Imposta e raccogli log di traccia UCCE

Sommario

Introduzione

In questo documento viene descritto come impostare la traccia in Cisco Unified Contact Center Enterprise (UCCE) per client, servizi GRE (Peripheral Gateway), Cisco Customer Voice Portal

(CVP), Cisco UCCE Outbound Dialer, Cisco Unified Communications Manager (CallManager) (CUCM) e gateway Cisco.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 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)
- Gateway Cisco

Impostazioni traccia e raccolta log

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**
>
> consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Finesse

Accedere al server Finesse con Secure Shell (SSH) e immettere questi comandi per raccogliere i log necessari. Viene chiesto di identificare un server FTP SSH (SFTP) in cui caricare i log.

Log	Comando
Installa registri	**file get install desktop-install.log**
Registri desktop	**file get activelog desktop recurs compress**
Log servm	**file get activelog platform/log/servm*.* comprimi**
Log Tomcat della piattaforma	**file get activelog tomcat/logs recurs compress**
Registri di installazione VOS (Voice Operating System)	**file get install.log**

Cisco Agent Desktop

In questa procedura viene descritto come creare e raccogliere i file di debug:

1. Sul computer agente, andare alla directory C:\Program Files\Cisco\Desktop\Config e aprire il file Agent.cfg.

2. Modificare la soglia di debug da OFF a **DEBUG**. TRACE può essere utilizzato per un livello più profondo.

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

3. Assicurarsi che Size=3000000 (sei zeri).

4. Salvate il file di configurazione.

5. Arrestare il programma dell'agente.

6. Eliminare tutti i file nella directory C:\Program Files\Cisco\Desktop\log.

7. Avviare il programma dell'agente e ricreare il problema.

8. I file di debug vengono creati e posizionati in C:\Program Files\Cisco\Desktop\log:

   agent0001.dbgciosclientlog.xxx.log

Cisco Supervisor Desktop

In questa procedura viene descritto come creare e raccogliere i file di debug:

1. Sul computer agente, andare alla directory C:\Program Files\Cisco\Desktop\Config e aprire il file supervisor.cfg.

2. Modificare il valore di debug THRESHOLD da OFF a **DEBUG**. TRACE può essere utilizzato per un livello più profondo.

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

3. Assicurarsi che Size=3000000 (sei zeri).

4. Salvate il file di configurazione.

5. Arrestare il programma dell'agente.

6. Eliminare tutti i file nella directory C:\Program Files\Cisco\Desktop\log.

7. Avviare il programma dell'agente e ricreare il problema. Viene creato un file di debug denominato supervisor0001.dbg che viene posizionato in C:\Program

Files\Cisco\Desktop\log.

Desktop client Cisco

Sul PC client in cui è installato il client CTIOS, utilizzare Regedt32 per attivare la funzionalità di traccia. Cambia le impostazioni:

Release	Percorso Registro di sistema	Valore predefinito	Cambia
Release precedenti alla 7.x	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0x07	Aumentare il valore a 0xfff.
Release 7.x e successive	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS Tracing	0x40000307	Impostare il valore su 0xfff per la risoluzione dei problemi.

L'output predefinito viene creato e inserito in un file di testo denominato CtiosClientLog nella directory di installazione c:\Programmi\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\.

Problemi relativi al client con trace e login a PG

Debug servizio di sincronizzazione CAD

Di seguito sono riportate le impostazioni per eseguire il debug del servizio di sincronizzazione CAD.

Impostazione	Valore
File di configurazione	DirAccessSynSvr.cfg
Percorso predefinito	C:\Program Files\Cisco\Desktop\config
Problemi generali	Soglia=DEBUG
File di output	DirAccessSynSvr.log

Debug del server CAD 6.0(X) RASCAL

Di seguito sono riportate le impostazioni per eseguire il debug del server CAD 6.0(X) RASCAL:

Impostazione	Valore
File di configurazione	FCRasSvr.cfg
Percorso predefinito	C:\Program Files\Cisco\Desktop\config
Problemi generali	Intervallo = 1-4, 50, 3000-8000
Problemi relativi a LDAP:	Intervallo = 4000-4999
Problemi relativi a LRM:	Intervallo = 1999-2000
Problemi relativi al database	Intervallo = 50-59
File di output	FCRasSvr.log, FCRasSvr.dbg
Percorso predefinito	C:\Program Files\Cisco\Desktop\log

Debug del server di chat

Di seguito sono riportate le impostazioni per eseguire il debug del server di chat:

Impostazione	Valore
File di configurazione	ServerFCS.cfg
Percorso predefinito	C:\Program Files\Cisco\Desktop\config
Problemi generali	Soglia=DEBUG
File di output	FCCServer.log, FCCServer.dbg
Percorso predefinito	C:\Program Files\Cisco\Desktop\log

Altri registri e analisi relativi a PG

Vedere Utilizzare l'utilità Dumplog per eseguire il pull dei log per la raccolta dei log.

Abilita traccia PIM CallManager

Usare l'utilità di monitoraggio del processo (procmon) per attivare e disattivare i livelli di traccia. Questi comandi attivano la traccia di CallManager Peripheral Interface Manager (PIM):

```
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
```

Questo comando procmon disattiva la traccia PIM di CallManager:

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

Abilita traccia in CUCM

In questa procedura viene descritto come attivare la traccia CUCM:

1. Passare a Call Manager Unified Serviceability.
2. Selezionare **Trace/Configuration**.
3. Selezionare **CM Services**.
4. Selezionare **CTIManager (Attivo)**.
5. In alto a destra, selezionare **SDL Configuration**.
6. Attivare tutti gli elementi tranne Disattivare Stampa semplice di SDL Trace.

7. Mantenere il numero di file e le relative dimensioni sui valori predefiniti.

8. Nello strumento di monitoraggio in tempo reale (RTMT), raccogliere Cisco Call Manager e Cisco Computer Telephony Integration (CTI) Manager. Entrambi dispongono di registri SDI (System Diagnostic Interface) e SDL (Signal Distribution Layer).

Abilita JGW (Java Telephony Application Programming Interface) Gateway

I seguenti comandi procmon attivano il trace 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 di esempio è **procmon ipcc pg1a jgw1**.

Abilita traccia CTI Server (CTISVR) sul lato attivo

Questa procedura descrive come abilitare il trace del CTISVR sul lato attivo:

1. Utilizzare l'editor del Registro di sistema per modificare HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a e b)\EMS\CurrentVersion\library\Processes\ctisvr.

2. Impostare EMSTraceMask = f8.

Attiva VRU PIM di traccia

> **Nota:** I comandi distinguono tra maiuscole e minuscole. il gruppo di facce VRU (Voice Response Unit) è diverso dal gruppo di facce Cisco CallManager (CCM).

Questi comandi procmon attivano il trace per 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
```

Questo comando procmon disattiva la traccia PIM della VRU:

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

Abilita traccia server CTIOS su entrambi i server CTIOS

In questa procedura viene descritto come abilitare la traccia in entrambi i server CTIOS:

1. Prendere nota della maschera di traccia corrente per utilizzarla successivamente.

2. Usare l'editor del Registro di sistema per modificare HLKM >> Software\Cisco Systems Inc.\ICM\<cust_inst\CTIOS\EMS\CurrentVersion\library\Processes\ctios.

3. Imposta:

    - EMSTraceMask = 0x60A0F
    - EMSTraceMask su uno di questi valori, a seconda della versione:
        - 0x0A0F per la release 6.0 e precedenti
        - 0x20A0F per la release 7.0 e 7.1(1)
        - 0x60A0F per la release 7.1(2) e successive

La maschera di traccia predefinita è 0x3 in tutte le versioni ad eccezione della versione 7.0(0), dove è 0x2003.

Se il valore della maschera di traccia è elevato (0xf o superiore), le prestazioni del server CTIOS e la percentuale di completamento delle chiamate saranno notevolmente compromesse. Impostare la maschera di traccia su un valore alto solo quando si esegue il debug di un problema; dopo aver raccolto i registri necessari, è necessario impostare nuovamente la maschera di traccia sul valore predefinito.

Per la risoluzione dei problemi, impostare la maschera di traccia del server CTIOS su:

- 0x0A0F per la release 6.0 e precedenti
- 0x20A0F per la release 7.0 e 7.1(1)
- 0x60A0F per la release 7.1(2) e successive

Abilita traccia Open Peripheral Controller (OPC) su Active PG

I seguenti comandi ottici attivano il trace OPC su un PG attivo:

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

Questo è un esempio da un ambiente lab:

```
C:\Documents and Settings\ICMAdministrator>opctest /cust cc1 /node pg1a
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
```

Altri esempi sono:

```
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
```

Abilita traccia Eagtpim su Active PG

Questi comandi procmon attivano il tracciamento eagtpim su un PG attivo:

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

Questo è un esempio da un ambiente lab:

```
C:\Documents and Settings\ICMAdministrator>procmon cc1 pg1a pim1
>>>>trace tp* /on
>>>>trace precall /on
>>>>trace *event /on
>>>>trace csta* /on
>>>>quit
```

Utilizzo dell'utilità Dumplog per il pull dei log

Per ulteriori informazioni, consultare Uso dell'utilità Dumplog. Utilizzare il comando **cdlog** per accedere alla directory logfiles, come mostrato nell'esempio:

```
c:\cdlog <customer_name> pg1a   !-- Or, pgxa to depending on the PG number (x)
c:\icm\<customer_name>\<<PG#>>\logfiles\
```

In questi esempi viene illustrato come inserire l'output nel file predefinito; in tutti i casi, è possibile utilizzare */of* per definire un nome specifico per il file di output:

```
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> cg1a
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
```

Abilita traccia sui server CVP

SIP

In questa procedura viene descritto come abilitare la traccia sui server CVP con il software Cisco SIP IP Phone:

1. Sui server di chiamata, passare allo strumento di diagnostica CVP (http://localhost(CallServer):8000/cvp/diag) per ottenere lo stack SIP (Session Initiation Protocol).

2. Aggiungere com.dynamicsoft.Dslibs.DsUAlibs con debug.

3. Fare clic su **Imposta**.

4. Fare clic su **DEBUG/41**.

H323

In questa procedura viene descritto come abilitare la traccia sui server CVP con un gateway H323:

1. Nei server di chiamata, accedere a VBAdmin.

2. Abilitare queste tracce per il Voice Browser CVP:

```
setcalltrace on
setinterfacetrace on
```

Estrai registri CVP dai server di chiamata

Raccogliere il file CVP *.log e i file Error.log per l'ora del periodo di prova. Questi file si trovano nella directory C:\Cisco\CVP\logs su entrambi i server CVP.

Queste sono le posizioni dei file di log per Unified CVP, dove CVP_HOME è la directory in cui è installato il software Unified CVP.

Tipo di log	Posizione
Registri server di chiamata e/o server di report	CVP_HOME\logs\
Registri console operazioni	CVP_HOME\logs\OAMP\
Registri server Voice XML (VXML)	CVP_HOME\logs\VXML\
Registri agente SNMP (Simple Network Management Protocol)	CVP_HOME\logs\SNMP\
Registri di Unified CVP Resource Manager	CVP_HOME\logs\ORM\

Un esempio di percorso è C:\Cisco\CVP.

Registri server VXML

Per applicazioni Voice XML personalizzate, ad esempio un'applicazione Audium distribuita, è possibile attivare un registratore di debug.

Aggiungere questa riga alla sezione <loggers> (l'ultima sezione) del file di configurazione settings.xml nella directory C:\Cisco\CVP\VXMLServer\applications\APP_NAME\data\application\:

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

In fase di esecuzione, questo logger invia un log VoiceXML dettagliato alla directory \Cisco\CVP\VXMLServer\applications\APP_NAME\MyDebuggerLogger.

> **Nota:** È possibile modificare il nome del logger nel file di configurazione settings.xml da MyDebugLogger in qualsiasi nome scelto.

Traccia e raccolta log relativi a Dialer in uscita

In questa procedura viene descritto come aumentare i registri di processo di conversione in uscita (generalmente disponibili in PG).

1. Assicurarsi che EMSDisplaytoScreen = 0.

2. Usare l'editor del Registro di sistema per modificare HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer.

3. Imposta:

   - EMSTraceMask = 0xff
   - EMSUserData = ff (quattro f in modalità binaria)

4. Usare l'editor del Registro di sistema per modificare HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer.

5. Impostare DebugDumpAllEvents = 1.

Registri pull

Eseguire l'utilità dumplog dalla directory /icm/<istanza>/dialer/logfiles:

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

Sull'Importatore

In questa procedura viene descritto come aumentare il log del processo baimport.

1. Usare l'editor del Registro di sistema per modificare HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\ baImport.

2. Imposta:

- EMSTraceMask = 0xff
- EMSUserData = ff (quattro f in modalità binaria)

3. Eseguire l'utilità dumplog dalla directory /icm/<instance>/la/logfiles:

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

In Gestione campagne

In questa procedura viene descritto come aumentare il registro del processo di Gestione campagne.

1. Usare l'editor del Registro di sistema per modificare HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager.

2. Imposta:

   - EMSTraceMask = 0xff
   - EMSUserData = ff (quattro f in modalità binaria)

3. Eseguire l'utilità dumplog dalla directory /icm/<instance>/la/logfiles:

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

In Avaya Communications Manager (ACD) PG, utilizzare l'utilità **opctest** per aumentare i valori seguenti per CallManager e Avaya.

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

In questa procedura viene descritto come aumentare il valore di trace per il processo ctisvr.

1. Usare l'editor del Registro di sistema per modificare HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr.

2. Impostare EMSTraceMask = f8. Se lo si desidera, è possibile lasciare il valore su f0.

Abilita processo di accesso router al router

In questa procedura viene descritto come abilitare i log del router:

1. Sul router, selezionare **Start** > **Esegui**, quindi immettere **trtrace**.

2. Digitare il nome del cliente.

3. Fare clic su **Connetti**.

4. Selezionare le opzioni seguenti:

   modificheagenterichieste routerscriptselezionirouting in retetranslationrouteaccodamento chiamateora solare

5. Fare clic su **Apply** (Applica).

6. Uscire dall'utilità.

Per la versione Optical 8.5, utilizzare il Portico Diagnostic Framework.

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

Esegui il pull dei log del router

Usare la utility dumplog per estrarre i log del router da entrambi i router per il periodo di tempo specificato per i test. Per ulteriori informazioni, consultare Uso della utility dumplog.

Questo è un esempio di una richiesta di log in data 21/10/2011 tra le 09:00:00 e le 09:30:00 (nel formato 24 ore). Questo output viene inserito nel file 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
```

Inviare il file di output (C:/router_output.txt) a Cisco per la risoluzione dei problemi, se necessario.

SIP (Gateway Traces)

Questi comandi attivano la traccia sui server 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:** Qualsiasi modifica apportata al software di produzione Cisco IOS® GW potrebbe causare un'interruzione delle attività.

Si tratta di una piattaforma molto solida in grado di gestire i debug consigliati sul volume di chiamata fornito senza problemi. Tuttavia, Cisco consiglia di:

- Inviare tutti i registri a un server syslog anziché al buffer di registrazione:

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

- Applicare i comandi di debug uno alla volta e controllare l'utilizzo della CPU dopo ciascuno di essi:

```
show proc cpu hist
```

Nota: Se l'utilizzo della CPU raggiunge il 70-80%, il rischio di un impatto sui servizi correlati alle prestazioni aumenta notevolmente. Pertanto, non abilitare i debug aggiuntivi se il GW raggiunge il 60%.

Abilita questi debug:

```
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
```

Dopo aver effettuato la chiamata e aver simulato il problema, interrompere il debug:

```
#undebug all
```

Raccogli questo output:

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

Traccia CUSP

Questi comandi attivano la traccia SIP su Cisco Unified SIP Proxy (CUSP):

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

Ricordarsi di disattivare la registrazione al termine dell'operazione.

In questa procedura viene descritto come raccogliere i log:

1. Configurare un utente sulla CUSP (ad esempio, test).

2. Aggiungere questa configurazione al prompt CUSP:

```
username <userid> create
```

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

3. FTP all'indirizzo IP CUSP. Utilizzare il nome utente (test) e la password definiti nel passaggio precedente.

4. Cambiare directory in /cusp/log/trace.

5. Ottenere log_<nomefile>.

Uso della CLI per il trace

In UCCE release 8 e successive, è possibile utilizzare l'interfaccia della riga di comando (CLI) del sistema unificato per raccogliere le tracce. Rispetto alle utility dumplog, la CLI è un metodo molto veloce ed efficiente per ottenere un intero set di log da un server come PG o Rogger.

In questa procedura viene descritto come avviare l'analisi dei problemi e come determinare quale analisi abilitare. Nell'esempio vengono raccolti i registri dai seguenti server:

- ROUTER-A/ROUTER-B
- LOGGER-A/LOGGER-B
- PGXA/PGXB
- Tutti i server di chiamata CVP
- Tutti i server VXML/Media CVP (se presenti)

1. Su ciascun sistema dell'elenco, aprire Unified System CLI su ciascun server ed eseguire questo comando:

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

   Sostituire la prima stringa *mm-gg-aaaa:hh:mm* con una data e un'ora che precedono di circa 15 minuti l'evento.

   Sostituire la seconda stringa *mm-gg-aaaa:hh:mm* con una data e un'ora che corrispondono a circa 15 minuti dopo la risoluzione dell'evento. Se l'evento si verifica ancora, raccoglierne almeno 15 minuti.Viene creato un file denominato clioutputX.zip, dove X è il numero successivo nella sequenza.

2. Esportare i registri di sistema di Windows Application/Security/System in formato CSV (Comma-Separated Values) e salvarli nella directory C:\Temp.

3. Aggiungere i registri CSV di Windows al file zip dal passaggio 1 e rinominare il file zip nel formato seguente:

   <NOMESERVER>-SystCLILogs-EvntOn-AAAAMMGG_HHMMSS.zip

4. Su qualsiasi PG agente, raccogliere i log nella directory C:\Program Files\Cisco\Desktop\logs ogni volta che viene rilevato l'errore. Comprimere i log in un file con un nome nel formato seguente:

<NOMESERVER>-CADLogs-EventOn-AAAMMGG_HHMMSS.zip

Se si utilizza CAD-Browser Edition (CAD-BE) o qualsiasi prodotto Web CAD, raccogliere i log dalla directory C:\Program Files\Cisco\Desktop\Tomcat\logs e aggiungerli allo stesso file zip.

Se si esegue su uno dei prodotti Windows 2008 x64, la directory di registro si trova in C:\Program Files (x86)\Cisco\Desktop\.

5. Allegare questi file alla richiesta di assistenza o caricare i file su FTP se sono troppo grandi per essere inviati tramite e-mail o allegati.

Raccogliere queste informazioni aggiuntive, se possibile:

- Ora di inizio e di fine dell'evento.
- Diversi esempi di ANI/DNIS/AgentID coinvolti nell'evento. Come minimo, Cisco ha bisogno di almeno uno di questi per vedere l'evento.
- RouteCallDetail (RCD) e TerminationCallDetail (TCD) per il periodo di tempo relativo all'evento. Query su CD:
  SELECT * FROM Route_Call_Detail WHERE DbDateTime > 'AAAA-MM-GG HH:MM:SS.MMM' and DbDateTime < 'AAAA-MM-GG HH:MM:SS.MMM'Query TCD:
  SELECT * FROM Termination_Call_Detail WHERE DbDateTime > 'AAAA-MM-GG HH:MM:SS.MMM' and DbDateTime < 'AAAA-MM-GG HH:MM:SS.MMM'

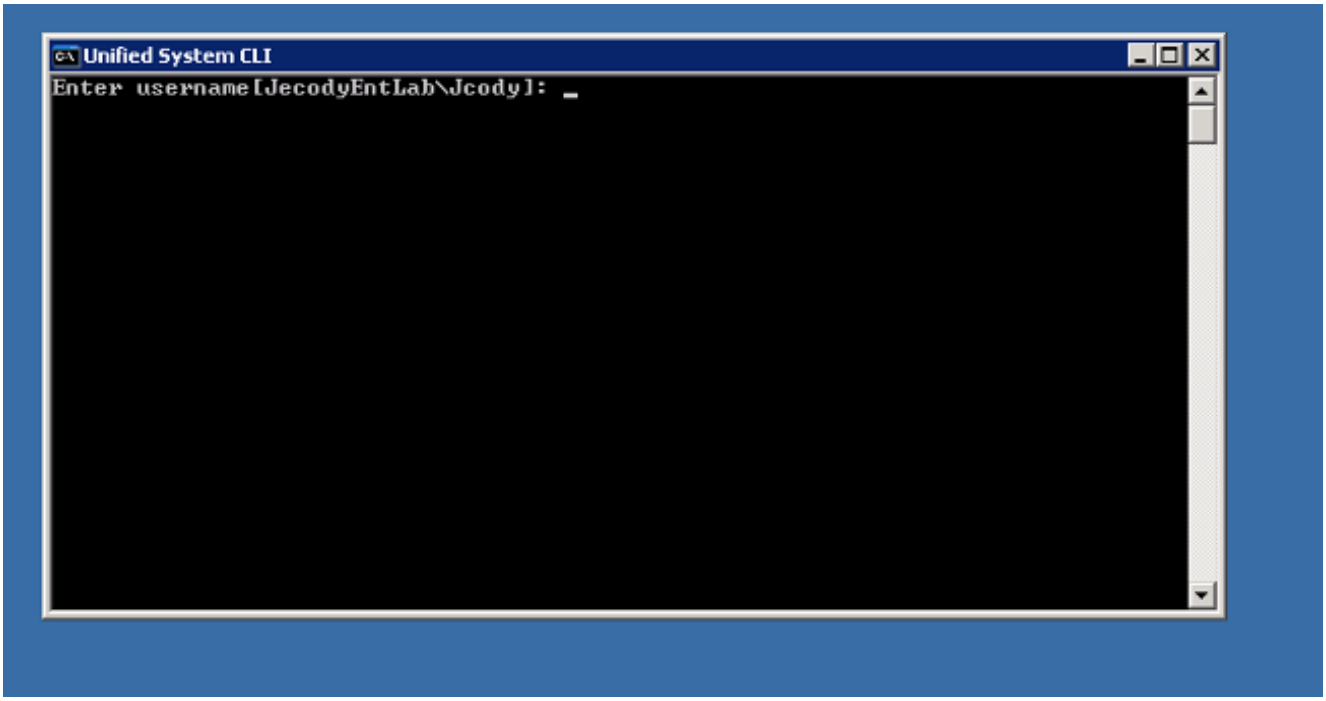
Esempio di CLI

Nota: Viene visualizzato un messaggio di avvertenza che avvisa che queste azioni potrebbero influire sul sistema, pertanto è consigliabile eseguire questa operazione durante gli orari non lavorativi o in un orario lento.

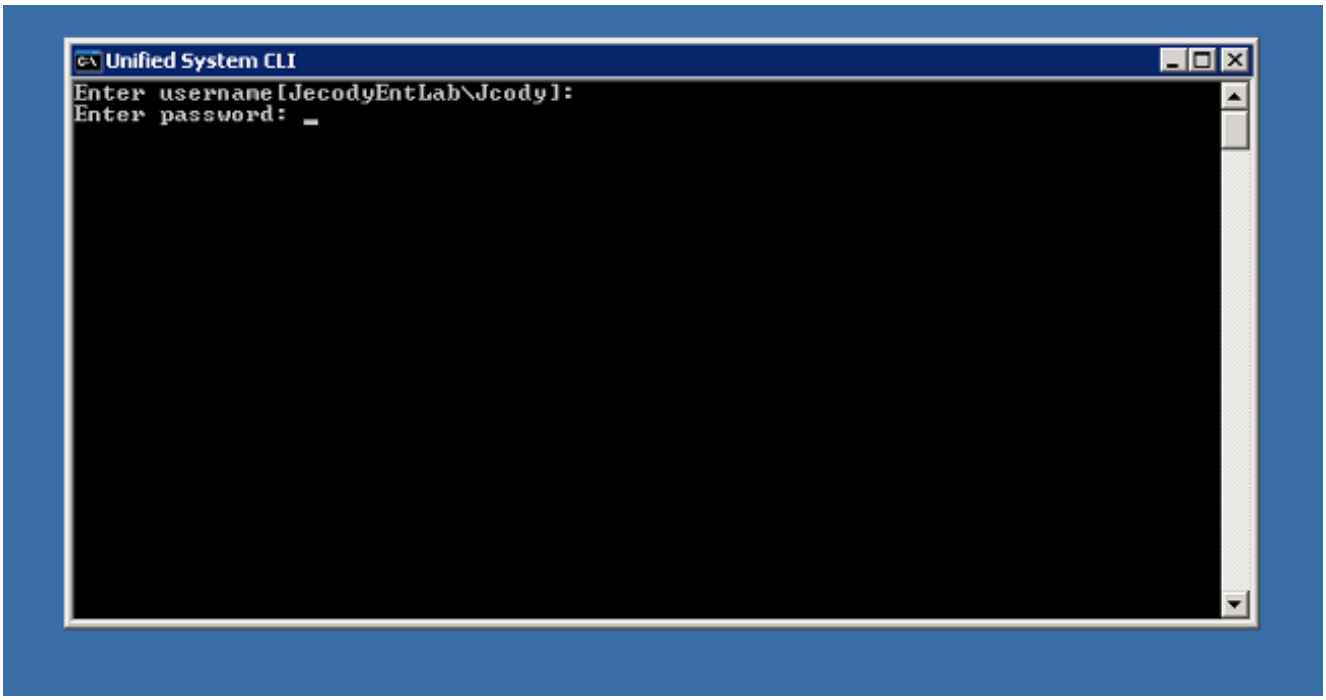
Sono disponibili due strumenti: uno strumento di Diagnostic Framework e uno strumento CLI di sistema. Entrambe sono icone sul desktop o nella directory Programmi di ciascun server.

In questa procedura viene descritto come utilizzare la CLI di Unified System per il trace.

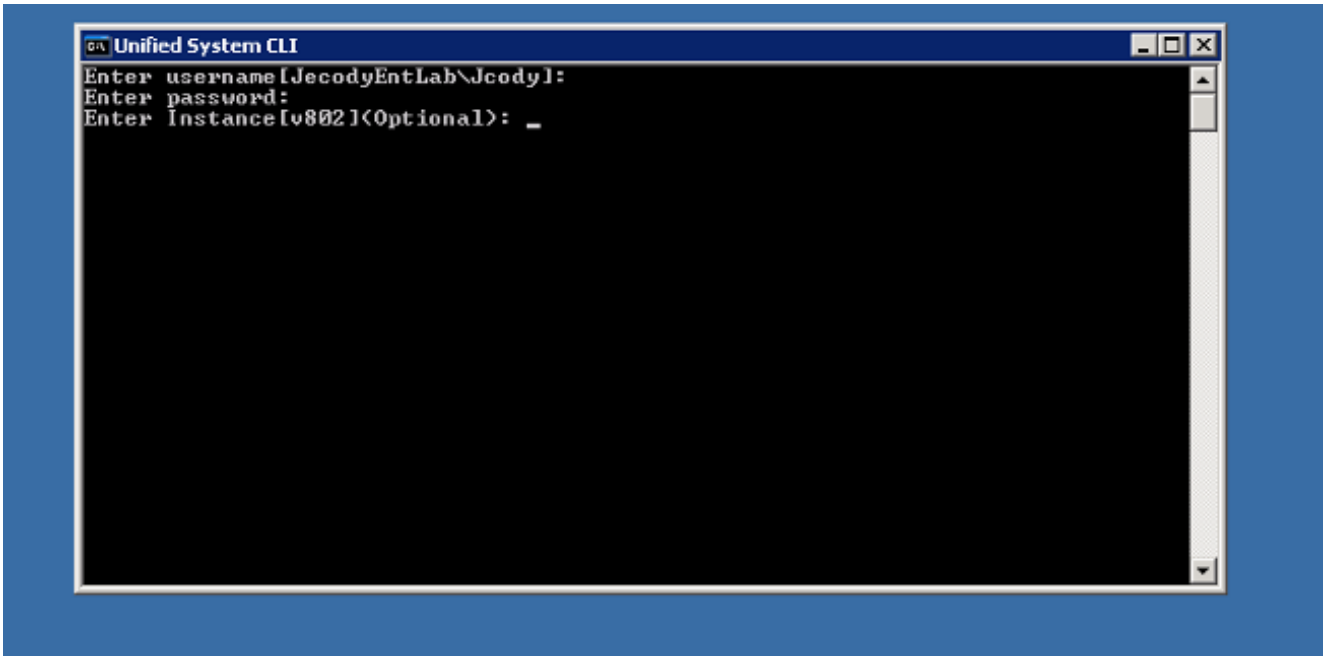
1. Fare clic sull'icona della CLI di Unified System, quindi accedere con il dominio e il nome utente. In questo esempio, l'amministratore del dominio ha già eseguito l'accesso in precedenza, quindi la CLI conosce già il dominio (JecodyEntLab) e il nome utente (Jcody).



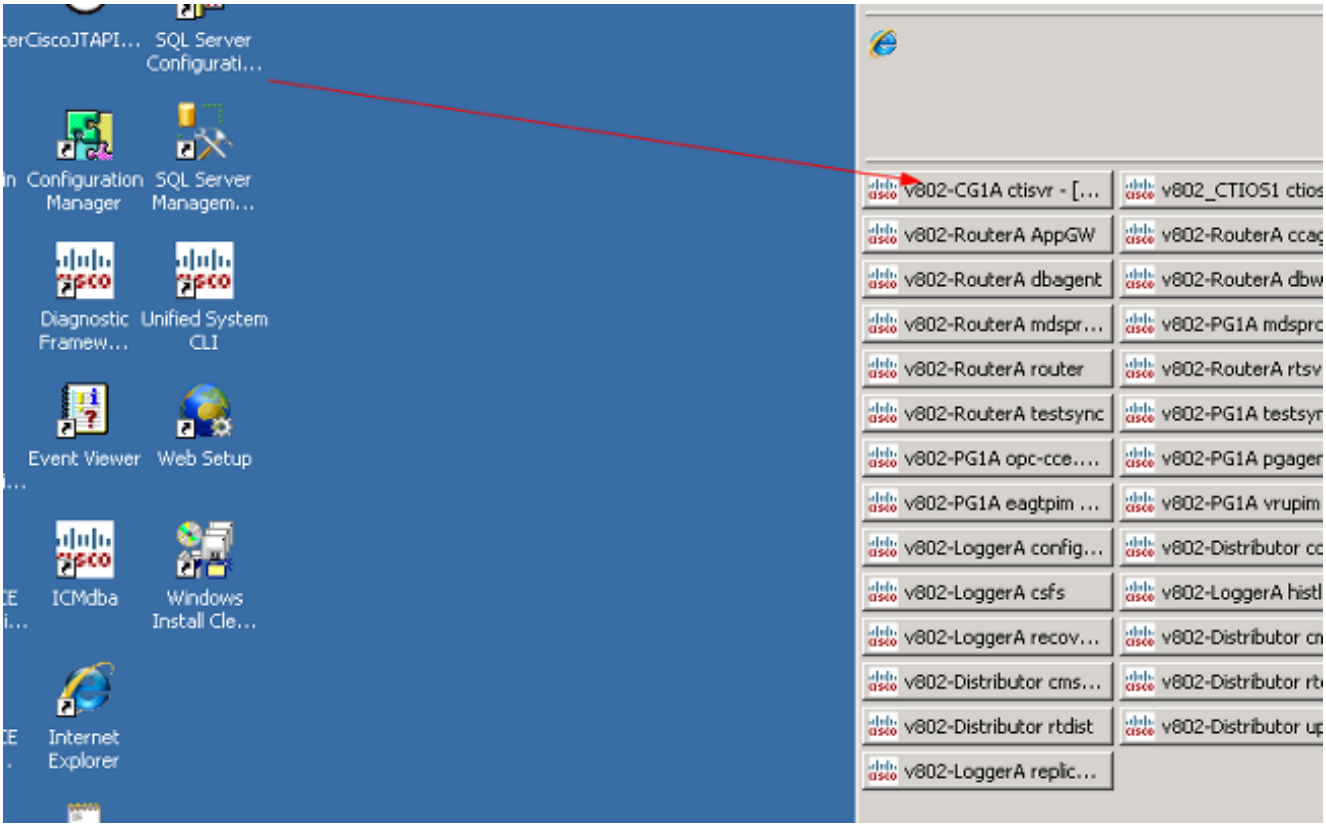
2. Immettere la password.



3. Immettere il nome dell'istanza; in questo esempio, è v802. Osservare il PG in uno dei servizi; il nome dell'istanza è la prima parte del nome del servizio.



4. Un modo semplice per trovare il nome dell'istanza consiste nell'esaminare i servizi in esecuzione sul server.



5. Dopo aver visualizzato il messaggio di benvenuto, immettere questo comando:

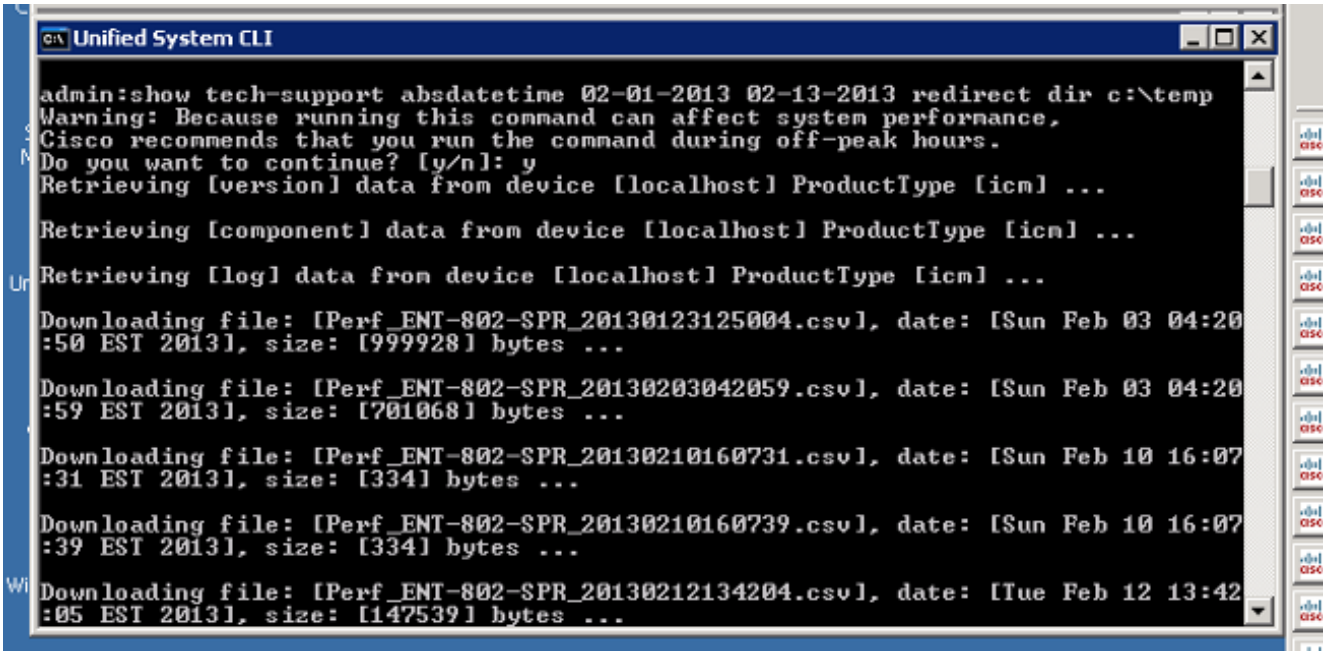
`show tech-support absdatetime` *`mm-dd-yyyy:hh:mm`* *`mm-dd-yyyy:hh:mm`* `redirect dir c:\temp`
Sostituire la prima stringa *mm-gg-aaaa:hh:mm* con una data e un'ora che precedono di circa 15 minuti l'evento.

Sostituire la seconda stringa *mm-gg-aaaa:hh:mm* con una data e un'ora che corrispondono a

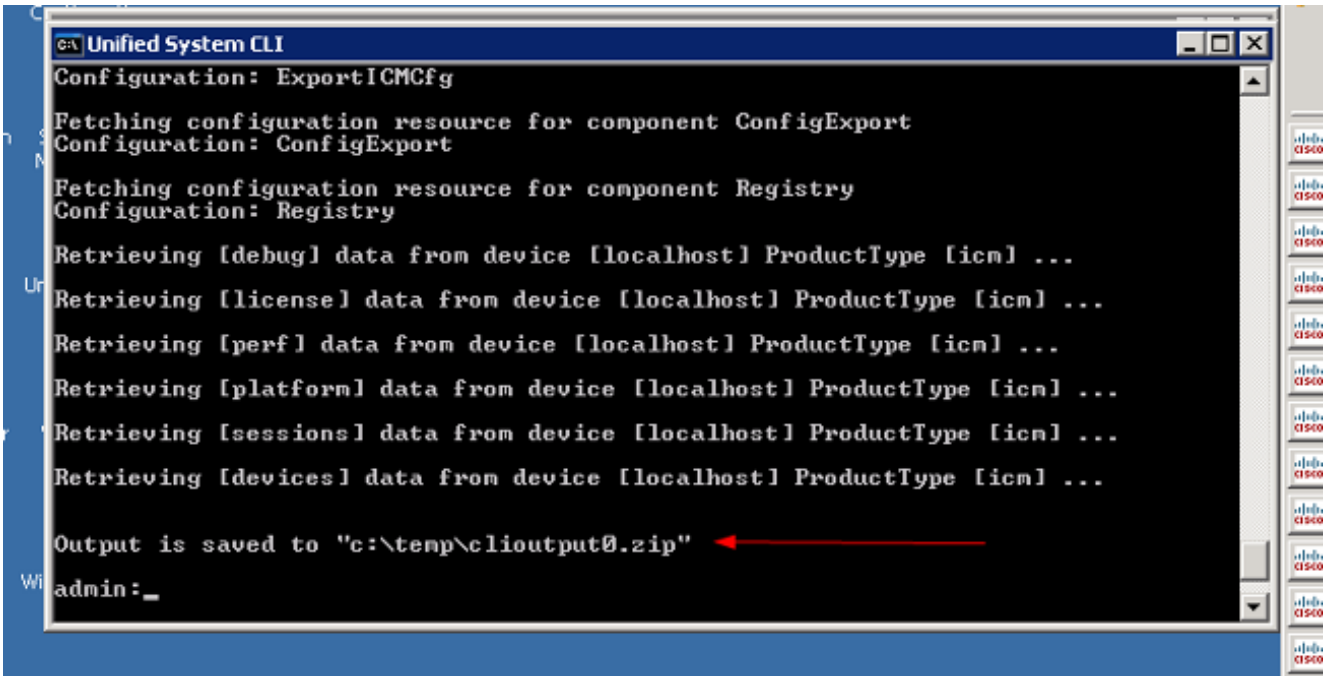
circa 15 minuti dopo la risoluzione dell'evento.

Se l'evento si verifica ancora, raccoglierne almeno 15 minuti.

Viene creato un file denominato *clioutputX*.zip, dove *X* è il numero successivo nella sequenza.

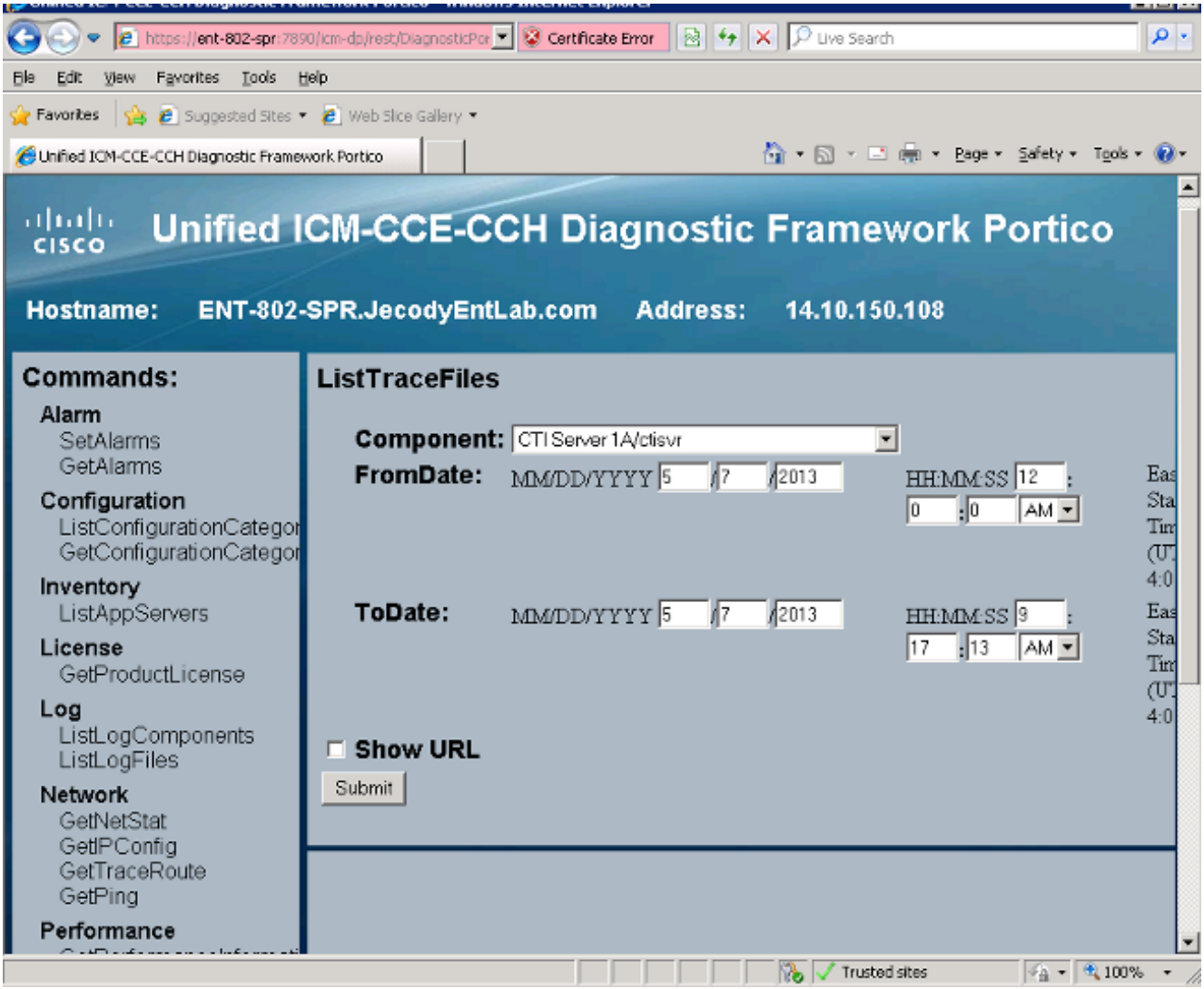


6. Una volta completato il processo, cercare il file *clioutputX*.zip nella directory:



Nota: Questo file è in genere molto grande perché contiene tutti i file relativi a UCCE per tutti i servizi sul server.

7. Se è necessario un solo log, potrebbe essere più semplice utilizzare l'utilità dumplog meno recente o utilizzare il Portico di Diagnostic Framework:


Certificate Error
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
Unified ICM-CCE-CCH Diagnostic Framework Portico
Page Safety Tools
Unified ICM-CCE-CCH Diagnostic Framework Portico
Hostname: ENT-802-SPR.JecodyEntLab.com Address: 14.10.150.108
Commands:
Alarm
SetAlarms
GetAlarms
Configuration
ListConfigurationCategor
GetConfigurationCategor
Inventory
ListAppServers
License
GetProductLicense
Log
ListLogComponents
ListLogFiles
Network
GetNetStat
GetIPConfig
GetTraceRoute
GetPing
Performance
ListTraceFiles
Component: CTI Server 1A/ctisvr
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%