

Establecer seguimientos y recopilar registros en CCE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Establecer seguimientos y recopilar registros de Finesse](#)

[Cliente Finesse](#)

[Opción 1: Recopilar registros de clientes a través del informe de errores de envío](#)

[Opción 2: Establecer registro persistente](#)

[Opción 3: Consola del explorador Web](#)

[Servidor Finesse](#)

[Opción 1: A través de la interfaz de usuario \(IU\): servicios web \(obligatorio\) y registros adicionales](#)

[Opción 2: Mediante SSH y el protocolo seguro de transferencia de archivos \(SFTP\): opción recomendada](#)

[Establecer seguimientos y recopilar registros de CVP y CVB](#)

[Servidor de llamadas CVP](#)

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

[Portal de administración y operaciones de CVP \(OAMP\)](#)

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

[Opción 1: A través de la cuenta de administración](#)

[Opción 2: Vía SSH y SFTP - Opción recomendada](#)

[Establecer registros de seguimiento y recopilación para CUBE y CUSP](#)

[CUBE \(SIP\)](#)

[CÚSPIDE](#)

[Recopilar los registros](#)

[Establecer el seguimiento y recopilar registros de UCCE](#)

[Establecer nivel de seguimiento](#)

[Recopilación de registros](#)

[Establecer registros de seguimiento y recopilación de PCCE](#)

[Establecer el seguimiento y recopilar registros de CUIC/Live Data/IDS](#)

[Descargar registros con SSH](#)

[Descargar registros con RTMT](#)

[Captura de paquetes en VoS \(Finesse, CUIC, VB\)](#)

Introducción

Este documento describe cómo establecer y recopilar seguimientos en Cisco Unified Contact Center Enterprise (CCE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Enterprise (UCCE)
- Paquete Contact Center Enterprise (PCCE)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Navegador de voz virtualizado (VB) de Cisco
- Cisco Unified Border Element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- Proxy Cisco Unified Session Initiation Protocol (SIP) (CUSP)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Versión 12.5 de Cisco Finesse
- Versión 12.5 del servidor CVP
- Versión 12.5 de UCCE/PCCE
- Versión 12.5 de Cisco VB
- Versión 12.5 de CUIC

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

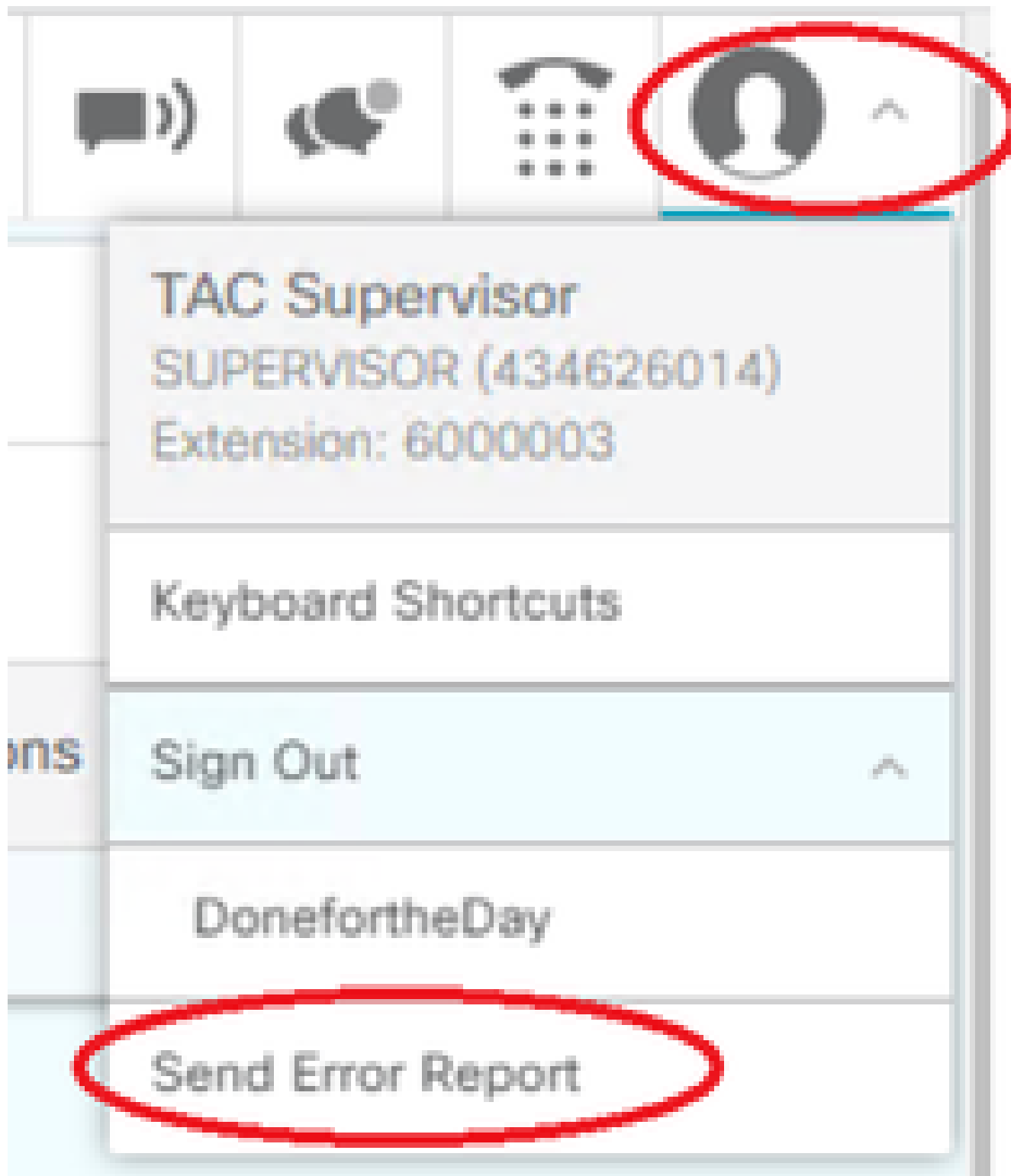
Establecer seguimientos y recopilar registros de Finesse

Cliente Finesse

Hay varias opciones para recopilar registros del cliente Finesse.

Opción 1: Recopilar registros de clientes a través del informe de errores de envío

1. Inicie sesión con un agente.
2. Si un agente experimenta algún problema durante una llamada o evento multimedia, indique al agente que haga clic en el enlace Enviar informe de errores situado en la esquina superior derecha del escritorio de Finesse.



3. El agente ve los registros enviados correctamente. mensaje.
4. Los registros del cliente se envían al servidor Finesse. Navegue hasta [Finesse Logs](#) e inicie sesión con una cuenta de administración.
5. Recopile los registros bajo el directorio clientlogs/.

Directory Listing For /logs/ - Up To /

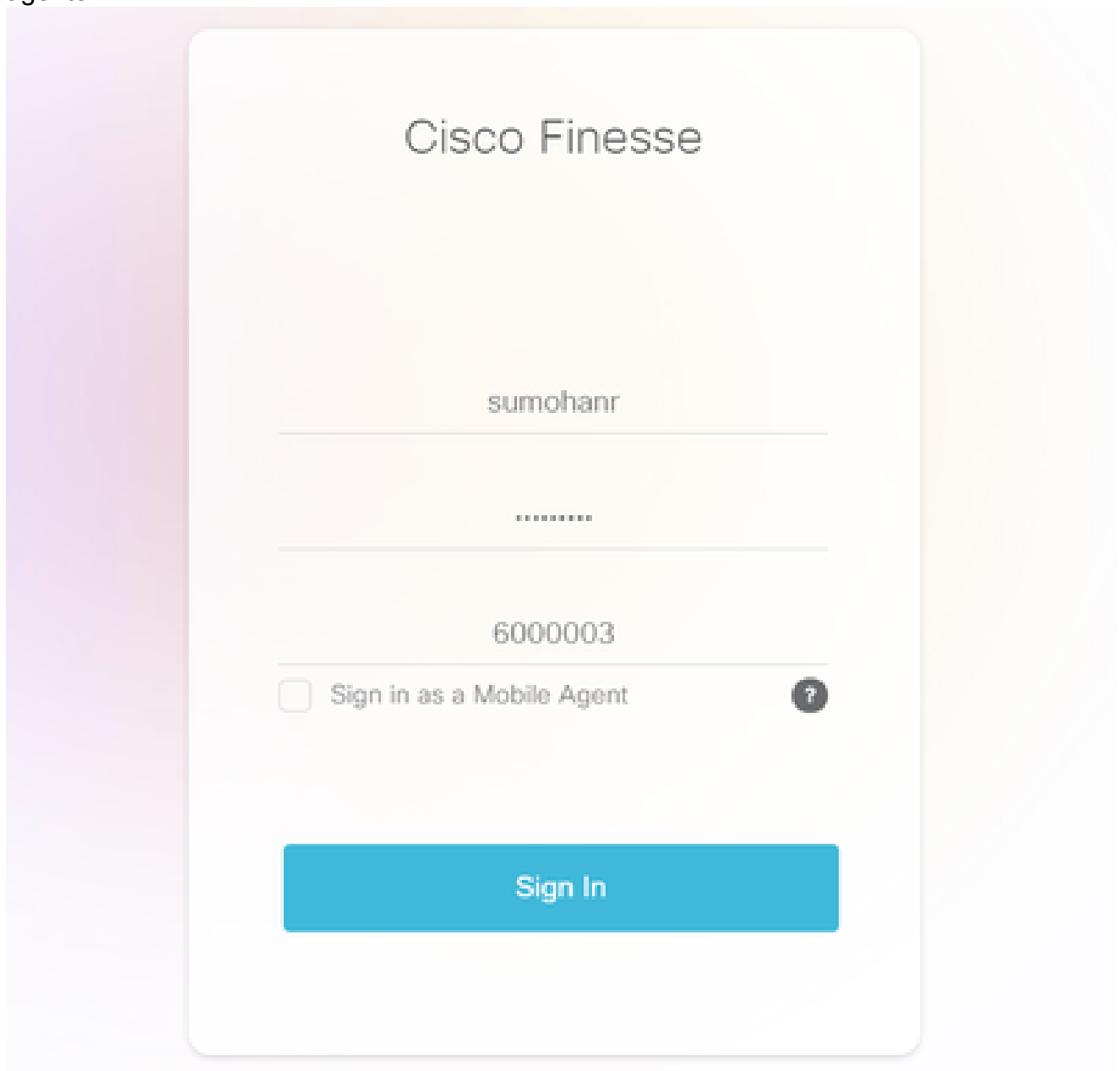
Filename	Size	Last Modif
3rdpartygadget/		Mon, 22 Feb 2021 23:06:32
admin/		Tue, 12 Jul 2022 18:52:53
cli.log	0.0 kb	Mon, 22 Feb 2021 22:59:10
clientlogs/		Wed, 17 Aug 2022 15:35:52

Opción 2: Establecer registro persistente

1. Vaya a [Registro local del escritorio](#).
2. Haga Clic En Iniciar Sesión Con Registro Persistente.



3. Se abre la página de inicio de sesión en Cisco Finesse Agent Desktop. Inicie sesión con el agente.

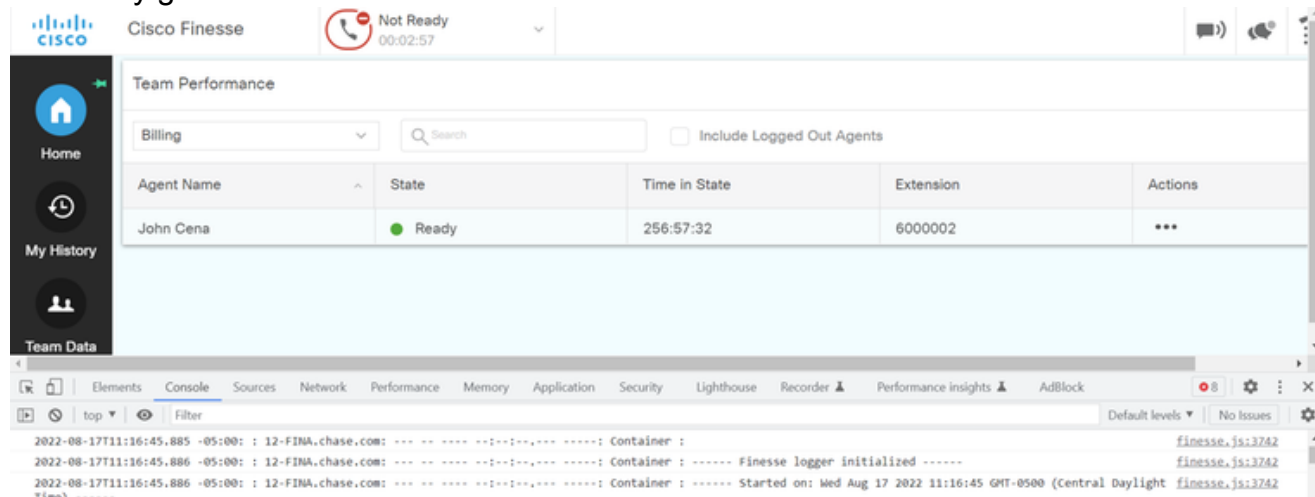


4. Toda la interacción del escritorio del agente se registra y se envía a los registros de almacenamiento local. Para recopilar los registros, navegue hasta [Registro local de](#)

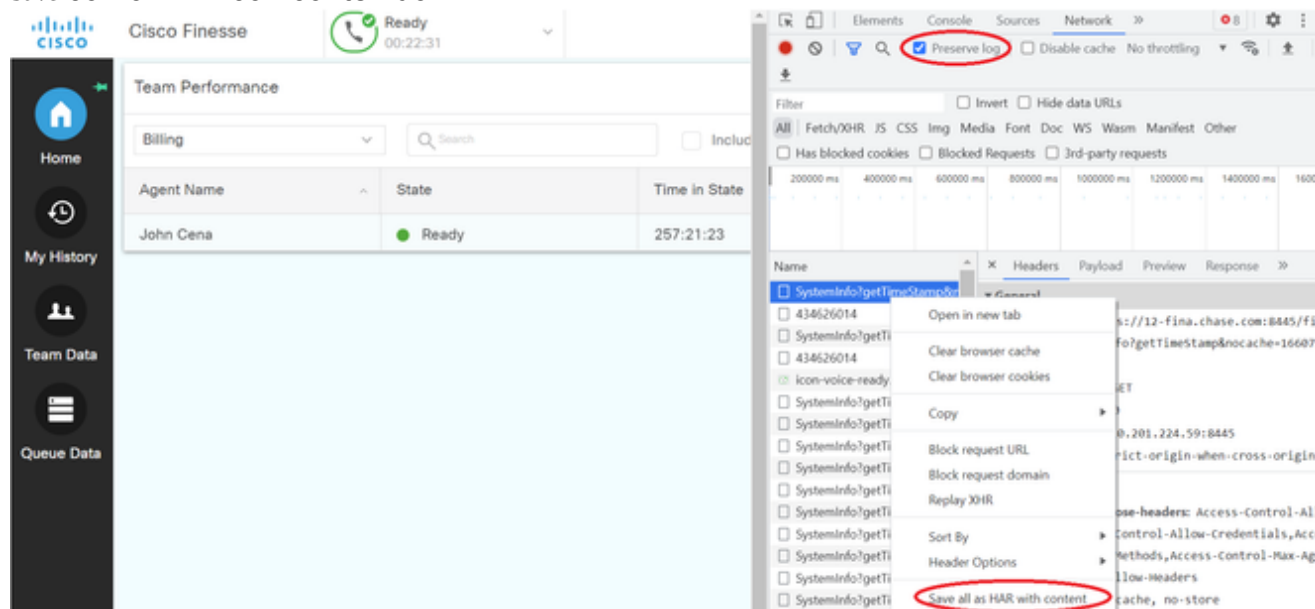
[escritorio](#) y copie el contenido en un archivo de texto. Guarde el archivo para analizarlo más a fondo.

Opción 3: Consola del explorador Web

1. Después de que un agente inicie sesión, presione F12 para abrir la consola del explorador.
2. Seleccione la pestaña Console.
3. Verifique la consola del navegador para ver si hay errores. Copie el contenido en un archivo de texto y guárdelo.



4. Seleccione la ficha Network y marque la opción Preserve log.
5. Haga clic con el botón derecho en cualquiera de los eventos de nombre de red y seleccione save como HAR con contenido.



Servidor Finesse

Opción 1: A través de la interfaz de usuario (IU): servicios web (obligatorio) y registros adicionales

1. Navegue hasta [Finesse Logs](#) e inicie sesión con la cuenta de administración.
2. Expanda el directorio 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
webservices/	Sun, 14 Aug 2022 07:41:43 G

Apache Tomcat/7.0.94

- Recopile los últimos registros de servicios web. Seleccione el último archivo de descompresión. Por ejemplo, Desktop-Webservices.201X-.log.zip. Haga clic en el enlace del archivo y verá la opción para Guardar el archivo.

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

- Recopile los otros registros requeridos (depende del escenario). Por ejemplo, openfire para problemas de servicio de notificación, registros de rango para problemas de autenticación y tomcatlogs para problemas de API.

 Nota: El método recomendado para recopilar los registros del servidor Cisco Finesse es a través de Secure Shell (SSH) y Secure File Transfer Protocol (SFTP). Este método no solo le permite recopilar los registros de servicios web, sino todos los registros adicionales, como Fippa, openfire, Realm y Clientlogs.

Opción 2: Mediante SSH y el protocolo seguro de transferencia de archivos (SFTP): opción recomendada

- Inicie sesión en el servidor Finesse con el SSH.
- Ingrese este comando para recopilar los registros que necesita. El comando recoge los registros durante 2 horas. Se le solicitará que identifique el servidor SFTP en el que se cargan los registros.

`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: 
```

- Estos registros se almacenan en la ruta del servidor SFTP: <IP address>\<date time stamp>\active_nnn.tgz , donde nnn es timestamp en formato largo.
- Para recopilar registros adicionales como tomcat, Context Service, Servm y los registros de instalación, consulte la sección Recopilación de registros de la [Guía de administración de Cisco Finesse versión 12.5\(1\)](#).

Establecer seguimientos y recopilar registros de CVP y CVB

Servidor de llamadas CVP

- El nivel predeterminado de seguimientos de CVP CallServer es suficiente para resolver la

mayoría de los casos. Sin embargo, cuando necesite obtener más detalles sobre los mensajes del Protocolo de inicio de sesión (SIP), debe establecer los seguimientos de la pila SIP en el nivel DEBUG.

2. Vaya a la página web de CVP CallServer Diag URL Local Host 8000.



Nota: Esta página proporciona buena información sobre CVP CallServer y es muy útil para resolver ciertos escenarios.

3. Seleccione com.dynamicSoft.DsLibs.DsUALibs en el Serv. Menú desplegable Mgr en la esquina superior izquierda.

The screenshot shows a web interface with a table-like structure. The first column contains labels: 'Serv Mgr:', 'Level:', 'INFRA', '_SUBSYSTEM', 'ID:', 'DETAIL:', and 'AGE_HANDLI'. The second column contains a dropdown menu for 'Serv Mgr:' which is currently open, displaying a list of options. The options are: 'org.springframework', 'org.springframework', 'SIP', 'org.apache', 'RPT', 'SIP.INOUT', 'com.dynamicsoft.DsLibs.DsUALibs' (which is highlighted in blue), 'Infrastructure', 'IVR', 'mmca', 'ICM', 'VMS', and 'MSGBUS'.

Serv Mgr:	org.springframework
Level:	org.springframework
	SIP
INFRA	org.apache
	RPT
_SUBSYSTEM	SIP.INOUT
ID:	com.dynamicsoft.DsLibs.DsUALibs
	Infrastructure
	IVR
DETAIL:	mmca
	ICM
AGE_HANDLI	VMS
	MSGBUS

4. Haga clic en el botón Set.

MESSAGE:

RPT_JDBC:

RPT_CALL_REG:

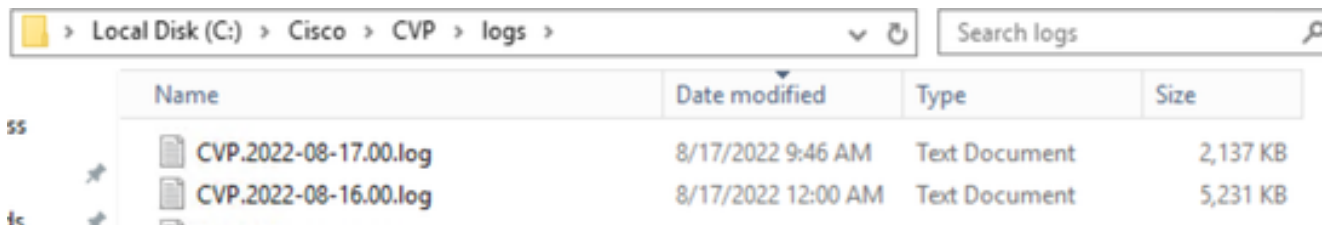
RPT_BATCH:

Set

5. Desplácese hacia abajo en la ventana de seguimiento para asegurarse de que el nivel de seguimientos se ha establecido correctamente. Estos son los ajustes de depuración.

NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
SIPINOUT	WARN	0
com.dynamicsoft.DsLibs.DsUALibs	DEBUG	0
Infrastructure	INFO	0
IVR	DEBUG	41
imca	INFO	0
ICM	DEBUG	41
MSOBUS	INFO	0

6. Cuando reproduzca el problema, recopile los registros de C:\Cisco\CVP\logs y seleccione el archivo de registro de CVP en función de la hora a la que se produjo el problema.



7. Después de reproducir el problema, asegúrese de restaurar los seguimientos al nivel predeterminado. Seleccione `com.dynamicsoft.DsLibs.DsUALibs` en el Serv. Menú desplegable Mgr en la esquina superior izquierda y establézcalo en error.

Serv Mgr: `com.dynamicsoft.DsLibs.DsUALibs` Level: `DEBUG`

STANDARD		INFRA		LEGACY MSG		ICM CUSTOM	
ALL:	☐	LOAD_SUBSYSTEM:	☐	MSG_LAYER_MESSAGE:	☐	GED125_LOW_LEVEL:	☐
CALL:	☐	THREAD:	☐	MSG_LAYER_METHOD:	☐	MSGBUS_LOW_LEVEL:	☐
METHOD:	☐	MSG:	☐	MSG_LAYER_HANDLED_EXCEPTION:	☐	ICM_SUBSYSTEM_ADMIN:	☐
PARAM:	☐	MSG_DETAIL:	☐	MSG_LAYER_PARAM:	☐		
LOW_LEVEL:	☐	MESSAGE_HANDLING:	☐	GLOBAL_EVENT:	☐		
CLASSDUMP:	☐	TIMER:	☐	EXTERNAL_EVENT:	☐		
HEARTBEAT:	☐	STATE:	☐	STATIC_FIELD:	☐		
HANDLED_EXCEPTION:	☐	SECURITY:	☐	EXTERNAL_STATE:	☐		
OOOQUEUE:	☐	LICENSING:	☐	INTERNAL_STATE:	☐		
GARBAGE_COLLECTOR:	☐	STARTUP:	☐	CODE_BRANCH:	☐		
MESSAGE:	☐	SHUTDOWN:	☐	CODE_MARKER:	☐		
RPT_JDBC:	☐	STATS:	☐	CLASS_DUMP:	☐		
RPT_CALL_REG:	☐	SNMP:	☐	LOCAL_DUMP:	☐		
RPT_BATCH:	☐	SAF:	☐				

Set

DEBUG/0 - DEBUG/41 - DEBUG/40

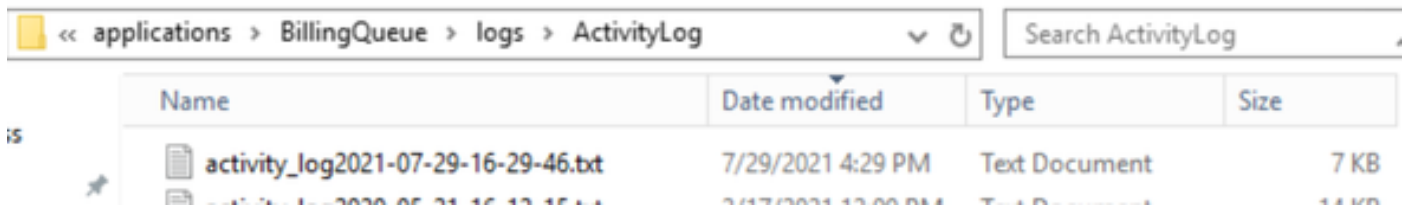
NAME	LEVEL	MASK
SIP	DEBUG	41
org.springframework	WARN	0
org.apache	ERROR	0
RPT	INFO	0
SIP.INOUT	WARN	0
<code>com.dynamicsoft.DsLibs.DsUALibs</code>	ERROR	0
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
ALL_SS	INFO	0
MSGBUS	INFO	0

Aplicación CVP Voice XML (VXML)

En muy raras circunstancias, es necesario aumentar el nivel de seguimientos de las aplicaciones del servidor VXML. Por otro lado, no se recomienda aumentarlo a menos que lo solicite un ingeniero de Cisco.

Para recopilar los registros de la aplicación del servidor VXML, desplácese hasta el directorio de aplicación específico bajo el servidor VXML, por ejemplo:

`C:\Cisco\CVP\VXMLServer\applications\{nombre de la aplicación}\logs\ActivityLog\` y recopile los registros de actividad.



Portal de administración y operaciones de CVP (OAMP)

En la mayoría de los casos, el nivel predeterminado de trazas de OAMP y ORM es suficiente para determinar la causa raíz del problema. Sin embargo, si es necesario aumentar el nivel de seguimientos, estos son los pasos para ejecutar esta acción:

1. Copia de seguridad de %CVP_HOME%\conf\oamp.properties.
2. Edite %CVP_HOME%\conf\oamp.properties.

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

3. Reinicie OPSConsoleServer después de la modificación como se muestra.

Información de nivel de seguimiento

Nivel de seguimiento	Descripción	Nivel de registro	Máscara de seguimiento
0	Instalación predeterminada del producto. Se espera un impacto mínimo en el rendimiento.	INFO	Ninguno
1	Mensajes de seguimiento menos detallados con un pequeño impacto en el rendimiento.	DEPURAR	DEVICE_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x01011000
2	Mensajes de seguimiento detallados con un impacto medio en el rendimiento.	DEPURAR	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x05011000

Nivel de seguimiento	Descripción	Nivel de registro	Máscara de seguimiento
3	Mensaje de seguimiento detallado con un impacto de alto rendimiento.	DEPURAR	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + OPERACIONES_MASIVAS + DATABASE_MODIFY + MANAGEMENT=0x05111000
4	Mensaje de seguimiento detallado con un impacto de muy alto rendimiento.	DEPURAR	MISC + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + OPERACIONES_MASIVAS + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + DATABASE_SELECT + INFORMACIÓN_PO_BASE_DATOS + GESTIÓN + MÉTODO_DE_SEGUIMIENTO + TRACE_PARAM=0x17371000
5	Mensaje de seguimiento más detallado.	DEPURAR	MISC + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + OPERACIONES_MASIVAS + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + DATABASE_SELECT + INFORMACIÓN_PO_BASE_DATOS + GESTIÓN + MÉTODO_DE_SEGUIMIENTO + TRACE_PARAM=0x17371006

Cisco Virtualized Voice Browser (CVB)

En CVB, un archivo de seguimiento es un archivo de registro que registra la actividad de los subsistemas y pasos de los componentes de Cisco VB.

Cisco VB tiene dos componentes principales:

- 1. Los seguimientos de Cisco VB Administration se denominan registros MADM
- 2. Los seguimientos del motor Cisco VB se denominan registros MIVR

Puede especificar los componentes para los que desea recopilar información y el nivel de información que desea recopilar.

Los niveles de registro se extienden desde:

- Depuración: detalles básicos del flujo para
- XDebugging 5 - Nivel detallado con Stack Trace

Cisco Virtualized Voice Browser Serviceability

For Cisco Virtualized Voice Browser

Navigation Cisco VVB Serviceability

Administrator | About | L

Alarm Trace Tools Help

Trace Configuration - Cisco Virtualized Voice Browser Engine

Save

Restore Defaults

Check All

UnCheck All

Status

Ready

Select Service

Select Service * Engine

Go

Trace Output settings

Maximum No. of Files * 300

Maximum File Size (KB) * 10485

Trace Filter Setting

Subfacility	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
LIBRARIES						
LIB_CFG	☐	☐	☐	☐	☐	☐
LIB_EVENT	☐	☐	☐	☒	☐	☐
LIB_JDBC	☐	☐	☐	☐	☐	☐
LIB_JINI	☐	☐	☐	☐	☐	☐
LIB_LICENSE	☐	☐	☐	☐	☐	☐
LIB_MEDIA	☐	☐	☐	☐	☐	☐
LIB_RMI	☐	☐	☐	☐	☐	☐
LIB_SERVLET	☐	☐	☐	☐	☐	☐
LIB_TC	☐	☐	☐	☐	☐	☐
MANAGERS						

 Advertencia: No se debe habilitar Xdebugging5 en el sistema de producción cargado.

Los registros más comunes que debe recopilar son el motor. El nivel predeterminado de seguimientos para los seguimientos del motor CVB es suficiente para resolver la mayoría de los problemas. Sin embargo, si necesita cambiar el nivel de seguimientos para un escenario específico, Cisco recomienda que utilice los perfiles de registro del sistema predefinidos.

Perfiles de registro del sistema

Nombre	Escenario en el que se debe activar este perfil
VB predeterminado	Los registros genéricos están habilitados.
AppAdminVB	Para problemas con la administración web a través de AppAdmin, Cisco VB Serviceability y otras páginas web.

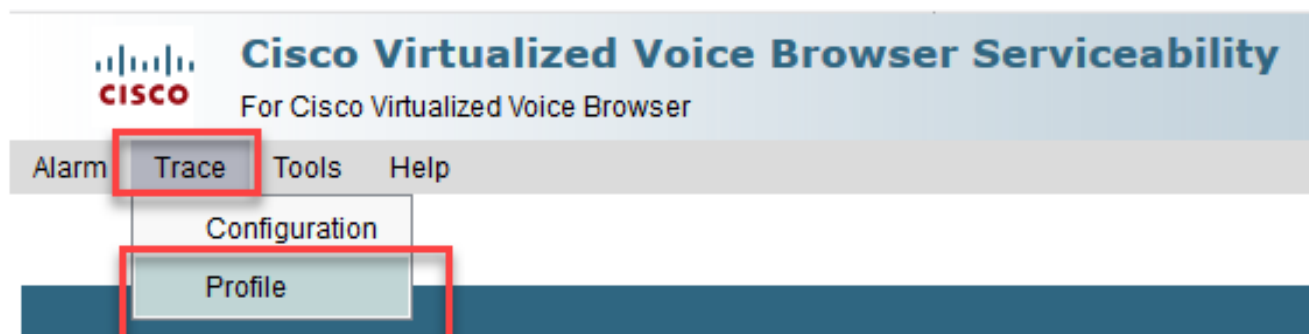
MediaVB	Para problemas con la configuración o transmisión de medios.
NavegadorVozVB	Para problemas con el manejo de llamadas.
MRCPVB	Para problemas con ASR/TTS con la interacción de Cisco VB.
CallControlVVB	Para problemas relacionados con la señal SIP, se publican en el registro.

Opción 1: A través de la cuenta de administración

1. Abra la página principal de CVB, [UCCX Service Main](#), y navegue hasta la página Cisco VB Serviceability. Inicie sesión con la cuenta de administración.



2. Seleccione Trace > Profile.



3. Marque el perfil que desea habilitar para el escenario específico y haga clic en el botón Enable. Por ejemplo, habilite el perfil CallControlVB para problemas relacionados con SIP o MRCPVB para problemas relacionados con la interacción de reconocimiento automático de voz y texto a voz (ASR/TTS).



Cisco Virtualized Voice Browser Serviceability

For Cisco Virtualized Voice Browser

AlarmTraceToolsHelp

Log Profiles Management

 Enable

Status

 Ready

Profiles

☐ [MediaVVB](#)

☐ [DefaultVVB](#)

☐ [AppAdminVVB](#)

☐ [VoiceBrowserVVB](#)

☒ [CallControlVVB](#)

☐ [MRCPVVB](#)

Enable

4. Verá el mensaje de confirmación después de hacer clic en el botón enable.



Cisco Virtualized Voice Browser Serviceability

For Cisco Virtualized Voice Browser

AlarmTraceToolsHelp

Log Profiles Management

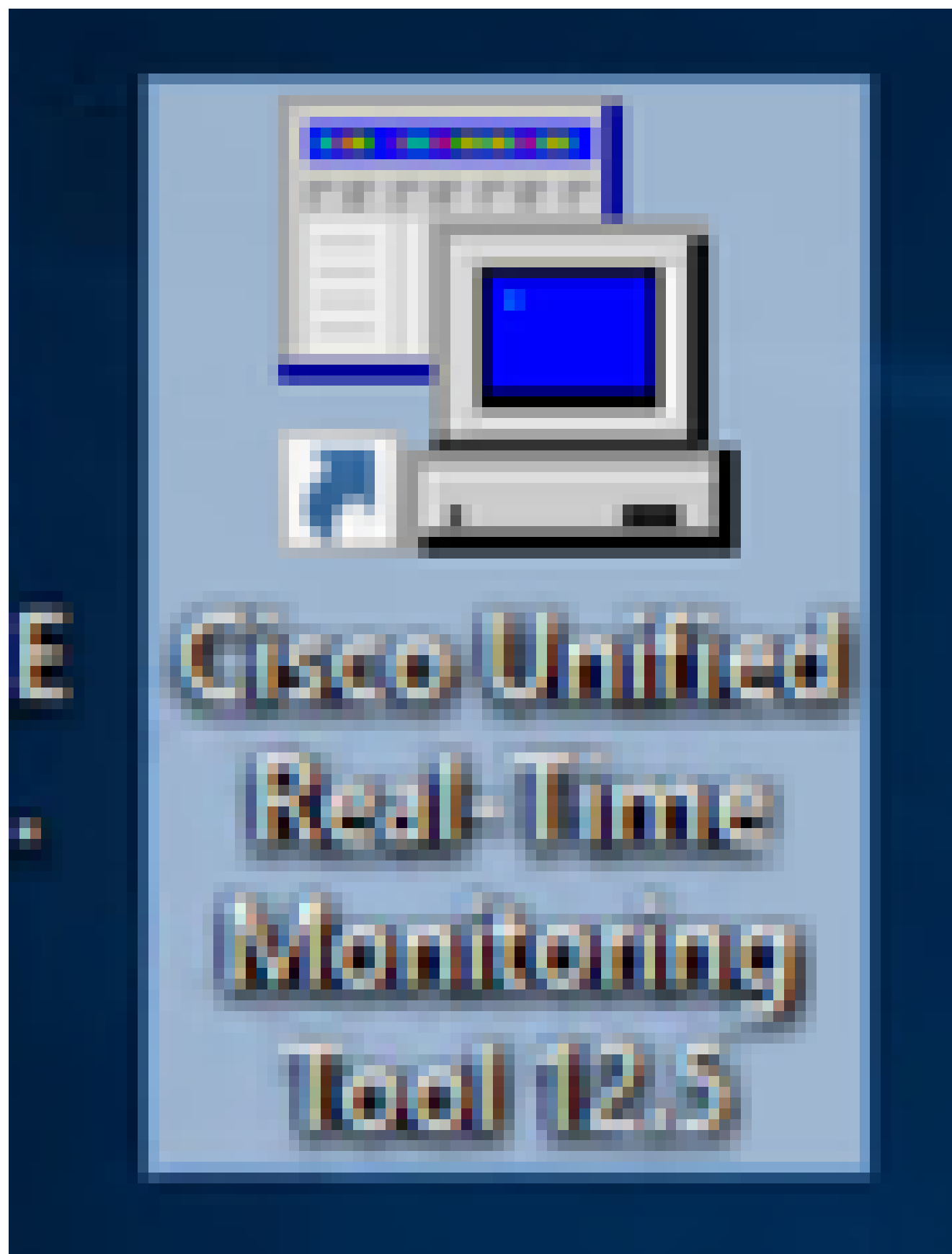
 Enable

Status

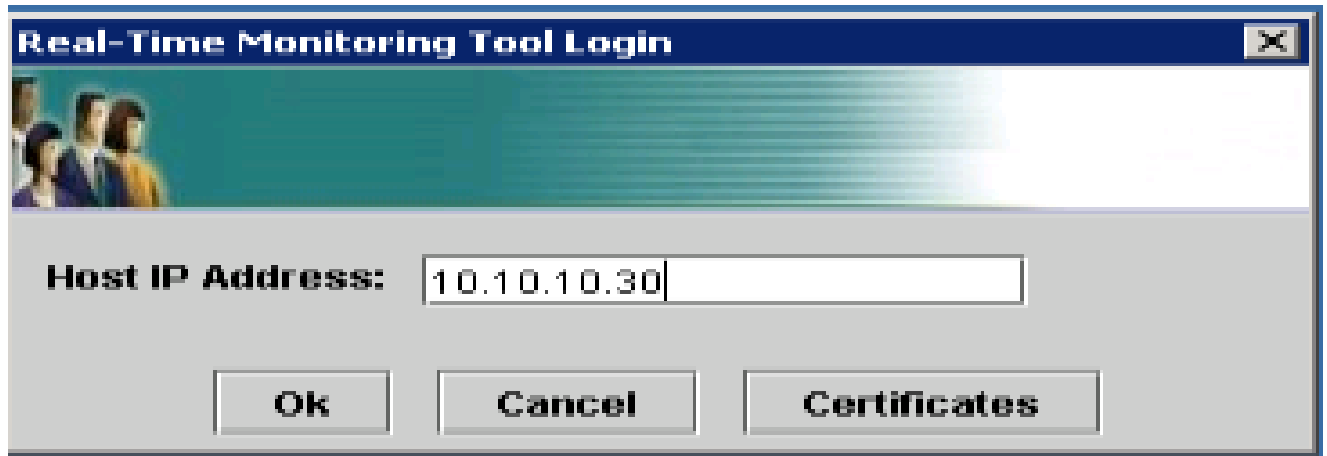
 CallControlVVB log profile configurations have been enabled successfully.

5. Una vez reproducido el problema, recopile los registros. Utilice la herramienta Real Time Monitor Tool (RTMT) que viene con CVB para recopilar los registros.
6. Haga clic en el icono Cisco Unified Real-Time Monitoring Tool en el escritorio (si es

necesario, descargue esta herramienta del CVB).



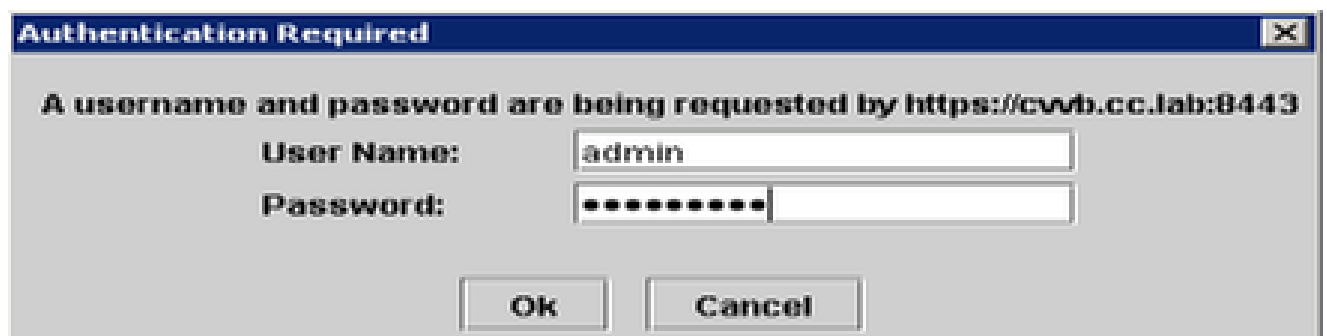
7. Proporcione la dirección IP del VB y haga clic en OK.



8. Acepte la información del certificado, si se muestra



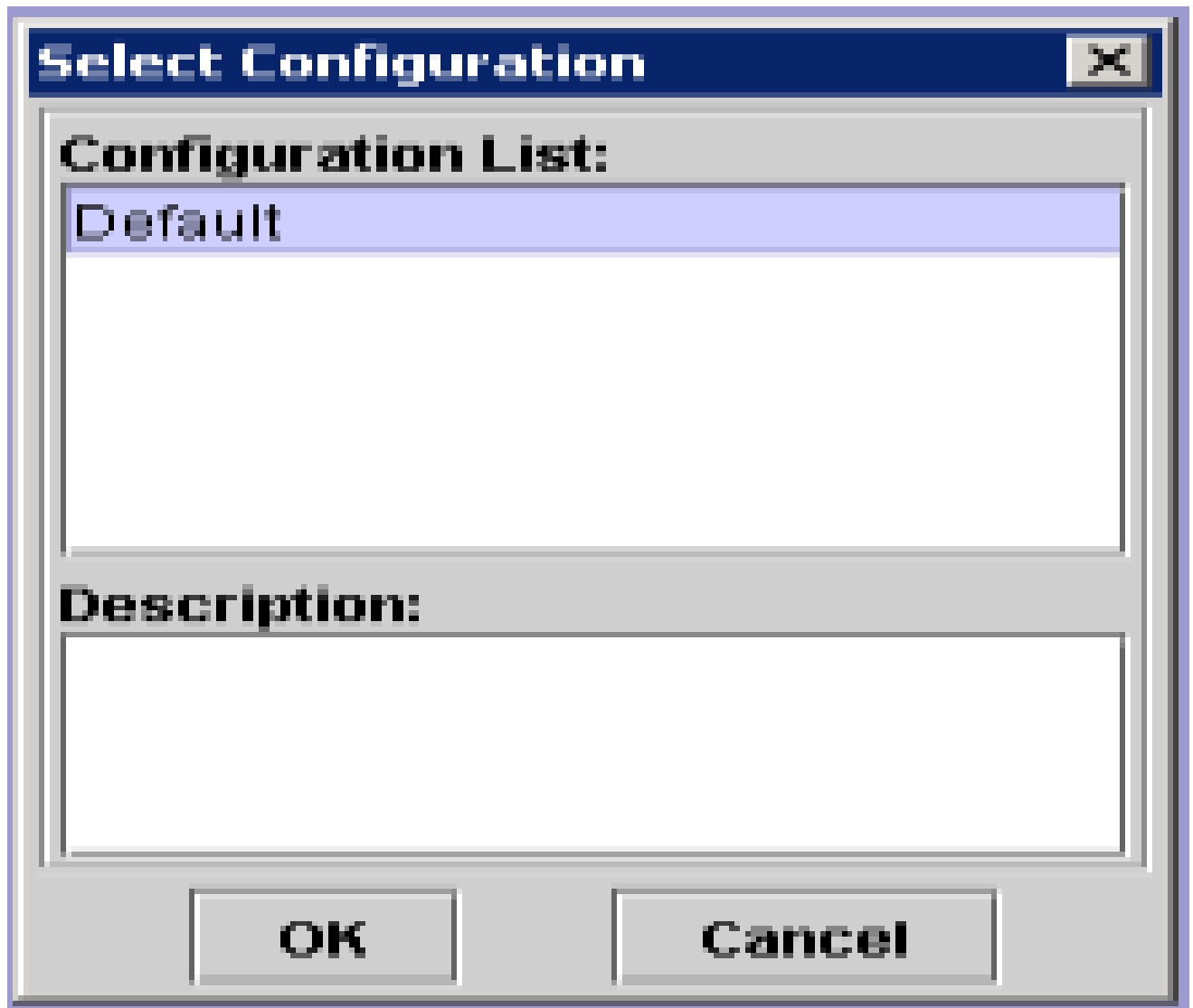
9. Proporcione la credencial y haga clic en Aceptar.



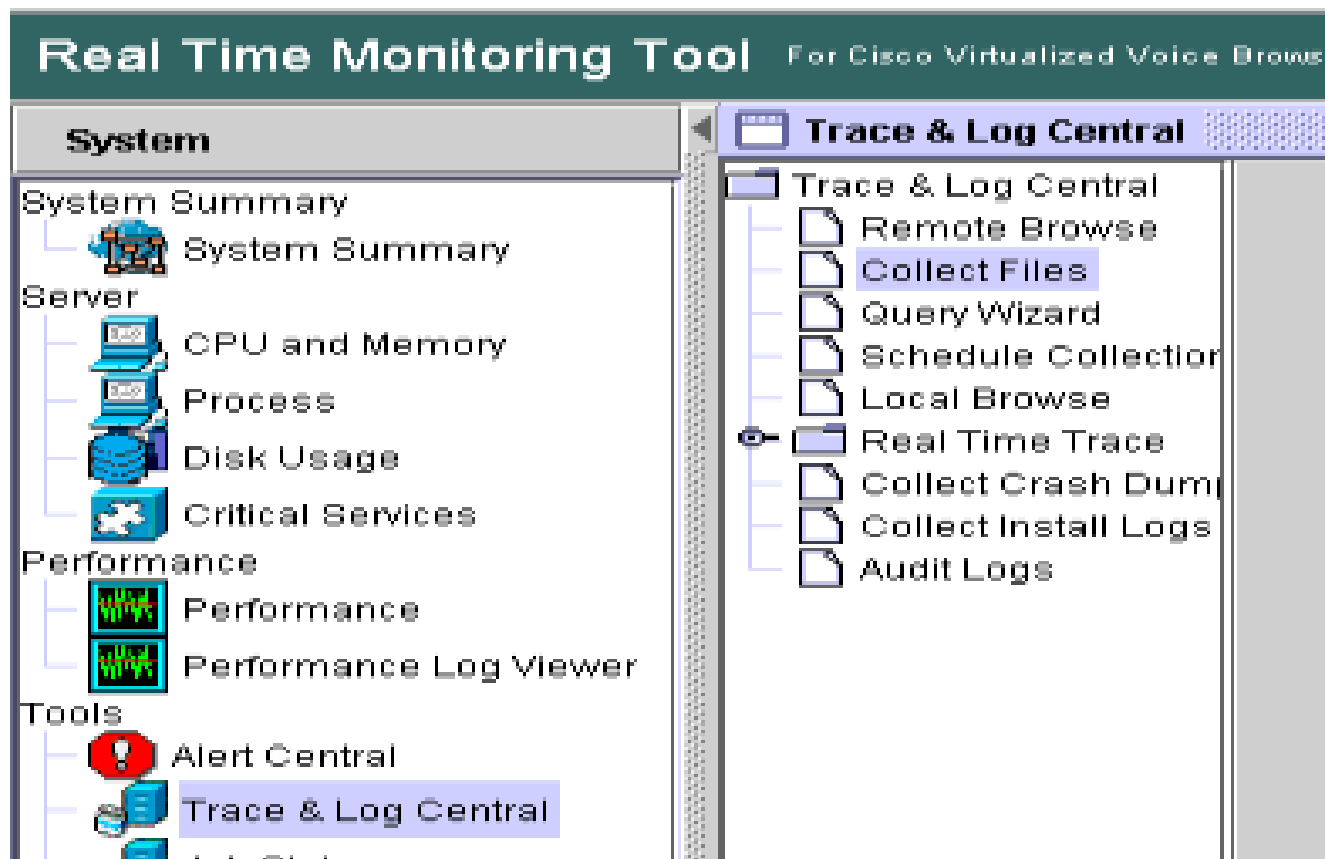
10. Si recibe el error TimeZone, RTMT puede cerrarse después de hacer clic en el botón Yes. Vuelva a iniciar la herramienta RTMT.



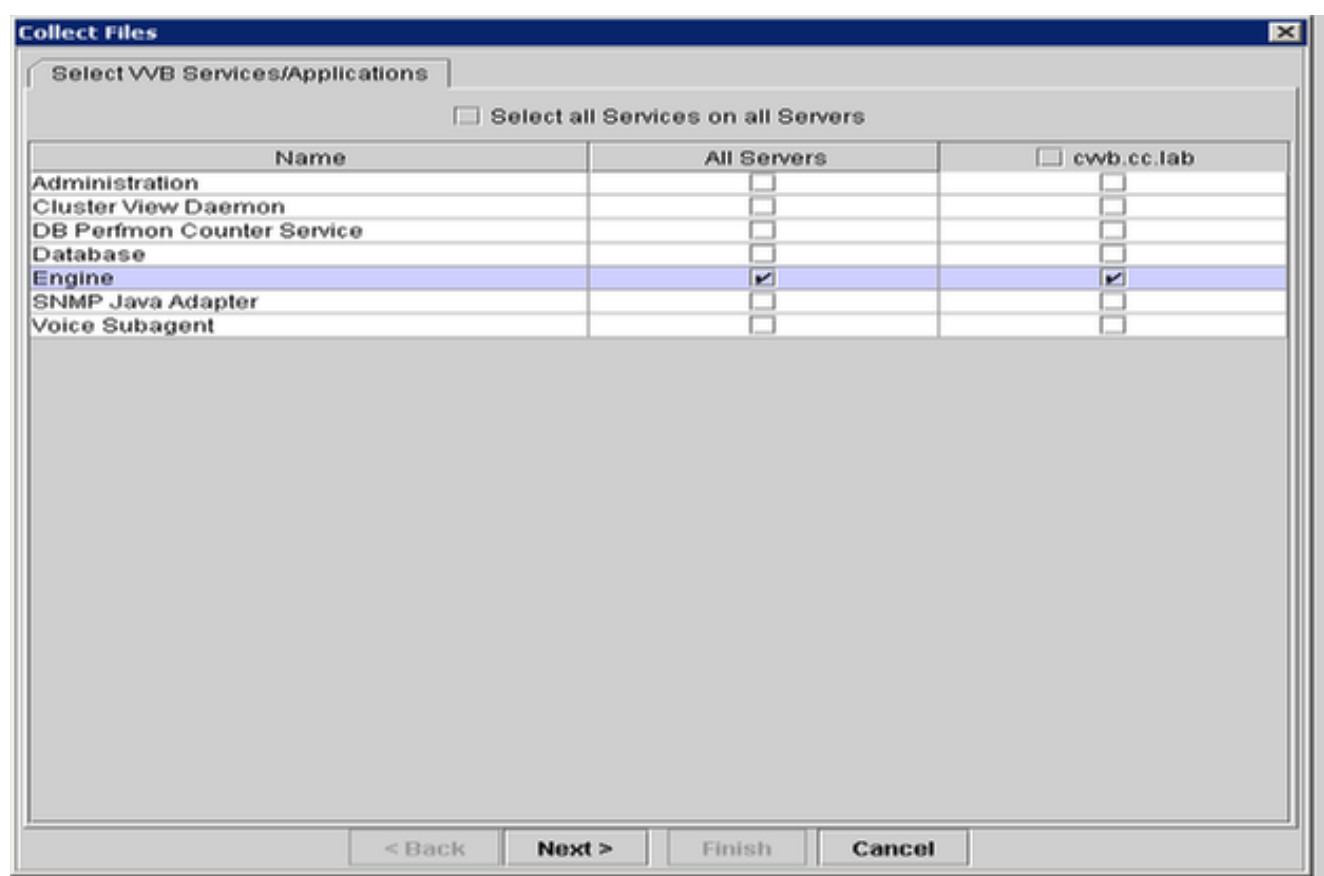
11. Deje seleccionada la configuración predeterminada y haga clic en Aceptar.



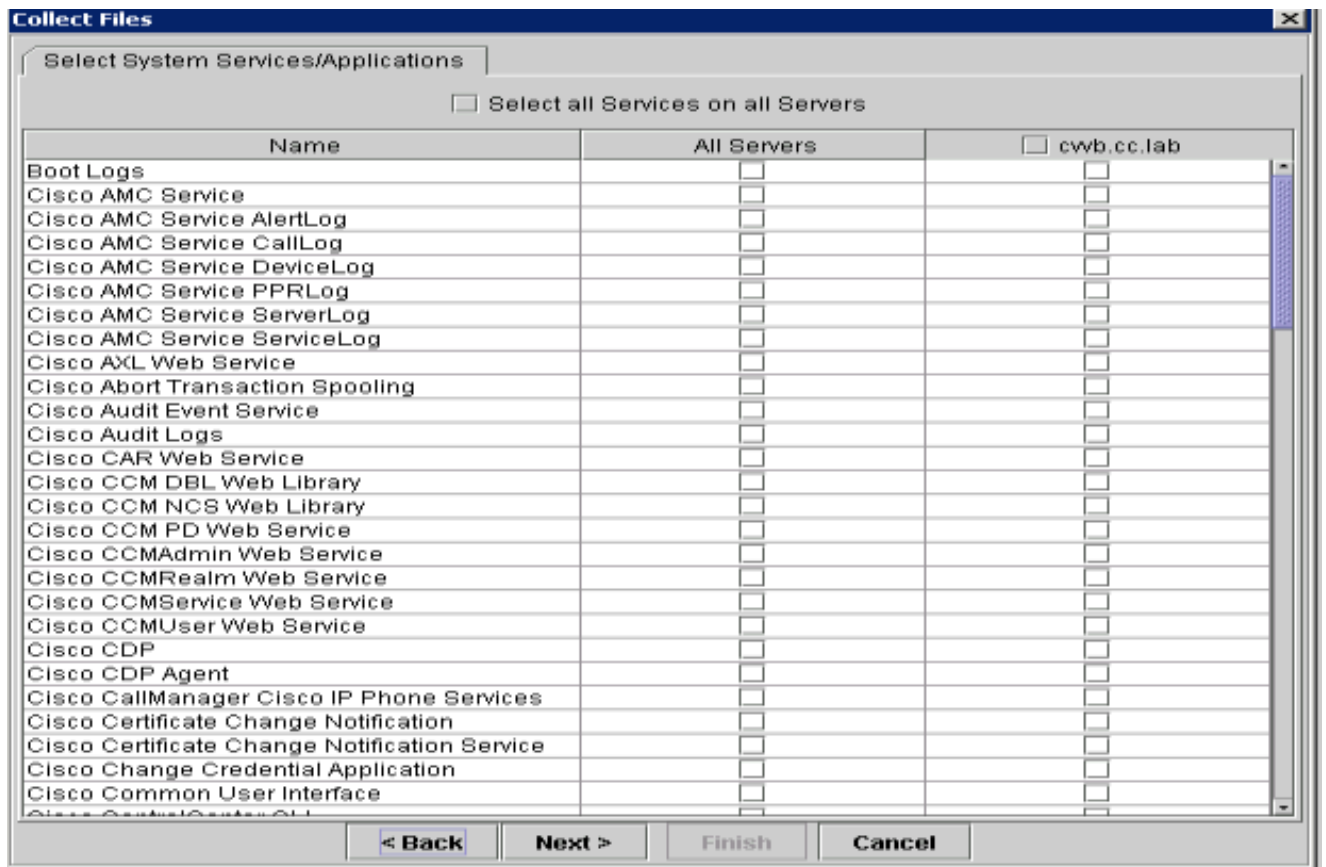
12. Seleccione Trace & Log Central y, a continuación, haga doble clic en Collect Files.



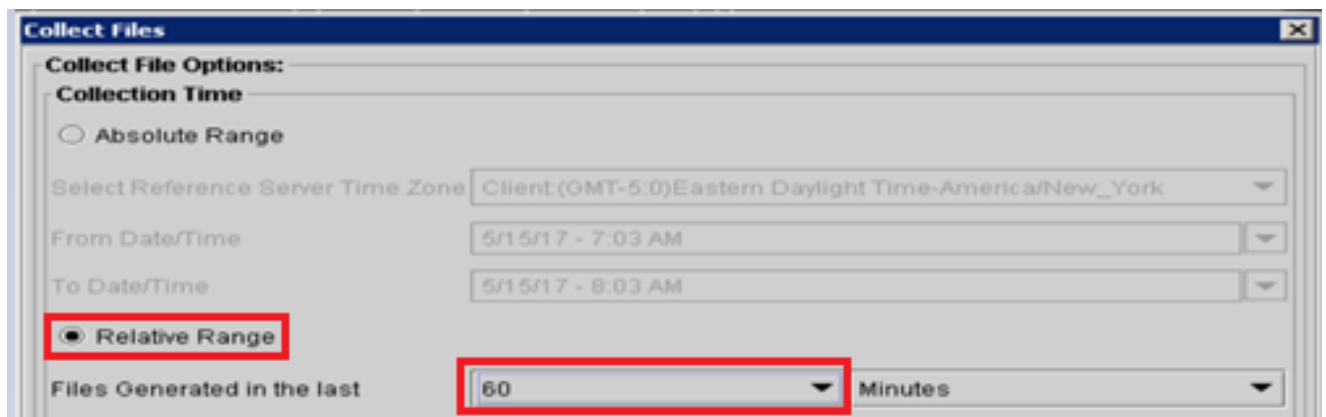
13. En la nueva ventana abierta, seleccione el Motor y haga clic en Siguiente.



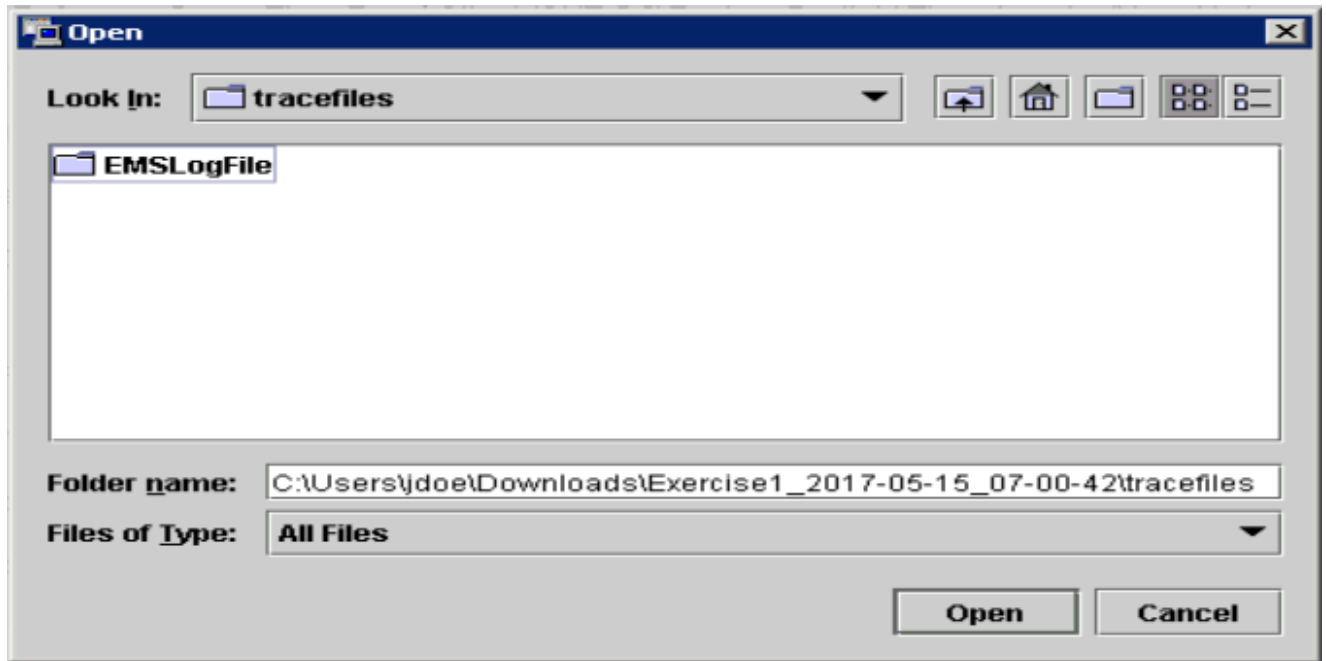
14. Haga clic en Next nuevamente en la siguiente ventana.



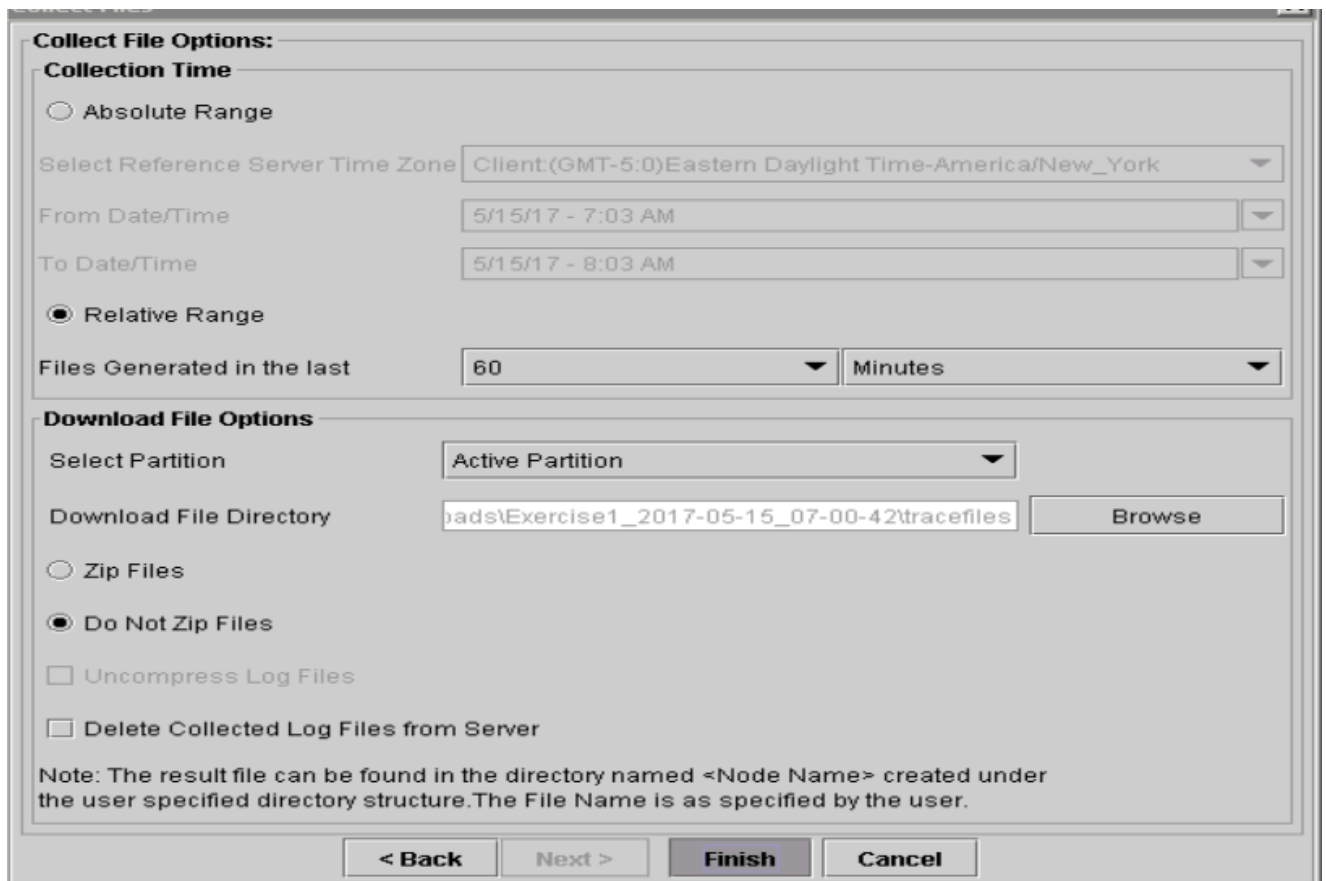
15. Seleccione Relative Range y asegúrese de seleccionar time para cubrir el tiempo de la llamada incorrecta.



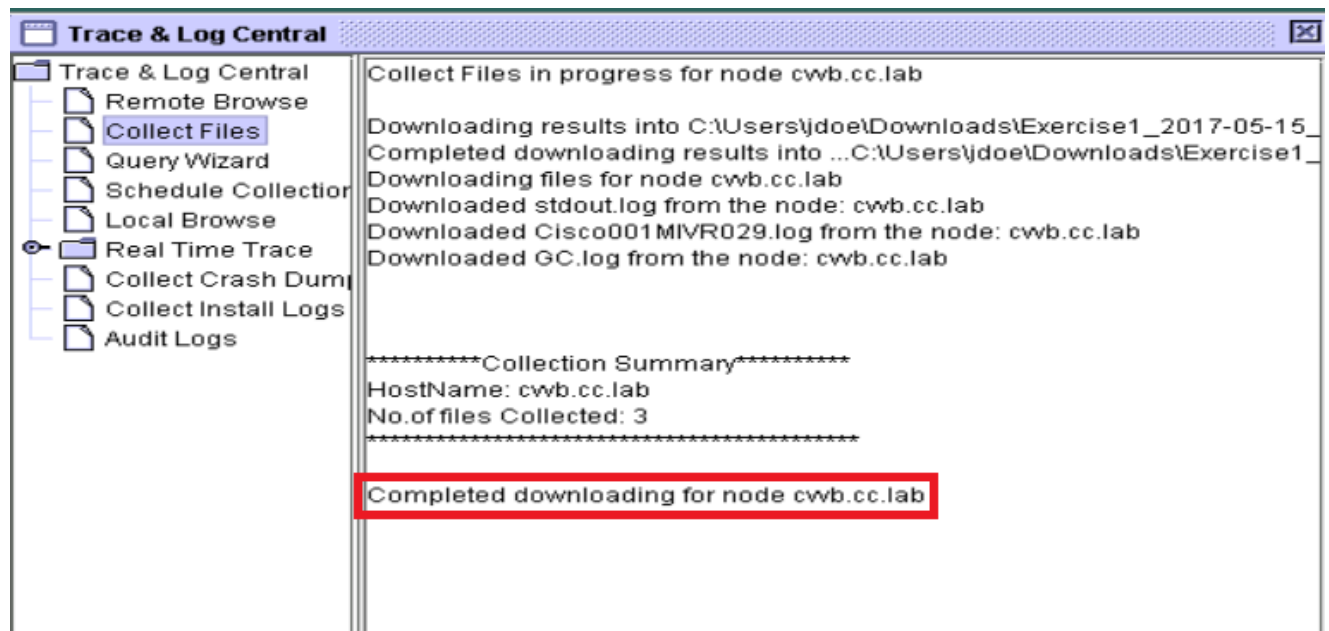
16. En Download File Options, haga clic en Browse y seleccione el directorio donde desea guardar el archivo, luego haga clic en Open.



17. Una vez seleccionado todo, haga clic en el botón Finalizar.



18. Esto recopila los archivos de registro. Espere hasta que vea el mensaje de confirmación en RTMT.



19. Vaya a la carpeta donde se guardan los seguimientos.
20. Los registros del motor son todo lo que necesita. Para encontrarlos, navegue hasta la carpeta `\<time stamp>\uccx\log\MIVR`.

Opción 2: Vía SSH y SFTP - Opción recomendada

1. Inicie sesión en el servidor VB con Secure Shell (SSH).
2. Ingrese este comando para recopilar los registros que necesita. Los registros se comprimen y se le solicita que identifique el servidor SFTP donde se cargan los registros. `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. Estos registros se almacenan en la ruta del servidor SFTP: `<dirección IP>\<marca de fecha y hora>\active_nnn.tgz`, donde nnn es una marca de hora en formato largo.

Establecer registros de seguimiento y recopilación para CUBE y CUSP

CUBE (SIP)

1. Establezca la marca de tiempo de los registros y habilite el búfer de registro.

```

#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
```



Advertencia: Cualquier cambio en un GW de software del IOS® de Cisco de producción puede causar una interrupción.

2. Esta es una plataforma muy robusta que puede manejar las depuraciones sugeridas en el volumen de llamadas proporcionado sin problemas. Sin embargo, Cisco recomienda que:
- Envíe todos los registros a un servidor syslog en lugar de al buffer de registro.

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

- Aplique los comandos debug de uno en uno y verifique el uso de la CPU después de cada uno.

```
show proc cpu hist
```



Advertencia: Si la CPU alcanza una utilización de la CPU de hasta el 70-80%, el riesgo de un impacto en el servicio relacionado con el rendimiento aumenta considerablemente. Por lo tanto, no habilite depuraciones adicionales si el GW alcanza el 60%.

3. Habilite estas depuraciones:

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

4. Reproducción del problema
5. Desactive los seguimientos.

```
#undebug all
```

6. Recopile los registros.

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

CÚSPIDE

1. Active los seguimientos SIP en CUSP.

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

2. Reproducción del problema
3. Desactive el registro cuando haya terminado.

Recopilar los registros

1. Configure un usuario en el CUSP (por ejemplo, prueba).
2. Agregue esta configuración en el prompt CUSP.

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

3. FTP a la dirección IP CUSP. Utilice el nombre de usuario (prueba) y la contraseña tal como se definieron en el paso anterior.
4. Cambie los directorios a /cusp/log/trace.
5. Obtenga el log_<filename>.

Establecer el seguimiento y recopilar registros de UCCE

Cisco recomienda establecer niveles de seguimiento y recopilar seguimientos mediante Diagnostic Framework Portico o las herramientas de System CLI.

 Nota: Para obtener más información sobre Diagnostic Framework Portico y System CLI, visite el capítulo [Herramientas de diagnóstico](#) de la Guía de mantenimiento para Cisco Unified ICM/Contact Center Enterprise, versión 12.5(1).

Cuando resuelva problemas en la mayoría de los escenarios de UCCE, si el nivel predeterminado de seguimientos no proporciona suficiente información, establezca el nivel de seguimientos en 3 en los componentes necesarios (con algunas excepciones).

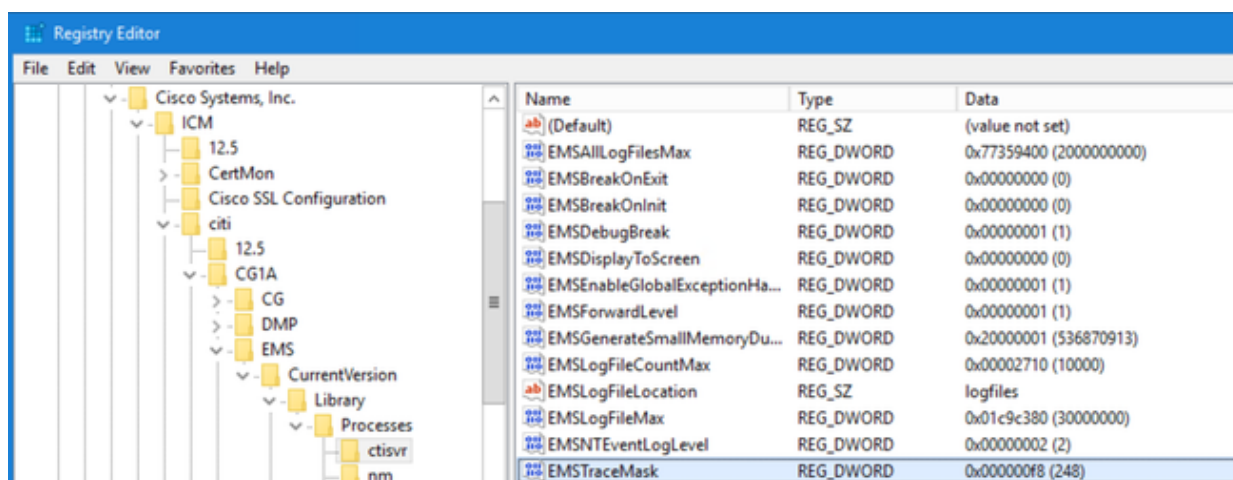
 Nota: Visite la sección [Nivel de seguimiento](#) de la Guía de mantenimiento para Cisco Unified ICM/Contact Center Enterprise, versión 12.5(1) para obtener más información.

Por ejemplo, si resuelve problemas del Marcador de salida, el nivel de seguimientos debe

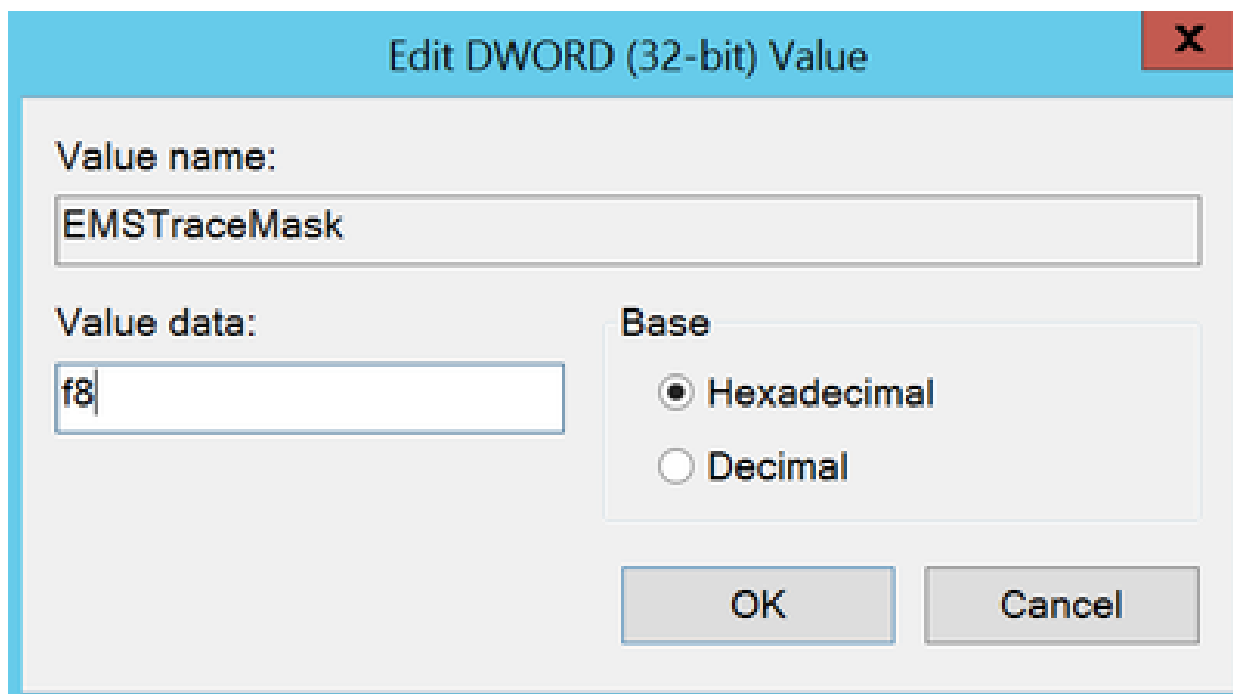
establecerse en el nivel 2 si el Marcador está ocupado.

Para CTISVR (CTISVR), los niveles 2 y 3 no establecen el nivel de registro exacto recomendado por Cisco. El registro de seguimiento recomendado para CTISVR es 0XF8.

1. En el PG Agente de UCCE, abra el Editor del Registro (Regedit).
2. Vaya a HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a y b)\EMS\CurrentVersion\library\Processes\ctisvr.



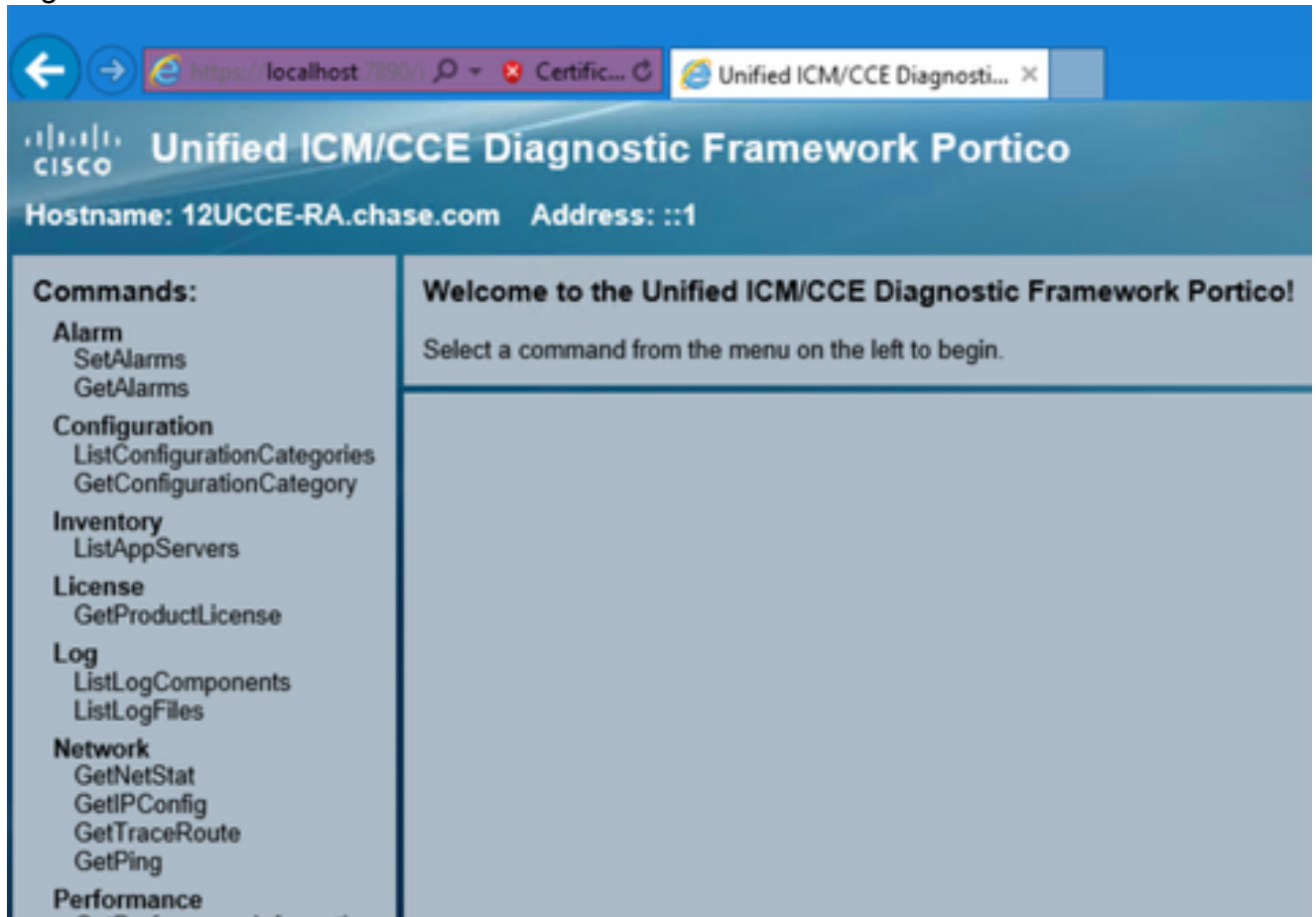
3. Haga doble clic en EMSTraceMask y establezca el valor en f8.



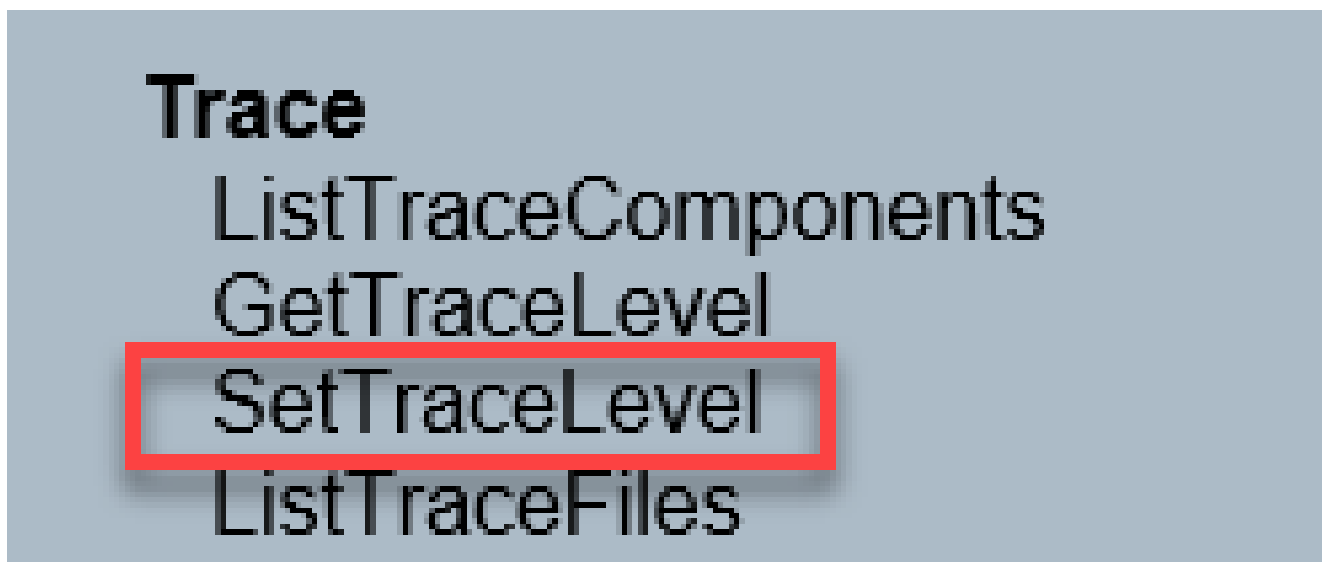
4. Haga clic en Aceptar y cierre el Editor del Registro. Estos son los pasos para establecer cualquiera de los seguimientos de componentes de UCCE (el proceso RTR se utiliza como ejemplo).

Establecer nivel de seguimiento

1. Abra Diagnostic Framework Portico desde el servidor que necesita para establecer los seguimientos e inicie sesión como el usuario Administrator.



2. En la sección Comandos, desplácese hasta Seguimiento y seleccione SetTraceLevel.



3. En la ventana SetTraceLevel, seleccione el componente y el nivel.

4. Haga clic en Submit (Enviar). Cuando haya terminado, verá el mensaje Aceptar.

Advertencia: Establezca el nivel de seguimientos en el nivel 3 mientras intenta reproducir el problema. Una vez reproducido el problema, establezca el nivel de seguimiento en el valor predeterminado. Tenga especial cuidado cuando establezca los seguimientos de JTAPIGW, ya que los niveles 2 y 3 establecen los seguimientos de nivel bajo y esto puede causar un impacto en el rendimiento. Establezca el nivel 2 o el nivel 3 en JTAPIGW durante el tiempo de no producción o en un entorno de laboratorio.

Recopilación de registros

1. Desde Diagnostic Framework Portico, en la sección Commands, navegue hasta Trace y seleccione ListTraceFile.

Trace

ListTraceComponents

GetTraceLevel

SetTraceLevel

ListTraceFiles

2. En la ventana ListTraceFile, seleccione Component, FromDate y ToDate. Active la casilla Mostrar URL y, a continuación, haga clic en Enviar.

The screenshot shows the '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'. On the left, there is a 'Commands:' menu with categories: Alarm, Configuration, Inventory, License, and Log. The main area is titled 'ListTraceFiles'. It contains a form with the following fields: 'Component' (a dropdown menu with 'Router A/rtr' selected), 'FromDate' (MM/DD/YYYY 1/8/2018), 'ToDate' (MM/DD/YYYY 1/8/2018), 'UseTzadjustoff' (a dropdown menu with 'NO' selected), and 'Show URL' (a checkbox that is checked). There is a 'Submit' button at the bottom of the form. On the right side of the form, there are time zone settings: 'Central Standard Time (UTC -6:00)' and 'Central Standard Time (UTC -6:00)'.

3. Cuando finalice la solicitud, verá el mensaje OK (Aceptar) con el enlace del archivo de registro ZIP.

The screenshot shows the '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'. On the left, there is a 'Commands:' menu with categories: Alarm, Configuration, Inventory, License, and Log. The main area is titled 'ListTraceFiles'. It contains a form with the following fields: 'Component' (a dropdown menu with 'Router A/rtr' selected), 'FromDate' (MM/DD/YYYY 8/17/2022), 'ToDate' (MM/DD/YYYY 8/17/2022), 'UseTzadjustoff' (a dropdown menu with 'NO' selected), and 'Show URL' (a checkbox that is checked). There is a 'Submit' button at the bottom of the form. Below the form, there is a section titled 'ListTraceFilesReply (OK)'. It contains a link to the ZIP file: 'RouterA/citil_rtr_20220817124205018_4176769.zip'. Below the link, it says 'Date: Wed Aug 17 2022 00:00:00 GMT-0500 (Central Daylight Time)'.

4. Haga clic en el enlace del archivo ZIP y guarde el archivo en la ubicación que elija.

Establecer registros de seguimiento y recopilación de PCCE

PCCE tiene su propia herramienta para configurar los niveles de seguimiento. No es aplicable al entorno UCCE, donde Diagnostic Framework Portico o la CLI del sistema son las formas preferidas de habilitar y recopilar registros.

1. Desde el servidor PCCE AW, abra la herramienta Unified CCE Web Administration e inicie sesión en la cuenta Administrator.

Unified CCE Administration

Enter your password

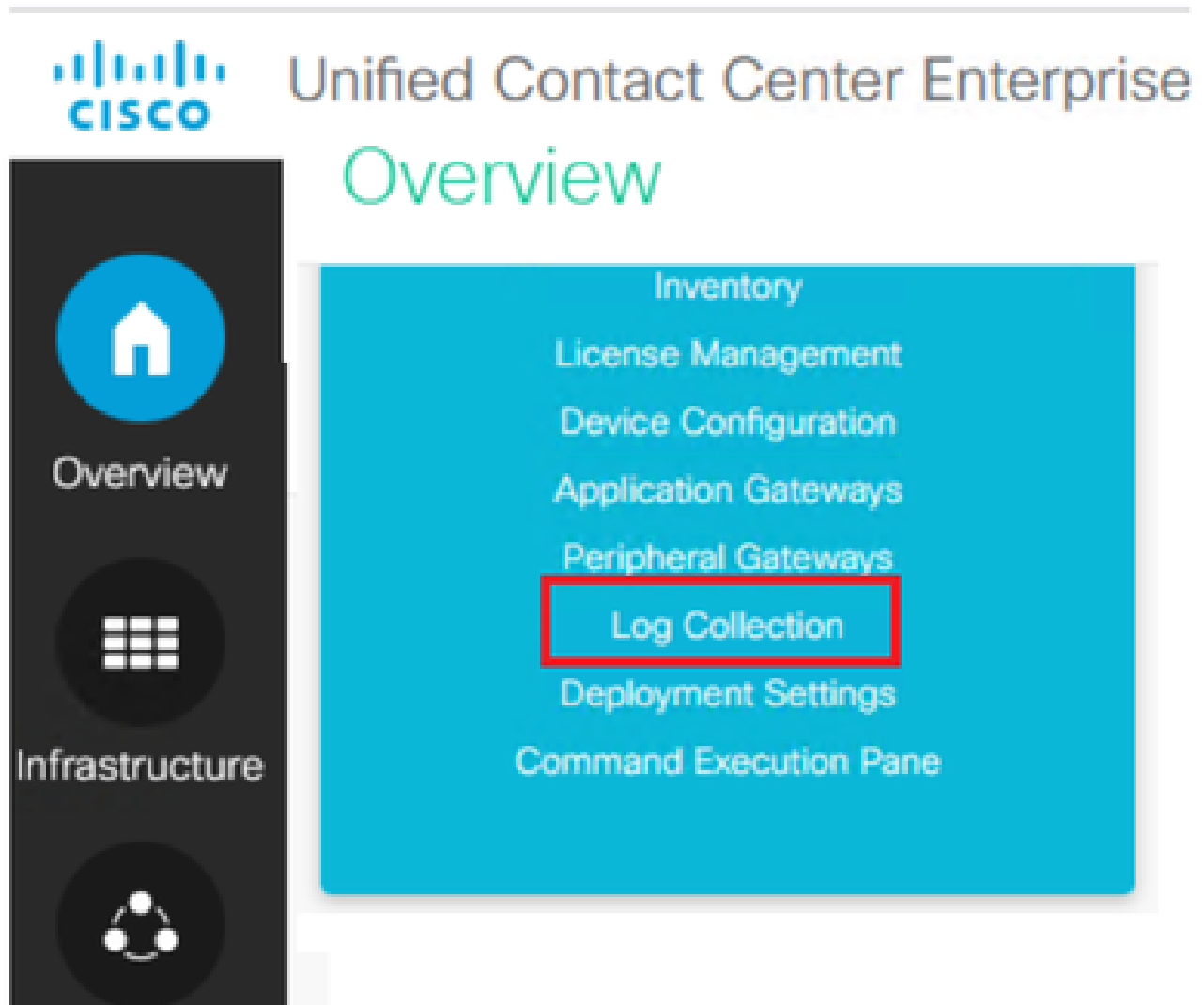
administrator@pccc.com

••••••••••

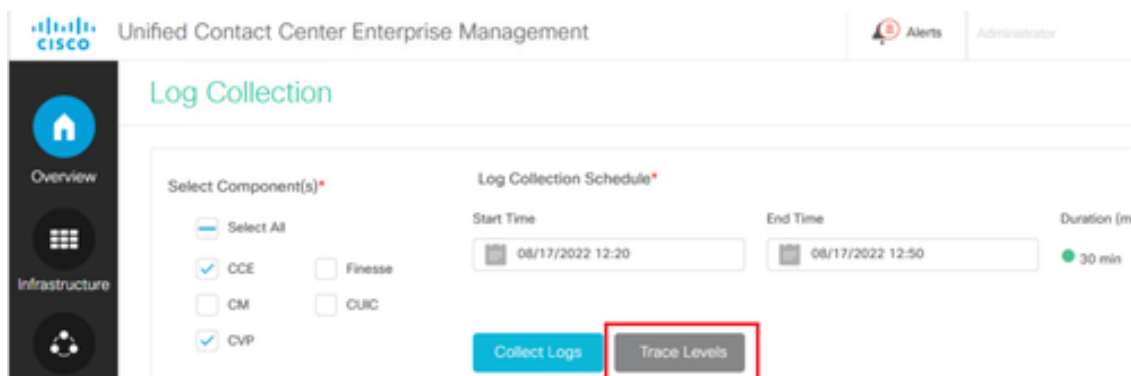
Sign In

[Sign in as a different user](#)

2. Navegue hasta Descripción general > Configuración de infraestructura > Recopilación de registro para abrir la página Recopilación de registro.



3. En la página Recopilación de registros, haga clic en Niveles de seguimiento, que abre el cuadro de diálogo Niveles de seguimiento.



4. Establezca el Nivel de seguimiento en Detallado en CCE y déjelo como Sin cambios para CM y CVP, luego haga clic en Actualizar niveles de seguimiento.

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. Haga clic en Yes para aceptar la Advertencia.



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

Yes

No

- Una vez reproducido el problema, abra Unified CCE Administration y vuelva a System >Log Collection.
- Seleccione CCE y CVP en el panel Componentes.
- Seleccione el tiempo de recopilación de registros correspondiente (el valor predeterminado es los últimos 30 minutos).
- Haga clic en Recopilar registros y Sí para ver la advertencia del cuadro de diálogo. Se inicia la recopilación de registros. Espere unos minutos antes de que termine.

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		

- Una vez finalizado, haga clic en el botón Download en la columna Actions para descargar un archivo comprimido con todos los registros en él. Guarde el archivo zip en la ubicación que considere adecuada.

Establecer el seguimiento y recopilar registros de CUIC/Live Data/IDS

Descargar registros con SSH

- Inicie sesión en la línea de comandos SSH (CLI) de CUIC, LD e IDS.
- Ejecute el comando para recopilar los registros relacionados con 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
```

3. Ejecute el comando para recopilar los registros relacionados con LD.

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

4. Ejecute el comando para recopilar los registros relacionados con IdS.

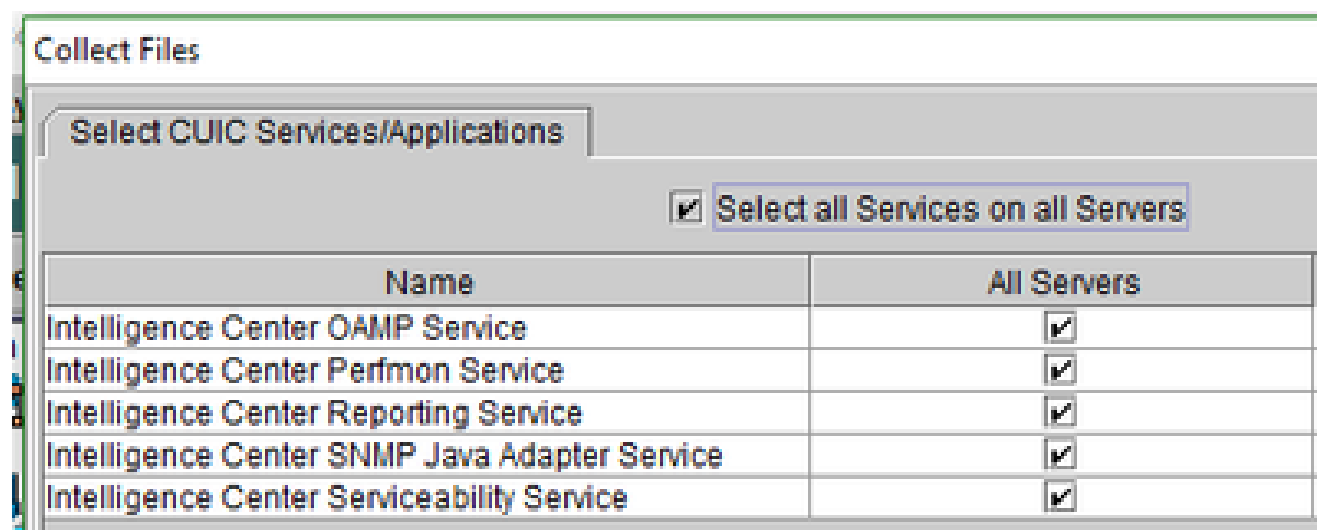
```
file get activelog ids/log/*.* recurs compress reltime days 1
```

5. Estos registros se almacenan en la ruta del servidor SFTP: <IP address>\<date time stamp>\active_nnn.tgz , donde nnn es timestamp en formato largo.

Descargar registros con RTMT

1. Descargue RTMT de la página OAMP. Inicie sesión en <https://<HOST ADDRESS>/oamp>, donde HOST ADDRESS es la dirección IP del servidor.
2. Navegue hasta Herramientas > Descarga del complemento RTMT. Descargue e instale el complemento.
3. Inicie RTMT e inicie sesión en el servidor con las credenciales de administrador.
4. Haga doble clic en Trace and Log Central y luego haga doble clic en Collect Files.
5. Puede ver estas fichas para los servicios específicos. Debe seleccionar todos los servicios/servidores para CUIC, LD e IDS.

Para CUIC:



Name	All Servers
Intelligence Center OAMP Service	☒
Intelligence Center Perfmon Service	☒
Intelligence Center Reporting Service	☒
Intelligence Center SNMP Java Adapter Service	☒
Intelligence Center Serviceability Service	☒

Para LD:

Collect Files

Select LiveData Services/Applications

☒ Select all Services on all Servers

Name	All Servers
CCE Live Data ActiveMQ Service	☒
CCE Live Data Cassandra Service	☒
CCE Live Data NGINX Service	☒
CCE Live Data SocketIO Service	☒
CCE Live Data Storm Services	☒
CCE Live Data Web Service	☒
CCE Live Data Zookeeper Service	☒

Para IDS:

Collect Files

Select IdS Services/Applications

☒ Select all Services on all Servers

Name	All Servers
Cisco Identity Service	☒

Para los servicios de plataforma, generalmente es una buena idea seleccionar los registros de **Tomcat** y **Event viewer**:

Collect Files

Select System Services/Applications

☐ Select all Services on all Servers

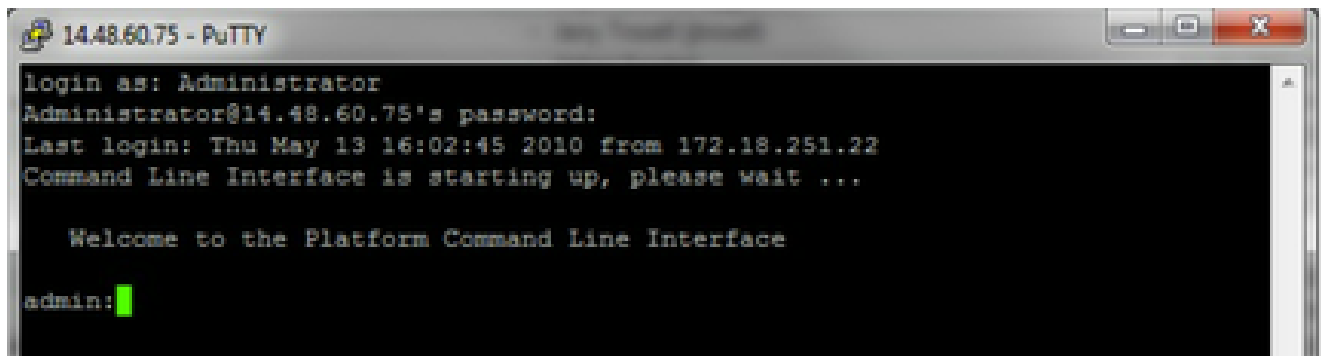
Name	All Servers
Cisco Serviceability Reporter CallActivitiesReport	☐
Cisco Serviceability Reporter DeviceReport	☐
Cisco Serviceability Reporter PPRReport	☐
Cisco Serviceability Reporter ServerReport	☐
Cisco Serviceability Reporter ServiceReport	☐
Cisco Stored Procedure Trace	☐
Cisco Syslog Agent	☐
Cisco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

6. Seleccione la Fecha y la Hora junto con la carpeta destination para Guardar los registros.

Captura de paquetes en VoS (Finesse, CUIC, VB)

1. Inicie la captura

Para iniciar la captura, establezca una sesión SSH en el servidor VOS autenticado con la cuenta de administrador de plataforma.



```
1448.60.75 - 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.

1 bis. Sintaxis del comando

El comando es `utils network capture` y la sintaxis es la siguiente:

<#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:

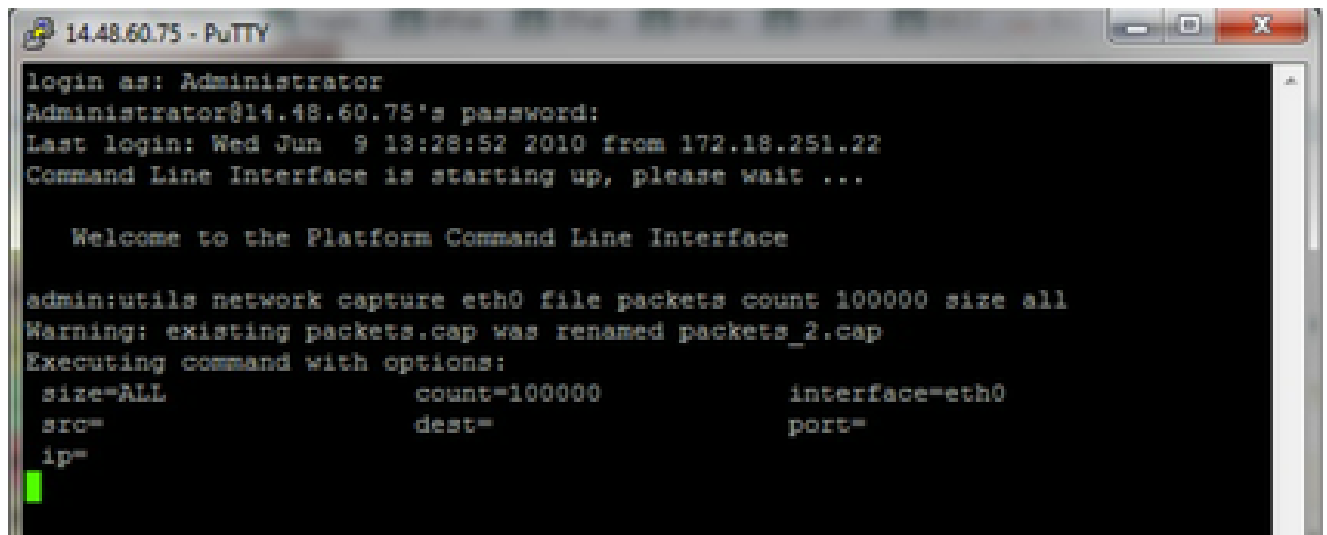
ip/arp/rarp/all. The host address of the packet as a host name or IPV4

address. This option will display all packets to and from that address.

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

1 ter. Capturar todos los tráficos

Para una captura típica, uno puede recopilar TODOS los paquetes de TODOS los tamaños desde y hacia TODAS las direcciones en un archivo de captura llamado packets.cap. Para ello, simplemente ejecute en la CLI de administración `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 ...

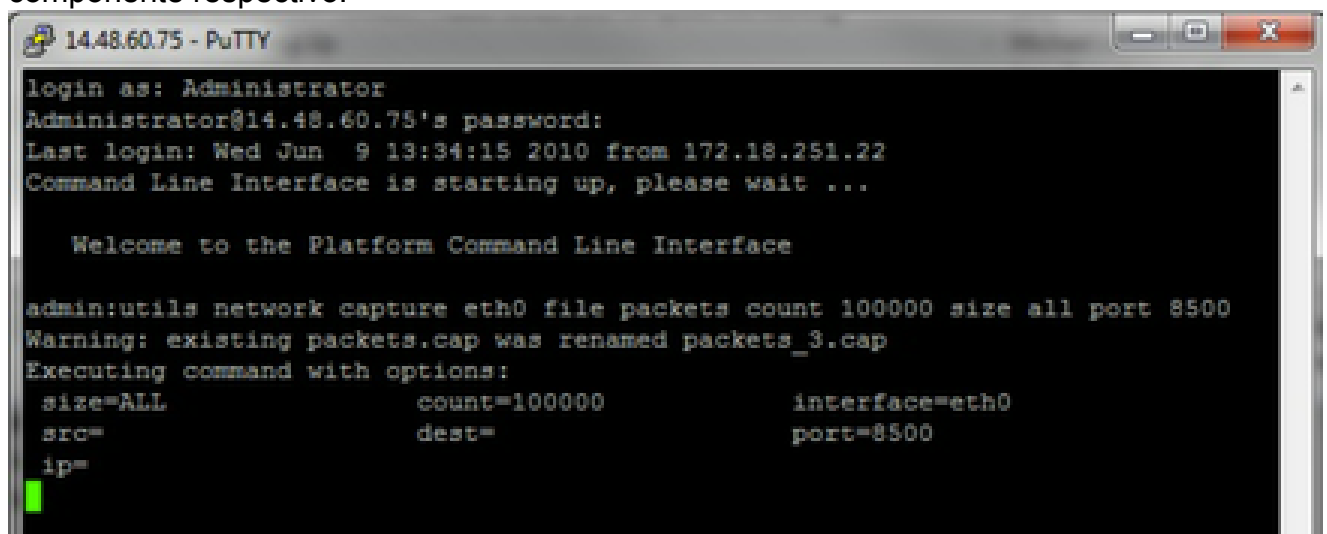
Welcome to the Platform Command Line Interface

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=
```

1 quáter. Captura basada en el número de puerto

Para resolver un problema de comunicación con el Administrador de clústeres, puede ser conveniente utilizar la opción de puerto para capturar en función de un puerto específico (8500).

Para obtener más información sobre qué servicios requieren comunicaciones en cada puerto, consulte [la Guía de Uso de Puertos TCP y UDP](#) para obtener la versión aplicable del componente respectivo.



```
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 ...

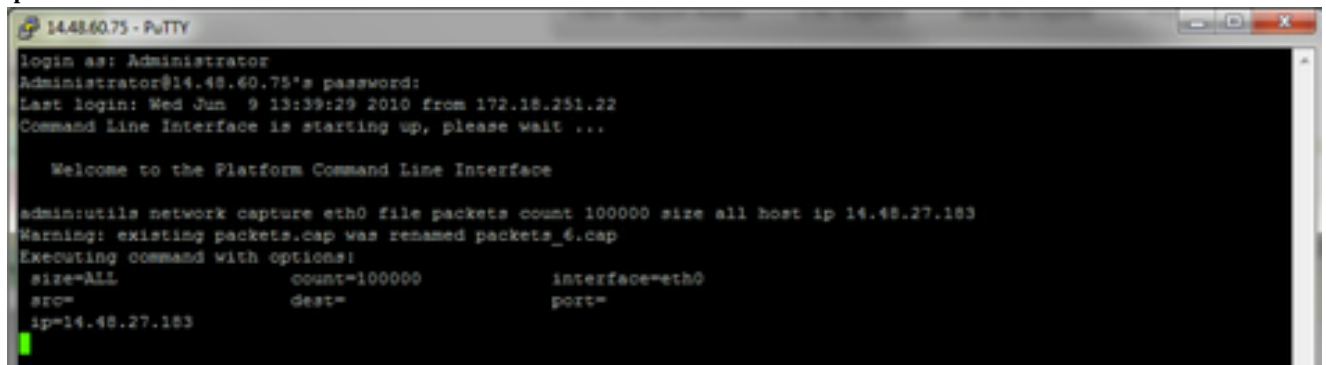
Welcome to the Platform Command Line Interface

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. Captura basada en host

Para solucionar un problema con VOS y un host determinado, puede ser necesario utilizar la opción 'host' para filtrar el tráfico hacia y desde un host determinado.

También puede ser necesario excluir un host en particular, en este caso utilice un "!" delante de la dirección IP. Un ejemplo de esto sería `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
```

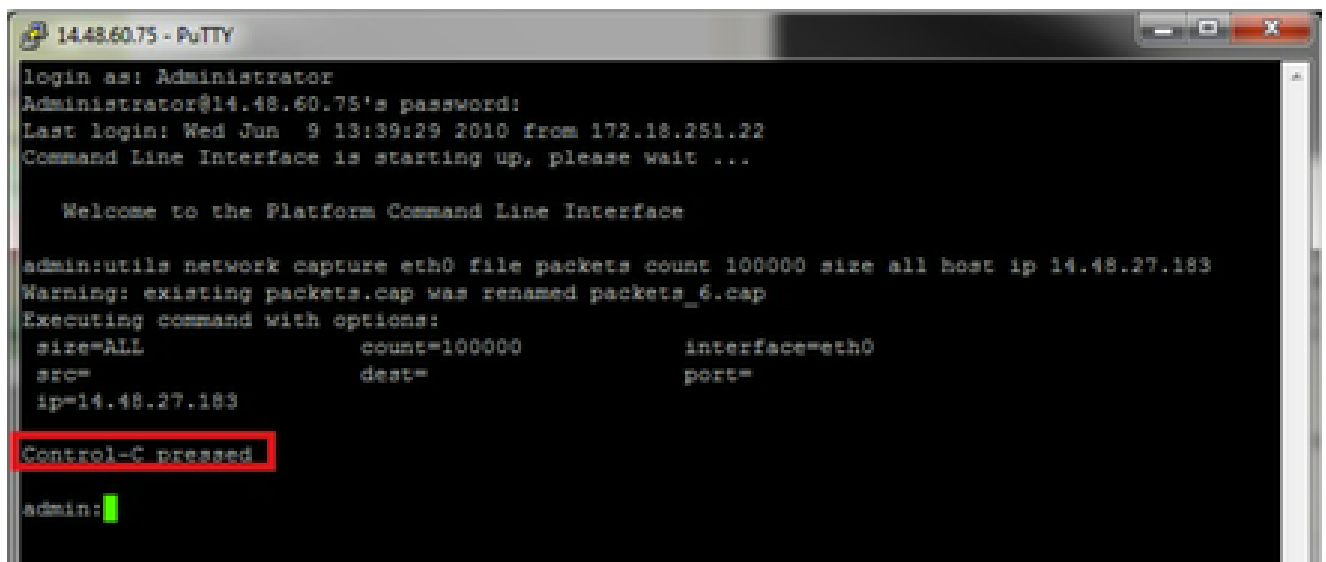
3. Reproduzca el síntoma del problema

Mientras la captura ha comenzado a reproducir el síntoma o condición del problema de modo que los paquetes necesarios se incluyan en la captura. Si el problema es intermitente, puede ser necesario ejecutar la captura durante un período prolongado. Si la captura finaliza, es porque el búfer está lleno. Reinicie la captura y la captura anterior cambiará de nombre automáticamente para que no se pierda la captura anterior. Si se necesita una captura durante un período de tiempo prolongado, utilice una sesión de supervisión en un switch para realizar la captura en el nivel de red.

4. Detenga la captura

Para detener la captura, mantenga presionada la tecla Control y presione C en el teclado. Esto hace que el proceso de captura finalice y no se agreguen paquetes nuevos al volcado de captura.

5.



```
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:
```

Una vez finalizado, se almacena un archivo de captura en el servidor en la ubicación 'activelog platform/cli/'

6. Recopile la captura del servidor

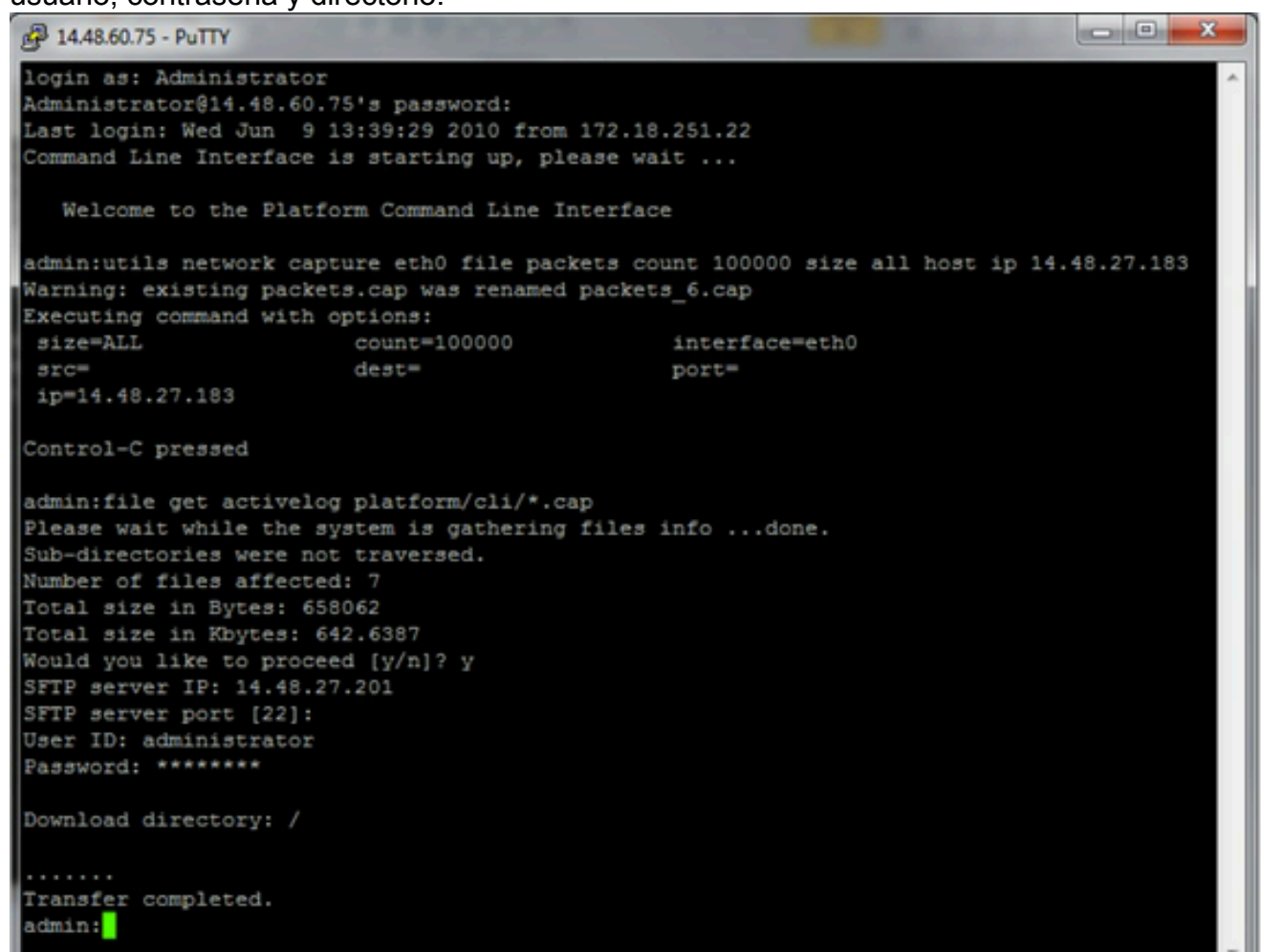
Los archivos de captura se almacenan en la plataforma/cli/ de registro activo en el servidor. Puede transferir los archivos a través de CLI a un servidor SFTP o al equipo local con el RTMT.

4 bis. Transferir el archivo de captura a través de la CLI a un servidor SFTP

Utilice el comando `file get activelog platform/cli/packets.cap` para recopilar el archivo `packets.cap` en el servidor SFTP.

Alternativamente, recopile todos los archivos `.cap` almacenados en el servidor, utilice `file get activelog platform/cli/*.cap`.

Por último, introduzca la información de IP/FQDN del servidor SFTP, puerto, nombre de usuario, contraseña y directorio:



```
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: *****

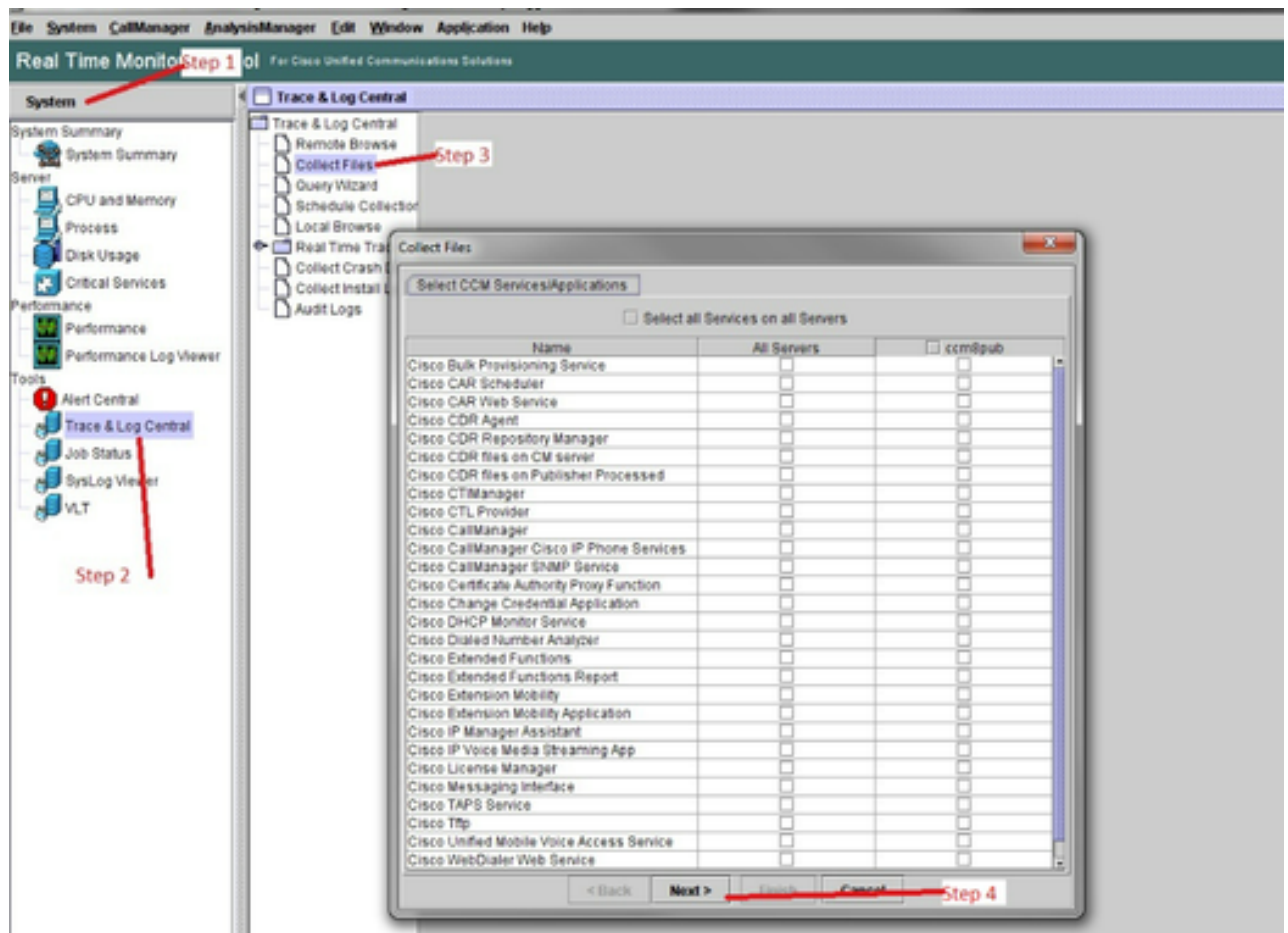
Download directory: /

.....
Transfer completed.
admin:
```

La CLI indica que la transferencia de archivos al servidor SFTP se ha realizado correctamente o no.

4 ter. Utilice RTMT para transferir un archivo de captura a un equipo local.

Inicie la RTMT. Si no está instalado en el equipo local, instale la versión adecuada desde la página de administración de VOS y luego navegue hasta el menú `Applications > Plugins`. Haga clic en `System`, luego en `Trace & Log Central`, luego haga doble clic en `Collect Files`. Haga clic en `Next` en el primer menú.



En el segundo menú, seleccione la casilla de verificación Registros de captura de paquetes en el servidor en el que se realizó la captura y, a continuación, haga clic en Siguiente.

Collect Files

Select System Services/Applications

☐ Select all Services on all Servers

Name	All Servers	☐ ccm8pub
Cisco WebDialerRedirector Web Service	☐	☐
Cron Logs	☐	☐
Event Viewer-Application Log	☐	☐
Event Viewer-System Log	☐	☐
Host Resources Agent	☐	☐
IPT Platform CLI Created Reports	☐	☐
IPT Platform CLI Logs	☐	☐
IPT Platform Cert Monitor Logs	☐	☐
IPT Platform CertMgr Logs	☐	☐
IPT Platform Cluster Manager Logs	☐	☐
IPT Platform GUI Logs	☐	☐
IPT Platform IPsecMgmt Logs	☐	☐
IPT Platform RemoteSupport Logs	☐	☐
Install File Signing	☐	☐
Install and Upgrade Logs	☐	☐
MIB2 Agent	☐	☐
Mail Logs	☐	☐
Mgetty Logs	☐	☐
NTP Logs	☐	☐
Netdump Logs	☐	☐
Packet Capture Logs	☐	☐
Prog Logs	☐	☐
SAR Logs	☐	☐
SNMP Master Agent	☐	☐
Security Logs	☐	☐
Service Manager	☐	☐
Spooler Logs	☐	☐
System Application Agent	☐	☐

< Back Next > Finish Cancel

En la pantalla final, elija un rango de tiempo cuando se realizó la captura, y un directorio de descarga en el equipo local.

Collect Files

Collect File Options:

Collection Time

☐ Absolute Range

Select Reference Server Time Zone: Client (GMT-5:0) Eastern Daylight Time-America/New_York

From Date/Time: 6/9/10 - 1:56 PM

To Date/Time: 6/9/10 - 1:56 PM

☒ **Relative Range**

Files Generated in the last: 5 Hours

Download File Options

Select Partition: Active Partition

Download File Directory: D:\traces Browse

☐ Zip Files

☒ **Do Not Zip Files**

☐ Uncompress Log Files

☐ Delete Collected Log Files from Server

Note: The result file can be found in the directory named <Node Name> created under the user specified directory structure. The File Name is as specified by the user.

< Back Next > **Finish** Cancel

RTMT cierra esta ventana y procede a recopilar el archivo y almacenarlo en el equipo local en la ubicación especificada.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).