

# Définir et collecter les journaux de suivi UCCE

## Contenu

[Introduction](#)

[Conditions requises](#)

[Paramètres de suivi et collection de journaux](#)

[Finesse](#)

[Cisco Agent Desktop](#)

[Cisco Supervisor Desktop](#)

[Ordinateurs de bureau client CTIOS](#)

[Problèmes liés aux clients avec le suivi et les connexions sur PG](#)

[Debug CAD Sync Service](#)

[Déboguer le serveur RASCAL CAD 6.0\(X\)](#)

[Déboguer le serveur de conversation](#)

[Autres journaux et traçage liés aux PG](#)

[Activer le suivi de CallManager PIM](#)

[Activer le suivi sur CUCM](#)

[Activer la passerelle JTAPI \(Java Telephony Application Programming Interface\) \(JGW\)](#)

[Activer le suivi du serveur CTI \(CTISVR\) côté actif](#)

[Activer le suivi de VRU PIM](#)

[Activer le suivi du serveur CTIOS sur les deux serveurs CTIOS](#)

[Activer le suivi OPC \(Open Peripheral Controller\) sur Active PG](#)

[Activer le suivi Eagtpim sur le groupe de compétences actif](#)

[Utiliser l'utilitaire Dumplog pour extraire les journaux](#)

[Activer le suivi sur les serveurs CVP](#)

[Suivi et collecte de journaux liés au numéroteur sortant](#)

[Journaux d'extraction](#)

[Sur l'importateur](#)

[Sur le gestionnaire de campagnes](#)

[Activer les connexions du routeur sur le processus du routeur](#)

[Récupérer les journaux du routeur](#)

[Traces de passerelle \(SIP\)](#)

[Suivi CUSP](#)

[Utilisation de l'interface de ligne de commande pour le suivi](#)

[Exemple CLI](#)

## Introduction

Ce document décrit comment définir le suivi dans Cisco Unified Contact Center Enterprise (UCCE) pour les clients, les services de passerelle périphérique (PG), Cisco Customer Voice

Portal (CVP), Cisco UCCE Outbound Dialer, Cisco Unified Communications Manager (CallManager) (CUCM) et les passerelles Cisco.

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Agent Desktop (CAD)
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco Unified Communications Manager (CallManager) (CUCM)
- Passerelles Cisco

## Paramètres de suivi et collection de journaux

### Remarques :

Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\) pour obtenir plus d'informations sur les commandes utilisées dans cette section.](#)

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

## Finesse

Connectez-vous au serveur Finesse avec Secure Shell (SSH) et entrez ces commandes afin de collecter les journaux dont vous avez besoin. Vous êtes invité à identifier un serveur FTP SSH (SFTP) sur lequel les journaux seront téléchargés.

### Journaux

Journaux d'installation

Journaux de bureau

Journaux de service

Journaux Tomcat de la plate-forme

Journaux d'installation du système d'exploitation vocal (VOS)

### Commande

fichier get install desktop-install.log

fichier get activelog desktop recess

fichier get activelog platform/log/servm\*.\*  
compacter

fichier get activelog tomcat/logs recess

fichier get install install.log

## Cisco Agent Desktop

Cette procédure décrit comment créer et collecter des fichiers de débogage :

1. Sur l'ordinateur de l'agent, accédez au fichier C:\Program Files\Cisco\Desktop\Config directory and open the Agent.cfg.
2. Modifiez le seuil de débogage de OFF en **DEBUG**. TRACE peut être utilisé pour un niveau plus profond.

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

3. Assurez-vous que Size=300000 (six zéros).
4. Enregistrez le fichier de configuration.
5. Arrêtez le programme de l'agent.
6. Supprimez tous les fichiers dans le répertoire C:\Program Files\Cisco\Desktop\log directory.
7. Démarrez le programme de l'agent et recréez le problème.
8. Ces fichiers de débogage sont créés et placés dans C:\Program Files\Cisco\Desktop\log:

agent0001.dbgctiosclientlog.xxx.log

## Cisco Supervisor Desktop

Cette procédure décrit comment créer et collecter des fichiers de débogage :

1. Sur l'ordinateur de l'agent, accédez au fichier C:\Program Files\Cisco\Desktop\Config directory and open the supervisor.cfg.
2. Modifiez le SEUIL de débogage de OFF à **DEBUG**. TRACE peut être utilisé pour un niveau plus profond.

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

3. Assurez-vous que Size=300000 (six zéros).
4. Enregistrez le fichier de configuration.
5. Arrêtez le programme de l'agent.
6. Supprimez tous les fichiers dans le répertoire C:\Program Files\Cisco\Desktop\log directory.

7. Démarrez le programme de l'agent et recréez le problème. Un fichier de débogage nommé supervisor0001.dbg est créé et placé dans C:\Program Files\Cisco\Desktop\log.

## Ordinateurs de bureau client CTIOS

Sur le PC client sur lequel le client CTIOS est installé, utilisez Regedt32 afin d'activer le suivi. Modifiez ces paramètres :

Libérer	Emplacement du registre	Valeur par défaut	Modifier
Versions antérieures à 7.x	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0x07	Augmentez la valeur à 0xfff.
Version 7.x et ultérieure	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Suivi CTIOS	0x40000307	Définissez la valeur 0xfff pour le dépannage.

La sortie par défaut est créée et placée dans un fichier texte nommé CtiosClientLog dans le fichier c:\Program Files\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\ install directory.

## Problèmes liés aux clients avec le suivi et les connexions sur PG

### Debug CAD Sync Service

Voici les paramètres de débogage du service de synchronisation CAD :

Paramètre	Valeur
Fichier de configuration	DirAccessSynSvr.cfg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\config
Questions générales	Seuil=DEBUG
Fichiers de sortie	DirAccessSynSvr.log

### Déboguer le serveur RASCAL CAD 6.0(X)

Voici les paramètres de débogage du serveur RASCAL CAD 6.0(X) :

Paramètre	Valeur
Fichier de configuration	FCRasSvr.cfg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\config
Questions générales	Plage = 1-4, 50, 3000-8000
Problèmes liés à LDAP :	Plage = 4 000-4 999
Problèmes liés à LRM :	Plage = 1999-2000
Problèmes liés à la base de données	Plage = 50-59
Fichiers de sortie	FCRasSvr.log, FCRasSvr.dbg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\log

## Débuguer le serveur de conversation

Voici les paramètres de débogage du serveur de discussion :

Paramètre	Valeur
Fichier de configuration	FCCServer.cfg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\config
Questions générales	Seuil=DEBUG
Fichiers de sortie	FCCServer.log, FCCServer.dbg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\log

## Autres journaux et traçage liés aux PG

Reportez-vous à [Utilisation de l'utilitaire Dumplog pour extraire les journaux](#) pour la collection de journaux.

## Activer le suivi de CallManager PIM

Utilisez l'utilitaire de surveillance du processus (procmon) afin d'activer et de désactiver les niveaux de suivi. Ces commandes activent le suivi du gestionnaire d'interface périphérique (PIM) 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
```

Cette commande procmon désactive le suivi PIM de CallManager :

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

## Activer le suivi sur CUCM

Cette procédure décrit comment activer le suivi CUCM :

1. Accédez à Call Manager Unified Serviceability.
2. Sélectionnez **Trace/Configuration**.
3. Sélectionnez **Services CM**.
4. Sélectionnez **CTIManager (Actif)**.
5. En haut à droite, sélectionnez **Configuration SDL**.
6. Activez tout sauf Désactiver l'impression de SDL Trace.

7. Laissez le nombre de fichiers et leur taille aux valeurs par défaut.

8. Dans l'outil de surveillance en temps réel (RTMT), collectez Cisco Call Manager et Cisco Computer Telephony Integration (CTI) Manager. Tous deux ont des journaux SDI (System Diagnostic Interface) et SDL (Signal Distribution Layer).

## Activer la passerelle JTAPI (Java Telephony Application Programming Interface) (JGW)

Ces commandes procmon activent le suivi 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 exemple de commande est **procmon ipcc pg1a jgw1**.

## Activer le suivi du serveur CTI (CTISVR) côté actif

Cette procédure décrit comment activer le suivi CTISVR du côté actif :

1. Utilisez l'éditeur du Registre afin de modifier HKLM\software\Cisco Systems, Inc\icm\<cust\_inst>\CG1(a et b)\EMS\CurrentVersion\library\Processes\ctisvr.
2. Définissez EMSTraceMask = f8.

## Activer le suivi de VRU PIM

**Note:** Les commandes sont sensibles à la casse. La passerelle VRU (Voice Response Unit) PG est différente de la passerelle Cisco CallManager (CCM) PG.

Ces commandes procmon activent le suivi pour VRU PIM :

```
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
```

Cette commande procmon désactive le suivi VRU PIM :

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

## Activer le suivi du serveur CTIOS sur les deux serveurs CTIOS

Cette procédure décrit comment activer le suivi sur les deux serveurs CTIOS :

1. Notez le masque de trace actuel pour une utilisation ultérieure.
2. Utilisez l'éditeur du Registre afin de modifier HLKM » Software\Cisco Systems Inc.\ICM\<cust\_inst\CTIOS\EMS\CurrentVersion\library\Processes\ctios.
3. Définir :
  - EMSTraceMask = 0x60A0F
  - EMSTraceMask à l'une de ces valeurs, selon la version :
    - 0x0A0F pour la version 6.0 et antérieure
    - 0x20A0F pour les versions 7.0 et 7.1(1)
    - 0x60A0F pour version 7.1(2) et ultérieure

Le masque de suivi par défaut est 0x3 dans toutes les versions sauf la version 7.0(0), où il est 0x20003.

Si le masque de trace a une valeur élevée (0xf ou supérieure), il y a un impact important sur les performances du serveur CTIOS et le taux de réalisation des appels. Définissez le masque de trace à une valeur élevée uniquement lorsque vous déboguez un problème ; une fois que vous avez collecté les journaux nécessaires, vous devez rétablir la valeur par défaut du masque de trace.

À des fins de dépannage, définissez le masque de trace du serveur CTIOS sur :

- 0x0A0F pour la version 6.0 et antérieure
- 0x20A0F pour les versions 7.0 et 7.1(1)
- 0x60A0F pour version 7.1(2) et ultérieure

## Activer le suivi OPC (Open Peripheral Controller) sur Active PG

Ces commandes opctest activent le suivi OPC sur une PG active :

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

Voici un exemple tiré d'un environnement de travaux pratiques :

```
C:\Documents and Settings\ICMAdministrator>opctest /cust ccl /node pgl1
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
```

Voici d'autres exemples :

```
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
```

## Activer le suivi Eagtpim sur le groupe de compétences actif

Ces commandes procmon activent le suivi eagtpim sur une PG active :

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

Voici un exemple tiré d'un environnement de travaux pratiques :

```
C:\Documents and Settings\ICMAdministrator>procmon cc1 pgl1a pim1
>>>>trace tp* /on
>>>>trace precall /on
>>>>trace *event /on
>>>>trace csta* /on
>>>>quit
```

## Utiliser l'utilitaire Dumplog pour extraire les journaux

Référez-vous à [Utilisation de l'utilitaire Dumplog](#) pour plus de détails. Utilisez la commande **cdlog** afin d'accéder au répertoire logfiles, comme illustré dans cet exemple :

```
c:\cdlog <customer_name> pgl1a !-- Or, pgXa to depending on the PG number (X)
c:\icm\<customer_name>\<<PG#>>\logfiles\
```

Ces exemples montrent comment placer la sortie dans le fichier par défaut ; dans tous les cas, vous pouvez utiliser **/of** afin de définir un nom spécifique pour le fichier de sortie :

```
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> cgl1a
c:\icm\<customer_name>\<cg#>\logfiles\
!-- This JTAPI example places output in a default jgw1.txt file
```

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

## Activer le suivi sur les serveurs CVP



## SIP

Cette procédure décrit comment activer le suivi sur les serveurs CVP avec le logiciel de téléphone IP Cisco SIP :

1. Sur le ou les serveurs d'appels, accédez à l'outil de diagnostic CVP ([http://localhost\(CallServer\):8000/cvp/diag](http://localhost(CallServer):8000/cvp/diag)) afin d'obtenir la pile SIP (Session Initiation Protocol).
2. Ajoutez com.dynamicsoft.Dslibs.DsUAlibs avec debug.
3. Cliquez sur **Set**.
4. Cliquez sur **DEBUG/41**.

## H323

Cette procédure décrit comment activer le suivi sur les serveurs CVP avec une passerelle H323 :

1. Sur le ou les serveurs d'appels, connectez-vous à VBAAdmin.
2. Activez ces traces pour le navigateur vocal CVP :

```
setcalltrace on  
setinterfacetrace on
```

### Extraire les journaux CVP des serveurs d'appels

Collectez les fichiers CVP \*.log et Error.log pour la période de test. Ces fichiers se trouvent dans le répertoire C:\Cisco\CVP\logs directory on both CVP servers.

Il s'agit des emplacements des fichiers journaux pour Unified CVP, où CVP\_HOME est le répertoire dans lequel le logiciel Unified CVP est installé.

Type de journal	Emplacement
Journaux du serveur d'appels et/ou du serveur de rapports	CVP_HOME\logs\
Journaux de la console d'exploitation	CVP_HOME\logs\OAMP\
Journaux du serveur VXML (Voice XML)	CVP_HOME\logs\VXML\
Journaux des agents SNMP (Simple Network Management Protocol)	CVP_HOME\logs\SNMP\
Journaux du gestionnaire de ressources Unified CVP	CVP_HOME\logs\ORM\

Un exemple d'emplacement est C:\Cisco\CVP.

### Journaux du serveur VXML

Pour les applications vocales XML personnalisées telles qu'une application Audium déployée, vous pouvez activer un enregistreur de débogage.

Ajoutez cette ligne à la section <loggers> (dernière section) du fichier de configuration settings.xml

dans le fichier C:\Cisco\CVP\VXMLServer\applications\APP\_NAME\data\application\ directory:

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

Au moment de l'exécution, cet enregistreur affiche un journal VoiceXML détaillé sur le site \Cisco\CVP\VXMLServer\applications\APP\_NAME\MyDebugLogger directory.

**Note:** Vous pouvez modifier le nom de l'enregistreur dans le fichier de configuration settings.xml de MyDebugLogger à n'importe quel nom que vous choisirez.

## Suivi et collecte de journaux liés au numéroteur sortant

Cette procédure décrit comment augmenter les journaux de processus de badialer sur le Outbound Dialer (qui se trouve généralement sur une PG).

1. Assurez-vous que EMSDisplaytoScreen = 0.
2. Utilisez l'éditeur du Registre afin de modifier HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer.
3. Définir :
  - EMSTraceMask = 0xff
  - EMSUserData = ff ff (quatre f en mode binaire)
4. Utilisez l'éditeur du Registre afin de modifier HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer.
5. Définissez DebugDumpAllEvents = 1.

## Journaux d'extraction

Exécutez l'utilitaire dumplog à partir du répertoire /icm/<instance>/dialer/logfiles :

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

## Sur l'importateur

Cette procédure décrit comment augmenter le journal du processus de port de baigne.

1. Utilisez l'éditeur du Registre afin de modifier HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\ balimport.
2. Définir :
  - EMSTraceMask = 0xff

- EMSUserData = ff ff (quatre f en mode binaire)

3. Exécutez l'utilitaire dumplog à partir du répertoire /icm/<instance>/la/logfiles :

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

## Sur le gestionnaire de campagnes

Cette procédure décrit comment augmenter le journal des processus du gestionnaire de campagne.

1. Utilisez l'éditeur du Registre afin de modifier HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Logger\EMS\CurrentVersion\Library\Processes\CampaignManager.

2. Définir :

- EMSTraceMask = 0xff
- EMSUserData = ff ff (quatre f en mode binaire)

3. Exécutez l'utilitaire dumplog à partir du répertoire /icm/<instance>/la/logfiles :

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

Sur la PG d'Avaya Communications Manager (ACD), utilisez l'utilitaire **opctest** afin d'augmenter les éléments suivants pour CallManager et Avaya.

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

Cette procédure décrit comment augmenter le suivi du processus ctisvr.

1. Utilisez l'éditeur du Registre afin de modifier HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr.

2. Définissez EMSTraceMask = f8. Vous pouvez laisser la valeur à f0 si vous le souhaitez.

## Activer les connexions du routeur sur le processus du routeur

Cette procédure décrit comment activer les journaux de routeur :

1. Sur le routeur, accédez à **Start > Run**, puis saisissez **rttrace**.
2. Tapez le nom du client.
3. Cliquez sur **Connect**.

#### 4. Sélectionnez les options suivantes :

modifications d'agentquêtes de routeurscriptselectsréseauroutage de traductionmise en file  
d'attentecalltyperealtime

#### 5. Cliquez sur Apply.

#### 6. Quittez l'utilitaire.

Pour la version de test 8.5, utilisez plutôt le Portico du cadre de diagnostic.

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

### Récupérer les journaux du routeur

Utilisez l'utilitaire dumplog pour extraire les journaux de routeur de l'un des routeurs pendant la période des tests. Référez-vous à [Utilisation de l'utilitaire Dumplog](#) pour plus de détails.

Ceci est un exemple de demande de journal pour les journaux le 21/10/2011 entre 09:00:00 et 09:30:00 (au format 24 heures). Cette sortie est envoyée au fichier 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
```

Envoyez le fichier de sortie (C:/router\_output.txt) à Cisco pour le dépannage si nécessaire.

### Traces de passerelle (SIP)

Ces commandes activent le suivi sur les serveurs CVP avec 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
```

**Note:** Toute modification apportée à un logiciel GW Cisco IOS<sup>®</sup> de production peut entraîner une panne.

Il s'agit d'une plate-forme très robuste qui peut gérer les débogages suggérés au volume d'appels fourni sans problème. Cependant, Cisco vous recommande :

- Envoyez tous les journaux à un serveur syslog au lieu de les envoyer à la mémoire tampon de journalisation :

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

- Appliquez les commandes debug une par une, et vérifiez l'utilisation du CPU après chacune :

```
show proc cpu hist
```

**Note:** Si l'utilisation du processeur atteint 70 à 80 %, le risque d'un impact sur les performances du service est considérablement accru. Ainsi, n'activez pas les débogages supplémentaires si la GW atteint 60%.

Activez ces débogages :

```
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
```

Après avoir passé l'appel et simulé le problème, arrêtez le débogage :

```
#undebug all
```

Collectez ce résultat :

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

## Suivi CUSP

Ces commandes activent le suivi SIP sur Cisco Unified SIP Proxy (CUSP) :

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

N'oubliez pas de désactiver la connexion une fois que vous avez terminé.

Cette procédure décrit comment collecter les journaux :

1. Configurez un utilisateur sur le CUSP (par exemple, test).
2. Ajoutez cette configuration à l'invite CUSP :

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

3. FTP vers l'adresse IP CUSP. Utilisez le nom d'utilisateur (test) et le mot de passe définis à

l'étape précédente.

4. Remplacez les répertoires par /cusp/log/trace.
5. Obtenez le fichier journal\_<filename>.

## Utilisation de l'interface de ligne de commande pour le suivi

Dans UCCE version 8 et ultérieure, vous pouvez utiliser l'interface de ligne de commande (CLI) de Unified System afin de collecter les traces. Comparé aux utilitaires dumplog, l'interface de ligne de commande est une méthode très rapide et efficace pour obtenir un ensemble complet de journaux à partir d'un serveur tel qu'un PG ou un Rogger.

Cette procédure décrit comment démarrer l'analyse des problèmes et comment déterminer le traçage à activer. L'exemple collecte les journaux de ces serveurs :

- ROUTEUR A/ROUTEUR B
- LOGGER-A/LOGGER-B
- PGXA/PGXB
- Tous les serveurs d'appels CVP
- Tous les serveurs CVP VXML/Media (le cas échéant)

1. Sur chaque système de la liste, ouvrez Unified System CLI sur chaque serveur et exécutez cette commande :

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

Remplacez la première chaîne *mm-jj-aaaa:hh:mm* par une date et une heure qui sont environ 15 minutes avant l'événement.

Remplacez la deuxième chaîne *mm-jj-aaaa:hh:mm* par une date et une heure qui sont approximativement 15 minutes après la résolution de l'événement. Si l'événement se produit toujours, rassemblez au moins 15 minutes. Ceci produit un fichier appelé clioutputX.zip, où X est le numéro suivant dans l'ordre.

2. Exportez les journaux Application/Sécurité/Système Windows de chaque système au format CSV (valeurs séparées par des virgules) et enregistrez-les dans le répertoire C:\Temp directory.
3. Ajoutez les journaux CSV Windows au fichier zip à partir de l'étape 1 et renommez le fichier zip au format suivant :

<NOM DU SERVEUR>-SystCLILogs-EvntOn-YYMDD\_HHMMSS.zip

4. Sur n'importe quel groupe d'agents, collectez les journaux dans le répertoire C:\Program Files\Cisco\Desktop\logs every time the failure is seen. Envoyez les journaux dans un fichier portant un nom au format suivant :

<NOM DU SERVEUR>-CADLogs-EvntOn-YYYYMMDD\_HHMMSS.zip

Si vous utilisez CAD-Browser Edition (CAD-BE) ou tout autre produit Web CAD, collectez les journaux à partir du répertoire C:\Program Files\Cisco\Desktop\Tomcat\logs directory et ajoutez-les au même fichier zip.

Si vous utilisez l'un des produits Windows 2008 x64, le répertoire du journal se trouve sous C:\Program Files (x86)\Cisco\Desktop\...

5. Joignez ces fichiers à la demande de service ou téléchargez-les sur FTP s'ils sont trop volumineux pour être envoyés par e-mail ou joints.

Recueillez ces informations supplémentaires si possible :

- Heure de début et d'arrêt de l'événement.
- Plusieurs échantillons de l'ANI/DNIS/AgentID impliqués dans l'événement. Au minimum, Cisco a besoin d'au moins l'un d'eux pour voir l'événement.
- RouteCallDetail (RCD) et TerminationCallDetail (TCD) pour la période entourant l'événement.

La requête RCD est la suivante :

```
SELECT * FROM Route_Call_Detail WHERE DbDateTime > 'AAAA-MM-JJ HH:MM:SS.MMM'
et DbDateTime < 'AAAA-MM-JJ HH:MM:SS.MMM'
```

La requête TCD est la suivante :

```
SÉLECTIONNEZ * FROM Termination_Call_Detail WHERE DbDateTime > 'AAAA-MM-JJ
HH:MM:SS.MMM' et DbDateTime < 'AAAA-MM-JJ HH:MM:SS.MMM'
```

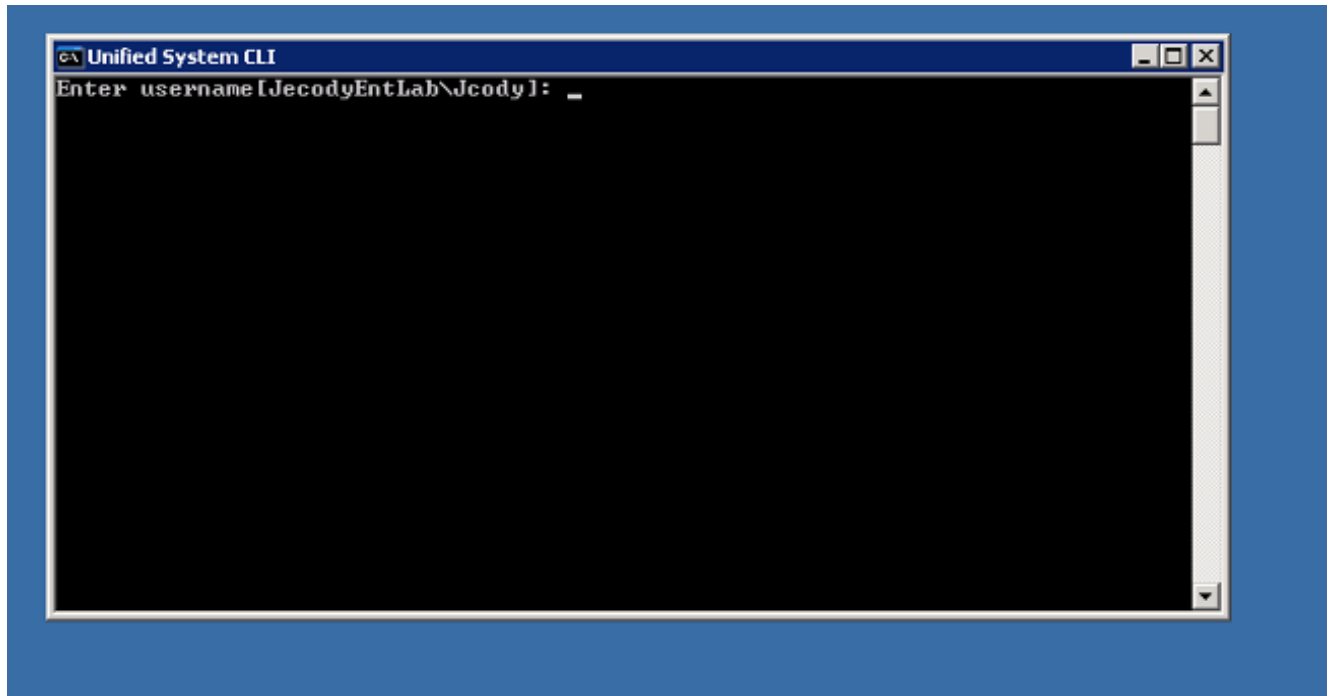
## Exemple CLI

**Note:** Vous êtes averti que ces actions peuvent avoir un impact sur le système. Il est donc possible que vous souhaitiez effectuer ce travail pendant les heures d'arrêt ou pendant une période lente.

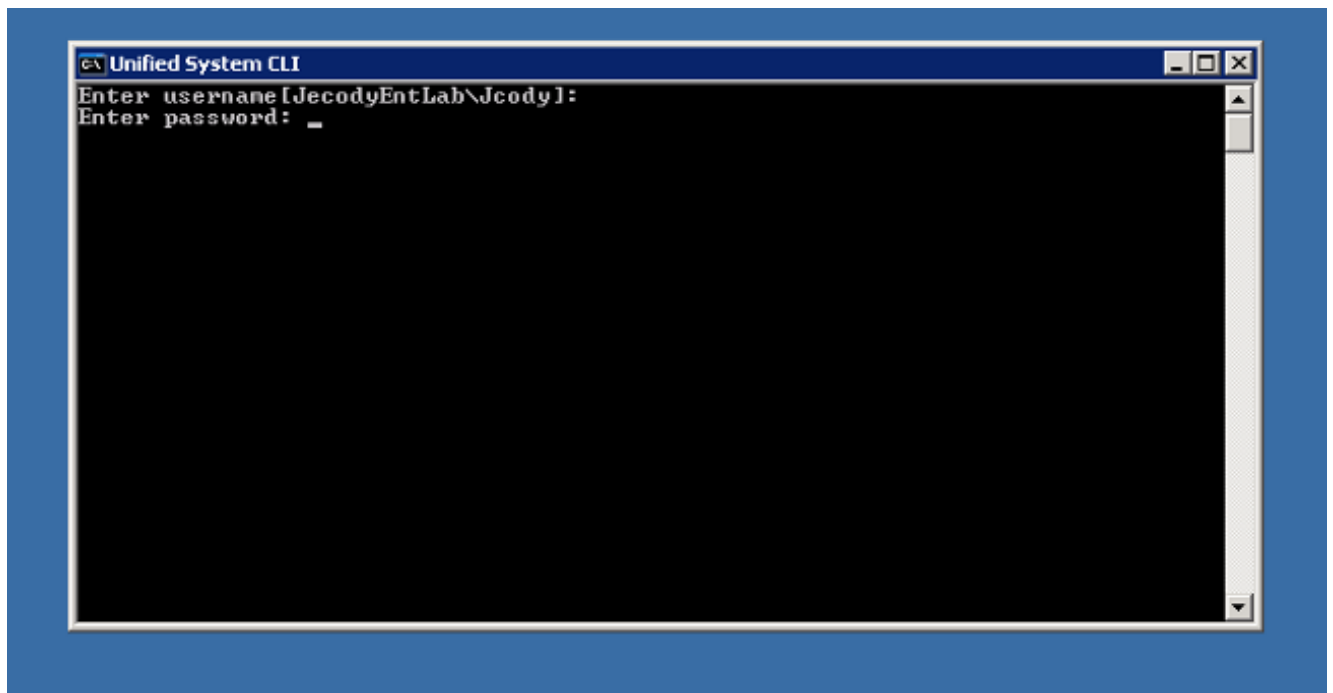
Il existe deux outils : un outil de cadre de diagnostic et l'outil CLI système. Les deux sont des icônes sur le bureau ou sous le répertoire Programs de chaque serveur.

Cette procédure décrit comment utiliser l'interface de ligne de commande Unified System pour le suivi.

1. Cliquez sur l'icône Unified System CLI, puis connectez-vous avec le domaine et le nom d'utilisateur. (Dans cet exemple, l'administrateur de domaine s'est déjà connecté, de sorte que l'interface de ligne de commande connaît déjà le domaine (JecodyEntLab) et le nom d'utilisateur (Jcody).

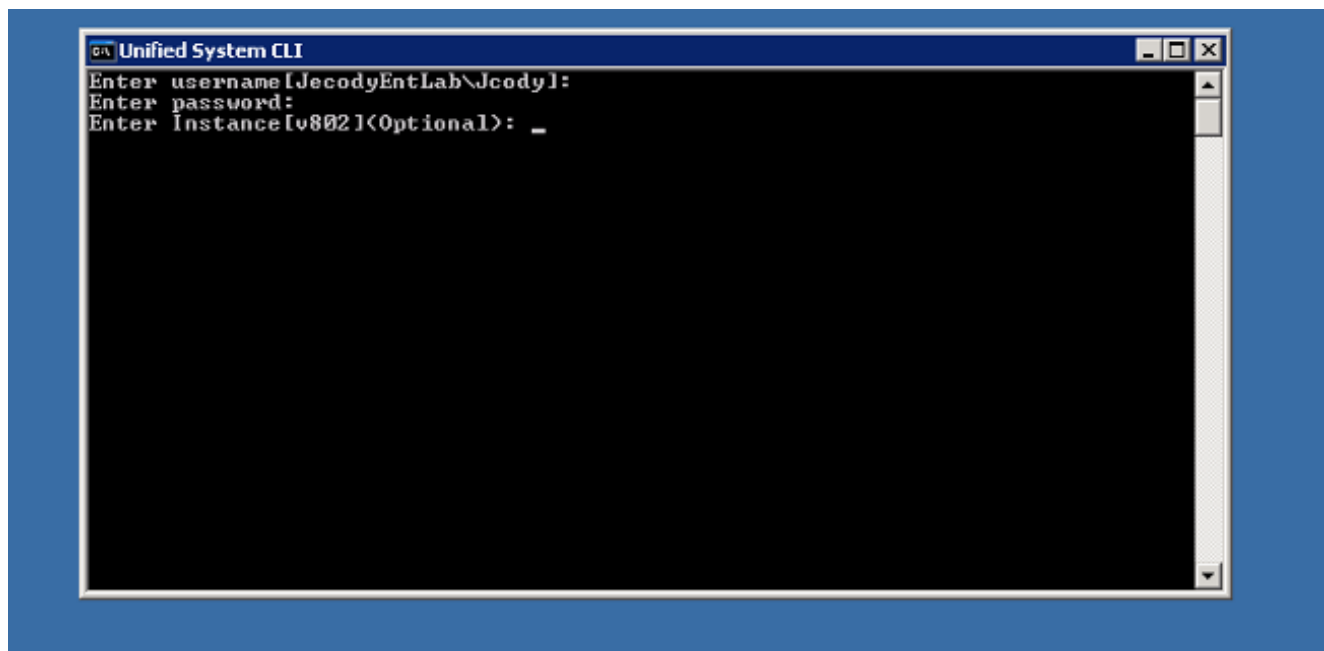


2. Entrez le mot de passe.

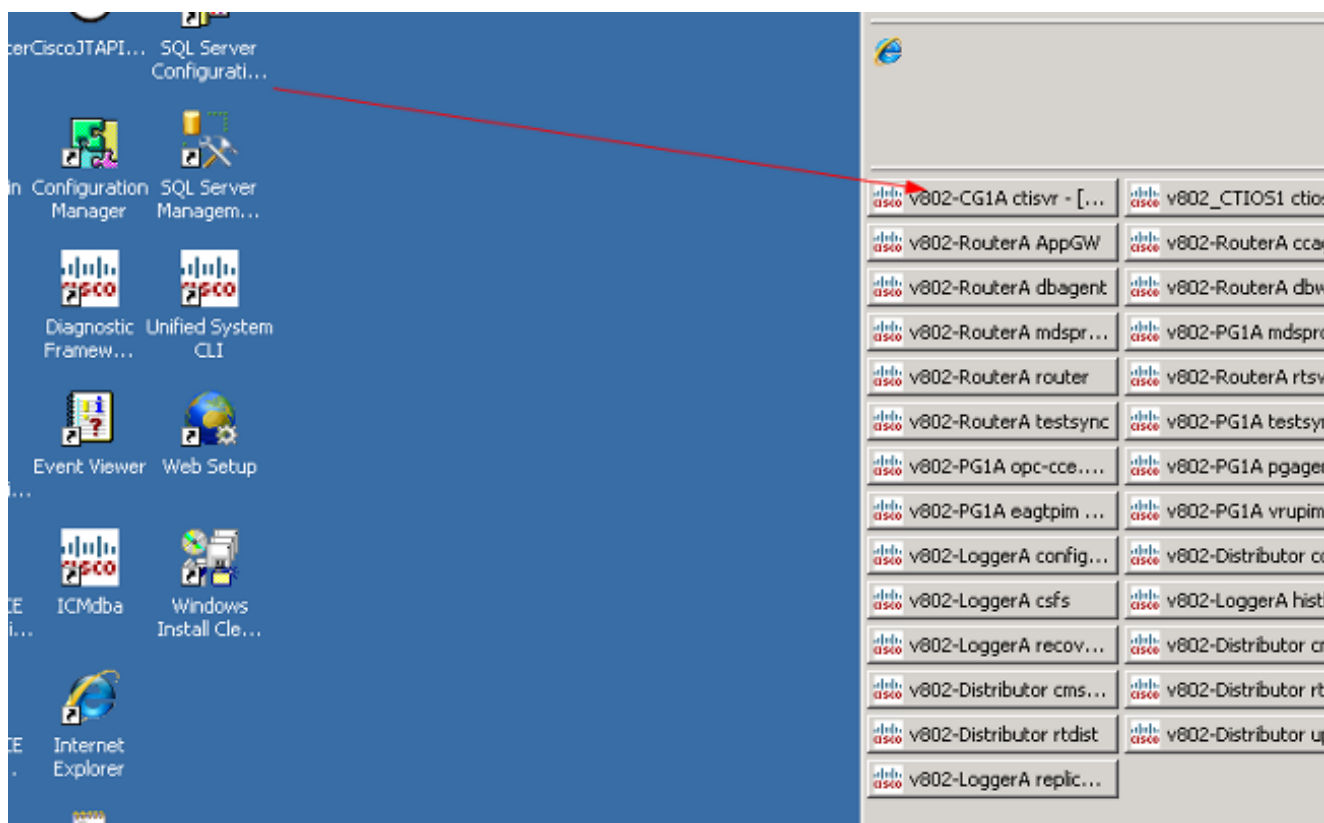


3. Entrez le nom de l'instance ; dans cet exemple, il s'agit de v802. Regardez la PG à l'un des services; le nom de l'instance est la première partie du nom du service.





4. Pour trouver le nom de l'instance, il suffit de consulter les services qui s'exécutent sur le serveur .



5. Une fois le message de bienvenue affiché, entrez cette commande :

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

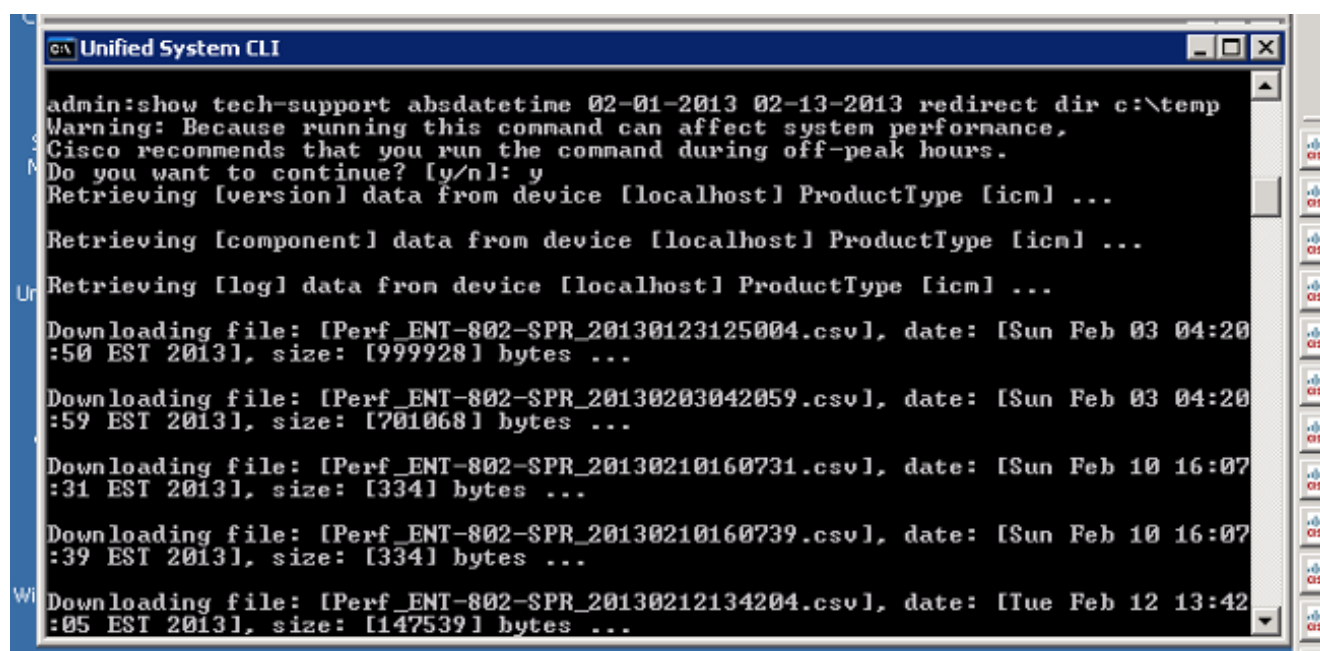
Remplacez la première chaîne *mm-jj-aaaa:hh:mm* par une date et une heure qui sont environ 15 minutes avant l'événement.

Remplacez la deuxième chaîne *mm-jj-aaaa:hh:mm* par une date et une heure qui sont

approximativement 15 minutes après la résolution de l'événement.

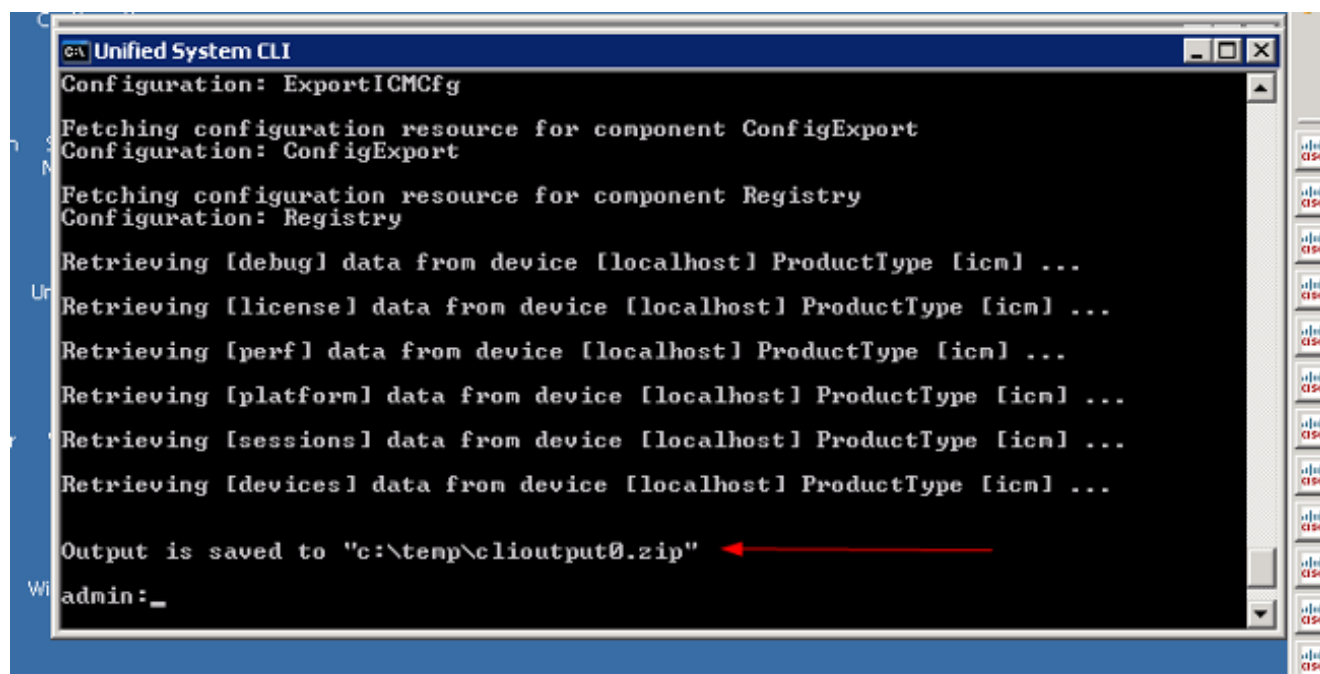
Si l'événement se produit toujours, rassemblez au moins 15 minutes.

Ceci produit un fichier nommé *clioutputX.zip*, où *X* est le numéro suivant dans l'ordre.



```
Unified System CLI
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. Une fois le processus terminé, recherchez le fichier *clioutputX.zip* dans le répertoire :



```
Unified System CLI
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:_
```

**Note:** Ce fichier est généralement très volumineux car il contient tous les fichiers liés à UCCE pour tous les services de ce serveur.

7. Si vous n'avez besoin que d'un seul journal, il peut être plus facile d'utiliser l'utilitaire *dumplog* plus ancien ou d'utiliser le *Portico* du cadre de diagnostic :

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%