UCCE 추적 로그 설정 및 수집

목차

소개

이 문서에서는 클라이언트, 주변 장치 게이트웨이(PG) 서비스, Cisco CVP(Customer Voice Portal), Cisco UCCE Outbound Dialer, Cisco Unified Communications Manager(CUCM) 및 Cisco 게이트웨

이에 대한 Cisco UCCE(Unified Contact Center Enterprise)에서 추적을 설정하는 방법에 대해 설명합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

추적 설정 및 로그 수집

> **참고:**
>
> 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.
>
> Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.
>
> **debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

Finesse

SSH(Secure Shell)로 Finesse 서버에 로그인하고 필요한 로그를 수집하기 위해 이러한 명령을 입력합니다.로그가 업로드될 SSH FTP(SFTP) 서버를 식별하라는 메시지가 표시됩니다.

로그	명령
로그 설치	**install desktop-install.log 가져오기**
데스크톱 로그	**파일 가져오기 activelog desktop recurls compress**
서버 로그	**file get activelog platform/log/servm** compress**
플랫폼 Tomcat 로그	**파일 가져오기 활성 로그 tomcat/logs 반복 압축**
VOS(Voice Operating System) 설치 로그	**install.log 가져오기**

Cisco Agent Desktop

다음 절차에서는 디버그 파일을 만들고 수집하는 방법에 대해 설명합니다.

1. 에이전트 컴퓨터에서 C:\Program Files\Cisco\Desktop\Config directory and open the

Agent.cfg 파일로 이동합니다.

2. 디버그 임계값을 OFF에서 DEBUG로 **변경합니다**.TRACE는 심층적인 수준에 사용할 수 있습니다.

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

3. Size=3000000(0 6개)을 확인합니다.

4. 구성 파일을 저장합니다.

5. 에이전트 프로그램을 중지합니다.

6. C:\Program Files\Cisco\Desktop\log directory폴더에서 모든 파일을 삭제합니다.

7. 에이전트 프로그램을 시작하고 문제를 다시 만듭니다.

8. 이러한 디버그 파일은 C:\Program Files\Cisco\Desktop\log에 만들어 배치됩니다.

   agent0001.dbgctiosclientlog.xxx.log

Cisco Supervisor Desktop

다음 절차에서는 디버그 파일을 만들고 수집하는 방법에 대해 설명합니다.

1. 에이전트 컴퓨터에서 C:\Program Files\Cisco\Desktop\Config directory and open the supervisor.cfg 파일로 이동합니다.

2. 디버그 임계값을 OFF에서 DEBUG로 **변경합니다**.TRACE는 심층적인 수준에 사용할 수 있습니다.

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

3. Size=3000000(0 6개)을 확인합니다.

4. 구성 파일을 저장합니다.

5. 에이전트 프로그램을 중지합니다.

6. C:\Program Files\Cisco\Desktop\log directory폴더에서 모든 파일을 삭제합니다.

7. 에이전트 프로그램을 시작하고 문제를 다시 만듭니다.이름이 supervisor0001.dbg인 디버그 파일이 생성되어 C:\Program Files\Cisco\Desktop\log에 배치됩니다.

CTIOS 클라이언트 데스크톱

CTIOS 클라이언트가 설치된 클라이언트 PC에서 추적을 설정하려면 Regedt32를 사용합니다.다음 설정을 변경합니다.

릴리스	레지스트리 위치	기본값	변경
7.x 이전 릴리스	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0x07	값을 0xfff로 높입니다.
릴리스 7.x 이상	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS 추적	0x40000307	문제 해결을 위해 값을 0xfff로 설정합니다.

기본 출력은 c:\Program Files\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\ install directory디렉터리에 있는 CtiosClientLog라는 텍스트 파일에 만들어지고 배치됩니다.

PG의 추적 및 로그와 관련된 클라이언트 관련 문제

CAD 동기화 서비스 디버그

다음은 CAD 동기화 서비스를 디버깅하는 설정입니다.

설정	가치
구성 파일	디렉토리 액세스SynSvr.cfg
기본 위치	C:\Program Files\Cisco\Desktop\config
일반 문제	임계값=디버그
출력 파일	디렉토리 액세스SynSvr.log

CAD 6.0(X) RASCAL 서버 디버그

다음은 CAD 6.0(X) RASCAL 서버를 디버깅하는 설정입니다.

설정	가치
구성 파일	FCRasSvr.cfg
기본 위치	C:\Program Files\Cisco\Desktop\config
일반 문제	범위 = 1-4, 50, 3000-8000
LDAP 관련 문제:	범위 = 4000-4999
LRM 관련 문제:	범위 = 1999-2000
데이터베이스 관련 문제	범위 = 50-59
출력 파일	FCRasSvr.log, FCRasSvr.dbg
기본 위치	C:\Program Files\Cisco\Desktop\log

채팅 서버 디버그

다음은 채팅 서버를 디버깅하는 설정입니다.

설정	가치
구성 파일	FCCServer.cfg

기본 위치	C:\Program Files\Cisco\Desktop\config
일반 문제	임계값=디버그
출력 파일	FCCServer.log, FCCServer.dbg
기본 위치	C:\Program Files\Cisco\Desktop\log

기타 PG 관련 추적 및 로그

로그 수집을 위해 휴지통 유틸리티를 사용하여 로그를 폴기를 참조하십시오.

CallManager PIM 추적 사용

추적 수준을 켜거나 끄려면 프로세스 모니터링(procmon) 유틸리티를 사용합니다.다음 명령은 PIM(CallManager 주변 장치 인터페이스 관리자) 추적을 설정합니다.

```
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
```

이 procmon 명령은 CallManager PIM 추적을 끕니다.

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

CUCM에서 추적 사용

다음 절차에서는 CUCM 추적을 설정하는 방법에 대해 설명합니다.

1. Call Manager Unified Serviceability로 이동합니다.
2. Trace/**Configuration을 선택합니다**.
3. CM **Services(CM 서비스)를 선택합니다**.
4. CTIManager**(Active)를 선택합니다**.
5. 오른쪽 상단에서 SDL **Configuration을 선택합니다**.
6. Disable Pretty Print of SDL Trace(SDL 추적 예쁜 인쇄 비활성화)를 제외한 모든 항목을 활성화합니다.
7. 파일 수와 파일 크기를 기본값으로 둡니다.
8. RTMT(Real-Time Monitoring Tool)에서 Cisco Call Manager 및 Cisco CTI(Computer Telephony Integration) Manager를 수집합니다.둘 다 SDI(시스템 진단 인터페이스) 및 SDL(신호 분산 레이어) 로그를 가지고 있습니다.

JTAPI(Java Telephony Application Programming Interface) 게이트웨이(JGW) 활성화

다음 procmon 명령은 JGW 추적을 설정합니다.

```
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
```

명령 예는 procmon ipcc **pg1a jgw1입니다**.

활성 쪽에서 CTISVR(CTI Server) 추적 사용

이 절차에서는 활성 측에서 CTISVR 추적을 활성화하는 방법에 대해 설명합니다.

1. HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a 및 b)\EMS.\CurrentVersion\library\Processes\ctisvr을 편집하려면 레지스트리 편집기를 사용하십시오.

2. EMSTraceMask = f8을 설정합니다.

추적 VRU PIM 사용

> **참고:**명령은 대/소문자를 구분합니다.VRU(Voice Response Unit) PG가 CCM(Cisco CallManager) PG와 다릅니다.

다음 procmon 명령은 VRU PIM에 대한 추적을 설정합니다.

```
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
```

이 procmon 명령은 VRU PIM 추적을 끕니다.

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

두 CTIOS 서버에서 CTIOS 서버 추적 활성화

이 절차에서는 두 CTIOS 서버에서 추적을 활성화하는 방법에 대해 설명합니다.

1. 나중에 사용할 수 있도록 현재 추적 마스크를 기록해 둡니다.

2. 레지스트리 편집기를 사용하여 HLKM >> Software\Cisco Systems Inc.\ICM\<cust_inst\CTIOS\EMS.\CurrentVersion\library\Processes\ctios을 편집합니다.

3. 설정:

   - EMSTraceMask = 0x60A0F
   - 릴리스에 따라 EMSTraceMask가 다음 값 중 하나로 설정됩니다.
     - 릴리스 6.0 이하의 경우 0x0A0F
     - 릴리스 7.0 및 7.1(1)의 경우 0x20A0F
     - 릴리스 7.1(2) 이상용 0x60A0F

기본 추적 마스크는 Release 7.0(0)을 제외한 모든 릴리스에서 0x3이며, 여기서 0x20003입니다.

추적 마스크의 값이 높은 경우(0xf 이상) CTIOS 서버 성능 및 통화 완료 속도에 큰 영향을 줍니다.문제를 디버깅하는 경우에만 추적 마스크를 높은 값으로 설정합니다.필요한 로그를 수집했으면 추적 마스크를 기본값으로 다시 설정해야 합니다.

문제 해결을 위해 CTIOS 서버 추적 마스크를 다음으로 설정합니다.

- 릴리스 6.0 이하의 경우 0x0A0F
- 릴리스 7.0의 경우 0x20A0F 및 7.1(1)
- 릴리스 7.1(2) 이상용 0x60A0F

활성 PG에서 OPC(Open Peripheral Controller) 추적 활성화

다음 opctest 명령은 활성 PG에서 OPC 추적을 활성화합니다.

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

다음은 랩 환경의 예입니다.

```
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
```

추가 예는 다음과 같습니다.

```
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
```

활성 PG에서 Eagtpim 추적 사용

다음 procmon 명령은 활성 PG에서 eagtpim 추적을 설정합니다.

```
C:\>procmon <cust_inst> <node> pim<pim instance
>>>>trace tp* /on
>>>trace precall /on
>>>trace *event /on
>>>trace csta* /on
```
다음은 랩 환경의 예입니다.

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

휴지통 유틸리티를 사용하여 로그 가져오기

자세한 내용은 휴지통 유틸리티 사용 방법을 참조하십시오.다음 예와 같이 logfiles 디렉토리로 이동하려면 cdlog 명령을 사용합니다.

```
c:\cdlog <customer_name> pg1a   !-- Or, pgXa to depending on the PG number (X)
c:\icm\<customer_name>\<<PG#>>\logfiles\
```
다음 예에서는 기본 파일에 출력을 배치하는 방법을 보여 줍니다.모든 경우 출력 파일의 특정 이름을 정의하기 위해 /of를 사용할 수 있습니다.

```
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
```

CVP 서버에서 추적 사용

SIP

다음 절차에서는 Cisco SIP IP Phone 소프트웨어를 사용하여 CVP 서버에서 추적을 활성화하는 방법에 대해 설명합니다.

1. 통화 서버에서 SIP(Session Initiation Protocol) 스택을 가져오려면 CVP 진단 도구 (http://localhost(CallServer):8000/cvp/diag)로 이동합니다.

2. 디버그와 함께 com.dynamicsoft.Dslibs.DsUAlibs를 추가합니다.

3. 설정**을 클릭합니다**.

4. DEBUG**/41을 클릭합니다**.

H323

다음 절차에서는 H323 게이트웨이가 있는 CVP 서버에서 추적을 활성화하는 방법에 대해 설명합니다.

1. 통화 서버에서 VBAdmin에 로그인합니다.

2. CVP 음성 브라우저에 대해 다음 추적을 활성화합니다.

```
setcalltrace on
setinterfacetrace on
```

통화 서버에서 CVP 로그 가져오기

테스트 기간 동안 CVP *.log 파일 및 Error.log 파일을 수집합니다.이러한 파일은 C:\Cisco\CVP\logs directory on both CVP servers폴더에 있습니다.

Unified CVP의 로그 파일 위치입니다. 여기서 CVP_HOME은 Unified CVP 소프트웨어가 설치된 디렉토리입니다.

로그 유형	위치
통화 서버 및/또는 보고 서버 로그	CVP_HOME\logs\
운영 콘솔 로그	CVP_HOME\logs\OAMP\
VXML(Voice XML) 서버 로그	CVP_HOME\logs\VXML\
SNMP(Simple Network Management Protocol) 에이전트 로그	CVP_HOME\logs\SNMP\
Unified CVP 리소스 관리자 로그	CVP_HOME\logs\ORM\

예제 위치는 C:\Cisco\CVP입니다.

VXML 서버 로그

배포된 Audium 응용 프로그램과 같은 사용자 지정 음성 XML 응용 프로그램의 경우 디버그 로거를 설정할 수 있습니다.

C:\Cisco\CVP\VXMLServer\applications\APP_NAME\data\application\ directory폴더에 있는 settings.xml 구성 파일의 **<loggers>** 섹션(마지막 섹션)에 이 행을 추가합니다.

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

런타임에 이 로거는 자세한 VoiceXML 로그를 \Cisco\CVP\VXMLServer\applications\APP_NAME\MyDebuggerLogger directory폴더로 출력합니다.

참고:settings.xml 구성 파일의 로거 이름을 MyDebugLogger에서 선택한 이름으로 변경할 수 있습니다.

아웃바운드 다이얼러 관련 추적 및 로그 수집

이 절차에서는 아웃바운드 다이얼러(일반적으로 PG에 있음)에서 기본 프로세스 로그를 늘리는 방법에 대해 설명합니다.

1. EMSDisplaytoScreen = 0을 확인합니다.

2. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS.\CurrentVersion\Library\Processes\baDialer을 편집하려면 레지스트리 편집기를 사용하십시오.

3. 설정:

   - EMSTraceMask = 0xff
   - EMSUserData = ff(바이너리 모드의 4f)

4. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer를 편집하려면 레지스트리 편집기를 사용하십시오.

5. DebugDumpAllEvents = 1을 설정합니다.

풀 로그

/icm/<instance>/dialer/logfiles 디렉토리에서 dumplog 유틸리티를 실행합니다.

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

가져오기 도구

이 절차에서는 기본 포트 프로세스 로그를 늘리는 방법에 대해 설명합니다.

1. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS.\CurrentVersion\Library\Processes\ baImport을 편집하려면 레지스트리 편집기를 사용하십시오.

2. 설정:

   - EMSTraceMask = 0xff
   - EMSUserData = ff(바이너리 모드의 4f)

3. /icm/<instance>/la/logfiles 디렉토리에서 dumplog 유틸리티를 실행합니다.

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

캠페인 관리자

이 절차에서는 캠페인 관리자 프로세스 로그를 늘리는 방법에 대해 설명합니다.

1. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS.\CurrentVersion\Library\Processes\CampaignManager을 편집하려면 레지스트리 편집기를 사용하십시오.

2. 설정:

   - EMSTraceMask = 0xff
   - EMSUserData = ff(바이너리 모드의 4f)

3. /icm/<instance>/la/logfiles 디렉토리에서 dumplog 유틸리티를 실행합니다.

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

Avaya Communications Manager(ACD) PG에서 opctest 유틸리티를 사용하여 CallManager와 Avaya 모두에 대해 다음을 늘립니다.

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

이 절차에서는 cisvr 프로세스에 대한 추적을 늘리는 방법에 대해 설명합니다.

1. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS.\CurrentVersion\Library\Processes\ctisvr을 편집하려면 레지스트리 편집기를 사용합니다.

2. EMSTraceMask = f8을 설정합니다. 원하는 경우 값을 f0으로 유지할 수 있습니다.

라우터 프로세스에서 라우터 로그 활성화

다음 절차에서는 라우터 로그를 활성화하는 방법에 대해 설명합니다.

1. 라우터에서 **Start(시작)** > **Run(실행)**으로 이동하고 rtrtrace를 **입력합니다**.

2. 고객 이름을 입력합니다.

3. **연결**을 **클릭합니다**.

4. 다음 옵션을 선택합니다.

   에이전트 변경라우팅 요청스크립트선택됨네트워크URL추적변환경로통화 대기 calltyperealtime

5. Apply를 **클릭합니다**.

6. 유틸리티를 종료합니다.

Test Release 8.5의 경우 대신 Diagnostic Framework Portico를 사용하십시오.

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

끌어오기 라우터 로그

테스트 기간 동안 라우터에서 라우터 로그를 가져오려면 dumplog 유틸리티를 사용합니다. 자세한 내용은 휴지통 유틸리티 사용 방법을 참조하십시오.

이것은 09:00:00~09:30:00(24시간 형식)의 10/21/2011에 대한 로그 요청의 예입니다. 이 출력은 C:/router_output.txt 파일로 이동합니다.

```
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
```

필요한 경우 문제 해결을 위해 출력 파일(C:/router_output.txt)을 Cisco에 제출합니다.

게이트웨이 추적(SIP)

다음 명령은 SIP를 사용하는 CVP 서버에서 추적을 설정합니다.

```
#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
```

참고:프로덕션 Cisco IOS® 소프트웨어 GW에서 변경을 수행하면 중단이 발생할 수 있습니다.

이 플랫폼은 제공된 통화 볼륨에서 문제 없이 제안된 디버그를 처리할 수 있는 매우 강력한 플랫폼입니다.그러나 Cisco는 다음과 같은 권장 사항을 제공합니다.

- 모든 로그를 로깅 버퍼 대신 syslog 서버로 전송합니다.

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

- debug 명령을 한 번에 하나씩 적용하고 각 명령 이후의 CPU 사용률을 확인합니다.

```
show proc cpu hist
```

참고:CPU가 최대 70-80%의 CPU 사용률을 달성하면 성능 관련 서비스 영향의 위험이 크게

증가합니다.따라서 GW가 60%에 도달하면 추가 디버그를 활성화하지 마십시오.

다음 디버깅 사용:

```
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
```

통화를 하고 문제를 시뮬레이션한 후 디버깅을 중지합니다.

```
#undebug all
```

다음 출력을 수집합니다.

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

CUSP 추적

다음 명령은 Cisco Unified SIP Proxy(CUSP)에서 SIP 추적을 설정합니다.

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

완료되면 로깅을 해제하십시오.

이 절차에서는 로그를 수집하는 방법에 대해 설명합니다.

1. CUSP에서 사용자를 구성합니다(예: 테스트).
2. CUSP 프롬프트에서 이 컨피그레이션을 추가합니다.

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

3. CUSP IP 주소에 대한 FTP.이전 단계에서 정의한 대로 사용자 이름(테스트) 및 비밀번호를 사용합니다.
4. 디렉토리를 /cusp/log/trace로 변경합니다.
5. log_<filename>을(를) 가져옵니다.

추적을 위한 CLI 사용

UCCE 릴리스 8 이상에서는 추적을 수집하기 위해 Unified System CLI(Command-Line Interface)를 사용할 수 있습니다.CLI는 dumplog 유틸리티에 비해 PG 또는 Rogger와 같은 한 서버에서 전체 로그 집합을 얻는 매우 빠르고 효율적인 방법입니다.

이 절차에서는 문제 분석을 시작하는 방법과 활성화할 추적을 확인하는 방법에 대해 설명합니다.이 예에서는 다음 서버에서 로그를 수집합니다.

- ROUTER-A/ROUTER-B
- 로거-A/로거-B
- PGXA/PGXB
- 모든 CVP 통화 서버
- 모든 CVP VXML/미디어 서버(있는 경우)

1. 목록의 각 시스템에서 각 서버에서 Unified System CLI를 열고 다음 명령을 실행합니다.

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

   첫 번째 *mm-dd-yyyy:hh:mm* 문자열을 이벤트 15분 전까지의 날짜 및 시간으로 바꿉니다.

   두 번째 *mm-dd-yyyy:hh:mm* 문자열을 이벤트가 해결된 후 약 15분 이후의 날짜 및 시간으로 바꿉니다.이벤트가 계속 진행 중이면 15분 이상 수집합니다.이렇게 하면 clioutputX.zip이라는 파일이 생성됩니다. 여기서 X는 시퀀스의 다음 번호입니다.

2. 각 시스템의 Windows 애플리케이션/보안/시스템 로그를 CSV(comma-separated values) 형식으로 내보내고 C:\Temp directory폴더에 저장합니다.

3. 1단계에서 zip에 Windows CSV 로그를 추가하고 zip 파일의 이름을 다음 형식으로 바꿉니다.

   <서버 이름>-SystCLILogs-EvntOn-YYYYMMDD_HHMMSS.zip

4. 모든 에이전트 PG에서 C:\Program Files\Cisco\Desktop\logs every time the failure is seen 디렉터리에서 로그를 수집합니다.다음 형식으로 이름을 가진 파일에 로그를 압축합니다.

   <서버 이름>-CADLogs-EvntOn-YYYYMMDD_HHMMSS.zip

   CAD-BE(CAD-Browser Edition) 또는 CAD 웹 제품을 사용하는 경우 C:\Program Files\Cisco\Desktop\Tomcat\logs directory폴더에서 로그를 수집하고 동일한 zip 파일에 추가합니다.

   Windows 2008 x64 제품에서 실행 중인 경우 로그 디렉터리는 C:\Program Files (x86)\Cisco\Desktop\... 아래에 있습니다.

5. 이러한 파일을 서비스 요청에 첨부하거나, 파일이 너무 커서 이메일이나 첨부할 수 없는 경우 FTP에 업로드합니다.

가능한 경우 다음 추가 정보를 수집합니다.

- 이벤트 시작 및 중지 시간입니다.
- 이벤트와 관련된 ANI/DNIS/AgentID의 여러 샘플.Cisco는 적어도 하나 이상의 이 중 하나가 필

요합니다.

- 이벤트를 둘러싼 기간의 RCD(RouteCallDetail) 및 TCD(TerminationCallDetail)입니다. RCD 쿼리는 다음과 같습니다.
  Route_Call_Detail에서 * FROM DbDateTime > 'YYYY-MM-DD HH:MM:SS.MMM' 및 DbDateTime < 'YYYY-MM-DD HH:MM:SS.MMM'을 선택합니다.TCD 쿼리는 다음과 같습니다. DBDateTime > 'YYYY-MM-DD HH:MM:SS.MMM' 및 DbDateTime < 'YYYY-MM-DD HH:MM:SS.MMM'에서 * FROM Termination_Call_Detail을 선택합니다.

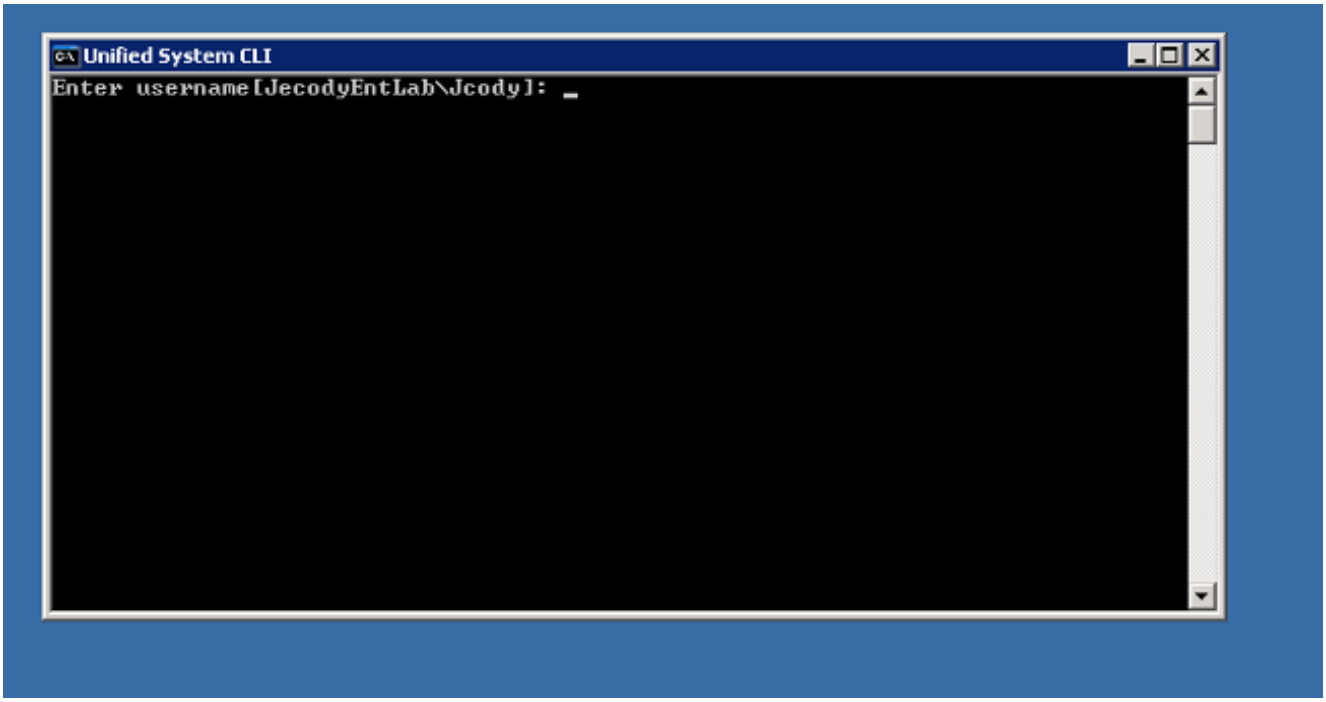
CLI 예

참고:이러한 작업이 시스템에 영향을 미칠 수 있으므로, 이 작업은 근무 외 시간 또는 느린 시간 동안 수행할 수 있습니다.

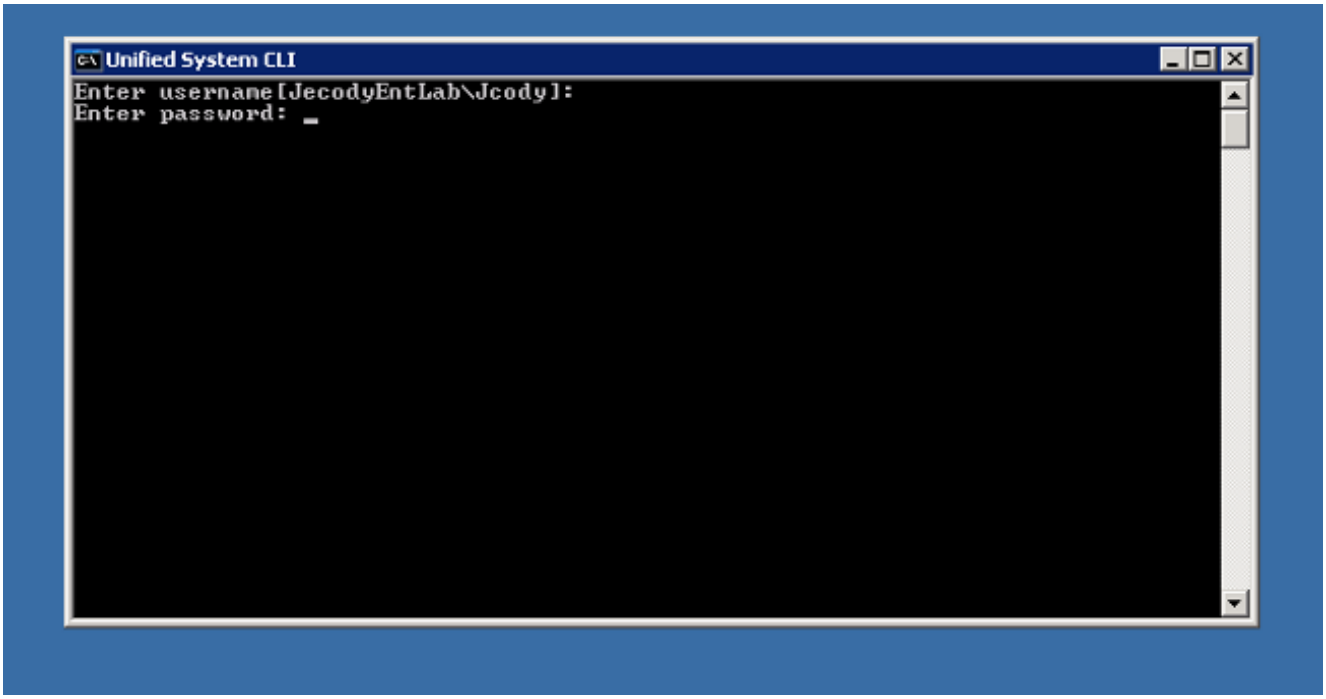
두 가지 툴이 있습니다.진단 프레임워크 툴 및 시스템 CLI 툴입니다.두 아이콘은 모두 데스크톱이나 각 서버의 Programs 디렉터리 아래에 있는 아이콘입니다.

이 절차에서는 추적을 위해 Unified System CLI를 사용하는 방법에 대해 설명합니다.

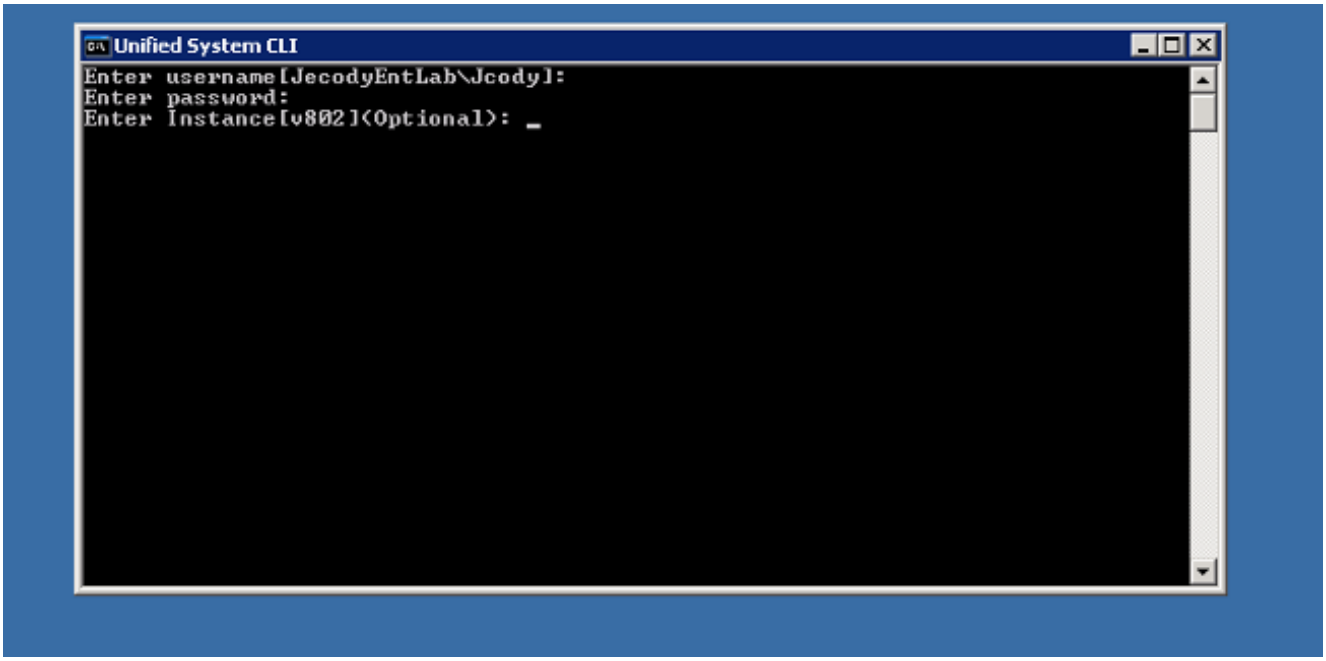
1. Unified System CLI 아이콘을 클릭한 다음 도메인 및 사용자 이름으로 로그인합니다.(이 예에서는 도메인 관리자가 이전에 로그인했으므로 CLI는 도메인(JcodyEntLab) 및 사용자 이름(Jcody)을 이미 알고 있습니다.



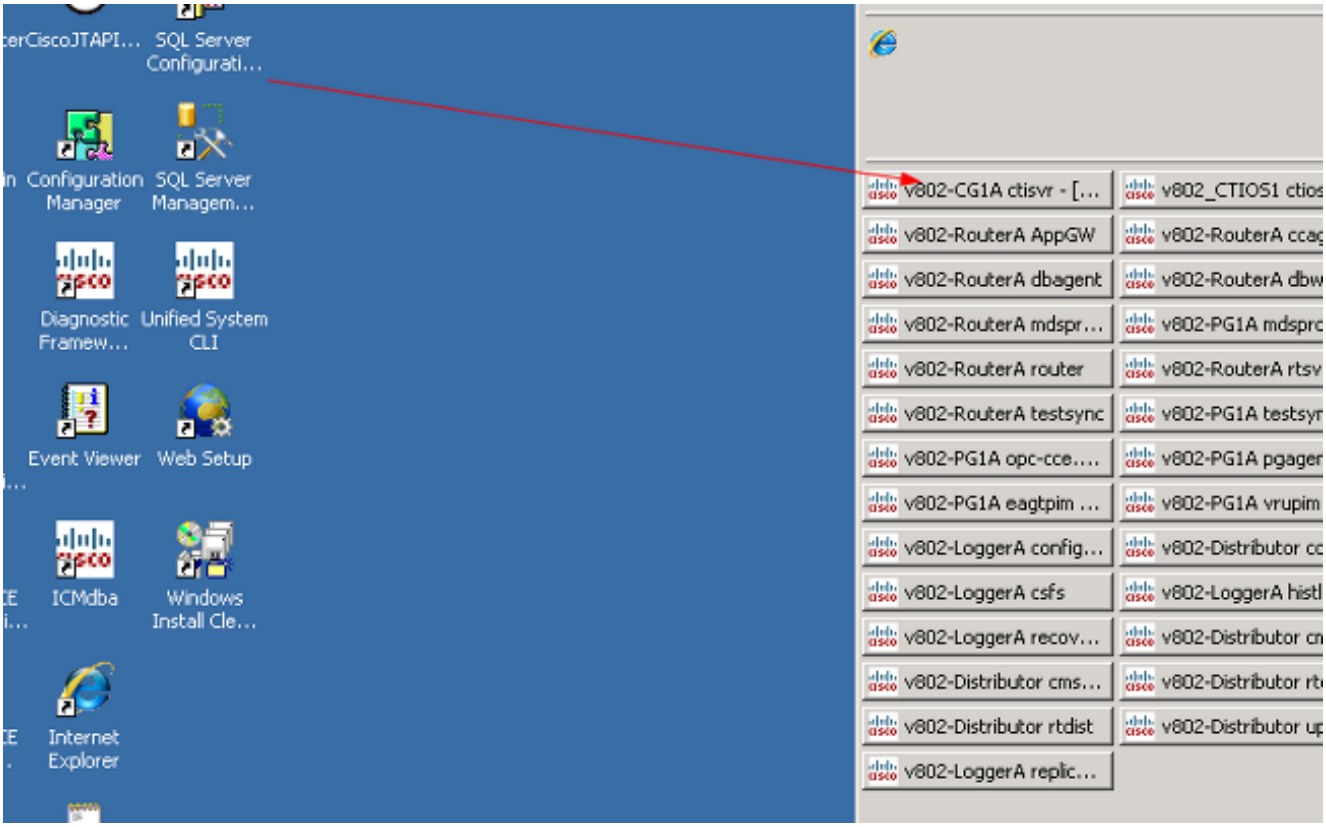
2. 비밀번호를 입력합니다.



3. 인스턴스 이름을 입력합니다.이 예에서는 v802입니다. 서비스 중 하나에서 PG를 확인합니다 .인스턴스 이름은 서비스 이름의 첫 번째 부분입니다.



4. 인스턴스 이름을 찾는 간단한 방법은 서버에서 실행 중인 서비스를 확인하는 것입니다.



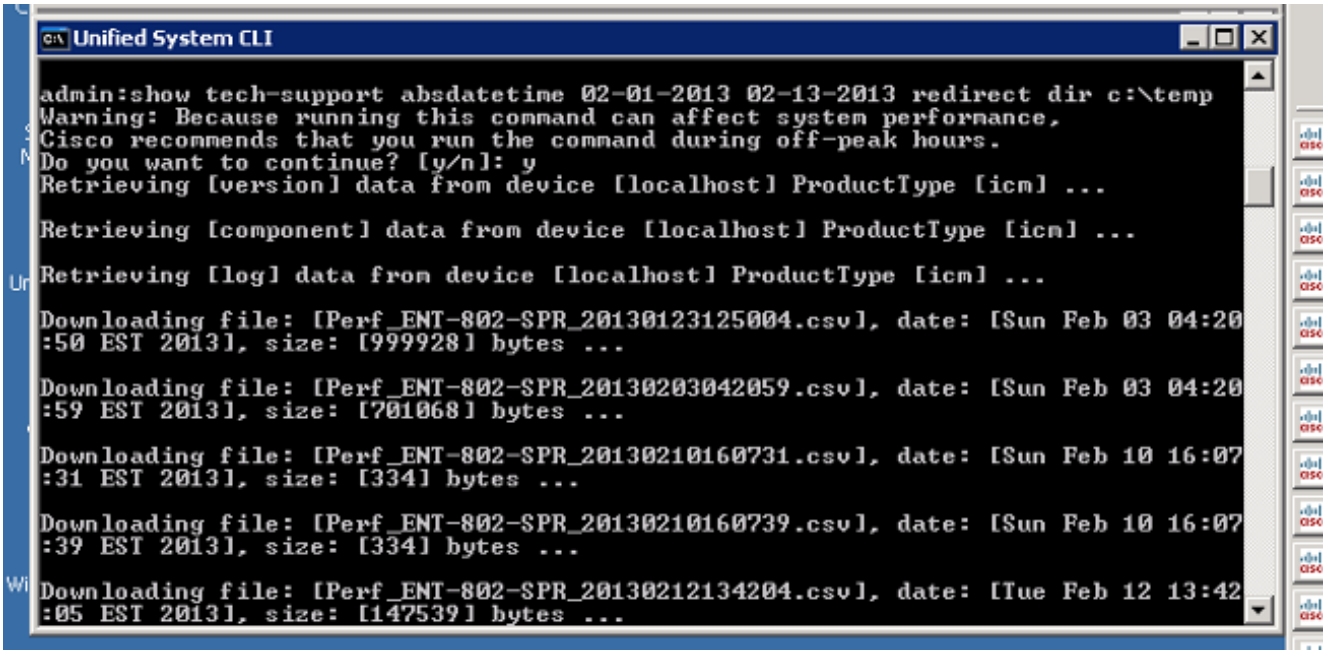
5. 시작 메시지가 표시되면 다음 명령을 입력합니다.

`show tech-support absdatetime` *`mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm`* `redirect dir c:\temp`
첫 번째 *mm-dd-yyyy:hh:mm* 문자열을 이벤트 15분 전까지의 날짜 및 시간으로 바꿉니다.

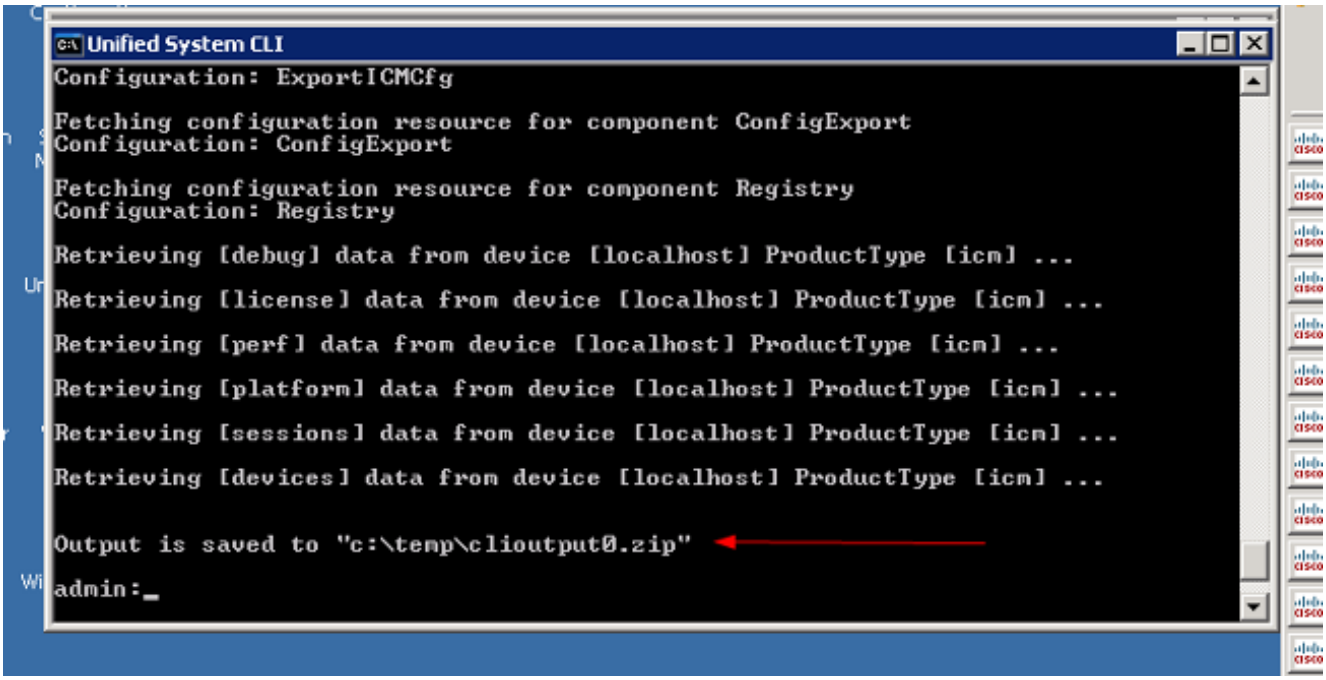
두 번째 *mm-dd-yyyy:hh:mm* 문자열을 이벤트가 해결된 후 약 15분 이후의 날짜 및 시간으로 바꿉니다.

이벤트가 계속 진행 중이면 15분 이상 수집합니다.

이렇게 하면 clioutputX.zip이라는 파일이 생성됩니다. 여기서 *X*는 시퀀스의 다음 번호입니다.

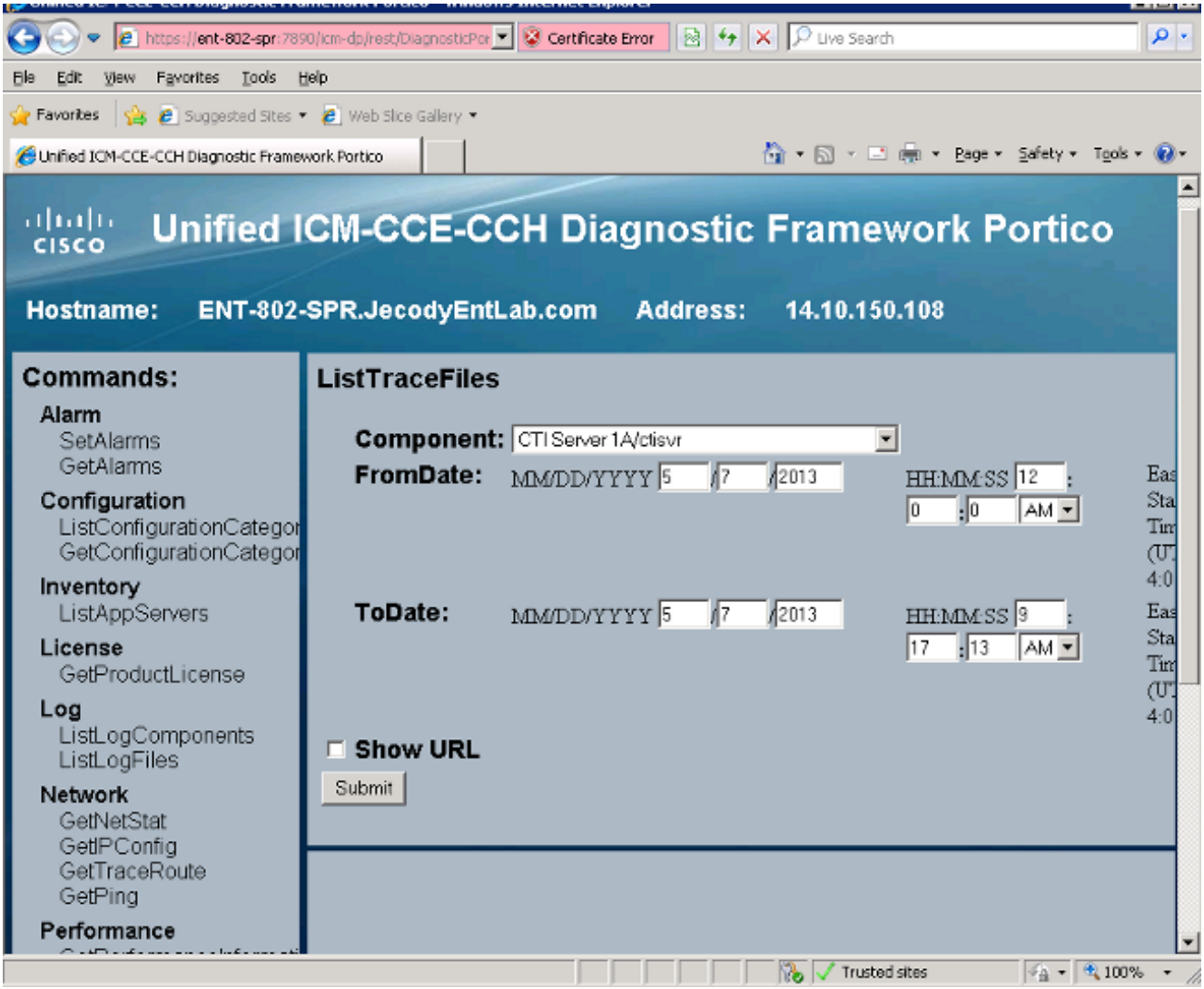


6. 프로세스가 완료되면 다음 디렉토리에서 *clioutputX*.zip 파일을 찾습니다.



참고:이 파일은 이 서버의 모든 서비스에 대한 모든 UCCE 관련 파일을 포함하므로 일반적으로 매우 큽니다.

7. 하나의 로그만 필요한 경우 이전 휴지통 로그 유틸리티를 사용하거나 진단 프레임워크 현관을 사용하는 것이 더 쉽습니다.


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%