

# Impostazione delle tracce e raccolta dei log in CCE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Imposta tracce e raccogli log Finesse](#)

[Finesse Client](#)

[Opzione 1: raccolta dei log client tramite la segnalazione errori di invio](#)

[Opzione 2: Impostare la registrazione permanente](#)

[Opzione 3: Console del browser Web](#)

[Finesse Server](#)

[Opzione 1: Tramite interfaccia utente - Servizi Web \(obbligatori\) e registri aggiuntivi](#)

[Opzione 2: Tramite SSH e SFTP \(Secure File Transfer Protocol\) - Opzione consigliata](#)

[Impostazione delle tracce e raccolta dei log CVP e CVB](#)

[CVP Call Server](#)

[Applicazione CVP Voice XML \(VXML\)](#)

[Portale di gestione operativa e amministrativa \(OAMP\) CVP](#)

[Cisco Virtualized Voice Browser \(CVB\)](#)

[Opzione 1: Tramite Account Amministrativo](#)

[Opzione 2: tramite SSH e SFTP - Opzione consigliata](#)

[Impostazione di registri di traccia e raccolta per CUBE e CUSP](#)

[SIP \(CUBE\)](#)

[CUSPIDE](#)

[Raccogli i log](#)

[Imposta traccia e raccogli log UCCE](#)

[Imposta livello traccia](#)

[Raccolta log](#)

[Imposta traccia e raccogli log PCCE](#)

[Imposta traccia e raccogli registri CUIC/Live Data/IDS](#)

[Download dei log con SSH](#)

[Scarica log con RTMT](#)

[Acquisizione pacchetti su VoS \(Finesse, CUIC, VB\)](#)

---

## Introduzione

In questo documento viene descritto come impostare e raccogliere tracce in Cisco Unified Contact Center Enterprise (CCE).

# 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 (VB)
- Cisco Unified Border Element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- CUSP (Cisco Unified Session Initiation Protocol) Proxy

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Finesse release 12.5
- CVP Server release 12.5
- UCCE/PCCE release 12.5
- Cisco VB release 12.5
- CUIC release 12.5

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.

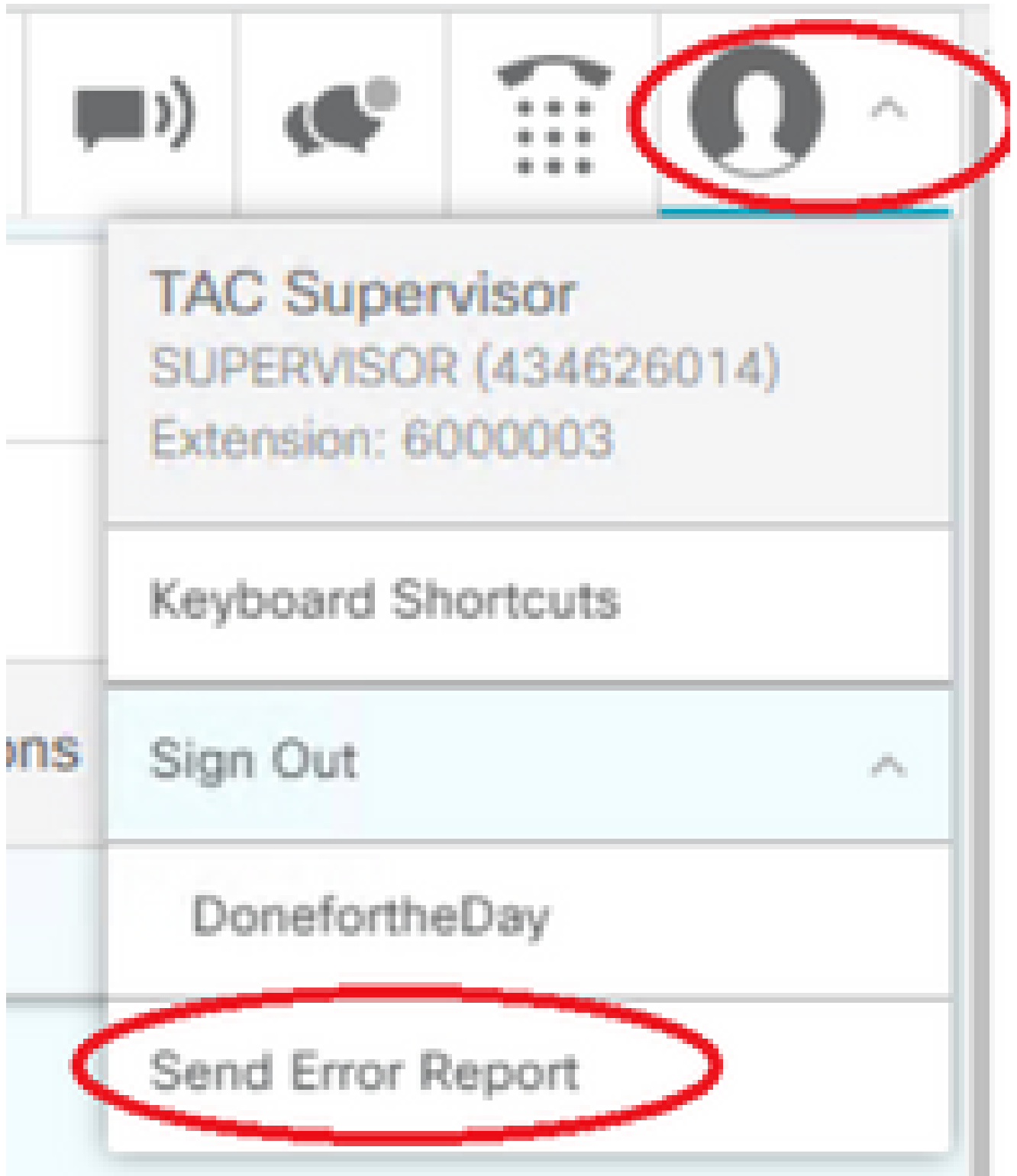
# Imposta tracce e raccogli log Finesse

## Finesse Client

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

Opzione 1: raccolta dei log client tramite la segnalazione errori di invio

1. Accedere a un agente.
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 superiore destro del desktop di Finesse.



3. L'agente visualizza il messaggio Registri inviati correttamente.
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.
5. Raccogliere i log nella directory clientlogs/.

#### Directory Listing For /logs/ - Up To /

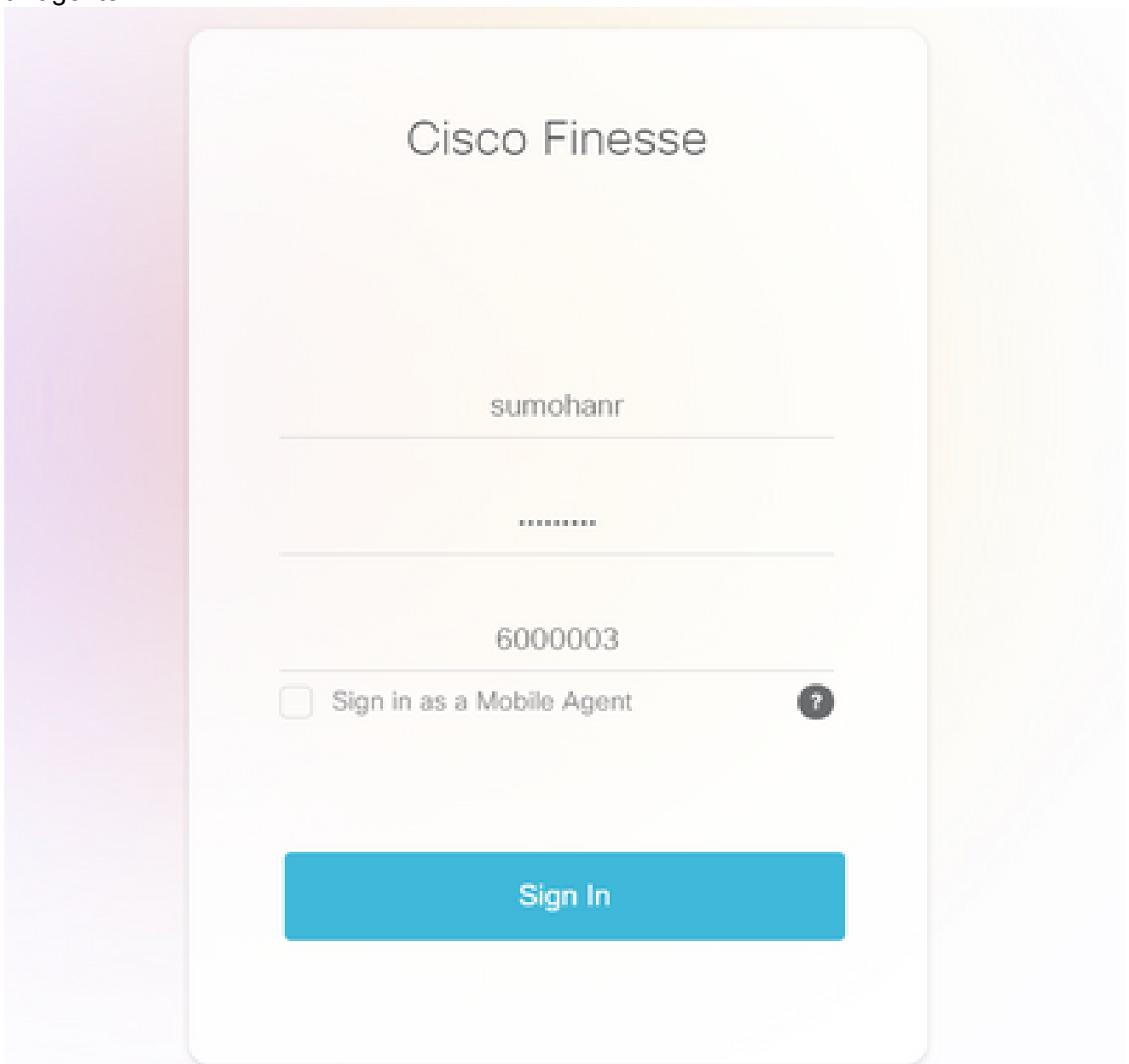
Filename	Size	Last Modified
<a href="#">3rdpartygadget/</a>		Mon, 22 Feb 2021 23:06:32
<a href="#">admin/</a>		Tue, 12 Jul 2022 18:52:53
<a href="#">cli.log</a>	0.0 kb	Mon, 22 Feb 2021 22:59:10
<a href="#">clientlogs/</a>		Wed, 17 Aug 2022 15:35:52

## Opzione 2: Impostare la registrazione permanente

1. Passare a <https://x.x.x.x:8445/desktop/locallog>.
2. Fare Clic Su Accedi Con Registrazione Persistente.



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

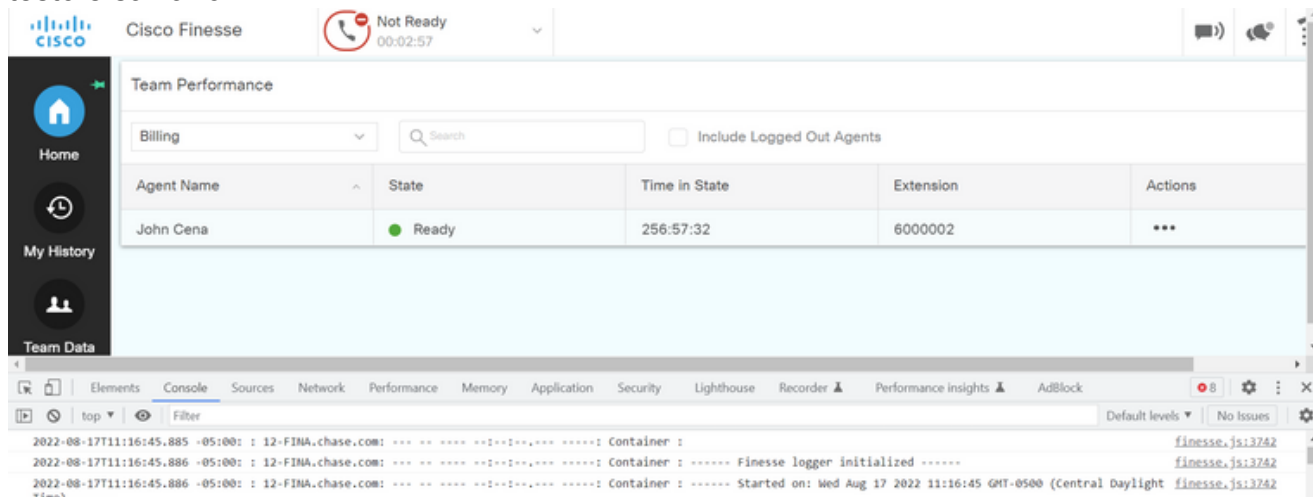


4. Tutta l'interazione desktop dell'agente viene registrata e inviata ai log di archiviazione locali. Per raccogliere i log, passare a <https://x.x.x.x:8445/desktop/locallog> e copiare il contenuto in

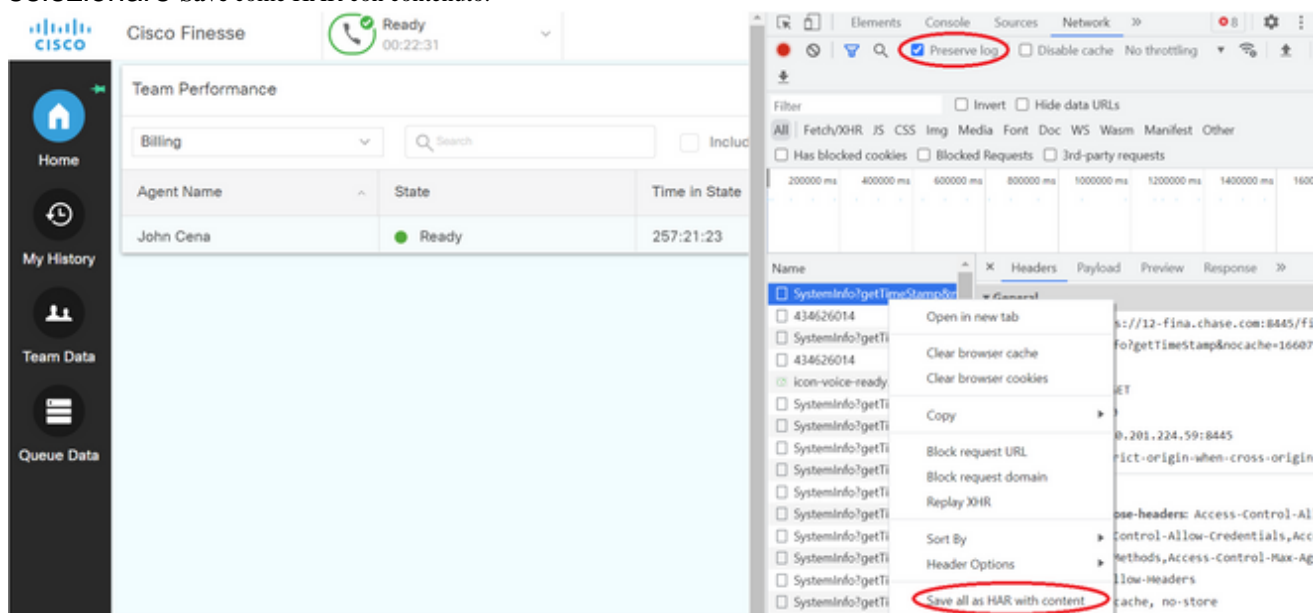
un file di testo. Salvate il file per ulteriori analisi.

### Opzione 3: Console del browser Web

1. Dopo che un agente ha eseguito l'accesso, premere F12 per aprire la console del browser.
2. Selezionare la scheda Console.
3. Verificare la presenza di errori nella console del browser. Copiare il contenuto in un file di testo e salvarlo.



4. Selezionare la scheda Rete e selezionare l'opzione Mantieni registro.
5. Fare clic con il pulsante destro del mouse su uno degli eventi relativi ai nomi di rete e selezionare Save come HAR con contenuto.



Finesse Server

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

- Passare a <https://x.x.x.x/finesse/logs> e accedere con l'account di amministrazione.

- Espandere la directory **webservices/**.

openfire/	Tue, 02 Aug 2022 00:45:59 G
openfireservice/	Thu, 07 May 2020 01:38:30 G
realm/	Wed, 17 Aug 2022 01:55:51 G
tomcat/	Sat, 13 Aug 2022 03:01:01 G
<b>webservices/</b>	Sun, 14 Aug 2022 07:41:43 G


Apache Tomcat/7.0.94

- 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 **Salva** il file.

**Directory Listing For /logs/webservices/ - Up To /logs**

Filename	Size	Last Modified
Desktop-webservices.2022-08-10T04-43-22.953.log.zip	4732.1 kb	Sun, 14 Aug 2022 07:40:54 GMT
Desktop-webservices.2022-08-14T00-40-54.953.log	90079.1 kb	Wed, 17 Aug 2022 16:26:44 GMT

- 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

- Accedere al server Finesse con SSH.
- Immettere questo comando per raccogliere i log necessari. Il comando raccoglie i registri per 2 ore. Viene richiesto di identificare il server SFTP in cui vengono caricati i log.

**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: 
```

- 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.
- Per raccogliere ulteriori log come tomcat, Context service, Servm e install logs, consultare la sezione Log Collection del manuale [Cisco Finesse Administration Guide release 12.5\(1\)](#).

Impostazione delle tracce e raccolta dei log CVP e CVB

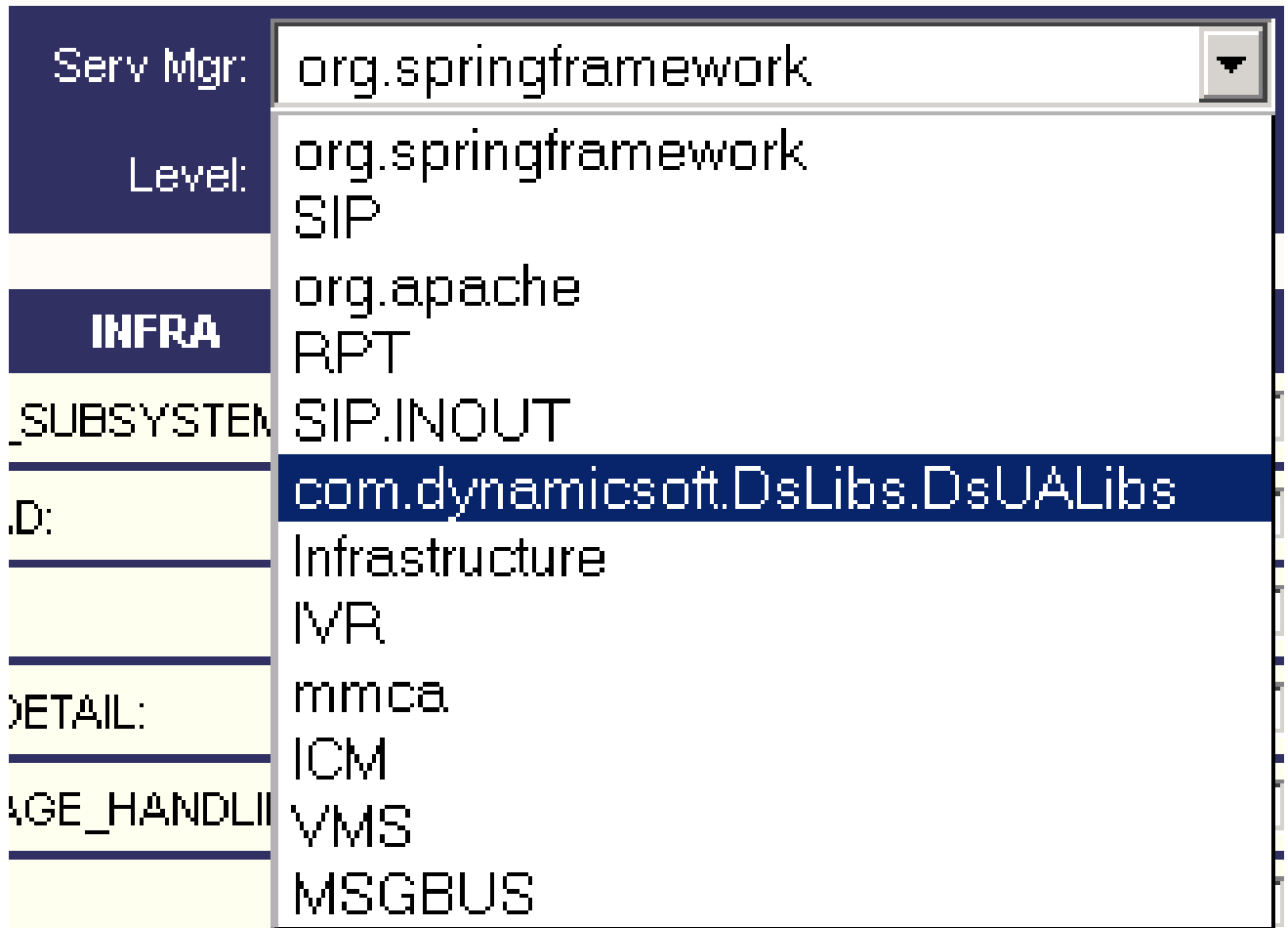
CVP Call Server

- 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.
- Accedere alla pagina Web CVP CallServer Diag all'URL <http://localhost:8000/cvp/diag>.



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

- Selezionare **com.dynamicsoft.DsLibs.DsUALibs** dal **server**. Menu a discesa di **Mgr** nell'angolo superiore sinistro.



- Fare clic sul pulsante **Imposta**.

MESSAGE:

RPT\_JDBC:

RPT\_CALL\_REG:

RPT\_BATCH:

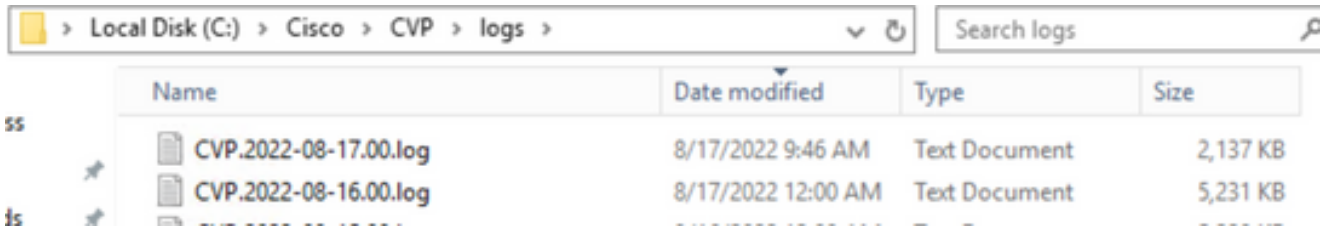


- Scorrere verso il basso nella finestra di traccia per verificare che il livello delle tracce sia stato impostato correttamente. Queste sono le impostazioni di debug.

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
MSQBUS	INFO	0

- 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.





7. Dopo aver riprodotto il problema, assicurarsi di ripristinare le tracce al livello predefinito. Selezionare **com.dynamicsoft.DsLibs.DsUALibs** dal **server. Mgr** menu a discesa nell'angolo superiore sinistro e impostarlo su errore.

Serv Mgr: **com.dynamicsoft.DsLibs.DsUALibs** (dropdown menu)  
 Level: **DEBUG** (dropdown menu)

STANDARD	INFRA	LEGACY MSG	ICM CUSTOM				
ALL:	<input type="checkbox"/>	LOAD_SUBSYSTEM:	<input type="checkbox"/>	MSGSLAYER_MESSAGE:	<input type="checkbox"/>	GED125_LOW_LEVEL:	<input type="checkbox"/>
CALL:	<input type="checkbox"/>	THREAD:	<input type="checkbox"/>	MSGSLAYER_METHOD:	<input type="checkbox"/>	MSGBUS_LOW_LEVEL:	<input type="checkbox"/>
METHOD:	<input type="checkbox"/>	MSG:	<input type="checkbox"/>	MSGSLAYER_HANDLED_EXCEPTION:	<input type="checkbox"/>	ICM_SUBSYSTEM_ADMIN:	<input type="checkbox"/>
PARAM:	<input type="checkbox"/>	MSG_DETAIL:	<input type="checkbox"/>	MSGSLAYER_PARAM:	<input type="checkbox"/>		
LOW_LEVEL:	<input type="checkbox"/>	MESSAGE_HANDLING:	<input type="checkbox"/>	GLOBAL_EVENT:	<input type="checkbox"/>		
CLASSDUMP:	<input type="checkbox"/>	TIMER:	<input type="checkbox"/>	EXTERNAL_EVENT:	<input type="checkbox"/>		
HEARTBEAT:	<input type="checkbox"/>	STATE:	<input type="checkbox"/>	STATIC_FIELD:	<input type="checkbox"/>		
HANDLED_EXCEPTION:	<input type="checkbox"/>	SECURITY:	<input type="checkbox"/>	EXTERNAL_STATE:	<input type="checkbox"/>		
OOOQUEUE:	<input type="checkbox"/>	LICENSING:	<input type="checkbox"/>	INTERNAL_STATE:	<input type="checkbox"/>		
GARBAGE_COLLECTOR:	<input type="checkbox"/>	STARTUP:	<input type="checkbox"/>	CODE_BRANCH:	<input type="checkbox"/>		
MESSAGE:	<input type="checkbox"/>	SHUTDOWN:	<input type="checkbox"/>	CODE_MARKER:	<input type="checkbox"/>		
RPT_JDBC:	<input type="checkbox"/>	STATS:	<input type="checkbox"/>	CLASS_DUMP:	<input type="checkbox"/>		
RPT_CALL_REG:	<input type="checkbox"/>	SNMP:	<input type="checkbox"/>	LOCAL_DUMP:	<input type="checkbox"/>		
RPT_BATCH:	<input type="checkbox"/>	SAF:	<input type="checkbox"/>				

Set

DEBUG/0 - DEBUG/41 - DEBUG/40

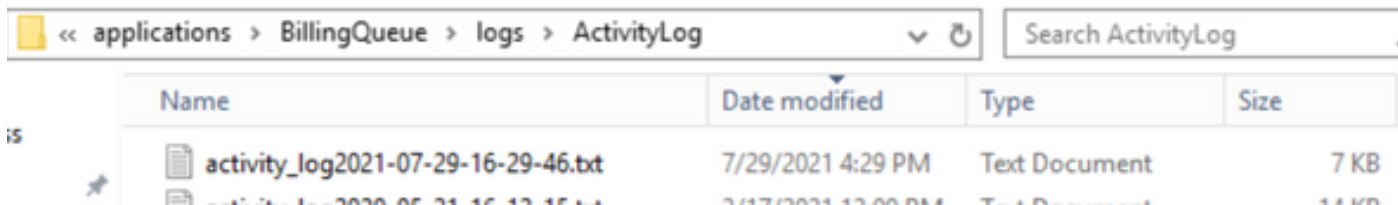
NAME	LEVEL	MASK
SIP	DEBUG	41
org.springframework	WARN	0
org.apache	ERROR	0
RPT	INFO	0
SIPINOUT	WARN	0
<b>com.dynamicsoft.DsLibs.DsUALibs</b>	<b>ERROR</b>	<b>0</b>
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
ALL_SS	INFO	0
MSGBUS	INFO	0

### 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.



Portale di gestione operativa e amministrativa (OAMP) CVP

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:

- Eseguire backup di `%CVP_HOME%\conf\oamp.properties`
- Modificare `%CVP_HOME%\conf\oamp.properties`

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

- Riavviare OPSConsoleServer dopo la modifica, come illustrato.

Informazioni sui livelli di traccia

Livello traccia	Descrizione	Livello log	Maschera di traccia
0	Installazione predefinita del prodotto. Impatto minimo o nullo sulle prestazioni.	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 +

Livello traccia	Descrizione	Livello log	Maschera di traccia
			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 + 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 di amministrazione Cisco VB definite come log MADM
- Tracce del motore Cisco VB 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

Subfacility	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
*LIBRARIES						
LIB_CFG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_EVENT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_JDBC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_JINI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_LICENSE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_MEDIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_RMI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_SERVLET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIB_TC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
*MANAGERS						

 **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 attivare il profilo
------	-------------------------------------

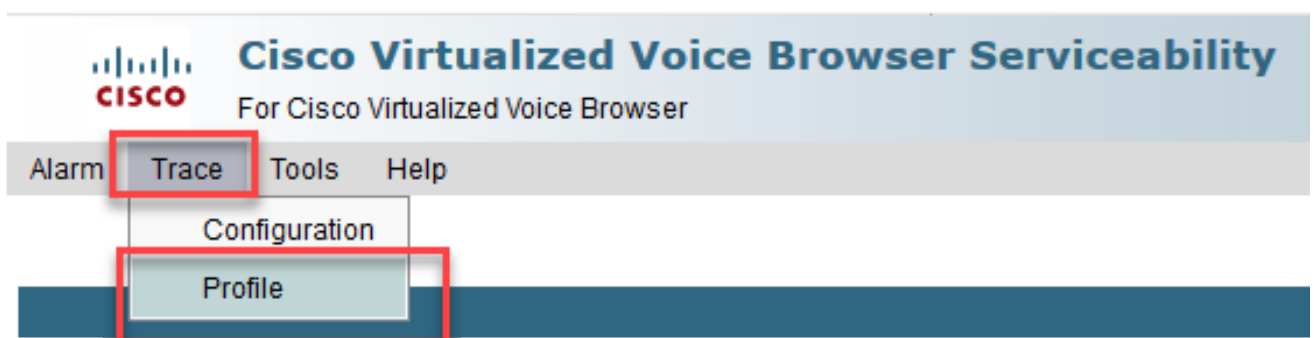
VVBpredefinito	I registri generici sono abilitati.
AppAdminVB	Per problemi relativi all'amministrazione Web tramite AppAdmin, Cisco VB Serviceability e altre pagine Web.
MediaVB	Per problemi relativi alla configurazione o alla trasmissione dei supporti.
VoiceBrowser VB	Per i problemi relativi all'handle delle chiamate.
MRCPVb	Per problemi con ASR/TTS con interazione Cisco VB.
CallControlVB	Per i problemi relativi al segnale SIP, vengono pubblicati nel registro.

Opzione 1: Tramite Account Amministrativo

- Aprire la pagina principale di CVB (<https://X.X.X.X/uccxservice/main.htm>) e accedere alla pagina Cisco VB Serviceability. Accedere con l'account di amministrazione



- Selezionare **Traccia > Profilo**.



- 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).



## Log Profiles Management



Enable

Status



Ready

### Profiles

[MediaVVB](#)

[DefaultVVB](#)

[AppAdminVVB](#)

[VoiceBrowserVVB](#)

[CallControlVVB](#)

[MRCPVVB](#)

Enable

- Facendo clic sul pulsante **Attiva** viene visualizzato il messaggio di operazione riuscita.



## Log Profiles Management



Enable

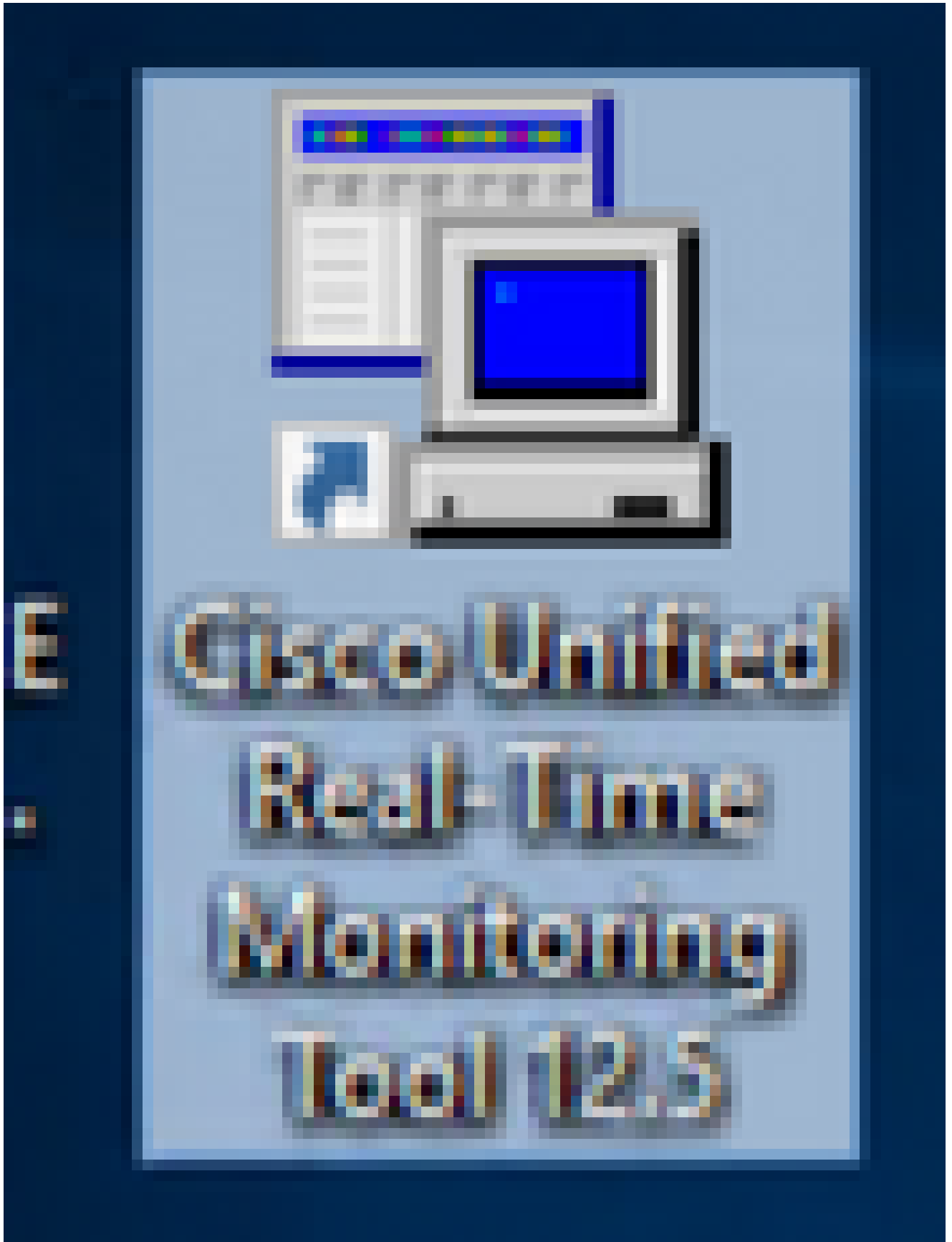
Status



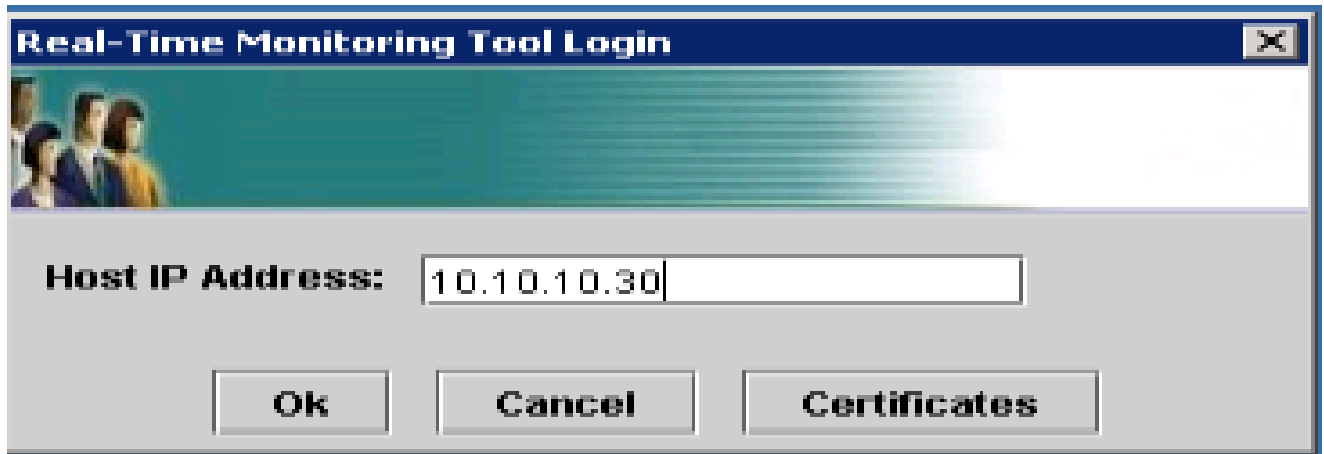
CallControlVVB log profile configurations have been enabled successfully.

- Una volta riprodotto il problema, raccogliere i log. Utilizzare lo strumento Real Time Monitor Tool (RTMT) fornito con il CVB per raccogliere i log.

- Fare clic sull'icona **Cisco Unified Real-Time Monitoring Tool** sul desktop (se necessario, scaricare lo strumento dal CVB).



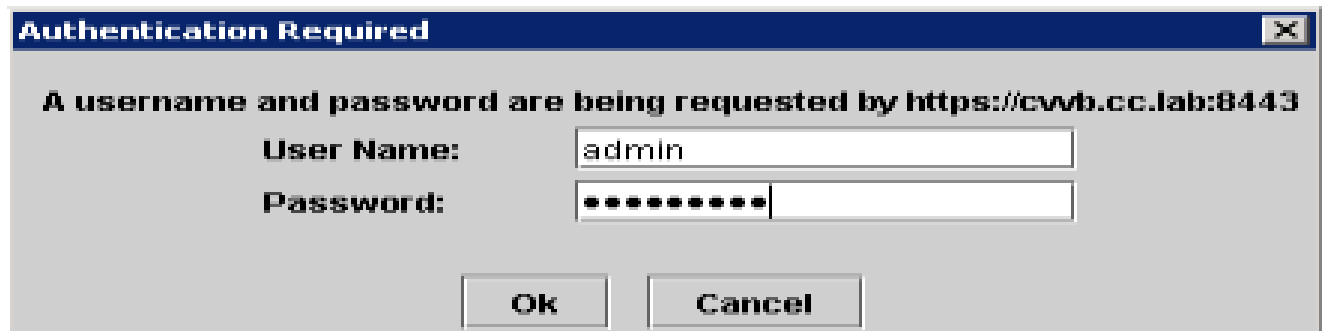
- Specificare l'indirizzo IP del VB e fare clic su **OK**.



- Accetta le informazioni sul certificato, se visualizzate



- Specificare le credenziali e fare clic su **OK**.

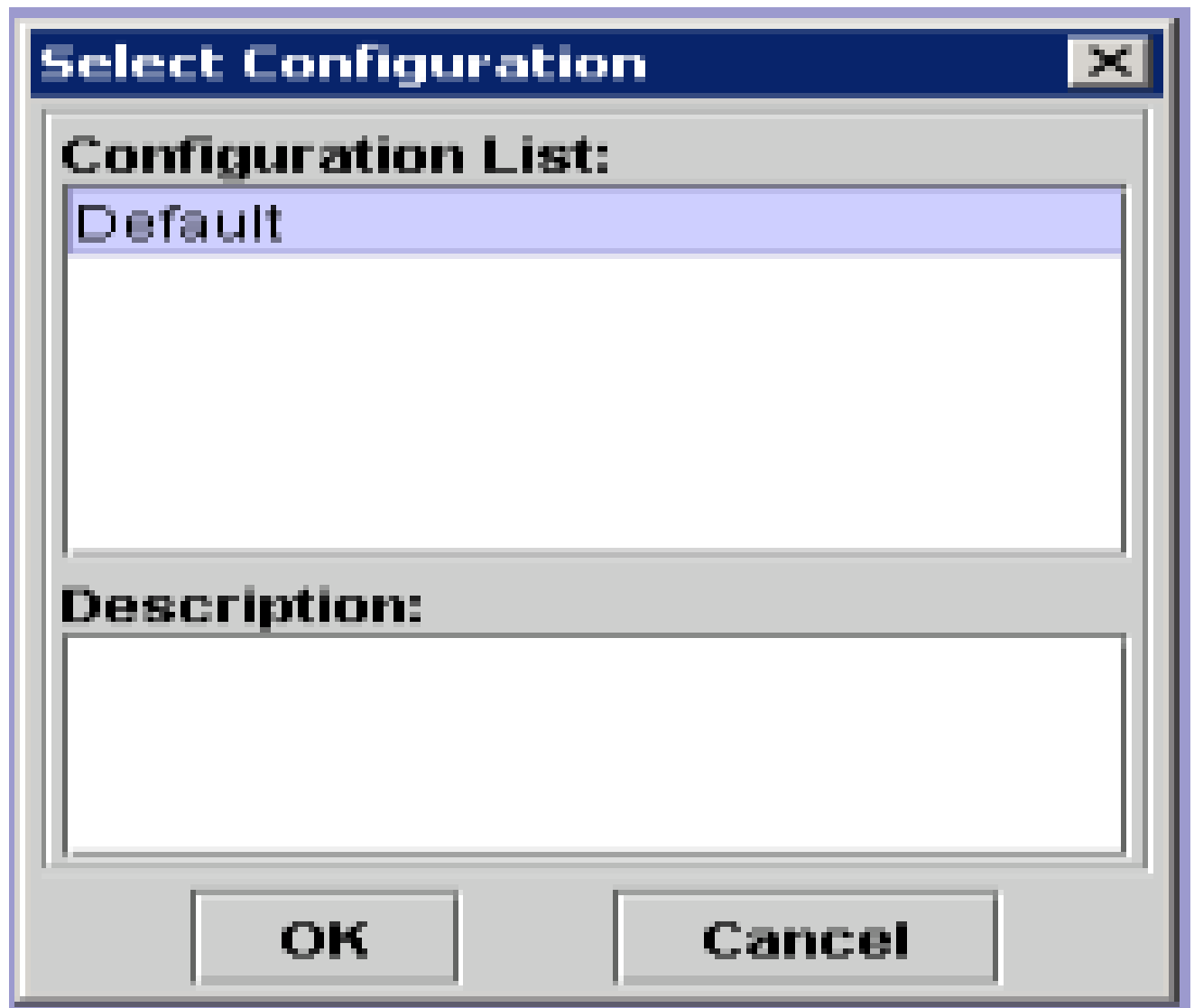


- Se è stato visualizzato il messaggio di errore Fuso orario, è possibile chiudere RTMT dopo aver fatto clic sul pulsante **Sì**. Riavviare lo strumento RTMT.



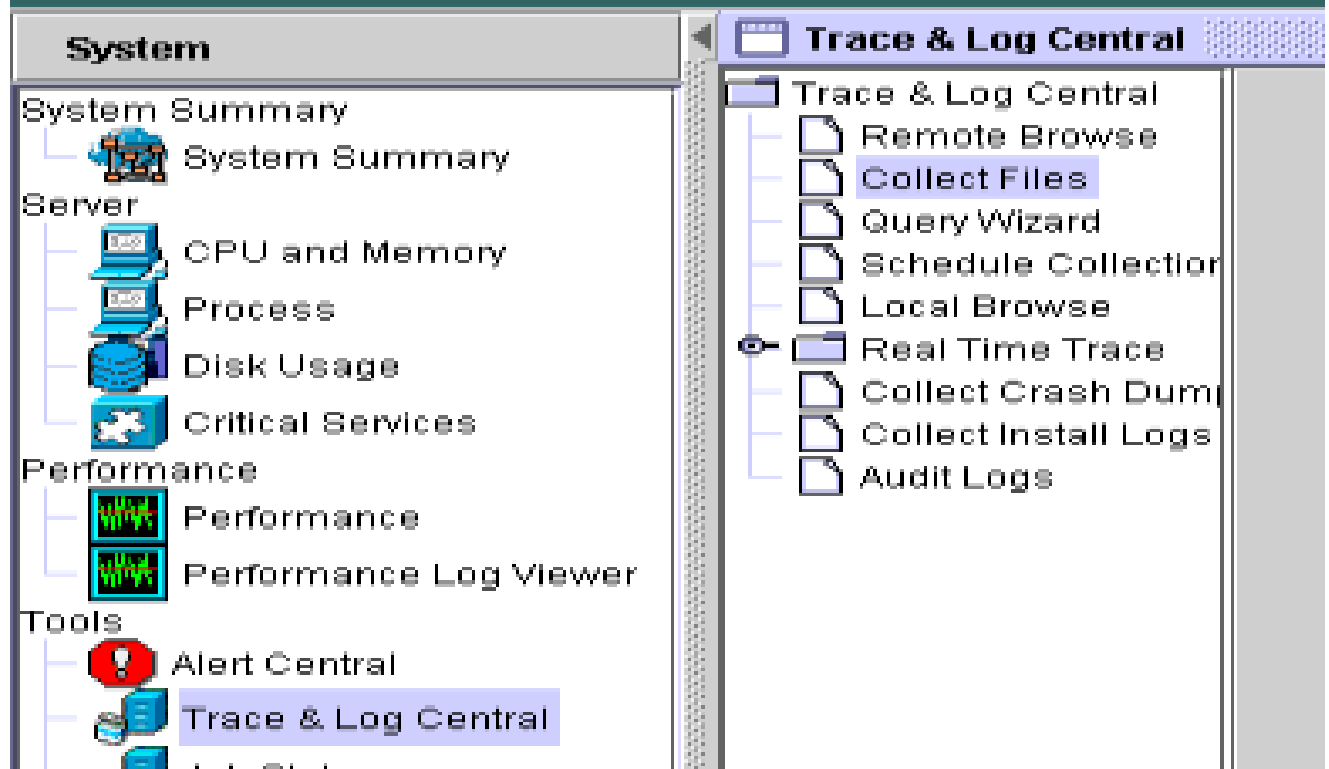


- Lasciare selezionata la configurazione di default e fare clic su **OK**.

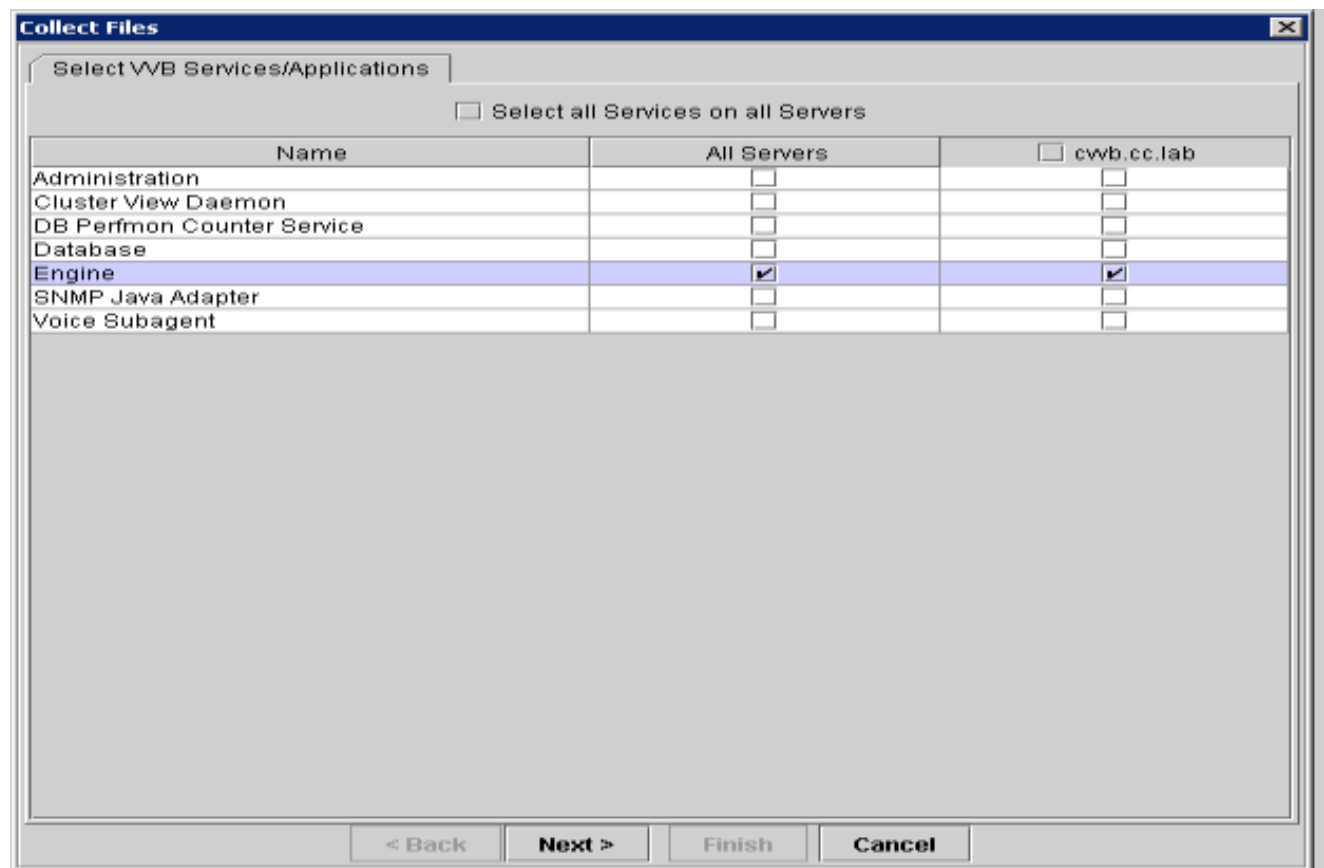


- Selezionare **Trace & Log Central**, quindi fare doppio clic su **Raccogli file**.

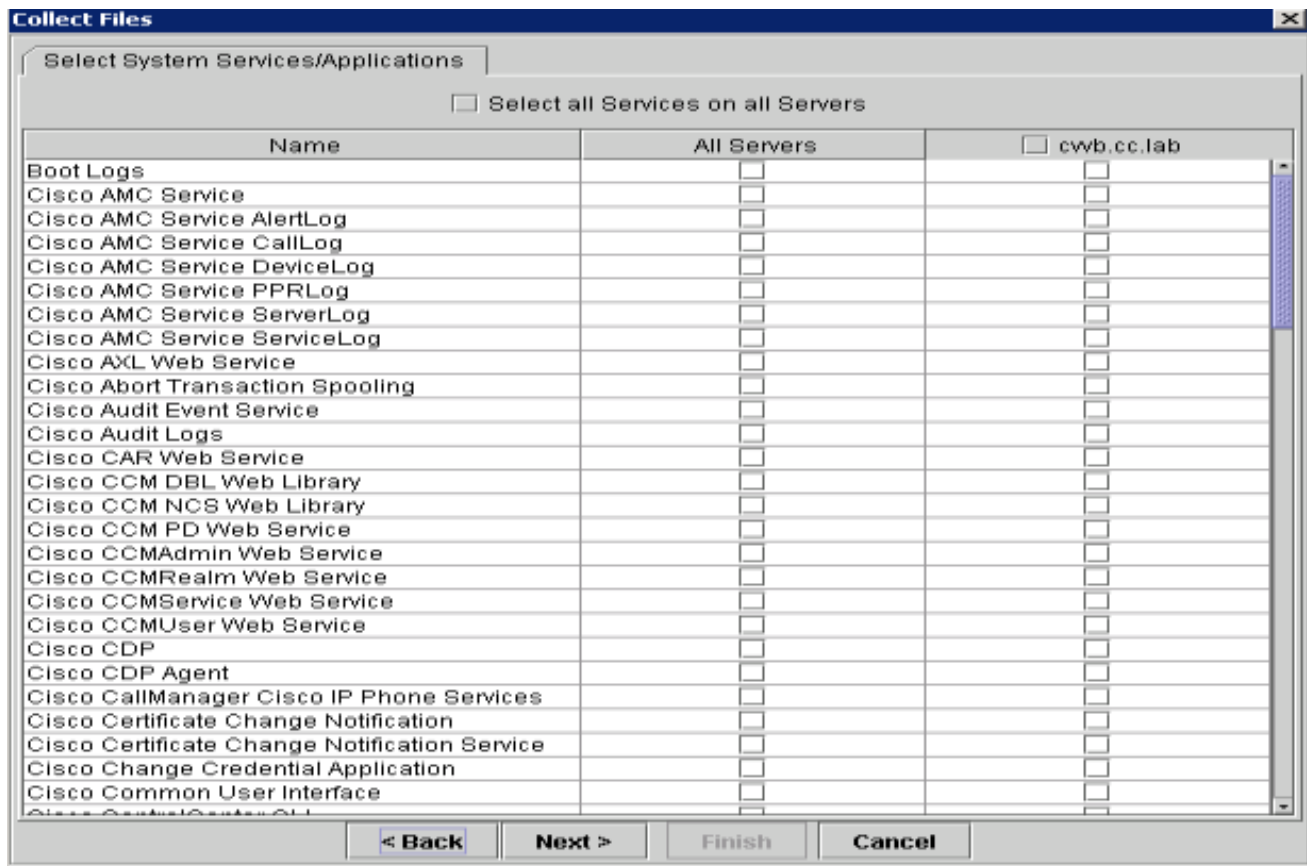
# Real Time Monitoring Tool For Cisco Virtualized Voice Browsers



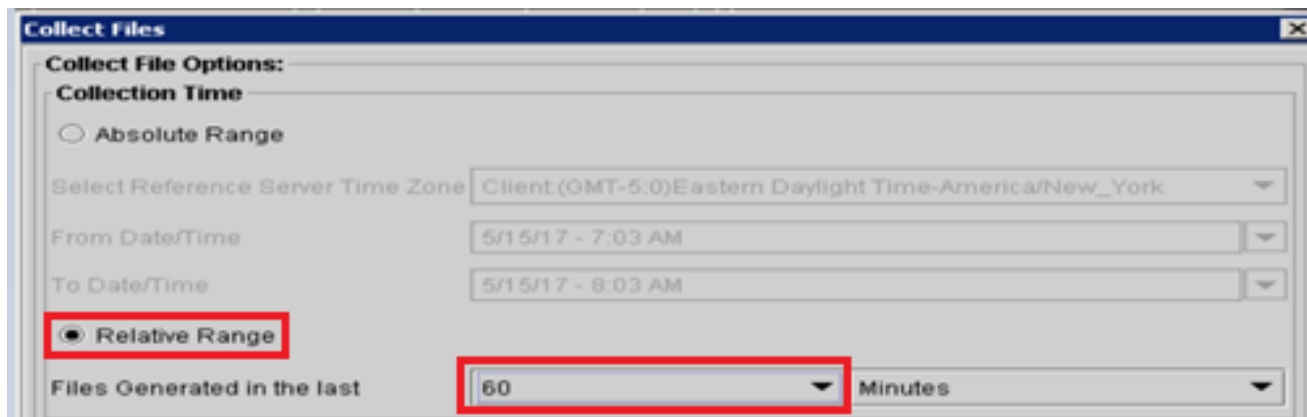
- Nella nuova finestra aperta, selezionare il Motore e fare clic su Avanti.



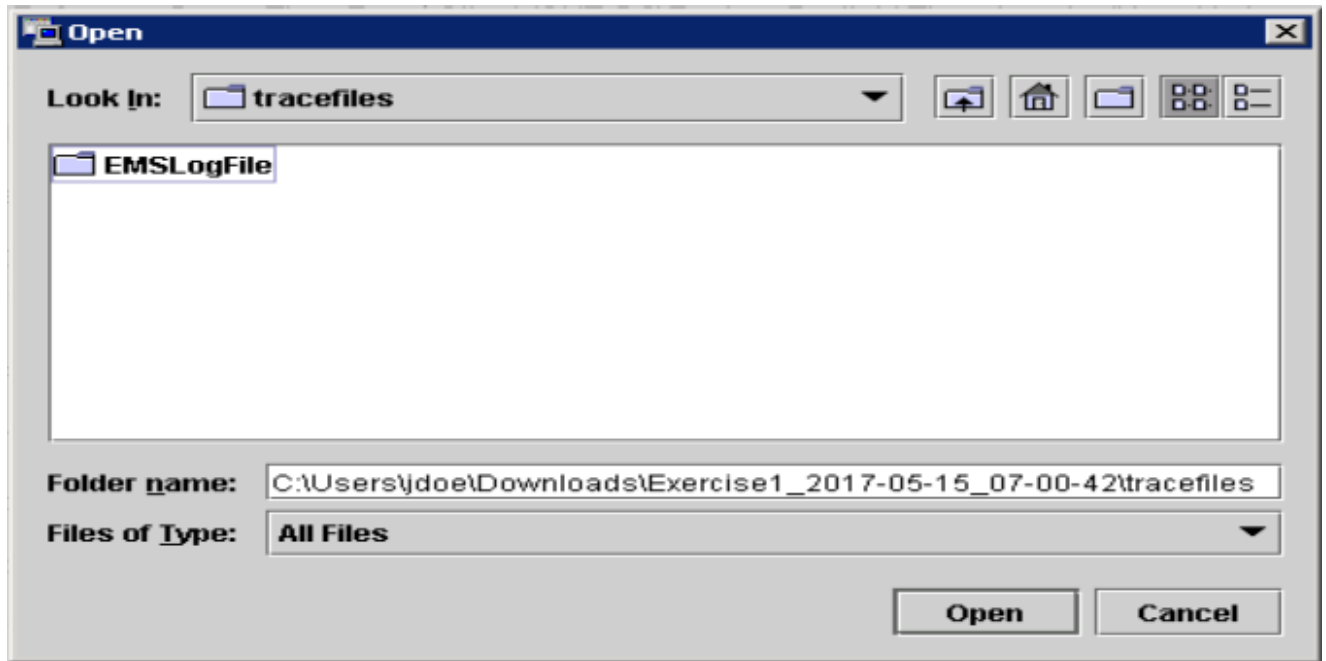
- Fare di nuovo clic su **Avanti** nella finestra successiva.



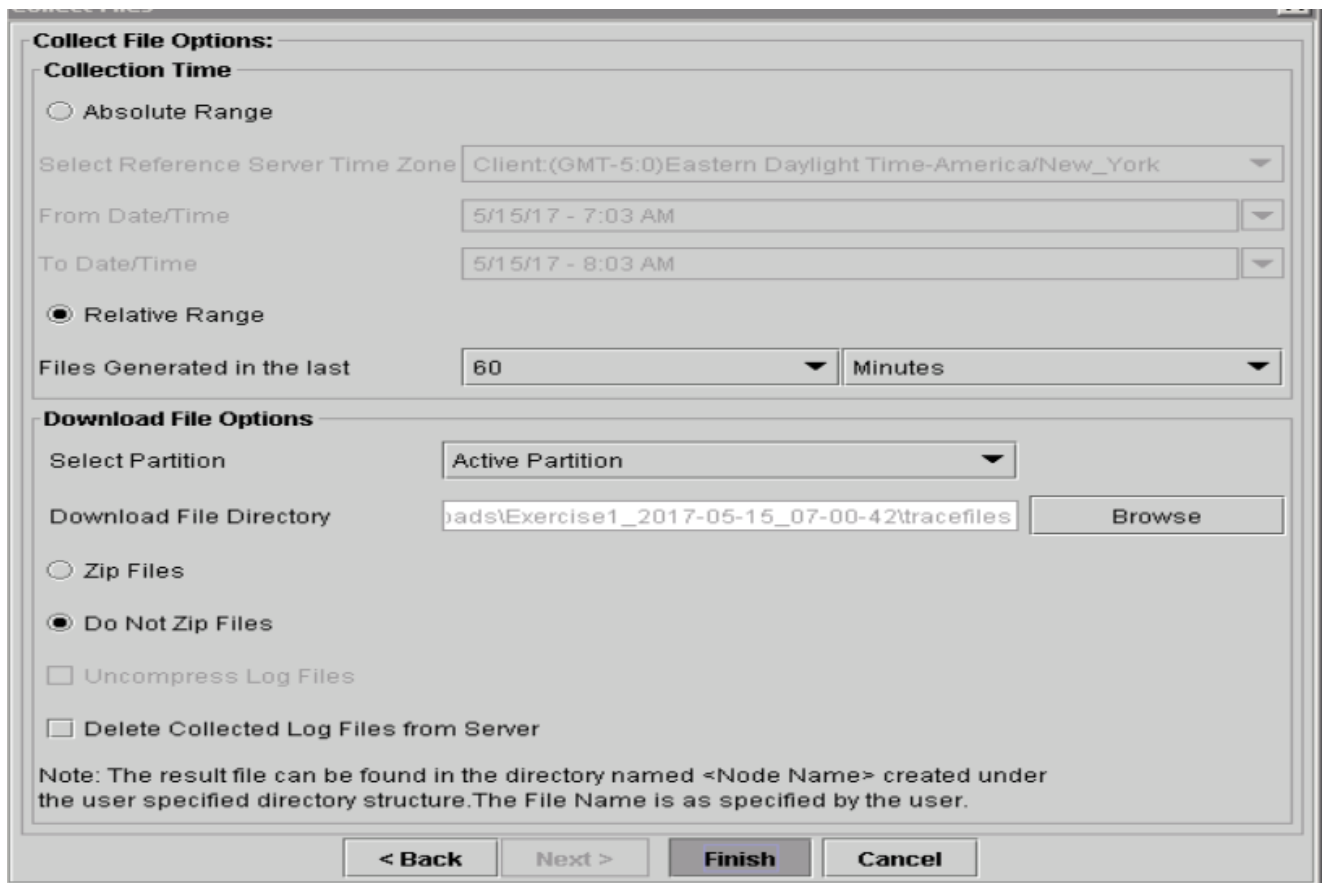
- Selezionare **Intervallo relativo** e assicurarsi di selezionare l'ora in cui coprire l'ora della chiamata non valida.



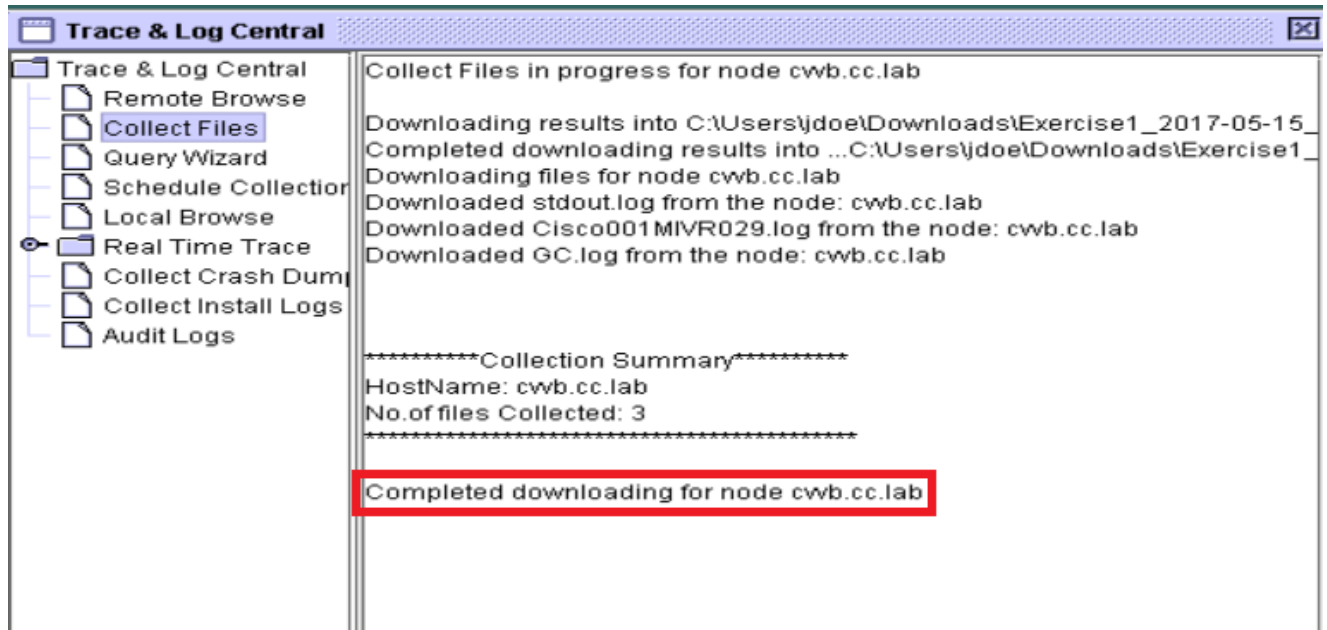
- In Opzioni download file fare clic su **Sfoggia**, selezionare la directory in cui si desidera salvare il file e quindi fare clic su **Apri**.



- Una volta selezionato tutto, fare clic su **Fine** pulsante.



- In questo modo vengono raccolti i file di registro. Attendere finché non viene visualizzato il messaggio di conferma in RTMT.



- Passare alla cartella in cui sono state salvate le tracce.
- I registri del motore sono tutto ciò che serve. Per trovarli, passare alla cartella `<timestamp>\uccx\log\MIVR`.

#### Opzione 2: tramite SSH e SFTP - Opzione consigliata

- Accedere al server VB con Secure Shell (SSH).
- Immettere questo comando per raccogliere i log necessari. I registri vengono compressi e viene richiesto di identificare il server

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

SFTP in cui vengono caricati. `file get activelog /uccx/log/MIVR/*`

- 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.

Impostazione di registri di traccia e raccolta per CUBE e CUSP

SIP (CUBE)

- 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 Cisco IOS® GW di produzione 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 i debug aggiuntivi se il GW raggiunge il 60%.

---

- Abilita questi debug:

```
debug voip ccapi inout
debug ccsip mess
```

After you make the call and simulate the issue, stop the debugging:

- Riprodurre il problema.

- Disabilitare le tracce.

```
#undebug all
```

- Raccogliere i registri.

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

## CUSPIDE

- Attiva le tracce SIP su CUSP.

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

- Riprodurre il problema.
- Al termine, disattivare la registrazione.

## Raccogli i log

- Configurare un utente sulla CUSP (ad esempio, test).
- Aggiungere questa configurazione al prompt CUSP.

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

- FTP all'indirizzo IP CUSP. Utilizzare il nome utente (test) e la password definiti nel passaggio precedente.
- Cambiare directory in /cusp/log/trace.
- Ottenere log\_<nomefile>.

Imposta traccia e raccogli log UCCE

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



**Nota:** per ulteriori informazioni su Diagnostic Framework Portico e System CLI, visitare il capitolo [Diagnostic tools](#) in the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, release 12.5(1).

Quando si risolvono i 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).

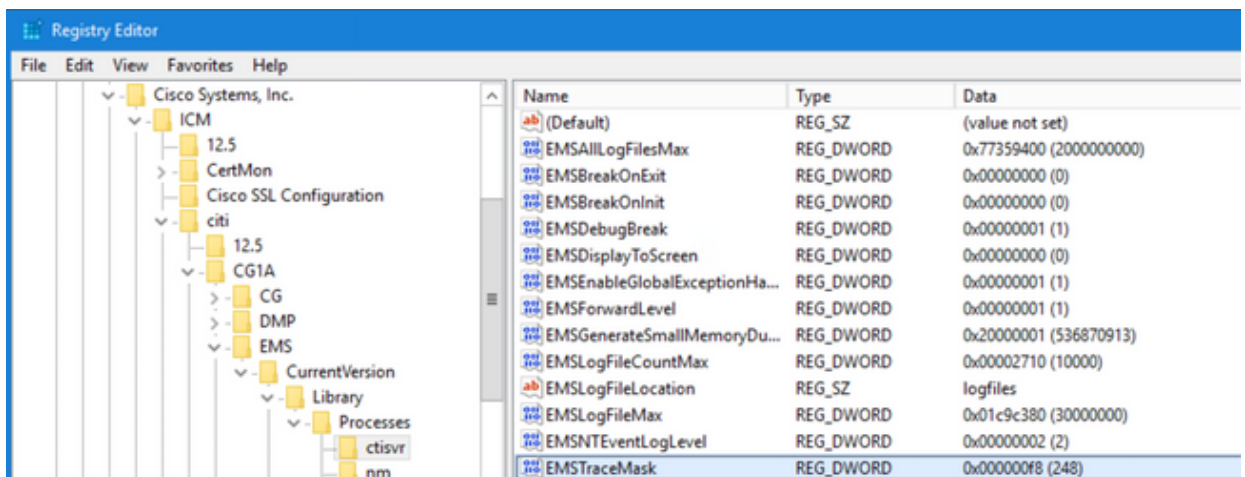


**Nota:** per ulteriori informazioni, visitare la sezione [Trace Level](#) nella guida alla disponibilità di Cisco Unified ICM/Contact Center Enterprise, versione 12.5(1).

Ad esempio, se si risolvono i problemi relativi a Dialer in uscita, il livello delle tracce deve essere impostato sul livello 2 se Dialer è occupato.

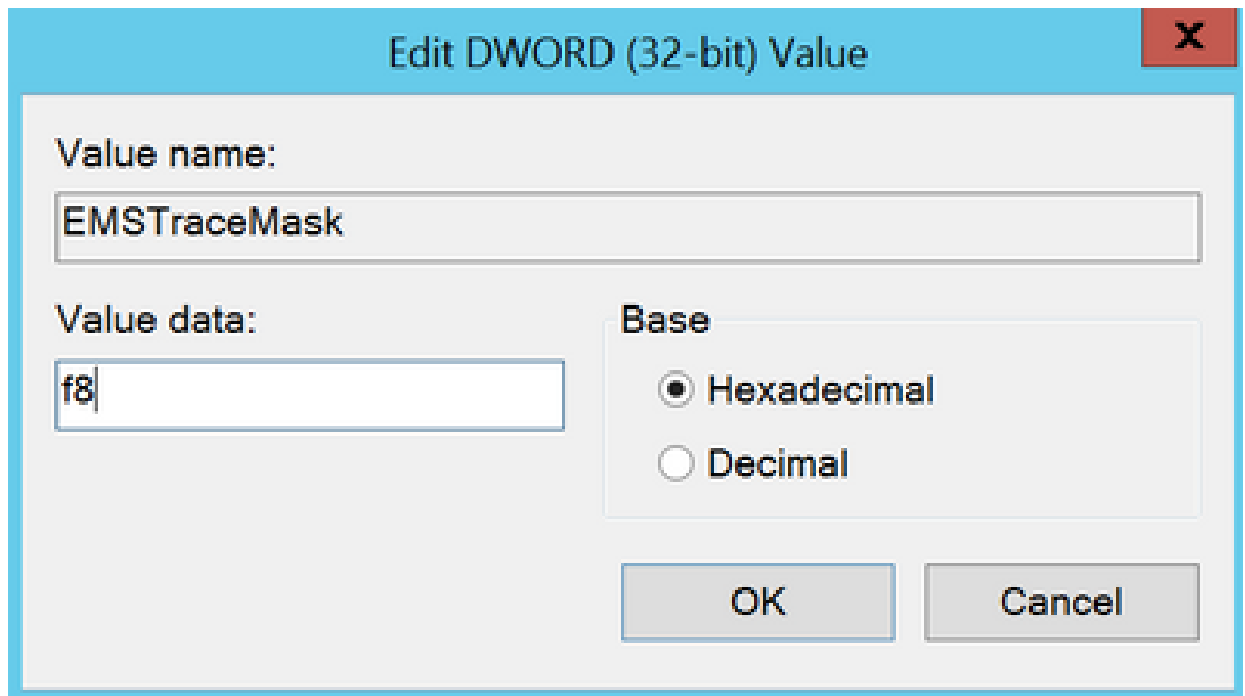
Per il CTISVR (CTISVR), il livello 2 e il livello 3 non impostano lo stesso livello del Registro di sistema consigliato da Cisco. Il registro di traccia consigliato per CTISVR è 0XF8.

1. In UCCE Agent PG, aprire l'Editor del Registro di sistema (Regedit).
2. Passare a **HKLM\software\Cisco Systems, Inc\icm<cust\_inst>\CG1(a e b)\EMS\CurrentVersion\library\Processes\ctisvr**.



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

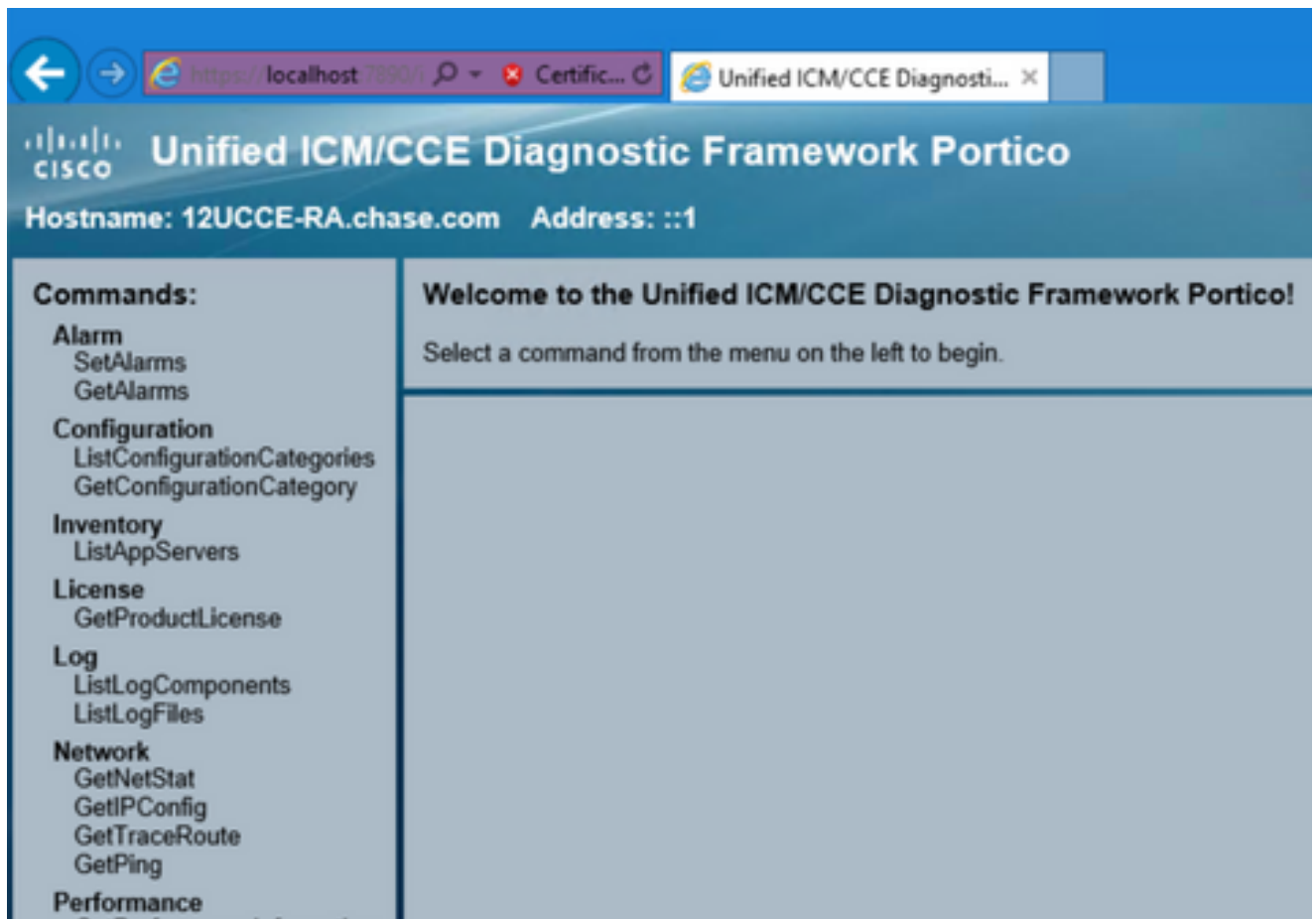




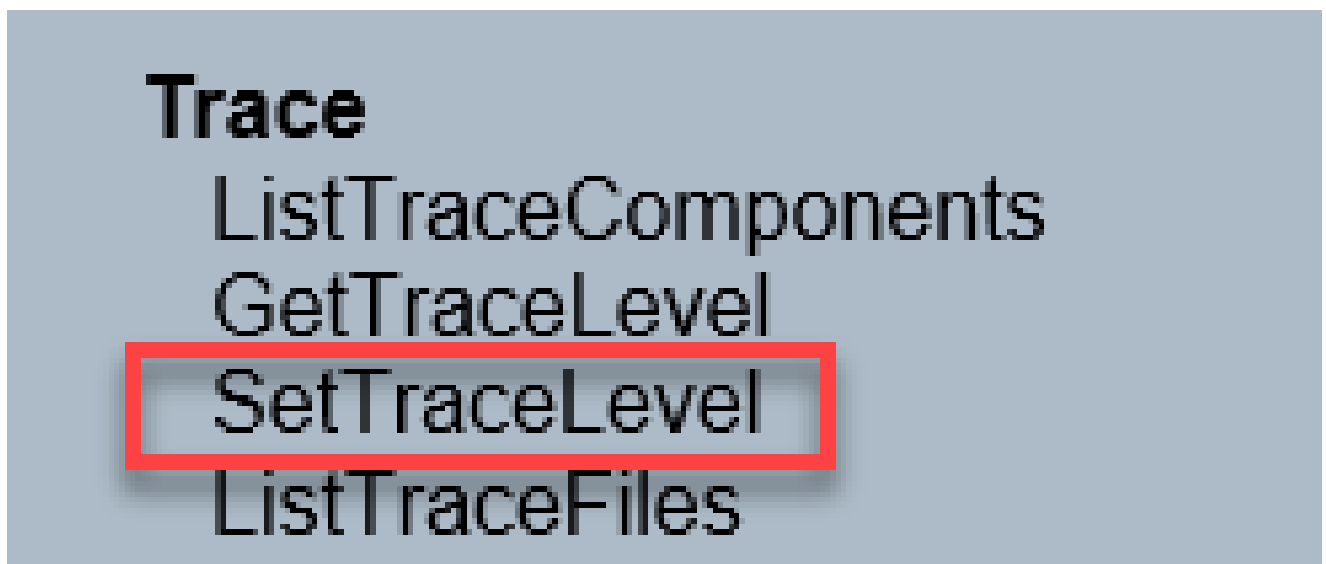
4. Fare clic su **Ok** e chiudere l'Editor del Registro di sistema. Di seguito viene riportata la procedura per impostare le tracce dei componenti UCCE (il processo RTR viene utilizzato come esempio).

#### **Imposta livello traccia**

- Aprire il Portico di Diagnostic Framework dal server in cui è necessario impostare le tracce ed eseguire l'accesso come utente Administrator.



- Nella sezione Comandi passare a **Trace**, quindi selezionare **SetTraceLevel**.



- Nella finestra **SetTraceLevel**, selezionare il **componente** e il **livello**.

- Fare clic su **Invia**. Al termine, verrà visualizzato il messaggio OK.

**⚠ Avvertenza:** impostare il livello delle tracce sul livello 3 durante il tentativo di riprodurre il problema. Dopo la riproduzione del problema, impostare il livello di traccia predefinito. Prestare particolare attenzione quando si impostano le tracce JTAPIGW, in quanto i livelli 2 e 3 impostano le tracce di livello basso, il che può avere 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

- Dal Portico Diagnostic Framework, nella sezione **Commands**, passare a **Trace** e selezionare **ListTraceFile**.

# Trace

ListTraceComponents

GetTraceLevel

SetTraceLevel

ListTraceFiles

- Nella finestra **ListTraceFile** selezionare il **componente**, **FromDate** e **ToDate**. Selezionare la **casella Mostra URL** e quindi fare clic su **Invia**.

The screenshot shows the Cisco Unified ICM-CCE-CCH Diagnostic Framework Portico interface. The browser address bar shows <https://localhost:7890>. The page title is "Unified ICM-CCE-CCH Diagnostic Framework Portico". The hostname is "Sprawler115.PCCEMEA.cisco.com" and the address is "::1".

The "ListTraceFiles" form is displayed with the following fields:

- Component:** Router A/rtr (highlighted with a red box)
- FromDate:** MM/DD/YYYY 1 / 8 / 2018 HH:MM:SS 12 : 0 : 0 AM Central Standard Time (UTC -6:00)
- ToDate:** MM/DD/YYYY 1 / 8 / 2018 HH:MM:SS 1 : 30 : 33 AM Central Standard Time (UTC -6:00)
- Use Tzadjustoff:** NO
- Show URL**
- 

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

The screenshot shows the Cisco Unified ICM/CCE Diagnostic Framework Portico interface. The browser address bar shows <https://localhost:7890>. The page title is "Unified ICM/CCE Diagnostic Framework Portico". The hostname is "12UCCE-RA.chase.com" and the address is "::1".

The "ListTraceFiles" form is displayed with the following fields:

- Component:** Router A/rtr
- FromDate:** MM/DD/YYYY 8 / 17 / 2022 HH:MM:SS 12 : 0 : 0 AM Central Standard Time (UTC -5:00)
- ToDate:** MM/DD/YYYY 8 / 17 / 2022 HH:MM:SS 12 : 23 : 41 PM Central Standard Time (UTC -5:00)
- Use Tzadjustoff:** NO
- Show URL**
- 

The "ListTraceFilesReply (OK)" message is displayed with the following content:

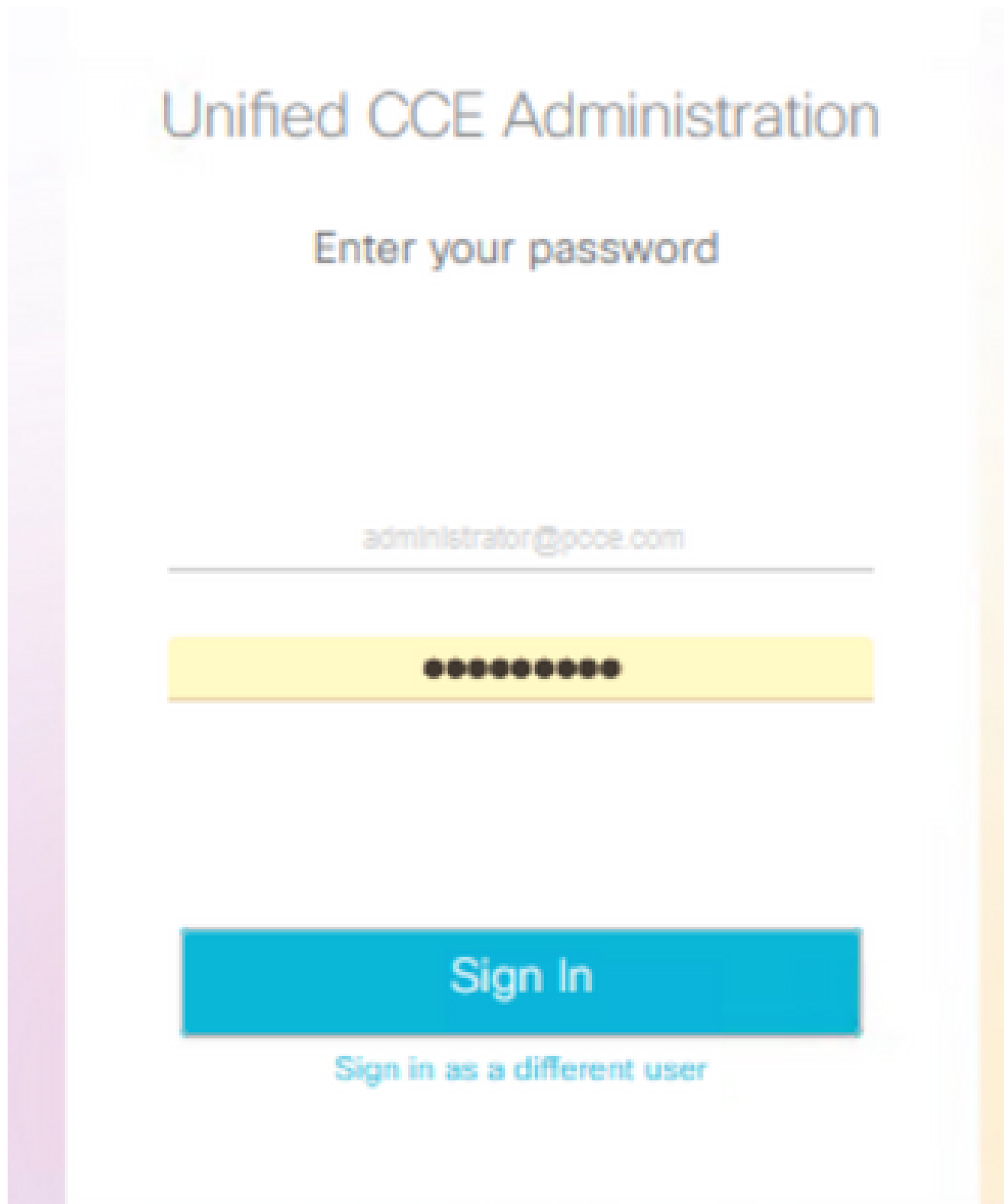
- [RouterA\[cti\]\\_rtr\\_20220817124205018\\_4176769.zip](#) (highlighted with a red box)
- Date: Wed Aug 17 2022 00:00:00 GMT-0500 (Central Daylight Time)

- Fare clic sul **collegamento** del file ZIP e **Salvare** il file nella posizione scelta.

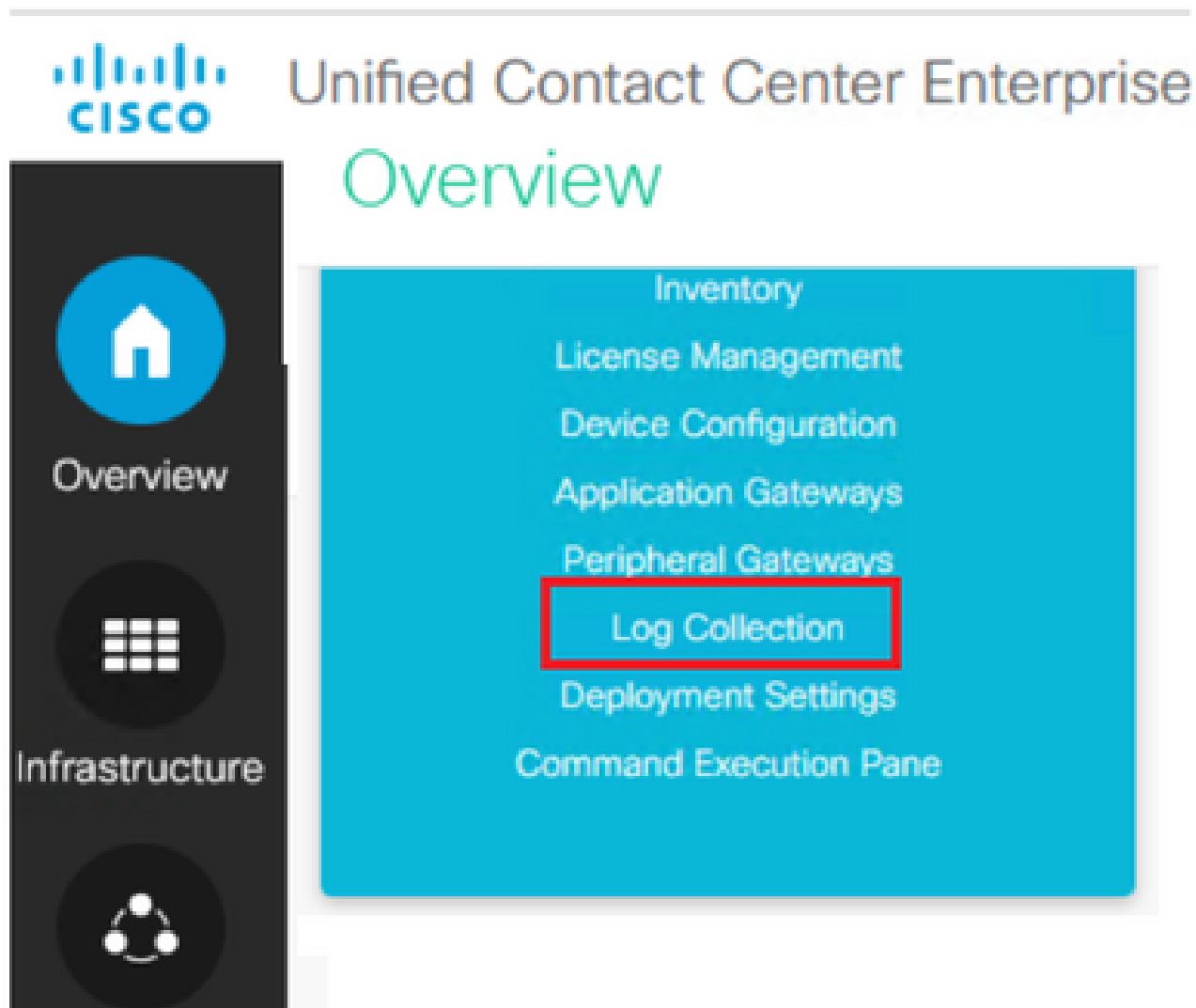
Imposta traccia e raccogli log PCCE

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.

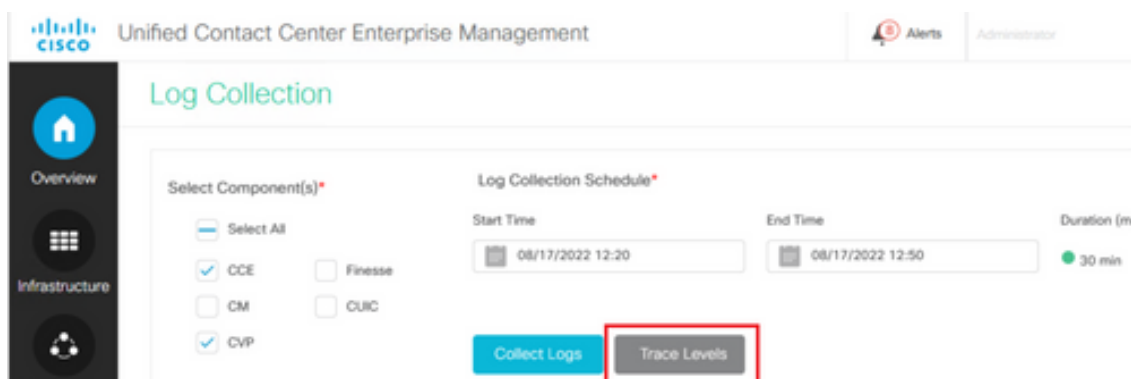
- Dal server PCCE AW, aprire lo strumento Unified CCE Web Administration e accedere all'account Administrator.



- Passare a **Panoramica** > **Impostazioni infrastruttura** > **Raccolta log** per aprire la pagina Raccolta log.



- Nella pagina Raccolta log fare clic su **Livelli di traccia** per aprire la finestra di dialogo **Livelli di traccia**.



- Impostare il livello di traccia su **Dettagliato** su CCE e lasciarlo come **Nessuna modifica** per CM e CVP, quindi fare clic su **Aggiorna livelli di traccia**.

### Trace Levels ✕

Component	Current Level	Set Level To
CCE	Normal	No Change
CM	Normal	No Change
CVP	Normal	No Change

- **Fare clic su Sì** per confermare l'avviso.



Changing trace levels could affect the performance. Are you sure you want to proceed?

- Una volta riprodotto il problema, aprire **Unified CCE Administration** e tornare a **System > Log Collection** (Sistema > **Raccolta log**).
- **Selezionare CCE e CVP** nel riquadro Componenti.
- Selezionare l'ora di raccolta del log appropriata (l'impostazione predefinita è gli ultimi 30 minuti).
- Fare clic su **Raccogli log** e su **Sì** per visualizzare l'avviso. Verrà avviata la raccolta dei log. Attendere qualche minuto prima che finisca.

Start Time	End Time	Duration	Components	Size	Status	Actions
08/17/2022 12:25	08/17/2022 12:55	30 min	CCE, CVP	1.8 MB		

- Al termine, fare clic sul pulsante **Download** nella colonna **Actions** (Azioni) per scaricare un file compresso con tutti i log in esso contenuti. **Salvare il file zip** nella posizione appropriata.

Imposta traccia e raccogli registri CUIC/Live Data/IDS

Download dei log con SSH

- Accedere alla riga di comando SSH (CLI) di CUIC, LD e IDS.
- Eseguire il comando per raccogliere i log relativi a CUIC.

```
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
```

- Eseguire il comando per raccogliere i log relativi a LD.

```
file get activelog livedata/logs/*.*
```

- Eseguire il comando per raccogliere i log relativi all'IDS.

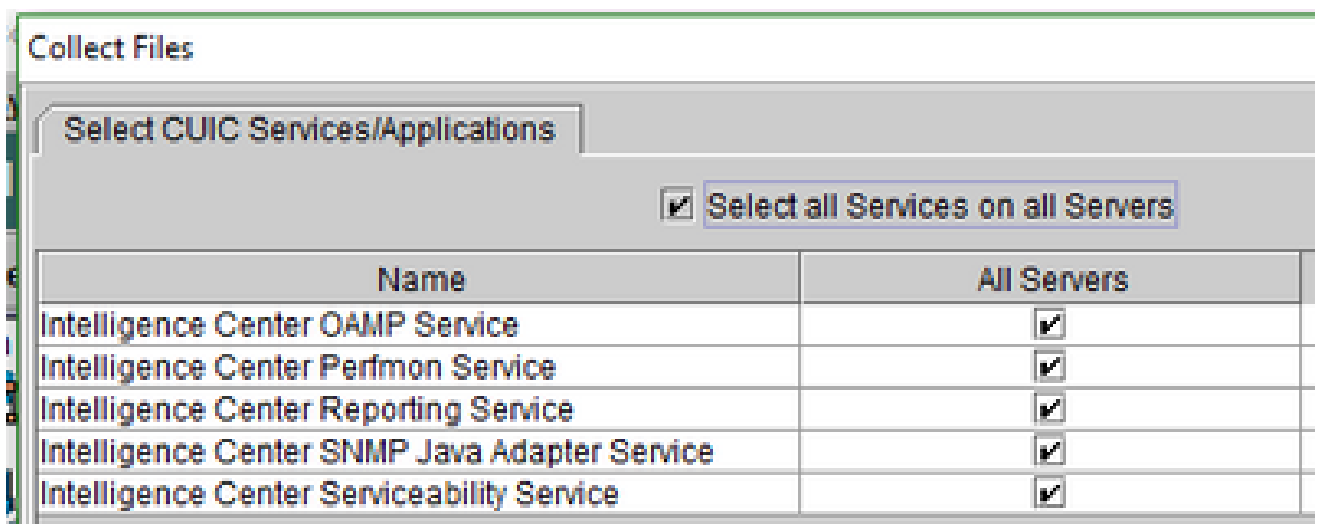
```
file get activelog ids/log/*.* recurs compress reltime days 1
```

- 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.

### Scarica log con RTMT

- Scaricare RTMT dalla pagina OAMP. Accedere a <https://<HOST ADDRESS>/oamp> dove **HOST ADDRESS** è l'indirizzo IP del server.
- Passare a **Strumenti > RTMT plugin download**. Scaricare e installare il plug-in.
- Avviare RTMT e accedere al server con le credenziali di amministratore.
- Fare doppio clic su **Trace and Log Central** e quindi su **Collect Files**.
- È possibile visualizzare queste schede per i servizi specifici. È necessario selezionare tutti i servizi/server per CUIC, LD e IDS.

Per CUIC:





Per LD:

**Collect Files**

Select LiveData Services/Applications

Select all Services on all Servers

Name	All Servers
CCE Live Data ActiveMQ Service	<input checked="" type="checkbox"/>
CCE Live Data Cassandra Service	<input checked="" type="checkbox"/>
CCE Live Data NGINX Service	<input checked="" type="checkbox"/>
CCE Live Data Socket.IO Service	<input checked="" type="checkbox"/>
CCE Live Data Storm Services	<input checked="" type="checkbox"/>
CCE Live Data Web Service	<input checked="" type="checkbox"/>
CCE Live Data Zookeeper Service	<input checked="" type="checkbox"/>

Per IDS:

**Collect Files**

Select IdS Services/Applications

Select all Services on all Servers

Name	All Servers
Cisco Identity Service	<input checked="" type="checkbox"/>

Per i servizi di piattaforma, è in genere consigliabile selezionare i registri **Tomcat** e **Visualizzatore eventi**:

## Collect Files

### Select System Services/Applications

Select all Services on all Servers

Name	All Servers
Cisco Serviceability Reporter CallActivitiesReport	<input type="checkbox"/>
Cisco Serviceability Reporter DeviceReport	<input type="checkbox"/>
Cisco Serviceability Reporter PPRReport	<input type="checkbox"/>
Cisco Serviceability Reporter ServerReport	<input type="checkbox"/>
Cisco Serviceability Reporter ServiceReport	<input type="checkbox"/>
Cisco Stored Procedure Trace	<input type="checkbox"/>
Cisco Syslog Agent	<input type="checkbox"/>
Cisco Tomcat	<input checked="" type="checkbox"/>
Cisco Tomcat Security Logs	<input type="checkbox"/>
Cisco Tomcat Stats Servlet	<input type="checkbox"/>
Cisco Trace Collection Service	<input type="checkbox"/>
Cisco Trust Verification Service	<input type="checkbox"/>
Cisco UXL Web Service	<input type="checkbox"/>
Cisco Unified Mobile Voice Access Service	<input type="checkbox"/>
Cisco Unified OS Admin Web Service	<input type="checkbox"/>
Cisco Unified OS Platform API	<input type="checkbox"/>
Cisco Unified Reporting Web Service	<input type="checkbox"/>
Cisco User Data Services	<input type="checkbox"/>
Cisco WebDialer Web Service	<input type="checkbox"/>
Cisco WebDialerRedirector Web Service	<input type="checkbox"/>
Cron Logs	<input type="checkbox"/>
Event Viewer-Application Log	<input checked="" type="checkbox"/>
Event Viewer-System Log	<input checked="" type="checkbox"/>
FIPS Logs	<input type="checkbox"/>

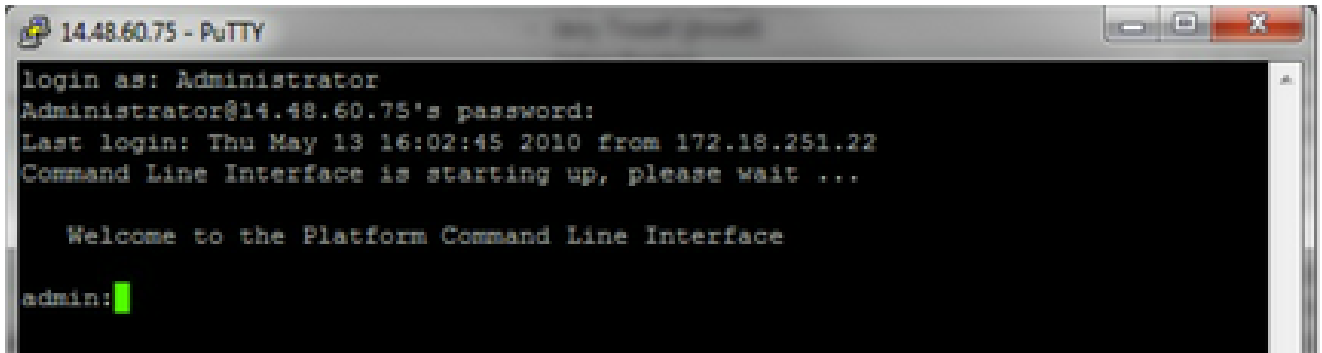
- Selezionare **Data e ora** insieme alla cartella di destinazione per **salvare** i registri.

### Acquisizione pacchetti su VoS (Finesse, CUIC, VB)

- Avvia l'acquisizione

Per avviare l'acquisizione, stabilire una sessione SSH sul server VOS da autenticare con l'account di amministratore della piattaforma.

-



```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Thu May 13 16:02:45 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

admin:█
```

1 bis. Sintassi dei comandi

Il comando è **utils network capture** e la sintassi è:

<#root>

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

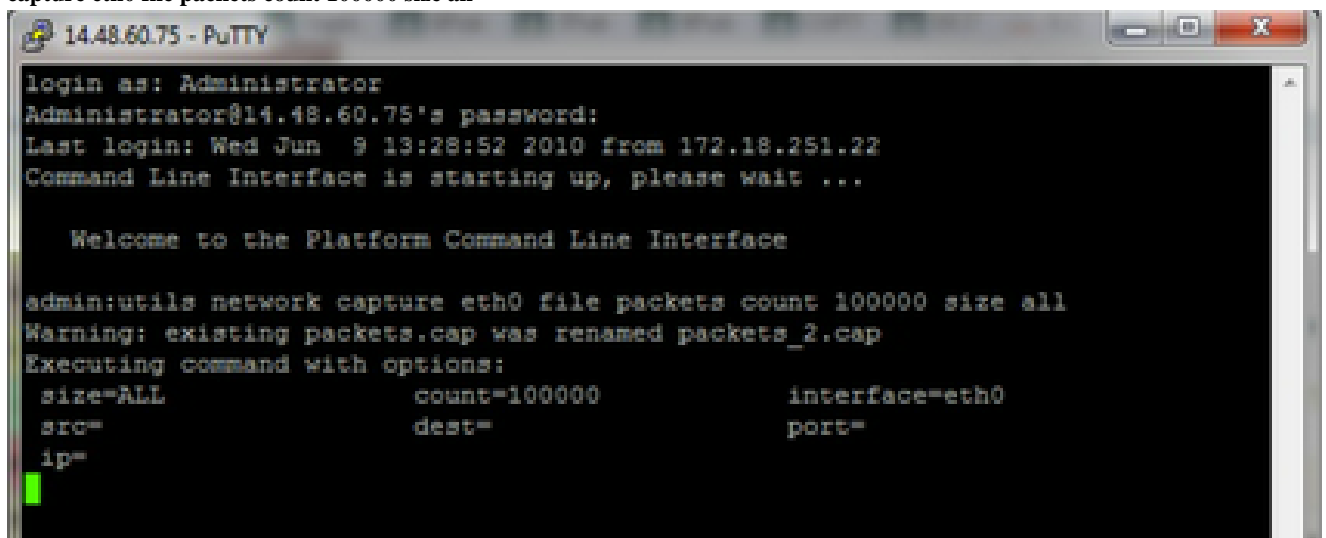
port

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"

I ter. Acquisisci tutti i traffici

Per un'acquisizione tipica, è possibile raccogliere TUTTI i pacchetti di tutte le dimensioni da e verso l'indirizzo ALL in un file di acquisizione denominato **packets.cap**. Per eseguire questa operazione, è sufficiente utilizzare la CLI di amministrazione **utils network capture eth0 file packets count 100000 size all**



```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun  9 13:28:52 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

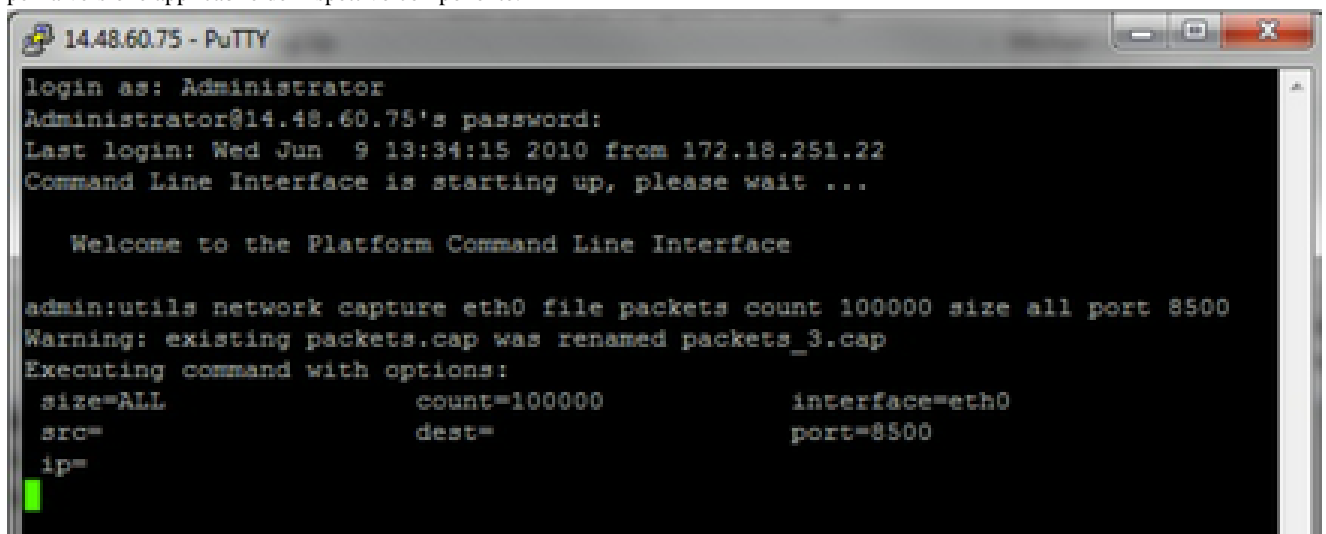
Welcome to the Platform Command Line Interface

admin:utils network capture eth0 file packets count 100000 size all
Warning: existing packets.cap was renamed packets_2.cap
Executing command with options:
  size=ALL          count=100000      interface=eth0
  src=              dest=              port=
  ip=
```

I quater. Acquisizione basata sul numero di porta

Per risolvere un problema di comunicazione con Cluster Manager, è possibile utilizzare l'opzione della porta per acquisire i dati in base a una porta specifica (8500).

Per ulteriori informazioni sui servizi che richiedono comunicazioni su ciascuna porta, consultare [la guida all'uso delle porte TCP e UDP](#) per la versione applicabile del rispettivo componente.



```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun  9 13:34:15 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

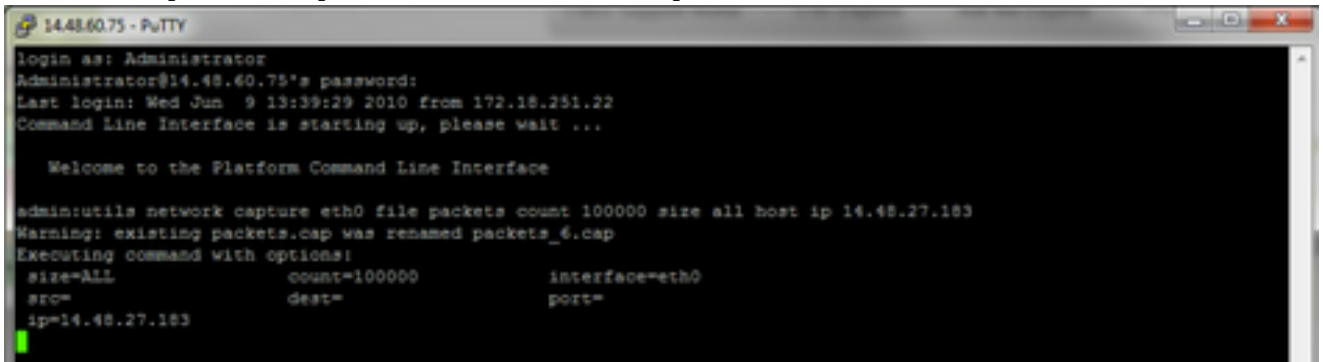
Welcome to the Platform Command Line Interface

admin:utils network capture eth0 file packets count 100000 size all port 8500
Warning: existing packets.cap was renamed packets_3.cap
Executing command with options:
  size=ALL          count=100000      interface=eth0
  src=              dest=              port=8500
  ip=
```

I quinquies. Acquisizione basata su host

Per risolvere un problema relativo a VOS e a un host specifico, può essere necessario utilizzare l'opzione 'host' per filtrare il traffico da e verso un host specifico.

Può anche essere necessario escludere un determinato host, in questo caso utilizzare un punto interrogativo (!) davanti all'indirizzo IP.  
**utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**



```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun  9 13:39:29 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

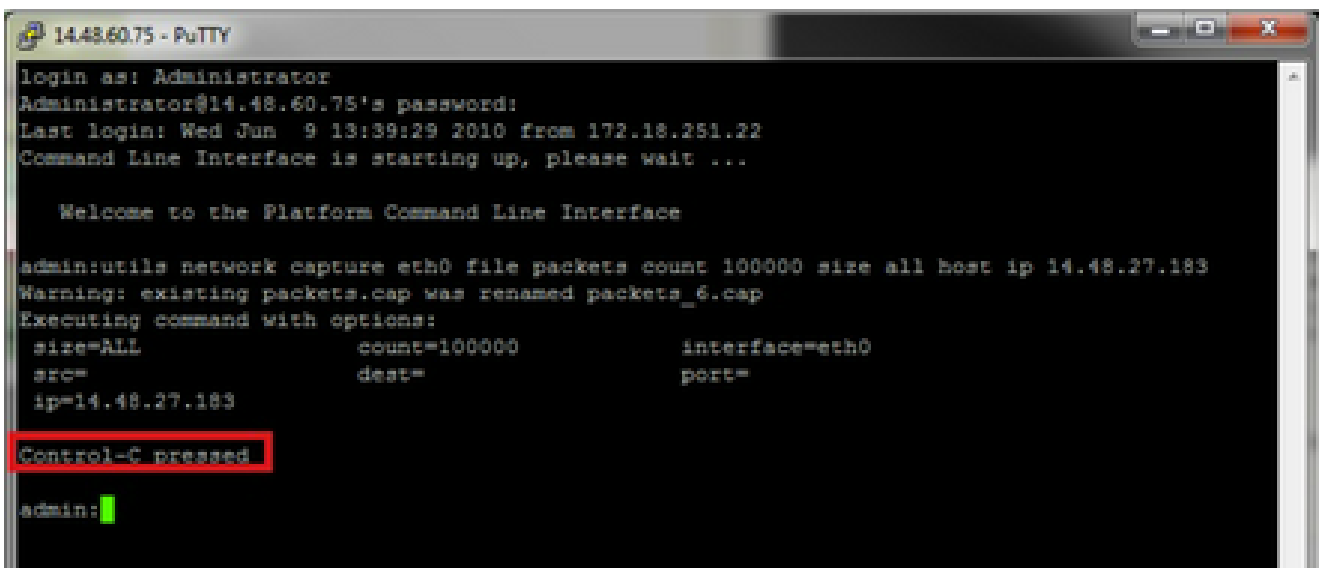
admin:utils network capture eth0 file packets count 100000 size all host ip 14.48.27.183
Warning: existing packets.cap was renamed packets_6.cap
Executing command with options:
size=ALL          count=100000      interface=eth0
src=              dest=            port=
ip=14.48.27.183
```

- Riprodurre il sintomo del problema

Durante l'acquisizione viene avviata la riproduzione del sintomo o della condizione di problema, in modo che i pacchetti necessari vengano inclusi nell'acquisizione. Se il problema è intermittente, può essere necessario eseguire l'acquisizione per un periodo di tempo esteso. Se l'acquisizione termina, è perché il buffer è pieno. Riavviate l'acquisizione e l'acquisizione precedente viene rinominata automaticamente in modo da non perdere l'acquisizione precedente. Se l'acquisizione è necessaria per un lungo periodo di tempo, utilizzare una sessione di monitoraggio su uno switch per l'acquisizione a livello di rete.

- Arresta l'acquisizione

Per interrompere la cattura, tenere premuto il tasto **Control** e premere C sulla tastiera. In questo modo, il processo di acquisizione viene terminato e non vengono aggiunti nuovi pacchetti al dump di acquisizione.



```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun  9 13:39:29 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

admin:utils network capture eth0 file packets count 100000 size all host ip 14.48.27.183
Warning: existing packets.cap was renamed packets_6.cap
Executing command with options:
size=ALL          count=100000      interface=eth0
src=              dest=            port=
ip=14.48.27.183
Control-C pressed
admin:
```

Al termine, un file di acquisizione viene archiviato sul server nel percorso 'activelog platform/cli/'

- Raccogli l'acquisizione dal server

I file di acquisizione vengono archiviati nella piattaforma ActiveLog/cli/ sul server. È possibile trasferire i file tramite CLI a un server

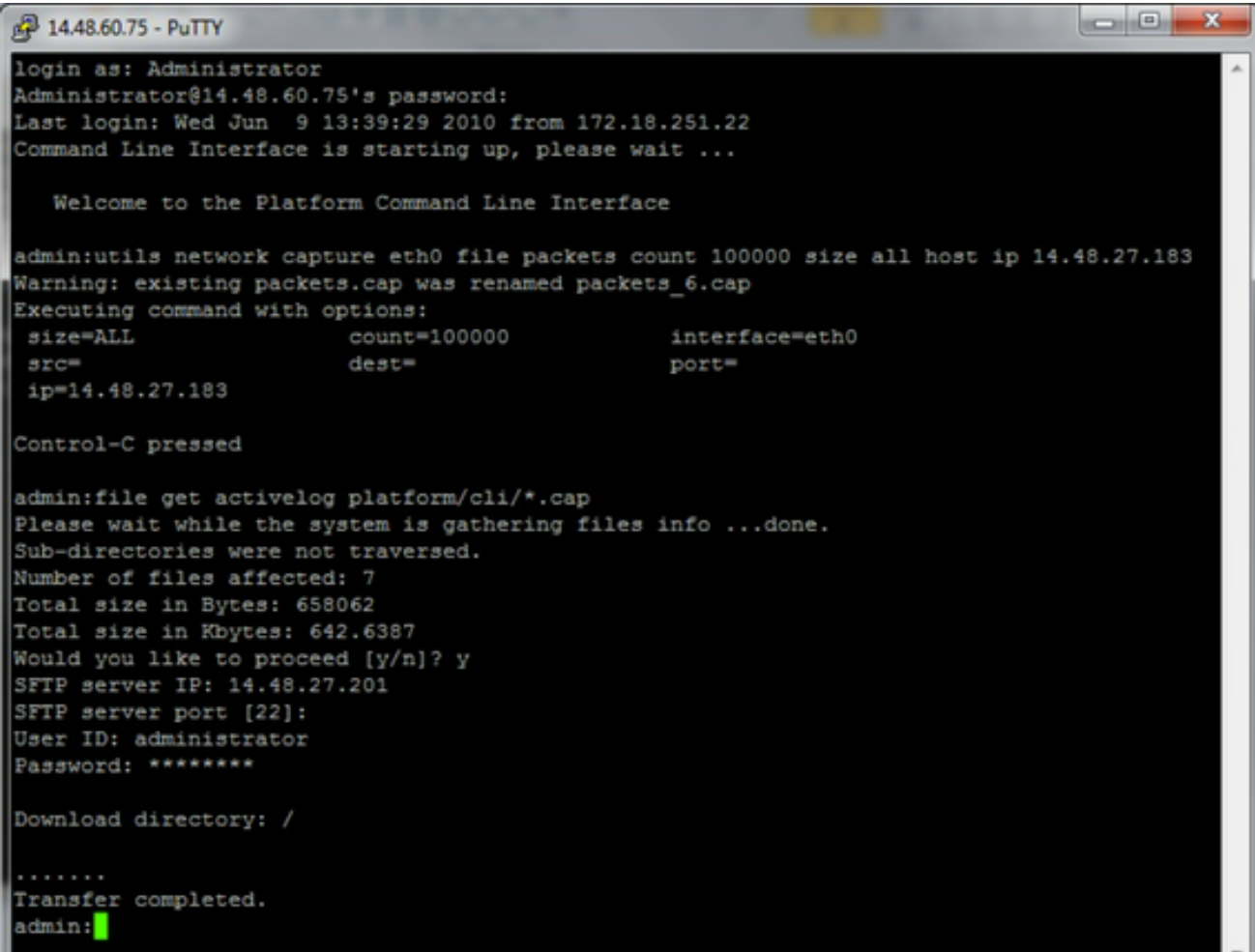
SFTP o al PC locale con RTMT.

4 bis. Trasferire il file di acquisizione dalla CLI a un server SFTP

Usare il comando **file get activelog platform/cli/packets.cap** per raccogliere il file packets.cap sul server SFTP.

In alternativa, raccogliere tutti i file .cap memorizzati sul server, utilizzare il file **get activelog platform/cli/\*.cap**.

Infine, immettere le informazioni relative all'IP/FQDN, alla porta, al nome utente, alla password e alla directory del server SFTP:



```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun  9 13:39:29 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

admin:utils network capture eth0 file packets count 100000 size all host ip 14.48.27.183
Warning: existing packets.cap was renamed packets_6.cap
Executing command with options:
  size=ALL          count=100000          interface=eth0
  src=              dest=              port=
  ip=14.48.27.183

Control-C pressed

admin:file get activelog platform/cli/*.cap
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 7
Total size in Bytes: 658062
Total size in Kbytes: 642.6387
Would you like to proceed [y/n]? y
SFTP server IP: 14.48.27.201
SFTP server port [22]:
User ID: administrator
Password: *****

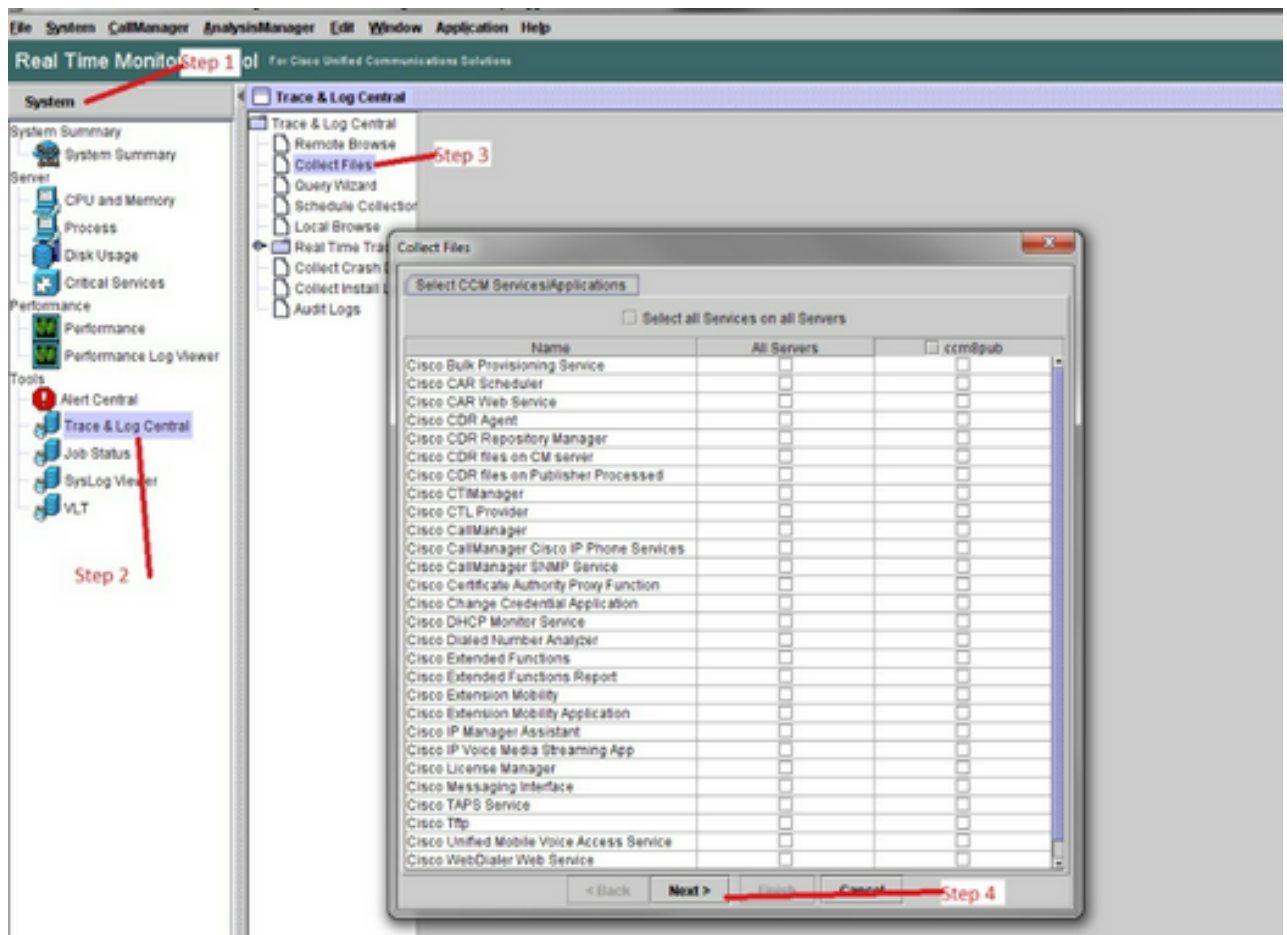
Download directory: /

.....
Transfer completed.
admin:█
```

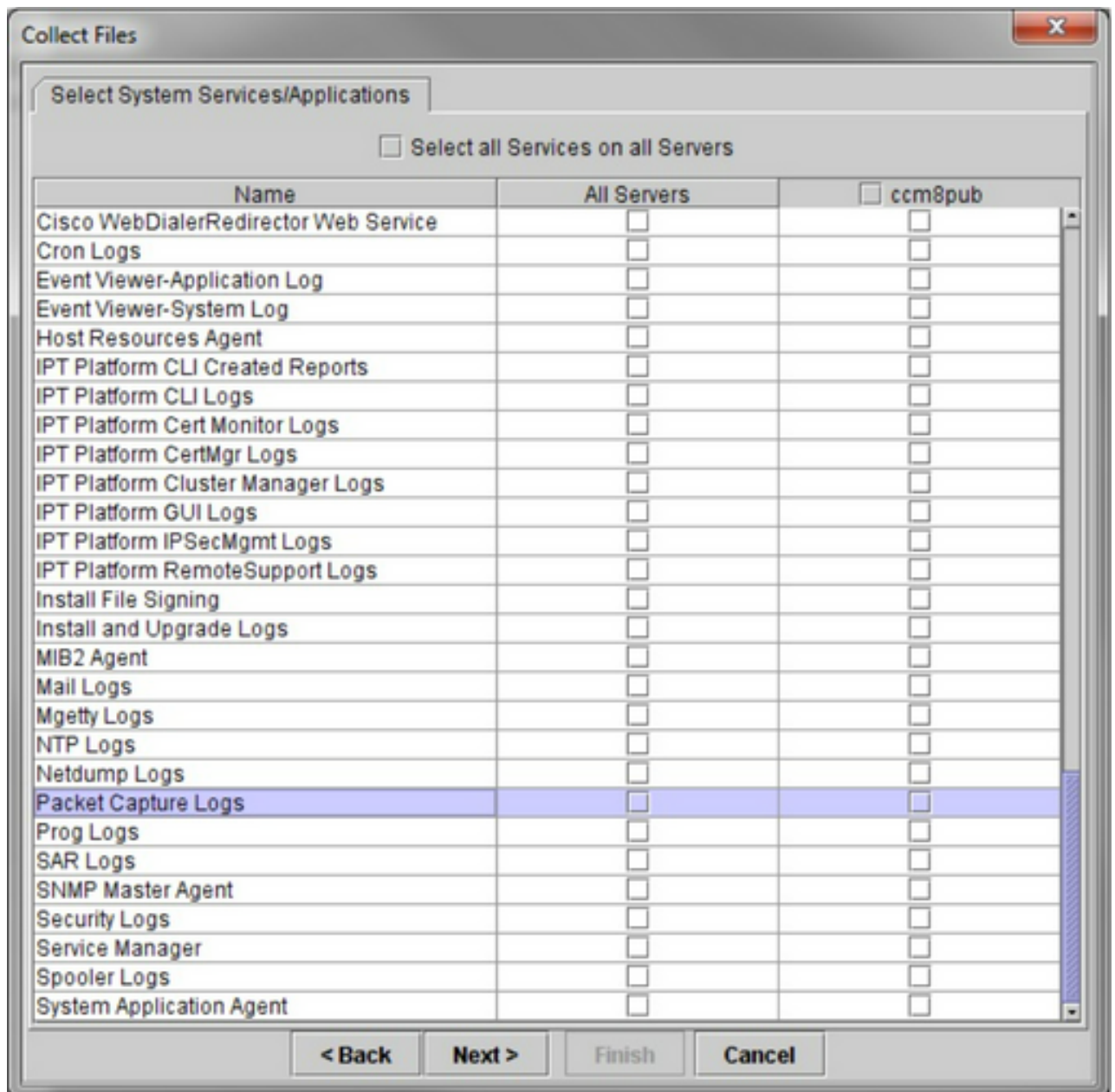
La CLI indica l'esito positivo o negativo del trasferimento di file al server SFTP.

4 ter. Utilizzare RTMT per trasferire un file di acquisizione su un PC locale.

Avviare RTMT. Se non è installato sul PC locale, installare la versione appropriata dalla pagina Amministrazione di VOS, quindi selezionare il menu **Applicazioni > Plugin**. Fare clic su **System, Trace & Log Central**, quindi fare doppio clic su **Collect Files**. Fare clic su **Avanti** nel primo menu.

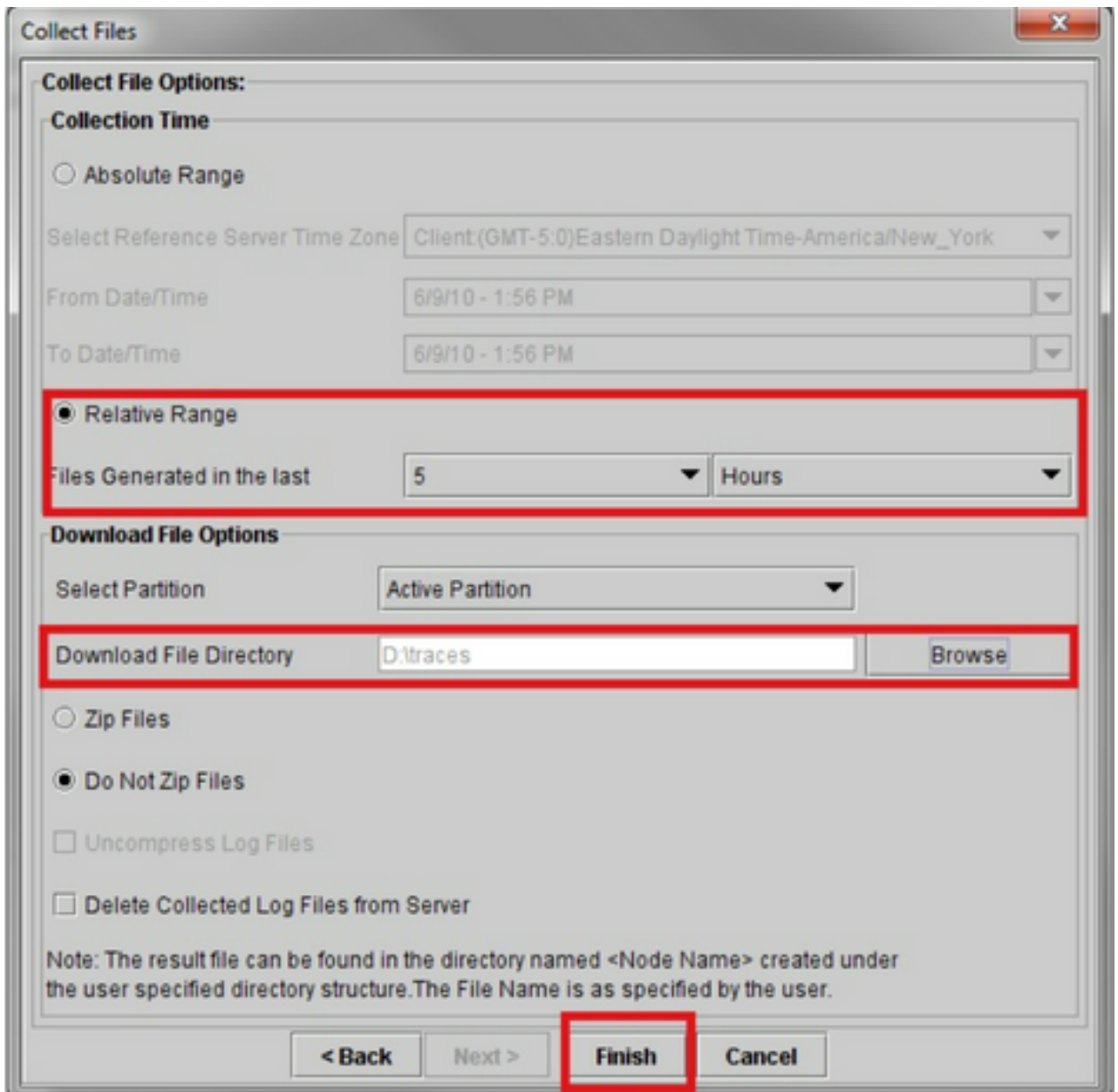


Nel secondo menu, scegliere la casella di controllo **Registri acquisizione pacchetti** sul server su cui è stata eseguita l'acquisizione, quindi fare clic su **Avanti**.



Nella schermata finale, scegliere un intervallo di tempo in cui è stata eseguita la cattura e una directory di download sul PC locale.





RTMT chiude questa finestra e procede a raccogliere il file e a memorizzarlo sul PC locale nella posizione specificata.

## 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).