

# Establecer y recopilar registros de seguimiento de UCCE

## Contenido

[Introducción](#)

[Requirements](#)

[Configuración de seguimiento y recopilación de registro](#)

[Finesse](#)

[Cisco Agent Desktop](#)

[Cisco Supervisor Desktop](#)

[Escritorios de Cliente CTIOS](#)

[Problemas relacionados con el cliente con seguimiento y registros en PG](#)

[Debug CAD Sync Service](#)

[Depurar el servidor RASCAL de CAD 6.0\(X\)](#)

[Debug Chat Server](#)

[Otros registros y seguimiento relacionados con PG](#)

[Habilitación del Seguimiento de PIM de CallManager](#)

[Habilitar seguimiento en CUCM](#)

[Gateway \(JGW\) Enable Java Telephony Application Programming Interface \(JTAPI\)](#)

[Habilitar el seguimiento del servidor CTI \(CTISVR\) en el lado activo](#)

[Habilitación del Seguimiento de PIM de VRU](#)

[Habilitación del Seguimiento del Servidor CTIOS en Ambos Servidores CTIOS](#)

[Habilitar el seguimiento de Open Peripheral Controller \(OPC\) en Active PG](#)

[Habilitar seguimiento de Eagtpim en PG activo](#)

[Utilizar la utilidad Dumplog para extraer registros](#)

[Habilitar seguimiento en servidores CVP](#)

[Seguimiento y recopilación de registros relacionados con el marcador de salida](#)

[Registros de extracción](#)

[En el importador](#)

[En el administrador de campañas](#)

[Activar registros del router en el proceso del router](#)

[Registro del router de extracción](#)

[Seguimiento de la puerta de enlace \(SIP\)](#)

[Seguimiento de CUSP](#)

[Uso de CLI para el Seguimiento](#)

[Ejemplo de CLI](#)

## Introducción

Este documento describe cómo configurar el seguimiento en Cisco Unified Contact Center Enterprise (UCCE) para clientes, servicios de gateway periférico (PG), el portal de voz del cliente (CVP) de Cisco, el Marcador de salida de Cisco UCCE, Cisco Unified Communications Manager (CallManager) (CUCM) y gateways de Cisco.

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Agent Desktop (CAD)
- Servidor de objetos de integración de telefonía y ordenador de Cisco (CTIOS)
- Cisco Finesse
- Portal de voz del cliente de Cisco (CVP)
- Cisco Unified Communications Manager (CallManager) (CUCM)
- Gateways de Cisco

## Configuración de seguimiento y recopilación de registro

### Notas:

Use la [Command Lookup Tool \(clientes registrados solamente\) para obtener más información sobre los comandos usados en esta sección.](#)

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando show.

Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

## Finesse

Inicie sesión en el servidor Finesse con Secure Shell (SSH) e introduzca estos comandos para recopilar los registros que necesita. Se le solicita que identifique un servidor FTP (SFTP) de SSH en el que se cargarán los registros.

### Registros

Instalar registros

Registros del escritorio

Registros del servicio

Registros de Tomcat de plataforma

Registros de instalación del sistema operativo de voz (VOS)

### Comando

`file get install desktop-install.log`

`archivo get activelog desktop recurs  
compress`

`archivo get activelog  
platform/log/servm*.* compress`

`archivo get activelog tomcat/logs recurs  
compress`

`file get install install.log`

## Cisco Agent Desktop

Este procedimiento describe cómo crear y recopilar archivos de depuración:

1. En el equipo agente, vaya al archivo C:\Program Files\Cisco\Desktop\Config directory and open the Agent.cfg.
2. Cambie el umbral de depuración de OFF a **DEBUG**. TRACE se puede utilizar para un nivel más profundo.

```
[Debug Log]
Path=..\log\agent.dbg
Size=3000000
Threshold=DEBUG
```

3. Asegúrese Size=300000 (seis ceros).
4. Guarde el archivo de configuración.
5. Detenga el programa del agente.
6. Elimine todos los archivos de C:\Program Files\Cisco\Desktop\log directory.
7. Inicie el programa de agentes y vuelva a crear el problema.
8. Estos archivos de depuración se crean y se colocan en C:\Program Files\Cisco\Desktop\log:

```
agent0001.dbgctiosclientlog.xxx.log
```

## Cisco Supervisor Desktop

Este procedimiento describe cómo crear y recopilar archivos de depuración:

1. En el equipo agente, vaya al archivo C:\Program Files\Cisco\Desktop\Config directory and open the supervisor.cfg.
2. Cambie el UMBRAL de depuración de OFF a **DEBUG**. TRACE se puede utilizar para un nivel más profundo.

```
[Debug Log]
Path=..\log\supervisor.dbg
Size=3000000
THRESHOLD=DEBUG
```

3. Asegúrese Size=300000 (seis ceros).
4. Guarde el archivo de configuración.
5. Detenga el programa del agente.

6. Elimine todos los archivos de C:\Program Files\Cisco\Desktop\log directory.
7. Inicie el programa de agentes y vuelva a crear el problema. Se crea un archivo de depuración denominado supervisor0001.dbg y se coloca en C:\Program Files\Cisco\Desktop\log.

## Escritorios de Cliente CTIOS

En el equipo cliente donde está instalado el cliente CTIOS, utilice Regedt32 para activar el seguimiento. Cambie esta configuración:

Versión	Ubicación del registro	Valor	Cambiar
Versiones anteriores a 7.x	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0x07	Aumente el valor a 0xffff.
Versión 7.x y posterior	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS Rastreo	0x4000307	Establezca el valor en 0xffff para la resolución de problemas.

El resultado predeterminado se crea y se coloca en un archivo de texto denominado CtiosClientLog en el directorio c:\Program Files\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\ install directory.

## Problemas relacionados con el cliente con seguimiento y registros en PG

### Debug CAD Sync Service

Estos son los ajustes para depurar el servicio CAD Sync:

Configuración	Valor
Archivo de configuración	DirAccessSynSvr.cfg
Ubicación predeterminada	C:\Program Files\Cisco\Desktop\config
Problemas generales	Threshold=DEBUG
Archivos de salida	DirAccessSynSvr.log

### Depurar el servidor RASCAL de CAD 6.0(X)

Estos son los ajustes para depurar el servidor RASCAL de CAD 6.0(X):

Configuración	Valor
Archivo de configuración	FCRasSvr.cfg
Ubicación predeterminada	C:\Program Files\Cisco\Desktop\config
Problemas generales	Intervalo = 1-4, 50, 3000-8000

Problemas relacionados con LDAP:	Intervalo = 4000-4999
Problemas relacionados con LRM:	Intervalo = 1999-2000
Problemas relacionados con la base de datos	Intervalo = 50-59
Archivos de salida	FCRasSvr.log, FCRasSvr.dbg
Ubicación predeterminada	C:\Program Files\Cisco\Desktop\log

## Debug Chat Server

Estos son los ajustes para depurar el servidor de chat:

Configuración	Valor
Archivo de configuración	FCCServer.cfg
Ubicación predeterminada	C:\Program Files\Cisco\Desktop\config
Problemas generales	Threshold=DEBUG
Archivos de salida	FCCServer.log, FCCServer.dbg
Ubicación predeterminada	C:\Program Files\Cisco\Desktop\log

## Otros registros y seguimiento relacionados con PG

Consulte [Uso de la utilidad Dumplog para extraer registros](#) para la recopilación de registros.

## Habilitación del Seguimiento de PIM de CallManager

Utilice la utilidad de supervisión de procesos (procmon) para activar y desactivar los niveles de seguimiento. Estos comandos activan el seguimiento del administrador de interfaz periférica (PIM) de CallManager:

```
C:\>procmon <Customer_Name> <PG_Name> <ProcessName>
>>>trace tp* !-- Turns on third party request tracing
>>>trace precall !-- Turns on precall event tracing
>>>trace *event !-- Turns on agent and call event tracing
>>>trace csta* !-- Turns on CSTA call event tracing
>>>ltrace !-- Output of all trace bits
>>>q !-- Quits
```

Este comando procmon desactiva el seguimiento de PIM de CallManager:

```
>>>trace * /off
```

## Habilitar seguimiento en CUCM

Este procedimiento describe cómo activar el seguimiento de CUCM:

1. Vaya a Call Manager Unified Serviceability.
2. Seleccione **Trace/Configuration**.
3. Seleccione **Servicios CM**.

4. Seleccione **CTIManager (Activo)**.
5. En la parte superior derecha, seleccione **SDL Configuration**.
6. Habilite todo excepto Desactivar impresión bonita de SDL Trace.
7. Deje el número de archivos y sus tamaños en los valores predeterminados.
8. En Real-Time Monitoring Tool (RTMT), recopile Cisco Call Manager y Cisco Computer Telephony Integration (CTI) Manager. Ambos tienen registros de interfaz de diagnóstico del sistema (SDI) y capa de distribución de señales (SDL).

## Gateway (JGW) Enable Java Telephony Application Programming Interface (JTAPI)

Estos comandos procmon activan el seguimiento JGW:

```
C:\procmon <Customer_Name> <node> process
>>>trace JT_TPREQUESTS !-- Turns on third-party request traces
>>>trace JT_JTAPI_EVENT_USED !-- Turns on traces for the JTAPI Events the PG uses
>>>trace JT_ROUTE_MESSAGE !-- Turns on routing client traces
>>>trace JT_LOW* !-- Traces based on the underlying JTAPI and CTI layers
```

Un comando de ejemplo es **procmon ipcc pg1a jgw1**.

## Habilitar el seguimiento del servidor CTI (CTISVR) en el lado activo

Este procedimiento describe cómo habilitar el seguimiento CTISVR en el lado activo:

1. Utilice el editor de registro para editar HKLM\software\Cisco Systems, Inc\icm\<cust\_inst>\CG1(a y b)\EMS\CurrentVersion\library\Processes\ctisvr.
2. Establezca EMSTraceMask = f8.

## Habilitación del Seguimiento de PIM de VRU

**Nota:** Los comandos distinguen entre mayúsculas y minúsculas. El PG de la unidad de respuesta de voz (VRU) es diferente del PG de Cisco CallManager (CCM).

Estos comandos procmon activan el seguimiento para el PIM VRU:

```
C:\procmon <Customer_Name> <PG_Name> <ProcessName>
procmon>>>trace *.* /off !-- Turns off
procmon>>>trace !-- Verifies what settings are on/off
procmon>>>trace cti* /onprocmon>>>trace opc* /on
procmon>>>trace *ecc* /onprocmon>>>trace *session* /off
procmon>>>trace *heartbeat* /off
procmon>>>ltrace /traceprocmon>>>quit
```

Este comando procmon desactiva el seguimiento de PIM de VRU:

```
>>>trace * /off
```

## Habilitación del Seguimiento del Servidor CTIOS en Ambos Servidores CTIOS

Este procedimiento describe cómo habilitar el seguimiento en ambos servidores CTIOS:

1. Tome nota de la máscara de seguimiento actual para su uso posterior.
2. Utilice el editor de registro para editar HLKM >> Software\Cisco Systems Inc.\ICM\- 3. Set:
  - EMSTraceMask = 0x60A0F
  - EMSTraceMask a uno de estos valores, dependiendo de la versión:
    - 0x0A0F para la versión 6.0 y anteriores
    - 0x20A0F para la versión 7.0 y 7.1(1)
    - 0x60A0F para la versión 7.1(2) y posteriores

La máscara de seguimiento predeterminada es 0x3 en todas las versiones excepto en la versión 7.0(0), donde es 0x20003.

Si la máscara de seguimiento tiene un valor alto (0xf o superior), hay un gran impacto en el rendimiento del servidor CTIOS y en la tasa de finalización de llamadas. Establezca la máscara de seguimiento en un valor alto sólo cuando esté depurando un problema; una vez que haya recopilado los registros necesarios, debe volver a establecer la máscara de seguimiento en su valor predeterminado.

Para solucionar problemas, configure la máscara de seguimiento del servidor CTIOS en:

- 0x0A0F para la versión 6.0 y anteriores
- 0x20A0F para la versión 7.0 y 7.1(1)
- 0x60A0F para la versión 7.1(2) y posteriores

## Habilitar el seguimiento de Open Peripheral Controller (OPC) en Active PG

Estos comandos opctest activan el seguimiento OPC en un PG activo:

```
opctest /cust <cust_inst> /node <node>  
opctest:debug /agent /routing /cstacer /tpmsg /closedcalls
```

Este es un ejemplo de un entorno de laboratorio:

```
C:\Documents and Settings\ICMAdministrator>opctest /cust ccl /node pgl  
OPCTEST Release 8.0.3.0 , Build 27188  
opctest: debug /agent /routing /cstacer /tpmsg /closedcalls !-- Use debug /on in  
order to restore default tracing levels  
opctest: quit
```

Otros ejemplos son:

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg
!-- General example
```

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /NCT
!-- Network transfer example
```

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /task /passthru
!-- Multimedia example
```

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /passthru
!-- VRU PG example
```

## Habilitar seguimiento de Eagtpim en PG activo

Estos comandos procmon activan el seguimiento de eagtpim en un PG activo:

```
C:\>procmon <cust_inst> <node> pim<pim instance
>>>trace tp* /on
>>>trace precall /on
>>>trace *event /on
>>>trace csta* /on
```

Este es un ejemplo de un entorno de laboratorio:

```
C:\Documents and Settings\ICAdministrator>procmon ccl pgl a pim1
>>>trace tp* /on
>>>trace precall /on
>>>trace *event /on
>>>trace csta* /on
>>>quit
```

## Utilizar la utilidad Dumplog para extraer registros

Refiérase a [Cómo Utilizar la Utilidad Dumplog](#) para obtener detalles adicionales. Utilice el comando **cdlog** para llegar al directorio logfiles, como se muestra en este ejemplo:

```
c:\cdlog <customer_name> pgl a !-- Or, pgXa to depending on the PG number (X)
c:\icm\<customer_name>\<<PG#>>\logfiles\
```

Estos ejemplos muestran cómo colocar el resultado en el archivo predeterminado; en todos los casos, puede utilizar **/de** para definir un nombre específico para el archivo de salida:

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog pim1 /bt <HH:MM> /et <HH:MM> /ms /o
!-- This PIM example places output in a default pim1.txt file
```

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog opc /bt <HH:MM> /et <HH:MM> /ms /o
!-- This OPC example places output in a default opc.txt file
```

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog jgw1 /bt <HH:MM> /et <HH:MM> /ms /o
c:\cdlog <customer_name> cgl a
c:\icm\<customer_name>\<cg#>\logfiles\
!-- This JTAPI example places output in a default jgw1.txt file
```

```
c:\icm\\cg#\logfiles\dumplog ctisvr /bt <HH:MM> /et <HH:MM> /ms /o
!-- This CTI server example places output in a default ctisvr.txt file
```

```
c:\ icm\\ctios\logfiles\dumplog ctios /bt <HH:MM> /et <HH:MM> /ms /o
!-- This CTIOS server example places output in a default ctios.txt file
```

## Habilitar seguimiento en servidores CVP

### SIP

Este procedimiento describe cómo habilitar el seguimiento en servidores CVP con el software del teléfono IP SIP de Cisco:

1. En los servidores de llamadas, vaya a la herramienta de diagnóstico CVP ([http://localhost\(CallServer\):8000/cvp/diag](http://localhost(CallServer):8000/cvp/diag)) para obtener la pila del protocolo de inicio de sesión (SIP).
2. Agregue com.dinamicsoft.Dslibs.DsUAlibs con debug.
3. Haga clic en **Establecer**.
4. Haga clic en **DEBUG/41**.

### H323

Este procedimiento describe cómo habilitar el seguimiento en servidores CVP con una gateway H323:

1. En los servidores de llamadas, inicie sesión en VBAAdmin.
2. Habilite estos seguimientos para el CVP Voice Browser:

```
setcalltrace on
setinterfacetrace on
```

### Extraer registros de CVP de servidores de llamadas

Recopile el archivo CVP \*.log y los archivos Error.log durante el período de prueba. Estos archivos se encuentran en el directorio C:\Cisco\CVP\logs directory on both CVP servers.

Estas son las ubicaciones de los archivos de registro de Unified CVP, donde CVP\_HOME es el directorio en el que está instalado el software Unified CVP.

#### Tipo de registros

Registros de servidor de llamadas o de servidor de informes  
Registros de la consola de operaciones  
Registros de servidor XML de voz (VXML)  
Registros de agentes del protocolo simple de administración de red (SNMP)  
Registros del administrador de recursos de Unified CVP

#### Ubicación

CVP\_HOME\logs\  
CVP\_HOME\logs\OAMP\  
CVP\_HOME\logs\VXML\  
CVP\_HOME\logs\SNMP\  
CVP\_HOME\logs\ORM\

Una ubicación de ejemplo es C:\Cisco\CVP.

## Registros del servidor VXML

Para aplicaciones XML de voz personalizadas como una aplicación audium implementada, puede activar un registrador de depuración.

Agregue esta línea a la sección <loggers> (la última sección) del archivo de configuración settings.xml en el directorio C:\Cisco\CVP\VXMLServer\applications\APP\_NAME\data\application\directory:

```
<logger_instance name="MyDebugLogger"  
class="com.audium.logger.application.debug.ApplicationDebugLogger"/>
```

En tiempo de ejecución, este registrador envía un registro VoiceXML detallado a \Cisco\CVP\VXMLServer\applications\APP\_NAME\MyDebugLogger directory.

**Nota:** Puede cambiar el nombre del registrador en el archivo de configuración settings.xml desde MyDebugLogger por cualquier nombre que elija.

## Seguimiento y recopilación de registros relacionados con el marcador de salida

Este procedimiento describe cómo aumentar los registros del proceso de badialer en el Marcador de salida (que normalmente se encuentra en un PG).

1. Asegúrese de que EMSDisplaytoScreen = 0.
2. Utilice el editor de registro para editar HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer.
3. Set:
  - Máscara de raza EMST = 0xff
  - EMSUserData = ff (cuatro f en modo binario)
4. Utilice el editor de registro para editar HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer.
5. Establecer DebugDumpAllEvents = 1.

## Registros de extracción

Ejecute la utilidad dumplog desde el directorio /icm/<instance>/dialer/logfiles:

```
dumplog badialer /bt hh:mm:ss /et hh:mm:ss /o
```

## En el importador

Este procedimiento describe cómo aumentar el registro del proceso baimport.

1. Utilice el editor de registro para editar HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Logger\EMS\CurrentVersion\Library\Processes\baimport.
2. Set:
  - Máscara de raza EMST = 0xff
  - EMSUserData = ff (cuatro f en modo binario)
3. Ejecute la utilidad dumplog desde el directorio /icm/<instance>/la/logfiles:

```
dumplog baimport /bt hh:mm:ss /et hh:mm:ss /o
```

## En el administrador de campañas

Este procedimiento describe cómo aumentar el registro del proceso del administrador de campañas.

1. Utilice el editor de registro para editar HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Logger\EMS\CurrentVersion\Library\Processes\CampaignManager.
2. Set:
  - Máscara de raza EMST = 0xff
  - EMSUserData = ff (cuatro f en modo binario)
3. Ejecute la utilidad dumplog desde el directorio /icm/<instance>/la/logfiles:

```
dumplog campaignmanager /bt hh:mm:ss /et hh:mm:ss /o
```

En el PG de Avaya Communications Manager (ACD), utilice la utilidad **opctest** para aumentar lo siguiente tanto para CallManager como para Avaya.

```
C:\opctest /cust <instance> /node <pgname>  
opctest: type debug /agent /closedcalls /cstacer /routing  
opctest: q !-- Quits
```

Este procedimiento describe cómo aumentar el seguimiento para el proceso ctisvr.

1. Utilice el editor de registro para editar HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr.
2. Establezca EMSTraceMask = f8. Puede dejar el valor en f0 si lo desea.

## Activar registros del router en el proceso del router

Este procedimiento describe cómo habilitar los registros del router:

1. En el router, navegue hasta **Inicio > Ejecutar** e ingrese **rtrtrace**.
2. Escriba el nombre del cliente.
3. Haga clic en **Connect (Conectar)**
4. Seleccione estas opciones:

cambios de agentessolicitudes de  
routerscriptselectnetworkvruseguimientotranslationroutecallqueuingcalltyperealttime

5. Haga clic en **Apply (Aplicar)**.
6. Salga de la utilidad.

Para opctest Release 8.5, use el Diagnostic Framework Portico en su lugar.

```
debug level 3 component "icm:Router A" subcomponent icm:rtr
```

## Registro del router de extracción

Utilice la utilidad dumplog para extraer los registros del router de cualquier router durante el período de tiempo de las pruebas. Refiérase a [Cómo Utilizar la Utilidad Dumplog](#) para obtener detalles adicionales.

Este es un ejemplo de una solicitud de registro para los registros del 21/10/2011 entre las 09:00:00 y las 09:30:00 (en formato de hora de 24 horas). Esta salida va al archivo C:/router\_output.txt:

```
C:\Documents and Settings\ICMAdministrator>cdlog u7x ra  
C:\icm\u7x\ra\logfiles>dumplog rtr /bd 10/21/2011 /bt 09:00:00 /ed 10/21/2011  
/et 09:30:00 /ms /of C:/router_output.txt
```

Envíe el archivo de resultados (C:/router\_output.txt) a Cisco para la resolución de problemas si es necesario.

## Seguimiento de la puerta de enlace (SIP)

Estos comandos activan el seguimiento en servidores CVP con SIP:

```
#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
```

**Nota:** Cualquier cambio en un GW de software Cisco IOS® de producción podría provocar una interrupción.

Se trata de una plataforma muy robusta que puede manejar las depuraciones sugeridas en el volumen de llamadas proporcionado sin problemas. Sin embargo, Cisco recomienda que:

- Enviar todos los registros a un servidor syslog en lugar de a la memoria intermedia de registro:

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

- Aplique los comandos debug de uno en uno y verifique la utilización de la CPU después de cada uno:

```
show proc cpu hist
```

**Nota:** Si la CPU obtiene 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 debugs adicionales si el GW alcanza el 60%.

Habilitar estos debugs:

```
debug isdn q931
debug voip ccapi inout
debug ccsip mess
debug http client all
debug voip application vxml all
debug vtsp all
debug voip application all
```

Después de realizar la llamada y simular el problema, detenga la depuración:

```
#undebug all
```

Recopile este resultado:

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

## Seguimiento de CUSP

Estos comandos activan el seguimiento SIP en el proxy SIP de Cisco Unified (CUSP):

```
(cusp)> config
(cusp-config)> sip logging
(cusp)> trace enable
```

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

Recuerde desactivar la sesión cuando haya terminado.

Este procedimiento describe cómo recopilar los registros:

1. Configure un usuario en el CUSP (por ejemplo, prueba).
2. Agregue esta configuración en el mensaje 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 definidos en el paso anterior.
4. Cambie los directorios a /cusp/log/trace.
5. Obtenga el log\_<filename>.

## Uso de CLI para el Seguimiento

En UCCE versión 8 y posteriores, puede utilizar la interfaz de línea de comandos (CLI) de Unified System para recopilar seguimientos. En comparación con las utilidades dumplog, la CLI es un método muy rápido y eficiente para obtener un conjunto completo de registros de un servidor como un PG o Rogger.

Este procedimiento describe cómo iniciar el análisis de problemas y cómo determinar qué seguimiento habilitar. El ejemplo recopila registros de estos servidores:

- ROUTER-A/ROUTER-B
- LOGGER-A/LOGGER-B
- PGXA/PGXB
- Todos los servidores de llamadas CVP
- Todos los CVP VXML/Media Servers (si están presentes)

1. En cada sistema de la lista, abra la CLI de Unified System en cada servidor y ejecute este comando:

```
show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect  
dir c:\temp
```

Reemplace la primera cadena *mm-dd-yyyy:hh:mm* por una fecha y hora aproximadamente 15 minutos antes del evento.

Reemplace la segunda cadena *mm-dd-yyyy:hh:mm* por una fecha y hora que es aproximadamente 15 minutos después de que se resuelva el evento. Si el evento continúa, reúna al menos 15 minutos. Esto produce un archivo llamado clioutputX.zip, donde X es el siguiente número en secuencia.

2. Exporte los registros de aplicación/seguridad/sistema de Windows de cada sistema en formato de valores separados por comas (CSV) y guárdelos en el directorio C:\Temp directory.

3. Agregue los registros CSV de Windows al zip desde el paso 1 y cambie el nombre del archivo zip con este formato:

<SERVERNAME>-SystCLILogs-EventOn-YYYYMMDD\_HMMSS.zip

4. En cualquier PG de agente, recopile los registros en el directorio C:\Program Files\Cisco\Desktop\logs every time the failure is seen. Introduzca los registros en un archivo con un nombre en este formato:

<SERVERNAME>-CADLogs-EventOn-YYYYMMDD\_HMMSS.zip

Si utiliza CAD-Browser Edition (CAD-BE) o cualquier producto web de CAD, recopile los registros de C:\Program Files\Cisco\Desktop\Tomcat\logs directory y agréguelos al mismo archivo zip.

Si se está ejecutando en alguno de los productos de Windows 2008 x64, el directorio de registro se encuentra en C:\Program Files (x86)\Cisco\Desktop\...

5. Adjunte estos archivos a la solicitud de servicio o cargue los archivos en FTP si son demasiado grandes para enviarlos por correo electrónico o adjuntarlos.

Recopile esta información adicional si es posible:

- La hora de inicio y parada del evento.
- Varios ejemplos de ANI/DNIS/AgentID involucrados en el evento. Como mínimo, Cisco necesita al menos uno de estos para ver el evento.
- RouteCallDetail (RCD) y TerminationCallDetail (TCD) para el período de tiempo que rodea el evento. La consulta RCD es:

```
SELECCIONE * DE Route_Call_Detail WHERE DbDateTime > 'AAAA-MM-DD
```

```
HH:MM:SS.MMM' y DbDateTime < 'AAAA-MM-DD HH:MM:SS.MMM'
```

La consulta TCD es:

```
SELECCIONE * FROM Termination_Call_Detail WHERE DbDateTime > 'AAAA-MM-DD
```

```
HH:MM:SS.MMM' y DbDateTime < 'AAAA-MM-DD HH:MM:SS.MMM'
```

## Ejemplo de CLI

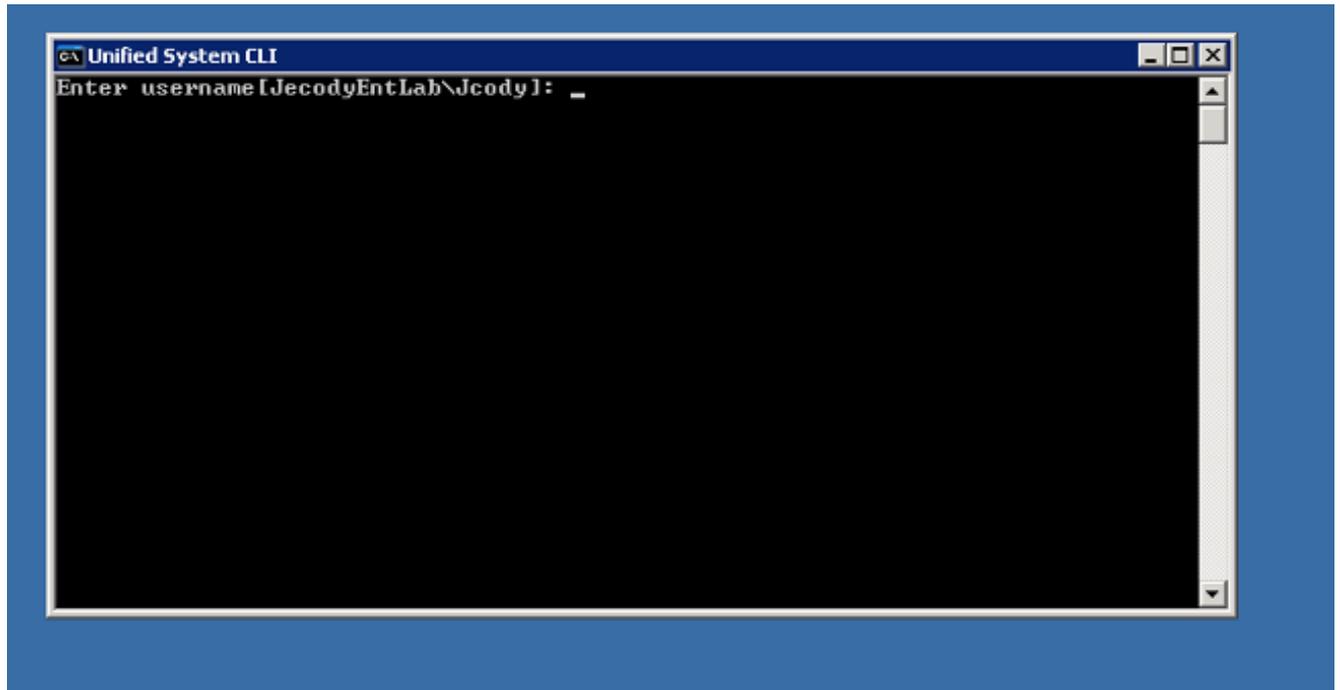
**Nota:** Se le advierte de que estas acciones pueden afectar al sistema, por lo que es posible que desee realizar este trabajo durante horas de inactividad o durante un tiempo lento.

Hay dos herramientas: una herramienta Diagnostic Framework y la herramienta CLI del sistema. Ambos son iconos en el escritorio o en el directorio Programs de cada servidor.

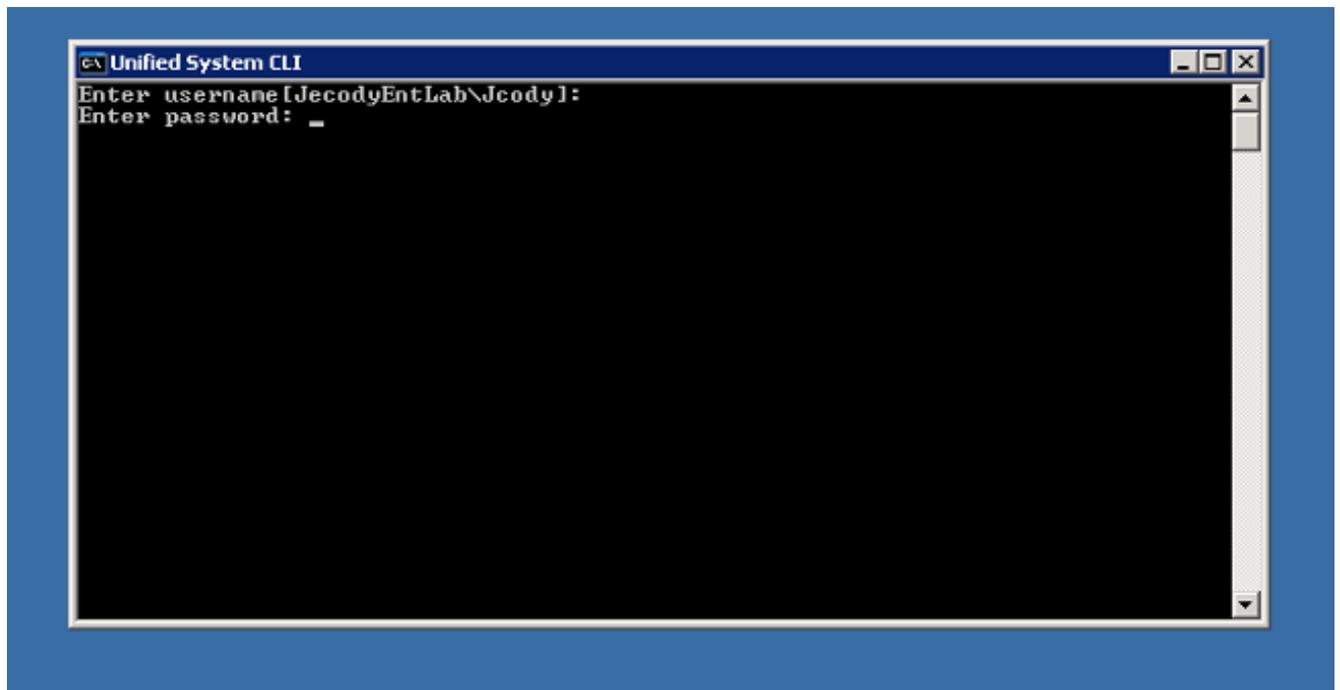
Este procedimiento describe cómo utilizar la CLI de Unified System para el seguimiento.

1. Haga clic en el icono de la CLI de Unified System y, a continuación, inicie sesión con el

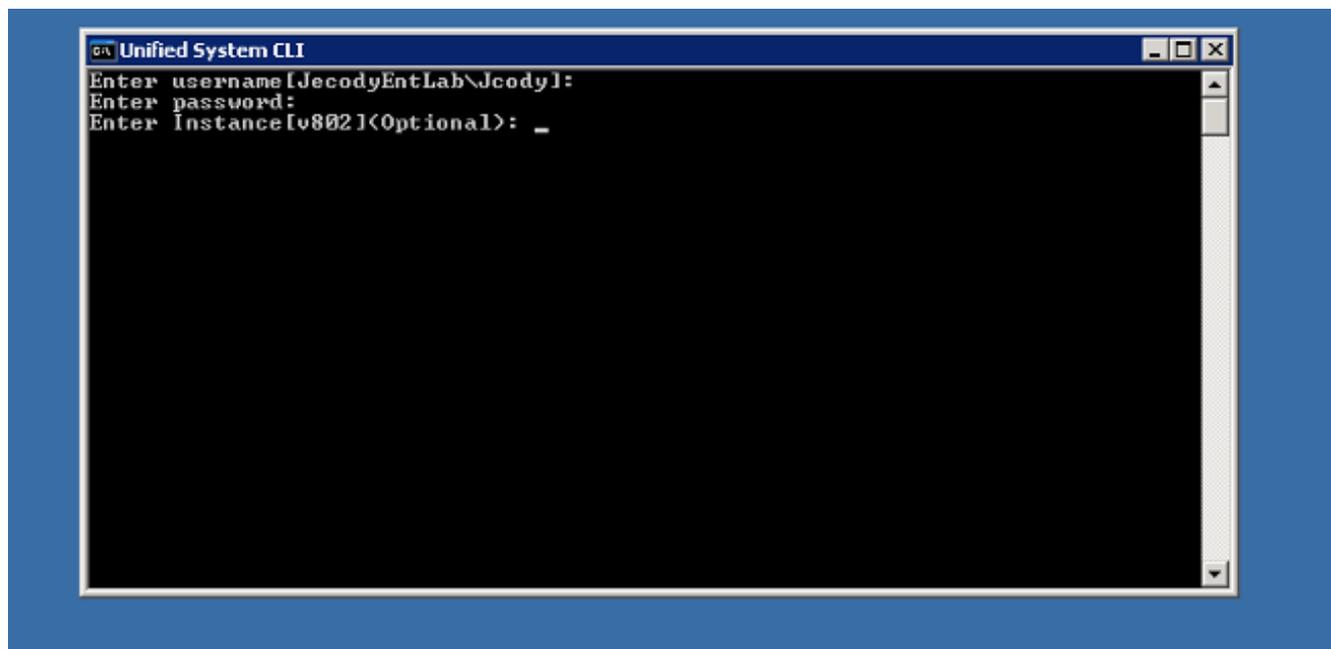
dominio y el nombre de usuario. (En este ejemplo, el administrador de dominio ha iniciado sesión anteriormente, por lo que la CLI ya conoce el dominio (JecodyEntLab) y el nombre de usuario (Jcody)).



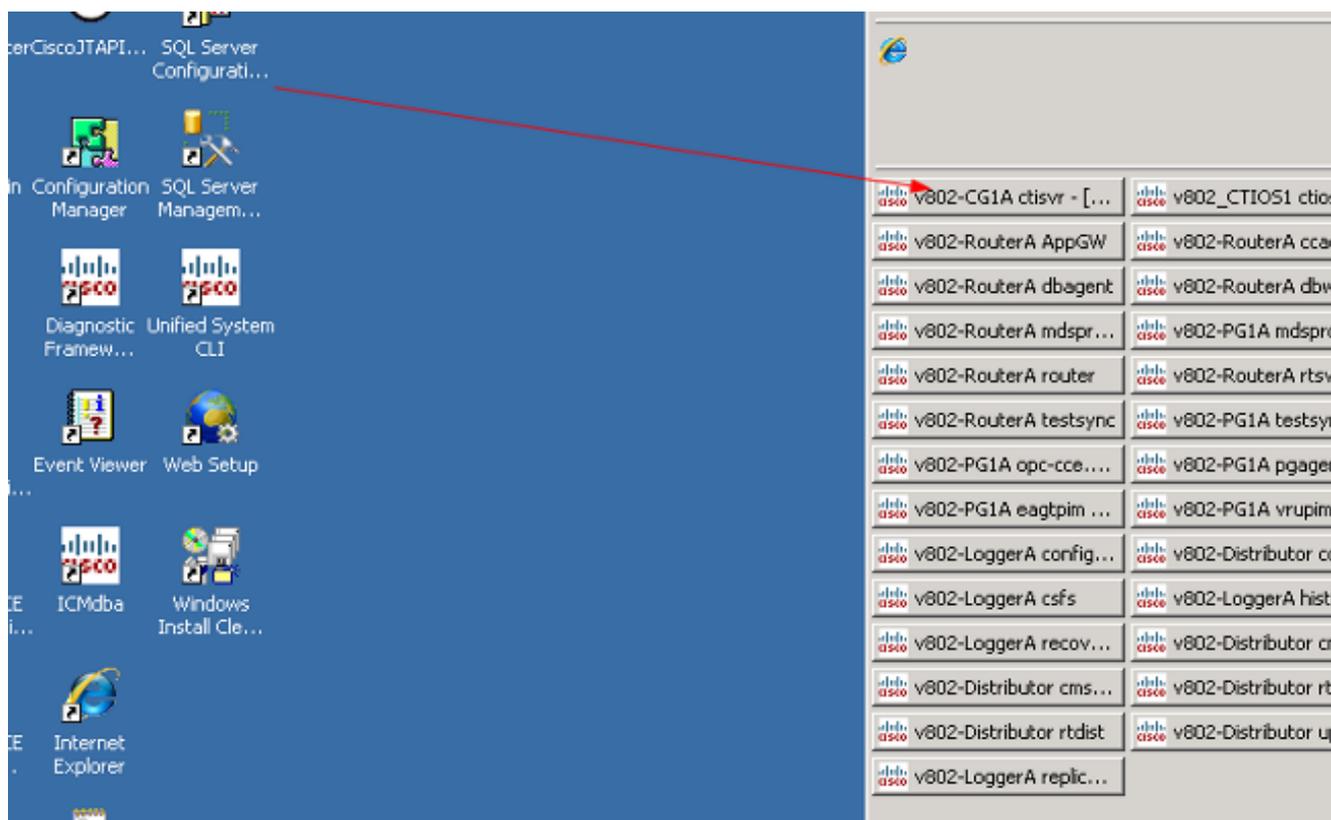
2. Ingrese la contraseña.



3. Introduzca el nombre de la instancia; en este ejemplo, es v802. Observe el PG en uno de los servicios; el nombre de la instancia es la primera parte del nombre del servicio.



4. Una forma sencilla de encontrar el nombre de la instancia es ver los servicios que se ejecutan en el servidor.



5. Una vez que vea el mensaje de bienvenida, ingrese este comando:

```
show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect dir c:\temp
```

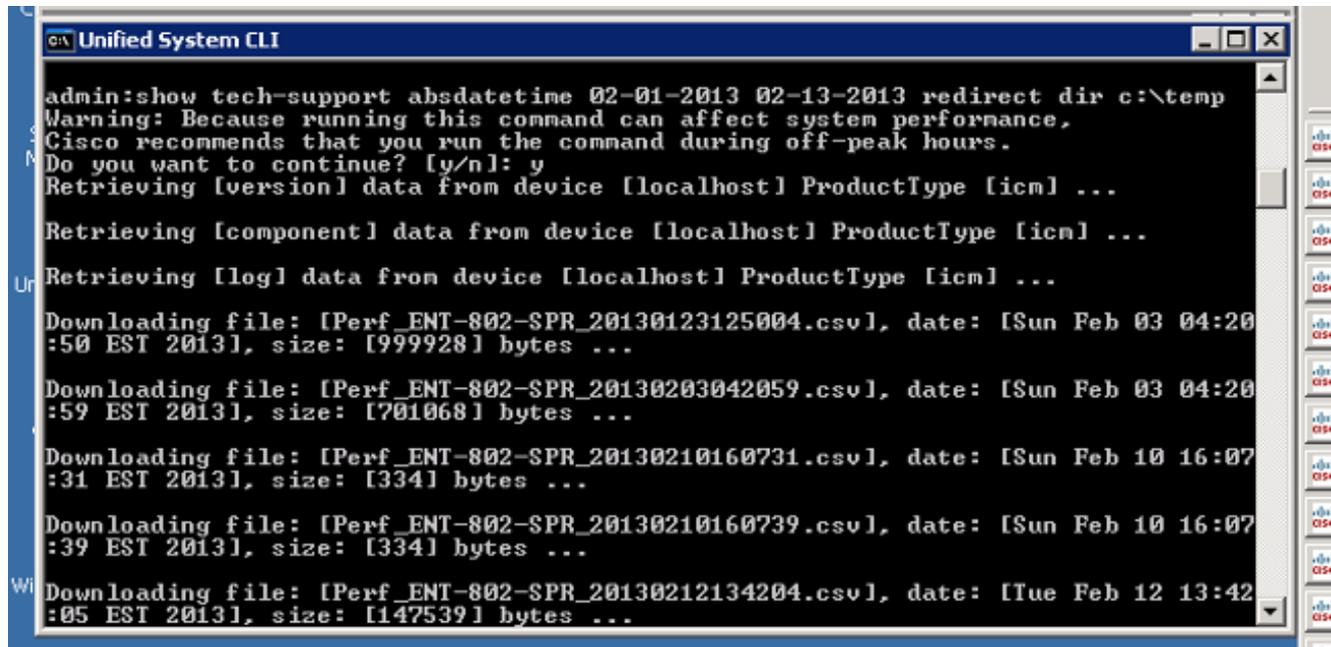
Reemplace la primera cadena *mm-dd-yyyy:hh:mm* por una fecha y hora aproximadamente 15 minutos antes del evento.

Reemplace la segunda cadena *mm-dd-yyyy:hh:mm* por una fecha y hora que es

aproximadamente 15 minutos después de que se resuelva el evento.

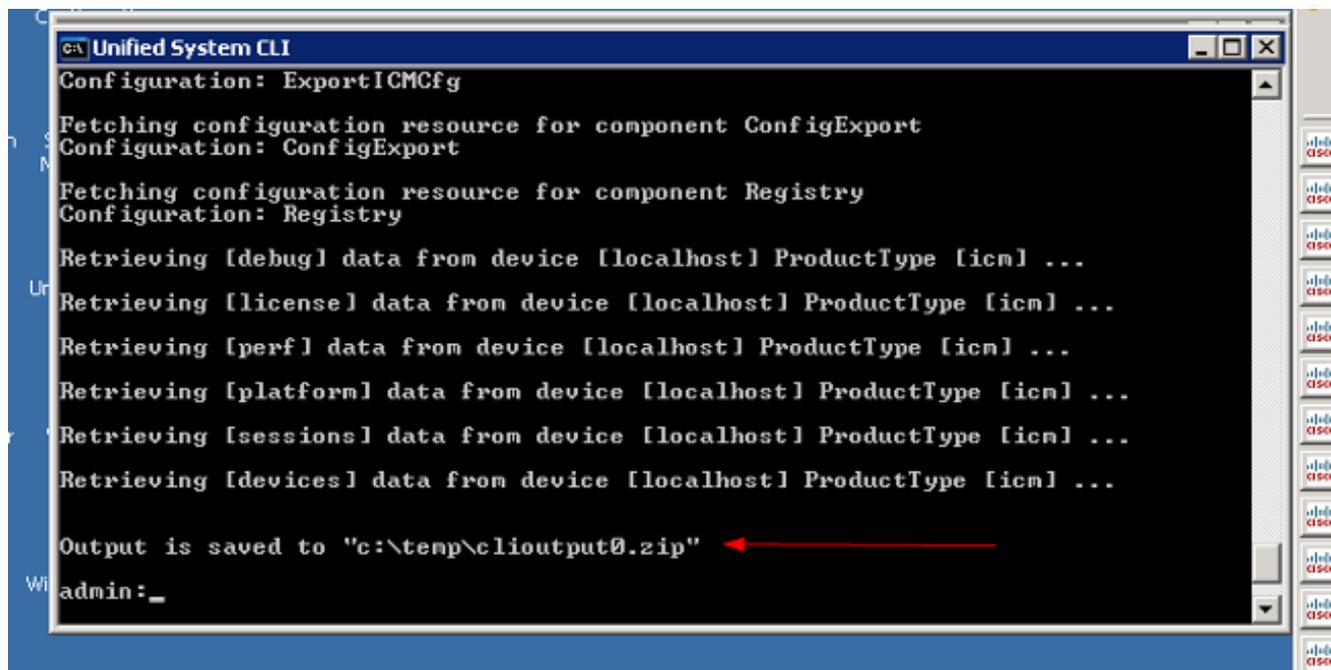
Si el evento continúa, reúna al menos 15 minutos.

Esto produce un archivo llamado *clioutputX.zip*, donde *X* es el siguiente número en secuencia.



```
admin:show tech-support absdatetime 02-01-2013 02-13-2013 redirect dir c:\temp
Warning: Because running this command can affect system performance,
Cisco recommends that you run the command during off-peak hours.
Do you want to continue? [y/n]: y
Retrieving [version] data from device [localhost] ProductType [icm] ...
Retrieving [component] data from device [localhost] ProductType [icm] ...
Retrieving [log] data from device [localhost] ProductType [icm] ...
Downloading file: [Perf_ENT-802-SPR_20130123125004.csv], date: [Sun Feb 03 04:20
:50 EST 2013], size: [999928] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130203042059.csv], date: [Sun Feb 03 04:20
:59 EST 2013], size: [701068] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130210160731.csv], date: [Sun Feb 10 16:07
:31 EST 2013], size: [334] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130210160739.csv], date: [Sun Feb 10 16:07
:39 EST 2013], size: [334] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130212134204.csv], date: [Tue Feb 12 13:42
:05 EST 2013], size: [147539] bytes ...
```

6. Una vez que se complete el proceso, busque el archivo *clioutputX.zip* en el directorio:



```
Configuration: ExportICMCFG
Fetching configuration resource for component ConfigExport
Configuration: ConfigExport
Fetching configuration resource for component Registry
Configuration: Registry
Retrieving [debug] data from device [localhost] ProductType [icm] ...
Retrieving [license] data from device [localhost] ProductType [icm] ...
Retrieving [perf] data from device [localhost] ProductType [icm] ...
Retrieving [platform] data from device [localhost] ProductType [icm] ...
Retrieving [sessions] data from device [localhost] ProductType [icm] ...
Retrieving [devices] data from device [localhost] ProductType [icm] ...
Output is saved to "c:\temp\clioutput0.zip"
admin:_
```

**Nota:** Este archivo suele ser muy grande porque contiene todos los archivos relacionados con UCCE para todos los servicios de este servidor.

7. Si sólo necesita un registro, puede que le resulte más fácil utilizar la utilidad *dumplog* antigua o utilizar el Portico de Marco de Diagnóstico:

Unified ICM-CCE-CCH Diagnostic Framework Portico

Hostname: ENT-802-SPR.JecodyEntLab.com Address: 14.10.150.108

**Commands:**

- Alarm**
  - SetAlarms
  - GetAlarms
- Configuration**
  - ListConfigurationCategories
  - GetConfigurationCategories
- Inventory**
  - ListAppServers
- License**
  - GetProductLicense
- Log**
  - ListLogComponents
  - ListLogFiles
- Network**
  - GetNetStat
  - GetPConfig
  - GetTraceRoute
  - GetPing
- Performance**
  - GetPerformanceSummary

**ListTraceFiles**

**Component:** CTI Server 1A/clisvr

**FromDate:** MM/DD/YYYY 5 / 7 / 2013 HH:MM:SS 12 : 0 : 0 AM

**ToDate:** MM/DD/YYYY 5 / 7 / 2013 HH:MM:SS 9 : 17 : 13 AM

Show URL

Submit

Trusted sites 100%