

在CCE中設定跟蹤和收集日誌

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定跟蹤和收集Finesse日誌](#)

[Finesse使用者端](#)

[選項1:通過傳送錯誤報告收集客戶端日誌。](#)

[選項2:設定永續性日誌記錄](#)

[Finesse伺服器](#)

[設定跟蹤並收集CVP和CVVB日誌](#)

[CVP通話伺服器](#)

[CVP語音XML\(VXML\)應用程式](#)

[CVP營運和管理入口網站\(OAMP\)](#)

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

[為CUBE和CUSP設定跟蹤和收集日誌](#)

[CUBE\(SIP\)](#)

[CUSP](#)

[設定跟蹤和收集UCCE日誌](#)

[SetTrace級別](#)

[設定跟蹤並收集PCCE日誌](#)

[設定跟蹤並收集CUIC/即時資料/IDS日誌](#)

[使用SSH下載日誌](#)

[使用RTMT下載日誌](#)

[VoS上的封包擷取\(Finesse、CUIC、VVB\)](#)

簡介

本檔案介紹如何在Cisco Unified Contact Center Enterprise(CCE)中設定和收集追蹤。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Unified Contact Center Enterprise(UCCE)
- 套裝客服中心企業版(PCCE)
- Cisco Finesse
- 思科客戶語音入口網站(CVP)
- Cisco Virtualized Voice Browser(VVB)

- 思科整合邊界元件(CUBE)
- 思科整合情報中心(CUIC)
- 思科整合作業階段啟始通訊協定(SIP)代理(CUSP)

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Finesse版本12.5
- CVP伺服器版本12.5
- UCCE/PCCE版本12.5
- Cisco VVB版本12.5
- CUIC版本12.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

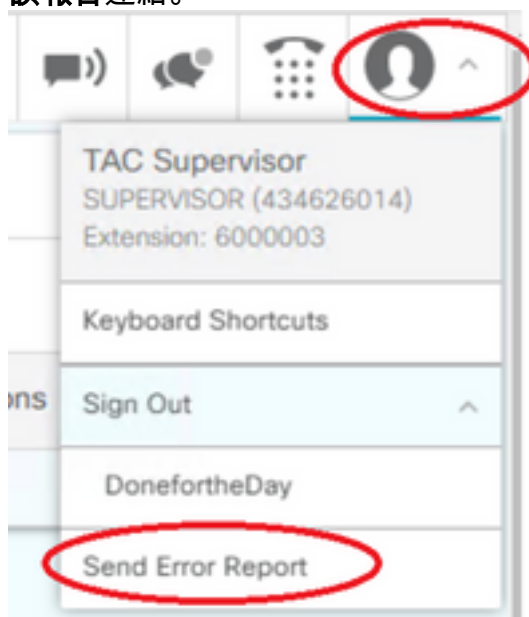
設定跟蹤和收集Finesse日誌

Finesse使用者端

有多個選項可用於收集Finesse客戶端日誌。

選項1:通過傳送錯誤報告收集客戶端日誌。

1. 登入代理。
2. 如果座席在呼叫或媒體事件過程中遇到任何問題，指示座席按一下finesse案頭右上角的**傳送錯誤報告**連結。



3. 代理看到日誌已**成功傳送**！消息。
4. 客戶端日誌被傳送到Finesse伺服器。導航到<https://x.x.x.x/finesse/logs>並使用管理帳戶登入。
5. 收集clientlogs/目錄下的日誌。

Directory Listing For /logs/ - Up To /

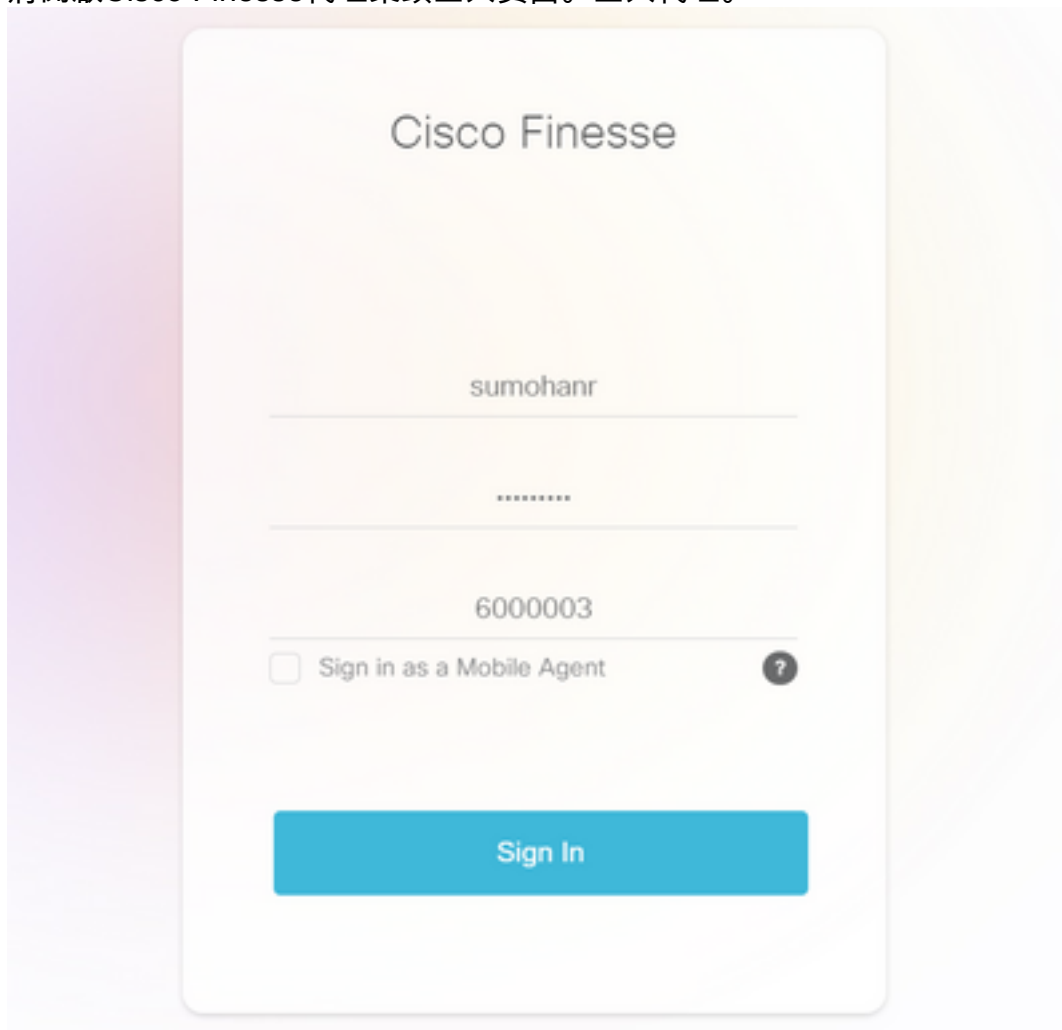
Filename	Size	Last Modified
3rdpartygadget/		Mon, 22 Feb 2021 23:06:32
admin/		Tue, 12 Jul 2022 18:52:53
cli.log	0.0 kb	Mon, 22 Feb 2021 22:59:10
clientlogs/		Wed, 17 Aug 2022 15:35:52

選項2:設定永續性日誌記錄

1. 導覽至<https://x.x.x.x:8445/desktop/locallog>。
2. 按一下Sign In With Persistent Logging。



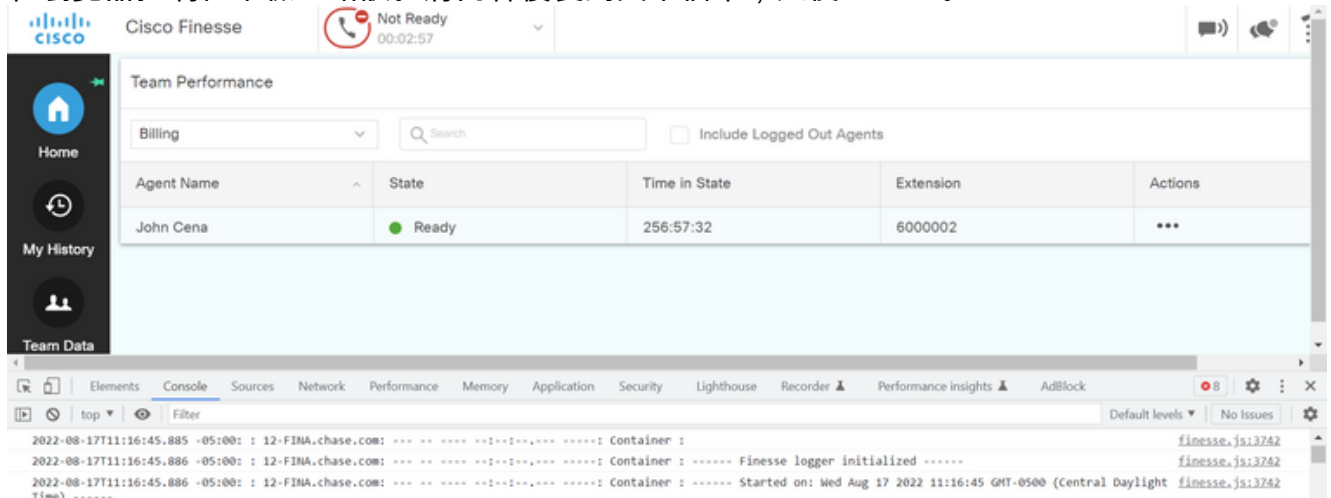
3. 將開啟Cisco Finesse代理案頭登入頁面。登入代理。



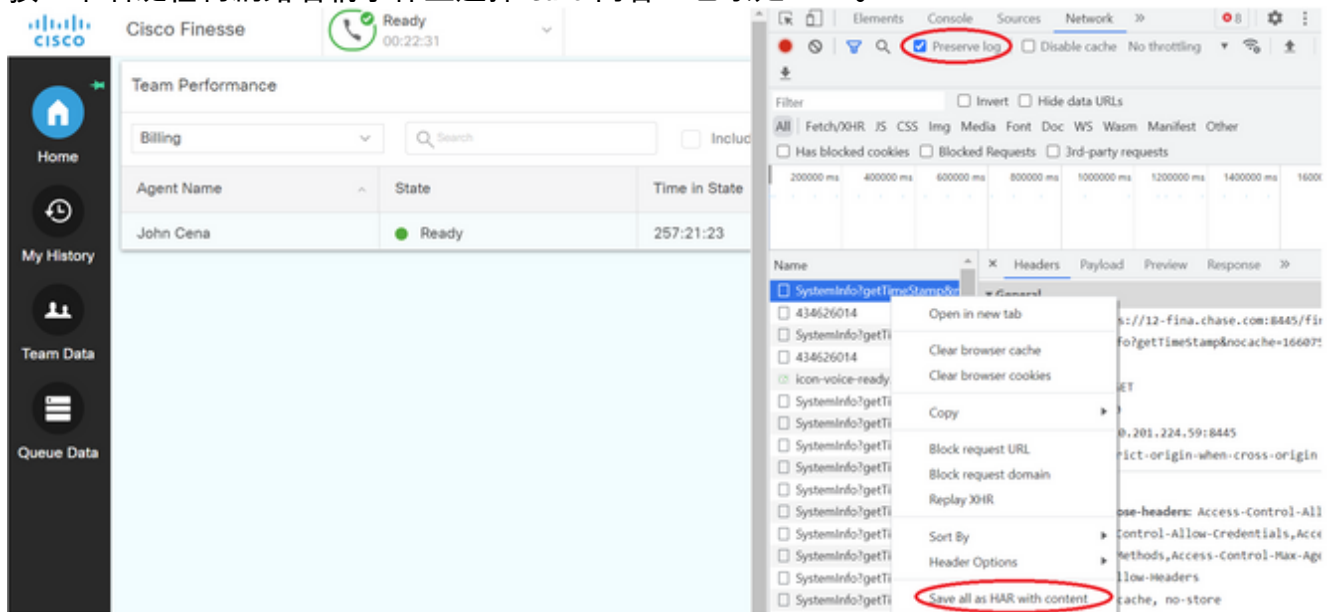
4. 所有Agent Desktop互動都將註冊並傳送到本地儲存日誌。要收集日誌，請導航到<https://x.x.x.x:8445/desktop/locallog>，然後將內容複製到文本檔案中。Save 檔案以供進一步分析。

選項3:Web瀏覽器控制檯

1. 代理登入後，按F12開啟瀏覽器控制檯。
2. 選擇Console頁籤。
3. 在瀏覽器控制檯中檢查錯誤。將內容複製到文本檔案，然後 save 它。



4. 選擇Network頁籤，並選中Preserve log選項。
5. 按一下右鍵任何網路名稱事件並選擇 Save 內容上也象是HAR。



Finesse伺服器

選項1:通過使用者介面(UI)- Web服務 (必需) 和其他日誌

1. 導航到 <https://x.x.x.x/finesse/logs> 並使用管理帳戶登入。
2. 展開目錄 `webservices/`



3. 收集最後一個Web服務日誌。選擇最後一個解壓縮檔案。例如 `Desktop-Webservices.201X-..log.zip`。按一下檔案連結，您會看到 save 檔案。

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 07:48:54 GMT
Desktop-webservices.2022-08-14T08-48-54.953.log	90079.1 kb	Wed, 17 Aug 2022 16:26:44 GMT

4. 收集其他所需的日誌 (取決於場景)。例如，針對通知服務問題的openfire、針對身份驗證問題的領域日誌以及API問題的tomcatlogs。

附註：建議通過安全外殼(SSH)和安全檔案傳輸協定(SFTP)收集Cisco Finesse伺服器日誌。此方法不僅允許您收集Web服務日誌，還允許您收集其他所有日誌，如Fippa、openfire、Realm和Clientlogs。

選項2:通過SSH和安全檔案傳輸協定(SFTP) — 推薦選項

1. 使用SSH登入到Finesse伺服器。
2. 輸入以下命令可收集所需的日誌。該命令將收集2小時的日誌。系統會提示您識別將日誌上傳到的SFTP伺服器。

```
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. 這些日誌儲存在SFTP伺服器路徑上：`<IP address>\<date time stamp>\active_nnn.tgz`，其中nnn是長格式的時間戳。
4. 要收集其他日誌 (如tomcat、上下文服務、服務和安裝日誌)，請檢視[Cisco Finesse管理指南12.5\(1\)版的「日誌收集」部分](#)。

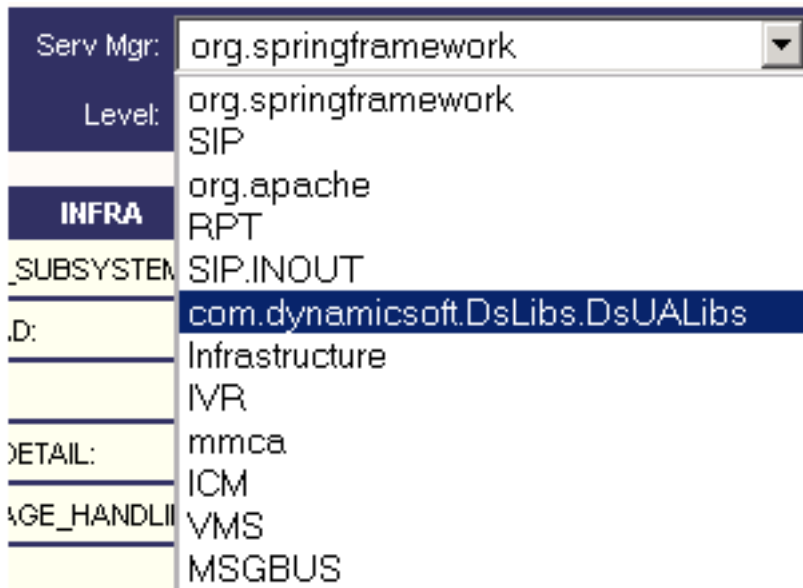
設定跟蹤並收集CVP和CVVB日誌

CVP通話伺服器

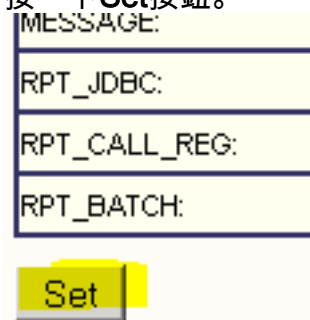
1. CVP CallServer跟蹤的預設級別足以對大多數情況進行故障排除。但是，如果您需要獲得有關會話發起協定(SIP)消息的更多詳細資訊，則需要將SIP堆疊跟蹤設定為DEBUG級別。
2. 導航到CVP CallServer診斷網頁URL <http://localhost:8000/cvp/diag>。

附註：此頁提供有關CVP CallServer的良好資訊，對特定方案進行故障排除非常有用。

3. 從伺服器中選擇com.dynamicsoft.DsLibs.DsUALibs。左上角的Mgr下拉選單



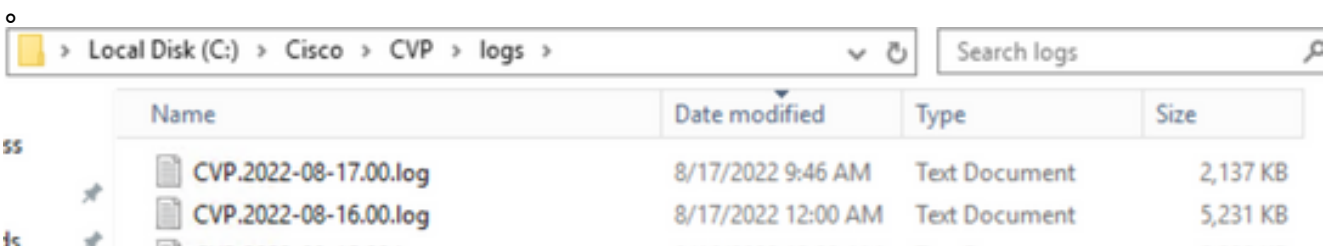
4. 按一下 **Set** 按鈕。



5. 在跟蹤視窗中向下滾動，以確保已正確設定跟蹤級別。這些是您的調試設定。

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

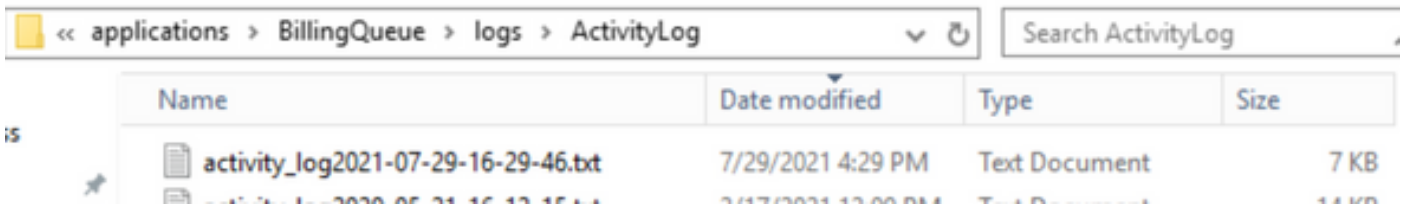
6. 重現問題時，請從 `C:\Cisco\CVP\logs` 收集日誌，然後根據問題發生的時間選擇 CVP 日誌檔案。



CVP 語音 XML (VXML) 應用程式

在極少數情況下，您需要提高 VXML 伺服器應用程式的跟蹤級別。另一方面，除非思科工程師提出請求，否則不建議增加此數量。

要收集 VXML 伺服器應用程式日誌，請導航到 VXML 伺服器下的特定應用程式目錄，例如：
`C:\Cisco\CVP\VXMLServer\applications\{應用程式名稱}\logs\ActivityLog` 並收集活動日誌。



CVP營運和管理管理入口網站(OAMP)

在大多數情況下，OAMP和ORM的預設跟蹤級別足以確定問題的根本原因。但是，如果需要增加跟蹤級別，以下是執行此操作的步驟：

1. 備份 %CVP_HOME%\confloamp.properties
2. 編輯 %CVP_HOME%\confloamp.properties

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

3. 修改後重新啟動OPSConsoleServer，如圖所示。

跟蹤級別資訊

跟蹤級別	說明	日誌級別	跟蹤掩碼
0	產品安裝預設值。預期效能沒有影響或影響極小。	資訊	無
1	更詳細的跟蹤消息，對效能影響較小。	調試	DEVICE_CONFIGURATION + DATABASE_MODIFY + 管理=0x01011000 DEVICE_CONFIGURATION +
2	詳細的跟蹤消息，對效能的影響適中。	調試	SYSLVL_CONFIGURATION + DATABASE_MODIFY + 管理=0x05011000 DEVICE_CONFIGURATION +
3	詳細的跟蹤消息對效能有影響。	調試	SYSLVL_CONFIGURATION + BULK_OPERATIONS + DATABASE_MODIFY + 管理=0x05111000 雜項+ DEVICE_CONFIGURATION +
4	詳細的跟蹤消息對效能有非常高的影響。	調試	ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK

TRACE +
DATABASE_MODIFY +
DATABASE_SELECT +
DATABASE_PO_INFO +
管理+
TRACE_METHOD +
TRACE_PARAM=0x173710
00

雜項+
DEVICE_CONFIGURATION
+
ST_CONFIGURATION +
SYSLVL_CONFIGURATION
+
BULK_OPERATIONS +
BULK_EXCEPTION_STACK
TRACE +
DATABASE_MODIFY +
DATABASE_SELECT +
DATABASE_PO_INFO +
管理+
TRACE_METHOD +
TRACE_PARAM=0x173710
06

5 最高詳細跟蹤消息。

調試

Cisco Virtualized Voice Browser(CVVB)

在CVVB中，跟蹤檔案是記錄來自Cisco VVB元件子系統和步驟的活動的日誌檔案。

Cisco VVB有兩個主要元件：

- 稱為MADM日誌的Cisco VVB「管理」跟蹤
- 稱為MIVR日誌的Cisco VVB「引擎」跟蹤

您可以指定要為其收集資訊的元件以及要收集的資訊級別。

日誌級別擴展自：

- 調試 — 基本流詳細資訊到
- XDebugging 5 — 使用堆疊追蹤軌跡的詳細層級

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						

警告：不能在生產載入的系統上啟用Xdebugging5。

您需要收集的最常見日誌是引擎。CVVB引擎跟蹤的預設跟蹤級別足以解決大多數問題。但是，如果您需要更改特定方案的跟蹤級別，思科建議您使用預定義的系統日誌配置檔案。

系統日誌配置檔案

名稱

必須啟用此配置檔案的方案

預設VVB

通用日誌已啟用。

AppAdminVVB

有關通過AppAdmin、Cisco VVB可維護性和其他網頁進行Web管理的問

MediaVVB

用於介質設定或介質傳輸問題。

VoiceBrowserVVB

用於呼叫處理問題。

MRCPVVB

有關使用Cisco VVB互動的ASR/TTS的問題。

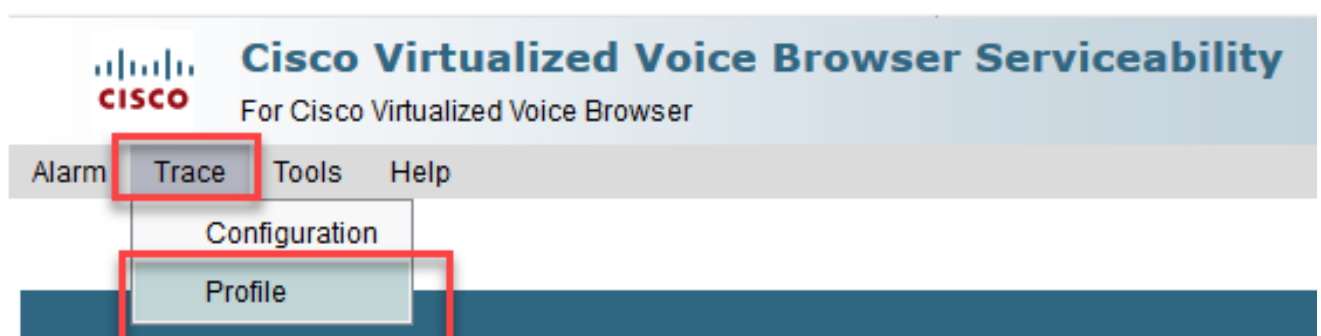
CallControlVVB

SIP訊號相關問題將在日誌中發佈。

1. 開啟CVVB首頁(<https://X.X.X.X/uccxservice/main.htm>)，然後導航至Cisco VVB可維護性頁面。使用管理帳戶登入



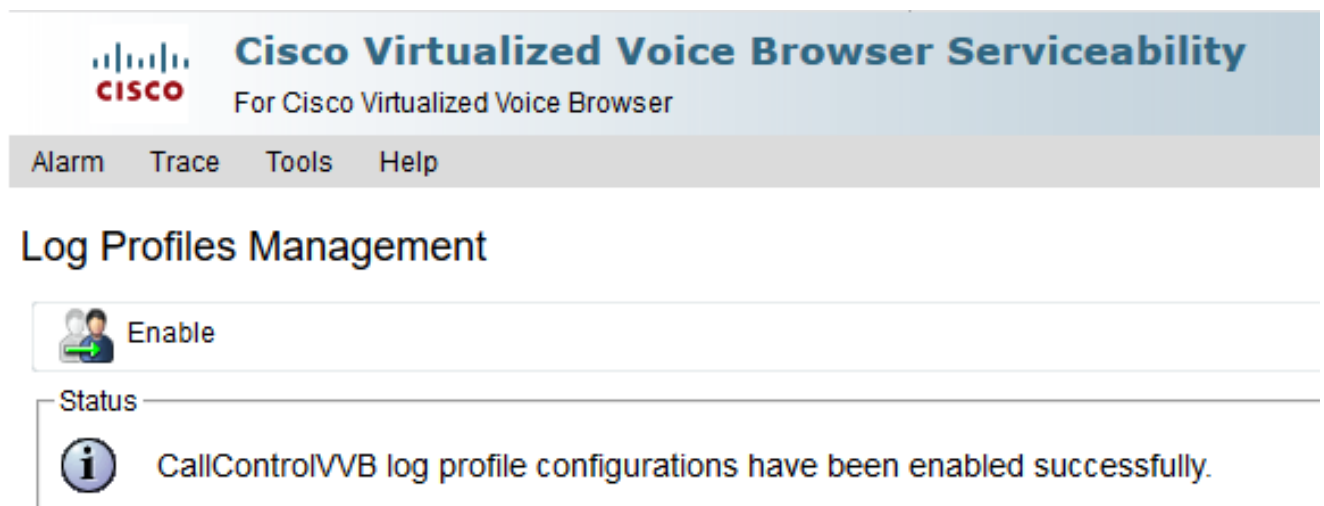
2. 選擇 Trace ->配置檔案。



3. 選中要為特定方案啟用的配置檔案，然後按一下**Enable**按鈕。例如，啟用SIP相關問題的配置檔案CallControlVVB或自動語音識別和文本到語音互動(ASR/TTS)互動相關問題的MRCPVVB。

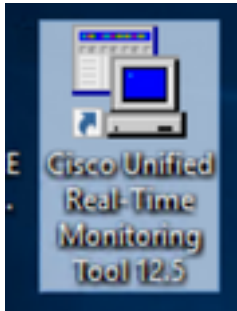
The screenshot shows the Cisco Virtualized Voice Browser Serviceability interface. At the top, there is a header with the Cisco logo and the text "Cisco Virtualized Voice Browser Serviceability For Cisco Virtualized Voice Browser". Below the header is a navigation bar with "Alarm", "Trace", "Tools", and "Help" links. The main content area is titled "Log Profiles Management". There is a "Enable" button with a person icon. Below that is a "Status" section with an information icon and the text "Ready". The "Profiles" section lists several profiles: "MediaVVB", "DefaultVVB", "AppAdminVVB", "VoiceBrowserVVB", "CallControlVVB", and "MRCPVVB". The "CallControlVVB" profile is selected, indicated by a radio button and a red box around it. Below the profiles list is another "Enable" button, also highlighted with a red box.

4. 按一下「enable (啟用)」按鈕後會顯示成功消息。

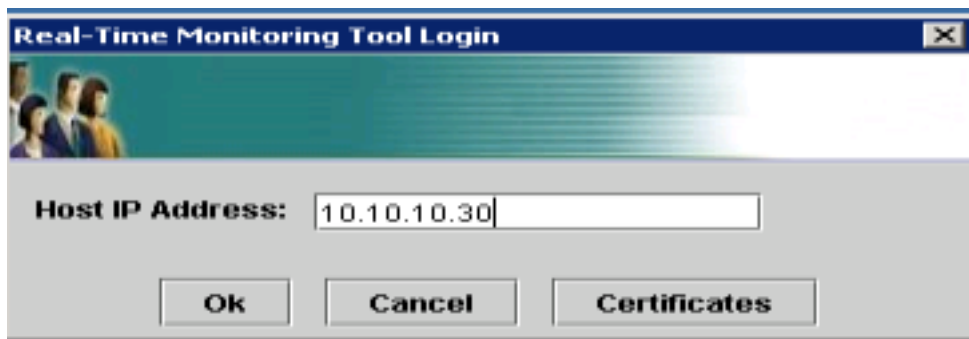


The screenshot shows the same Cisco Virtualized Voice Browser Serviceability interface as the previous one. The "CallControlVVB" profile is still selected. The "Enable" button is highlighted with a red box. Below the profiles list, a success message is displayed: "CallControlVVB log profile configurations have been enabled successfully." The message is preceded by an information icon.

5. 重現問題後，收集日誌。使用CVVB附帶的即時監視工具(RTMT)收集日誌。
6. 按一下案頭上的Cisco Unified Real-Time Monitoring Tool圖示 (如果需要，請從CVVB下載此工具)。



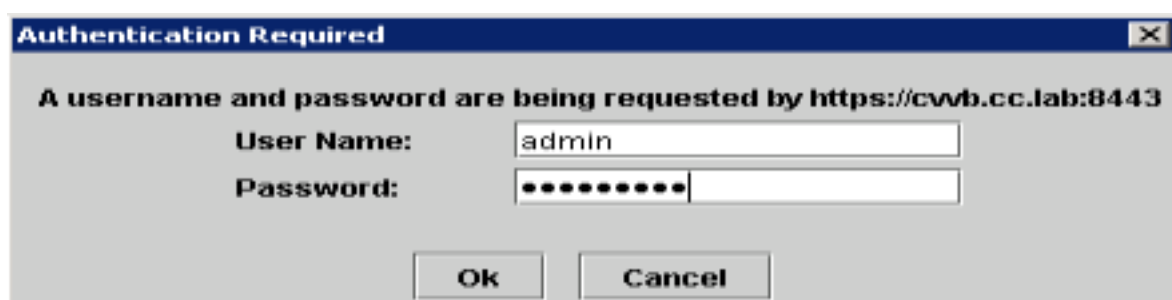
7. 提供VVB的IP地址，然後按一下OK。



8. 接受證書資訊 (如果顯示)



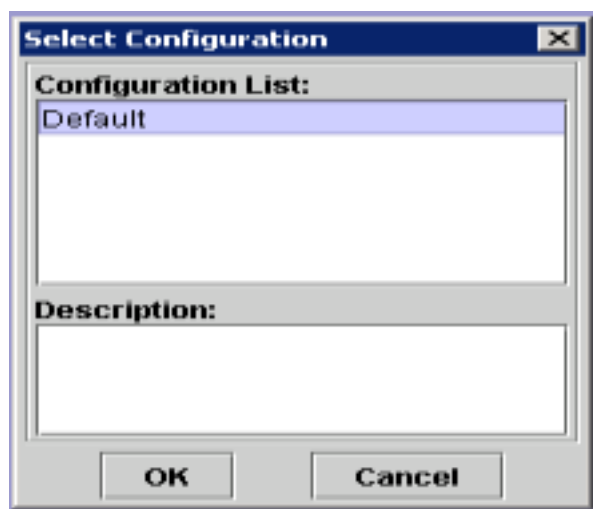
9. 提供憑證並按一下確定。



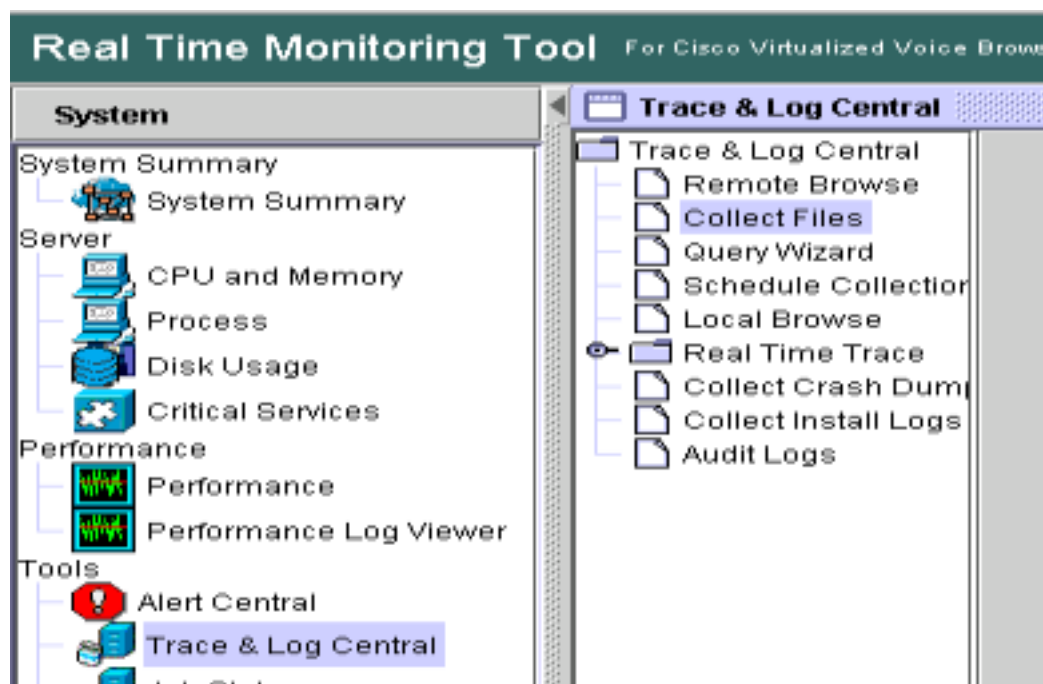
10. 如果收到TimeZone錯誤，則按一下**Yes**按鈕後，RTMT可以關閉。請重新啟動RTMT工具。



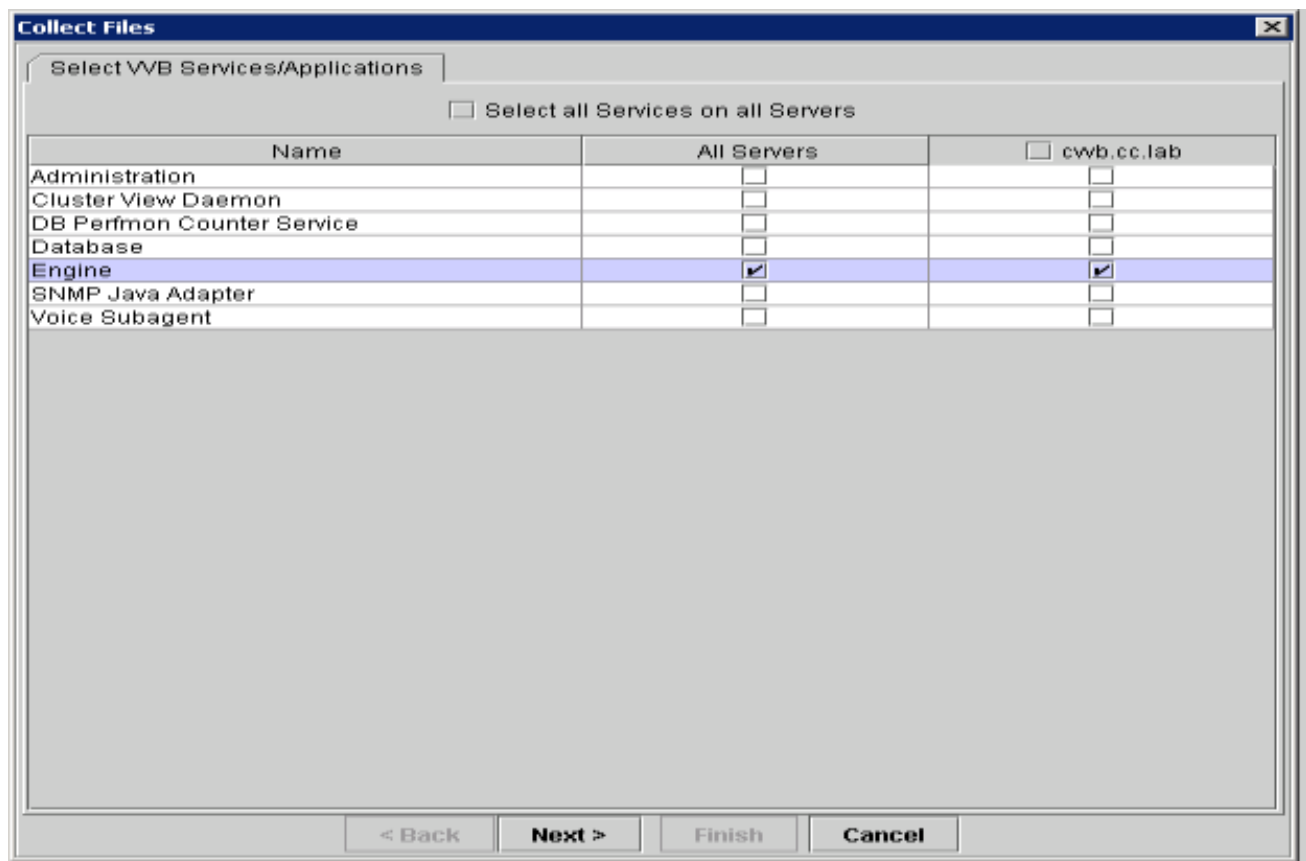
11. 保持選中「Default configuration (預設配置)」，然後按一下**OK**。



12. 選擇**Trace & Log Central**，然後按兩下**Collect Files**。



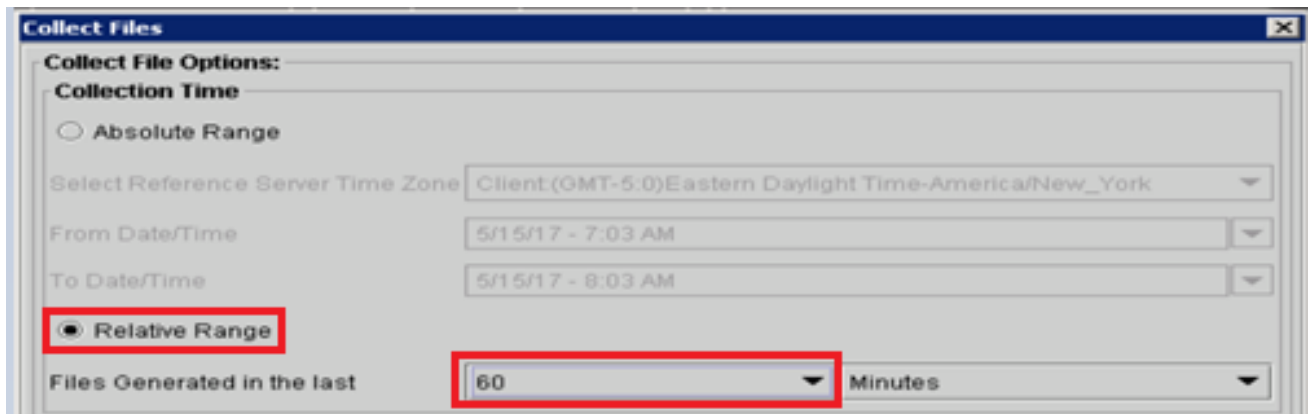
13. 在新開啟的視窗中，選擇**Engine**並按一下「**下一步**」。



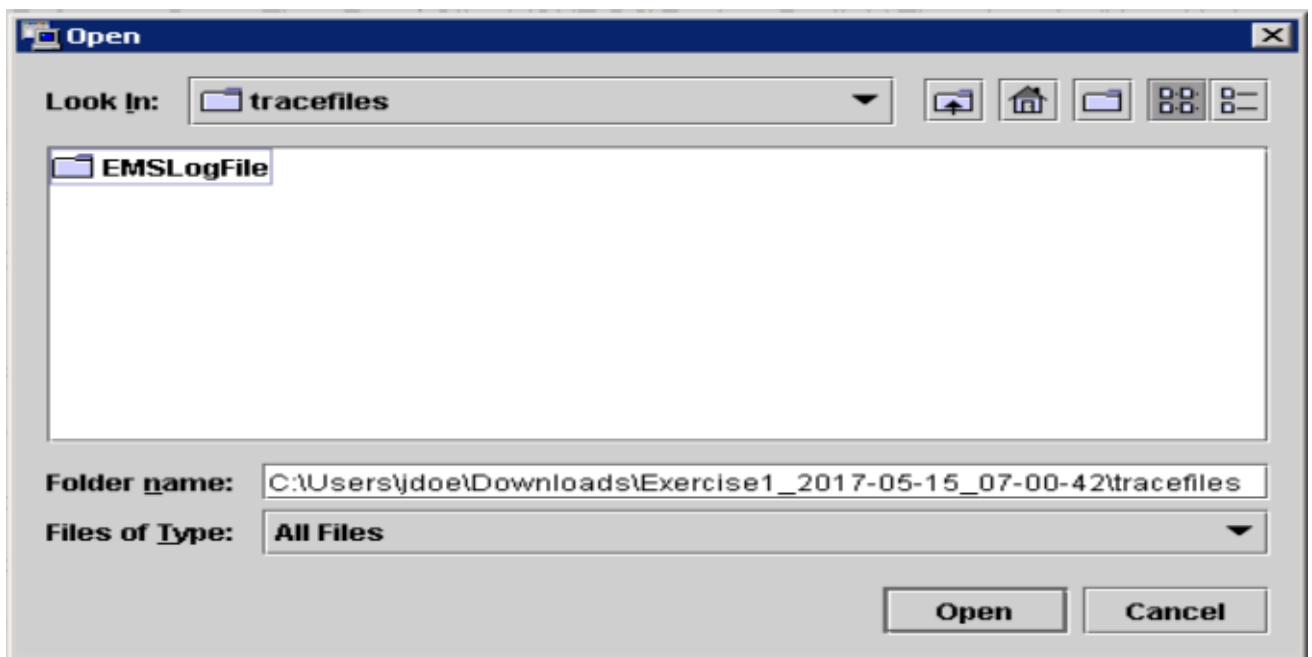
14. 在下一個視窗中再次按一下Next。



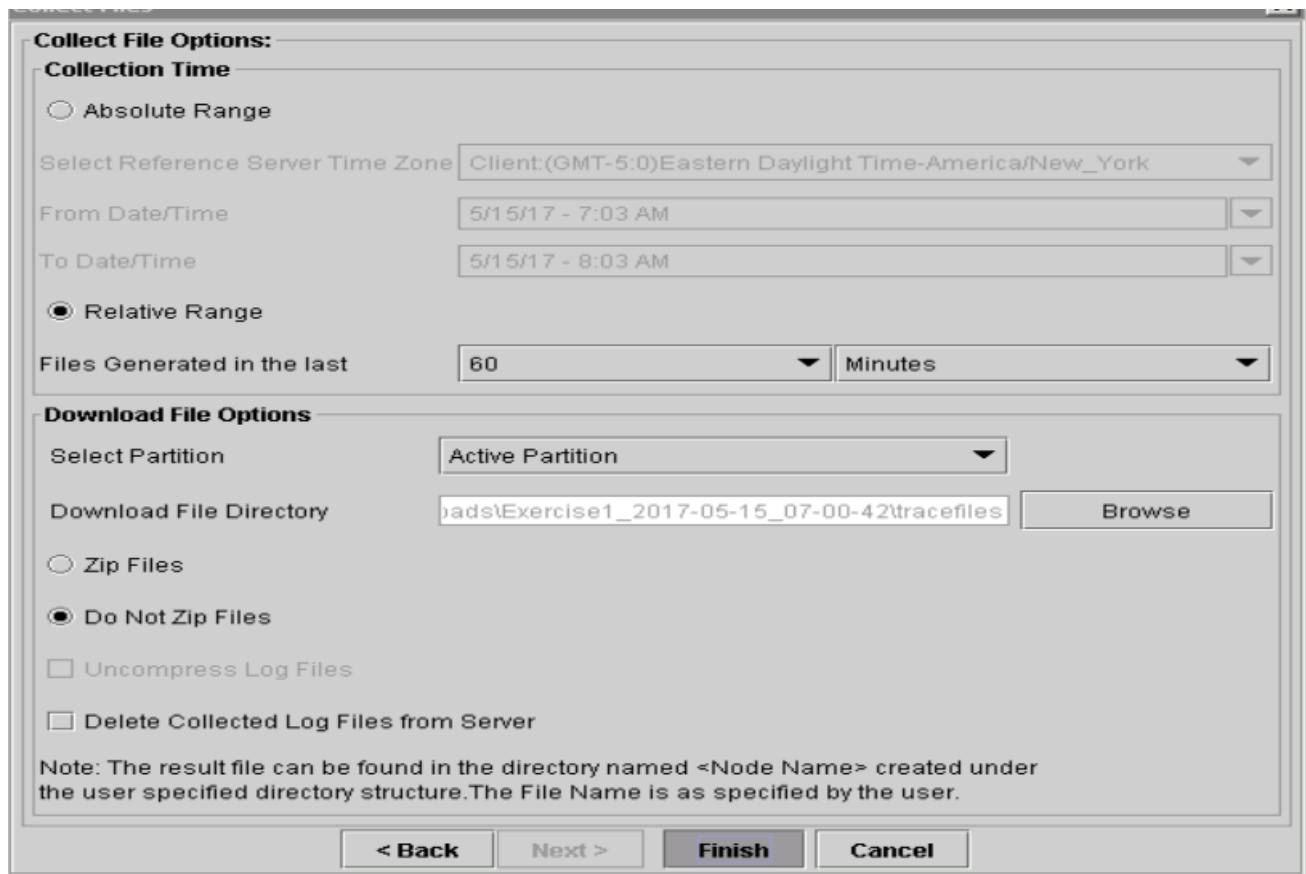
15. 選擇Relative Range，並確保您選擇時間以覆蓋錯誤呼叫的時間。



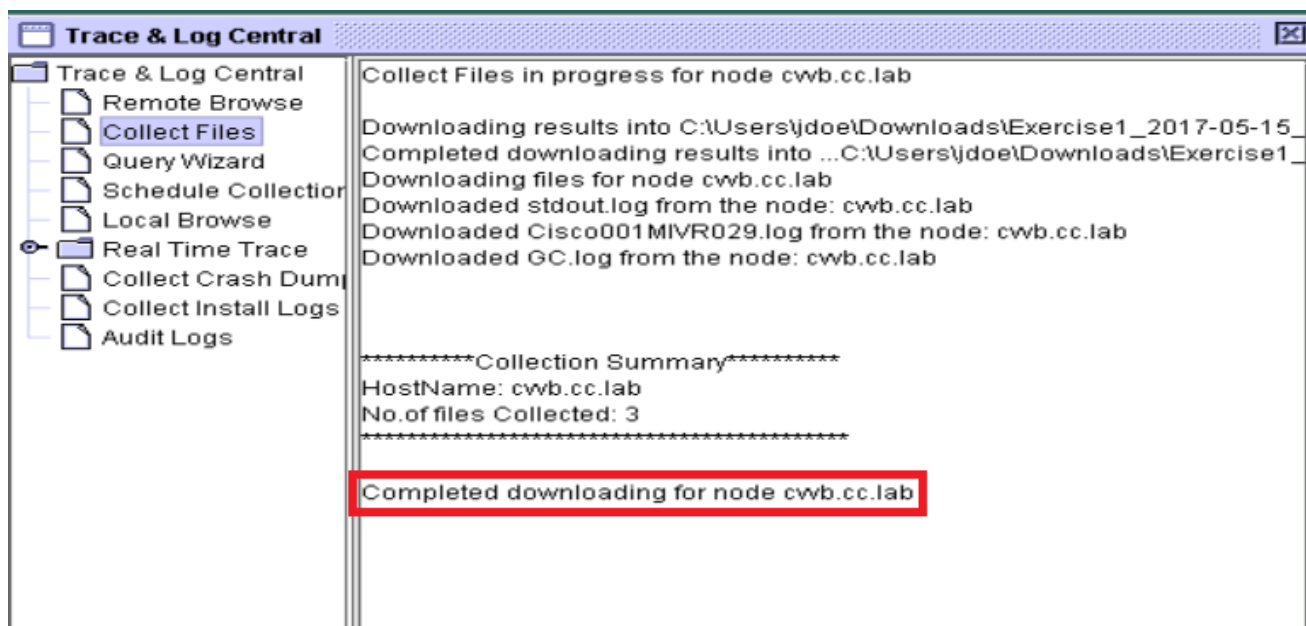
16. 在「Download File Options (下載檔案選項)」上，按一下**Browse**，然後選擇要使用的目錄 save 檔案，然後按一下**Open**。



17. 選中所有選項後，按一下**Finish**按鈕。



18. 這將收集日誌檔案。等待，直到您看到RTMT上的確認報文。



19. 導航到儲存跟蹤的資料夾。

20. 引擎日誌就是你所需要的。若要查詢這些檔案，請導覽至<時間戳>\uccx\log\MIVR文件夾。
選項2:通過SSH和SFTP — 推薦選項

1. 使用安全殼層(SSH)登入VVB伺服器。
2. 輸入以下命令可收集所需的日誌。系統會壓縮日誌，並提示您標識日誌上傳的SFTP伺服器。
`file get activelog /uccx/log/MIVR/*`

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

3. 這些日誌儲存在SFTP伺服器路徑上：`<IP address>\<date time stamp>lactive_nnn.tgz`，其中nnn是長格式的時間戳。

為CUBE和CUSP設定跟蹤和收集日誌

CUBE(SIP)

1. 設定日誌時間戳並啟用日誌記錄緩衝區。

```
#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
```

警告：對生產Cisco IOS[®]軟體GW的任何更改都可能會導致中斷。

2. 這是一個非常強大的平台，可以在所提供的呼叫量處理建議的調試，而不會出現問題。但是，思科建議您：將所有日誌傳送到系統日誌伺服器，而不是日誌緩衝區。

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

一次應用一個debug命令，並在每個命令之後檢查CPU利用率。

```
show proc cpu hist
```

警告：如果CPU利用率達到70-80%，效能相關服務影響的風險將大大增加。因此，如果GW達到60%，請不要啟用其他調試。

3. 啟用以下調試：

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

4. 重現問題。

5. 禁用跟蹤。

```
#undebug all
```

6. 收集日誌。

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

CUSP

1. 在CUSP上啟用SIP跟蹤。


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

2. 重現問題。
3. 完成後關閉登入。

收集日誌

1. 在CUSP上配置使用者(例如：測試)。
2. 在CUSP提示符處新增此配置。

```
username <userid> create
username <userid> password <password>
username <userid> group pfs-privusers
```
3. FTP到CUSP IP地址。使用上一步中定義的使用者名稱 (測試) 和密碼。
4. 將目錄更改為/cusp/log/trace。
5. 獲取log_<filename>。

設定跟蹤和收集UCCE日誌

思科建議通過Diagnostic Framework Portico或System CLI工具設定跟蹤級別並收集跟蹤。

附註： 有關診斷框架門戶和系統CLI的詳細資訊，請參閱[Diagnostic tools](#) (診斷工具) 一章，有關Cisco Unified ICM/Contact Center Enterprise版本12.5(1)的適用性指南。

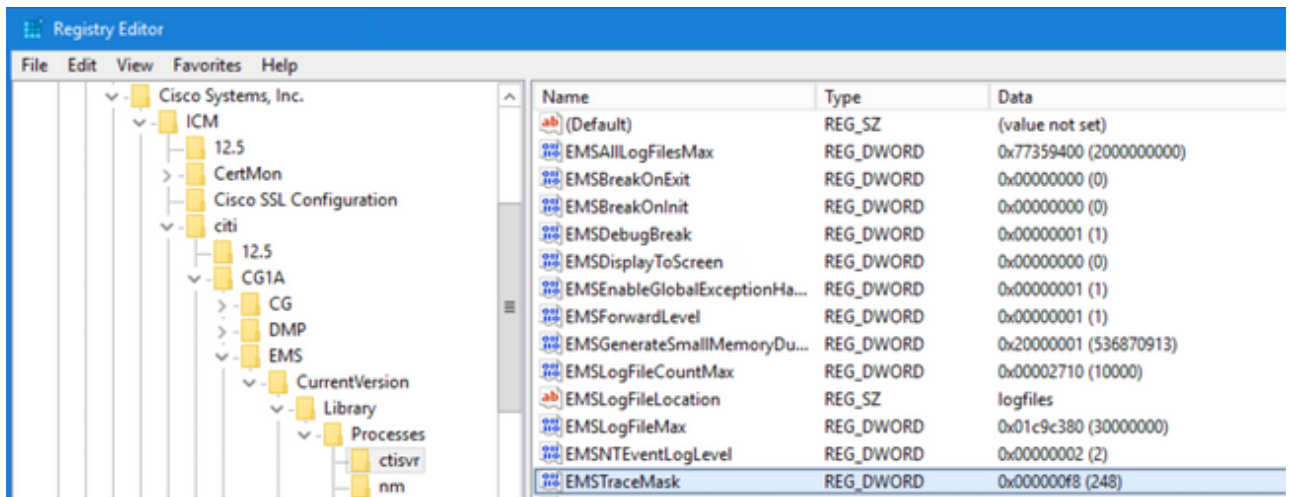
對大多數UCCE方案進行故障排除時，如果跟蹤的預設級別沒有提供足夠的資訊，請在所需元件中將跟蹤級別設定為3 (某些例外情況除外)。

附註： 如需詳細資訊，請參閱Cisco Unified ICM/客服中心企業版12.5(1)適用性指南上的[追蹤級別](#)一節。

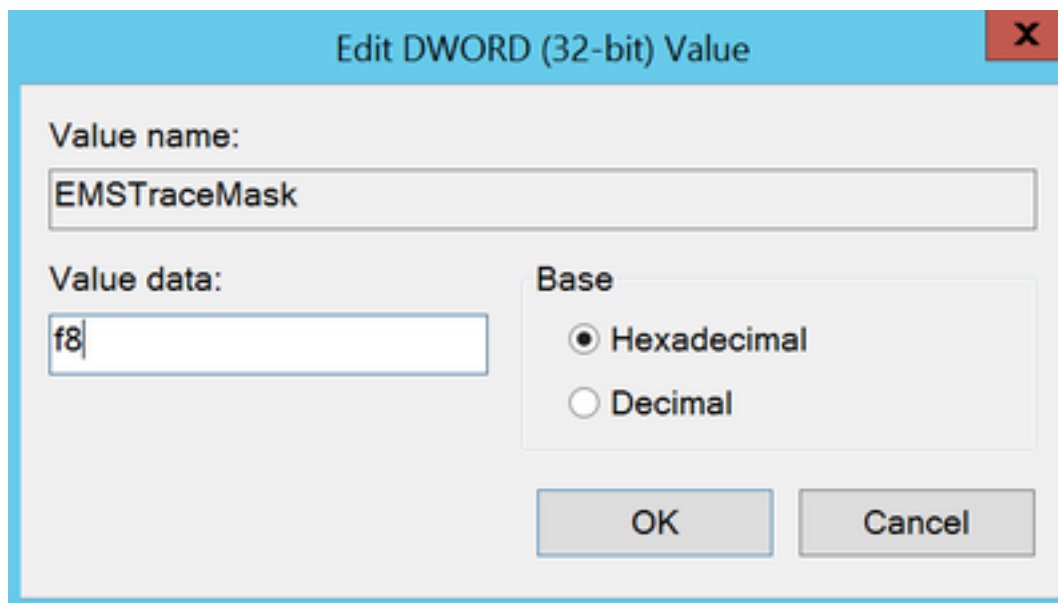
例如，如果對出站撥號器問題進行故障排除，如果撥號器忙，跟蹤級別必須設定為2。

對於CTISVR(CTISVR)，第2級和第3級未設定思科建議的確切登錄檔級別。CTISVR的推薦跟蹤登錄檔為0XF8。

1. 在UCCE代理PG上，開啟登錄檔編輯器(Regedit)。
2. 導航至HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1 (a和 b) \EMS\CurrentVersion\library\Processes\ctisvr。



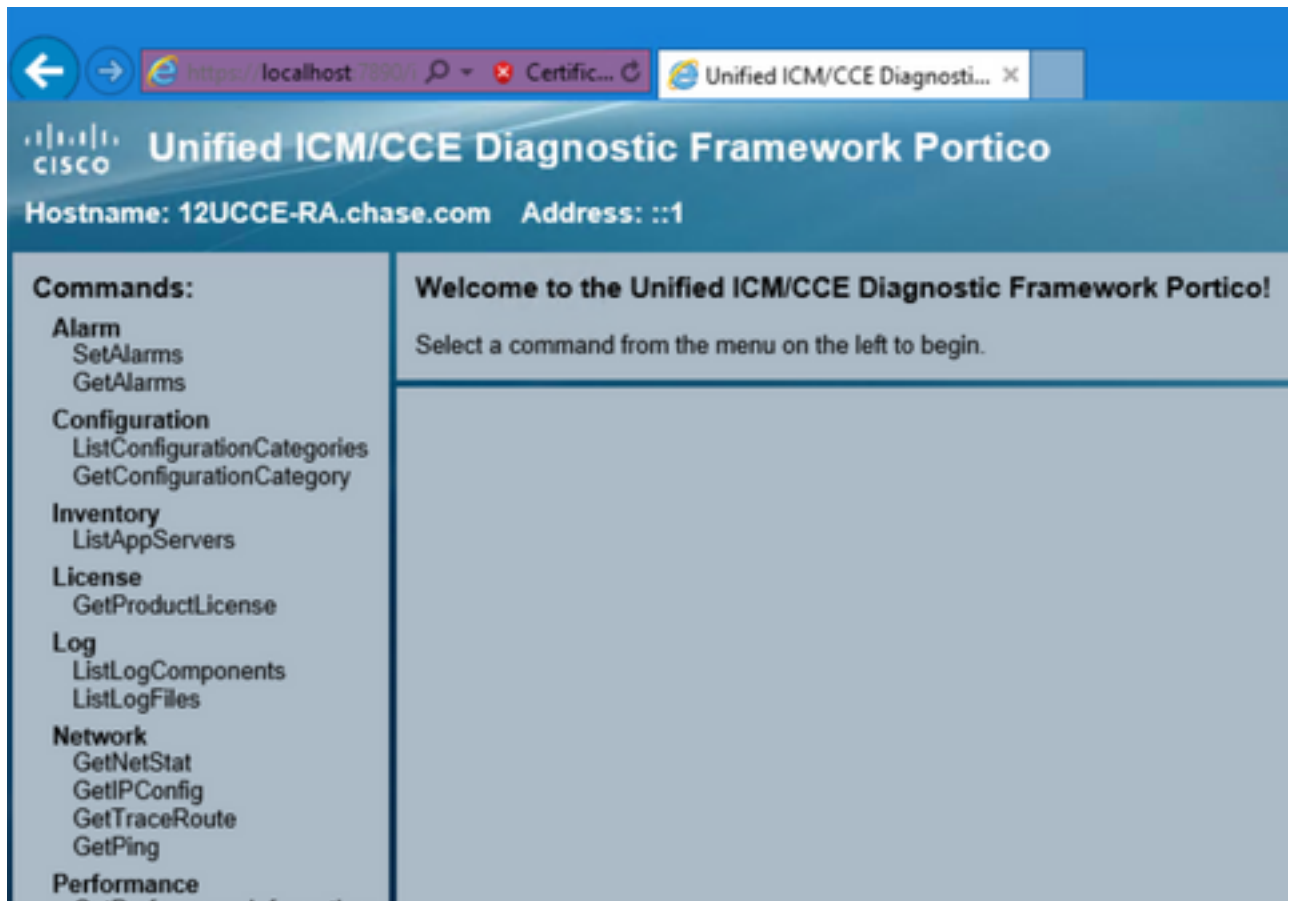
3. 按兩下EMSTraceMask，將值設定為f8。



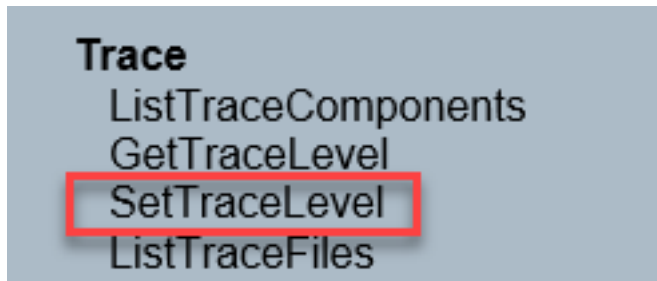
4. 按一下Ok並關閉登錄檔編輯器。以下是設定任何UCCE元件跟蹤的步驟（以RTR進程為例）。

SetTrace級別

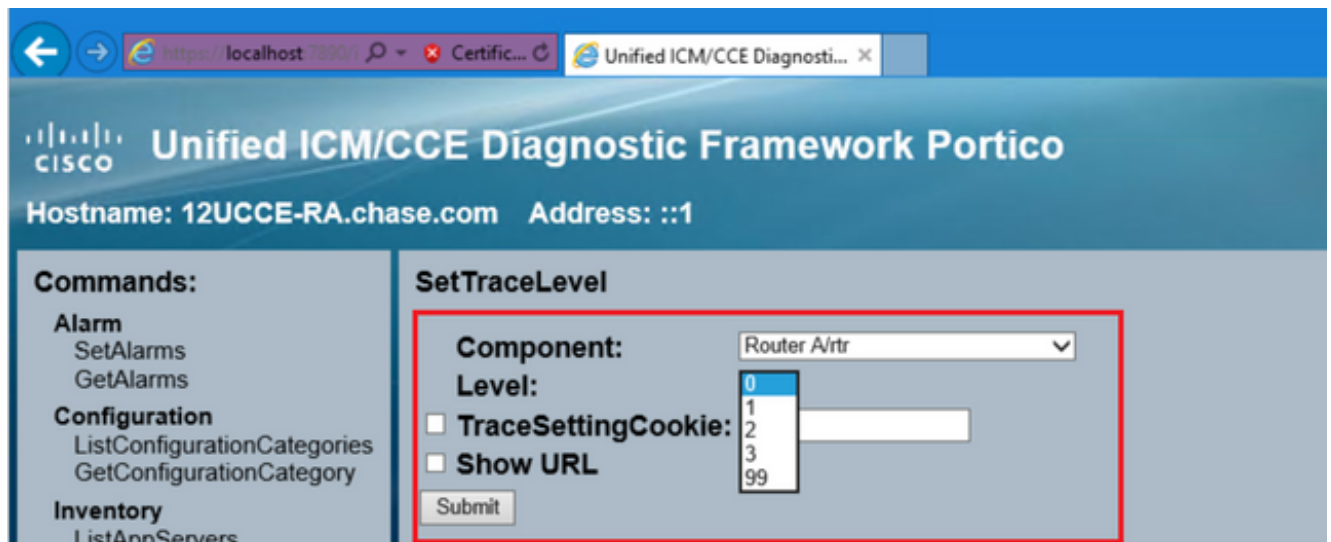
1. 從需要設定跟蹤的伺服器開啟Diagnostic Framework Portico，並以管理員使用者身份登入



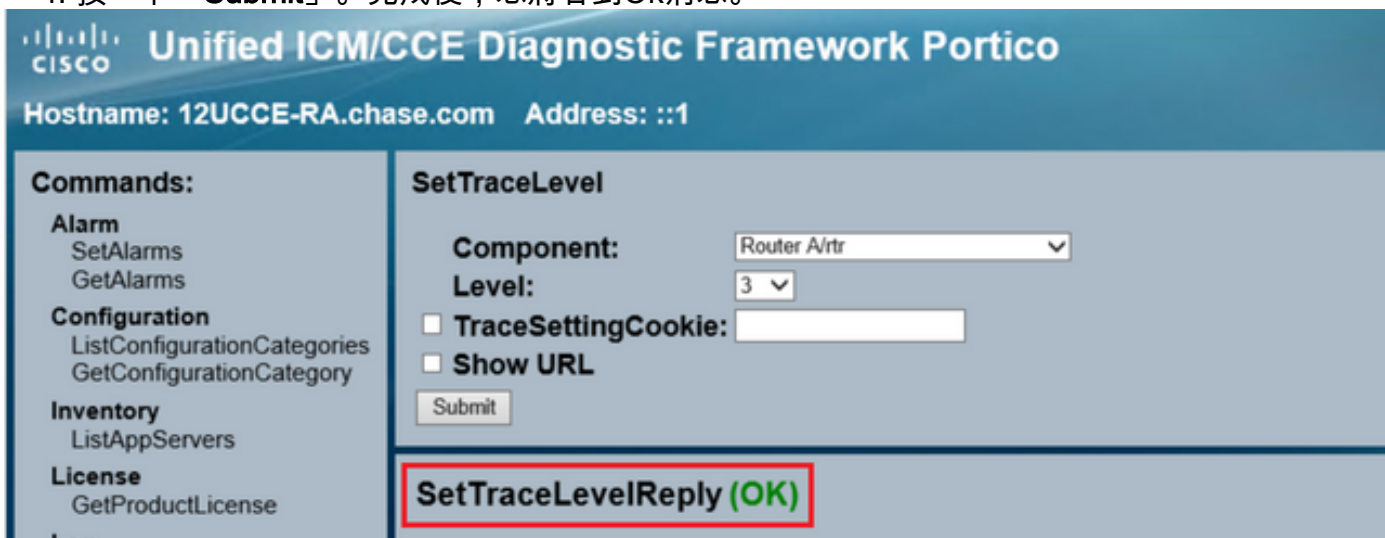
2. 在「命令」部分中，導航到Trace並選擇 **SetTraceLevel**。



3. 在「SetTraceLevel」視窗中，選擇元件和級別。



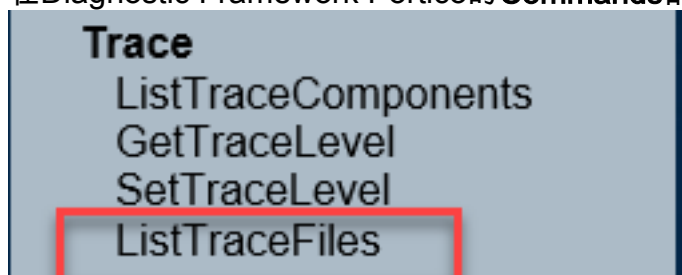
4. 按一下「Submit」。完成後，您將看到Ok消息。



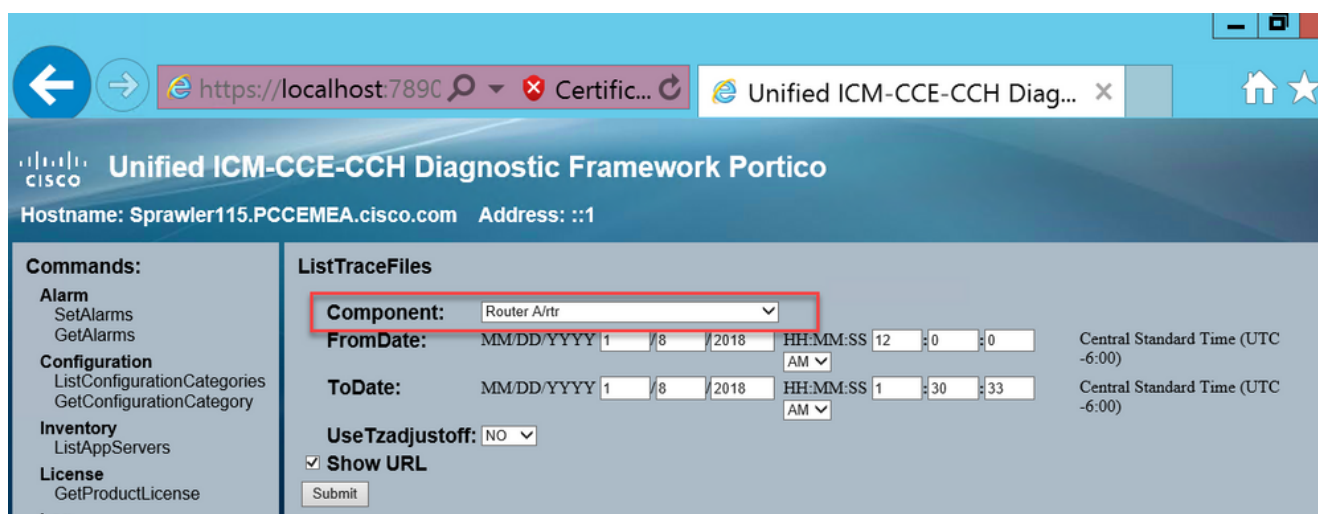
警告：嘗試重現問題時將跟蹤級別設定為級別3。重現問題後，將跟蹤級別設定為預設值。設定JTAPIGW跟蹤時應特別小心，因為級別2和級別3設定了低級別跟蹤，這可能會影響效能。在非生產時間或在實驗室環境中設定JTAPIGW中的第2級或第3級。

日誌收集

1. 在Diagnostic Framework Portico的Commands部分，導航到Trace，然後選擇ListTraceFile。



2. 在ListTraceFile窗口中，選擇Component、FromDate和ToDate。選中Show URL框，然後按一下Submit。



3. 請求完成後，您將看到帶有ZIP日誌檔案連結的OK消息。

4. 按一下ZIP檔案連結並 save 所選位置中的檔案。

設定跟蹤並收集PCCE日誌

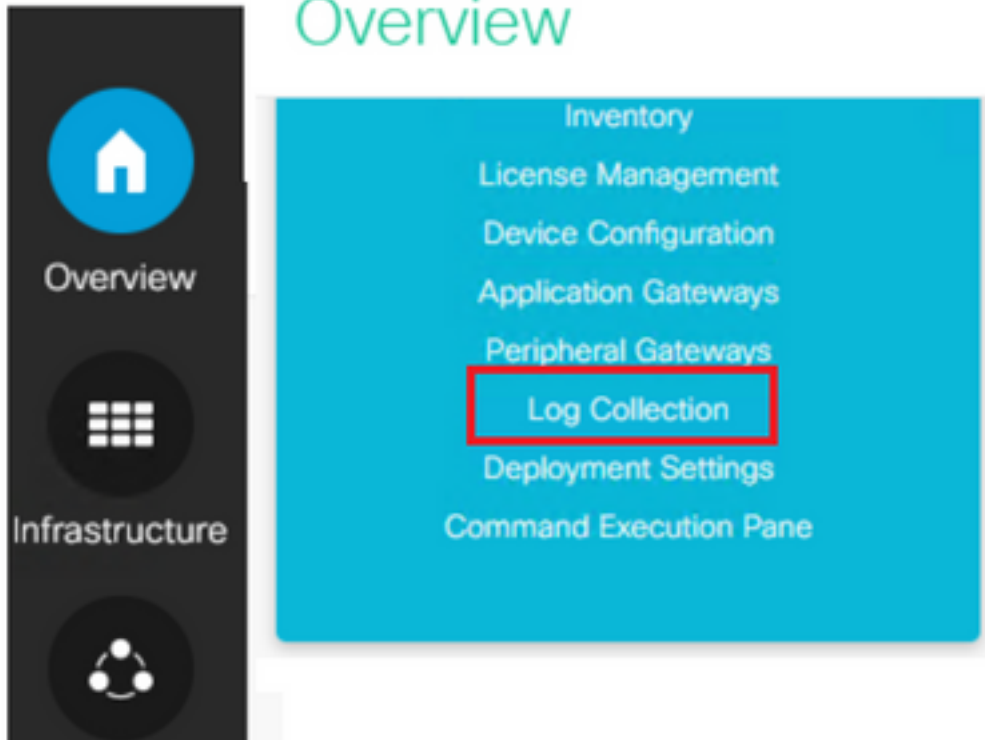
PCCE擁有自己的工具來設定跟蹤級別。它不適用於UCCE環境，其中診斷框架Portico或系統CLI是啟用和收集日誌的首選方法。

1. 在PCCE AW伺服器上，開啟Unified CCE Web Administration工具並登入到管理員帳戶。

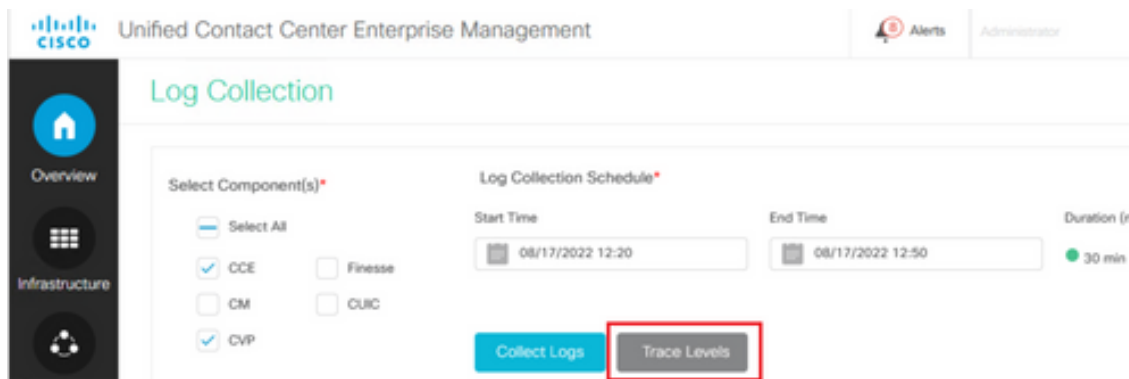
2. 導航到概述 —>基礎結構設定 —>日誌收集，以開啟「日誌收集」頁。



Unified Contact Center Enterprise Overview



3. 在「日誌收集」頁上，按一下**跟蹤級別**，這將開啟「跟蹤級別」對話方塊。



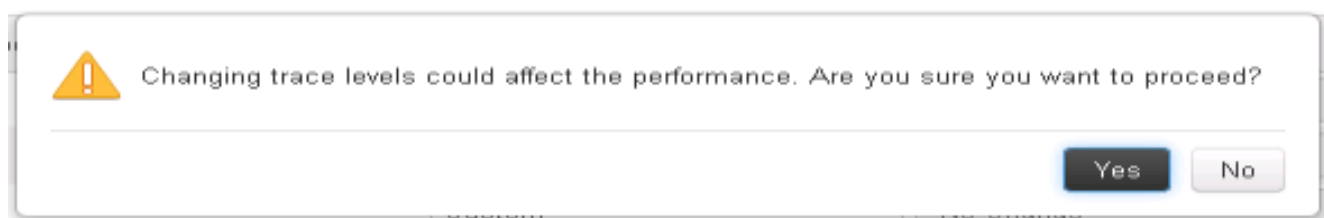
4. 在CCE上將跟蹤級別設定為**Detailed**，並保留為**No Change** for CM and CVP，然後按一下 **更新跟蹤級別**。

Trace Levels ✕

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

Update Trace Levels
Cancel

5. 按一下**Yes**確認警告。



6. 重現問題後，開啟**Unified CCE Administration**並導航回**System > 日誌收集**。
7. 在Components (元件) 窗格中選擇**CCE**和**CVP**。
8. 選擇適當的日誌收集時間 (預設值為過去30分鐘)。
9. 按一下**Collect Logs**和**Yes**可顯示對話方塊警告。開始日誌收集。請等待幾分鐘後結束。

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	🔄	⬇️ ⚙️

10. 完成後，按一下**操作**列中的**Download**按鈕，下載包含所有日誌的壓縮檔案。Save 找到適當位置的zip檔案。

設定跟蹤並收集CUIC/即時資料/IDS日誌

SSH

1. 登入到CUIC、LD和IDS的SSH命令列(CLI)。

2. 運行命令以收集CUIC相關的日誌。

```
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. 運行命令以收集LD相關的日誌。

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

4. 運行命令以收集ld相關日誌。

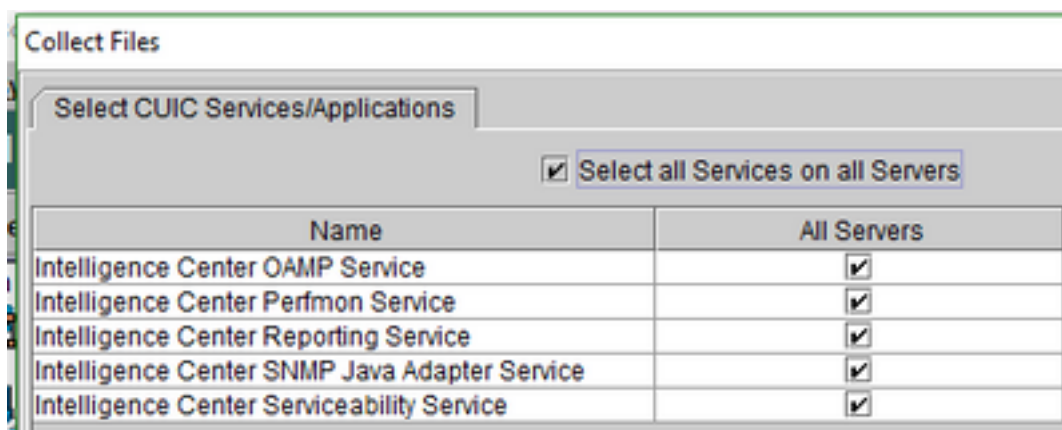
file get activelog ids/log/*.* recurs compress reltime days 1

5. 這些日誌儲存在SFTP伺服器路徑上：`<IP address>\<date time stamp>\active_nnn.tgz`，其中 nnn是長格式的時間戳。

RTMT

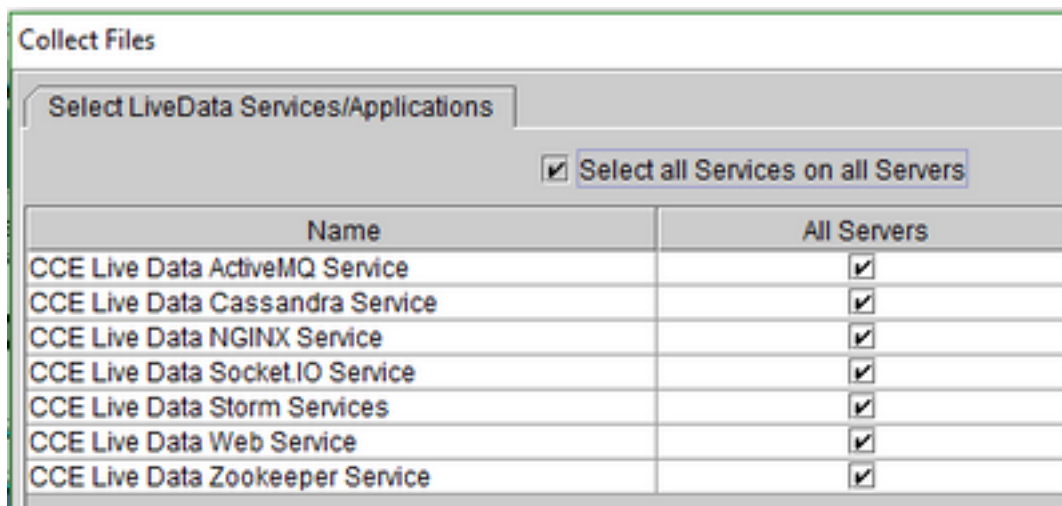
1. 從OAMP頁面下載RTMT。登入到`https://<HOST ADDRESS>/oamp`，其中HOST ADDRESS是伺服器的IP地址。
2. 導覽至Tools > RTMT plugin download。下載並安裝外掛。
3. 啟動RTMT並使用管理員憑據登入到伺服器。
4. 按兩下Trace and Log Central，然後按兩下Collect Files。
5. 您可以檢視特定服務的這些頁籤。您必須為CUIC、LD和IDS選擇所有服務/伺服器。

CUIC:



Name	All Servers
Intelligence Center OAMP Service	<input checked="" type="checkbox"/>
Intelligence Center Perfmon Service	<input checked="" type="checkbox"/>
Intelligence Center Reporting Service	<input checked="" type="checkbox"/>
Intelligence Center SNMP Java Adapter Service	<input checked="" type="checkbox"/>
Intelligence Center Serviceability Service	<input checked="" type="checkbox"/>

LD:



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"/>

IDS:

Collect Files

Select IdS Services/Applications

Select all Services on all Servers

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

PlatformTomcat

Event viewer

Collect Files

Select System Services/Applications

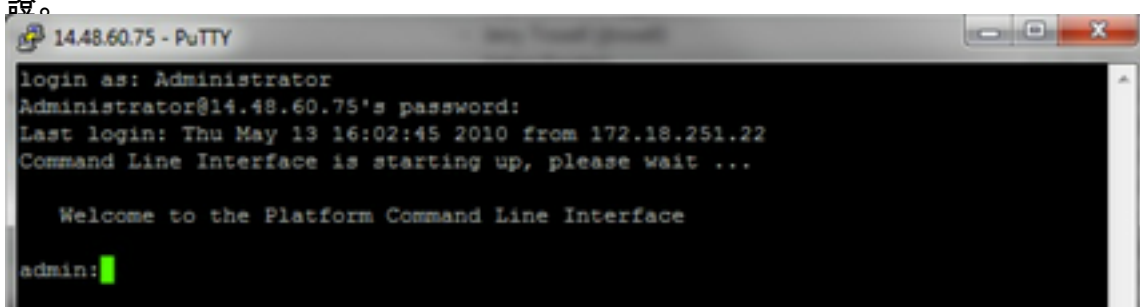
Select all Services on all Servers

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"/>

6. 選擇Date and Time以及目標資料夾，以便 save 日誌。

VoS上的封包擷取(Finesse、CUIC、VVB)

1. 開始捕獲 要開始捕獲，請建立到VOS伺服器的SSH會話，並使用平台管理員帳戶進行身份驗證。



```
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: █
```

2.

1a. 指令語法

命令如下 **utils network capture**語法如下：

Syntax:

utils network capture [options]

options optional

page,numeric,file fname,count num,size bytes,src addr,dest addr,port
num,host protocol addr

options are:

page

- pause output

numeric - show hosts as dotted IP

addresses

file fname - output the information to a file

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

fname should not contain the "." character

count num - a

count of the number of packets to capture

Note: The maximum count

for the screen is 1000, for a file is 100000

size bytes -

the number of bytes of the packet to capture

Note: The maximum

number of bytes for the screen is 128

For a file it can be

any number or ALL

src addr - the source address of the
packet as a host name or IPV4 address

dest addr - the
destination address of the packet as a host name or IPV4 address

port

num - the port number of the packet (either src or dest)

host

protocol addr - the protocol should be one of the following:

ip/arp/rarp/all. The host address of the packet as a host name or IPV4
address. This option will display all packets to and from that address.

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

1b. 捕獲所有流量

對於典型的捕獲，可以將所有大小的ALL地址之間的所有資料包收集到一個名為**packets.cap**的捕獲檔案中。為此，只需在管理員CLI上執行 **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=
```

1c。根據埠

號捕獲

為了排除群集管理器中的通訊問題，最好使用埠選項根據特定埠(8500)進行捕獲。

有關哪些服務需要在每個埠上通訊的詳細資訊，請參閱TCP和UDP埠使用指南以獲得相應元件的適用版本。

```
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=
```

1d。根據

主機捕獲

要排除VOS和特定主機的故障，必須使用「host」選項過濾進出特定主機的流量。

也可能必須排除特定主機，在這種情況下，請使用「！」在IP前面。 例如 `utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1`

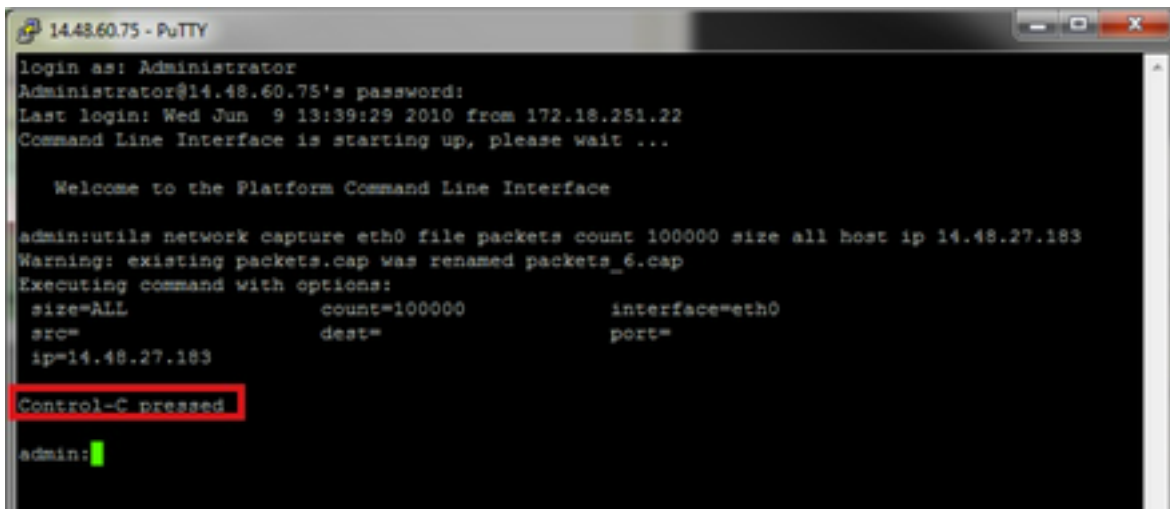
```
14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun  9 13:39:29 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...

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
```

3. 重現問題症狀 捕獲開始時，會重現問題症狀或狀況，以便在捕獲中包括必要的資料包。如果故障間歇性出現，則可能需要運行較長時間的捕獲。如果捕獲結束，則是因為緩衝區已滿，重新啟動捕獲，然後自動重新命名以前的捕獲，這樣就不會丟失以前的捕獲。如果需要長時間捕獲資料，請使用交換機上的監控會話在網路級別進行捕獲。
4. 停止捕獲 要停止捕獲，請按住**Control**鍵並按鍵盤上的**C**。這會導致捕獲進程結束，並且不會向捕獲轉儲中新增任何新資料包。

5.



```
1448.60.75 - 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

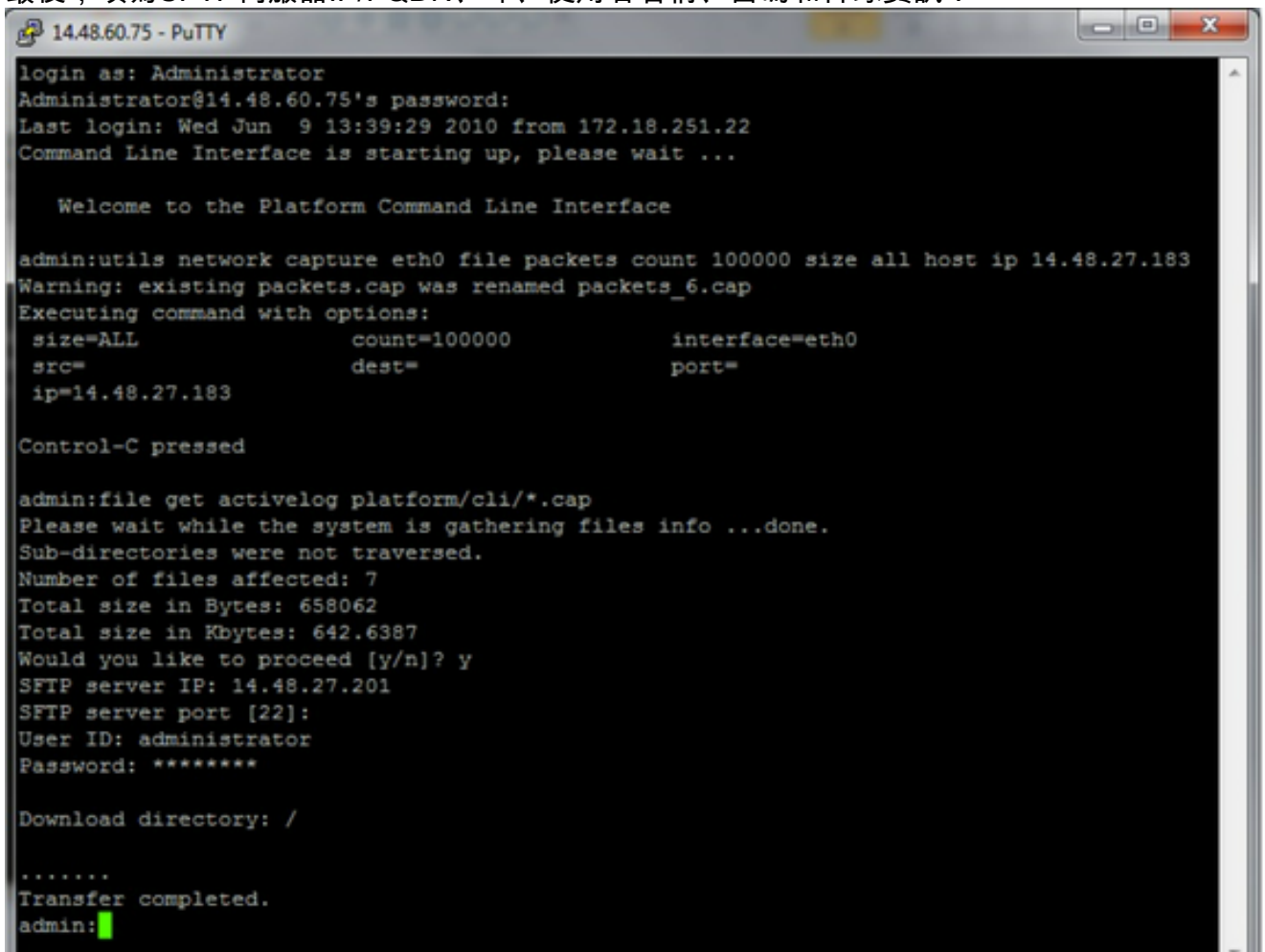
Control-C pressed

admin:
```

完成此操作後，捕獲檔案將儲存在伺服器上「activelog platform/cli/」位置

6. 從伺服器收集捕獲

捕獲檔案儲存在伺服器上的「activelog platform/cli/」位置。您可以使用RTMT通過CLI將檔案傳輸到SFTP伺服器或本地PC。4a。通過CLI將捕獲檔案傳輸到SFTP伺服器
使用命令 `file get activelog platform/cli/packets.cap` 將packets.cap檔案收集到SFTP伺服器。
或者，要收集伺服器上儲存的所有.cap檔案，請使用'`file get activelog platform/cli/*.cap`
最後，填寫SFTP伺服器IP/FQDN、埠、使用者名稱、密碼和目錄資訊：



```
1448.60.75 - 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:
```

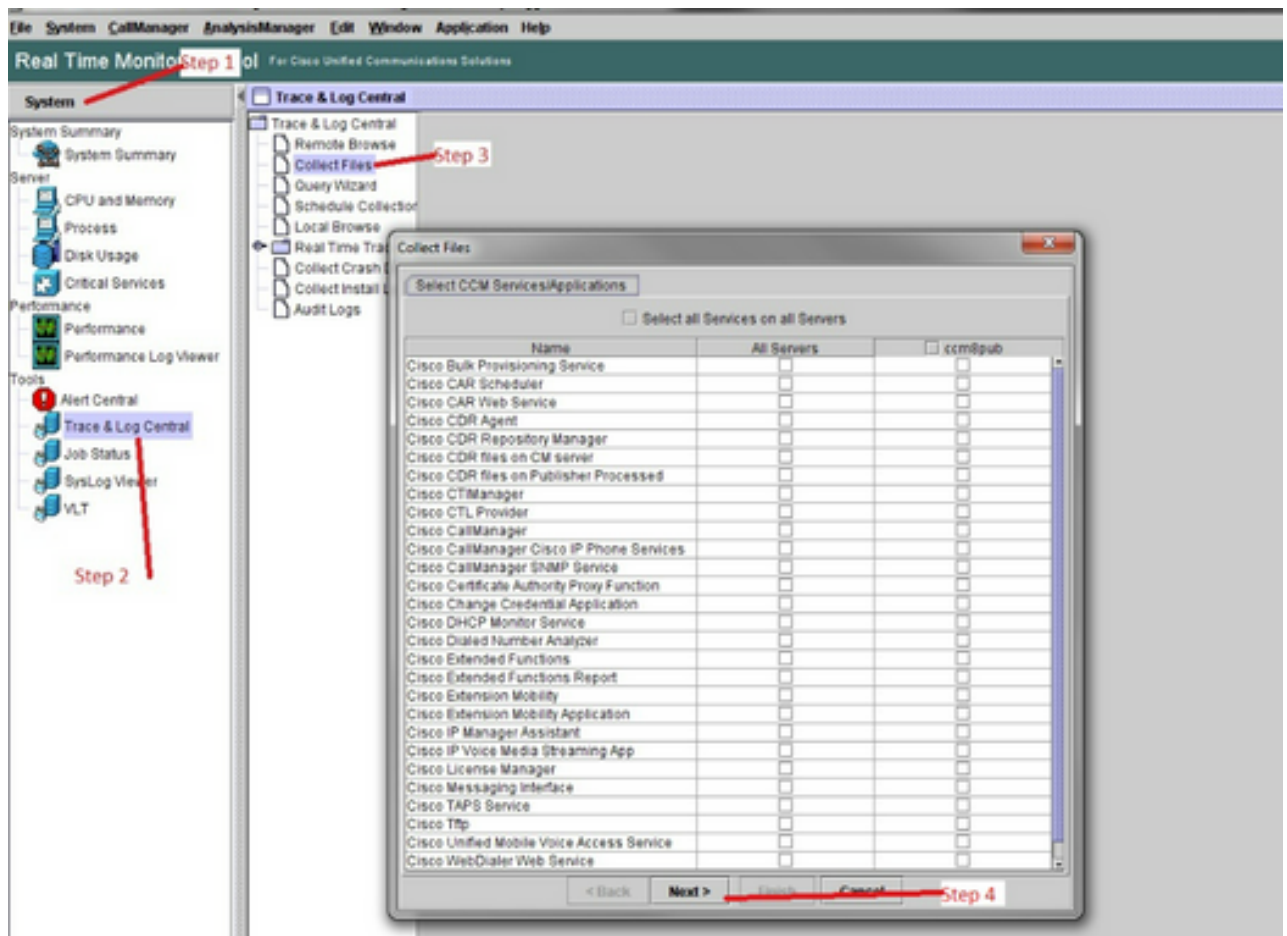
CLI指示檔案傳輸到SFTP伺服器的成敗。

4b. 使用RTMT將捕獲檔案傳輸到本地PC。

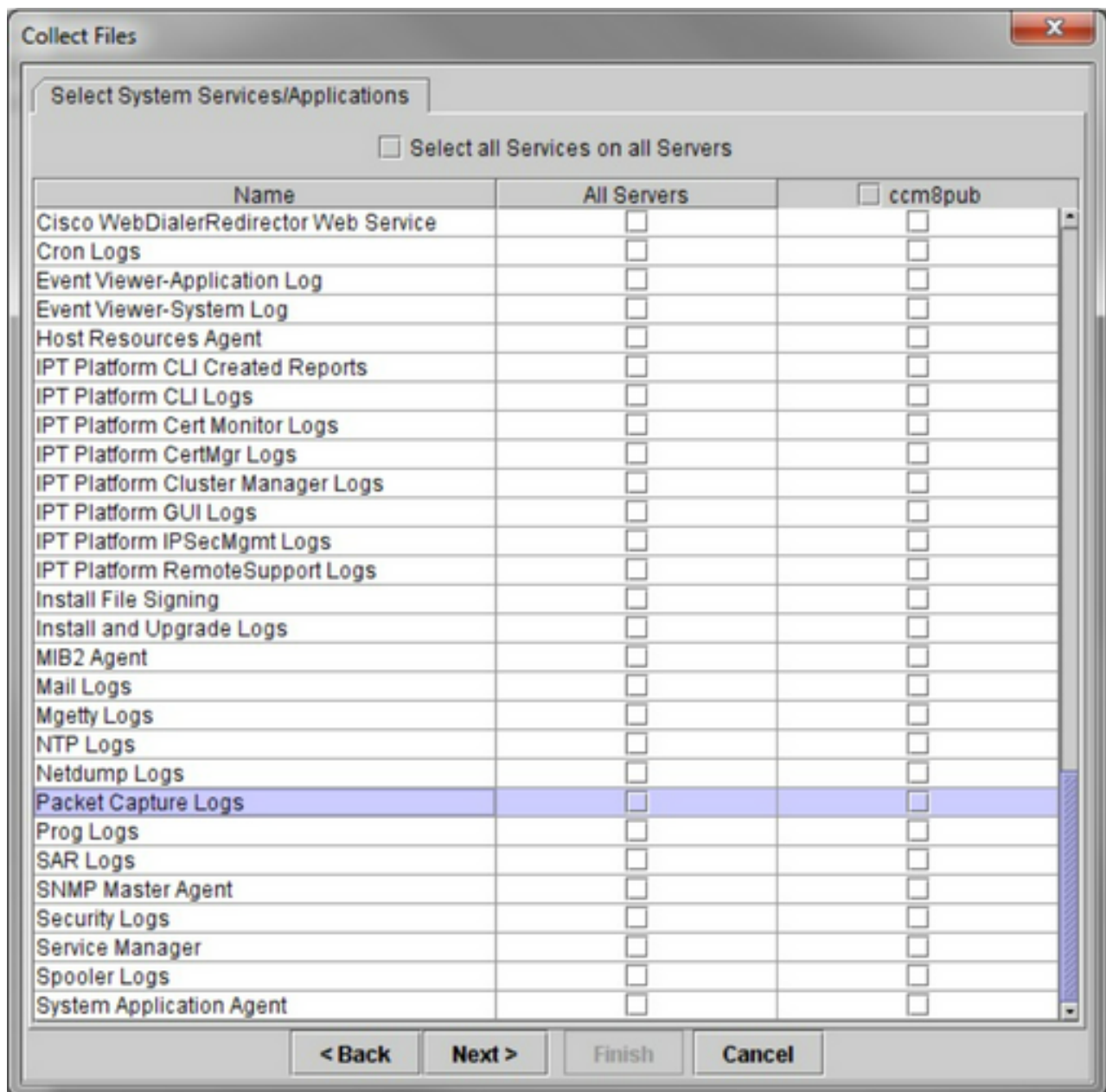
啟動RTMT。 如果未在本地PC上安裝，請從VOS管理頁面安裝適當的版本，轉到Applications-

>Plugins選單。

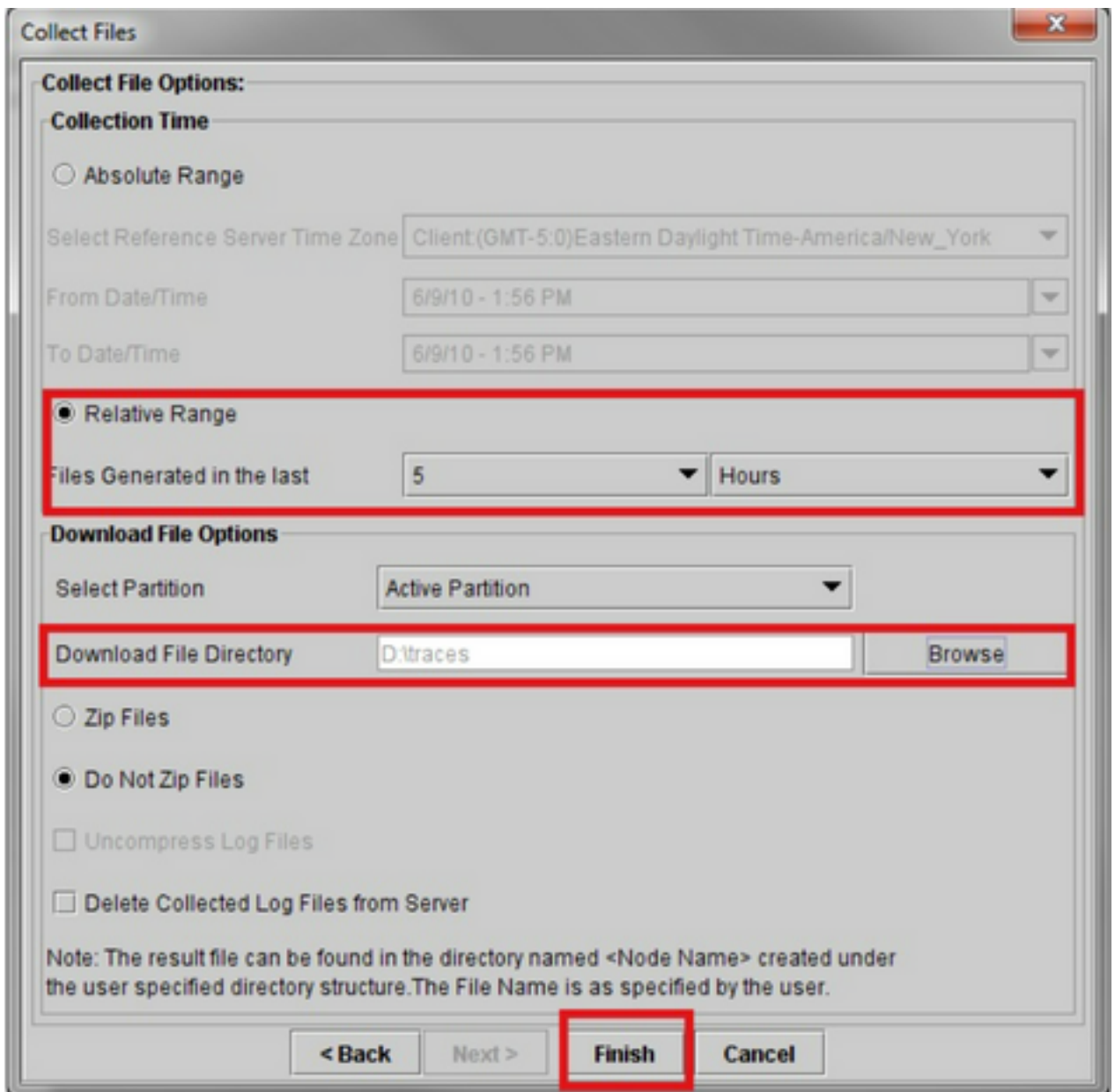
按一下System，然後按一下Trace & Log Central，然後按兩下Collect Files。 按一下第一個選單中的Next。



在第二個選單中，選中執行捕獲的伺服器上的Packet Capture Logs覈取方塊，然後按一下Next。



在最終螢幕上，選擇執行捕獲的時間範圍以及本地PC上的下載目錄。



RTMT將關閉此視窗並繼續收集檔案並將其儲存在指定位置的本地PC上。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。