Festlegen und Sammeln von UCCE-Ablaufverfolgungsprotokollen

Inhalt

[Einführung](#)
[Anforderungen](#)
[Ablaufverfolgungseinstellungen und Protokollerfassung](#)
[Finesse](#)
[Cisco Agent Desktop](#)
[Cisco Supervisor Desktop](#)
[CTIOS-Client-Desktops](#)
[Clientbezogene Probleme bei der Nachverfolgung und Anmeldung bei PG](#)
[Debuggen des CAD-Synchronisierungsdiensts](#)
[Debuggen des CAD 6.0(X) RASCAL-Servers](#)
[Debug-Chat-Server](#)
[Weitere PG-bezogene Ablaufverfolgung und Protokolle](#)
[Aktivieren der Ablaufverfolgung von CallManager PIM](#)
[Aktivieren der Ablaufverfolgung auf dem CUCM](#)
[Java Telefony Application Programming Interface (JTAPI) Gateway (JGW) aktivieren](#)
[Aktivieren der CTISVR-Tracing auf aktiver Seite](#)
[Aktivieren von Tracing VRU PIM](#)
[Aktivieren der CTIOS-Serververfolgung auf beiden CTIOS-Servern](#)
[Aktivieren der OPC-Ablaufverfolgung (Open Peripheral Controller) auf aktivem PG](#)
[Aktivieren der Eagtpim-Ablaufverfolgung auf aktivem PG](#)
[Verwenden des Dumplog-Dienstprogramms zum Abrufen von Protokollen](#)
[Tracing auf CVP-Server aktivieren](#)
[Verfolgen von ausgehenden Dialern und Erfassen von Protokollen](#)
[Pull-Protokolle](#)
[Einführer](#)
[Im Kampagnen-Manager](#)
[Routerprotokolle beim Routerprozess aktivieren](#)
[Pull-Router-Protokolle](#)
[Gateway Traces (SIP)](#)
[CUSP-Ablaufverfolgung](#)
[Verwendung der CLI für die Ablaufverfolgung](#)
[CLI-Beispiel](#)

Einführung

In diesem Dokument wird beschrieben, wie die Ablaufverfolgung in Cisco Unified Contact Center Enterprise (UCCE) für Clients, Peripheriegerät-Services (PG), das Cisco Customer Voice Portal (CVP), der Cisco UCCE Outbound Dialer, Cisco Unified Communications Manager (CallManager) (CUCM) und Cisco Gateways eingerichtet werden.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Ablaufverfolgungseinstellungen und Protokollerfassung

Hinweise:

Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.

Finesse

Melden Sie sich mit der Secure Shell (SSH) beim Finesse-Server an, und geben Sie diese Befehle ein, um die erforderlichen Protokolle zu sammeln. Sie werden aufgefordert, einen SSH-FTP-Server (SFTP) zu identifizieren, auf den die Protokolle hochgeladen werden.

Protokolle	**Command**
Installationsprotokolle	**Datei get install desktop-install.log**
Desktop-Protokolle	**Datei erhalten activelog Desktop wird komprimiert**
Serverprotokolle	**file get activelog platform/log/servm*.* komprimieren**
Plattform-Tomcat-Protokolle	**file get activelog tomcat/logs recurs komprimieren**
VOS-Installationsprotokolle (Voice Operating System)	**file get install install install.log**

Cisco Agent Desktop

In dieser Prozedur wird beschrieben, wie Sie Debugdateien erstellen und sammeln:

1. Öffnen Sie auf dem Agent-Computer die Datei C:\Program Files\Cisco\Desktop\Config directory and open the Agent.cfg.

2. Ändern Sie den Debugschwellenwert von OFF in **DEBUG**. TRACE kann für eine tiefere Ebene verwendet werden.

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

3. Größe = 3000000 (sechs Nullen) einstellen.

4. Speichern Sie die Konfigurationsdatei.

5. Stoppen Sie das Agent-Programm.

6. Löschen Sie alle Dateien im Ordner C:\Program Files\Cisco\Desktop\log directory.

7. Starten Sie das Agent-Programm, und erstellen Sie das Problem neu.

8. Diese Debugdateien werden erstellt und in C:\Program Files\Cisco\Desktop\log:

   agent0001.dbgctiosclientlog.xxx.log

Cisco Supervisor Desktop

In dieser Prozedur wird beschrieben, wie Sie Debugdateien erstellen und sammeln:

1. Öffnen Sie auf dem Agent-Computer die Datei C:\Program Files\Cisco\Desktop\Config directory and open the supervisor.cfg.

2. Ändern Sie den Debug-SCHWELLENWERT von OFF in **DEBUG**. TRACE kann für eine tiefere Ebene verwendet werden.

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

3. Größe = 3000000 (sechs Nullen) einstellen.

4. Speichern Sie die Konfigurationsdatei.

5. Stoppen Sie das Agent-Programm.

6. Löschen Sie alle Dateien im Ordner C:\Program Files\Cisco\Desktop\log directory.

7. Starten Sie das Agent-Programm, und erstellen Sie das Problem neu. Eine Debugdatei namens supervisor0001.dbg wird erstellt und in C:\Program Files\Cisco\Desktop\log abgelegt.

CTIOS-Client-Desktops

Verwenden Sie auf dem Client-PC, auf dem der CTIOS-Client installiert ist, Regedt32, um die Ablaufverfolgung zu aktivieren. Ändern Sie diese Einstellungen:

Version	Registrierungsort	Standardwert	Ändern
Versionen vor 7.x	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0 x 07	Erhöhen Sie den Wert auf 0xfff.
Version 7.x und höher	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS Tracing	0x40000307	Legen Sie für die Fehlerbehebung den Wert 0xfff fest.

Die Standardausgabe wird erstellt und in einer Textdatei mit dem Namen CtiosClientLog im Ordner c:\Program Files\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\ install directory.

Clientbezogene Probleme bei der Nachverfolgung und Anmeldung bei PG

Debuggen des CAD-Synchronisierungsdiensts

Dies sind die Einstellungen zum Debuggen des CAD Sync Service:

Einstellung	Wert
Konfigurationsdatei	DirAccessSynSvr.cfg
Standard-Speicherort	C:\Program Files\Cisco\Desktop\config
Allgemeine Fragen	Grenzwert=DEBUG
Ausgabedateien	DirAccessSynSvr.log

Debuggen des CAD 6.0(X) RASCAL-Servers

Dies sind die Einstellungen zum Debuggen des CAD 6.0(X) RASCAL-Servers:

Einstellung	Wert
Konfigurationsdatei	FCRasSvr.cfg
Standard-Speicherort	C:\Program Files\Cisco\Desktop\config
Allgemeine Fragen	Bereich = 1-4, 50, 3000-8000
LDAP-bezogene Probleme:	Bereich = 4000-4999
LRM-bezogene Probleme:	Bereich = 1999-2000
Datenbankbezogene Probleme	Bereich = 50-59
Ausgabedateien	FCRasSvr.log, FCRasSvr.dbg

Standard-Speicherort	C:\Program Files\Cisco\Desktop\log

Debug-Chat-Server

Dies sind die Einstellungen zum Debuggen des Chat-Servers:

Einstellung	Wert
Konfigurationsdatei	FCCServer.cfg
Standard-Speicherort	C:\Program Files\Cisco\Desktop\config
Allgemeine Fragen	Grenzwert=DEBUG
Ausgabedateien	FCCServer.log, FCCServer.dbg
Standard-Speicherort	C:\Program Files\Cisco\Desktop\log

Weitere PG-bezogene Ablaufverfolgung und Protokolle

Siehe Verwenden des Dumping-Dienstprogramms zum Abrufen von Protokollen für die Protokollsammlung.

Aktivieren der Ablaufverfolgung von CallManager PIM

Verwenden Sie das Dienstprogramm für die Prozessüberwachung (procmon), um die Ablaufverfolgungsebenen ein- und auszuschalten. Diese Befehle aktivieren die CallManager-PIM-Ablaufverfolgung:

```
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
```

Mit diesem Befehl von procmon wird die CallManager-PIM-Ablaufverfolgung deaktiviert:

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

Aktivieren der Ablaufverfolgung auf dem CUCM

In diesem Verfahren wird beschrieben, wie die CUCM-Ablaufverfolgung aktiviert wird:

1. Rufen Sie Call Manager Unified Serviceability auf.
2. Wählen Sie **Nachverfolgung/Konfiguration aus**.
3. Wählen Sie **CM Services aus**.
4. Wählen Sie **CTIManager (Aktiv)**.

5. Wählen Sie in der rechten oberen Ecke **SDL Configuration aus**.

6. Aktivieren Sie alles außer "Pretty Print of SDL Trace" deaktivieren.

7. Belassen Sie die Anzahl der Dateien und deren Größe bei den Standardwerten.

8. Erfassen Sie im Real-Time Monitoring Tool (RTMT) Cisco Call Manager und Cisco Computer Telefony Integration (CTI) Manager. Beide verfügen über Protokolle der Systemdiagnose-Schnittstellen (SDI) und der Signalverteilungsschicht (SDL).

Java Telefony Application Programming Interface (JTAPI) Gateway (JGW) aktivieren

Diese Befehle aktivieren die JGW-Ablaufverfolgung:

```
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
```

Ein Beispielbefehl ist **procmon ipcc pg1a jgw1**.

Aktivieren der CTISVR-Tracing auf aktiver Seite

In diesem Verfahren wird beschrieben, wie Sie die CTISVR-Ablaufverfolgung auf der aktiven Seite aktivieren:

1. Bearbeiten Sie mit dem Registrierungs-Editor HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a und b)\EMS\CurrentVersion\library\Processes\ctisvr.

2. Set EMSTraceMask = f8.

Aktivieren von Tracing VRU PIM

> **Hinweis:** Bei Befehlen wird Groß- und Kleinschreibung unterschieden. Der PG für die Voice Response Unit (VRU) unterscheidet sich von dem PG für Cisco CallManager (CCM).

Diese Befehle aktivieren die Ablaufverfolgung für 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
```

Mit diesem Promon-Befehl wird die VRU-PIM-Ablaufverfolgung deaktiviert:

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

Aktivieren der CTIOS-Serververfolgung auf beiden CTIOS-Servern

In diesem Verfahren wird beschrieben, wie die Ablaufverfolgung auf beiden CTIOS-Servern aktiviert wird:

1. Notieren Sie sich die aktuelle Ablaufverfolgungsmaske für die spätere Verwendung.

2. Verwenden Sie den Registrierungs-Editor, um HLKM >> Software\Cisco Systems Inc.\ICM\<cust_inst\CTIOS\EMS\CurrentVersion\library\Processes\ctios zu bearbeiten.

3. Festlegen:

    - EMSTraceMask = 0x60A0F
    - EMSTraceMask kann einem dieser Werte abhängig von der Version zugewiesen werden:
        - 0x0A0F für Version 6.0 oder frühere Version
        - 0x20A0F für Version 7.0 und 7.1(1)
        - 0x60A0F ab Version 7.1(2)

Die Standard-Trace-Maske ist 0x3 in allen Versionen außer Release 7.0(0), wobei sie 0x2003 ist.

Wenn die Ablaufverfolgungsmaske einen hohen Wert (0xf oder höher) hat, wirkt sich dies erheblich auf die Leistung des CTIOS-Servers und die Anrufvervollständigungsrate aus. Legen Sie die Ablaufverfolgungsmaske nur dann auf einen hohen Wert fest, wenn Sie ein Problem debuggen. Nachdem Sie die erforderlichen Protokolle gesammelt haben, müssen Sie die Ablaufverfolgungsmaske auf den Standardwert zurücksetzen.

Legen Sie für die Fehlerbehebung für die CTIOS-Server-Ablaufverfolgungsmaske Folgendes fest:

- 0x0A0F für Version 6.0 oder frühere Version
- 0x20A0F für Version 7.0 und 7.1(1)
- 0x60A0F ab Version 7.1(2)

Aktivieren der OPC-Ablaufverfolgung (Open Peripheral Controller) auf aktivem PG

Diese opctest-Befehle aktivieren die OPC-Ablaufverfolgung auf einem aktiven PG:

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

Dies ist ein Beispiel aus einer Laborumgebung:

```
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
```

Weitere Beispiele:

```
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
```

Aktivieren der Eagtpim-Ablaufverfolgung auf aktivem PG

Diese Prokmon-Befehle aktivieren die eagtpim-Ablaufverfolgung auf einem aktiven PG:

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

Dies ist ein Beispiel aus einer Laborumgebung:

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

Verwenden des Dumplog-Dienstprogramms zum Abrufen von Protokollen

Weitere Informationen finden Sie unter Verwendung des Dumping-Dienstprogramms. Verwenden Sie den Befehl **cdlog**, um zum Verzeichnis der Protokolldateien zu gelangen, wie in diesem Beispiel gezeigt:

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

In diesen Beispielen wird veranschaulicht, wie die Ausgabe in der Standarddatei gespeichert wird. In allen Fällen können Sie */v*on verwenden, um einen bestimmten Namen für die Ausgabedatei zu definieren:

```
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
```

Tracing auf CVP-Server aktivieren

SIP

Dieses Verfahren beschreibt, wie die Ablaufverfolgung auf CVP-Servern mit der Cisco SIP IP-Telefon-Software aktiviert wird:

1. Auf den Anrufservern rufen Sie das CVP-Diagnose-Tool (http://localhost(CallServer):8000/cvp/diag) auf, um den SIP-Stack (Session Initiation Protocol) aufzurufen.

2. Fügen Sie com.dynamicsoft.Dslibs.dsUAlibs mit debug hinzu.

3. Klicken Sie auf **Festlegen**.

4. Klicken Sie auf **DEBUG/41**.

H323

Dieses Verfahren beschreibt, wie die Ablaufverfolgung auf CVP-Servern mit einem H323-Gateway aktiviert wird:

1. Melden Sie sich auf den Anrufservern bei VBAdmin an.

2. Aktivieren Sie diese Ablaufverfolgungen für den CVP-Sprachbrowser:

```
setcalltrace on
setinterfacetrace on
```

Pull CVP-Protokolle von Anrufservern

Erfassen Sie die CVP *.log-Datei und die Error.log-Dateien für die Zeit des Testzeitraums. Diese Dateien befinden sich im Ordner C:\Cisco\CVP\logs directory on both CVP servers.

Dies sind die Speicherorte der Protokolldateien für Unified CVP, wobei CVP_HOME das Verzeichnis ist, in dem die Unified CVP-Software installiert wird.

Protokolltyp	Standort
Anrufserver- und/oder Reporting-Serverprotokolle	CVP_HOME\logs\
Operations Console-Protokolle	CVP_HOME\logs\OAMP\
Voice XML (VXML)-Serverprotokolle	CVP_HOME\logs\VXML\
SNMP-Agentenprotokolle (Simple Network Management Protocol)	CVP_HOME\logs\SNMP\
Unified CVP-Ressourcen-Manager-Protokolle	CVP_HOME\logs\ORM\

Ein Beispielspeicherort ist C:\Cisco\CVP.

VXML-Serverprotokolle

Bei benutzerdefinierten Sprach-XML-Anwendungen, z. B. einer bereitgestellten Audium-Anwendung, können Sie einen Debugprotokollierer aktivieren.

Fügen Sie diese Zeile dem Abschnitt <Loggers> (dem letzten Abschnitt) der Konfigurationsdatei settings.xml im Ordner C:\Cisco\CVP\VXMLServer\applications\APP_NAME\data\application\ directory:

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

Zur Laufzeit gibt diese Protokollierung ein detailliertes VoiceXML-Protokoll an \Cisco\CVP\VXMLServer\applications\APP_NAME\MyDebuggerLogger directory aus.

> **Hinweis:** Sie können den Namen der Protokollierung in der Konfigurationsdatei settings.xml von MyDebugLogger in einen beliebigen Namen ändern, den Sie auswählen.

Verfolgen von ausgehenden Dialern und Erfassen von Protokollen

Dieses Verfahren beschreibt, wie Sie die Badialprozess-Protokolle auf dem Outbound Dialer (der normalerweise auf einem PG zu finden ist) erhöhen.

1. Stellen Sie sicher, dass EMSDisplaytoScreen = 0 ist.
2. Bearbeiten Sie mit dem Registrierungs-Editor HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer.
3. Festlegen:
   - EMSTraceMask = 0xff
   - EMSUserData = ff ff (vier f s im Binärmodus)
4. Verwenden Sie den Registrierungs-Editor, um HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer zu bearbeiten.
5. Set DebugDumpAllEvents = 1.

Pull-Protokolle

Führen Sie das Dumlog-Dienstprogramm im Verzeichnis /icm/<instance>/dialer/logfiles aus:

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

Einführer

In dieser Prozedur wird beschrieben, wie das Protokoll des Importportprozesses erhöht wird.

1. Bearbeiten Sie mit dem Registrierungs-Editor HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\ baImport.

2. Festlegen:

   - EMSTraceMask = 0xff
   - EMSUserData = ff ff (vier f s im Binärmodus)

3. Führen Sie das Dumlog-Dienstprogramm im Verzeichnis /icm/<instance>/la/logfiles aus:

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

Im Kampagnen-Manager

In diesem Verfahren wird beschrieben, wie das Ereignisprotokoll für den Aktivierungsmanager erweitert wird.

1. Bearbeiten Sie mit dem Registrierungs-Editor HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager.

2. Festlegen:

   - EMSTraceMask = 0xff
   - EMSUserData = ff ff (vier f s im Binärmodus)

3. Führen Sie das Dumlog-Dienstprogramm im Verzeichnis /icm/<instance>/la/logfiles aus:

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

Verwenden Sie im Avaya Communications Manager (ACD) PG das **opctest-**Dienstprogramm, um die folgenden Werte für CallManager und Avaya zu erhöhen.

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

In diesem Verfahren wird beschrieben, wie die Ablaufverfolgung für den ctisvr-Prozess erhöht wird.

1. Bearbeiten Sie mit dem Registrierungs-Editor HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr.

2. Set EMSTraceMask = f8. Sie können den Wert bei f0 belassen, wenn Sie möchten.

Routerprotokolle beim Routerprozess aktivieren

In diesem Verfahren wird beschrieben, wie Router-Protokolle aktiviert werden:

1. Navigieren Sie auf dem Router zu **Start > Ausführen**, und geben Sie **tratrace ein**.
2. Geben Sie den Kundennamen ein.
3. Klicken Sie auf **Verbinden**.
4. Wählen Sie folgende Optionen aus:

   AgentenwechselRouteranforderungenScriptselektionNetzwerkumgebungÜbersetzungsroute AnrufwarteschlangeCalltyperezeit
5. Klicken Sie auf **Apply** (Anwenden).
6. Schließen Sie das Dienstprogramm.

Verwenden Sie stattdessen das Diagnostic Framework-Portal für opctest Version 8.5.

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

Pull-Router-Protokolle

Verwenden Sie das Dumlog-Dienstprogramm, um Router-Protokolle für den Testzeitraum von einem der Router abzurufen. Weitere Informationen finden Sie unter Verwendung des Dumping-Dienstprogramms.

Dies ist ein Beispiel für eine Protokollanforderung für Protokolle am 21.10.2011 zwischen 09:00:00 und 09:30:00 Uhr (im 24-Stunden-Format). Diese Ausgabe geht an die Datei 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
```

Senden Sie die Ausgabedatei (C:/router_output.txt) zur Fehlerbehebung an Cisco (falls erforderlich).

Gateway Traces (SIP)

Diese Befehle aktivieren die Ablaufverfolgung auf CVP-Servern mit 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
```

Hinweis: Jede Änderung eines Cisco IOS® Software-GW in der Produktion kann zu einem Ausfall führen.

Dies ist eine sehr robuste Plattform, die die vorgeschlagenen DebuggingInnen beim bereitgestellten Anrufvolumen problemlos verarbeiten kann. Cisco empfiehlt jedoch Folgendes:

- Senden Sie alle Protokolle an einen Syslog-Server statt an den Protokollierungspuffer:

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

- Wenden Sie die Debugbefehle nacheinander an, und überprüfen Sie die CPU-Auslastung nach jedem der folgenden Schritte:

```
show proc cpu hist
```

Hinweis: Wenn die CPU eine CPU-Auslastung von bis zu 70-80 % erreicht, erhöht sich das Risiko leistungsbedingter Servicebeeinträchtigungen erheblich. Aktivieren Sie daher keine zusätzlichen Debuggen, wenn der GW 60 % erreicht.

Aktivieren Sie diese Debugger:

```
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
```

Nachdem Sie den Anruf getätigt und das Problem simuliert haben, beenden Sie das Debuggen:

```
#undebug all
```

Erfassen Sie diese Ausgabe:

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

CUSP-Ablaufverfolgung

Diese Befehle aktivieren die SIP-Ablaufverfolgung auf dem Cisco Unified SIP Proxy (CUSP):

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

Vergessen Sie nicht, sich abzumelden, sobald Sie fertig sind.

In diesem Verfahren wird beschrieben, wie die Protokolle erfasst werden:

1. Konfigurieren Sie einen Benutzer auf dem CUSP (z. B. Test).

2. Fügen Sie diese Konfiguration an der CUSP-Eingabeaufforderung hinzu:

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

3. FTP an die CUSP-IP-Adresse Verwenden Sie den Benutzernamen (Test) und das Kennwort wie im vorherigen Schritt definiert.

4. Ändern Sie Verzeichnisse in /cusp/log/trace.

5. Rufen Sie das Protokoll_<Dateiname> ab.

Verwendung der CLI für die Ablaufverfolgung

In UCCE Release 8 und höher können Sie die Unified System Command-Line Interface (CLI) verwenden, um Ablaufverfolgungen zu erfassen. Im Vergleich zu Dumlog-Dienstprogrammen ist die CLI eine sehr schnelle und effiziente Methode, um einen ganzen Satz von Protokollen von einem Server wie einem PG oder Rogger zu erhalten.

In diesem Verfahren wird beschrieben, wie Sie die Problemanalyse starten und festlegen, welche Ablaufverfolgung aktiviert werden soll. Im Beispiel werden Protokolle von folgenden Servern gesammelt:

- ROUTER-A/ROUTER-B
- LOGGER-A/LOGGER-B
- PGXA/PGXB
- Alle CVP-Anrufserver
- Alle CVP VXML-/Medienserver (falls vorhanden)

1. Öffnen Sie auf jedem System in der Liste auf jedem Server die Unified System CLI, und führen Sie den folgenden Befehl aus:

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

   Ersetzen Sie die erste *mm-tt-jjjj:hh:mm*-Zeichenfolge durch ein Datum und eine Uhrzeit, die etwa 15 Minuten vor der Veranstaltung liegt.

   Ersetzen Sie die zweite *mm-tt-jjjj:hh:mm*-Zeichenfolge durch ein Datum und eine Uhrzeit, die ungefähr 15 Minuten nach dem Auflösen des Ereignisses beträgt. Wenn das Ereignis noch eintritt, sammeln Sie mindestens 15 Minuten.Dadurch wird eine Datei mit dem Namen clioutputX.zip erstellt, wobei X die nächste laufende Nummer ist.

2. Exportieren Sie die Windows-Anwendungs-/Sicherheits-/Systemprotokolle jedes Systems im CSV-Format (Comma-Separated Values), und speichern Sie sie im Ordner C:\Temp

directory.

3. Fügen Sie die Windows CSV-Protokolle aus Schritt 1 zur Zip-Datei hinzu, und benennen Sie die ZIP-Datei in diesem Format um:

   <SERVERNAME>-SystCLILogs-EventOn-YYYMMDD_HHMMSS.zip

4. Sammeln Sie auf jedem Agenten-PG die Protokolle im Verzeichnis C:\Program Files\Cisco\Desktop\logs every time the failure is seen. Kopieren Sie die Protokolle in eine Datei mit einem Namen in diesem Format:

   <SERVERNAME>-CADLogs-EventOn-YYYMMDD_HMMSS.zip

   Wenn Sie CAD-Browser Edition (CAD-BE) oder andere CAD-Webprodukte verwenden, sammeln Sie die Protokolle von C:\Program Files\Cisco\Desktop\Tomcat\logs directory und fügen Sie sie derselben ZIP-Datei hinzu.

   Wenn Sie mit einem der Windows 2008 x64-Produkte arbeiten, befindet sich das Protokollverzeichnis unter C:\Program Files (x86)\Cisco\Desktop\..

5. Fügen Sie diese Dateien der Serviceanfrage hinzu, oder laden Sie die Dateien auf FTP hoch, wenn sie zu groß für E-Mail oder zum Anhängen sind.

Sammeln Sie diese zusätzlichen Informationen, wenn möglich:

- Die Starts- und Stoppzeit der Veranstaltung.
- Mehrere Beispiele der an der Veranstaltung beteiligten ANI/DNIS/AgentID. Cisco benötigt mindestens eines davon, um die Veranstaltung anzuzeigen.
- Die RouteCallDetail (RCD) und TerminationCallDetail (TCD) für den Zeitraum um das Ereignis herum. Die RCD-Abfrage lautet:
  WÄHLEN SIE * VON Route_Call_Detail WHERE DbDateTime > 'YYY-MM-DD HH:MM:SS.MMM' und DbDateTime < 'YYY-MM-DD HH:MM:SS.MMM' aus.Die TCD-Abfrage lautet:
  WÄHLEN SIE * AUS Termination_Call_Detail WHERE DbDateTime > 'YYY-MM-DD HH:MM:SS.MMM' und DbDateTime < 'YYY-MM-DD HH:MM:SS.MMM' aus.

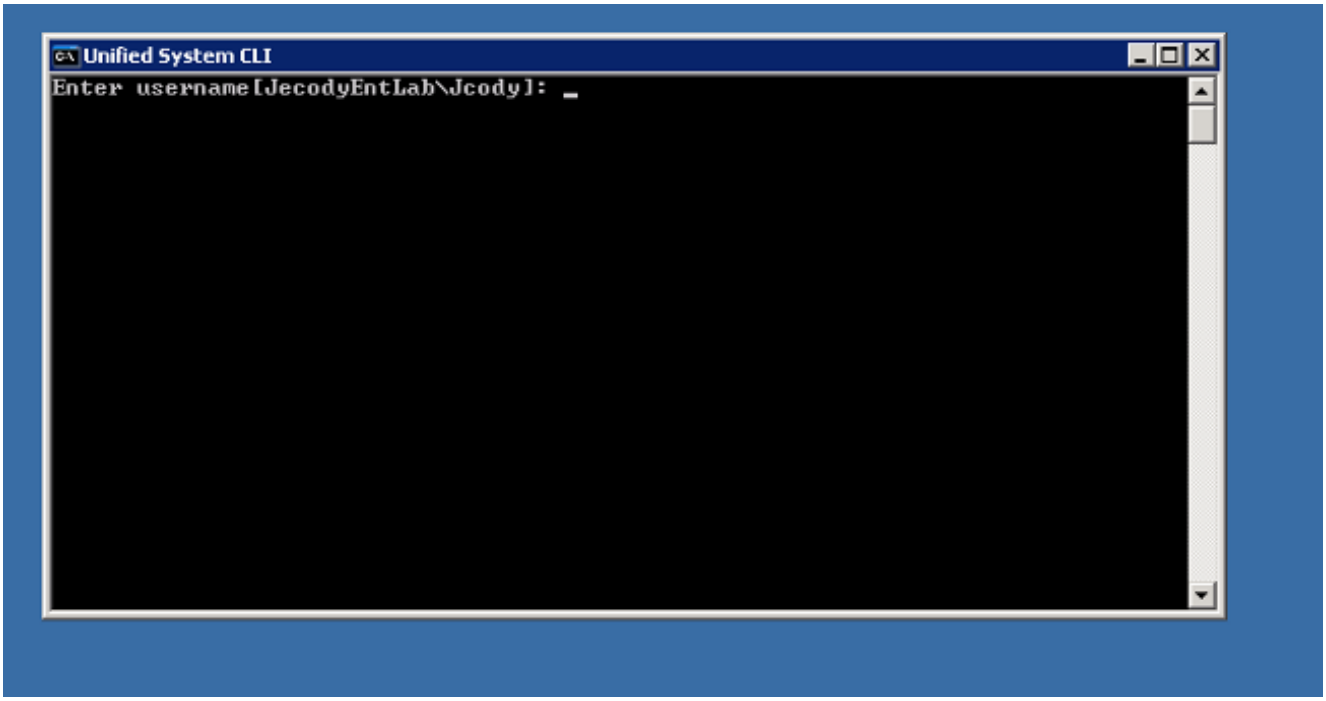
CLI-Beispiel

> **Hinweis:** Sie werden gewarnt, dass diese Aktionen Auswirkungen auf das System haben könnten. Sie sollten diese Arbeit daher außerhalb der Arbeitszeiten oder zu einem späteren Zeitpunkt durchführen.

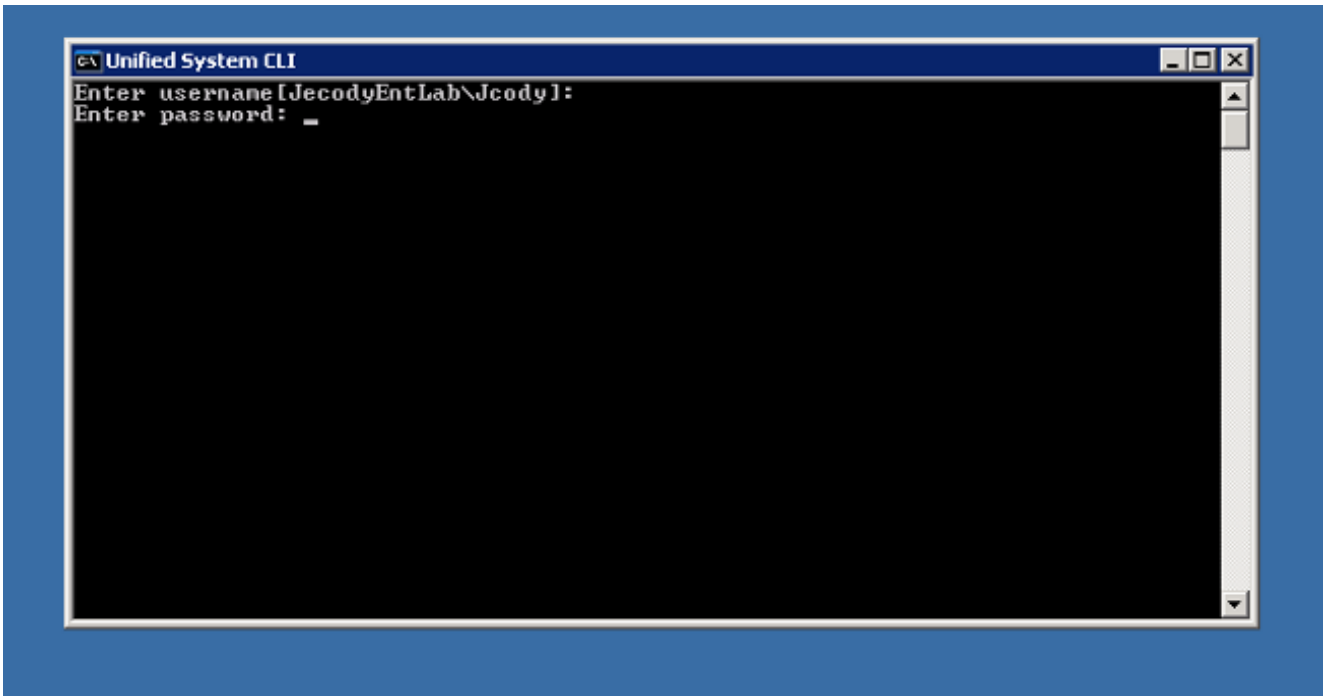
Es gibt zwei Tools: ein Diagnose-Framework-Tool und das System-CLI-Tool. Beide Symbole befinden sich entweder auf dem Desktop oder unter dem Verzeichnis Programme auf jedem Server.

In diesem Verfahren wird beschrieben, wie die Unified System-CLI für die Ablaufverfolgung verwendet wird.

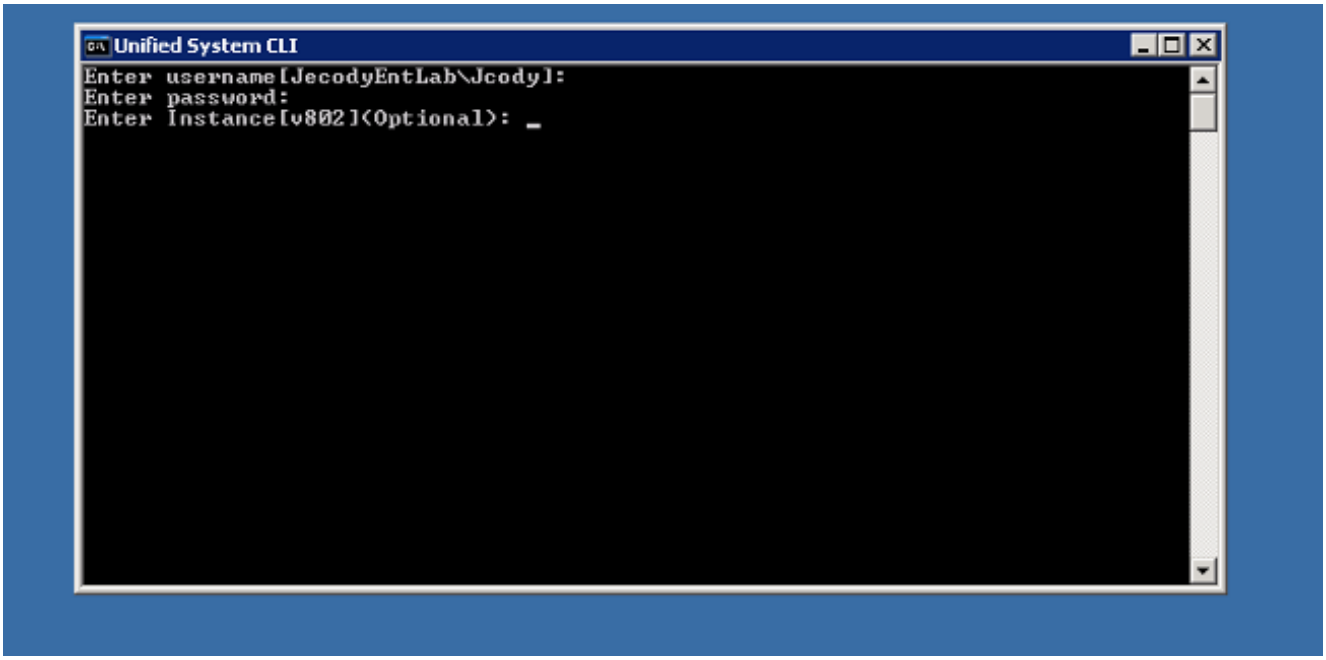
1. Klicken Sie auf das CLI-Symbol für das Unified System, und melden Sie sich mit der Domäne und dem Benutzernamen an. (In diesem Beispiel hat sich der Domänenadministrator bereits angemeldet, sodass die CLI bereits die Domäne (JecodyEntLab) und den Benutzernamen (Jcody) kennt.



2. Geben Sie das Kennwort ein.



3. Geben Sie den Instanznamen ein. in diesem Beispiel ist es v802. Suchen Sie auf der Übersetzungsdatenbank nach einem der Dienste. Der Instanzname ist der erste Teil des Dienstnamens.



4. Eine einfache Möglichkeit, den Instanznamen zu finden, besteht darin, sich die Dienste anzusehen, die auf dem Server ausgeführt werden.

5. Wenn Sie die Willkommensmeldung sehen, geben Sie den folgenden Befehl ein:

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

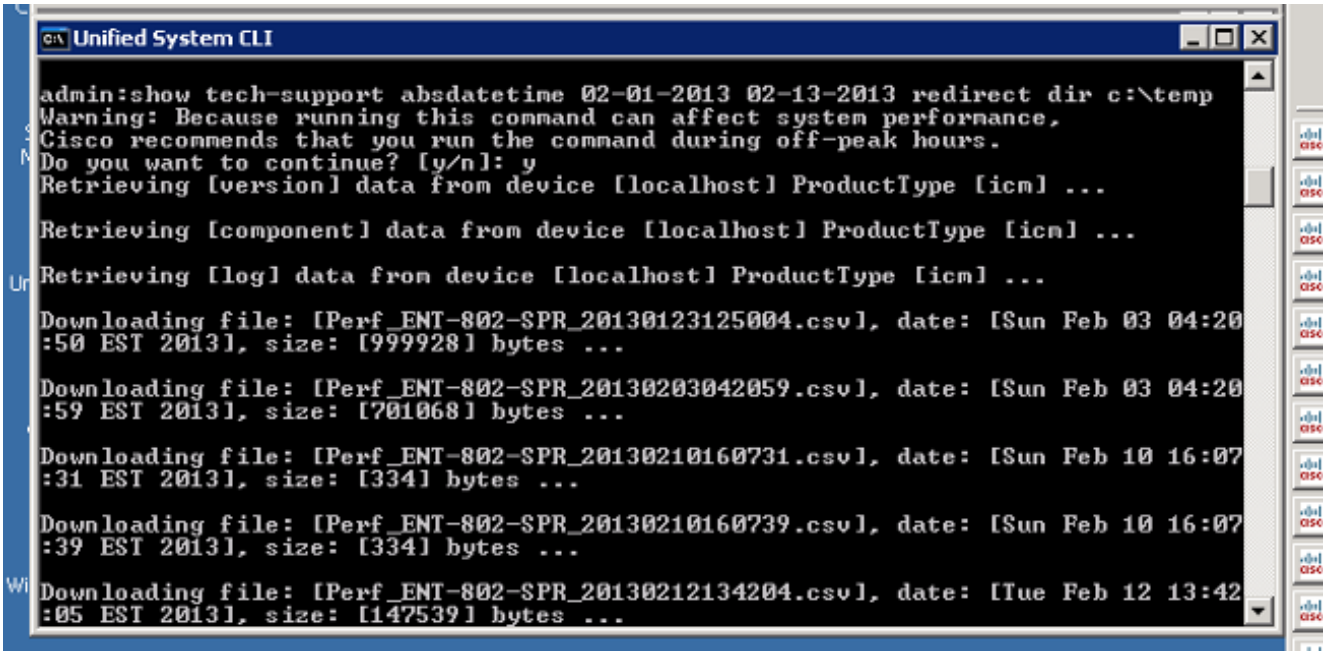
Ersetzen Sie die erste *mm-tt-jjjj:hh:mm*-Zeichenfolge durch ein Datum und eine Uhrzeit, die etwa 15 Minuten vor der Veranstaltung liegt.

Ersetzen Sie die zweite *mm-tt-jjjj:hh:mm*-Zeichenfolge durch ein Datum und eine Uhrzeit, die

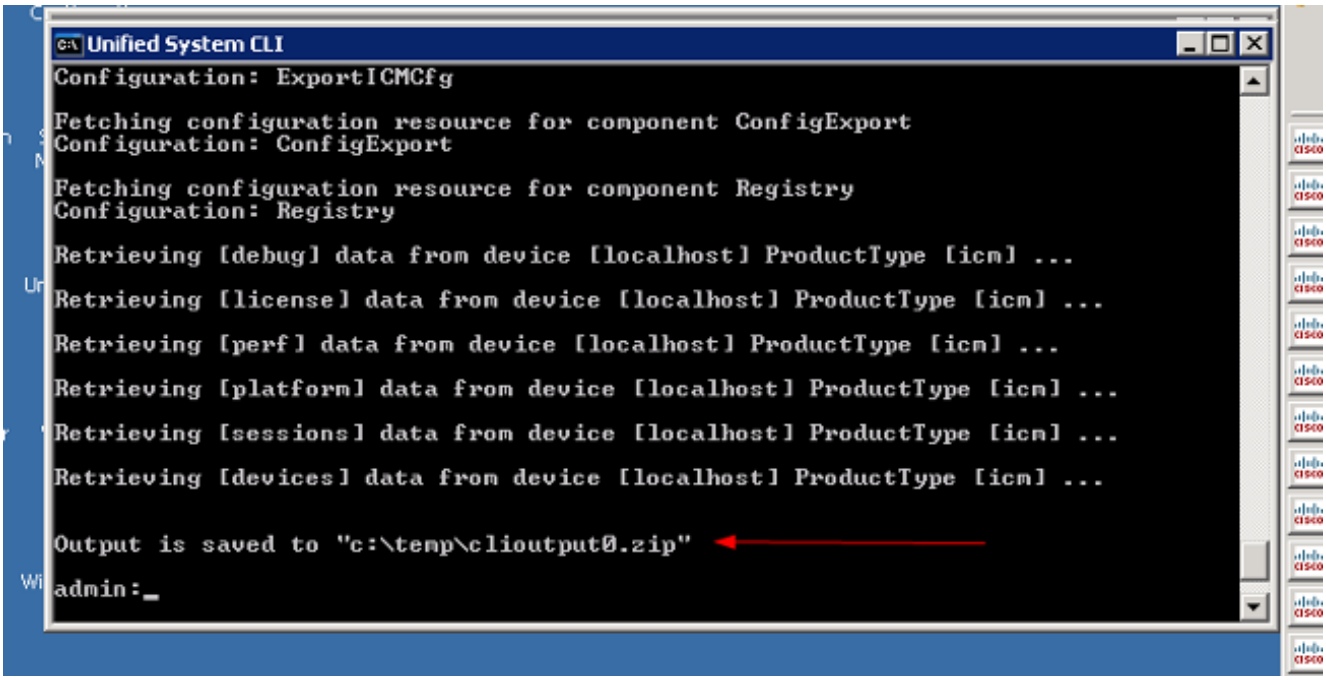
ungefähr 15 Minuten nach dem Auflösen des Ereignisses beträgt.

Wenn das Ereignis noch eintritt, sammeln Sie mindestens 15 Minuten.

Dadurch wird eine Datei mit dem Namen *clioutputX*.zip erstellt, wobei *X* die nächste Zahl in Folge ist.

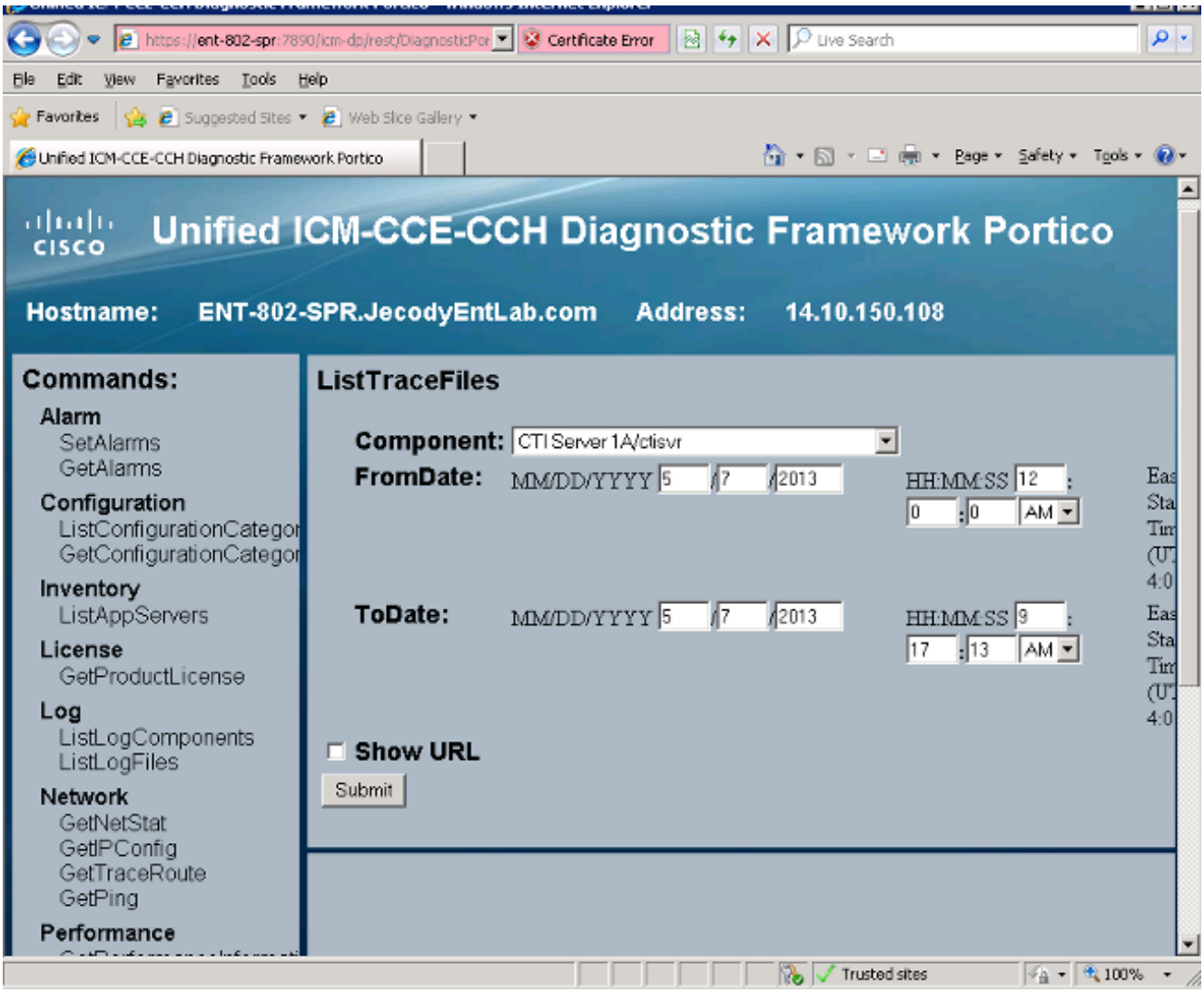


6. Wenn der Vorgang abgeschlossen ist, suchen Sie im Verzeichnis nach der Datei *clioutputX*.zip:



Hinweis: Diese Datei ist in der Regel sehr groß, da sie alle UCCE-bezogenen Dateien für alle Dienste auf diesem Server enthält.

7. Wenn Sie nur ein Protokoll benötigen, ist es möglicherweise einfacher, das ältere Dumlog-Dienstprogramm zu verwenden oder das Diagnostic Framework-Protokoll zu verwenden:


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%