYSLVL_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x05011000
3	Messaggio di traccia dettagliato con impatto sulle prestazioni elevato.	DEBUG	CONFIGURAZIONE_PERIFERICA + SYSLVL_CONFIGURATION + OPERAZIONI_AUSILIARIE + DATABASE_MODIFY + MANAGEMENT=0x05111000
4	Messaggio di analisi dettagliato con impatto molto elevato sulle prestazioni.	DEBUG	VARIE + CONFIGURAZIONE_PERIFERICA + ST_CONFIGURAZIONE + SYSLVL_CONFIGURATION +

Livello traccia	Descrizione	Livello log	Maschera di traccia
			OPERAZIONI_AUSILIARIE + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + SELEZIONA_DATABASE + DATABASE_PO_INFO + GESTIONE E TRACE_METHOD + TRACE_PARAM=0x17371000
5	Messaggio di traccia più dettagliato.	DEBUG	VARIE + CONFIGURAZIONE_PERIFERICA + ST_CONFIGURAZIONE + SYSLVL_CONFIGURATION + OPERAZIONI_AUSILIARIE + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + SELEZIONA_DATABASE + DATABASE_PO_INFO + GESTIONE E TRACE_METHOD + TRACE_PARAM=0x17371006

Cisco Virtualized Voice Browser (CVB)

In CVB, un file di traccia è un file di log che registra l'attività dei sottosistemi e dei passaggi del componente Cisco VB.

Cisco VB ha due componenti principali:

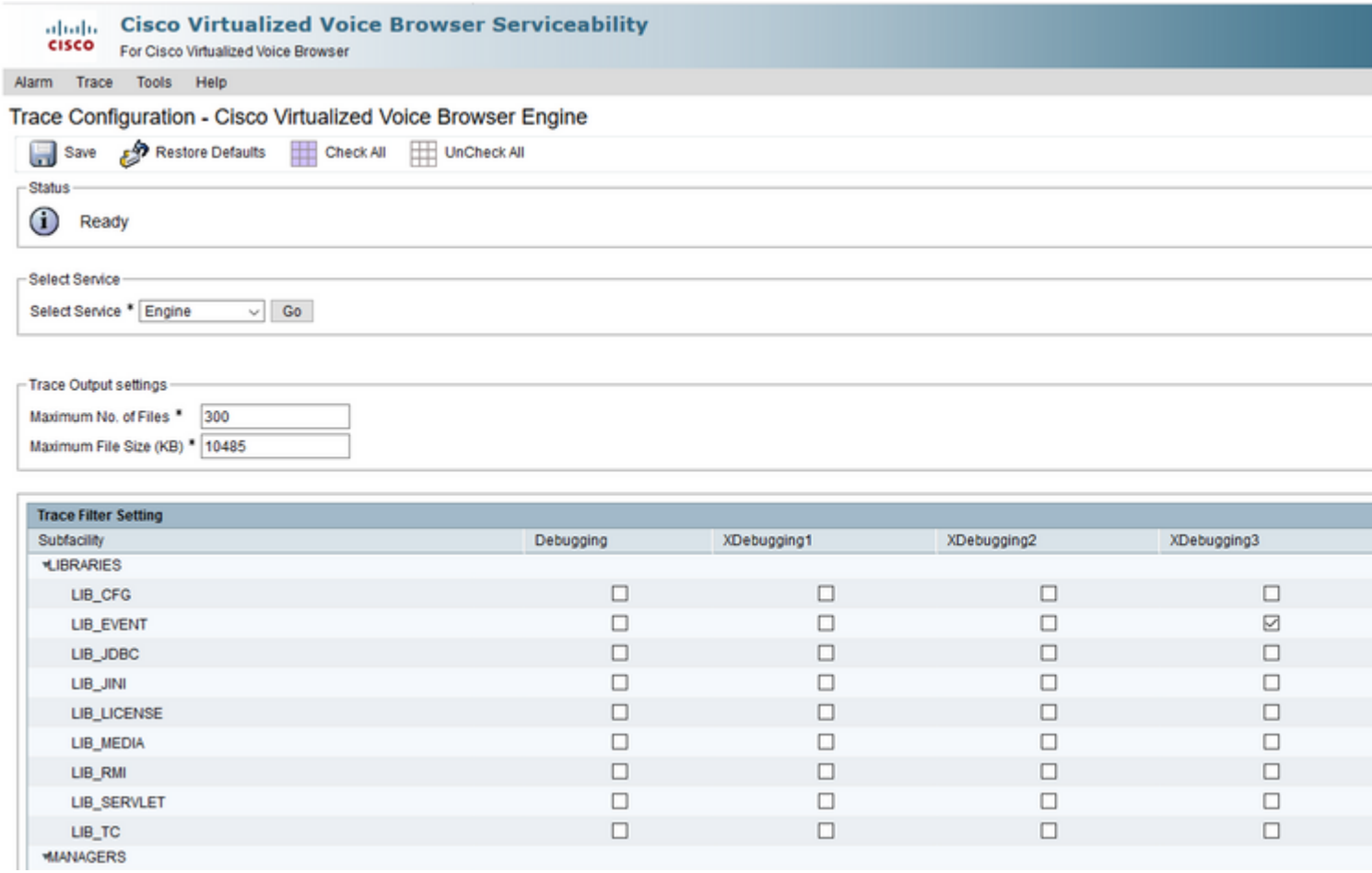
- Tracce "Administration" di Cisco VB definite come log MADM
- Tracce Cisco VB "Engine" denominate registri MIVR

È possibile specificare i componenti per i quali si desidera raccogliere informazioni e il livello di informazioni che si desidera raccogliere.

I livelli di log si estendono da:

Debug - Dettagli di flusso di base per

XDebugging 5 - Livello dettagliato con analisi dello stack



Avviso: Xdebugging5 non deve essere abilitato nel sistema di produzione caricato

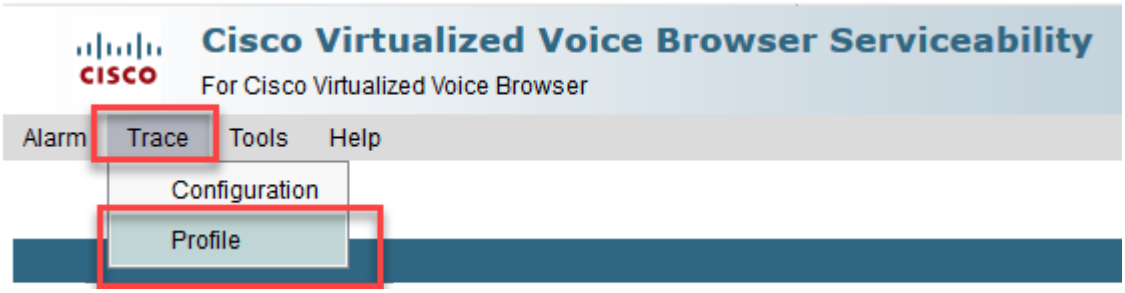
I log più comuni che è necessario raccogliere sono il motore. Il livello predefinito delle tracce per le tracce del motore CVB è sufficiente per risolvere la maggior parte dei problemi. Tuttavia, se è necessario modificare il livello delle tracce per uno scenario specifico, Cisco consiglia di utilizzare i profili di registro del sistema predefiniti

Profili registro di sistema	
Nome	Scenario in cui è necessario attivare il profilo
VVBpredefinito	I registri generici sono abilitati.
AppAdminVB	Per problemi relativi all'amministrazione Web tramite AppAdmin, Cisco VB Serviceability e altre pagine Web.
MediaVB	Per problemi relativi alla configurazione o alla trasmissione dei supporti.
VoiceBrowser VB	Per problemi relativi alla gestione delle chiamate.

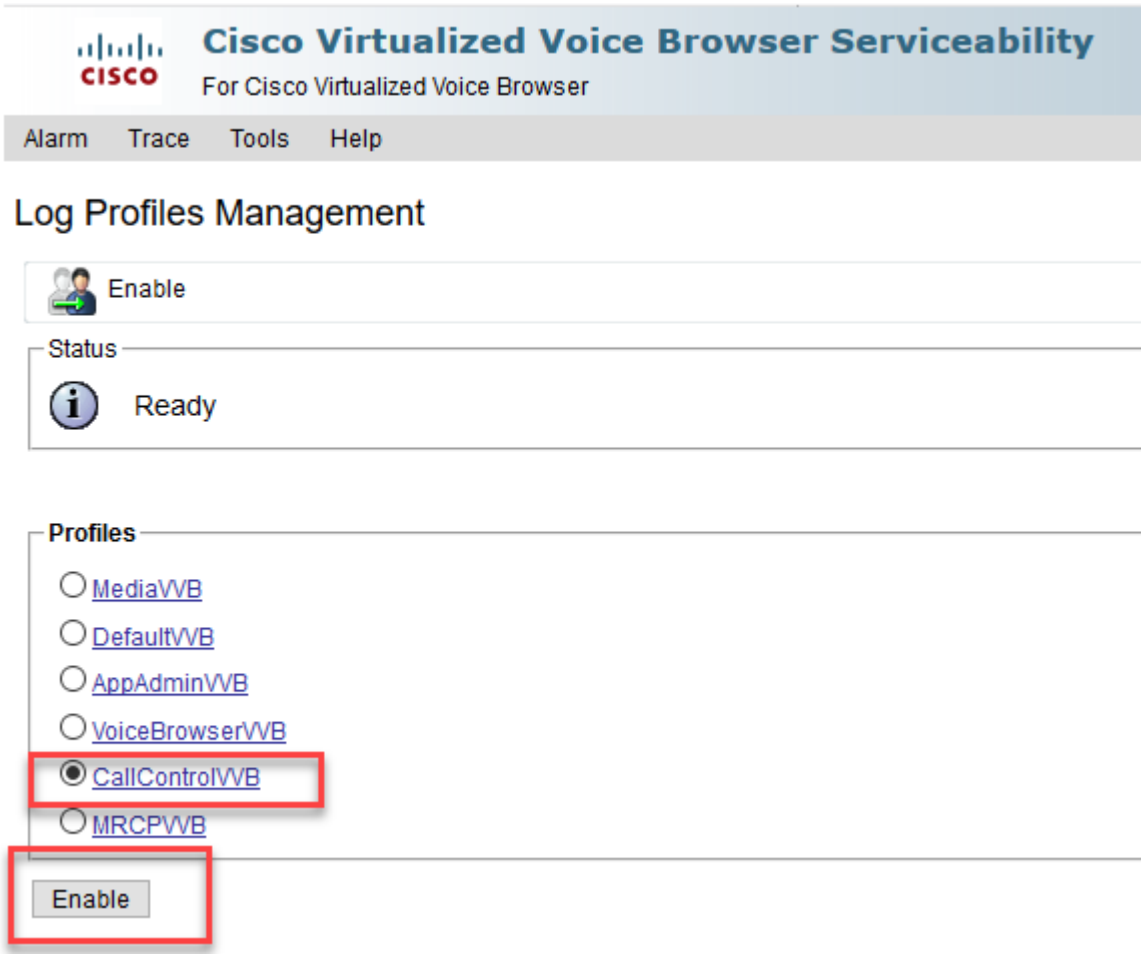
MRCPVB	Per problemi con ASR/TTS con interazione Cisco VB.
CallControlVB	Per i problemi relativi alla segnalazione SIP, vengono pubblicati nel registro.

Passaggio 1. Aprire la pagina principale di CVB (https://X.X.X.X/uccxservice/main.htm), passare alla pagina Cisco VB Serviceability e accedere con l'account di amministrazione

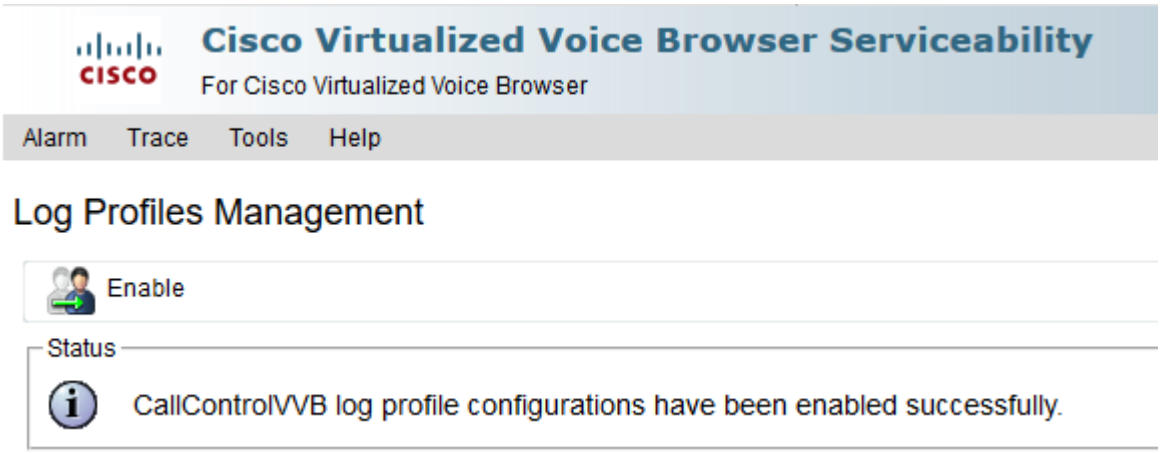
Passaggio 2. Seleziona traccia -> Profilo



Passaggio 3. Selezionare il profilo che si desidera abilitare per lo scenario specifico e fare clic sul pulsante Abilita. Ad esempio, abilitare il profilo CallControlVB per i problemi relativi al SIP o il profilo MRCPVB per i problemi relativi al riconoscimento vocale automatico e all'interazione da testo a voce (ASR/TTS).



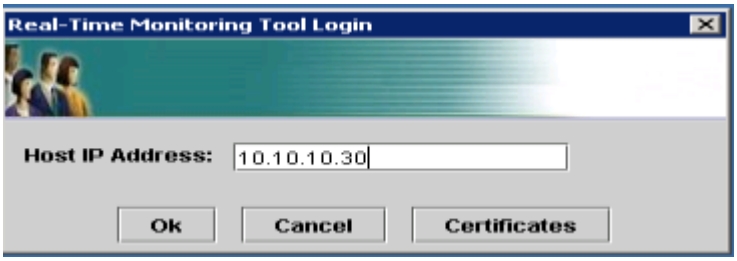
Dopo aver fatto clic sul pulsante di abilitazione, verrà visualizzato il messaggio di riuscita.



Passaggio 4. Una volta riprodotto il problema, raccogliere i registri. Utilizzare lo strumento di monitoraggio in tempo reale (RTMT, Real Time Monitor Tool) fornito con il CVB per raccogliere i log.

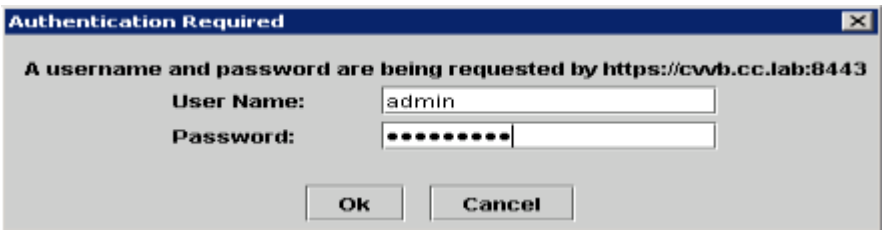
Passaggio 5. Fare clic sull'icona Cisco Unified Real-Time Monitoring Tool sul desktop (se lo strumento è già stato scaricato dal CVB)

Passaggio 6. Specificare l'indirizzo IP del VB e fare clic su OK.



Passaggio 7. Accettare le informazioni sul certificato, se visualizzate.

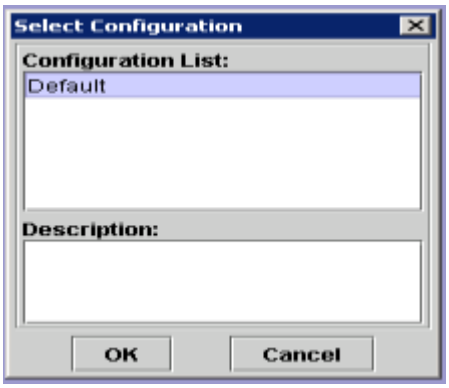
Passaggio 8. Fornire le credenziali e fare clic su OK.



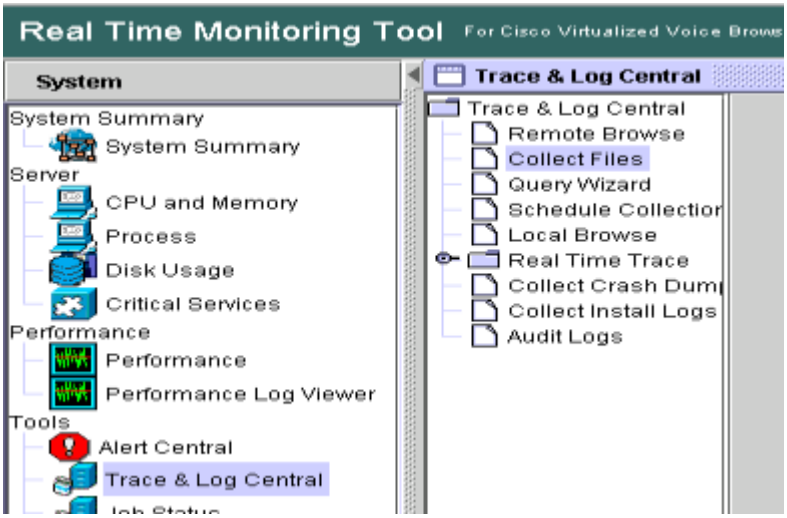
Passaggio 9. Se viene visualizzato un avviso di mancata corrispondenza del fuso orario, fare clic su YES (SÌ) e continuare.

Passaggio 10. Se si è ricevuto l'errore TimeZone, RTMT potrebbe chiudersi dopo aver fatto clic sul pulsante Sì. Riavviare lo strumento RTMT.

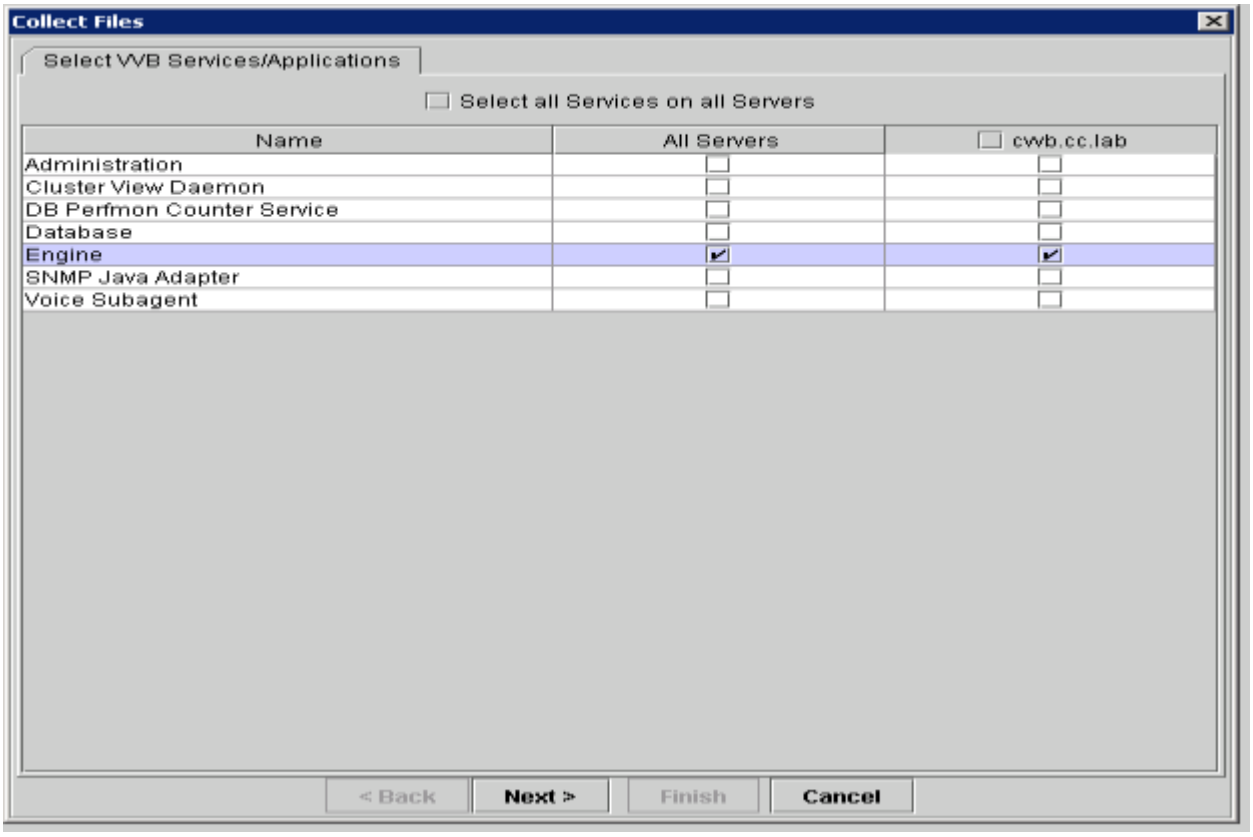
Passaggio 11. Lasciare selezionata la configurazione di default e fare clic su OK



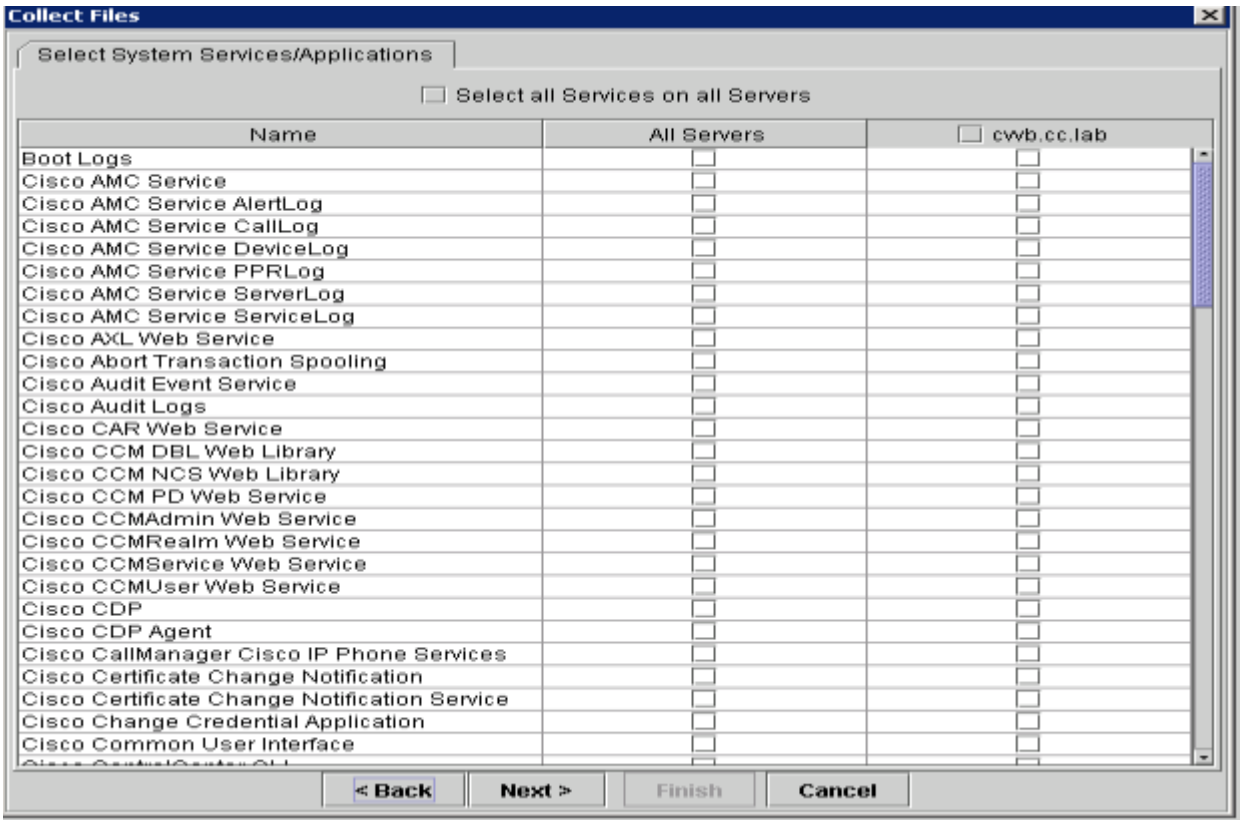
Passaggio 12. Selezionare Trace & Log Central, quindi fare doppio clic su Raccogli file



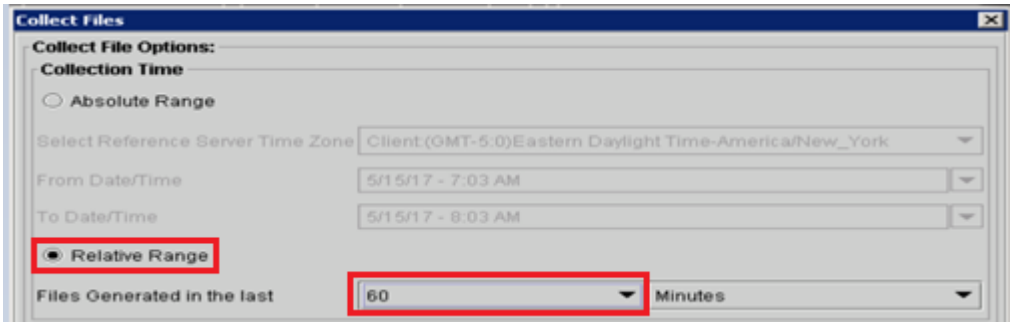
Passaggio 13. Nella nuova finestra aperta, selezionare il Motore e fare clic su Avanti



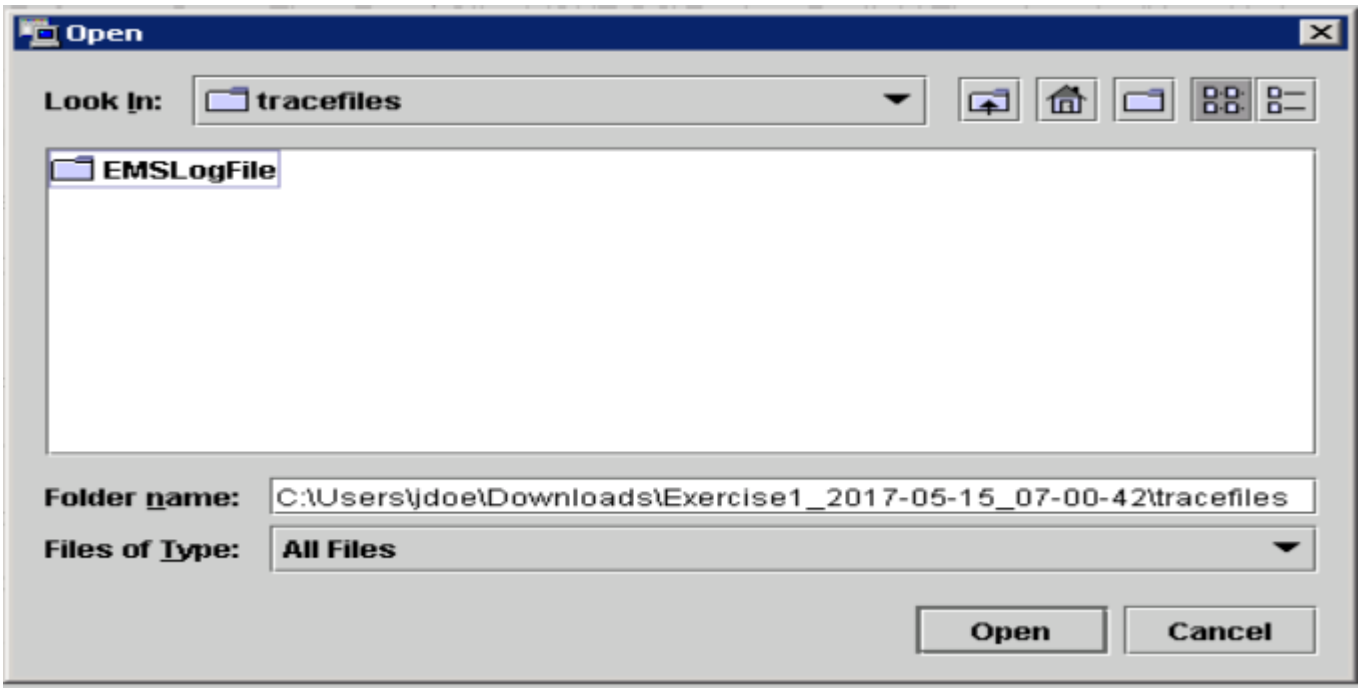
Passaggio 14. Fare di nuovo clic su Avanti nella finestra successiva



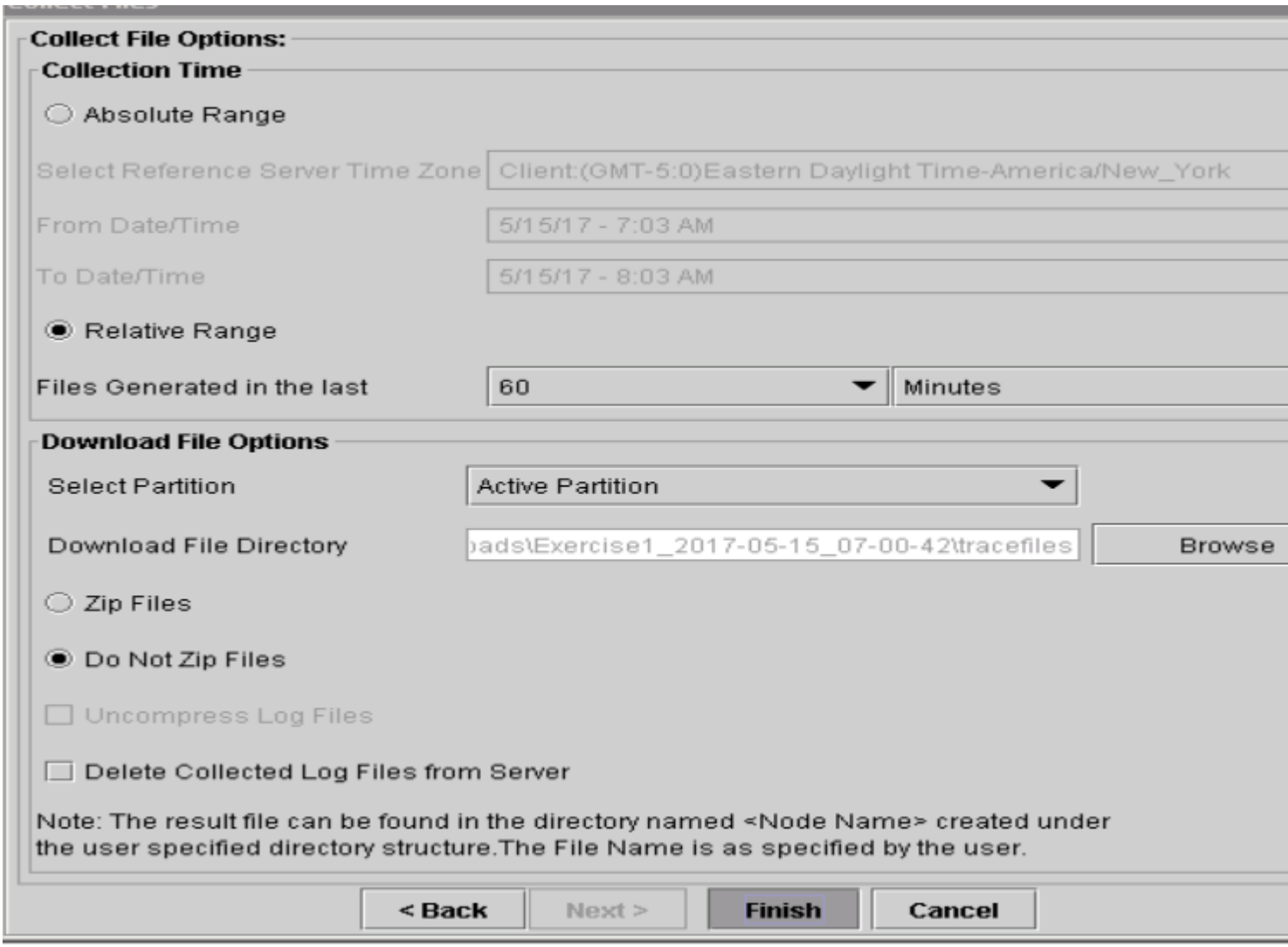
Passaggio 15. Selezionare Intervallo relativo e assicurarsi di selezionare l'ora per coprire l'ora della chiamata non valida



Passaggio 16. In Opzioni download file, fare clic su Sfoglia e selezionare la directory in cui si desidera salvare il file, quindi fare clic su Apri

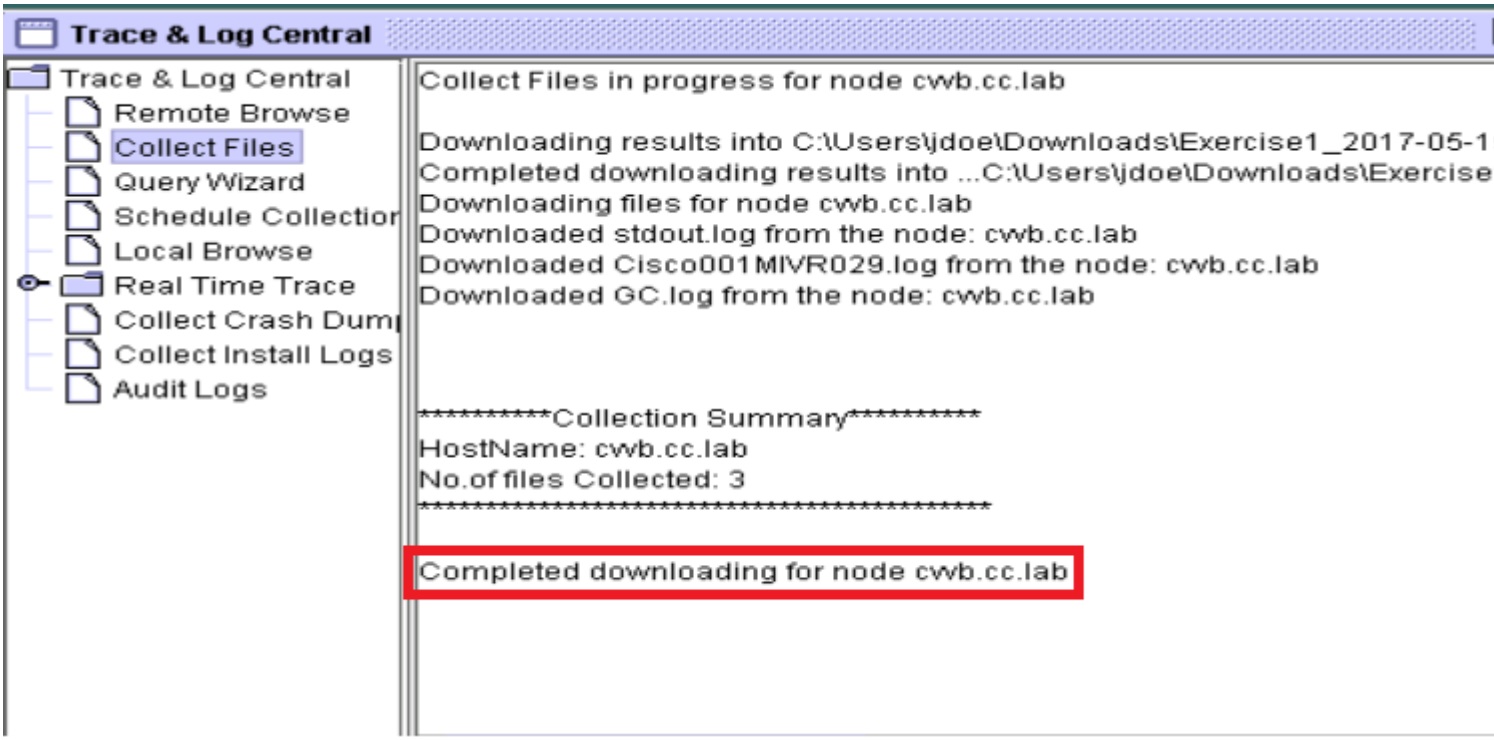


Passaggio 14. Dopo aver selezionato tutte le opzioni, fare clic sul pulsante Fine



Passaggio 15. In questo modo vengono raccolti i file di registro. Attendere la visualizzazione del messaggio

di conferma in RTMT



Passaggio 16. Passare alla cartella in cui sono state salvate le tracce.

Passaggio 17. I registri del motore sono tutti necessari. Per individuarli, passare alla cartella \<timestamp>\uccx\log\MIVR.

Impostazioni traccia e raccolta log per CUBE e CUSP

SIP (CUBE)

Passaggio 1. Impostare il timestamp dei log e abilitare il buffer di log

```
#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
```

Avviso: qualsiasi modifica apportata al software di produzione Cisco IOS® GW può causare un'interruzione delle attività.

Si tratta di una piattaforma molto solida in grado di gestire i debug consigliati sul volume di chiamata fornito senza problemi. Tuttavia, Cisco consiglia di:

- Inviare tutti i registri a un server syslog anziché al buffer di registrazione:

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

- Applicare i comandi di debug uno alla volta e controllare l'utilizzo della CPU dopo ciascuno di essi:

```
show proc cpu hist
```

Avviso: se l'utilizzo della CPU raggiunge il 70-80%, il rischio di un impatto sui servizi correlati alle prestazioni aumenta notevolmente. Pertanto, non abilitare debug aggiuntivi se il GW raggiunge il 60%

Passaggio 2. Abilita questi debug:

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

Passaggio 3. Riprodurre il problema.
Passaggio 4. Disattivare le tracce.

```
#undebug all
```

Passaggio 5. Raccogliere i registri.

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

CUSPIDE

Passaggio 1. Attiva le tracce SIP su CUSP.

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

Passaggio 2. Riprodurre il problema.

Passaggio 3. Al termine, disattivare la registrazione.

Raccogliere i registri.

Passaggio 1. Configurare un utente sulla CUSP (ad esempio, test).

Passaggio 2. Aggiungere questa configurazione al prompt CUSP.

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

Passaggio 3. FTP all'indirizzo IP CUSP. Utilizzare il nome utente (test) e la password definiti nel passaggio precedente.

Passaggio 4. Cambiare directory in /cusp/log/trace.

Passaggio 5. Ottenere log_<nomefile>.

Impostazioni traccia e raccolta log UCCE

Cisco consiglia di impostare i livelli di traccia e di raccogliere le tracce tramite il portale di Diagnostis Framework o gli strumenti CLI di sistema

Nota: per ulteriori informazioni su Diagnostic Framework Portico e System CLI, visitare il capitolo Diagnostic tools sulla Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, release 11.5(1).

Nella risoluzione dei problemi relativi alla maggior parte degli scenari UCCE, se il livello predefinito delle tracce non fornisce informazioni sufficienti, impostare il livello delle tracce su 3 nei componenti richiesti (con alcune eccezioni).

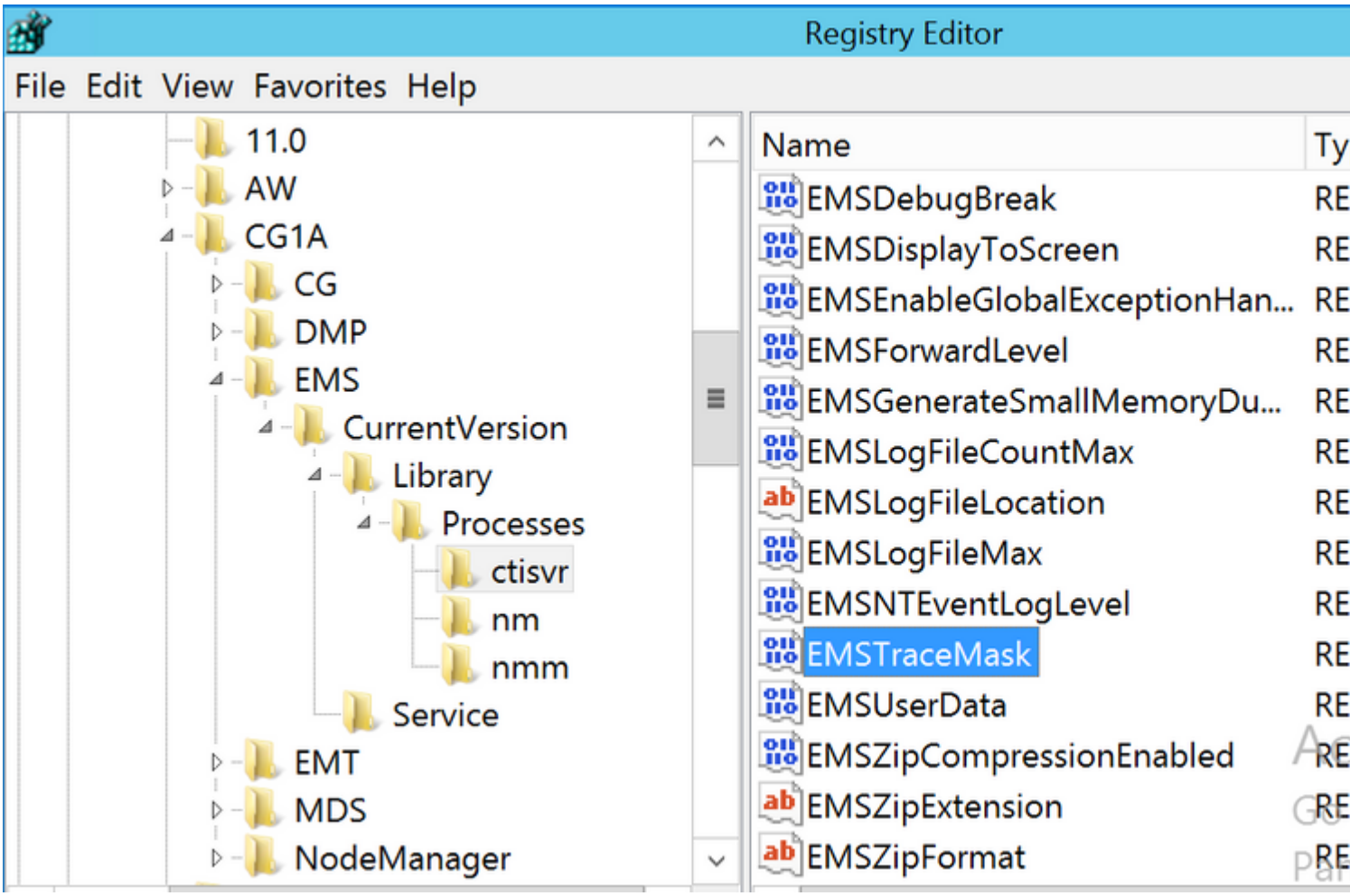
Nota: per ulteriori informazioni, vedere la sezione Trace Level della guida alla fornitura di servizi per Cisco Unified ICM/Contact Center Enterprise, versione 11.5(1).

Ad esempio, per la risoluzione dei problemi relativi a Dialer in uscita, impostare il livello delle tracce sul livello 2 se Dialer è occupato.

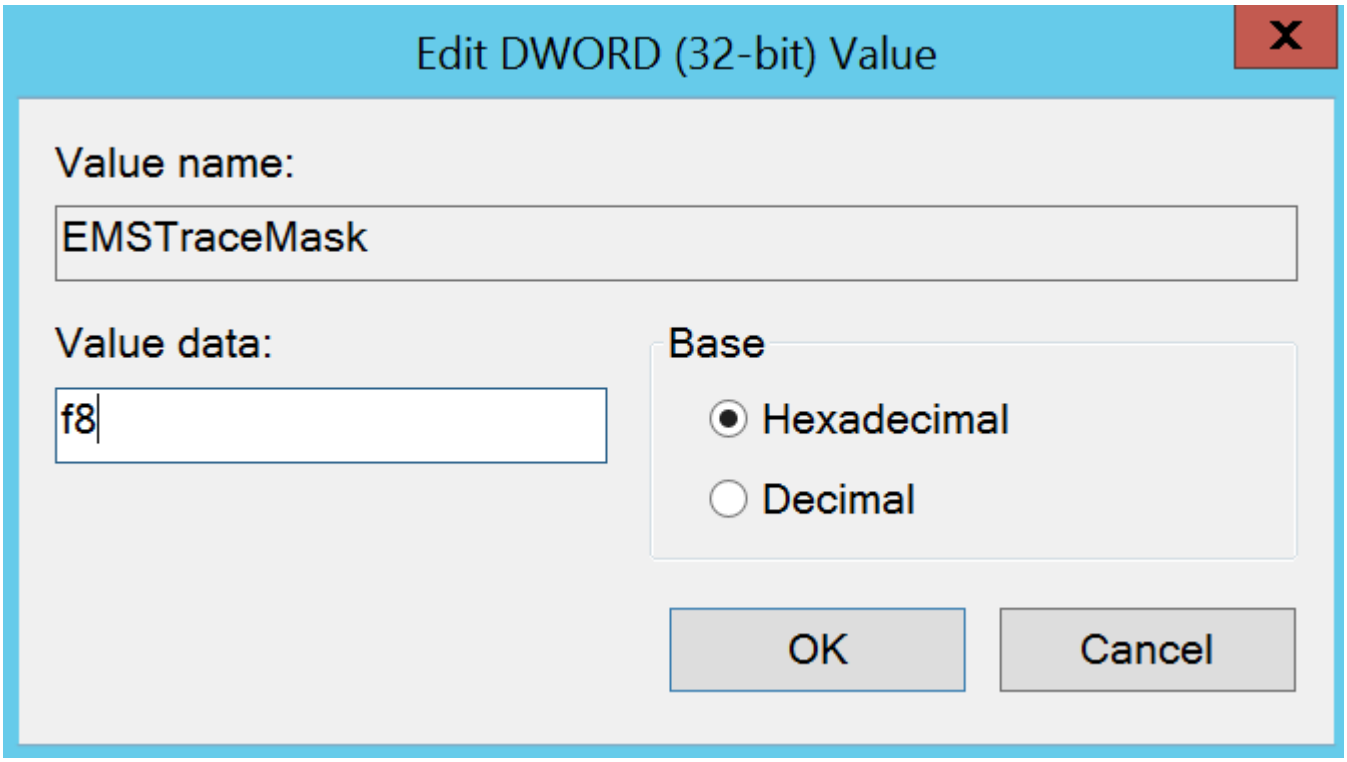
Per CTISVR (CTISVR) il livello 2 e il livello 3 non impostano l'esatto livello del Registro di sistema consigliato da Cisco. Il registro di traccia consigliato per CTISVR è 0XF8.

Passaggio 1. In UCCE Agent PG, aprire l'Editor del Registro di sistema (Regedit).

Passaggio 2. Passare a HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a e b)\EMS\CurrentVersion\library\Processes\ctisvr.



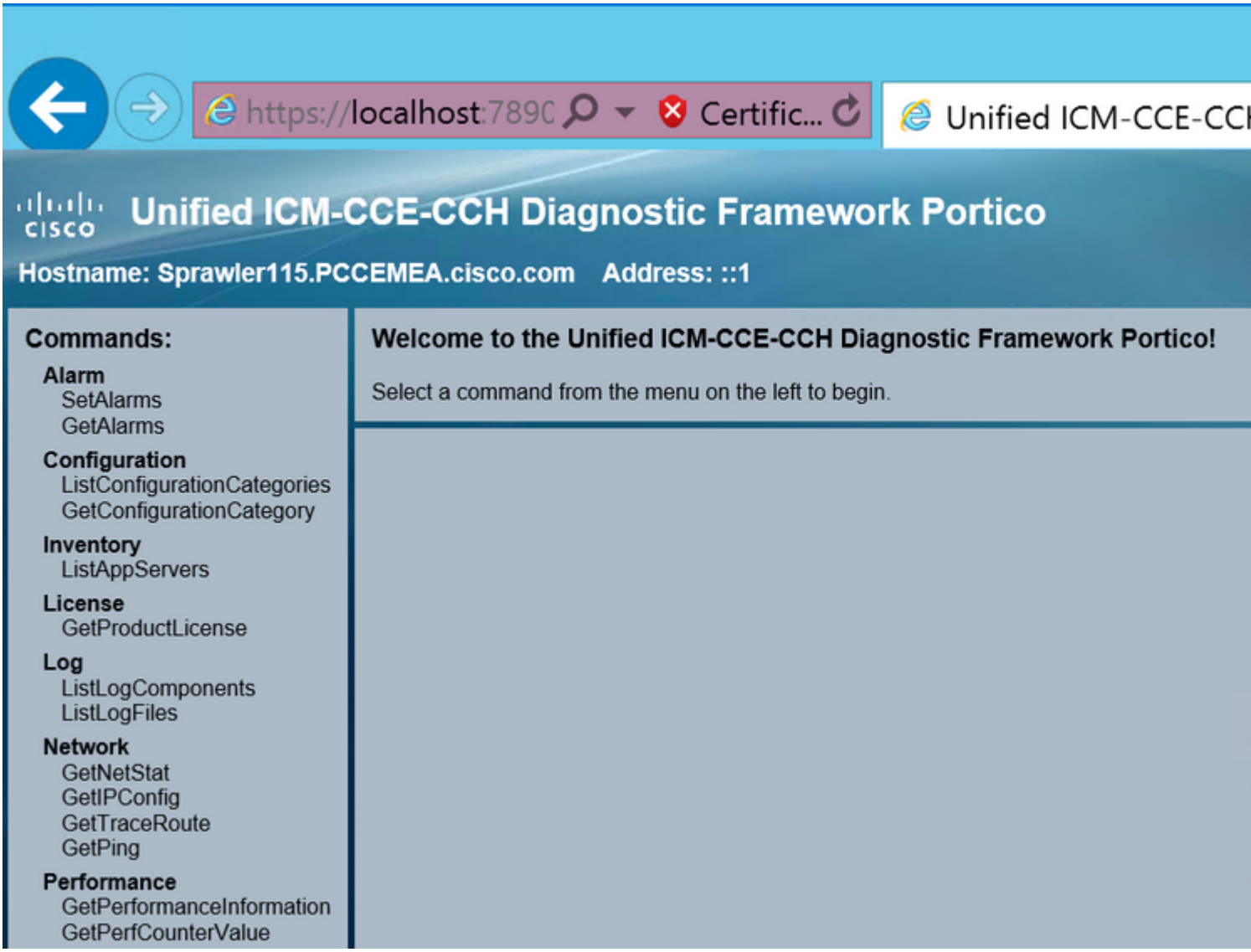
Passaggio 3. Fare doppio clic su EMSTraceMask e impostare il valore su f8.



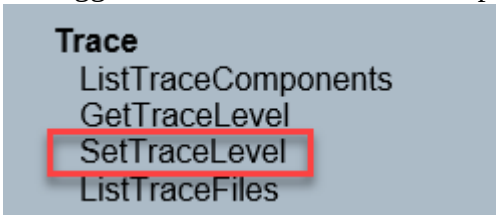
Passaggio 4. Fare clic su OK e chiudere l'Editor del Registro di sistema

Di seguito viene riportata la procedura per impostare le tracce dei componenti UCCE (processo RTR

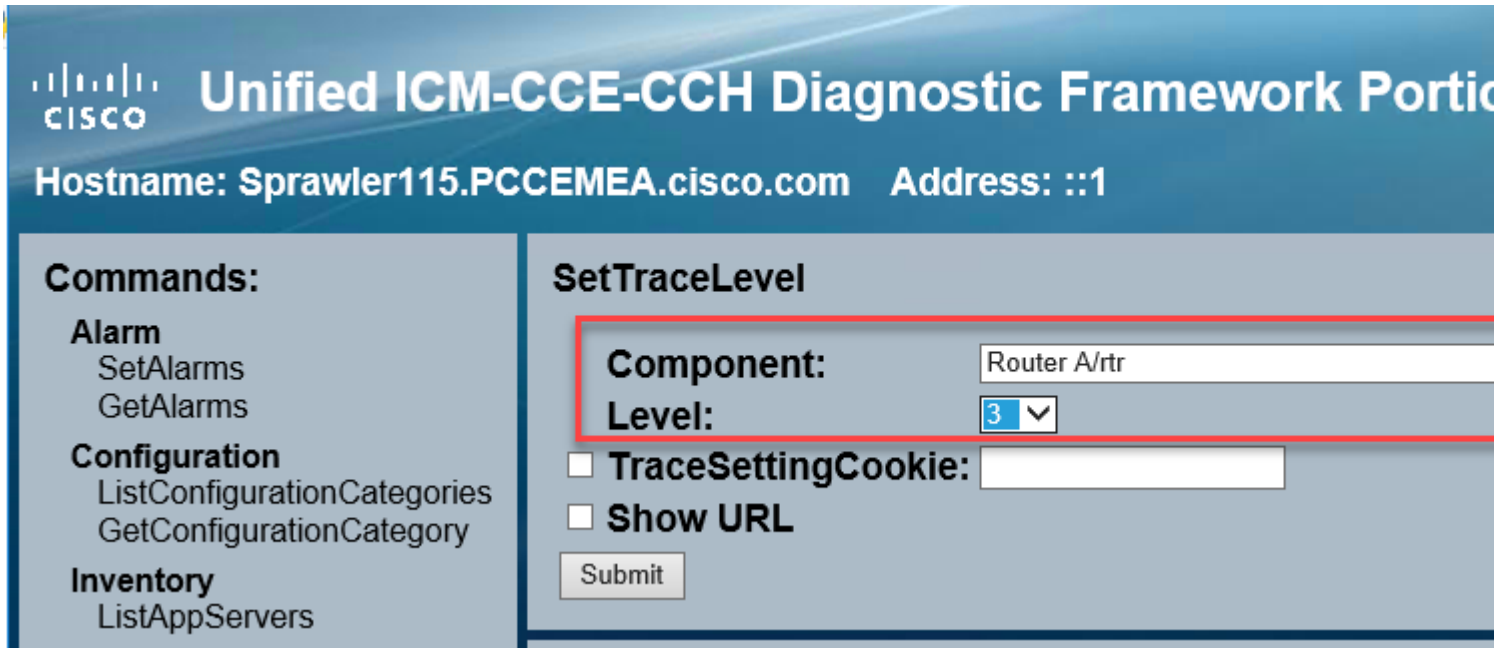
utilizzato come esempio).
Passaggio 1. Aprire il Portico del framework di diagnostica dal server per cui è necessario impostare le tracce. accedere con l'utente Administrator.



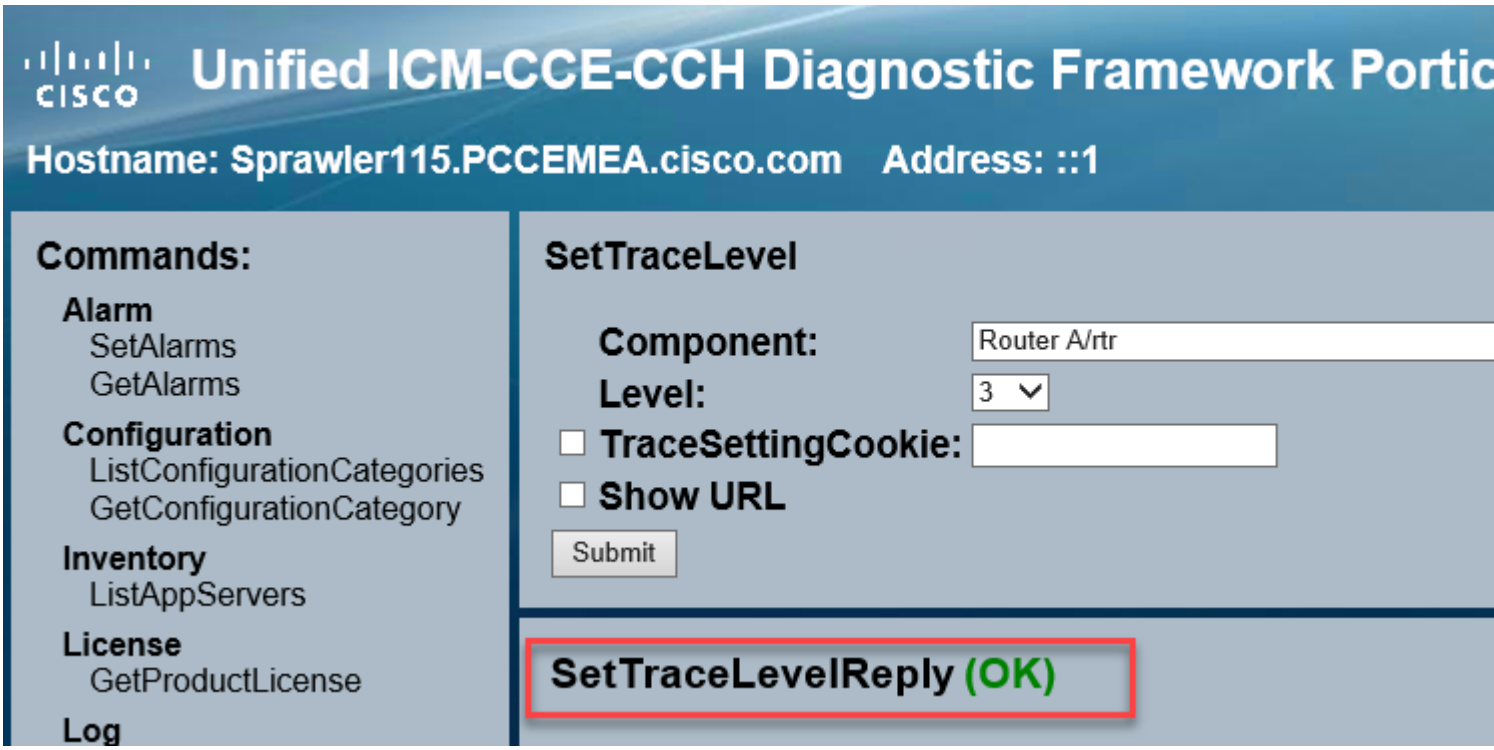
Passaggio 2. Nella sezione Comandi passare a Trace e selezionare SetTraceLevel.



Passaggio 3. Nella finestra SetTraceLevel selezionare il componente e il livello.

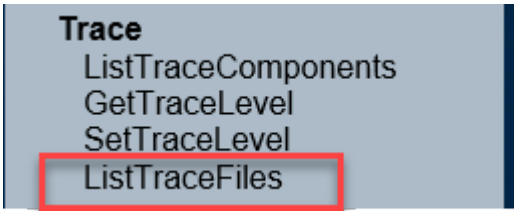


Passaggio 4. Fare clic su Invia. Al termine, verrà visualizzato il messaggio OK.

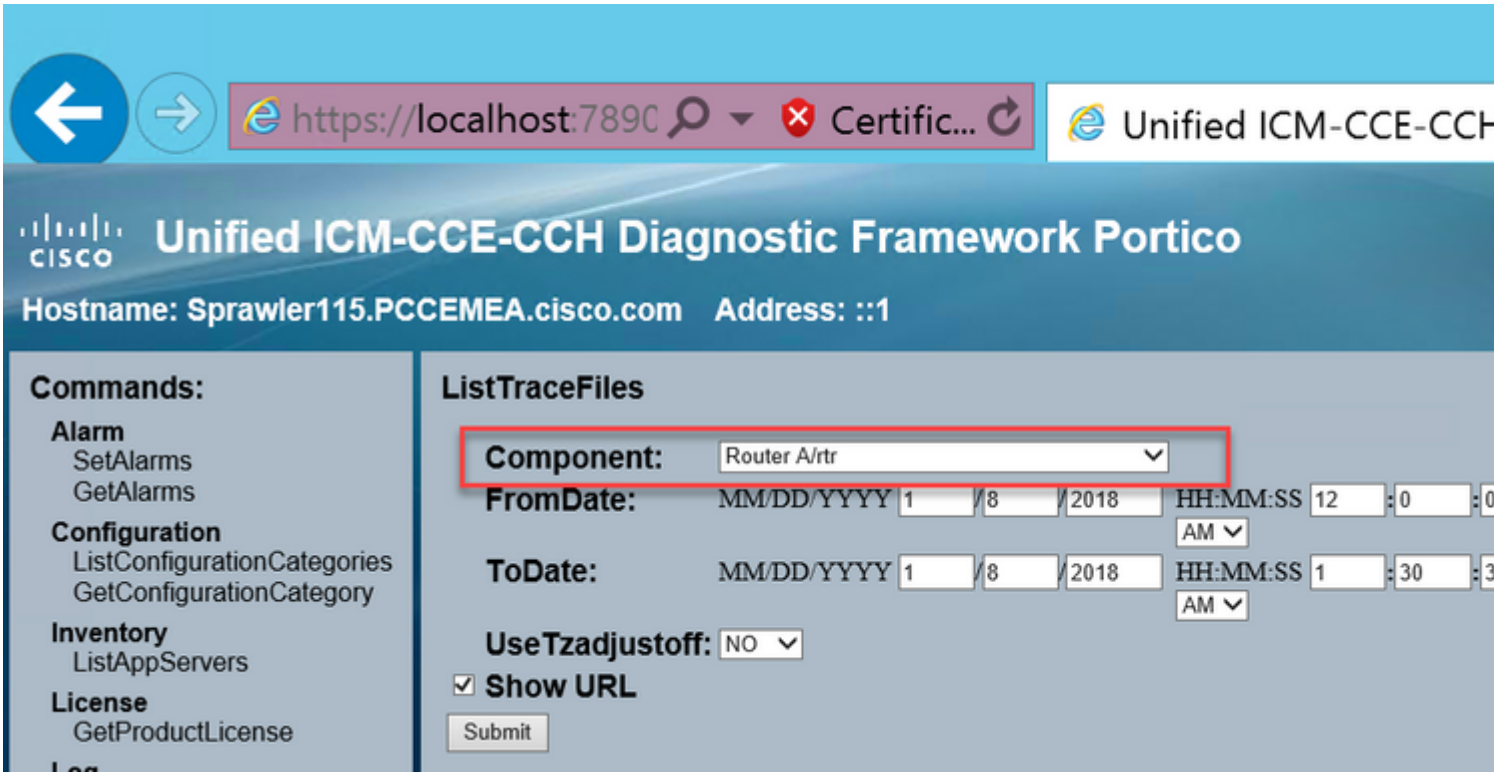


Avvertenza: impostare il livello delle tracce sul livello 3 mentre si cerca di riprodurre il problema. Dopo la riproduzione del problema, impostare il livello di traccia predefinito. Prestare particolare attenzione quando si impostano le tracce JTAPIGW, poiché il livello 2 e il livello 3 impostano le tracce di livello basso e questo può causare un impatto sulle prestazioni. Impostare il livello 2 o il livello 3 in JTAPIGW durante il tempo di non produzione o in un ambiente lab.

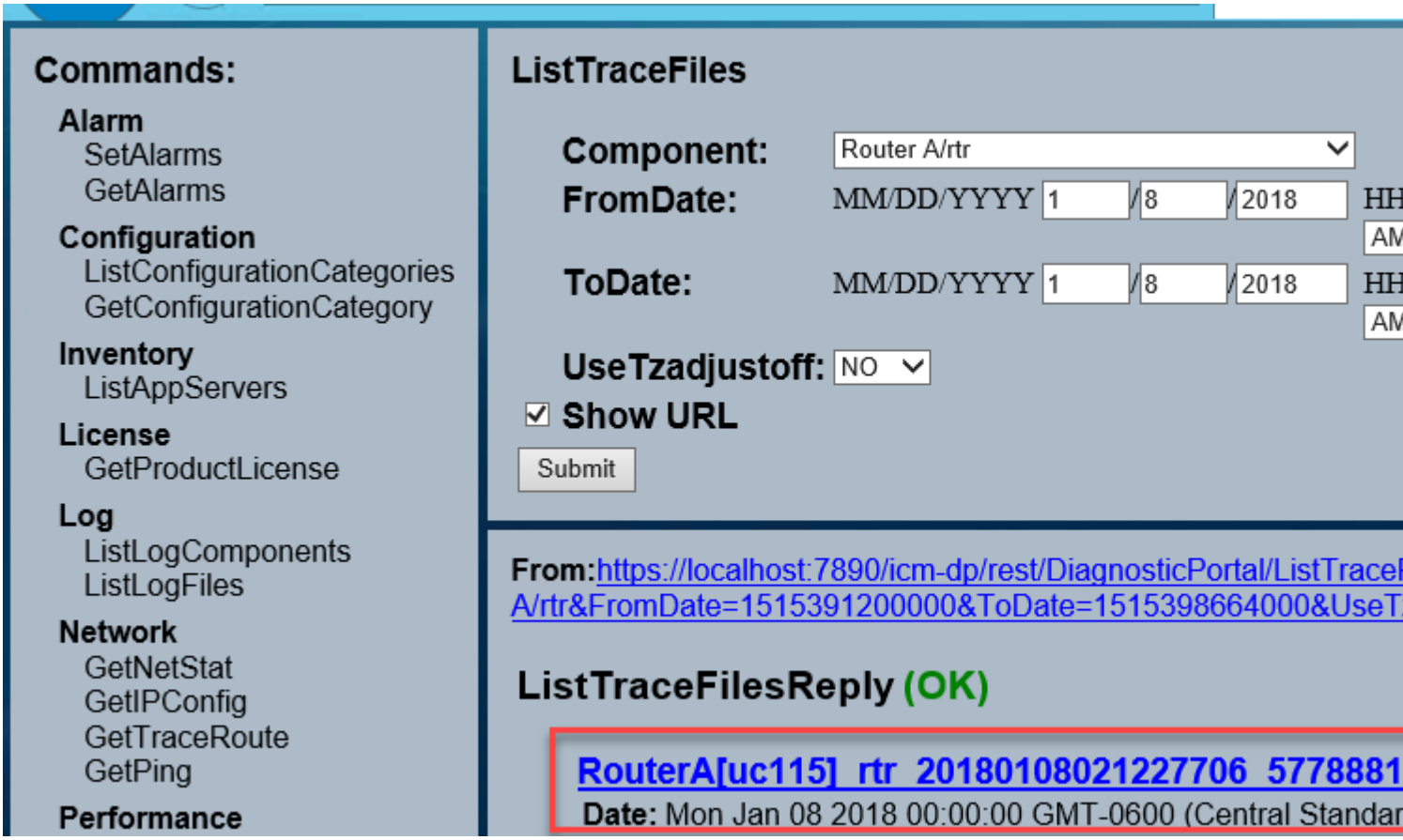
Raccolta log
Passaggio 1. Dal Portico Diagnostic Framework, nella sezione Commands, passare a Trace e selezionare ListTraceFile.



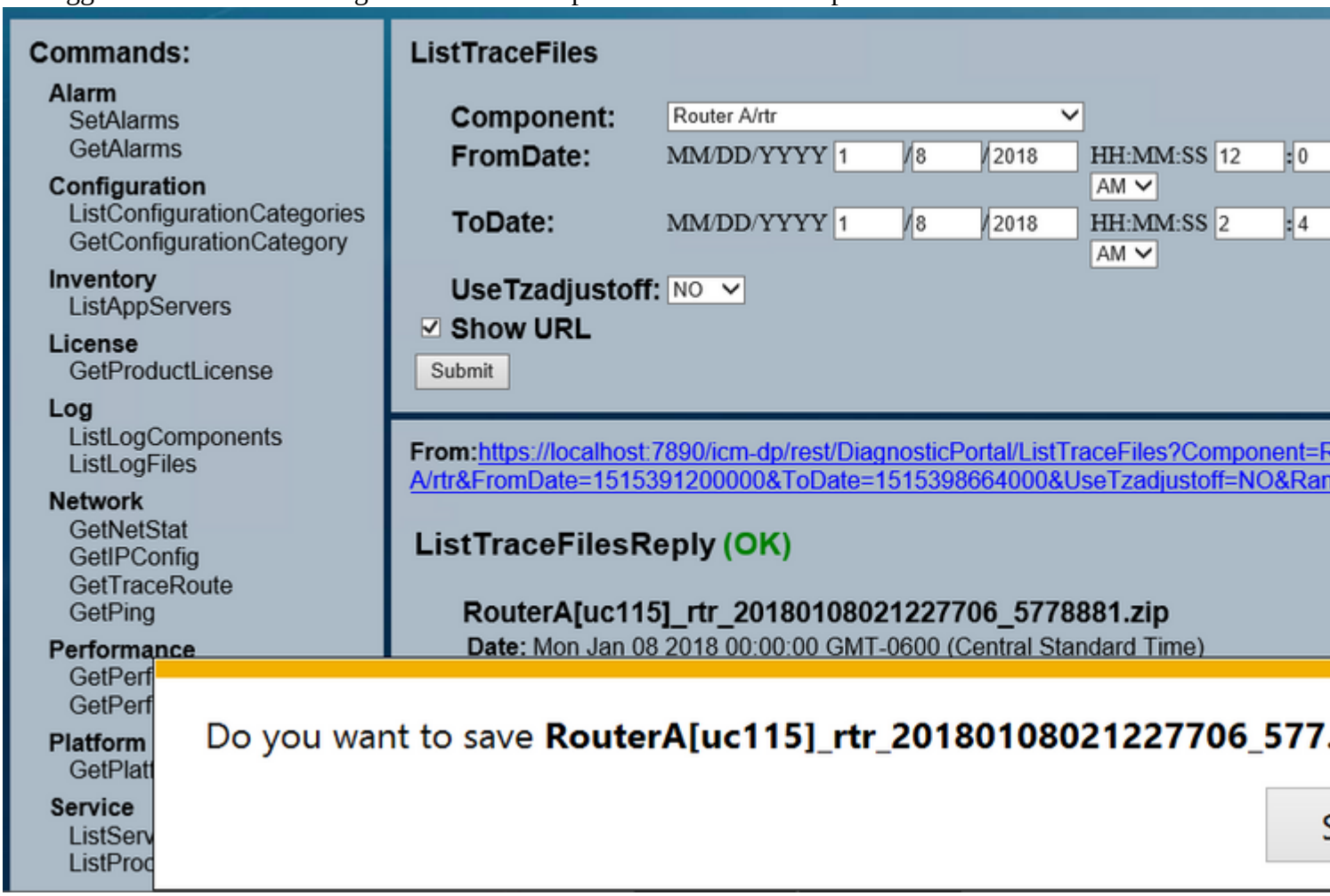
Passaggio 2. Nella finestra ListTraceFile selezionare Component, FromDate e ToDate. Seleziona la casella Mostra URL, quindi fai clic su Invia.



Passaggio 3. Al termine della richiesta, viene visualizzato il messaggio OK con il collegamento del file di log ZIP.



Passaggio 4. Fare clic sul collegamento del file Zip e salvare il file nella posizione scelta.

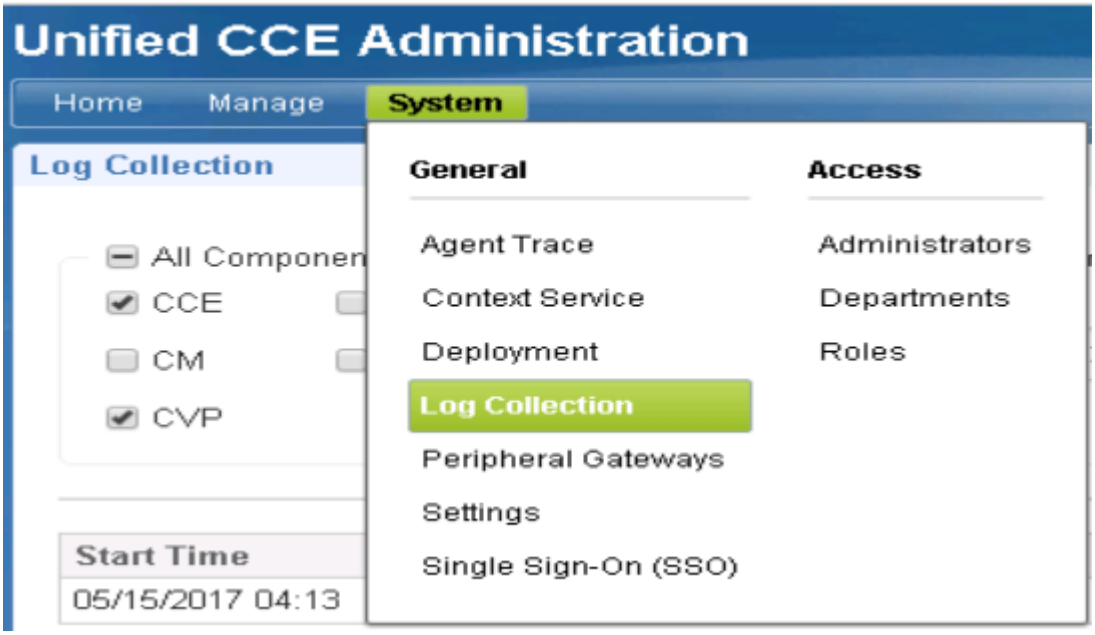


Impostazioni traccia e raccolta log PCCE

PCCE dispone di un proprio strumento per impostare i livelli di traccia. Non è applicabile agli ambienti UCCE in cui il Portico di Diagnostic Framework o la CLI di sistema sono i modi preferiti per abilitare e raccogliere i log.

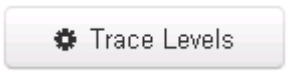
Passaggio 1. Dal server PCCE AW, aprire lo strumento Unified CCE Web Administration e accedere con l'account admin.

Passaggio 2. Passare a Sistema ->Raccolta log.

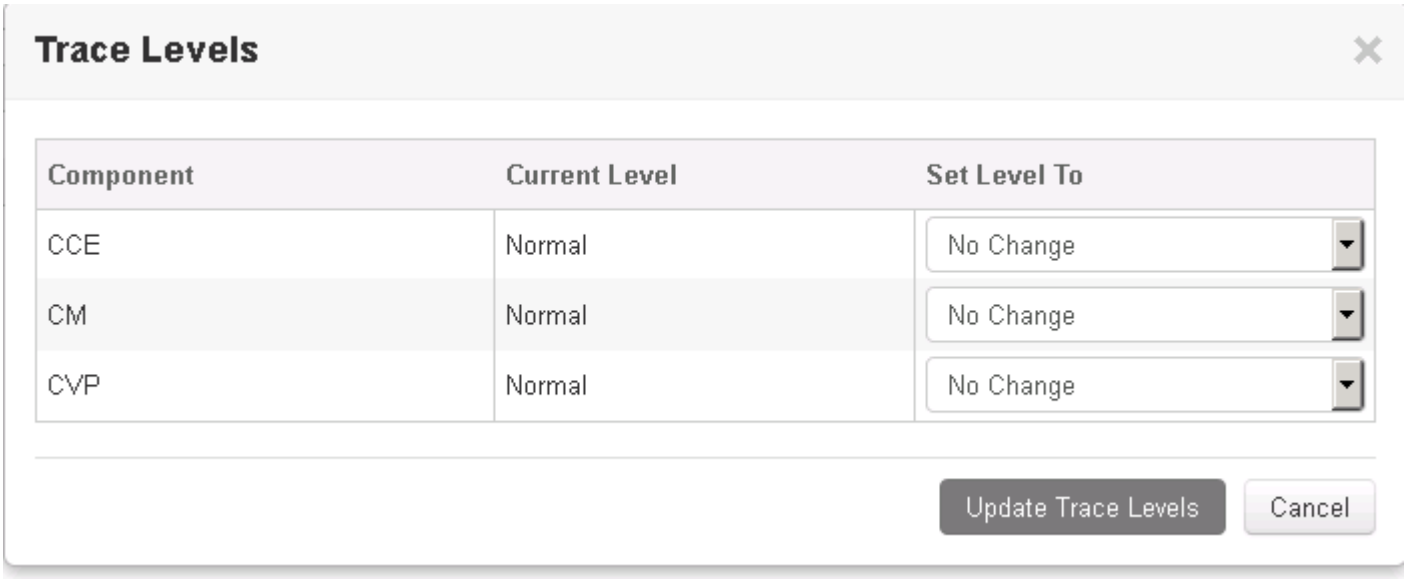


Passaggio 3. Viene visualizzata la pagina Raccolta log.

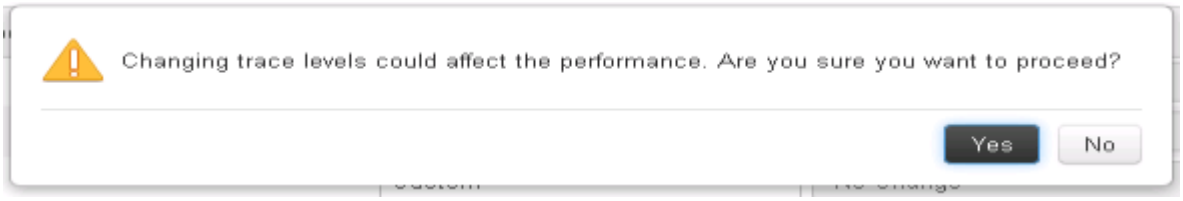
Passaggio 4. Fare clic su , Livelli di traccia, viene caricata una finestra di dialogo popup



Passaggio 5. Impostare Livello traccia su Dettagliato su CCE e lasciare invariato per CM, CVP. E fare clic su Aggiorna livelli di traccia



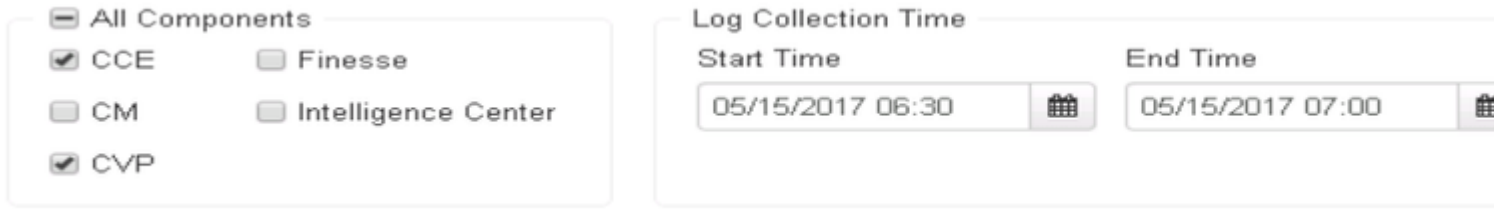
Passaggio 6. Fare clic su Sì per confermare l'avvertenza.



Passaggio 7. Una volta riprodotto il problema, aprire Unified CCE Administration e tornare a System -> Log Collection (Sistema -> Raccolta log).

Passaggio 8. Selezionate CCE e CVP nel riquadro Componenti.

Passaggio 9. Selezionare l'ora di raccolta del log appropriata (l'impostazione predefinita è gli ultimi 30 minuti).



Nota: aggiornare la pagina relativa all'ora di fine per aggiornarla con l'ora corrente

Passaggio 10. Fare clic su Raccogli log e su Sì per visualizzare l'avviso della finestra di dialogo. Verrà avviata la raccolta dei log. Attendere qualche minuto prima che finisca.

Passaggio 11. Al termine, fare clic sul pulsante Scarica nella colonna Azioni per scaricare un file compresso con tutti i log in esso contenuti. Salvare il file zip nella posizione appropriata.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).