Establecer seguimientos y recopilar registros en CCE

Contenido

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.

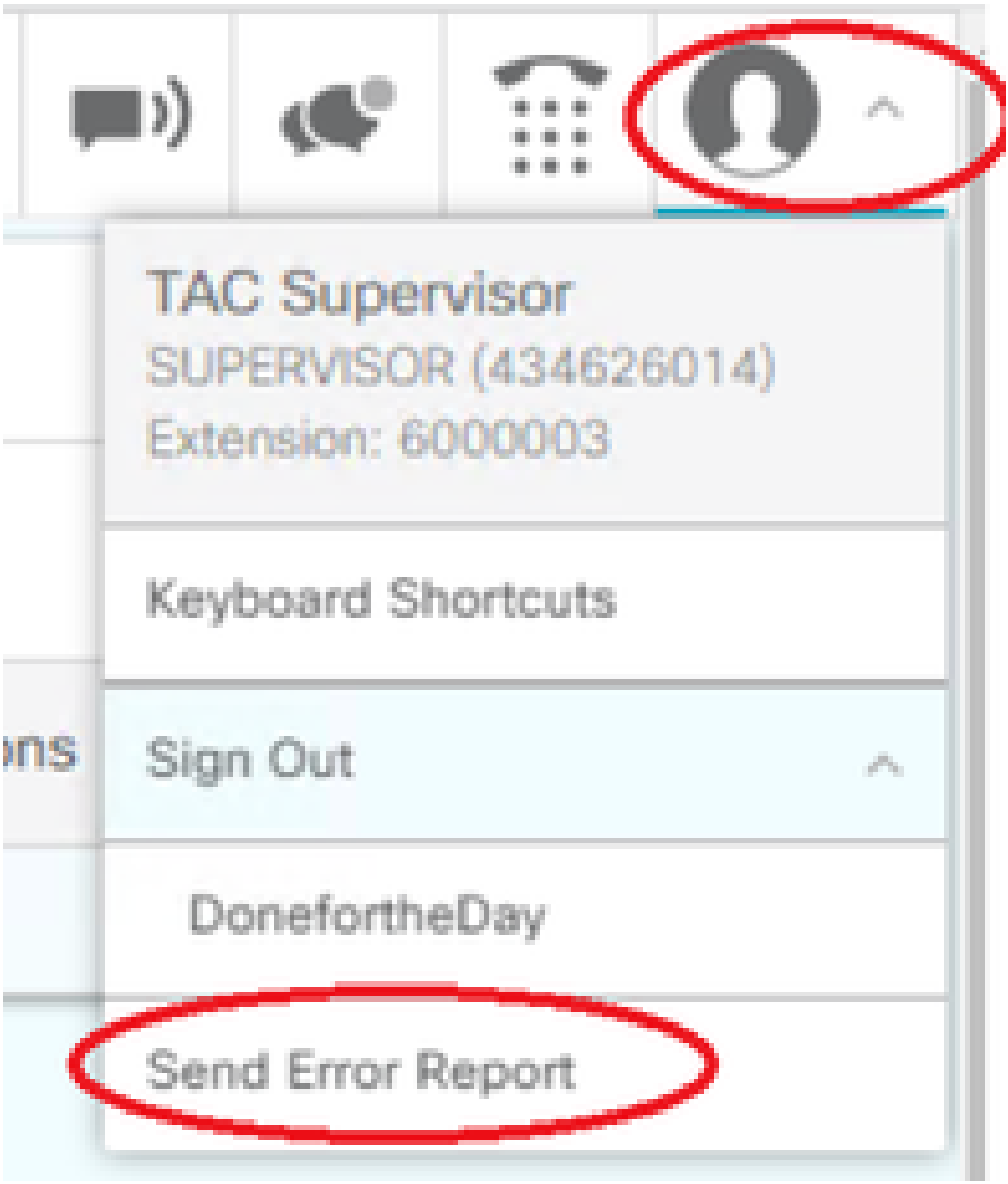
Establecer seguimientos y recopilar registros de Finesse

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

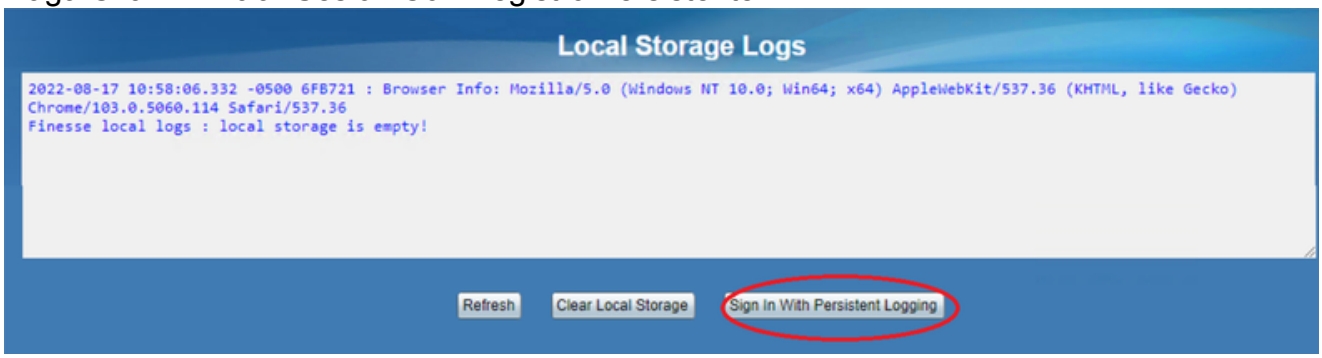
1. Inicie sesión con un agente.
2. Si un agente experimenta algún problema durante una llamada o evento multimedia, indique al agente que haga clic en el enlace Enviar informe de errores situado en la esquina superior derecha del escritorio de Finesse.



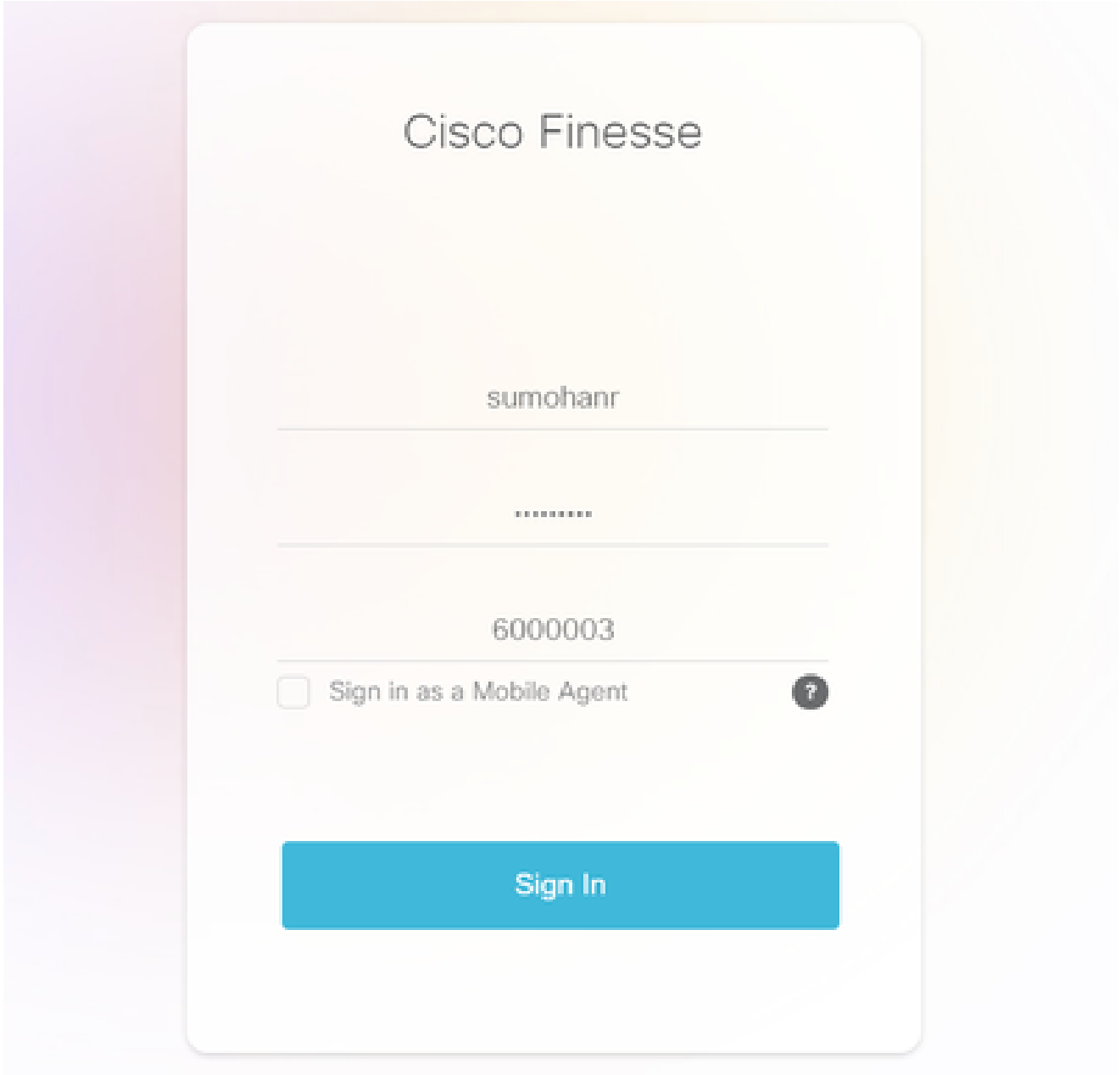
3. El agente ve los registros enviados correctamente. mensaje.
4. Los registros del cliente se envían al servidor Finesse. Navegue hasta Finesse Logs e inicie sesión con una cuenta de administración.
5. Recopile los registros bajo el directorio clientlogs/.

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.

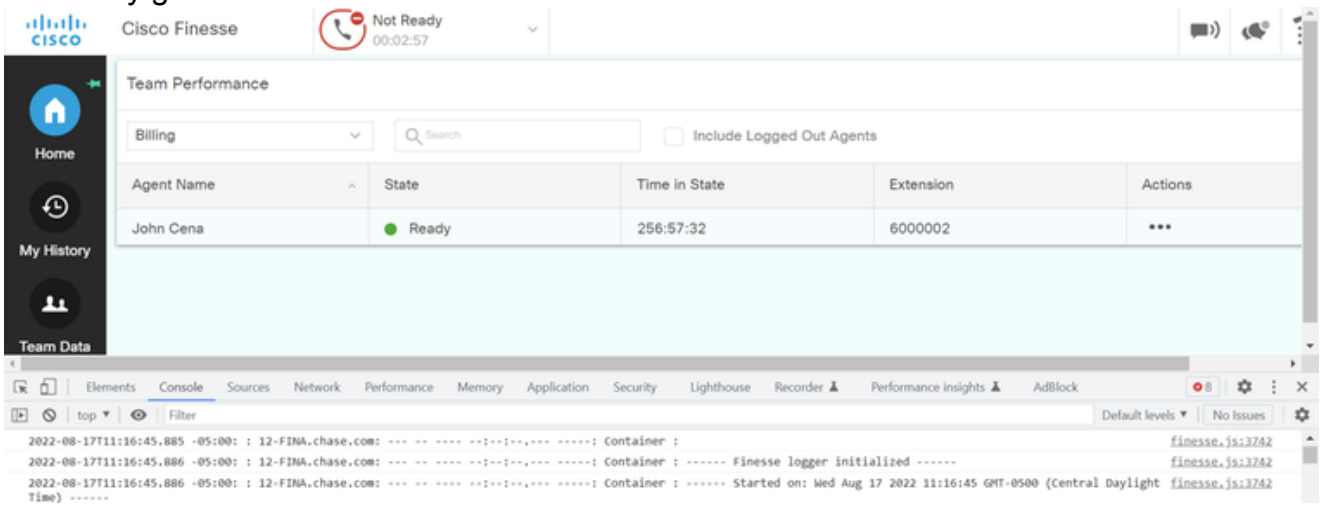


4. Toda la interacción del escritorio del agente se registra y se envía a los registros de almacenamiento local. Para recopilar los registros, navegue hasta Registro local de

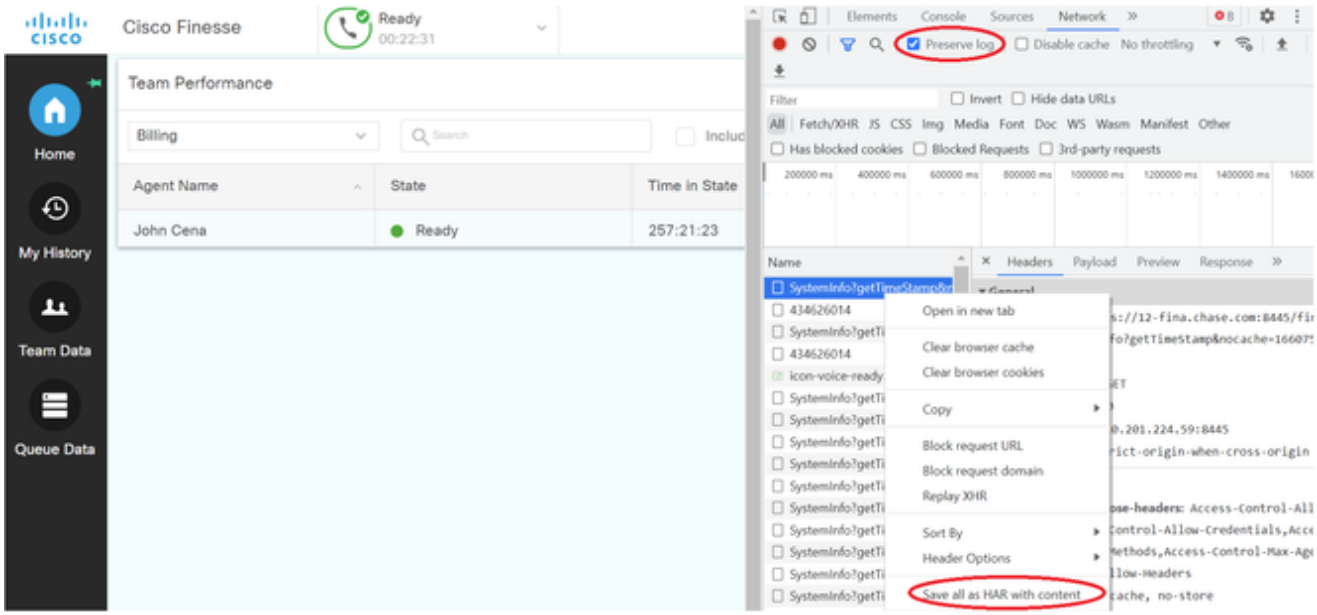
escritorio y copie el contenido en un archivo de texto. Guarde el archivo para analizarlo más a fondo.

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/.

3. 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.

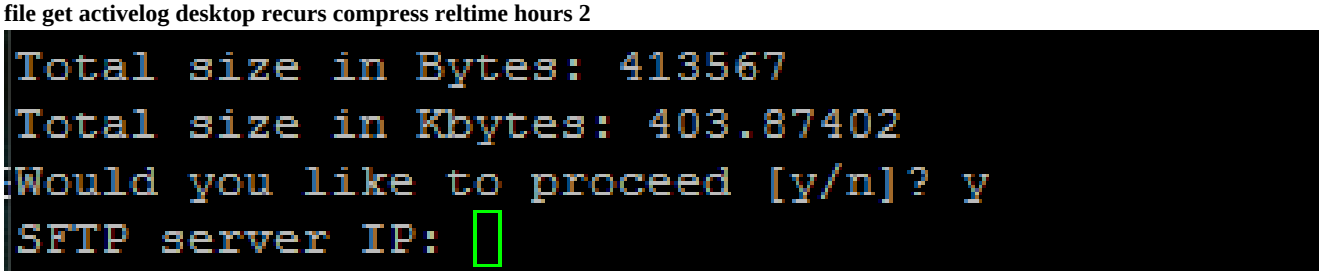
4. Recopile los otros registros requeridos (depende del escenario). Por ejemplo, openfire para problemas de servicio de notificación, registros de rango para problemas de autenticación y tomcatlogs para problemas de API.

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

1. Inicie sesión en el servidor Finesse con el SSH.
2. 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



3. 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.
4. 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

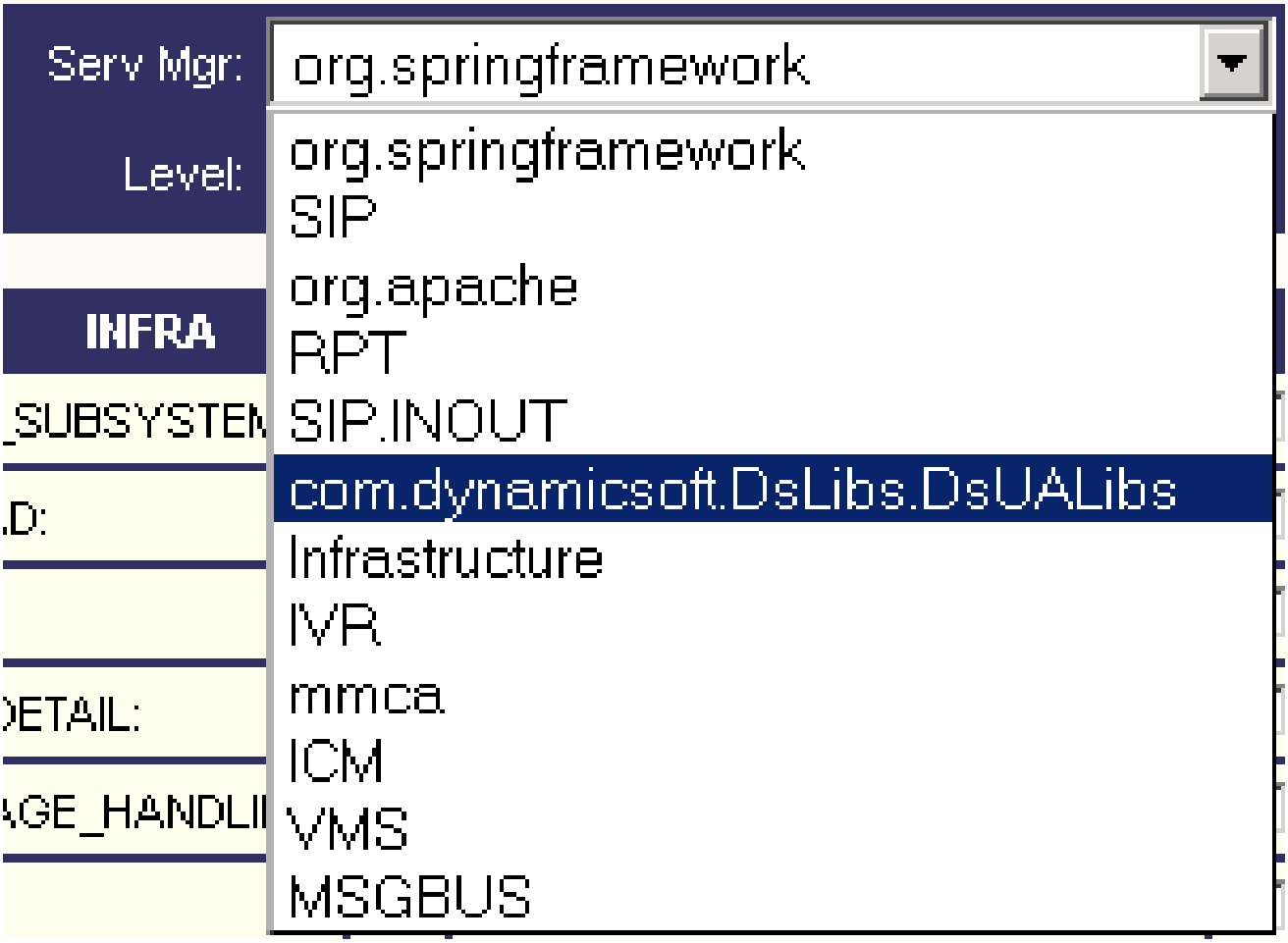
1. El nivel predeterminado de seguimientos de CVP CallServer es suficiente para resolver la

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.

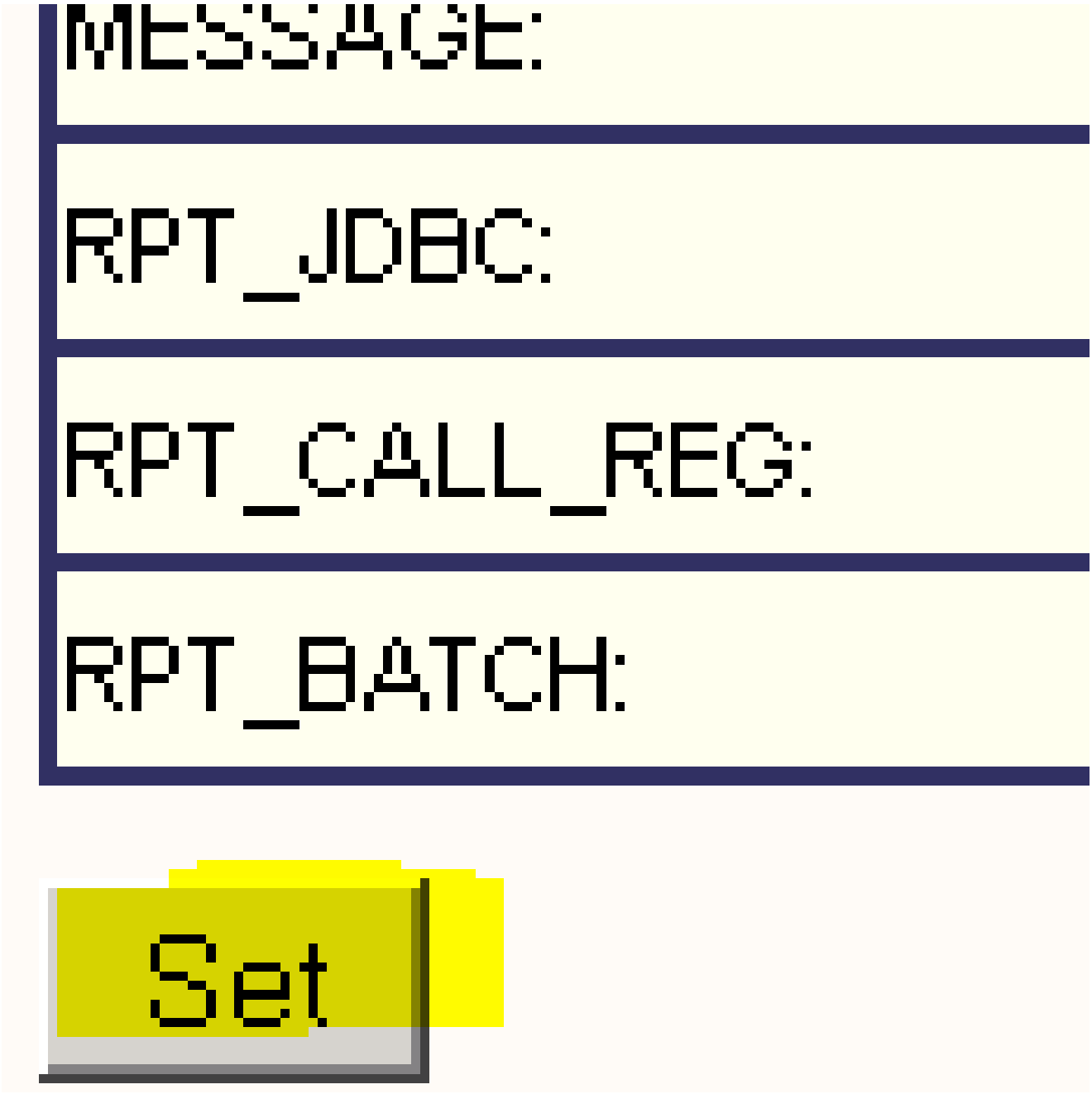
2. Vaya a la página web de CVP CallServer Diag URL Local Host 8000.

> 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.



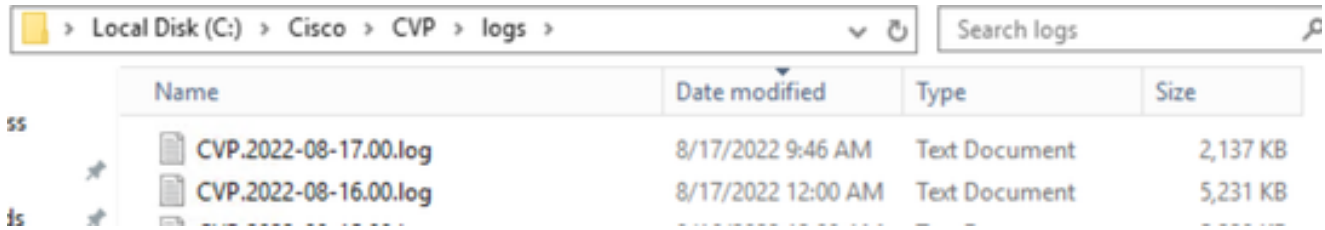
4. Haga clic en el botón Set.



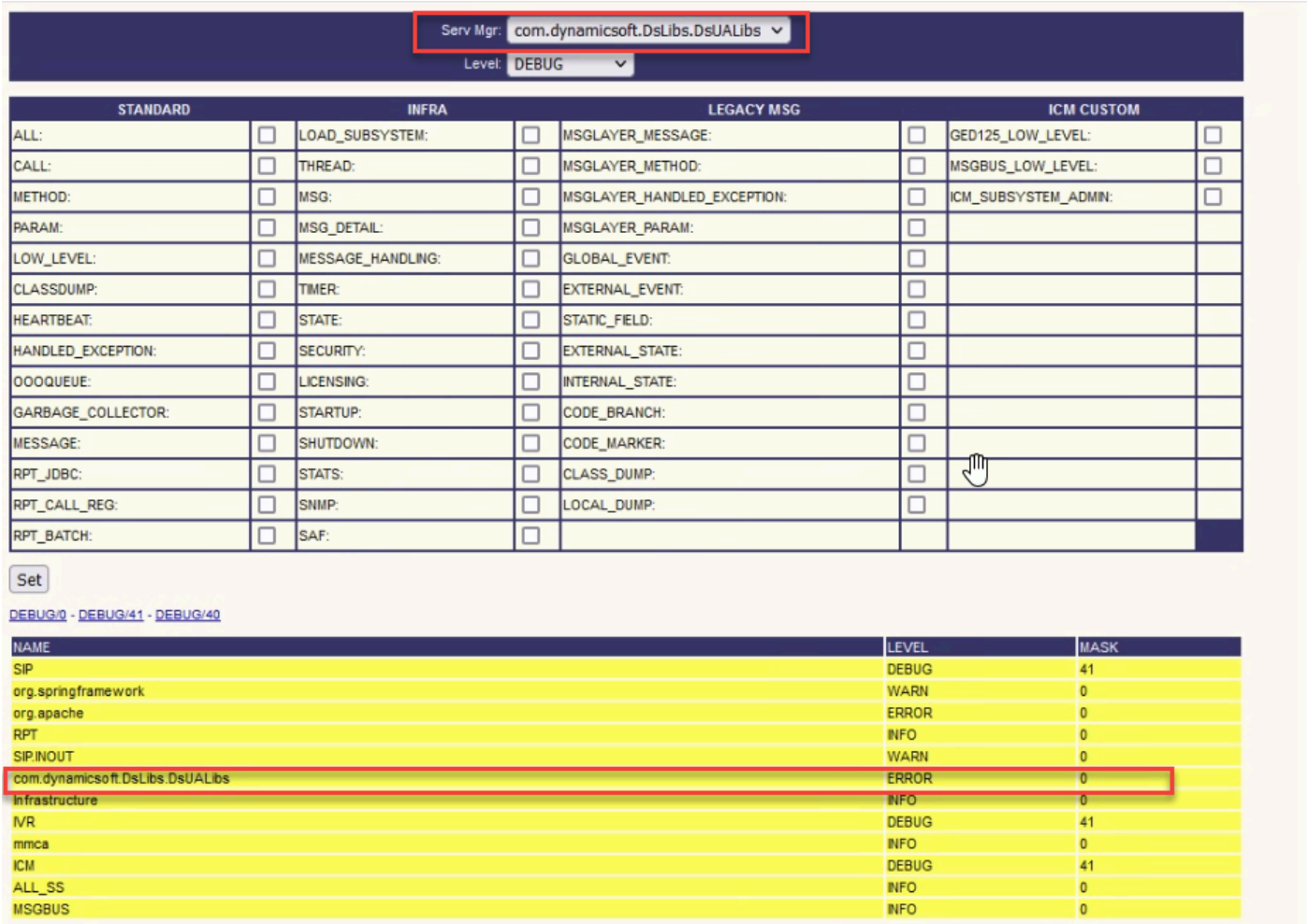
5. Desplácese hacia abajo en la ventana de seguimiento para asegurarse de que el nivel de seguimientos se ha establecido correctamente. Estos son los ajustes de depuración.

NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
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. 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.



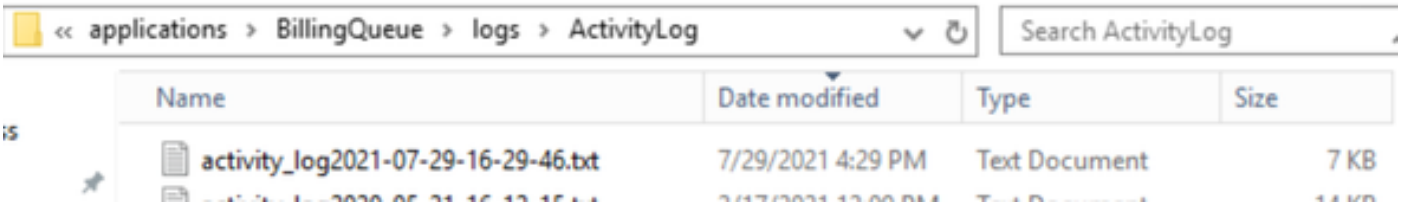
7. Después de reproducir el problema, asegúrese de restaurar los seguimientos al nivel predeterminado. Seleccione com.dynamicSoft.DsLibs.DsUALibs en el Serv. Menú desplegable Mgr en la esquina superior izquierda y establézcalo en error.



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.

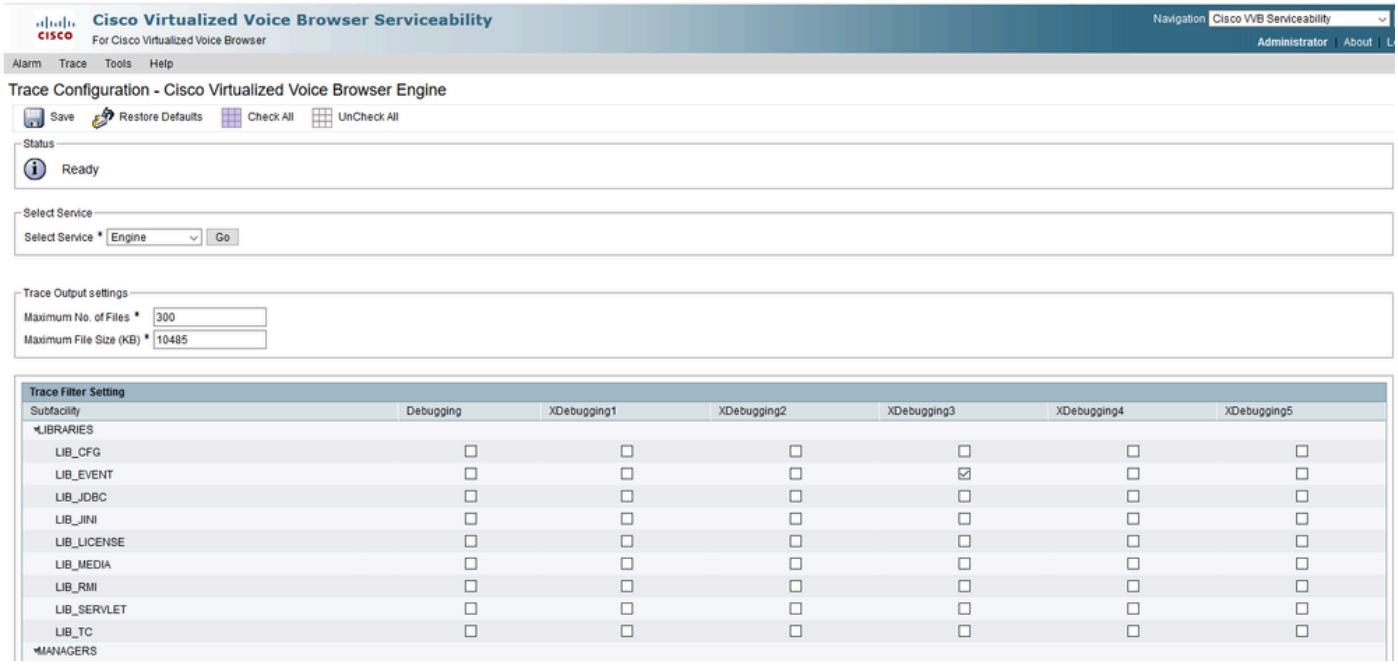
Cisco VB tiene dos componentes principales:

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



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

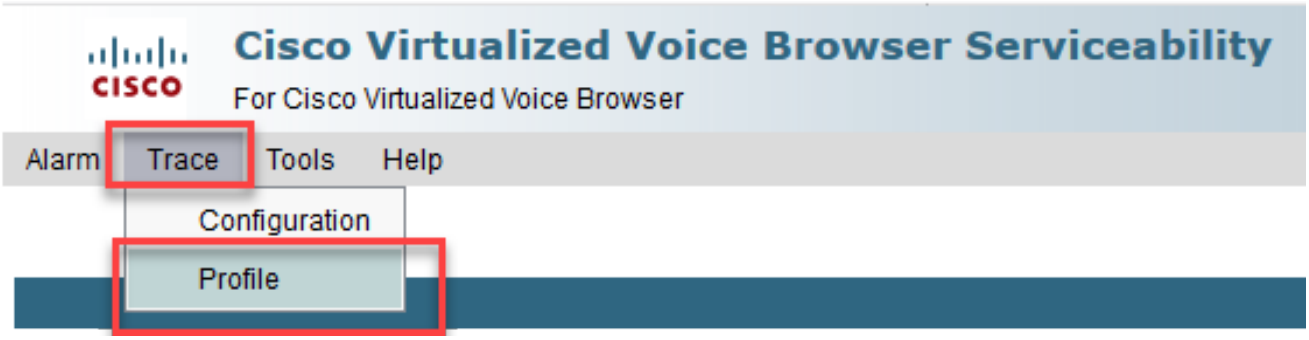
Nombre	Escenario en el que se debe activar este perfil
VB predeterminado	Los registros genéricos están habilitados.
AppAdminVB	Para problemas con la administración web a través de AppAdmin, Cisco VB Serviceability y otras páginas web.

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.

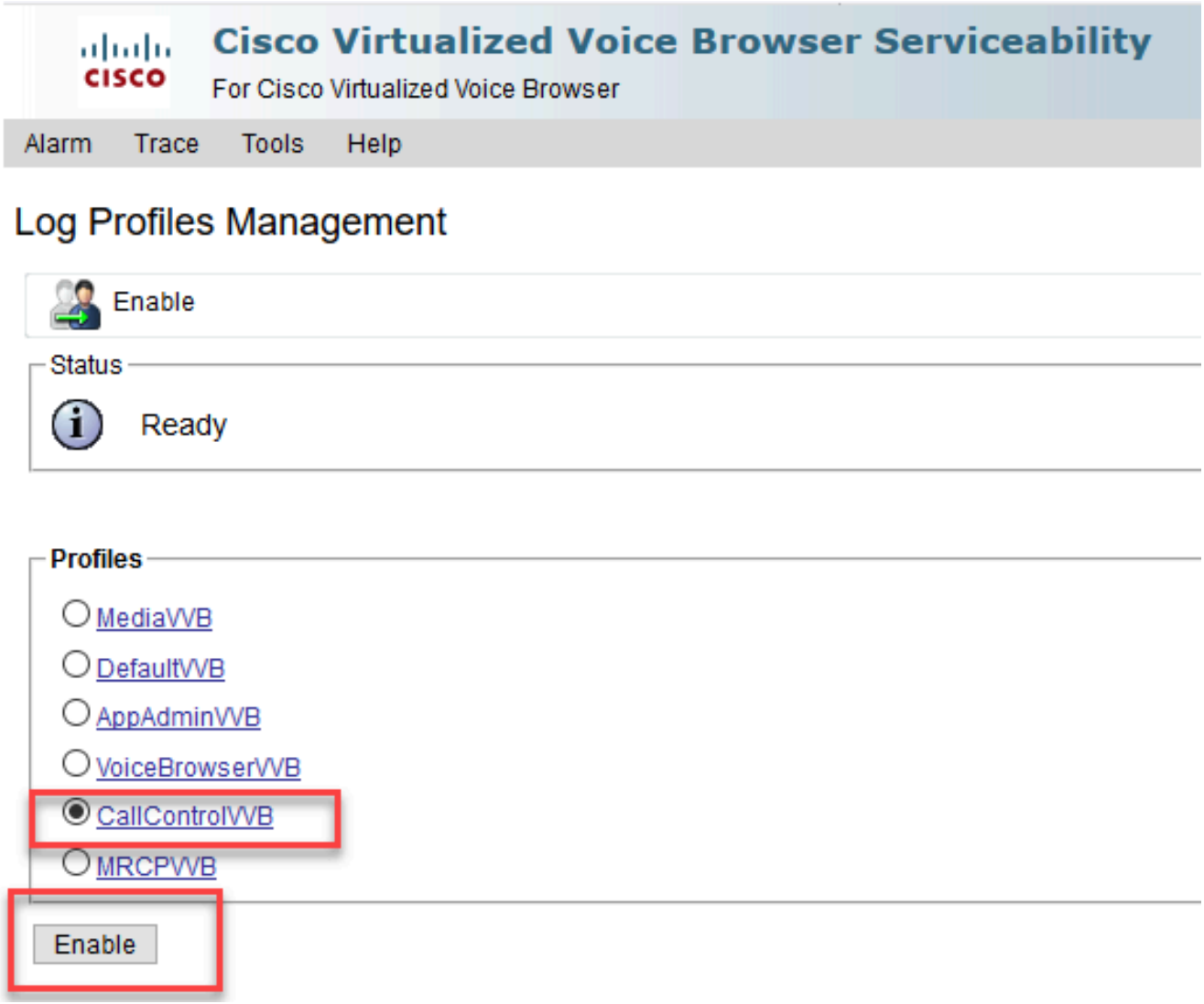
Opción 1: A través de la cuenta de administración

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.

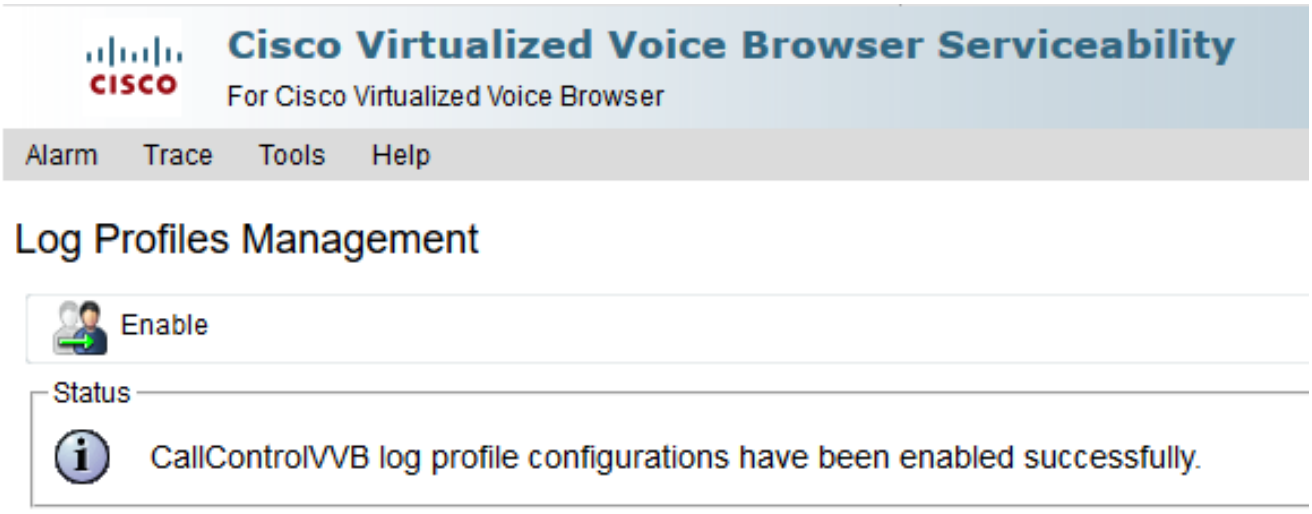
2. Seleccione Trace > Profile.



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).



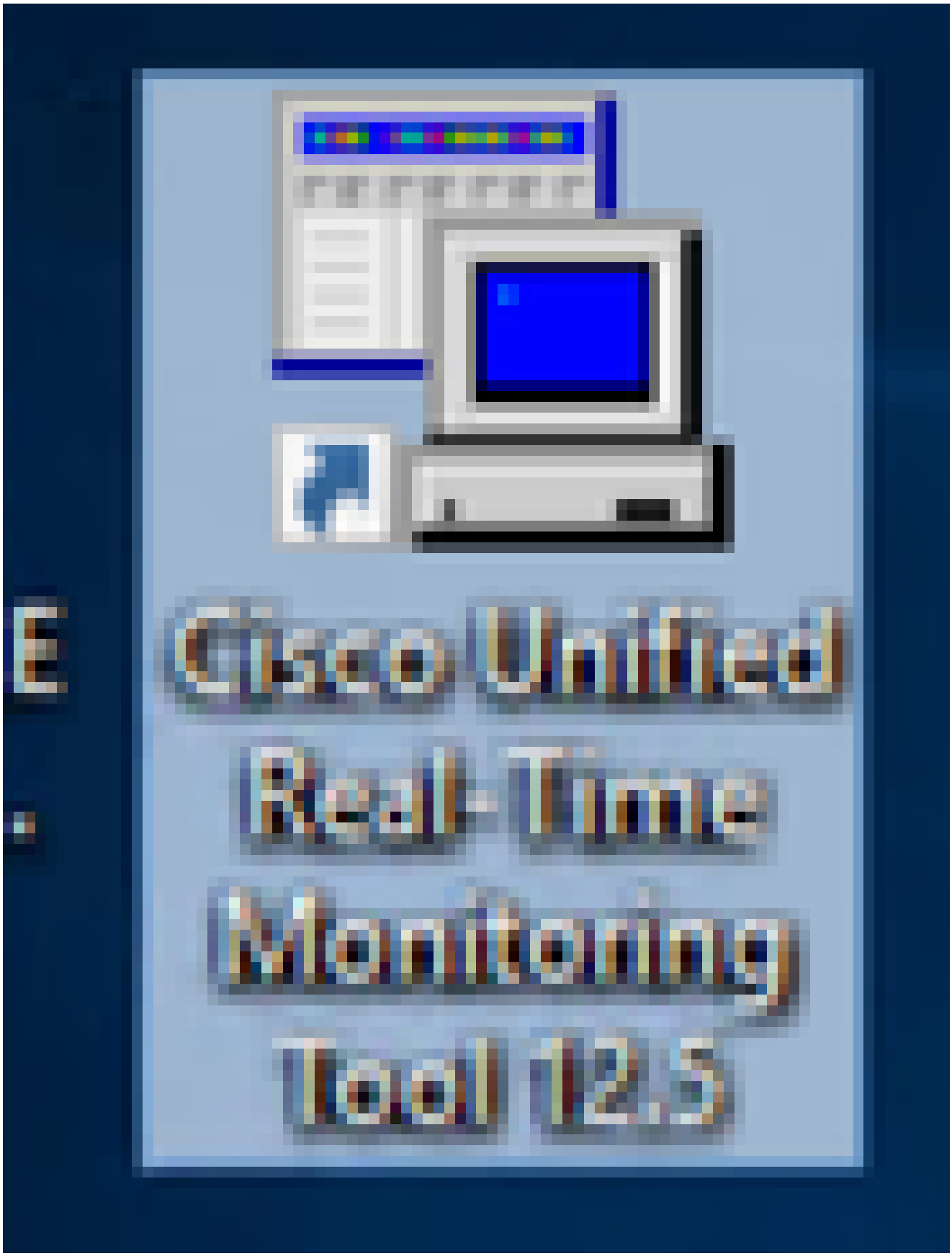
4. Verá el mensaje de confirmación después de hacer clic en el botón enable.



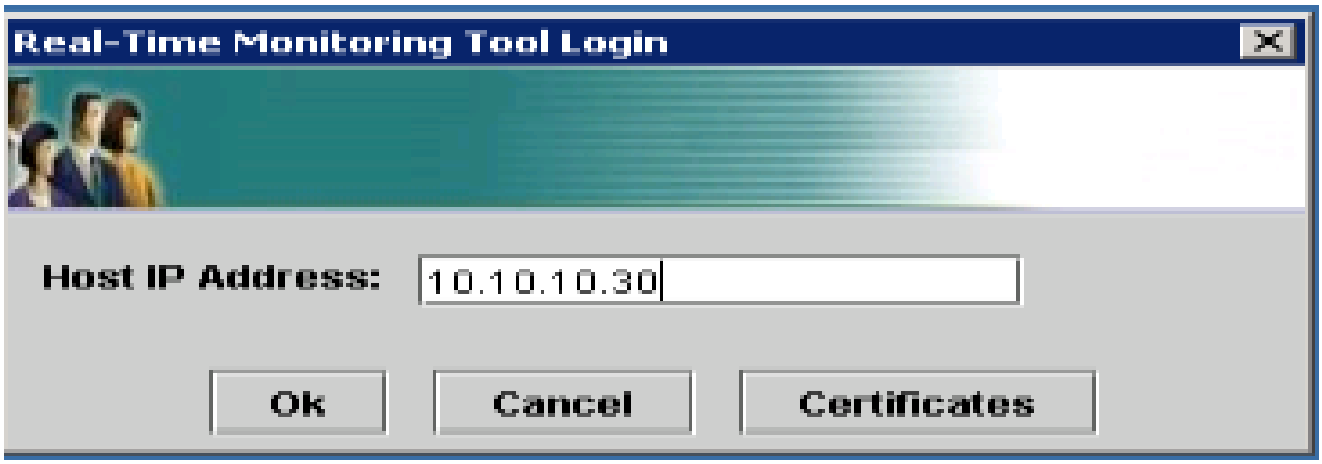
5. Una vez reproducido el problema, recopile los registros. Utilice la herramienta Real Time Monitor Tool (RTMT) que viene con CVB para recopilar los registros.

6. Haga clic en el icono Cisco Unified Real-Time Monitoring Tool en el escritorio (si es

necesario, descargue esta herramienta del CVB).

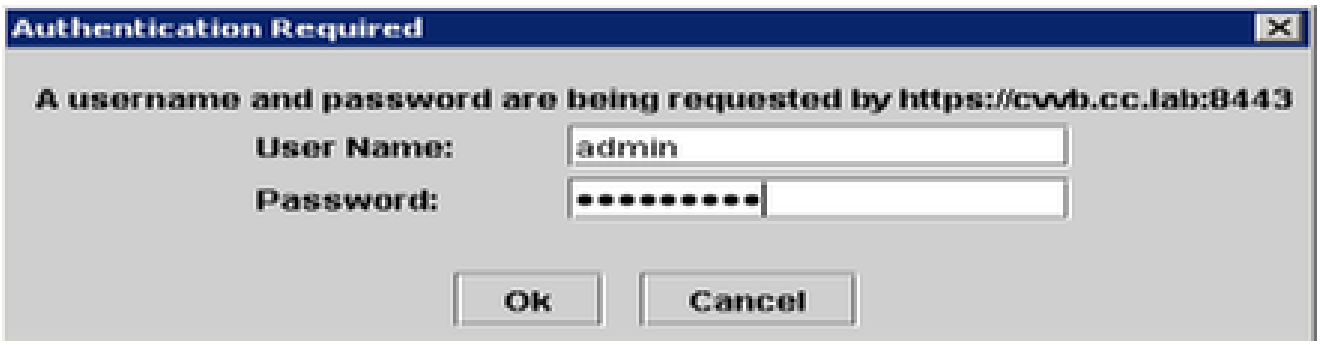


7. Proporcione la dirección IP del VB y haga clic en OK.



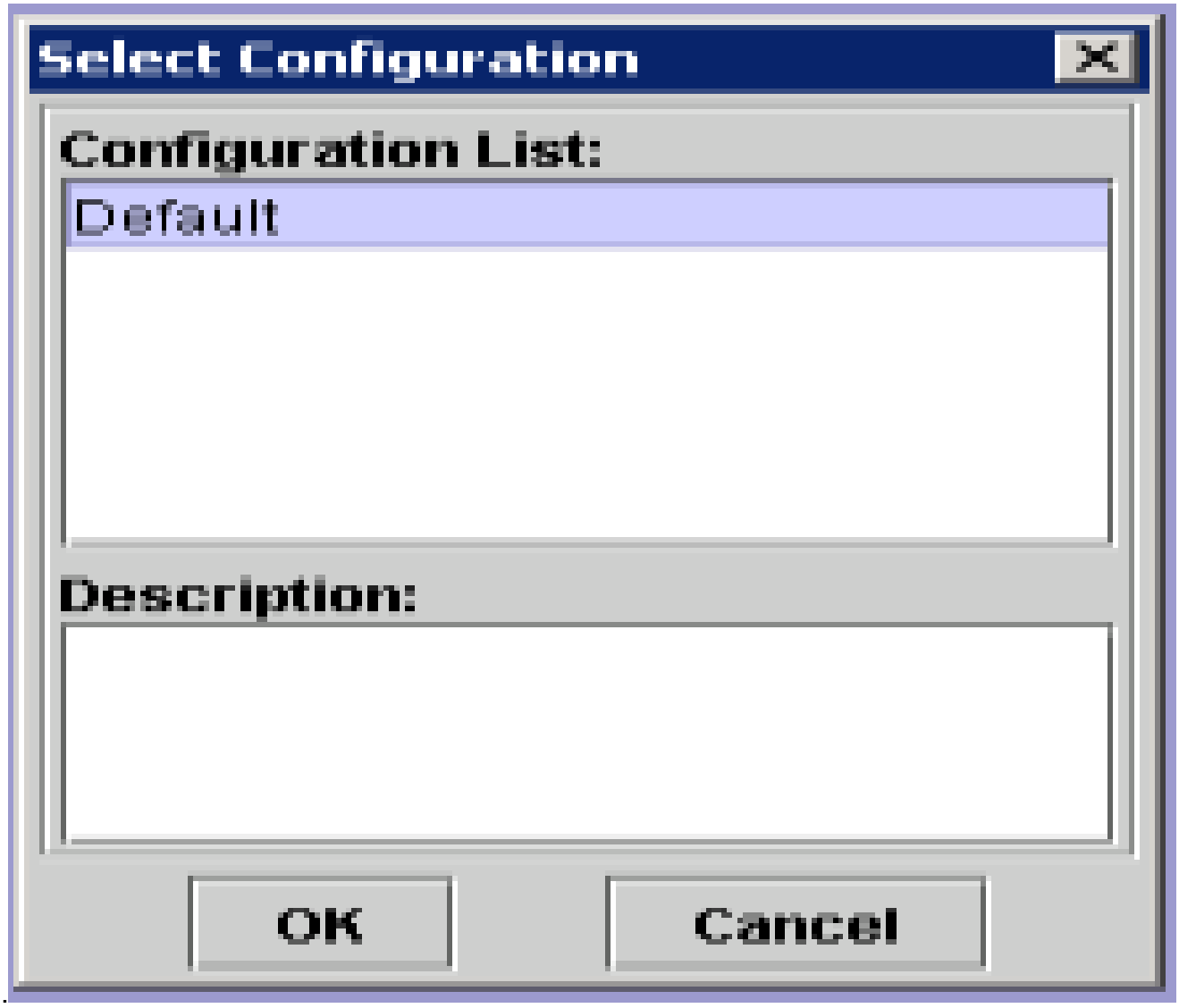
8. Acepte la información del certificado, si se muestra

9. Proporcione la credencial y haga clic en Aceptar.

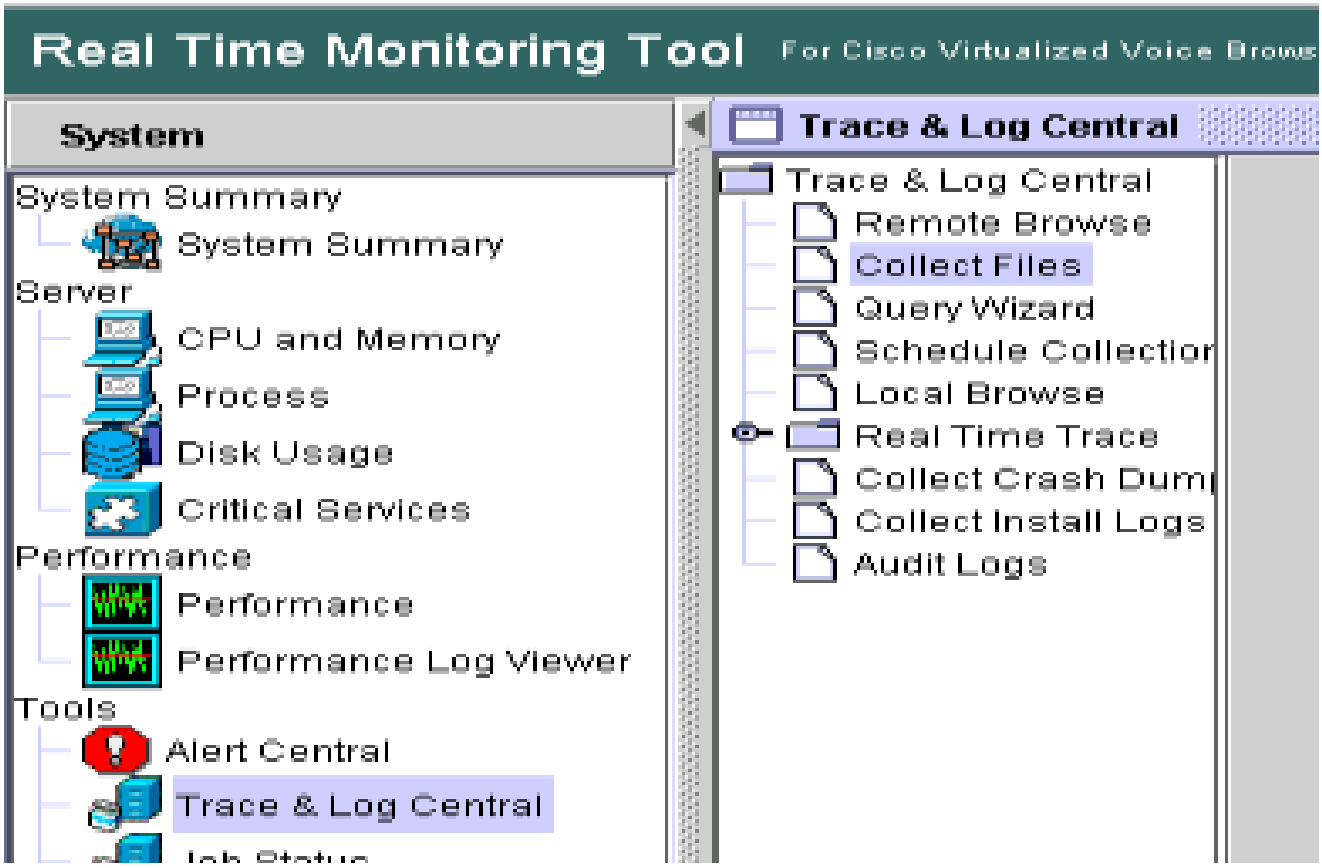


10. Si recibe el error TimeZone, RTMT puede cerrarse después de hacer clic en el botón Yes. Vuelva a iniciar la herramienta RTMT.

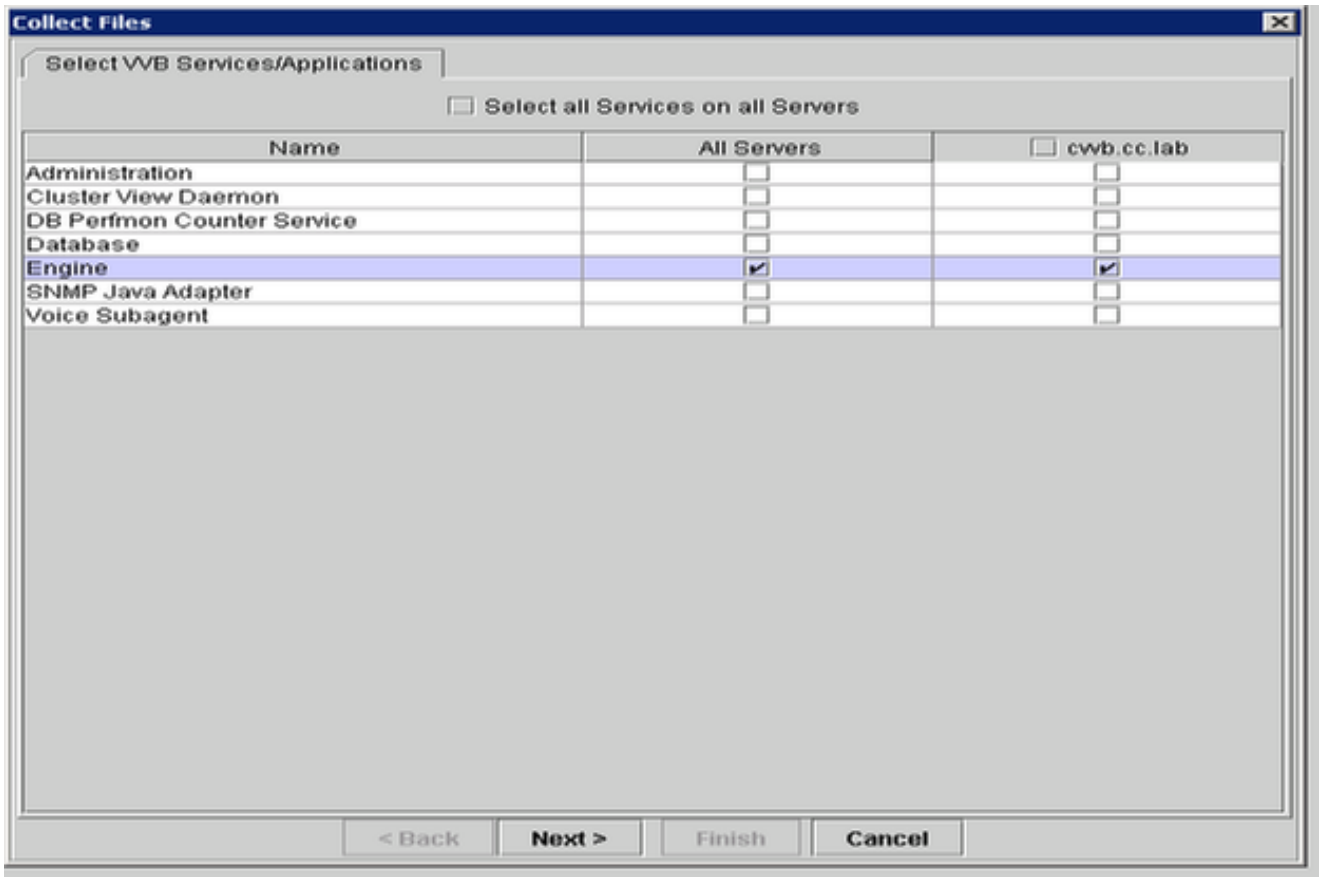
11. Deje seleccionada la configuración predeterminada y haga clic en Aceptar.



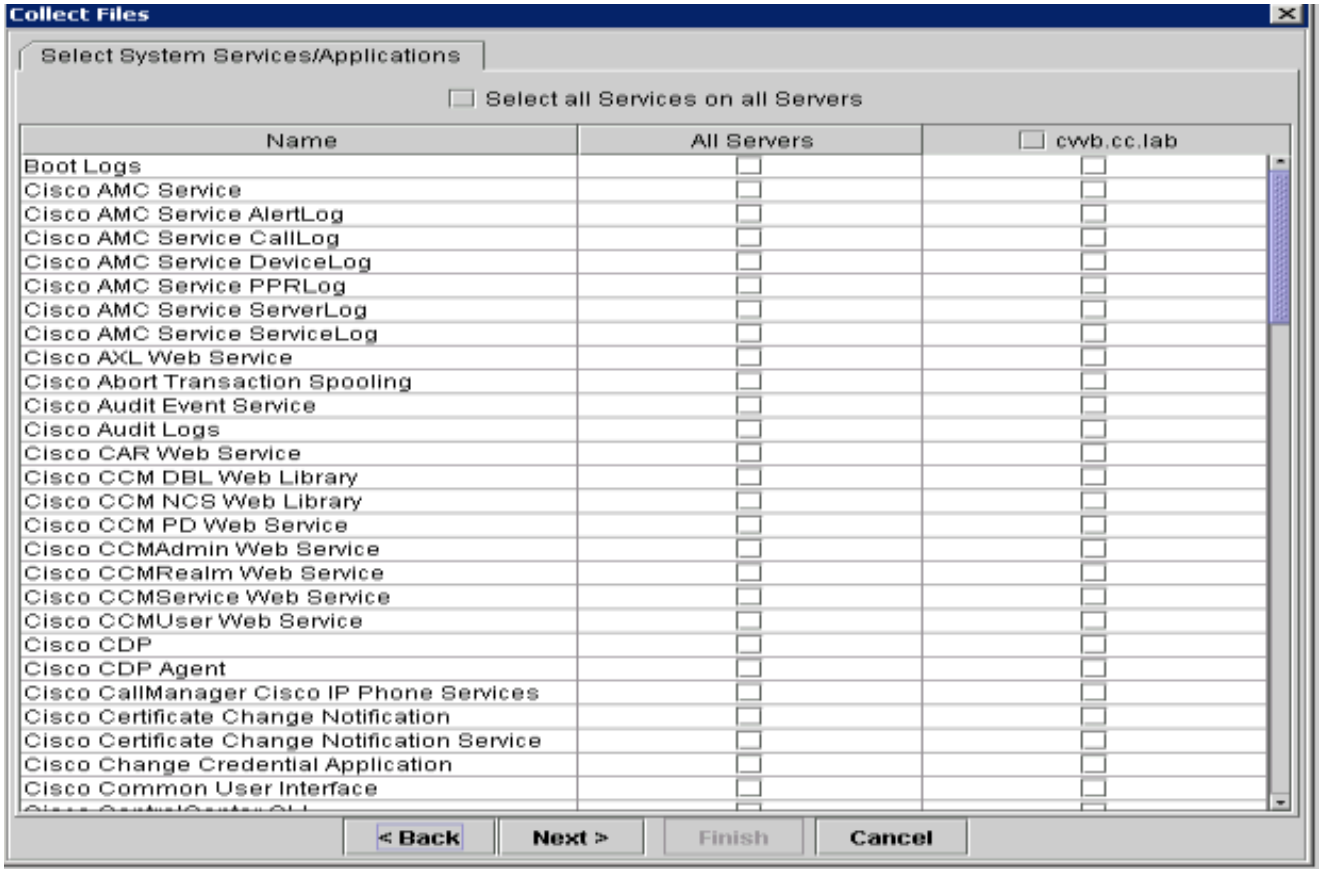
12. Seleccione Trace & Log Central y, a continuación, haga doble clic en Collect Files.



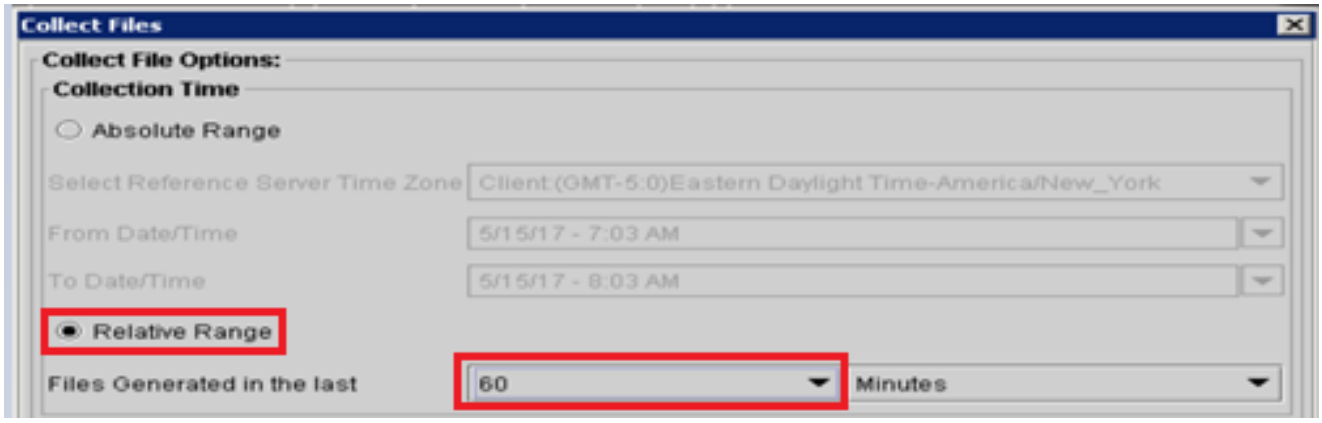
13. En la nueva ventana abierta, seleccione el Motor y haga clic en Siguiente.



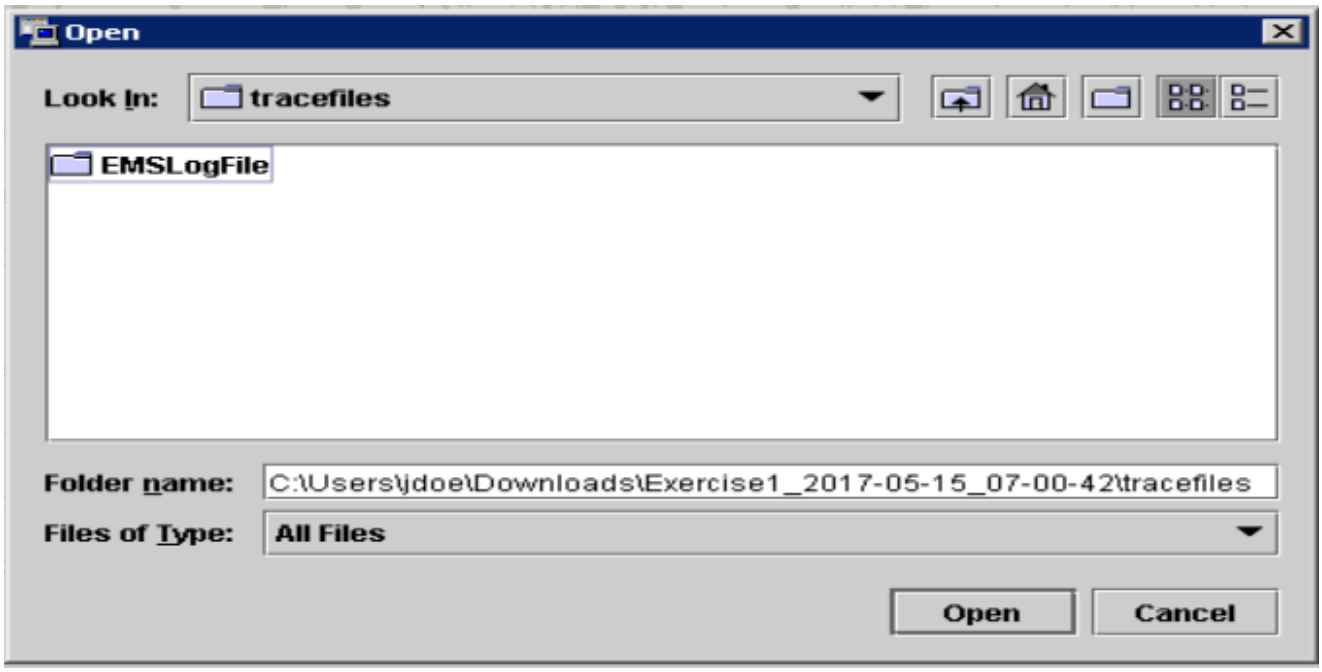
14. Haga clic en Next nuevamente en la siguiente ventana.



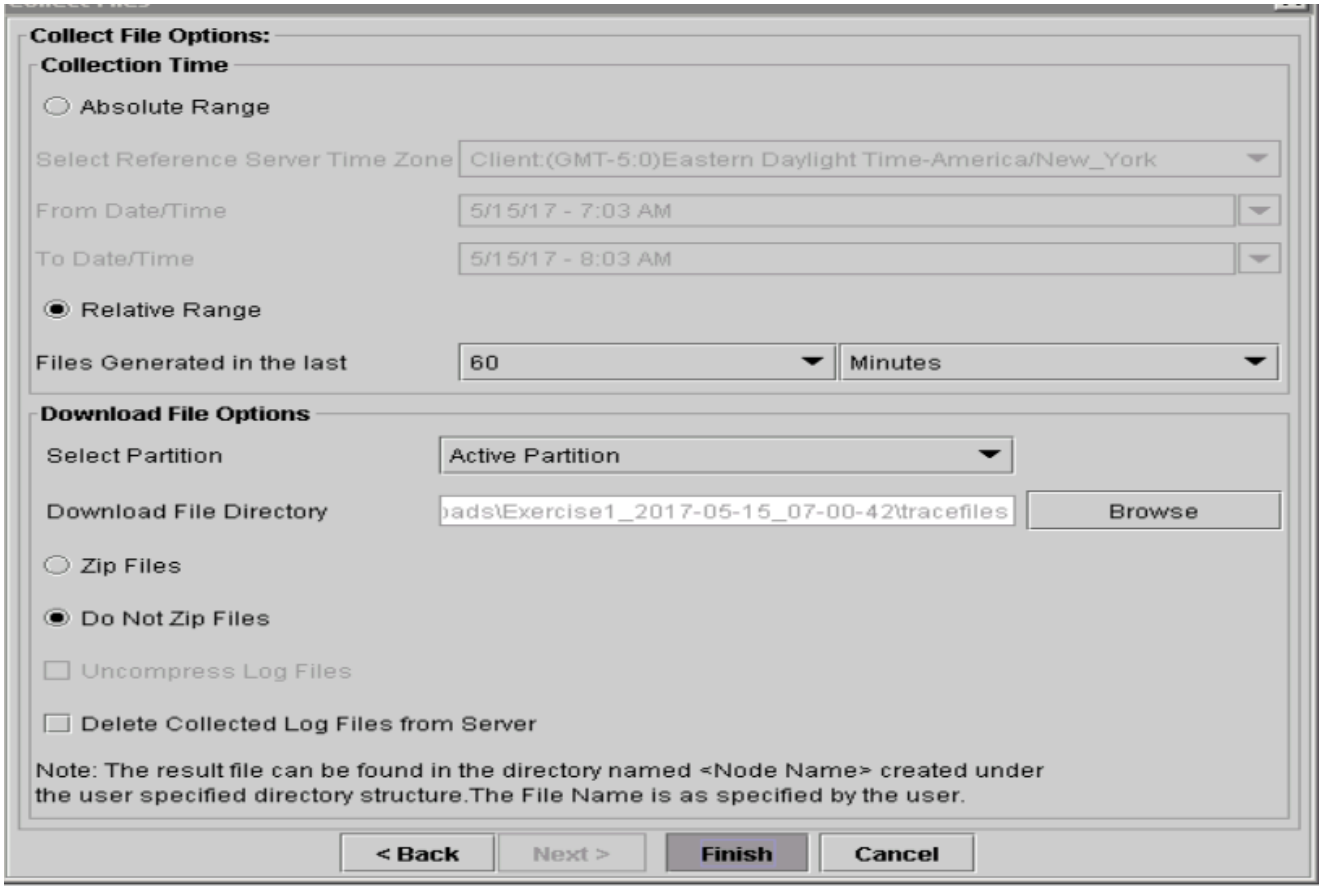
15. Seleccione Relative Range y asegúrese de seleccionar time para cubrir el tiempo de la llamada incorrecta.



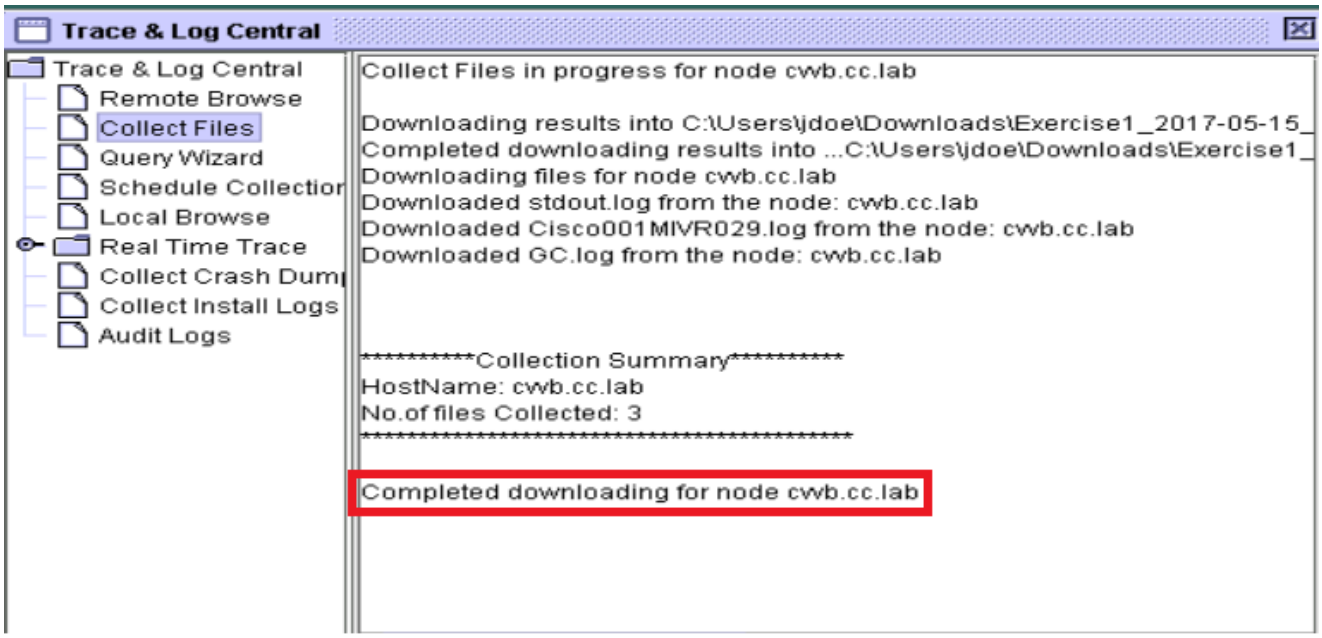
16. En Download File Options, haga clic en Browse y seleccione el directorio donde desea guardar el archivo, luego haga clic en Open.



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.

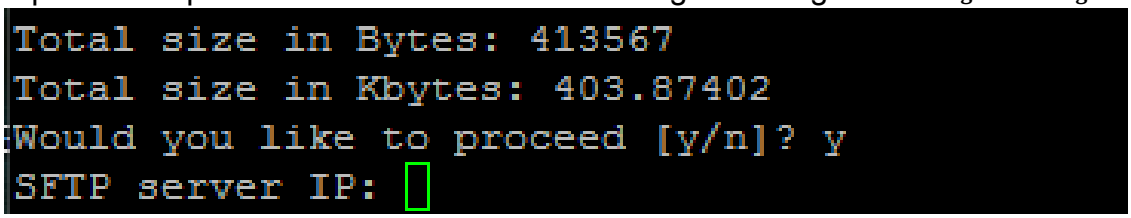


19. Vaya a la carpeta donde se guardan los seguimientos.

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/***



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.

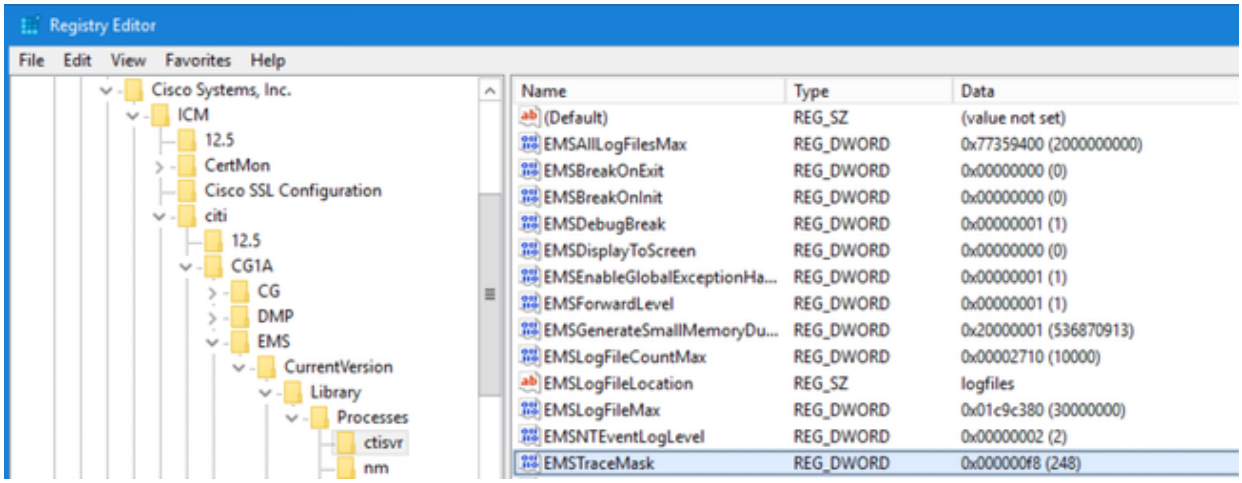
Por ejemplo, si resuelve problemas del Marcador de salida, el nivel de seguimientos debe

establecerse en el nivel 2 si el Marcador está ocupado.

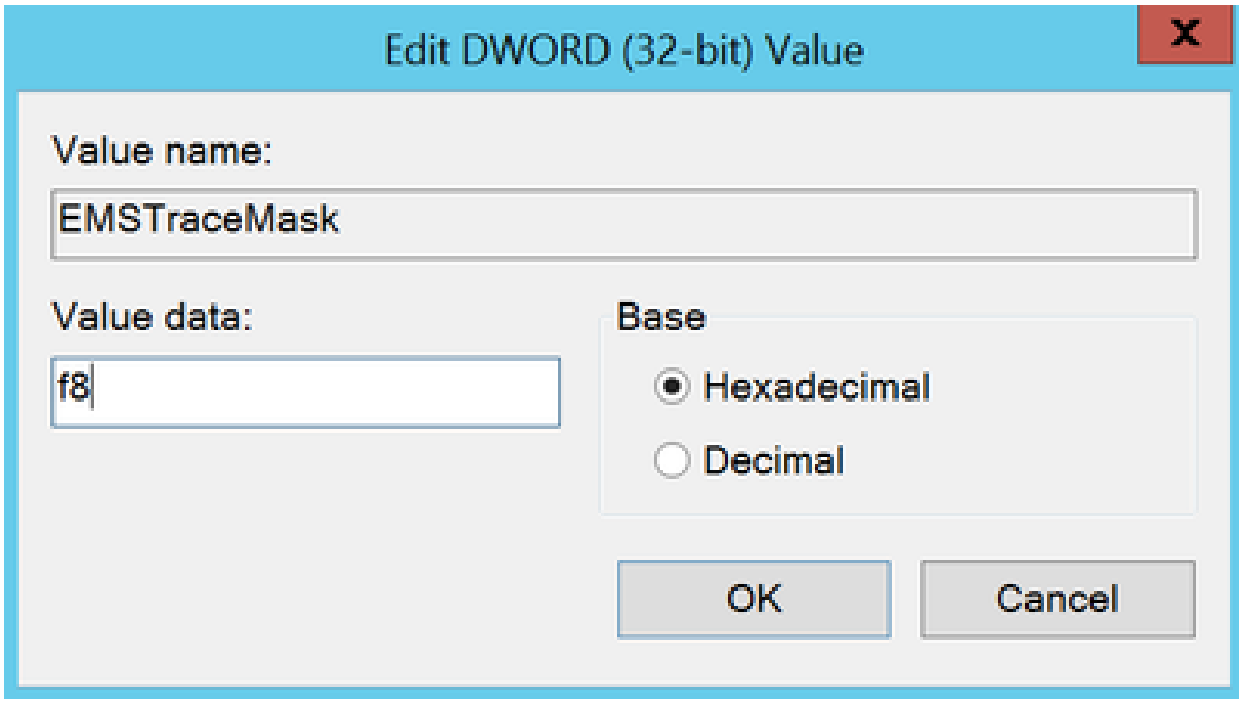
Para CTISVR (CTISVR), los niveles 2 y 3 no establecen el nivel de registro exacto recomendado por Cisco. El registro de seguimiento recomendado para CTISVR es 0XF8.

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.



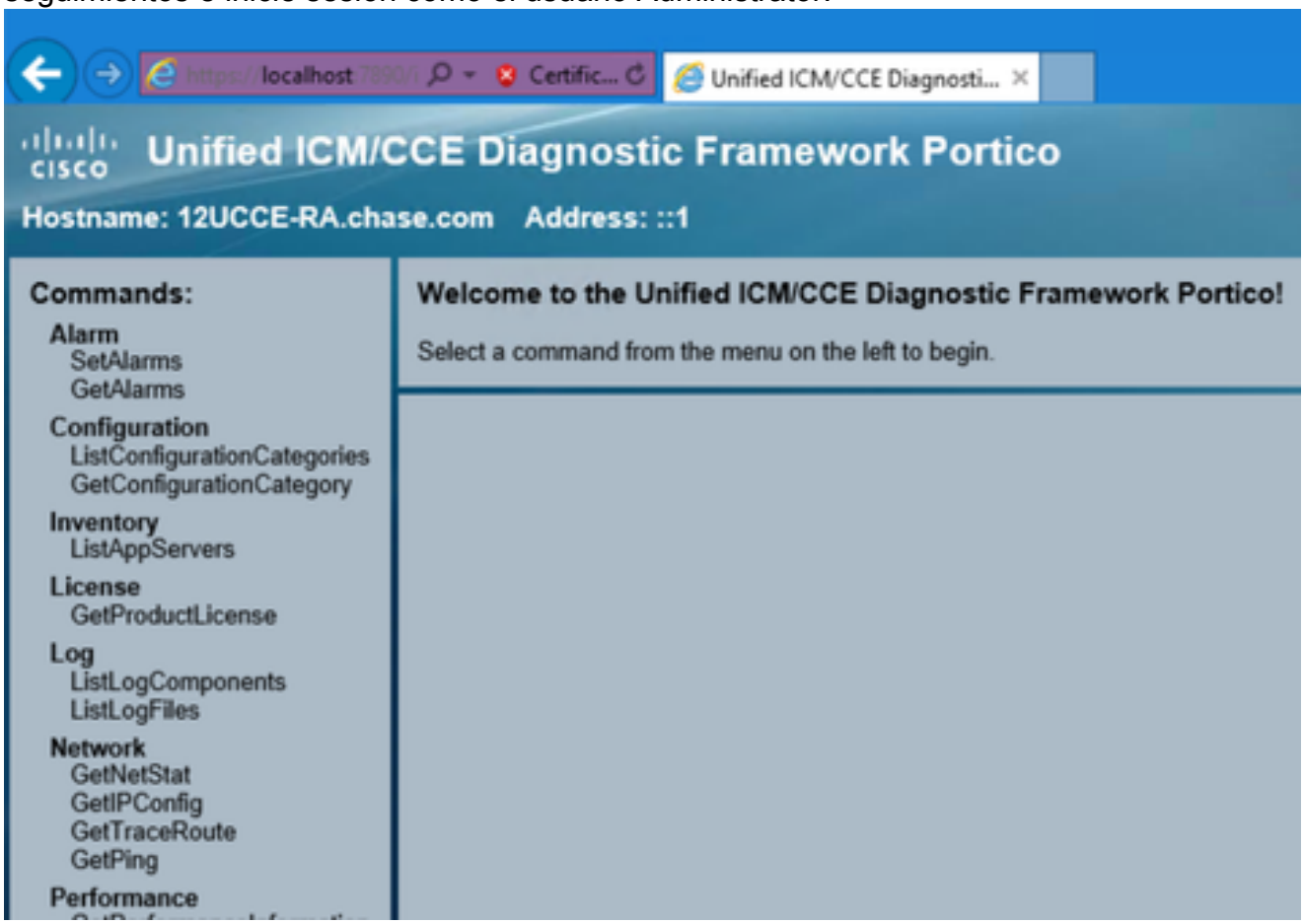
3. Haga doble clic en EMSTraceMask y establezca el valor en f8.



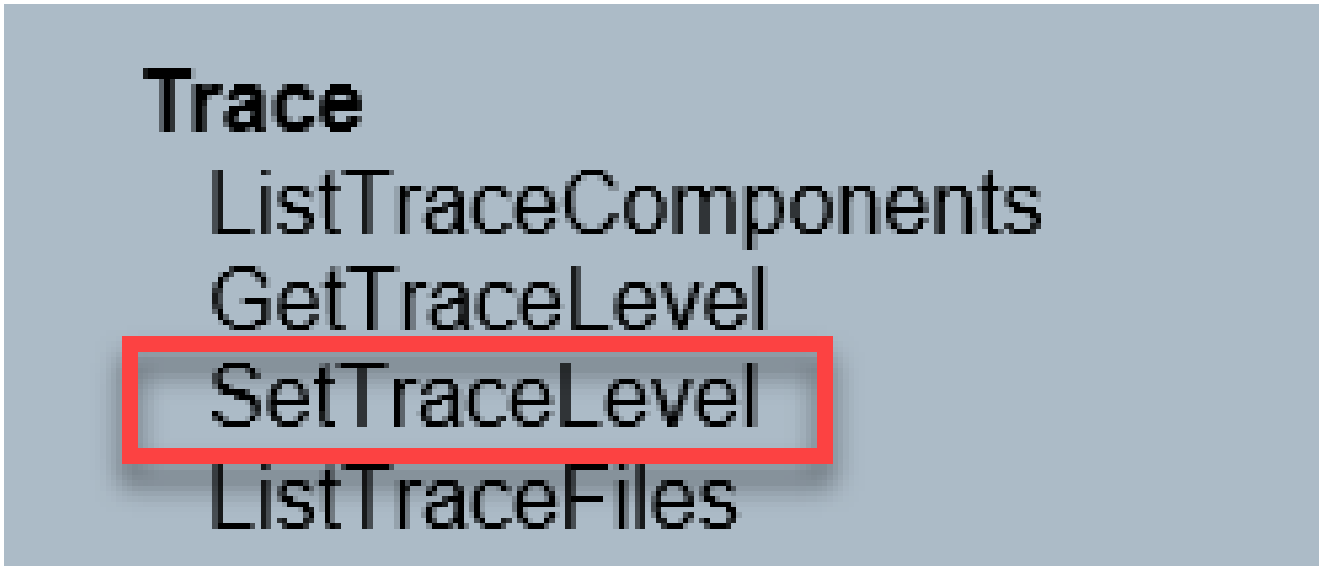
4. Haga clic en Aceptar y cierre el Editor del Registro. Estos son los pasos para establecer cualquiera de los seguimientos de componentes de UCCE (el proceso RTR se utiliza como ejemplo).

Establecer nivel de seguimiento

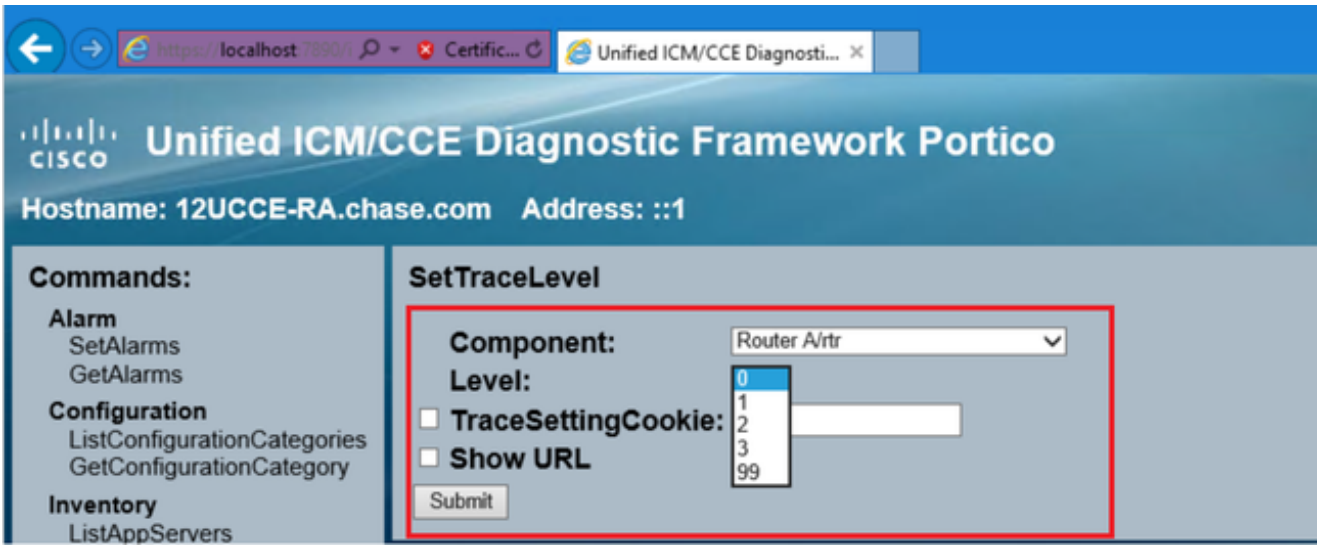
1. Abra Diagnostic Framework Portico desde el servidor que necesita para establecer los seguimientos e inicie sesión como el usuario Administrator.



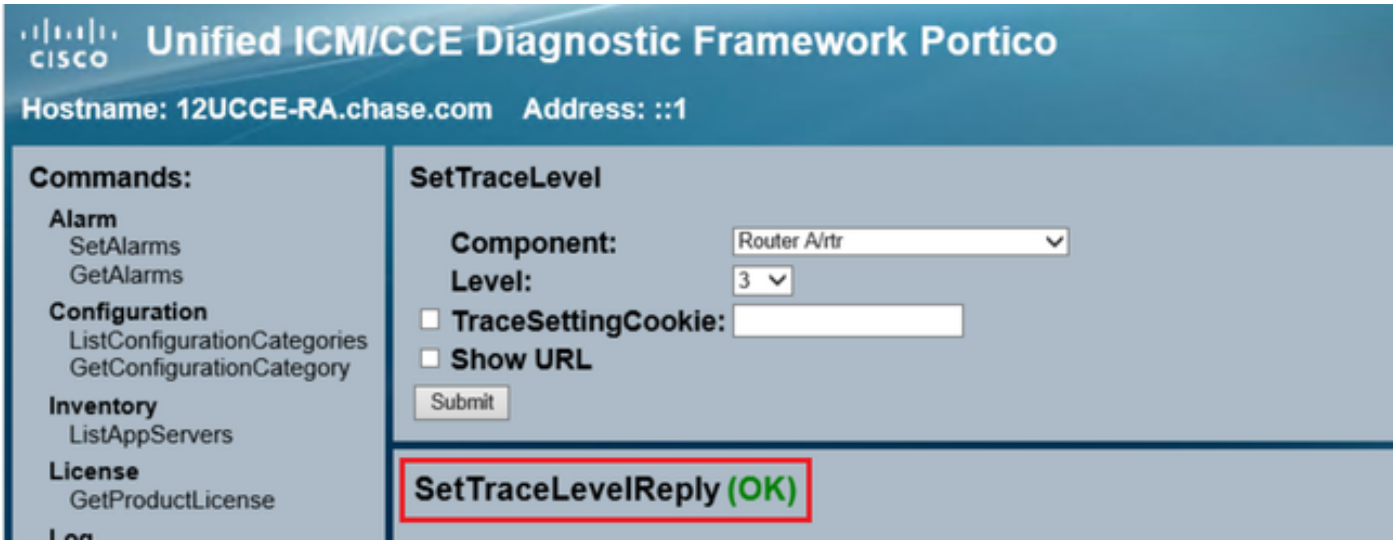
2. En la sección Comandos, desplácese hasta Seguimiento y seleccione SetTraceLevel.



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



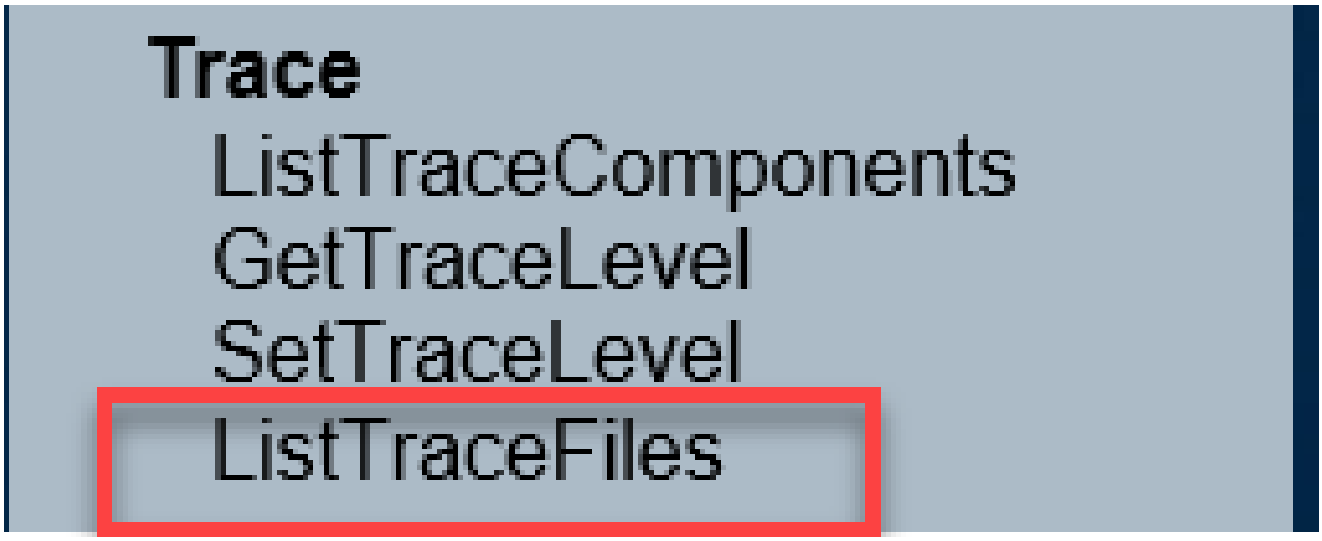
4. Haga clic en Submit (Enviar). Cuando haya terminado, verá el mensaje Aceptar.



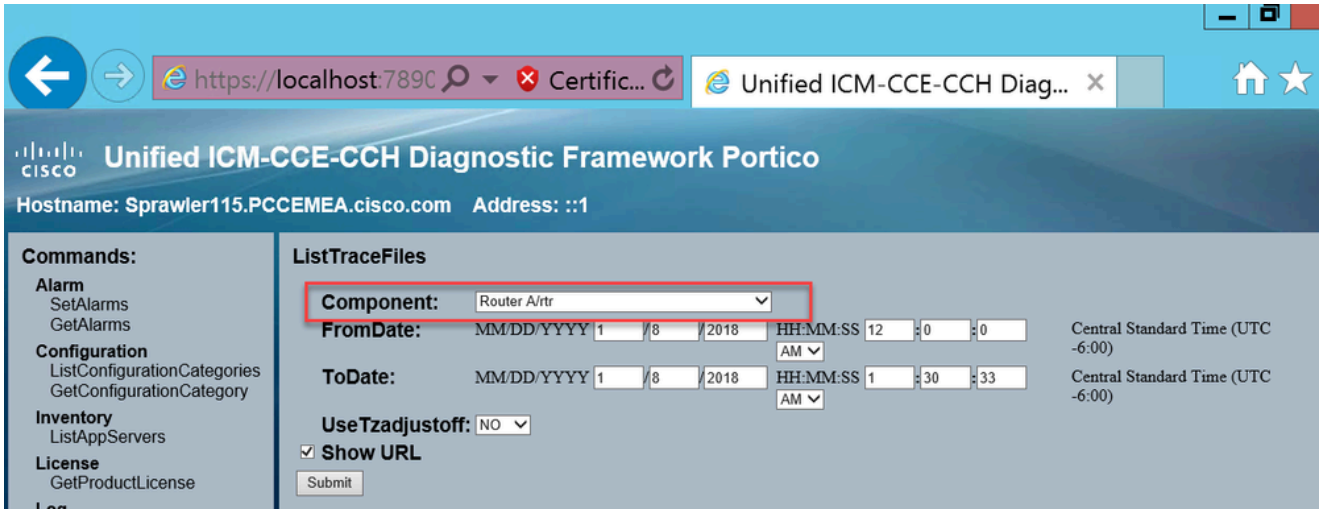
Advertencia: Establezca el nivel de seguimientos en el nivel 3 mientras intenta reproducir el problema. Una vez reproducido el problema, establezca el nivel de seguimiento en el valor predeterminado. Tenga especial cuidado cuando establezca los seguimientos de JTAPIGW, ya que los niveles 2 y 3 establecen 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

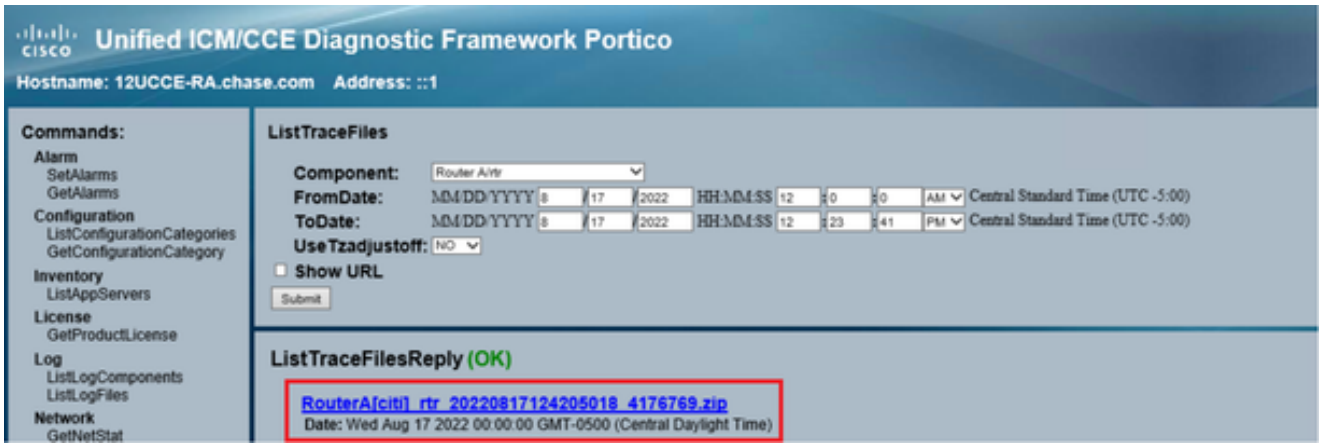
1. Desde Diagnostic Framework Portico, en la sección Commands, navegue hasta Trace y seleccione ListTraceFile.



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



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

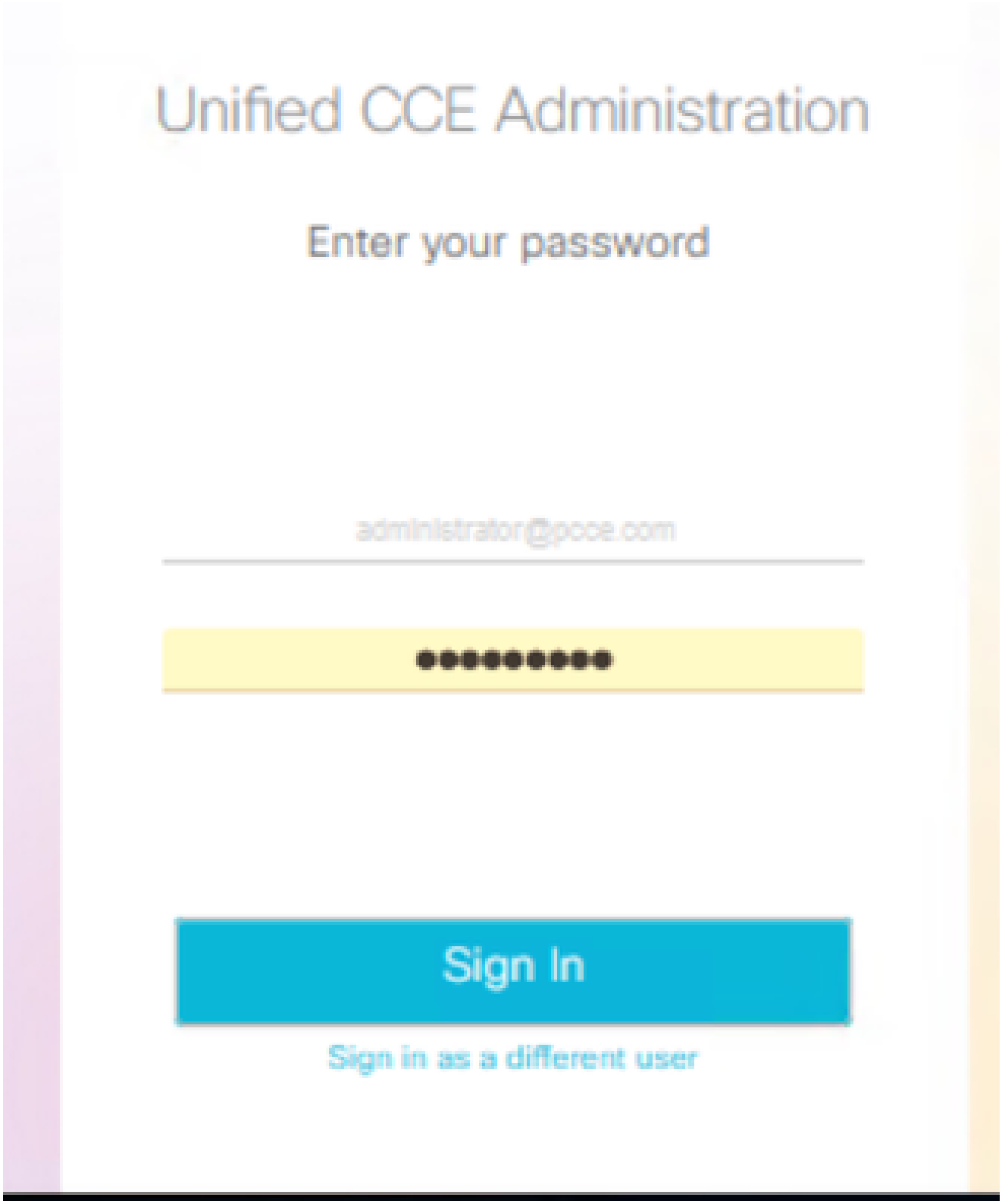


4. Haga clic en el enlace del archivo ZIP y guarde el archivo en la ubicación que elija.

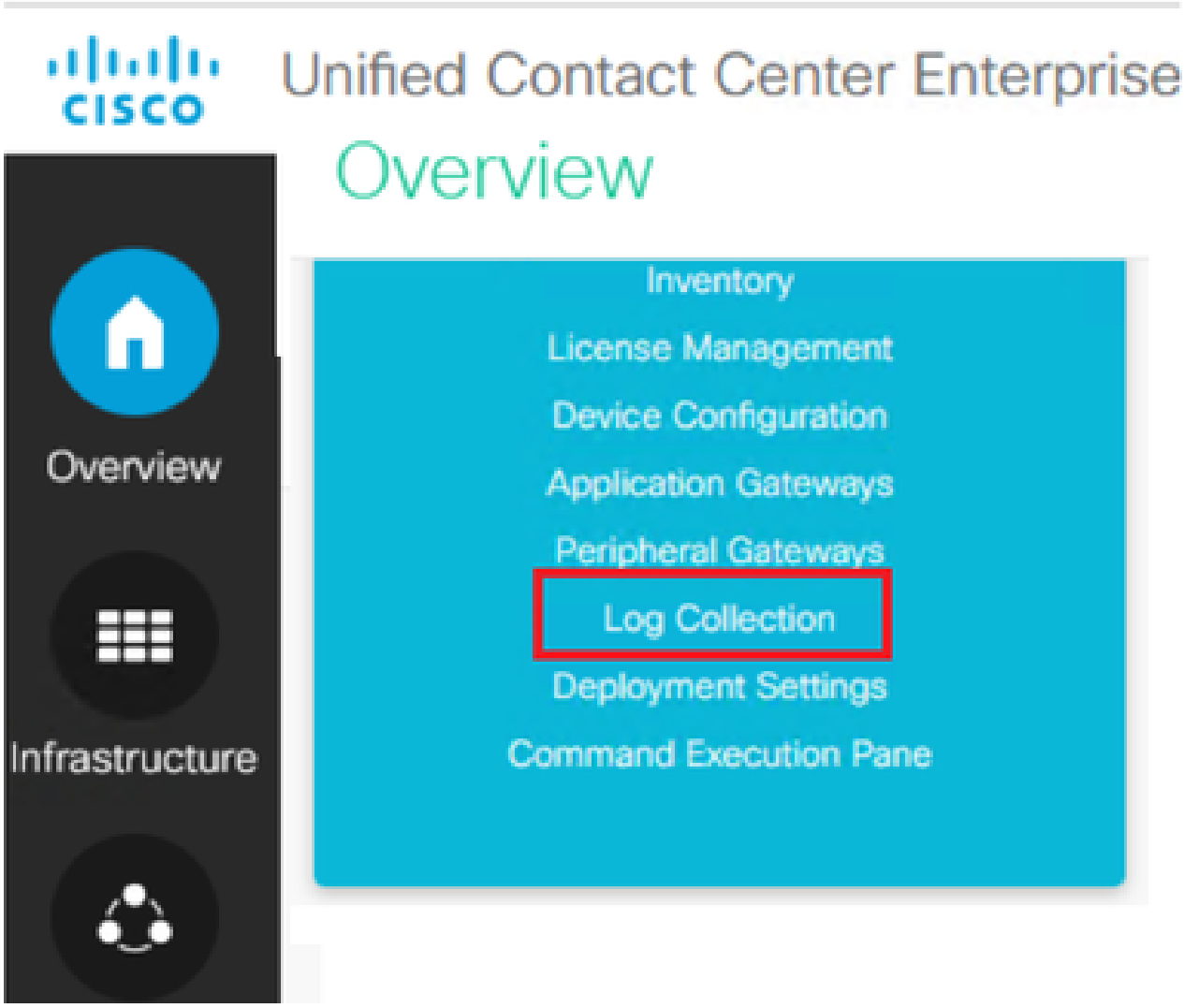
Establecer registros de seguimiento y recopilación de PCCE

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.

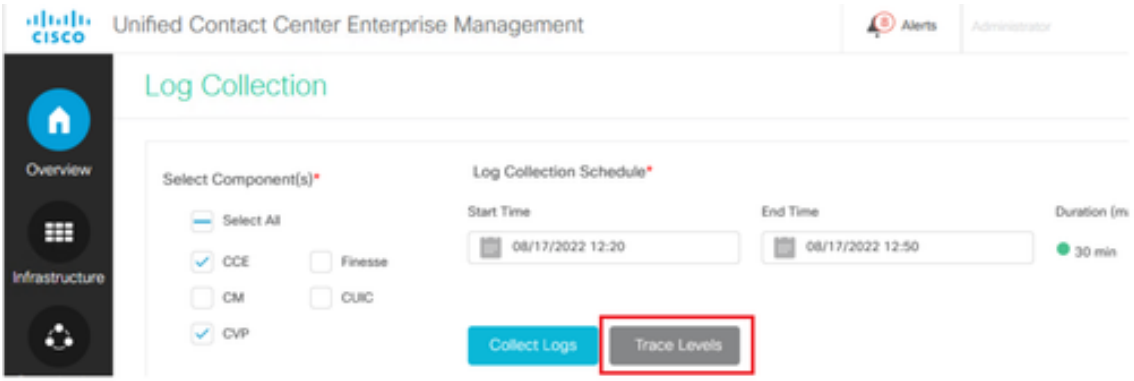
1. Desde el servidor PCCE AW, abra la herramienta Unified CCE Web Administration e inicie sesión en la cuenta Administrator.



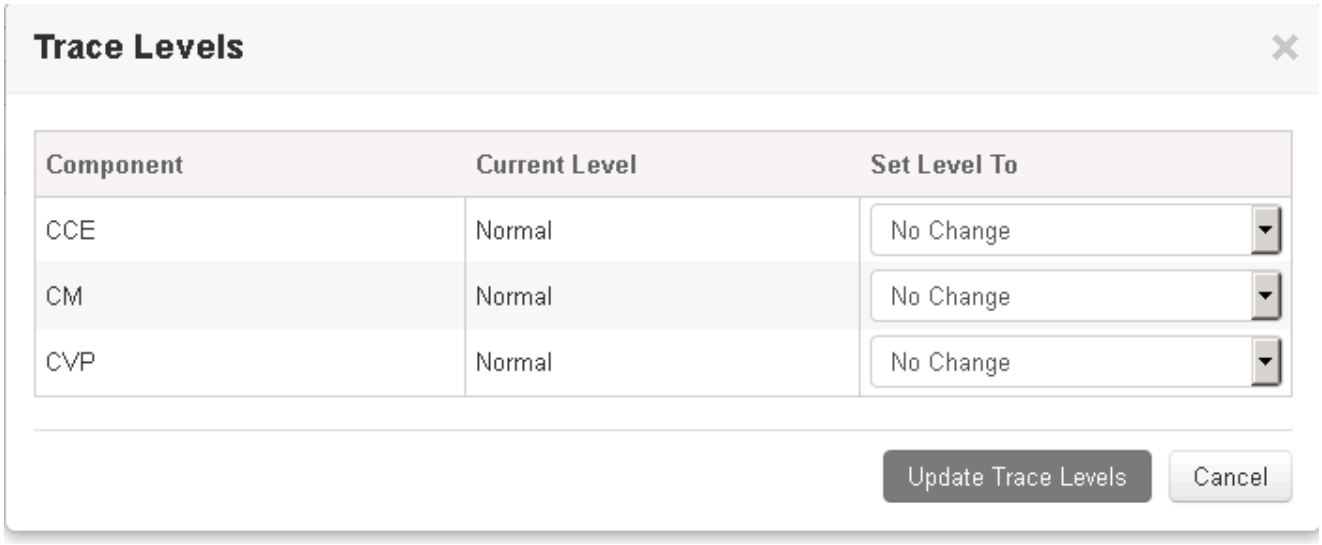
2. Navegue hasta Descripción general > Configuración de infraestructura > Recopilación de registro para abrir la página Recopilación de registro.



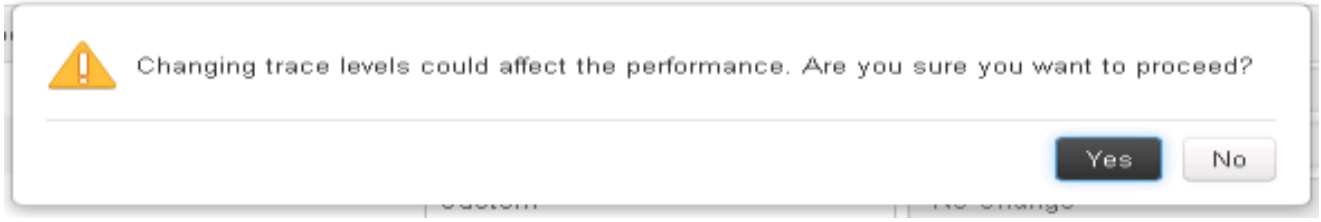
3. En la página Recopilación de registros, haga clic en Niveles de seguimiento, que abre el cuadro de diálogo Niveles de seguimiento.



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.



5. Haga clic en Yes para aceptar la Advertencia.



6. Una vez reproducido el problema, abra Unified CCE Administration y vuelva a System >Log Collection.
7. Seleccione CCE y CVP en el panel Componentes.
8. Seleccione el tiempo de recopilación de registros correspondiente (el valor predeterminado es los últimos 30 minutos).
9. 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.

10. 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

1. Inicie sesión en la línea de comandos SSH (CLI) de CUIC, LD e IDS.

2. 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.

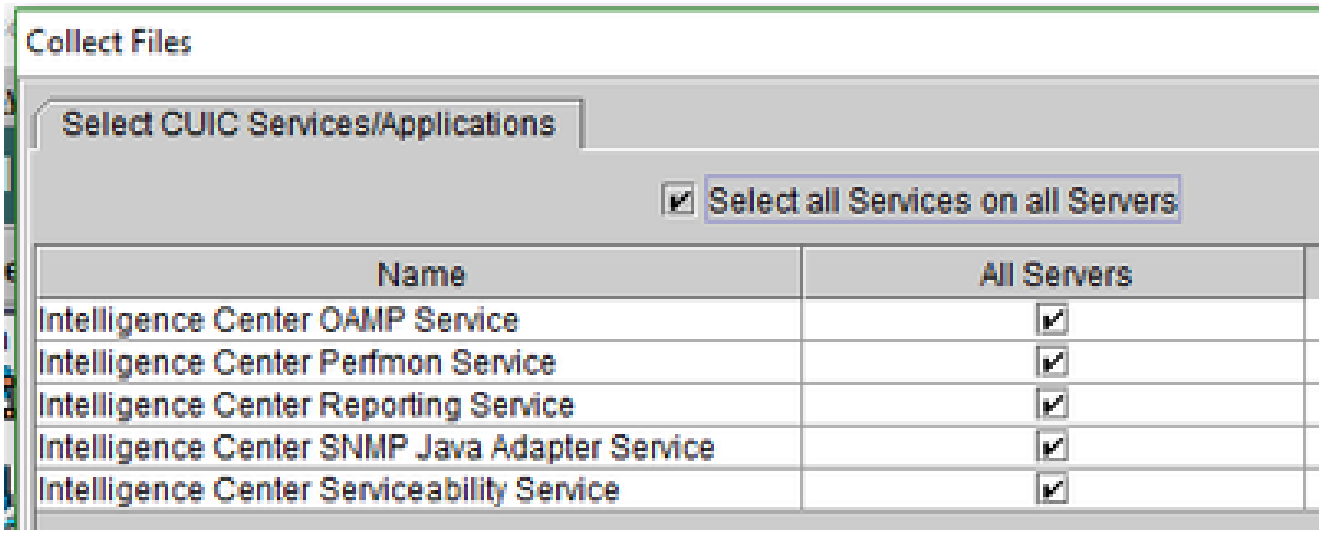
2. Navegue hasta Herramientas > Descarga del complemento RTMT. Descargue e instale el complemento.

3. Inicie RTMT e inicie sesión en el servidor con las credenciales de administrador.

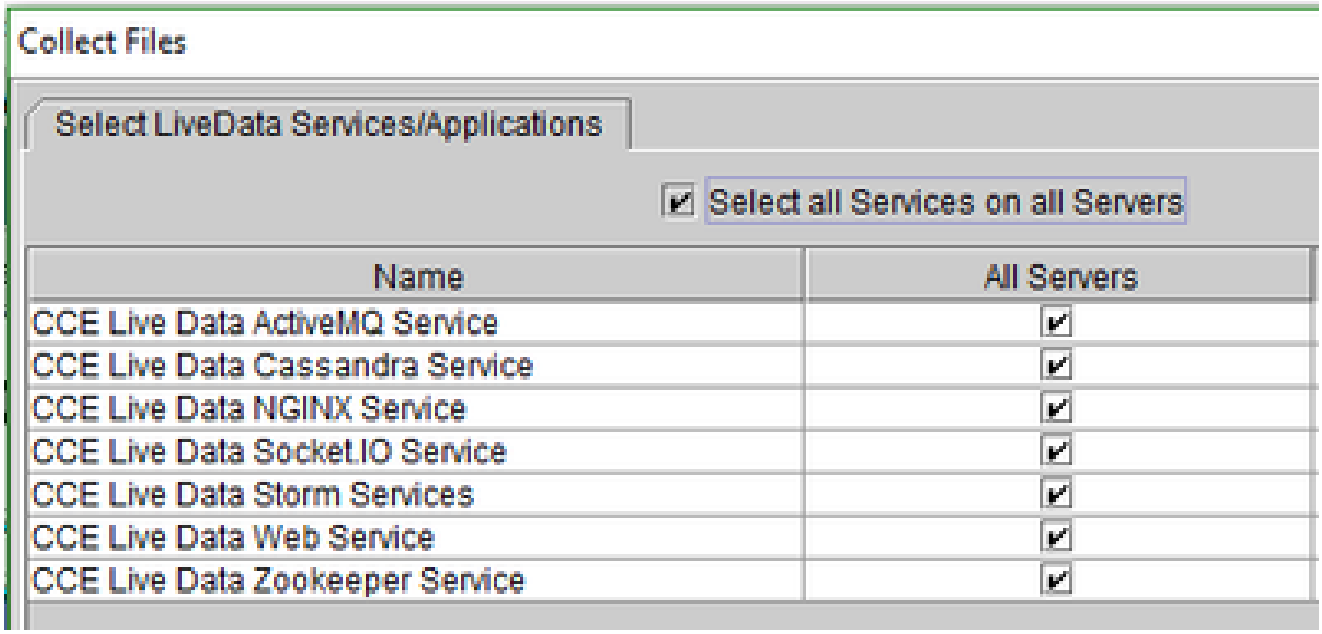
4. Haga doble clic en Trace and Log Central y luego haga doble clic en Collect Files.

5. Puede ver estas fichas para los servicios específicos. Debe seleccionar todos los servicios/servidores para CUIC, LD e IDS.

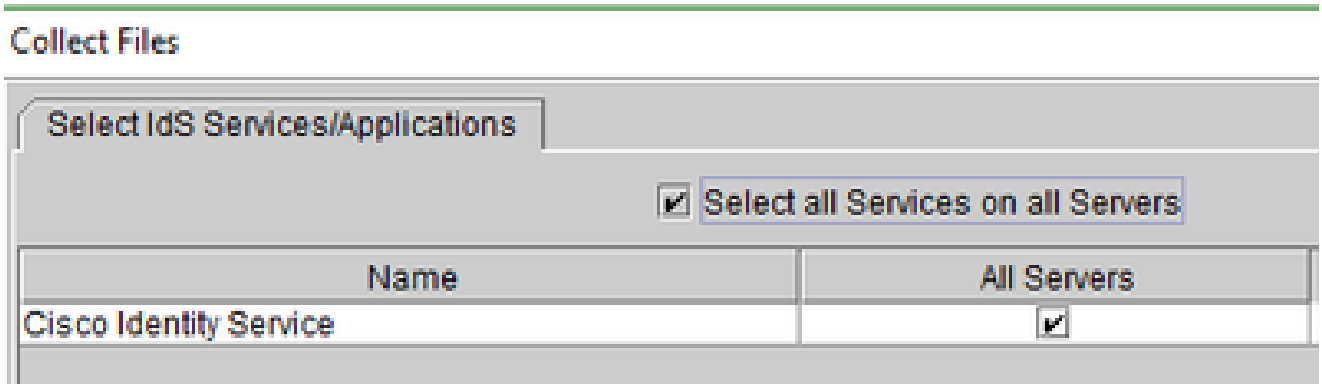
   Para CUIC:



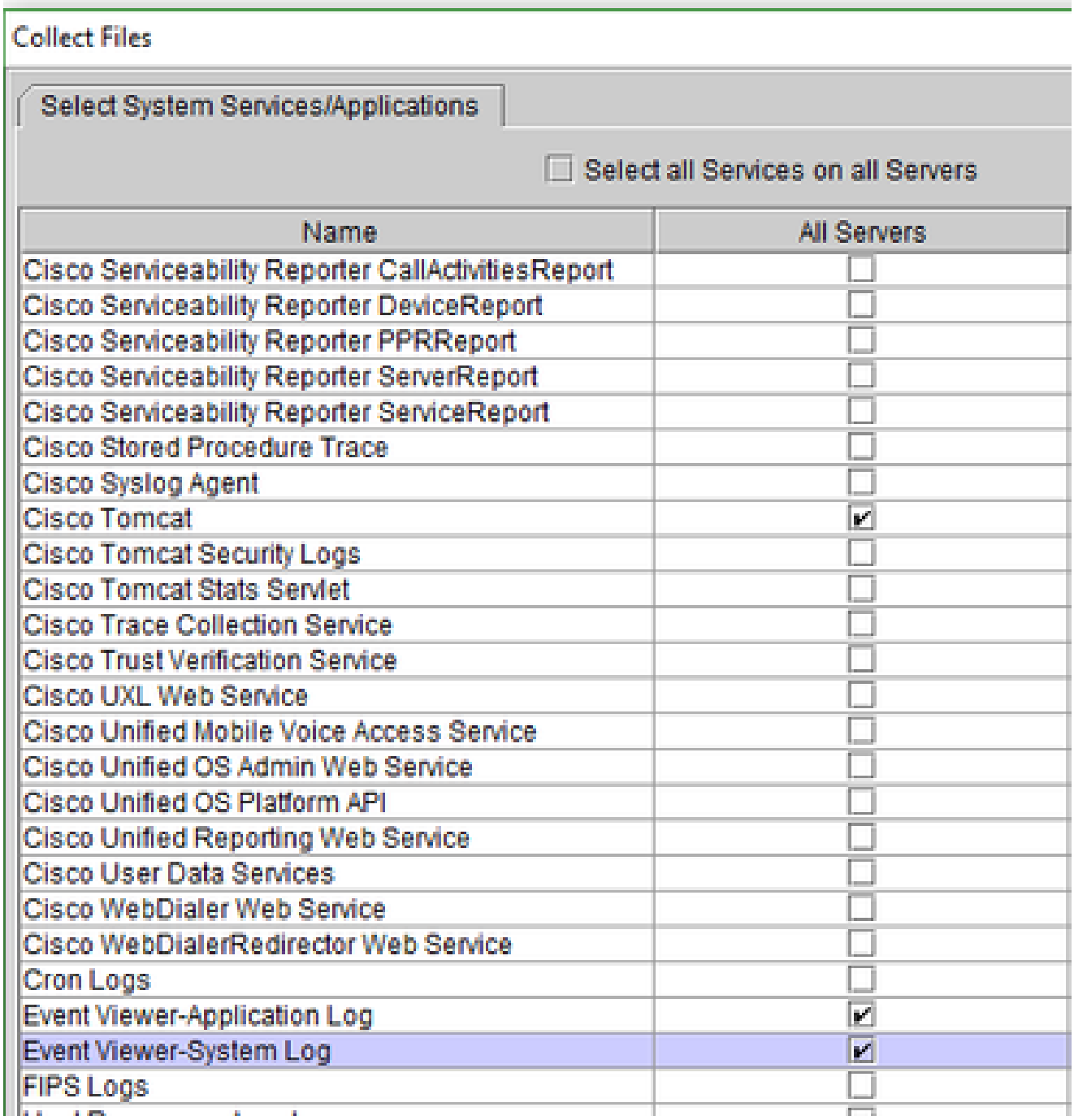
   Para LD:



Para IDS:



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

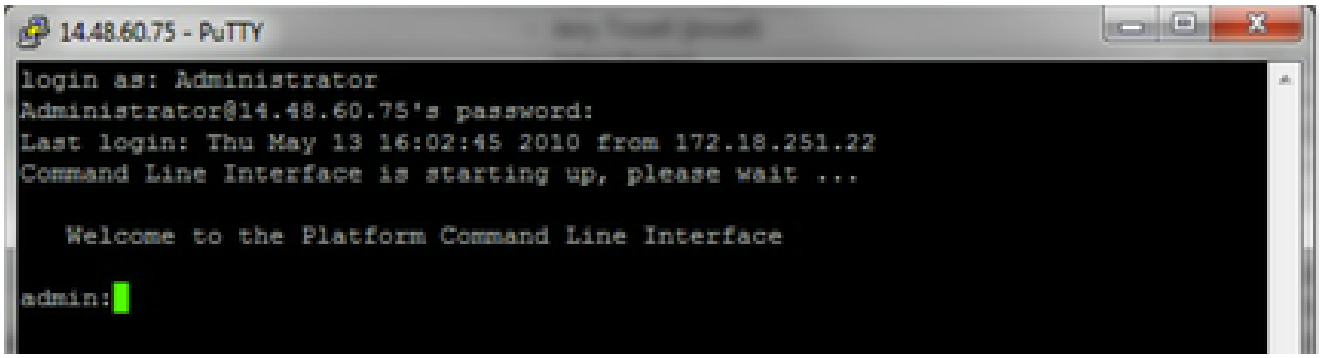


6. Seleccione la Fecha y la Hora junto con la carpeta destination para Guardar los registros.

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.

2. 

1 bis. Sintaxis del comando

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

<#root>

Syntax:

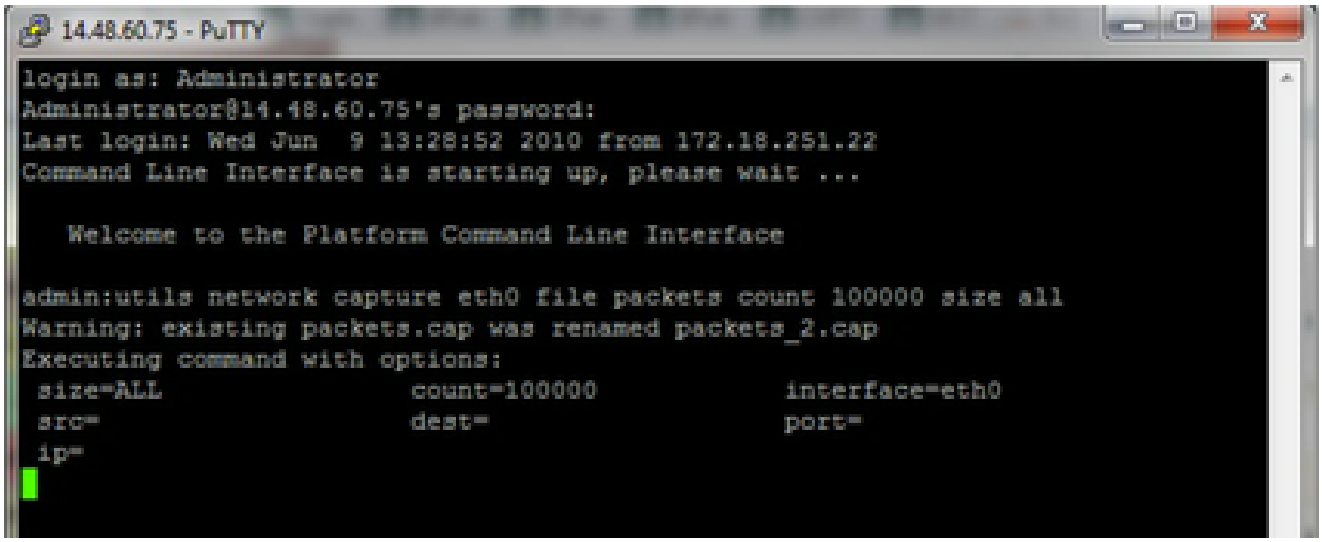
utils network capture

```
 [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

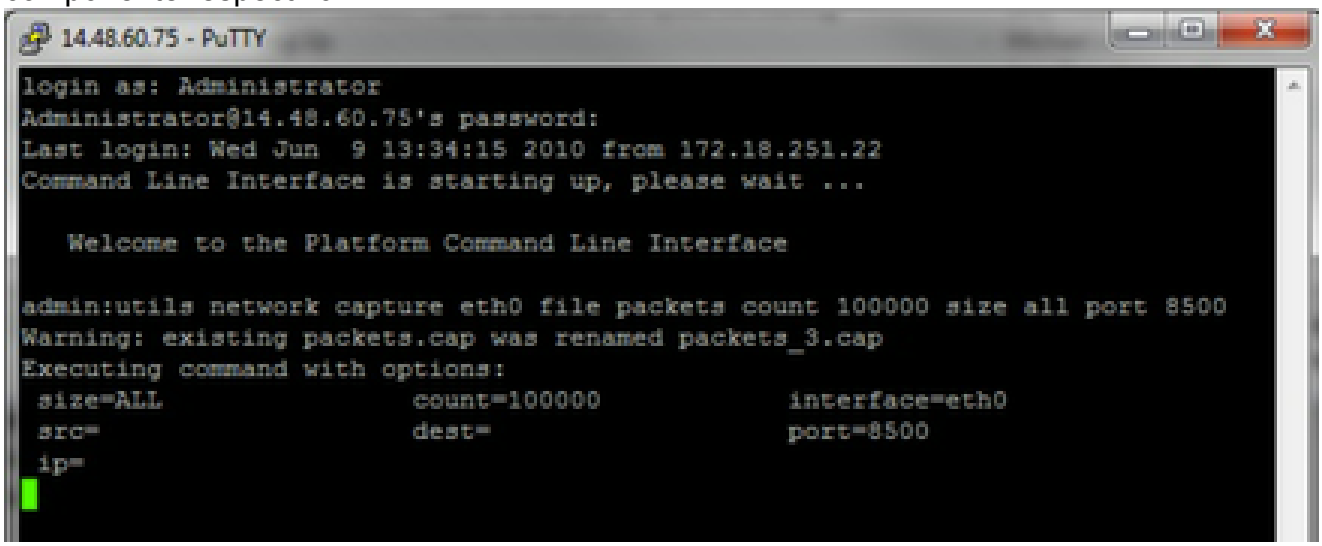
Para una captura típica, uno puede recopilar TODOS los paquetes de TODOS los tamaños desde y hacia TODAS las direcciones en un archivo de captura llamado packets.cap. Para ello, simplemente ejecute en la CLI de administración **utils network capture eth0 file packets count 100000 size all**



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).

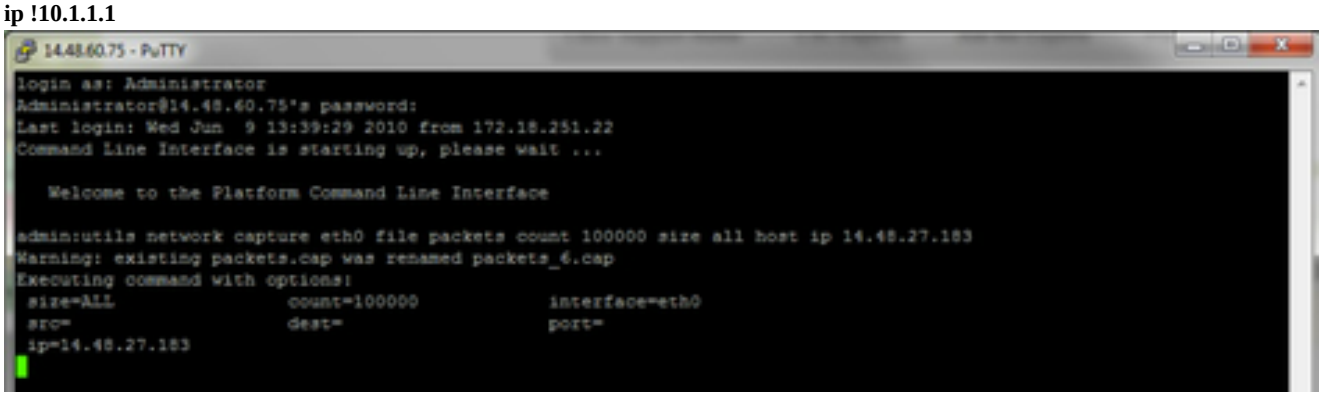
Para obtener más información sobre qué servicios requieren comunicaciones en cada puerto, consulte la Guía de Uso de Puertos TCP y UDP para obtener la versión aplicable del componente respectivo.



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**

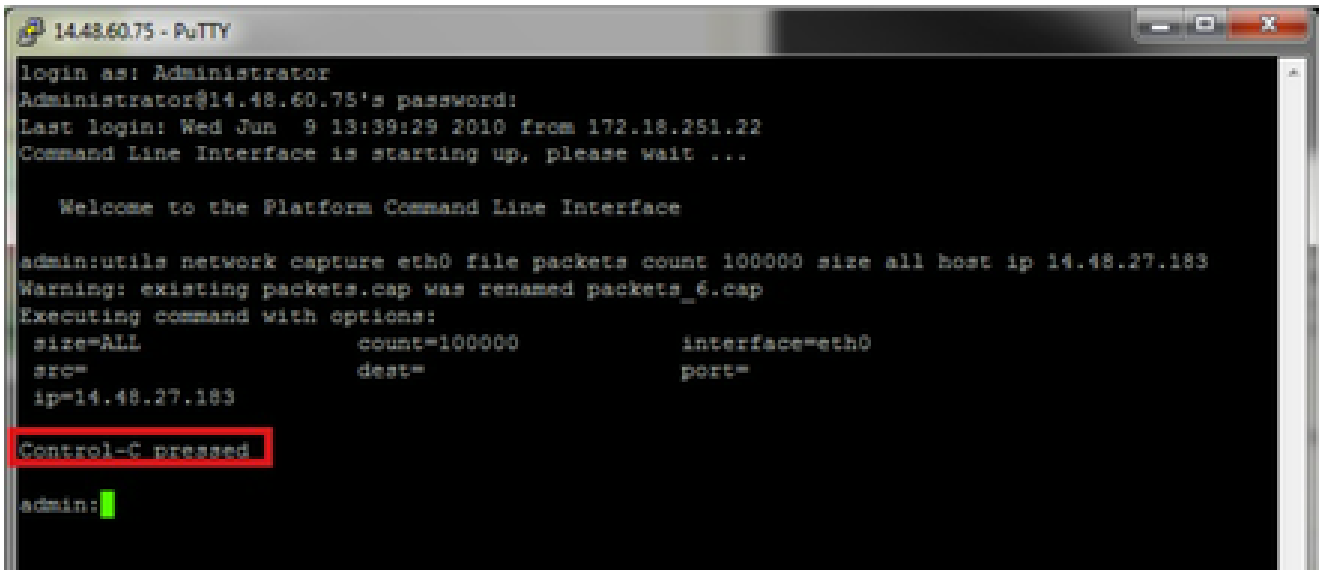


3. Reproduzca el síntoma del problema

   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

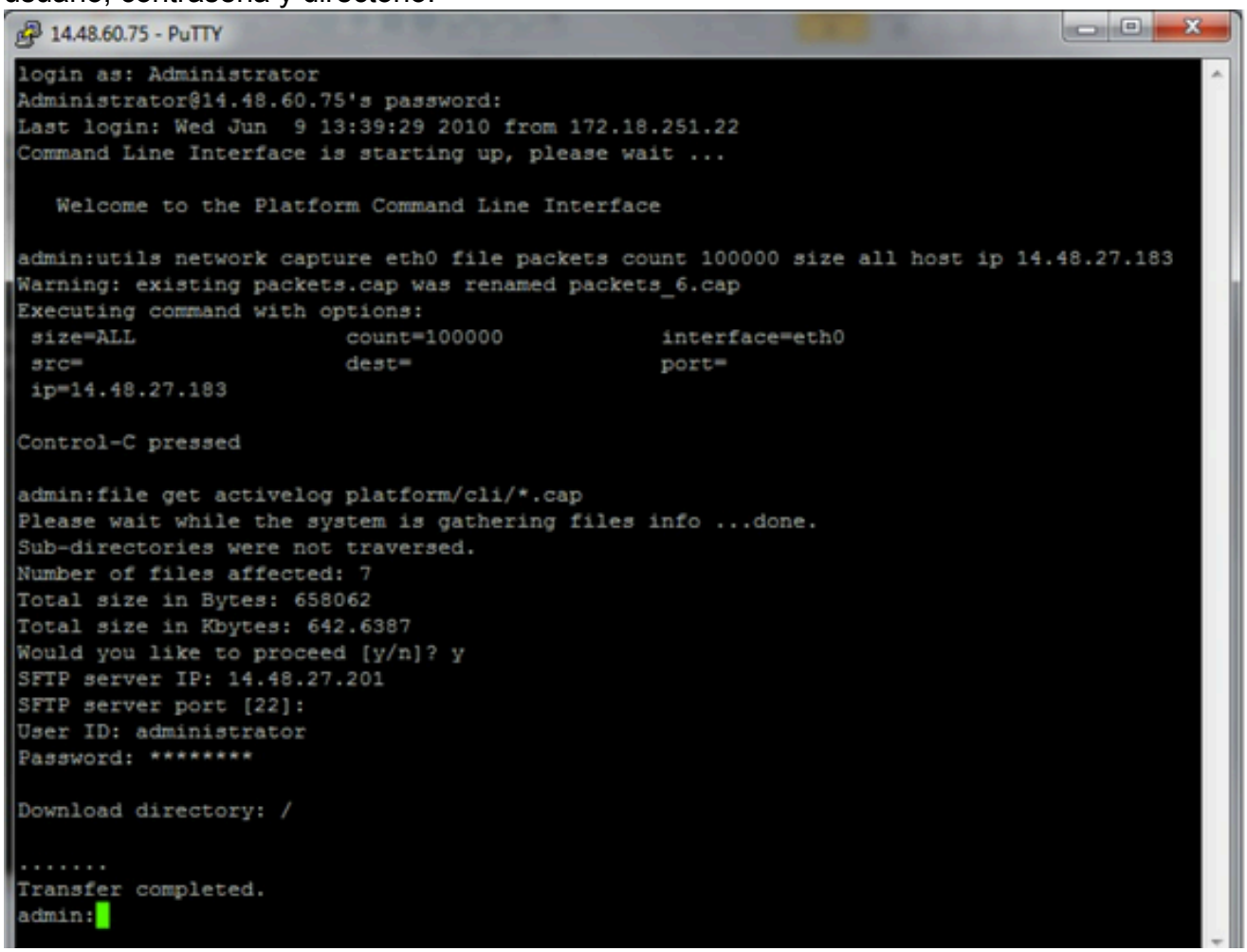
   Para detener la captura, mantenga presionada la tecla Control y presione C en el teclado. Esto hace que el proceso de captura finalice y no se agreguen paquetes nuevos al volcado de captura.

5. 

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

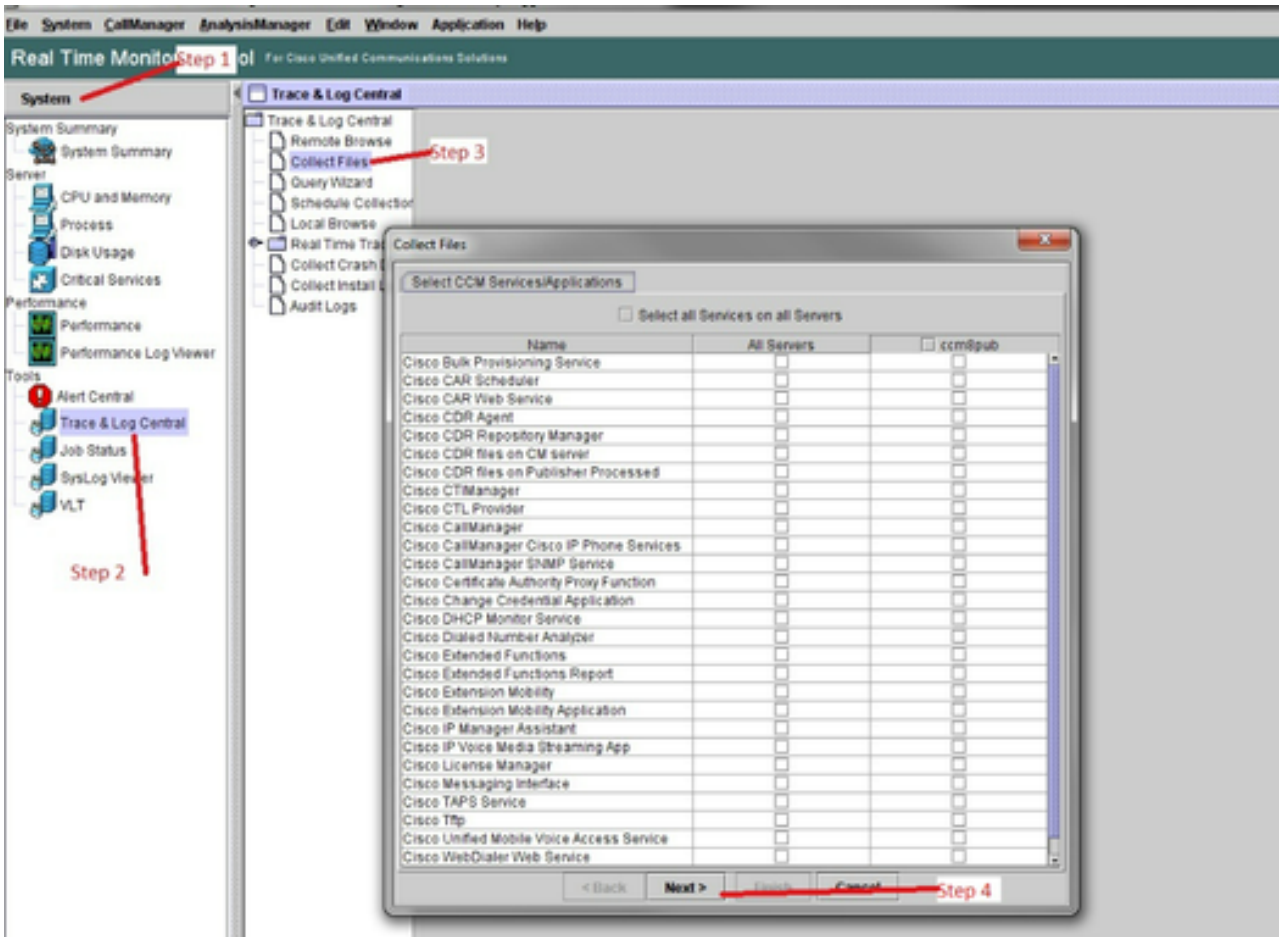
6. Recopile la captura del servidor
   Los archivos de captura se almacenan en la plataforma/cli/ de registro activo en el servidor. Puede transferir los archivos a través de CLI a un servidor SFTP o al equipo local con el RTMT.

   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:

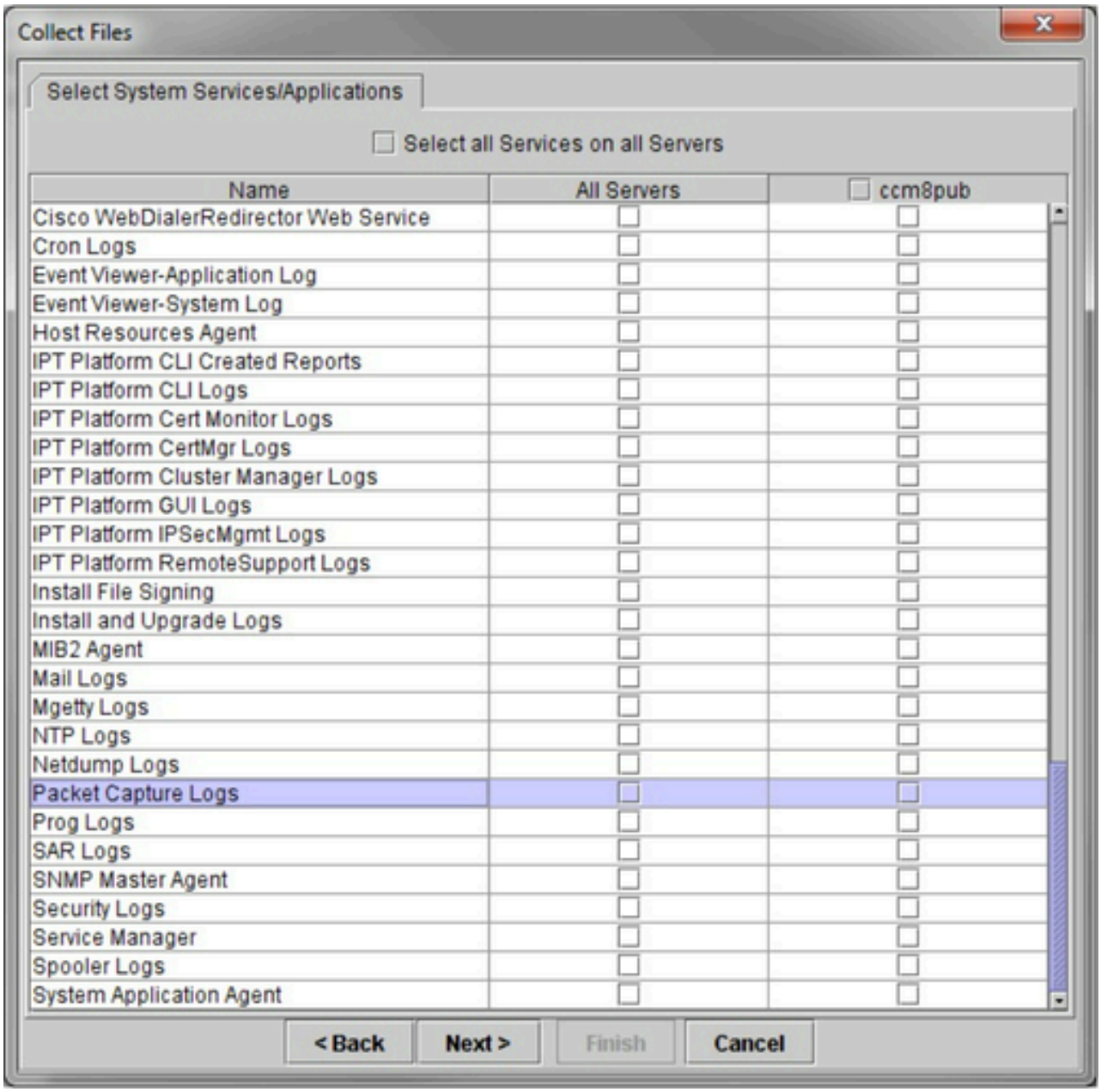


   La CLI indica que la transferencia de archivos al servidor SFTP se ha realizado correctamente o no.

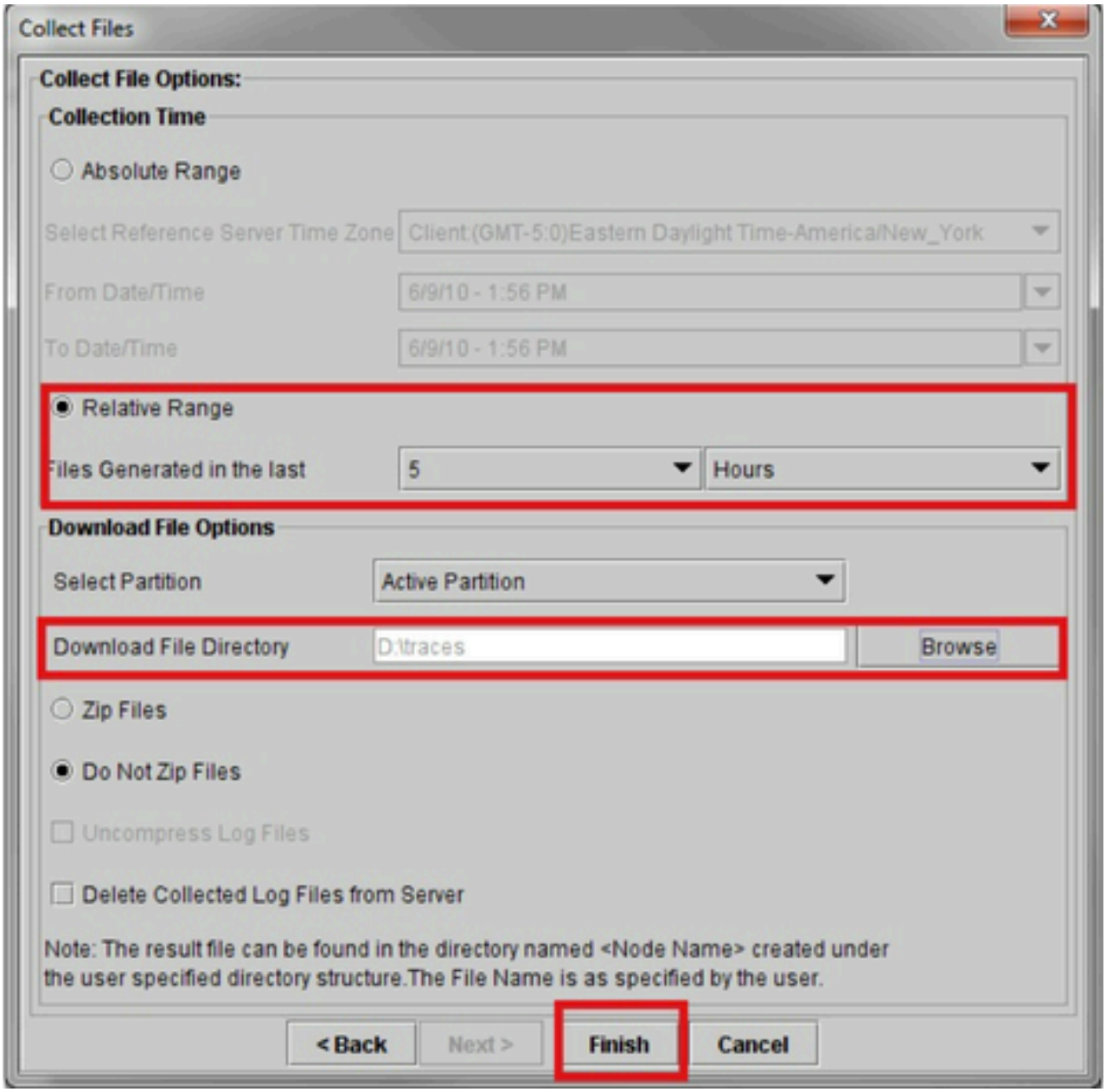
4 ter. Utilice RTMT para transferir un archivo de captura a un equipo local.
Inicie la RTMT. Si no está instalado en el equipo local, instale la versión adecuada desde la página de administración de VOS y luego navegue hasta el menú Applications > Plugins.
Haga clic en System, luego en Trace & Log Central, 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.



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



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).