CCE에서 추적 설정 및 로그 수집

목차

소개

이 문서에서는 Cisco Unified CCE(Contact Center Enterprise)에서 추적을 설정하고 수집하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco UCCE(Unified Contact Center Enterprise)
- PCCE(Contact Center Enterprise) 패키지
- Cisco Finesse
- Cisco CVP(Customer Voice Portal)

- Cisco VVB(Virtualized Voice Browser)
- CUBE(Cisco Unified Border Element)
- Cisco CUIC(Unified Intelligence Center)
- Cisco SIP(Unified Session Initiation Protocol) Proxy(CUSP)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Finesse 릴리스 12.5
- CVP 서버 릴리스 12.5
- UCCE/PCCE 릴리스 12.5
- Cisco VVB 릴리스 12.5
- CUIC 릴리스 12.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

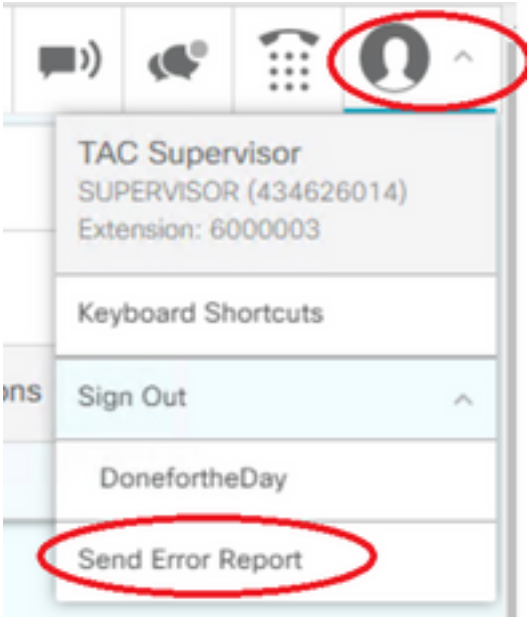
추적 설정 및 Finesse 로그 수집

Finesse 클라이언트

Finesse 클라이언트 로그를 수집하는 몇 가지 옵션이 있습니다.

옵션 1: Send Error Report(오류 보고서 보내기)를 통해 클라이언트 로그를 수집합니다.

1. 상담원을 로그인합니다.
2. 통화 또는 미디어 이벤트 중에 상담원에게 문제가 발생하는 경우, 상담원에게 finesse 데스크톱 오른쪽 상단 모서리에 있는 **Send Error Report(오류 보고서 보내기)** 링크를 클릭하도록 지시합니다.



3. 상담원은 성공적으로 **전송된 로그를 확인합니다.** 메시지.
4. 클라이언트 로그는 Finesse 서버로 전송됩니다. https://x.x.x.x/finesse/logs으로 이동하고 관리

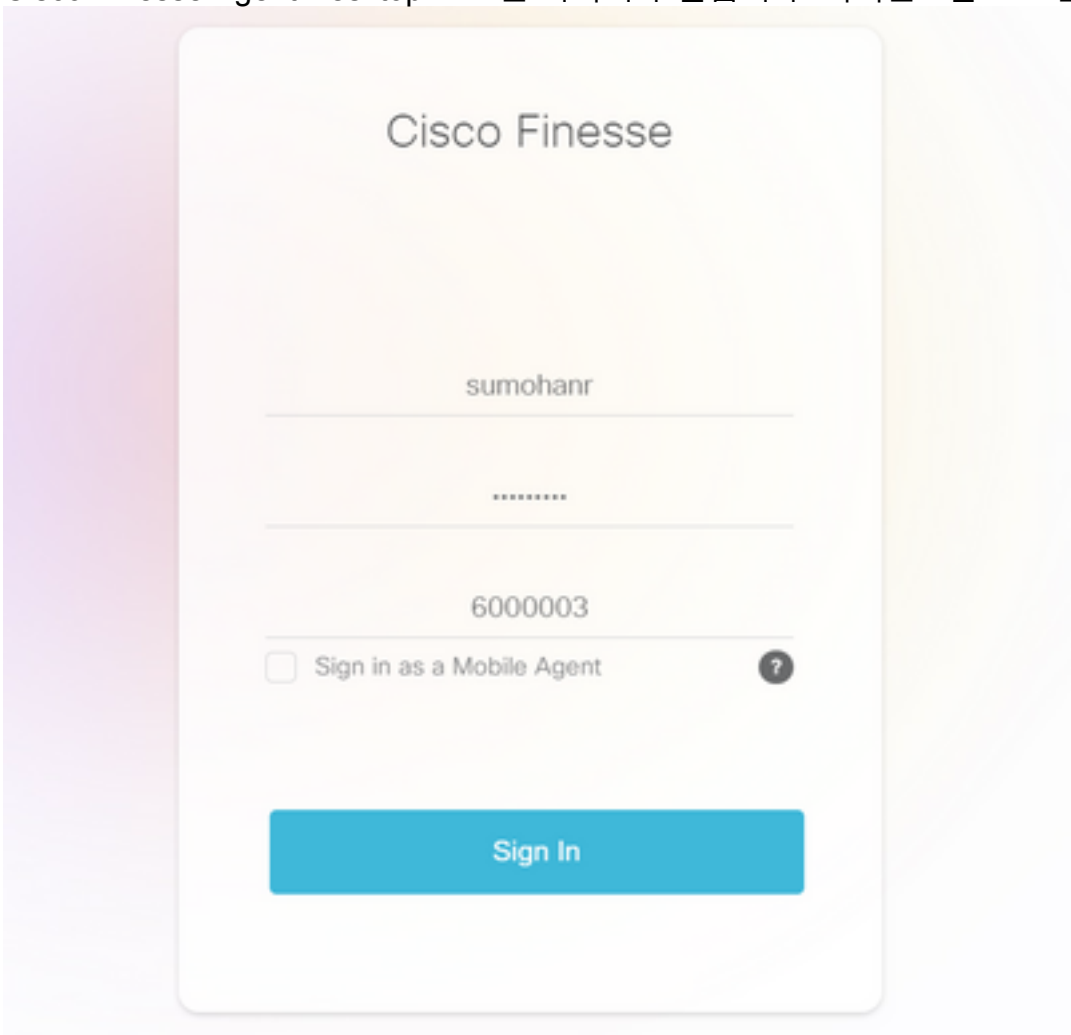
계정으로 로그인합니다.

5. clientlogs/ 디렉토리 아래에서 **로그를** 수집합니다.

옵션 2: 영구 로깅 설정

1. https://x.x.x.x:8445/desktop/locallog으로 이동합니다.
2. 영구 **로깅을 사용하여 로그인을 클릭합니다**.

3. Cisco Finesse Agent Desktop 로그인 페이지가 열립니다. 에이전트를 로그인합니다.

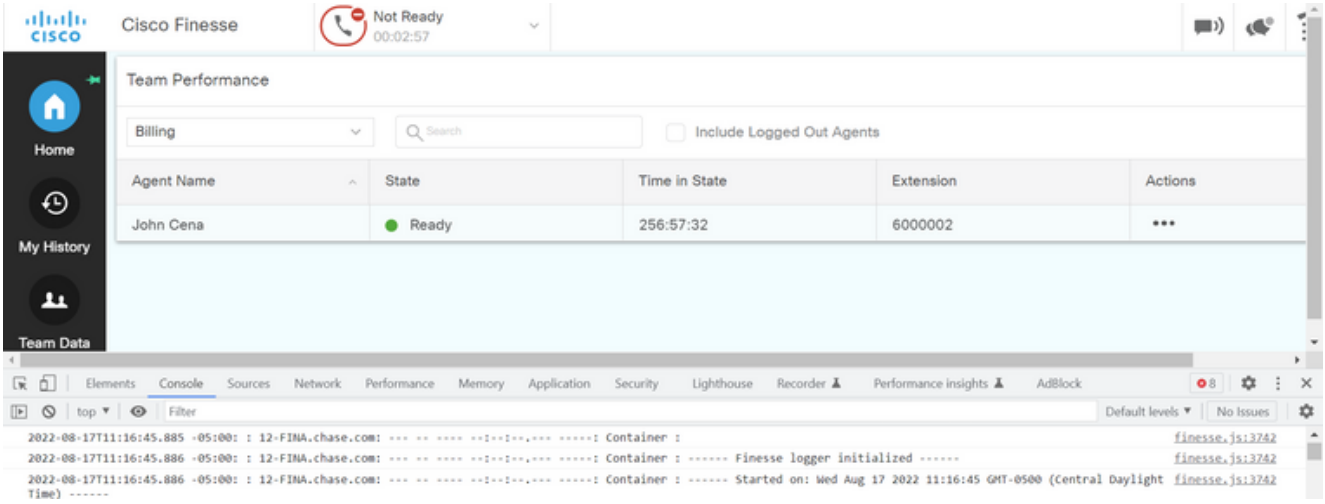


4. 모든 에이전트 데스크톱 상호 작용이 등록되고 로컬 스토리지 로그로 전송됩니다. 로그를 수

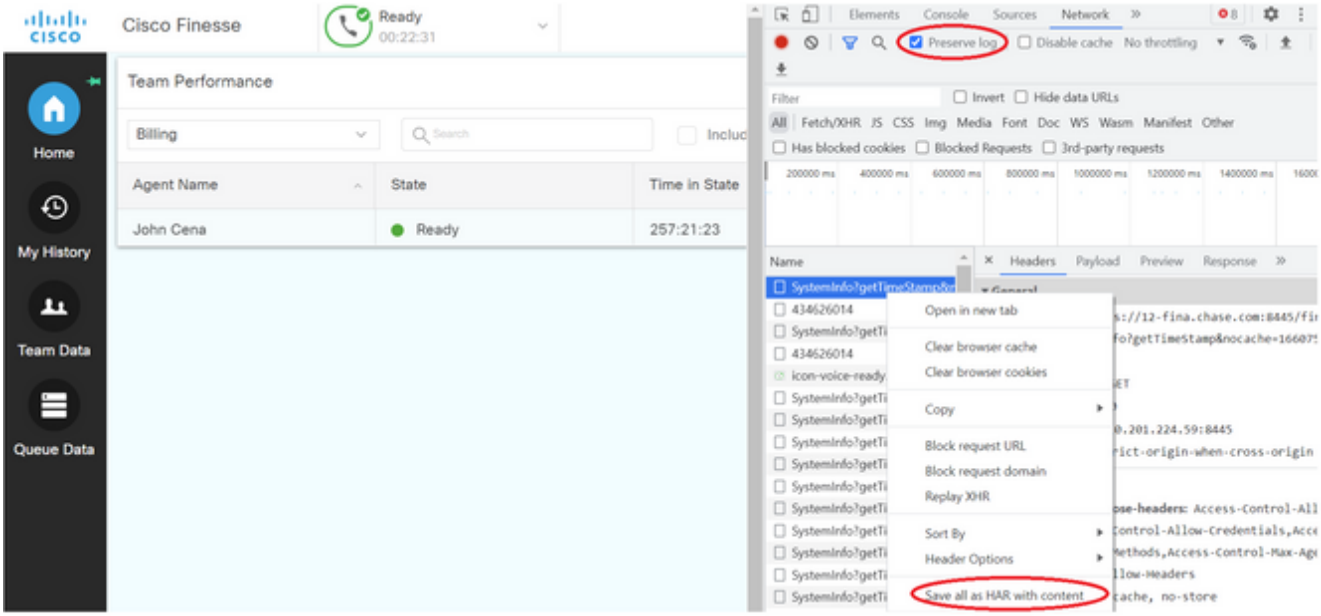
집하려면 https://x.x.x.x:8445/desktop/locallog으로 이동하여 텍스트 파일에 내용을 복사합니다. Save 추가 분석을 위한 파일입니다.

옵션 3: 웹 브라우저 콘솔

1. 상담원이 로그인하면 **F12**를 눌러 브라우저 콘솔을 엽니다.
2. **Console** 탭을 선택합니다.
3. 브라우저 콘솔에서 오류를 확인합니다. 내용을 텍스트 파일로 복사하고 save 그렇습니다.



4. **네트워크** 탭을 선택하고 로그 보존 옵션을 선택합니다.
5. 네트워크 이름 이벤트를 마우스 오른쪽 버튼으로 클릭하고 **Save** HAR과 같은 콘텐츠입니다.



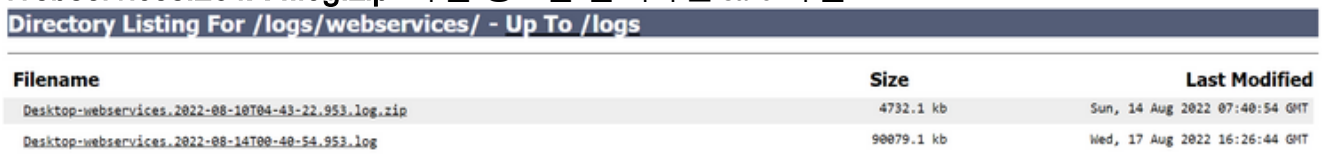
Finesse 서버

옵션 1: UI(사용자 인터페이스) - 웹 서비스(필수) 및 추가 로그

1. https://x.x.x.x/finesse/logs으로 이동하고 관리 계정으로 로그인합니다.
2. 디렉터리 webservices/

3. 마지막 웹 서비스 로그를 수집합니다. 마지막 압축 해제 파일을 선택합니다. 예: **Desktop-**

Webservices.201X-..log.zip. 파일 링크를 클릭하면 save 파일.



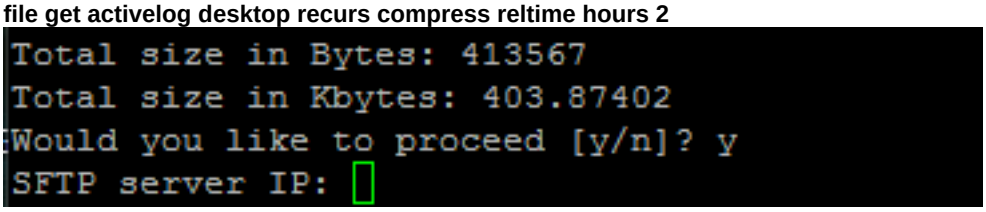
4. 다른 필수 로그를 수집합니다(시나리오에 따라 다름). 예를 들어, 알림 서비스 문제의 경우 openfire, 인증 문제의 경우 realm 로그, API 문제의 경우 tomcatlogs가 있습니다.

   참고: Cisco Finesse 서버 로그를 수집하는 권장 방법은 SSH(Secure Shell) 및 SFTP(Secure File Transfer Protocol)를 사용하는 것입니다. 이 방법을 사용하면 웹 서비스 로그뿐만 아니라 Fippa, openfire, Realm 및 Clientlogs와 같은 모든 추가 로그를 수집할 수 있습니다.

옵션 2: SSH 및 SFTP(Secure File Transfer Protocol)를 통해 - 권장 옵션

1. SSH를 사용하여 Finesse 서버에 로그인합니다.
2. 필요한 로그를 수집하려면 이 명령을 입력합니다. 이 명령은 2시간 동안 로그를 수집합니다. 로그가 업로드되는 SFTP 서버를 식별하라는 메시지가 표시됩니다.

   file get activelog desktop recurs compress reltime hours 2

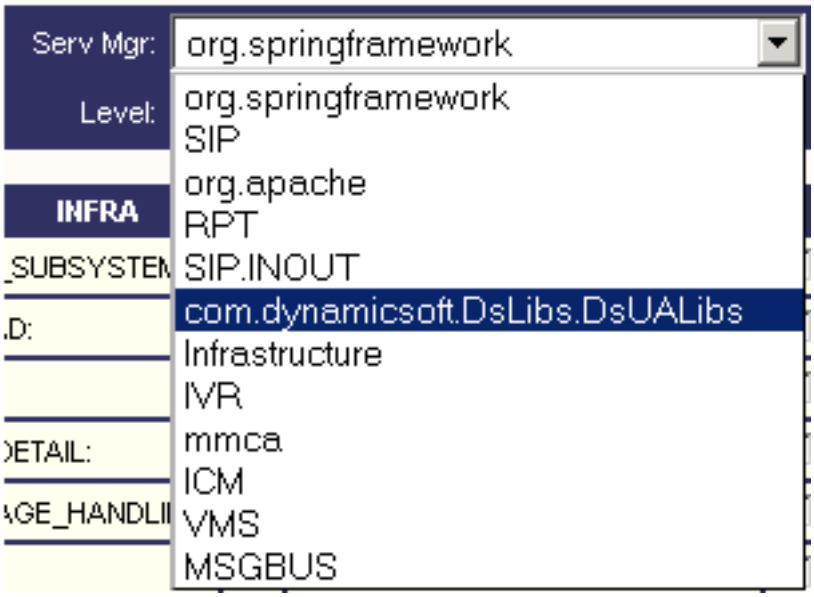


3. 이러한 로그는 SFTP 서버 경로에 저장됩니다. <IP address>\<date time stamp>\active_nnn.tgz 여기서 nnn은 긴 형식의 타임스탬프입니다.
4. tomcat, Context service, Servm 및 설치 로그와 같은 추가 로그를 수집하려면 Cisco Finesse 관리 설명서 릴리스 12.5(1)의 로그 수집 섹션을 참조하십시오.

추적 설정 및 CVP 및 CVVB 로그 수집

CVP 통화 서버

1. CVP CallServer 기본 추적 레벨만으로도 대부분의 문제를 해결할 수 있습니다. 그러나 SIP(Session Initiation Protocol) 메시지에 대한 자세한 내용을 보려면 SIP 추적 추적을 DEBUG 레벨로 설정해야 합니다.
2. CVP CallServer Diag 웹 페이지 URL(http:/localhost:8000/cvp/diag)로 이동합니다.
   참고: 이 페이지는 CVP CallServer에 대한 유용한 정보를 제공하며 특정 시나리오를 해결하는 데 매우 유용합니다.
3. 서버에서 **com.dynamicsoft.DsLibs.DsUALibs**를 **선택합니다.** 왼쪽 상단 모서리에 있는 관리자 드롭다운 메뉴

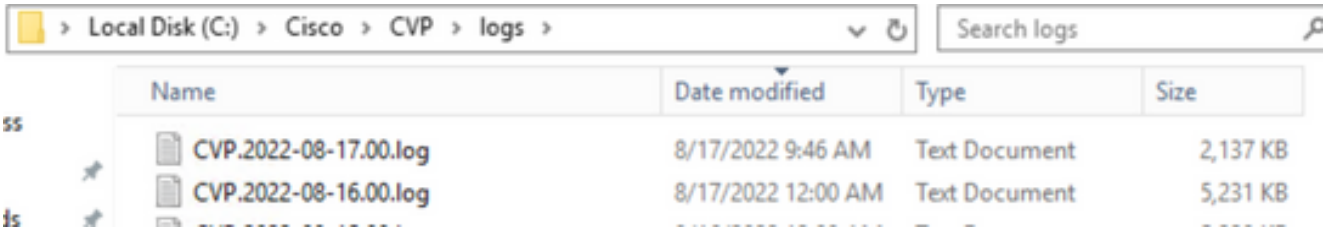


4. Set(설정) **버튼**을 클릭합니다.

5. 추적 수준이 올바르게 설정되었는지 확인하려면 추적 창에서 아래로 스크롤합니다. 디버그 설정입니다.

NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
SIP.INOUT	WARN	0
com.dynamicsoft.DsLibs.DsUALibs	DEBUG	0
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
MSGBUS	INFO	0

6. 문제를 재현하는 경우 C:\Cisco\CVP\logs에서 로그를 **수집하고** 문제가 발생한 시간을 기준으로 CVP 로그 파일을 선택합니다.

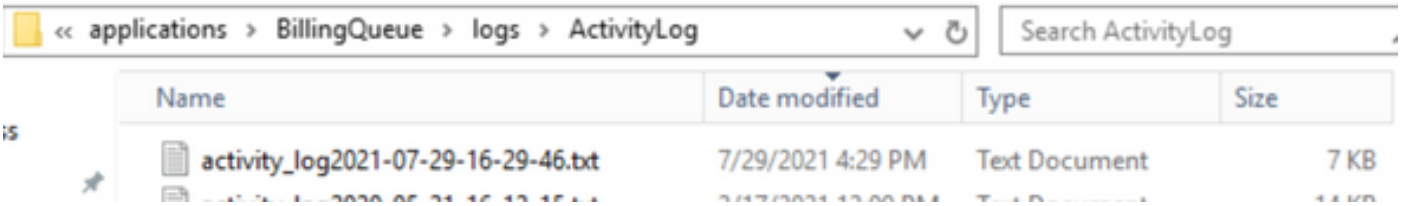


CVP VXML(음성 XML) 애플리케이션

매우 드문 경우이지만 VXML 서버 애플리케이션의 추적 수준을 높여야 합니다. 반면, Cisco 엔지니어가 요청하지 않는 한 늘리는 것은 권장되지 않습니다.

VXML 서버 애플리케이션 로그를 수집하려면 VXML 서버 아래의 특정 애플리케이션 디렉토리로 이동합니다. 예를 들면 다음과 같습니다. **C:\Cisco\CVP\VXMLServer\applications\{application의 이름**

}\logs\ActivityLog\을 입력하고 활동 로그를 수집합니다.



CVP OAMP(Operations and Administration Management Portal)

대부분의 경우 OAMP 및 ORM의 기본 추적 수준은 문제의 근본 원인을 파악하기에 충분합니다. 그러나 추적 레벨을 높여야 하는 경우 이 작업을 실행하는 단계는 다음과 같습니다.

1. 백업 **%CVP_HOME%\conf\oamp.properties**

2. 편집 **%CVP_HOME%\conf\oamp.properties**

```
omgr.traceMask=-1
omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERROR
net.sf.ehcache.logLevel=ERROR
```

3. 그림과 같이 수정 후 OPSConsoleServer를 다시 시작합니다.

추적 레벨 정보

추적 레벨	설명	로그 레벨	추적 마스크
0	제품 설치 기본값입니다. 성능에 미치는 영향이 없거나 최소화됩니다.	정보	없음
1	성능에 미치는 영향이 적은 덜 상세한 추적 메시지	디버그	장치 구성 + 데이터베이스 수정 + 관리=0x01011000
2	성능에 중간 정도의 영향을 주는 자세한 추적 메시지	디버그	장치 구성 + SYSVL_컨피그레이션 + 데이터베이스 수정 + 관리=0x05011000
3	성능에 큰 영향을 미치는 자세한 추적 메시지입니다.	디버그	장치 구성 + SYSVL_컨피그레이션 + 대량_작업 + 데이터베이스 수정 + 관리=0x05111000
4	성능에 매우 큰 영향을 미치는 자세한 추적 메시지입니다.	디버그	기타 + 장치 구성 + 설정(_C) + SYSVL_컨피그레이션 + 대량_작업 + BULK_EXCEPTION_STACK TRACE + 데이터베이스 수정 +

			데이터베이스 선택 + DATABASE_PO_INFO + 관리 + TRACE_METHOD + TRACE_PARAM=0x173710 00
5	가장 상세한 추적 메시지입니다.	디버그	기타 + 장치 구성 + 설정(_C) + SYSVL_컨피그레이션 + 대량_작업 + BULK_EXCEPTION_STACK TRACE + 데이터베이스 수정 + 데이터베이스 선택 + DATABASE_PO_INFO + 관리 + TRACE_METHOD + TRACE_PARAM=0x173710 06

Cisco CVVB(Virtualized Voice Browser)

CVVB에서 추적 파일은 Cisco VVB 구성 요소 하위 시스템 및 단계의 활동을 기록하는 로그 파일입니다.

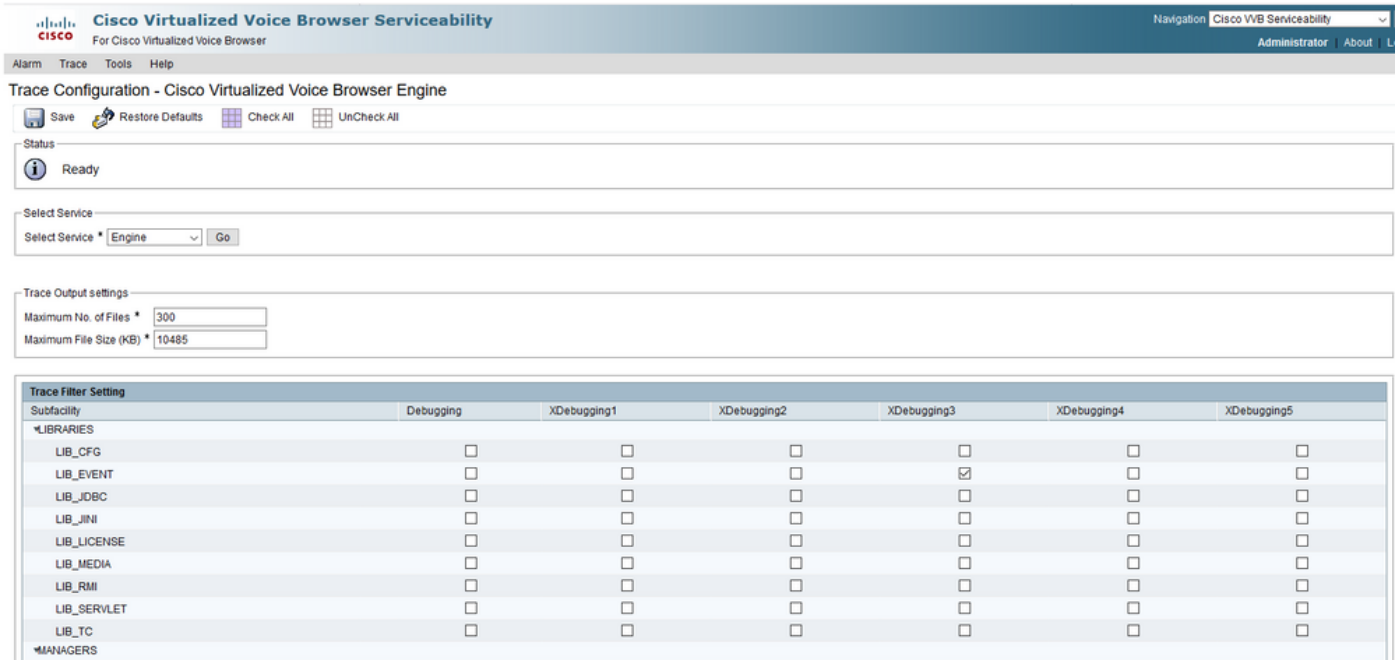
Cisco VVB에는 두 가지 주요 구성 요소가 있습니다.

- MADM 로그라고 하는 Cisco VVB "관리" 추적
- Cisco VVB "엔진" 추적을 MIVR 로그라고 함

정보를 수집할 구성 요소와 수집할 정보 레벨을 지정할 수 있습니다.

로그 수준 범위:

- 디버깅 - 기본 플로우 세부사항
- XDebugging 5 - 스택 추적을 통한 세부 레벨



경고: 프로덕션 로드된 시스템에서 Xdebugging5를 사용하도록 설정할 수 없습니다.

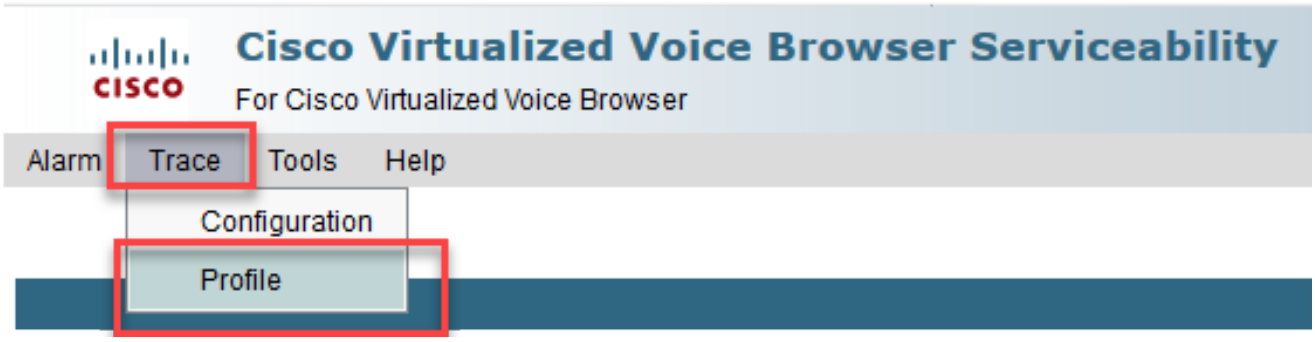
수집해야 하는 가장 일반적인 로그는 엔진입니다. CVVB 엔진 추적의 기본 추적 수준은 대부분의 문제를 해결하는 데 충분합니다. 그러나 특정 시나리오에 대한 추적 레벨을 변경해야 하는 경우 사전 정의된 시스템 로그 프로파일을 사용하는 것이 좋습니다.

시스템 로그 프로파일

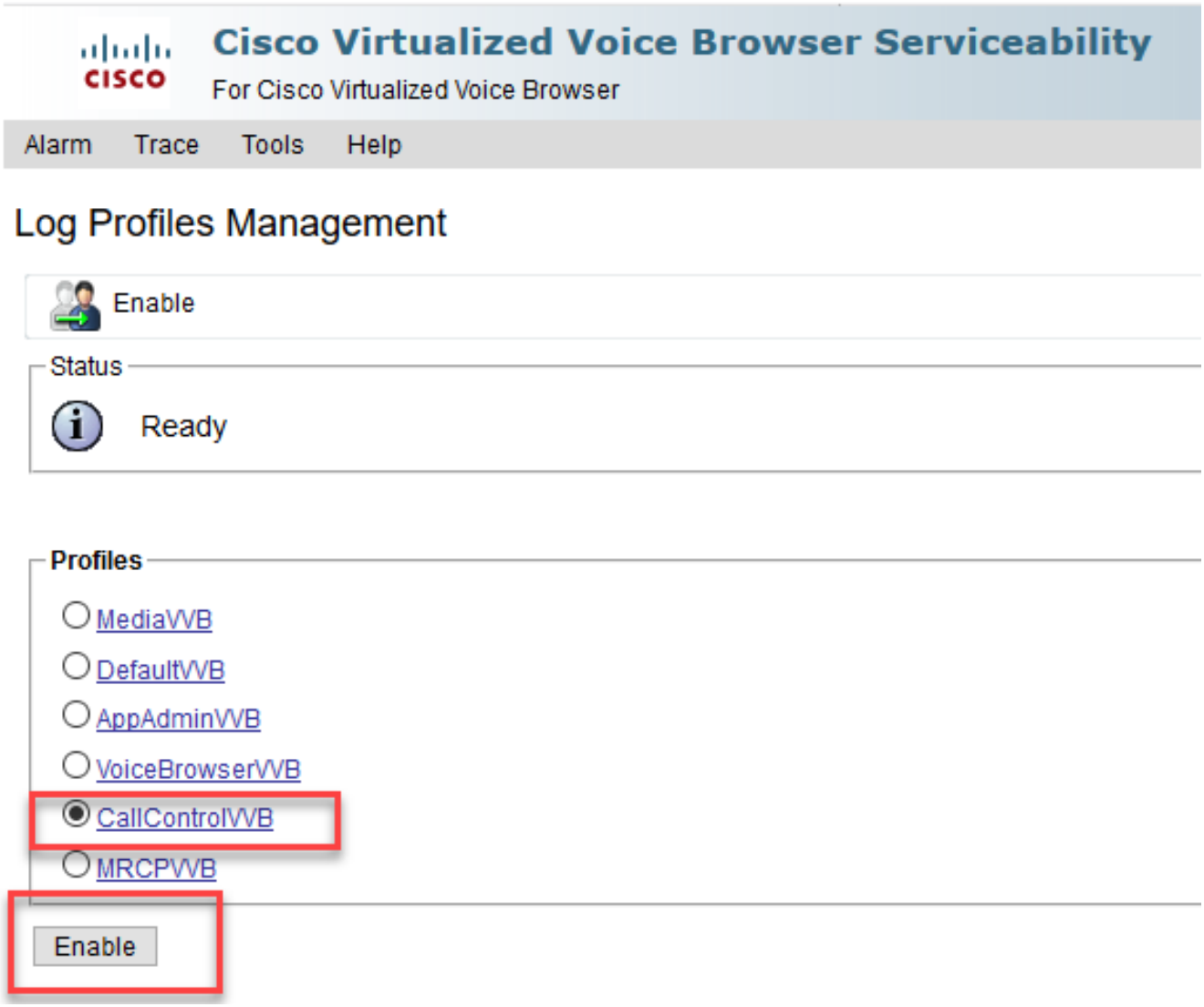
이름	이 프로필을 활성화해야 하는 시나리오
기본값VVB	일반 로그가 활성화됩니다.
AppAdminVVB	AppAdmin, Cisco VVB Serviceability 및 기타 웹 페이지를 통한 웹 관리 의 경우
미디어VVB	미디어 설정 또는 미디어 전송 관련 문제
음성브라우저VVB	통화 처리 관련 문제
MRCPVVB	Cisco VVB 상호 작용에서 ASR/TTS 관련 문제
통화 제어VVB	SIP 신호 관련 문제는 로그에 게시됩니다.

1. CVVB 기본 페이지(https://X.X.X.X/uccxservice/main.htm)를 열고 Cisco VVB 서비스 가용성 페이지로 이동합니다. 관리 계정으로 로그인

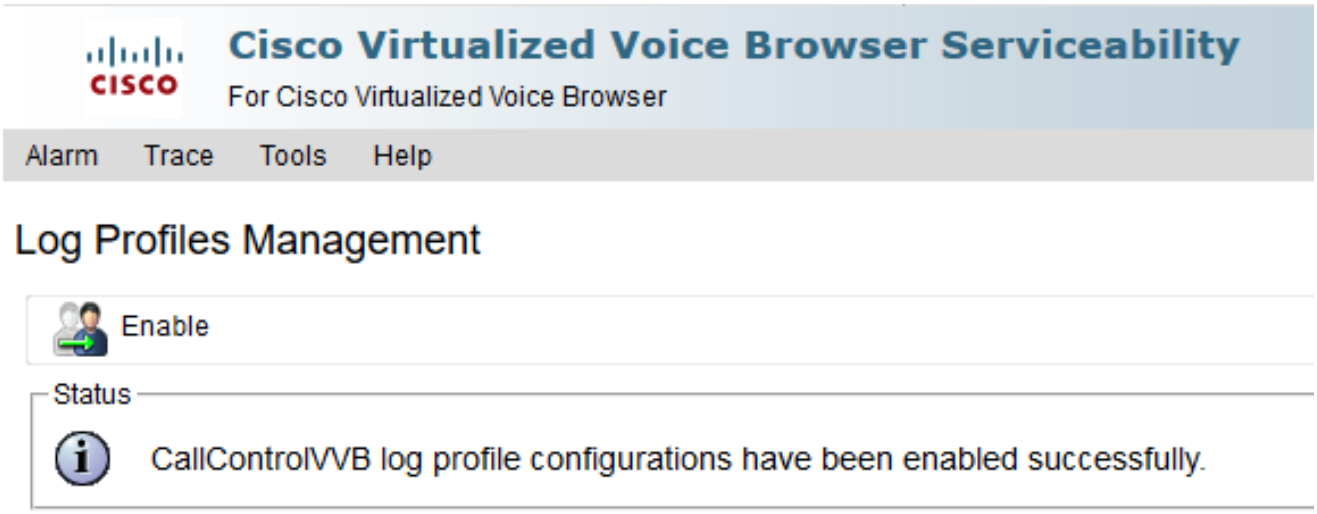
2. 선택 **추적 -> 프로파일**



3. 특정 시나리오에 대해 활성화할 프로필을 선택하고 Enable(활성화) 버튼을 클릭합니다. 예를 들어 SIP 관련 문제에 대해서는 CallControlVVB 프로파일을 활성화하고, ASR/TTS(Automatic Speech Recognition and Text to Speech) 상호 작용과 관련된 문제에 대해서는 MRCPVVB 프로파일을 활성화합니다.

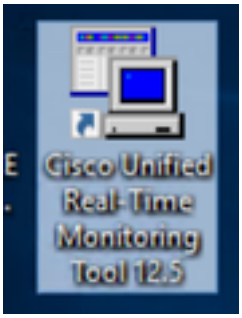


4. 활성화 버튼을 클릭하면 성공 메시지가 표시됩니다.

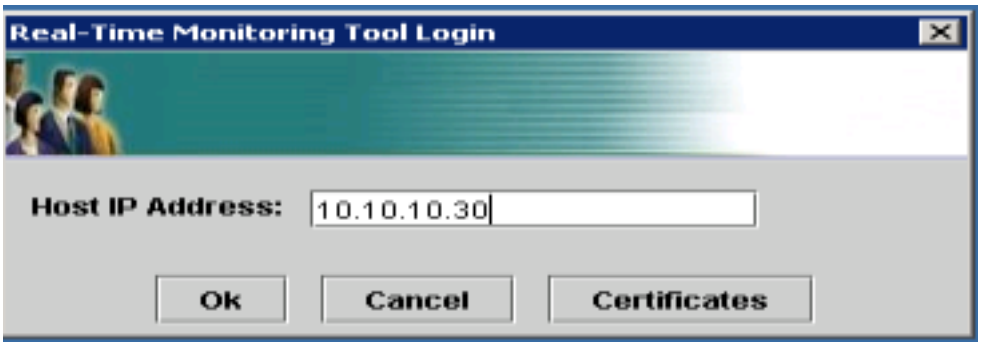


5. 문제가 재현된 후 로그를 수집합니다. CVVB와 함께 제공되는 RTMT(Real Time Monitor Tool)를 사용하여 로그를 수집합니다.

6. 데스크톱에서 Cisco Unified Real-Time Monitoring Tool 아이콘을 클릭합니다(필요한 경우 CVVB에서 이 툴을 다운로드합니다).

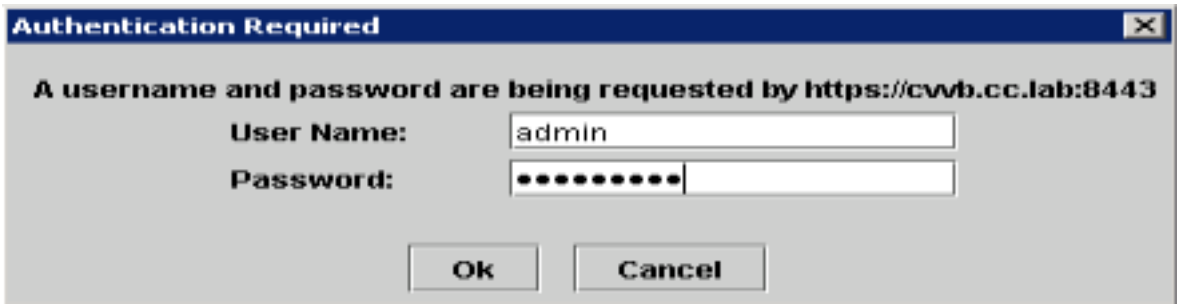


7. VVB의 IP 주소를 입력하고 **OK**(확인)를 클릭합니다.



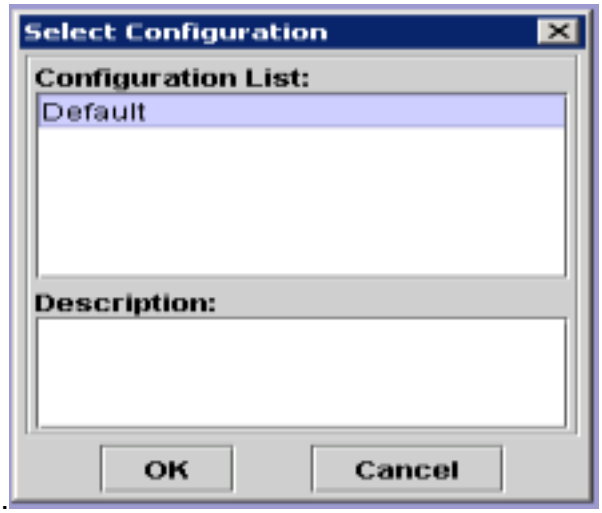
8. 표시되는 경우 인증서 정보 수락

9. 자격 증명을 제공하고 **OK**(확인)를 클릭합니다.

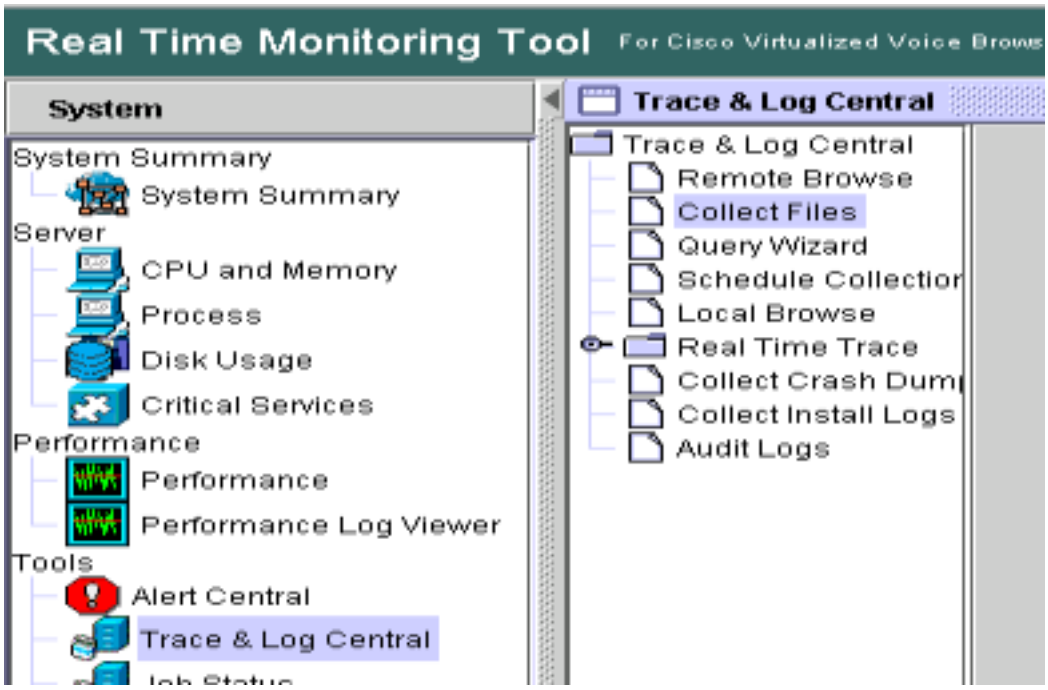


10. TimeZone(시간대) 오류가 발생한 경우 **Yes(예) 버튼**을 클릭하면 RTMT를 닫을 수 있습니다. RTMT 툴을 다시 시작하십시오.

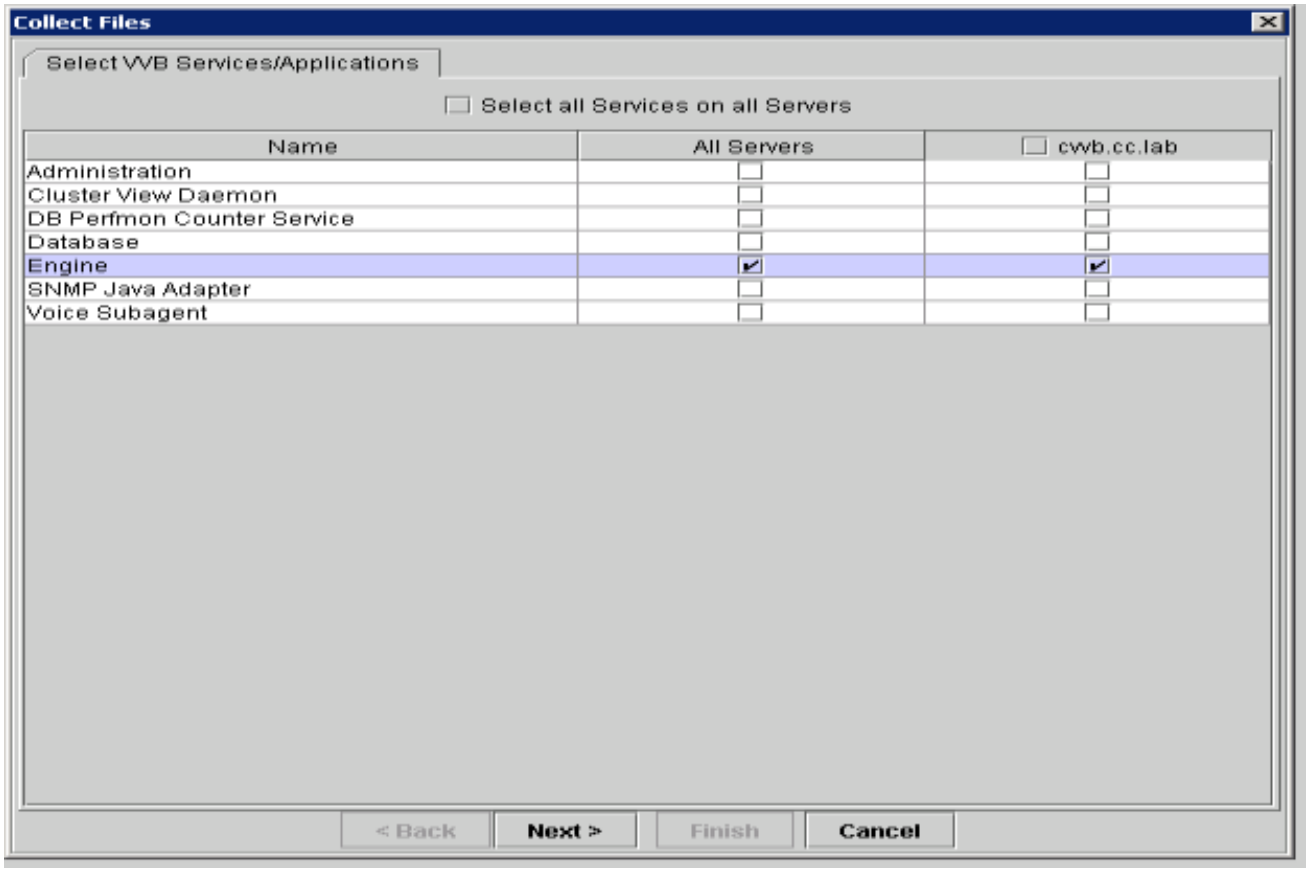
11. Default configuration(기본 컨피그레이션)을 선택한 상태로 두고 **OK(확인)**를 클릭합니다.



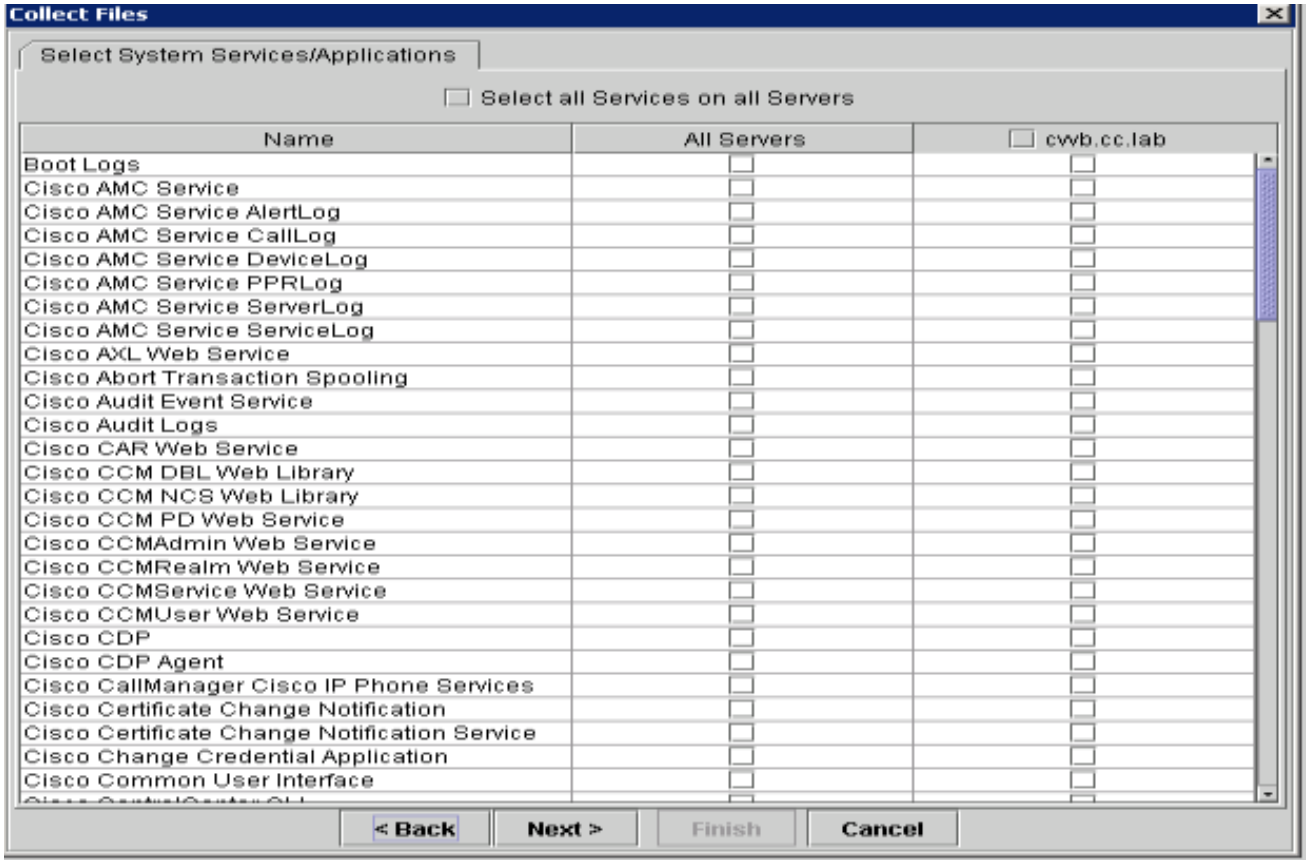
12. **Trace & Log Central을** 선택한 다음 Collect Files를 두 **번 클릭합니다**.



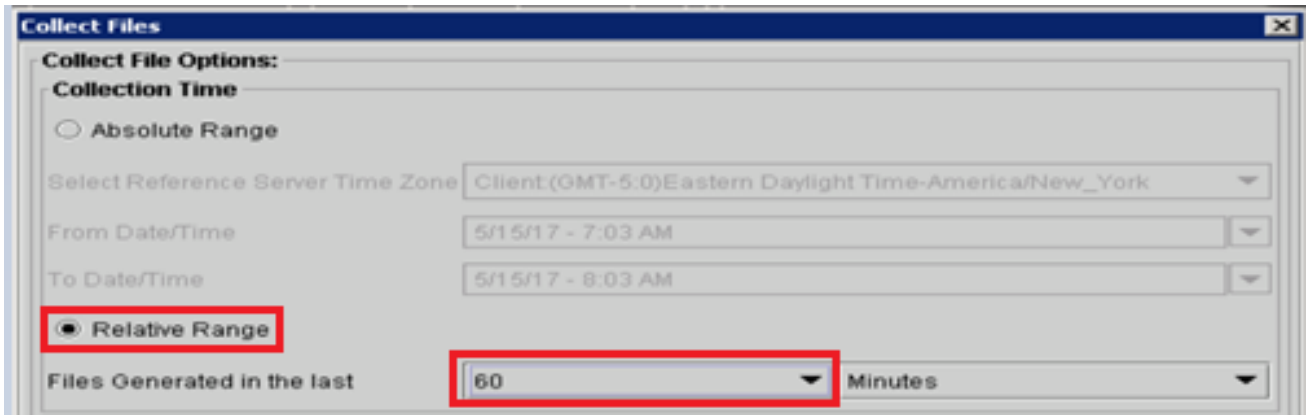
13. 열려 있는 새 창에서 엔진을 선택하고 **다음**을 클릭합니다.



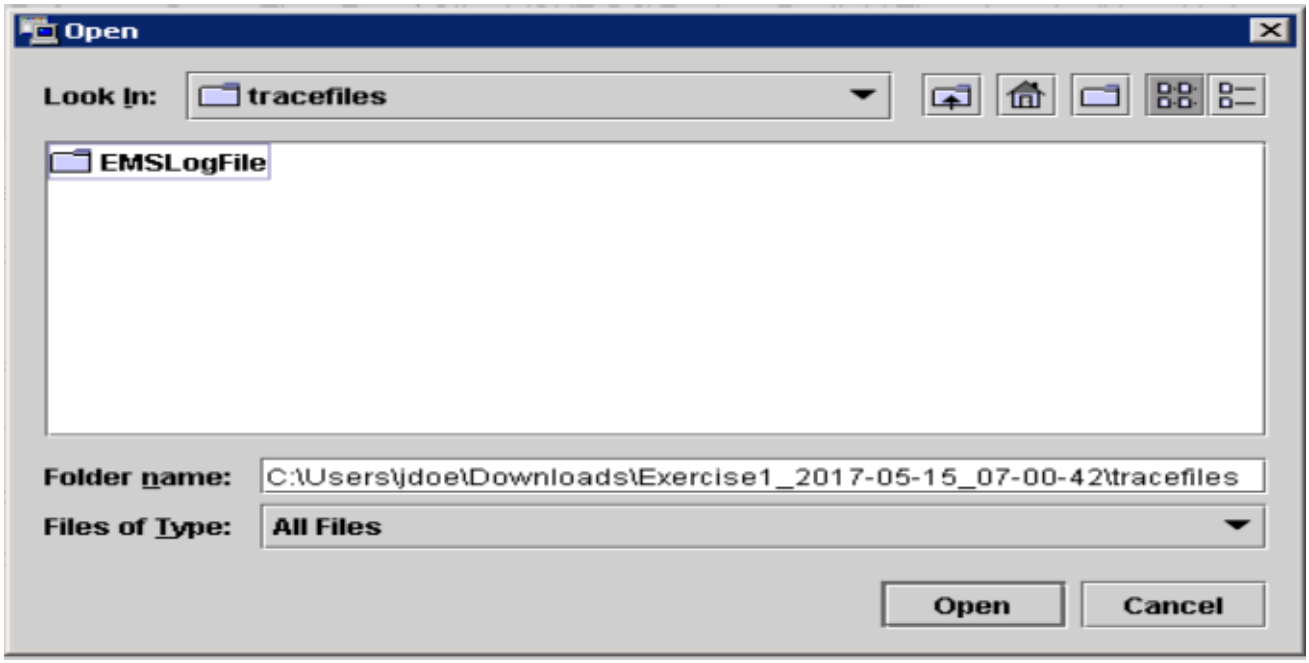
14. 다음 **창**에서 Next(다음)를 다시 클릭합니다.



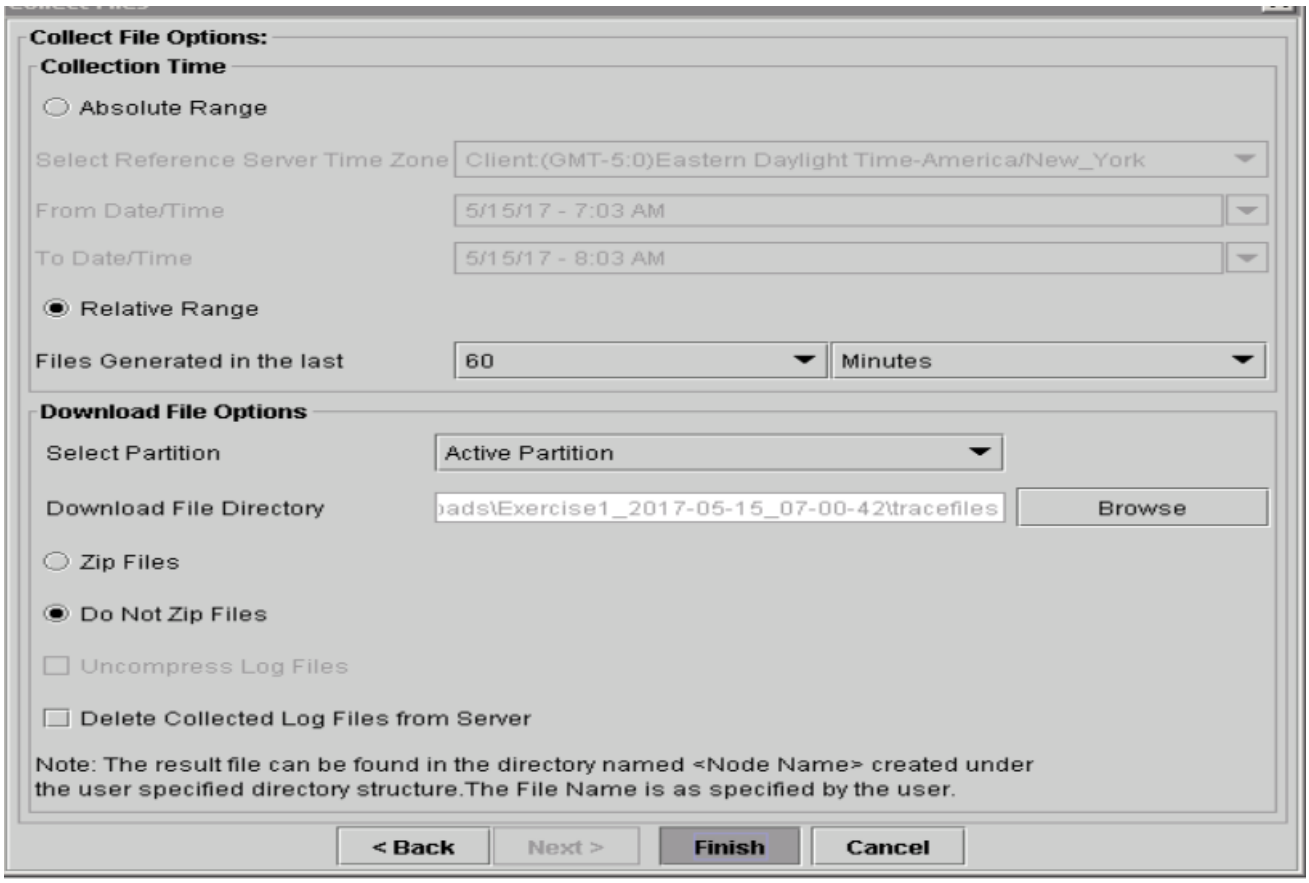
15. Relative **Range(상대** 범위)를 선택하고 잘못된 통화 시간을 처리할 시간을 선택합니다.



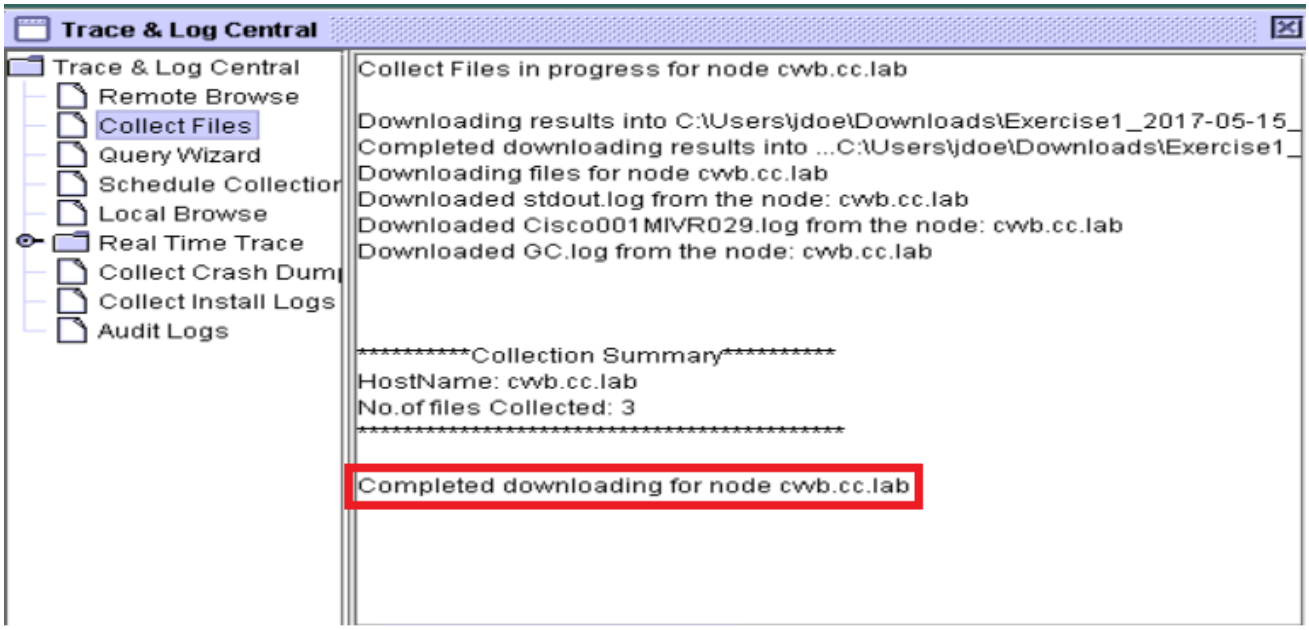
16. Download File Options(파일 다운로드 옵션)에서 **Browse(찾아보기)**를 클릭하고 원하는 디렉토리를 선택합니다 save 파일을 클릭한 다음 열기**를 클릭합니다**.



17. 모두 선택했으면 **Finish**(마침) 버튼을 클릭합니다.



18. 로그 파일을 수집합니다. RTMT에 확인 메시지가 표시될 때까지 기다립니다.



19. 추적이 저장된 폴더로 이동합니다.

20. 엔진 로그만 있으면 됩니다. 해당 항목을 찾으려면 **\<time stamp>\uccx\log\MIVR 폴더로** 이동하십시오.

옵션 2: SSH 및 SFTP 사용 - 권장 옵션

1. SSH(Secure Shell)로 VVB 서버에 로그인합니다.
2. 필요한 로그를 수집하려면 이 명령을 입력합니다. 로그가 압축되며 로그가 업로드되는 SFTP 서버를 식별하라는 메시지가 표시됩니다. **file get activelog /uccx/log/MIVR/***

```
Total size in Bytes: 413567
Total size in Kbytes: 403.87402
Would you like to proceed [y/n]? y
SFTP server IP:
```

3. 이러한 로그는 SFTP 서버 경로에 저장됩니다. *<IP address>\<date time stamp>\active_nnn.tgz* 여기서 nnn은 긴 형식의 타임스탬프입니다.

CUBE 및 CUSP에 대한 추적 설정 및 로그 수집

큐브(SIP)

1. 로그 타임스탬프를 설정하고 로깅 버퍼를 활성화합니다.

```
#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
```

경고: 프로덕션 Cisco IOS® 소프트웨어 GW를 변경하면 중단이 발생할 수 있습니다.

2. 이는 제공된 통화 볼륨에서 문제 없이 제안된 디버그를 처리할 수 있는 매우 강력한 플랫폼입

니다. 그러나 Cisco에서는 다음을 권장합니다. 모든 로그를 로깅 버퍼가 아닌 syslog 서버로 전송합니다.

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

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

```
show proc cpu hist
```

경고: CPU가 CPU 사용률의 70-80%까지 증가하면 성능 관련 서비스 영향의 위험이 크게 증가합니다. 따라서 GW가 60%에 도달할 경우 추가 디버그를 활성화하지 마십시오.

3. 다음 디버그를 활성화합니다.

```
debug voip ccapi inout
debug ccsip mess
After you make the call and simulate the issue, stop the debugging:
```

4. 문제를 재현합니다.
5. 추적을 비활성화합니다.

```
#undebug all
```

6. 로그를 수집합니다.

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

교두

1. CUSP에서 SIP 추적을 켭니다.

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

2. 문제를 재현합니다.
3. 완료되면 로깅을 끕니다.

로그 수집

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 사용자 이름(테스트) 및 비밀번호를 사용합니다.
4. 디렉토리를 /cusp/log/trace로 변경합니다.
5. 로그_<filename>을 가져옵니다.

추적 설정 및 UCCE 로그 수집

Diagnostis Framework Portico 또는 System CLI 툴을 통해 추적 수준을 설정하고 추적을 수집하는 것이 좋습니다.

참고: Diagnostic Framework Portico 및 System CLI에 대한 자세한 내용은 Cisco Unified ICM/Contact Center Enterprise 서비스 가용성 가이드, 릴리스 12.5(1)의 진단 도구 장을 참조하십시오.

대부분의 UCCE 시나리오를 트러블슈팅할 때 기본 추적 수준이 충분한 정보를 제공하지 않으면 필요한 구성 요소에서 추적 수준을 3으로 설정합니다(일부 예외).

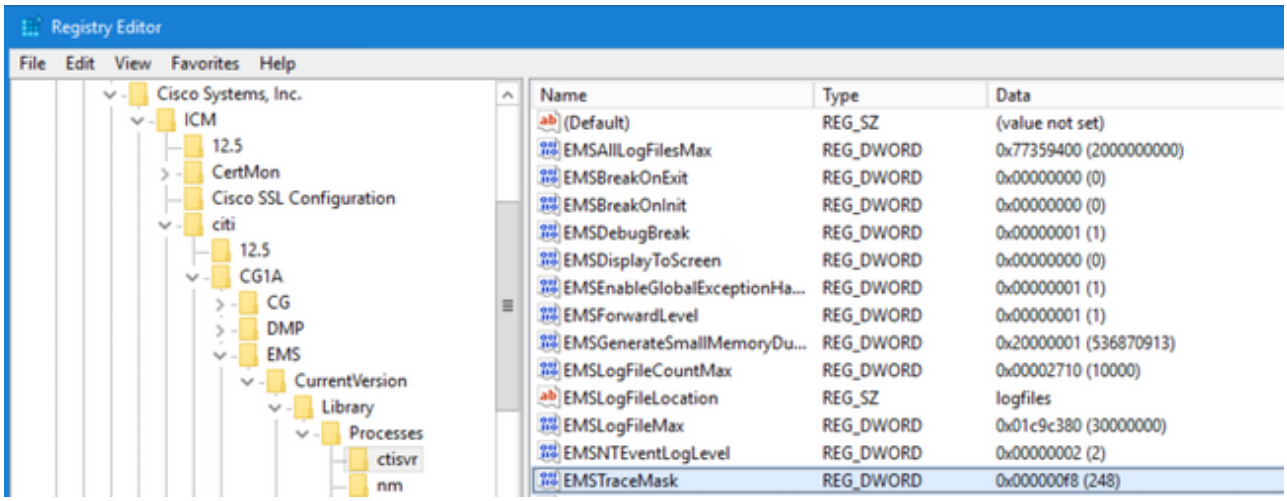
참고: 자세한 내용은 Cisco Unified ICM/Contact Center Enterprise 릴리스 12.5(1)의 서비스 가용성 가이드에서 추적 레벨 섹션을 참조하십시오.

예를 들어, 아웃바운드 다이얼러의 문제 해결 시 다이얼러가 사용 중인 경우 추적 수준을 수준 2로 설정해야 합니다.

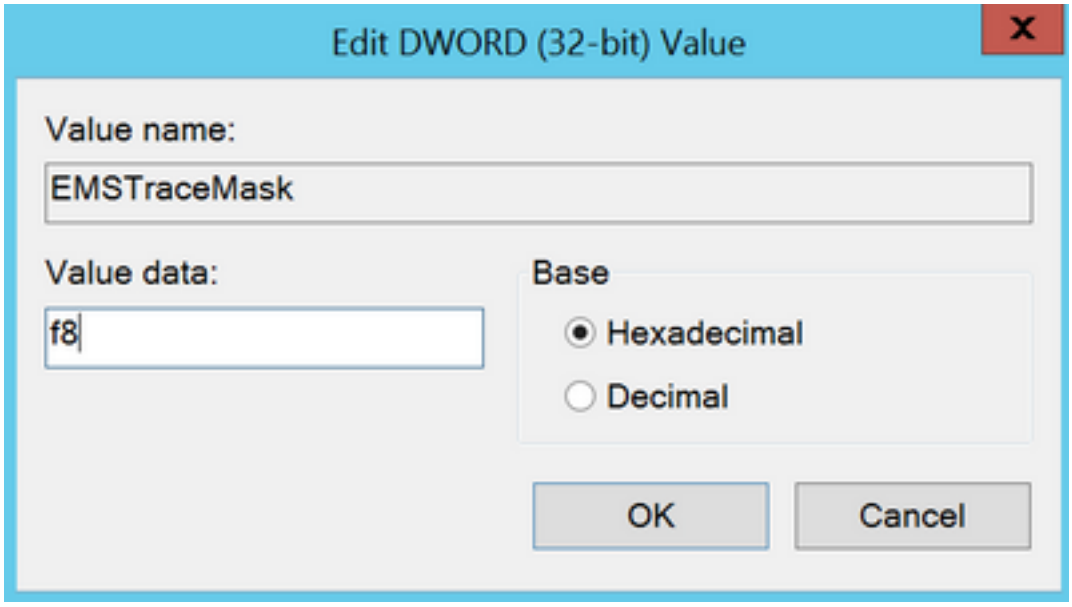
CTISVR(CTISVR) 레벨 2 및 레벨 3의 경우 Cisco에서 권장하는 정확한 레지스트리 레벨을 설정하지 않습니다. CTISVR의 권장 추적 레지스트리는 0XF8입니다.

1. UCCE 에이전트 PG에서 레지스트리 편집기(Regedit)를 엽니다.

2. HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a 및 b)\EMS\CurrentVersion\library\Processes\ctisvr으로 이동합니다.



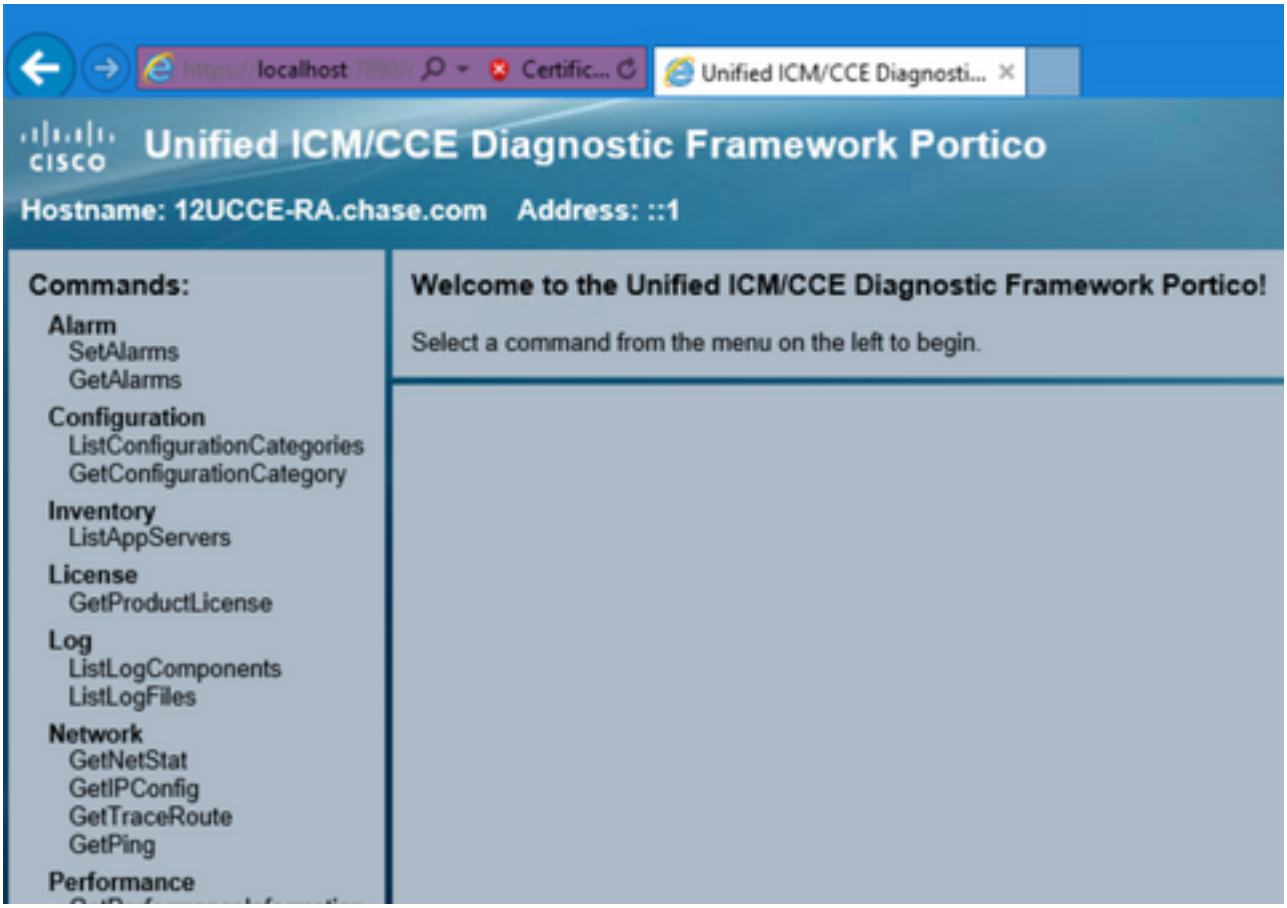
3. EMSTraceMask를 두 **번** 클릭하고 값을 **f8**로 **설정합니다**.



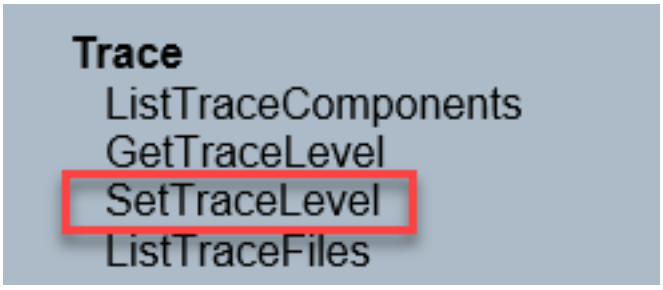
4. Ok(**확인**)를 클릭하고 레지스트리 편집기를 닫습니다. 다음은 UCCE 구성 요소 추적을 설정하는 단계입니다(RTR 프로세스가 예로 사용됨).

SetTrace 수준

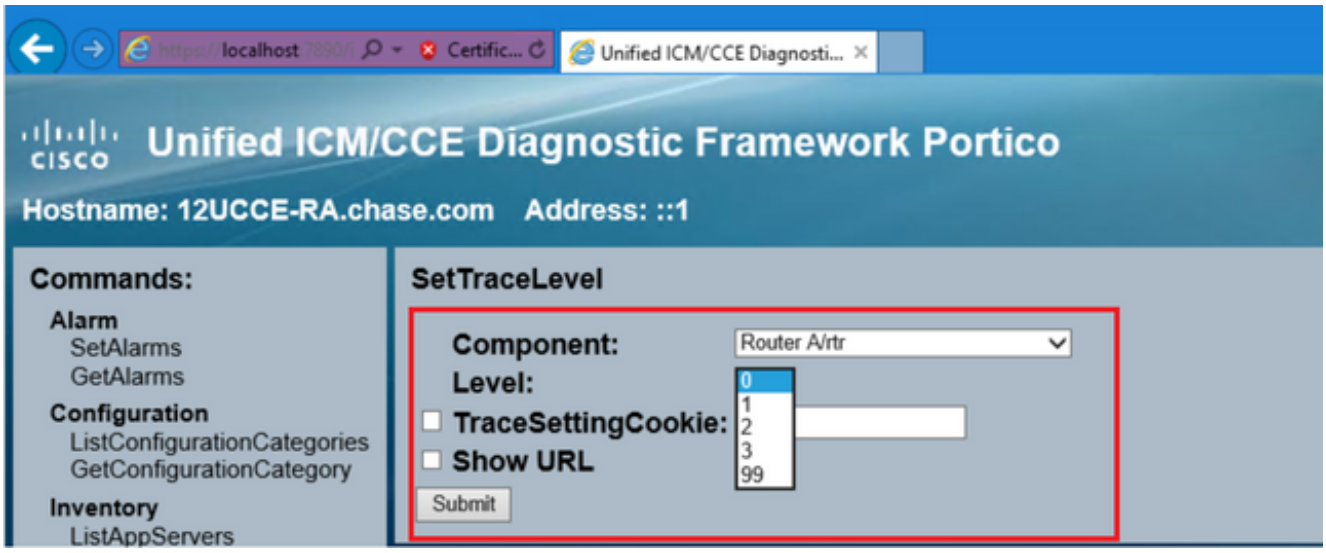
1. 추적을 설정하는 데 필요한 서버에서 Diagnostic Framework Portico를 열고 관리자 사용자로 로그인합니다



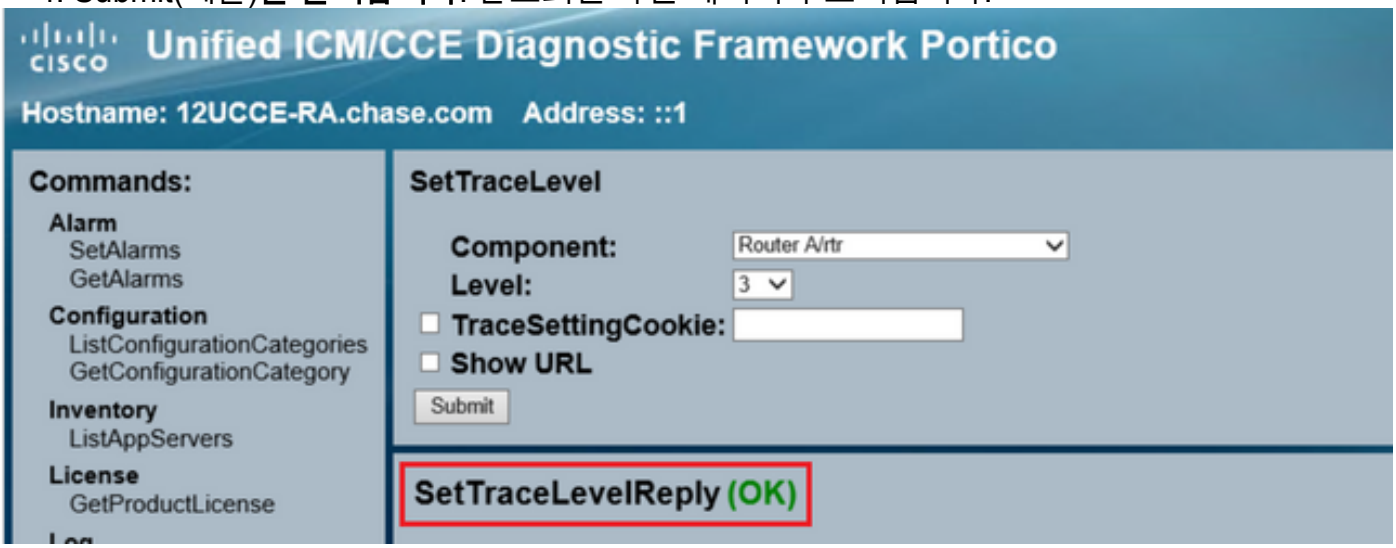
2. Commands 섹션에서 Trace(추적)로 **이동하여** 다음을 선택합니다 **SetTraceLevel입니다.**



3. SetTraceLevel **창**에서 구성 요소와 수준을 선택합니다.



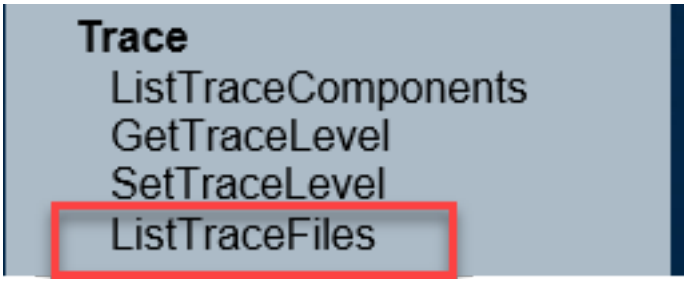
4. Submit(제출)**을 클릭합니다**. 완료되면 확인 메시지가 표시됩니다.



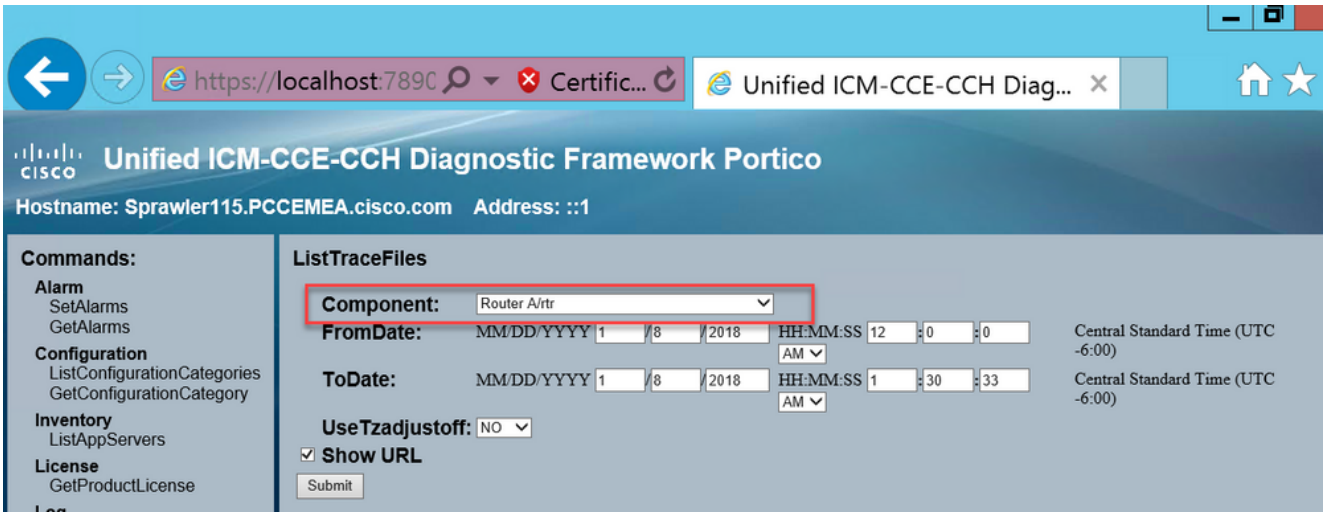
경고: 문제를 재현하는 동안 추적 수준을 수준 3으로 설정합니다. 문제가 재현되면 추적 수준을 기본값으로 설정합니다. JTAPIGW 추적을 설정할 때는 특히 주의해야 합니다. 레벨 2와 레벨 3은 낮은 레벨 추적을 설정하므로 이 경우 성능에 영향을 미칠 수 있습니다. JTAPIGW에서 비프로덕션 시간 또는 랩 환경에서 레벨 2 또는 레벨 3을 설정합니다.

로그 수집

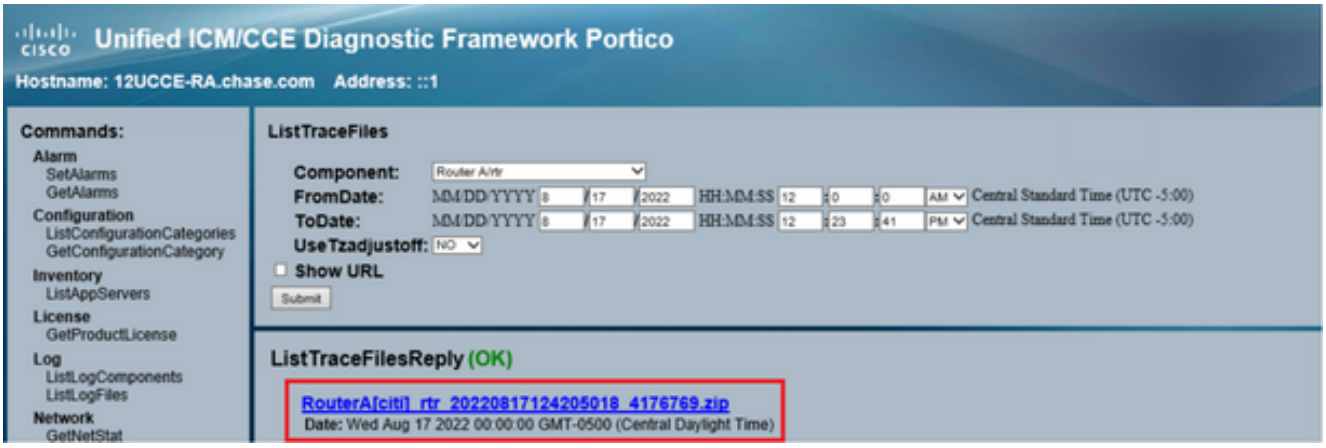
1. Diagnostic Framework Portico의 Commands 섹션에서 **Trace**로 이동하고 ListTraceFile**을** 선택합니다.



2. ListTraceFile **창**에서 **Component**, **FromDate** 및 **ToDate**를 **선택합니다**. **Show URL(URL 표시) 상자**를 선택한 다음 Submit(제출)을 **클릭합니다**.



3. 요청이 완료되면 ZIP 로그 파일의 링크가 포함된 OK 메시지가 표시됩니다.

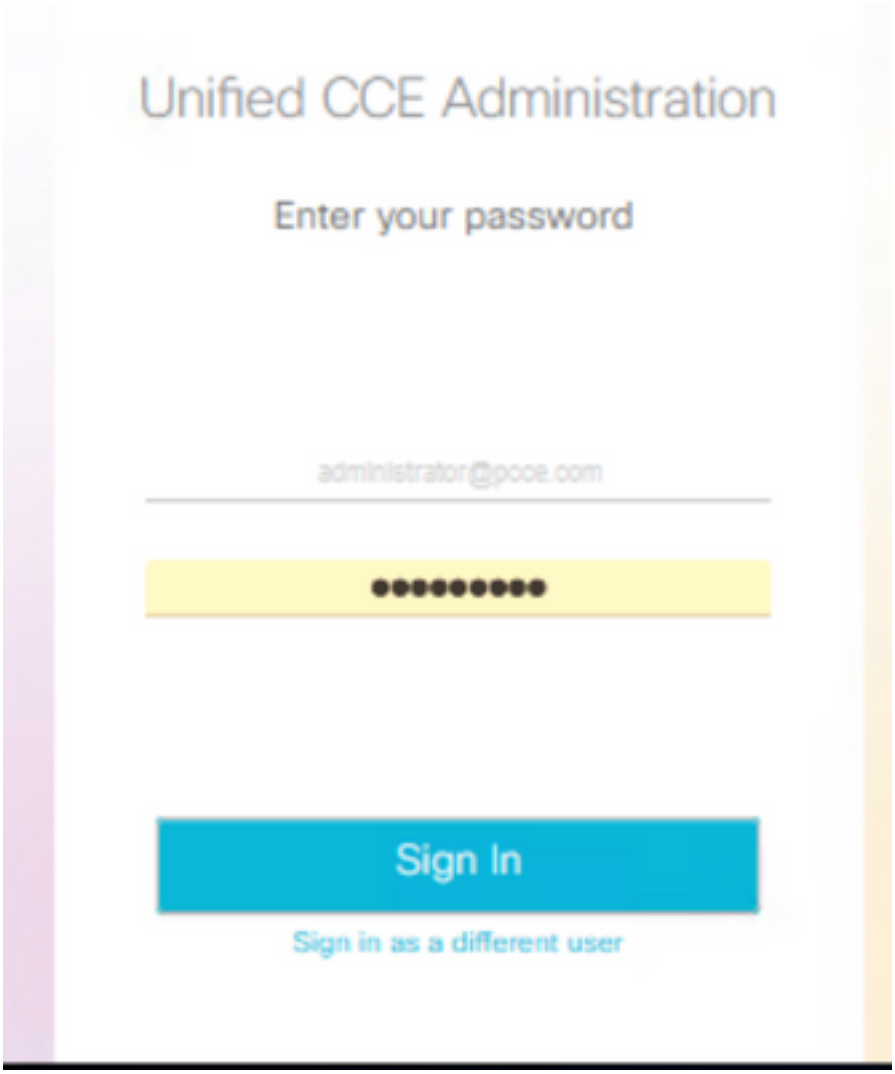


4. ZIP 파일 링크를 클릭하고 save 선택한 위치의 파일.

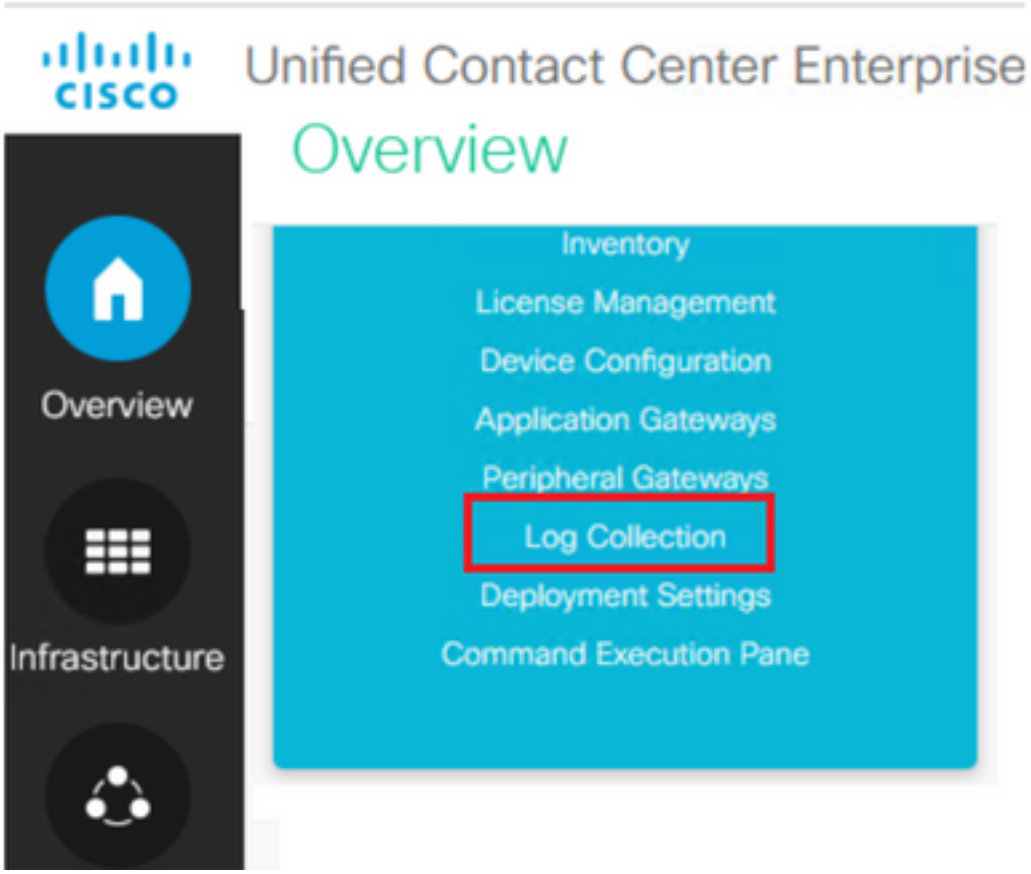
추적 설정 및 PCCE 로그 수집

PCCE에는 추적 레벨을 설정하는 자체 툴이 있습니다. Diagnostic Framework Portico 또는 시스템 CLI가 로그를 활성화하고 수집하는 기본 방법인 UCCE 환경에는 적용되지 않습니다.

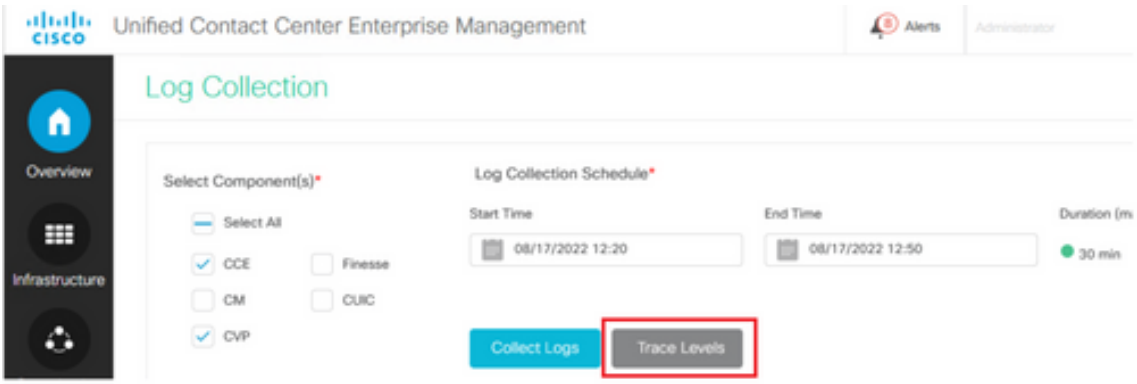
1. PCCE AW 서버에서 Unified CCE 웹 관리 도구를 열고 관리자 계정에 로그인합니다.



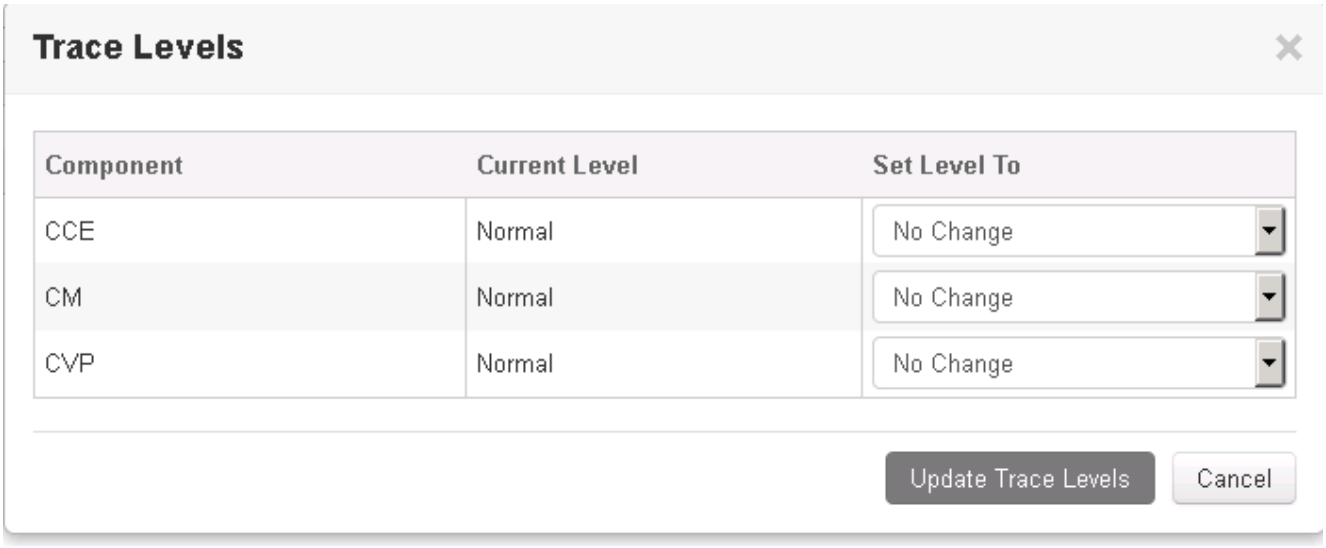
2. **Overview(개요)->Infrastructure Settings(인프라 설정)->Log Collection(로그 수집)**으로 이동하여 Log Collection(로그 수집) 페이지를 엽니다.



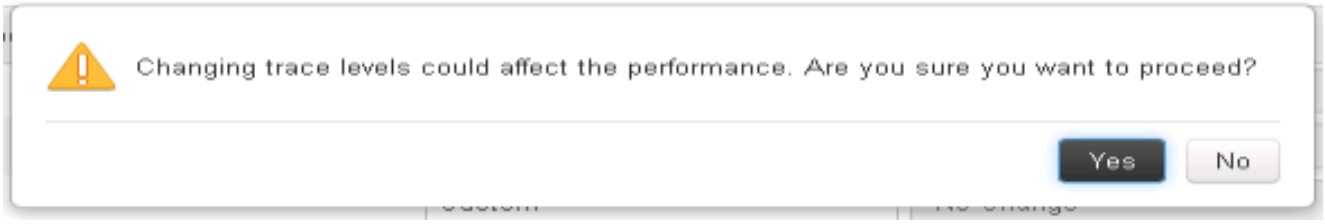
3. Log Collection 페이지에서 Trace Levels(추적 **레벨)를** 클릭하면 Trace Levels(**추적 레벨)** 대화 상자가 열립니다.



4. Trace Level(추적 레벨)을 **Detailed** on CCE(CCE에서 세부사항)로 설정하고 CM 및 CVP에 대해 **No Change(변경** 없음)로 그대로 둔 다음 **추적 수준을 업데이트합니다.**



5. Yes(**예**)를 클릭하여 경고를 승인합니다.



6. 문제가 재현된 후 Unified CCE Administration(Unified CCE **관리)을** 열고 **System(시스템) > 로그 수집**
7. Components **창**에서 **CCE** 및 CVP를 선택합니다.
8. 적절한 로그 수집 시간을 선택합니다(기본값은 최근 30분).
9. Collect Logs(**로그 수집)**를 클릭하고 **Yes(예**)를 클릭하여 대화 상자를 표시합니다. 로그 수집이 시작됩니다. 끝나기 전에 몇 분 기다리세요.

10. 완료되면 Actions(작업) **열**에서 Download(다운로드) **버튼**을 클릭하여 모든 로그가 포함된 압축된 파일을 다운로드합니다. Save 원하는 **위치**에 있는 zip 파일.

추적 설정 및 CUIC/Live Data/IDS 로그 수집

SSH

1. CUIC, LD 및 IDS의 SSH 명령줄(CLI)에 로그인합니다.
2. CUIC 관련 로그를 수집하려면 명령을 실행합니다.

```
file get activelog /cuic/logs/cuic/*.* recurs compress reltime hours 1
file get activelog /cuic/logs/cuicsrvr/*.* recurs compress reltime hours 1
file get activelog tomcat/logs/*.* recurs compress
```

3. LD 관련 로그를 수집하기 위해 명령을 실행합니다.

```
file get activelog livedata/logs/*.*
```

4. Id 관련 로그를 수집하기 위해 명령을 실행합니다.

   file get activelog ids/log/*.* recurs compress reltime days 1

5. 이러한 로그는 SFTP 서버 경로에 저장됩니다. <IP address>\<date time stamp>\active_nnn.tgz 여기서 nnn은 긴 형식의 타임스탬프입니다.

RTMT

1. OAMP 페이지에서 RTMT를 다운로드합니다. https://<HOST ADDRESS>/oamp에 로그인합니다. 여기서 HOST ADDRESS는 서버의 IP 주소입니다.

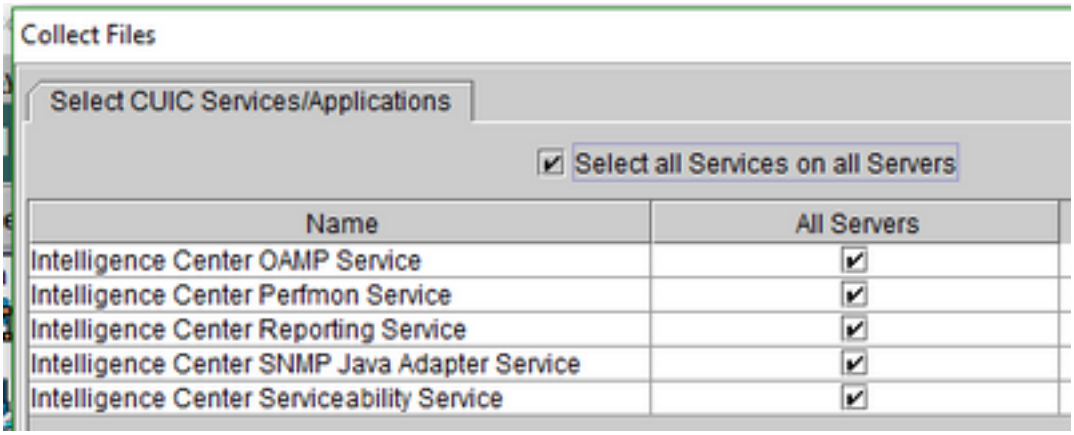
2. **Tools > RTMT plugin download로 이동합니다.** 플러그인을 다운로드하여 설치합니다.

3. RTMT를 시작하고 관리자 자격 증명으로 서버에 로그인합니다.

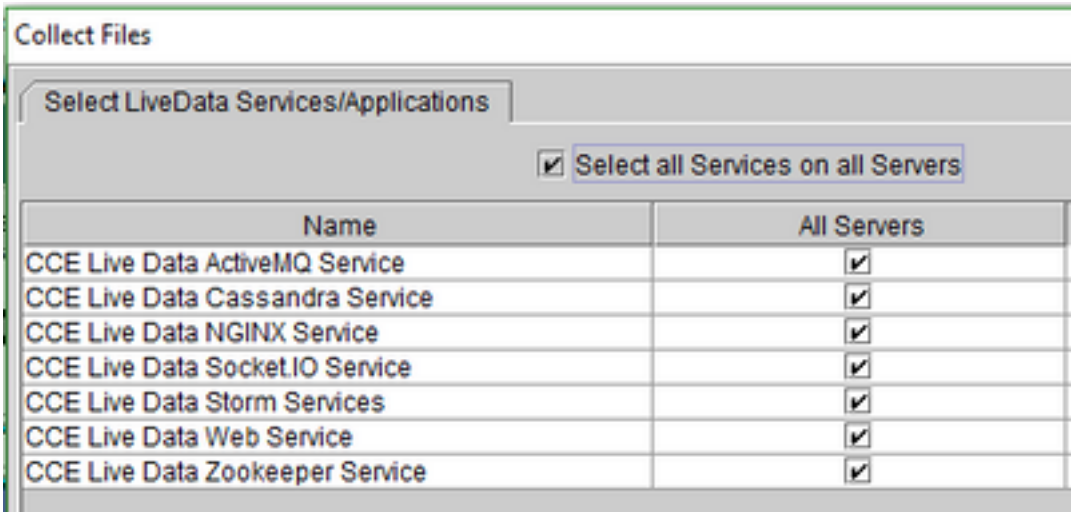
4. Trace(추적) **및 Log Central(로그 센트럴)을 두** 번 클릭한 다음 Collect **Files(파일 수집)를 두 번 클릭합니다**.

5. 특정 서비스에 대한 이러한 탭을 볼 수 있습니다. CUIC, LD 및 IDS에 대한 모든 서비스/서버를 선택해야 합니다.

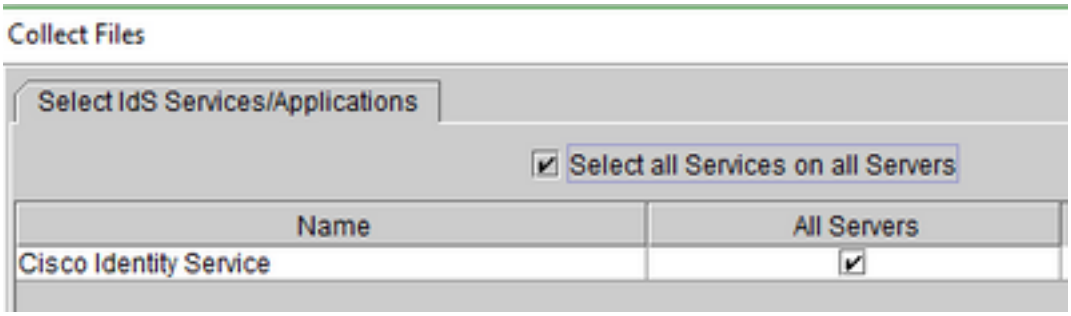
   CUIC :



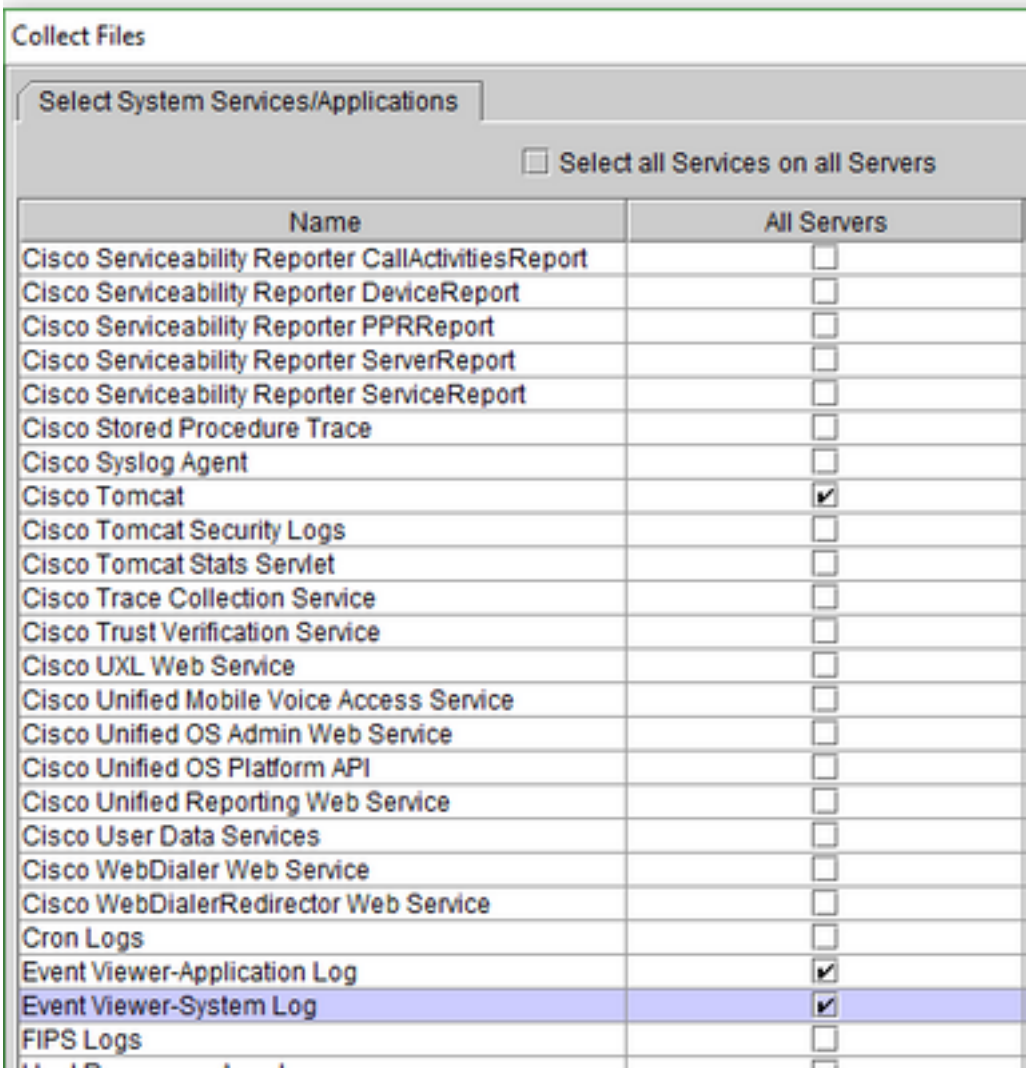
   LD :



IDS :

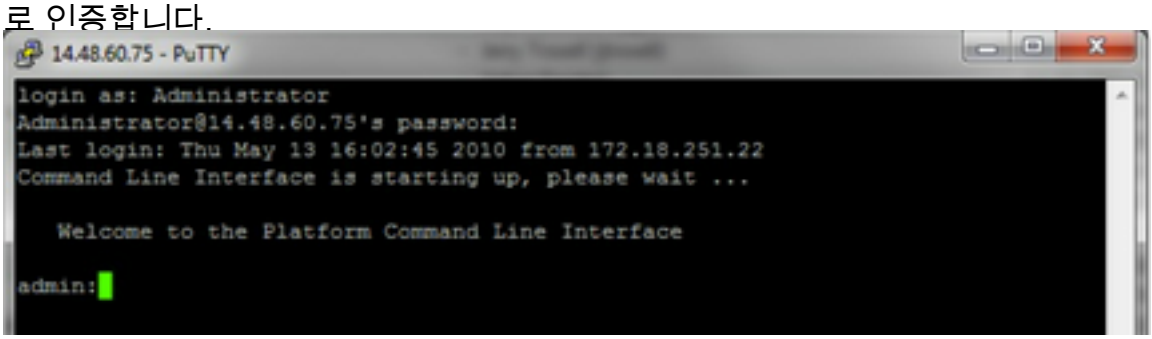


Tomcat .



6. 대상 폴더와 함께 **날짜 및** 시간을 선택하여 save 로그입니다.

VoS의 패킷 캡처(Finesse, CUIC, VVB)

1. 캡처 시작 캡처를 시작하려면 VOS 서버에 대한 SSH 세션을 설정하고 플랫폼 관리자 계정으로 인증합니다.
2. 

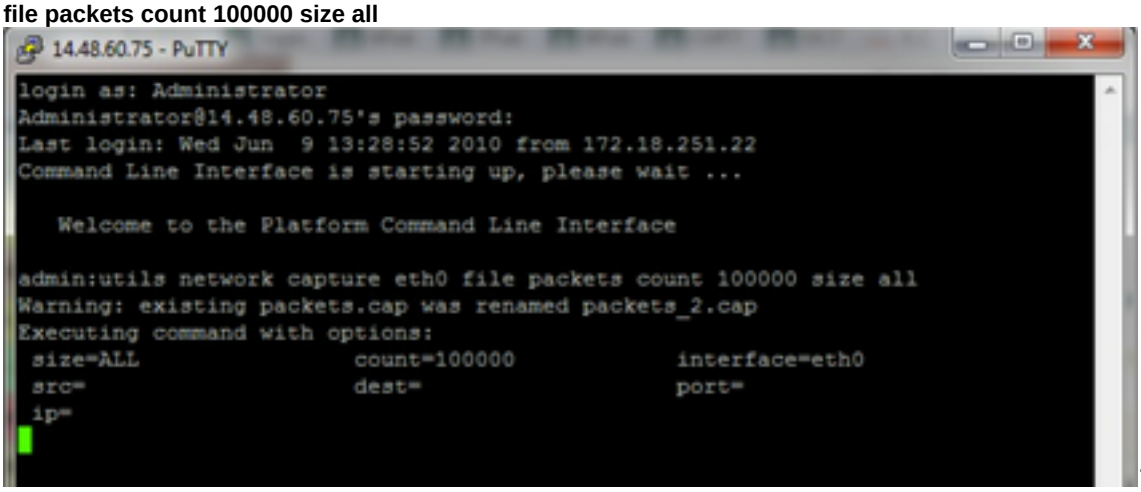
1a. 명령 구문

명령은 **utils network capture**구문은 다음과 같습니다.

```
Syntax:
utils network capture [options]
options  optional
page,numeric,file fname,count num,size bytes,src addr,dest addr,port
num,host protocol addr
options are:
page
- pause output
numeric               - show hosts as dotted IP
addresses
file fname            - output the information to a file

Note: The file is saved in platform/cli/fname.cap

fname should not contain the "." character
count num             - a
count of the number of packets to capture
   Note: The maximum count
for the screen is 1000, for a file is 100000
size bytes            -
the number of bytes of the packet to capture
   Note: The maximum
number of bytes for the screen is 128
         For a file it can be
any number or ALL
src addr              - the source address of the
packet as a host name or IPV4 address
dest addr             - the
destination address of the packet as a host name or IPV4 address
port
num              - the port number of the packet (either src or dest)
host
protocol addr    - the protocol should be one of the following:
ip/arp/rarp/all. The host address of the packet as a host name or IPV4
address. This option  will display all packets to and from that address.

Note: If "host" is provided, do not provide "src" or "dest"
```

1b. 모든 트래픽 캡처

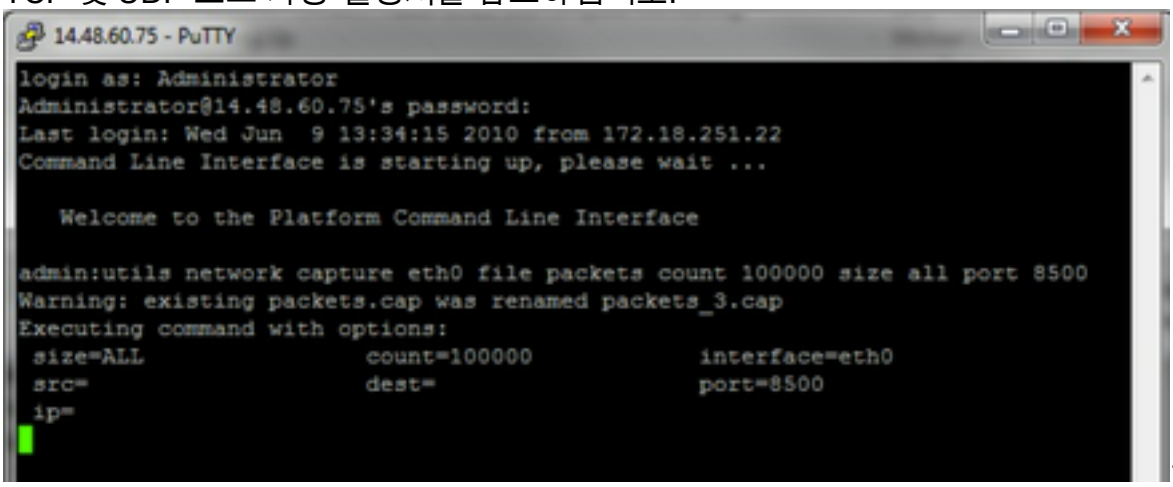
일반적인 캡처의 경우 모든 주소에서 모든 크기의 모든 패킷을 packets.cap이라는 캡처 파일에 수집할 수 있습니다. 이렇게 하려면 관리 CLI에서 실행하면 됩니다 **utils network capture eth0 file packets count 100000 size all**



1c. 포트 번호 기반 캡처

클러스터 관리자와의 통신 문제를 해결하려면 포트 옵션을 사용하여 특정 포트(8500)를 기준으로 캡처하는 것이 좋습니다.

각 포트에서 통신이 필요한 서비스에 대한 자세한 내용은 해당 구성 요소의 해당 버전에 대한 TCP 및 UDP 포트 사용 설명서를 참조하십시오.



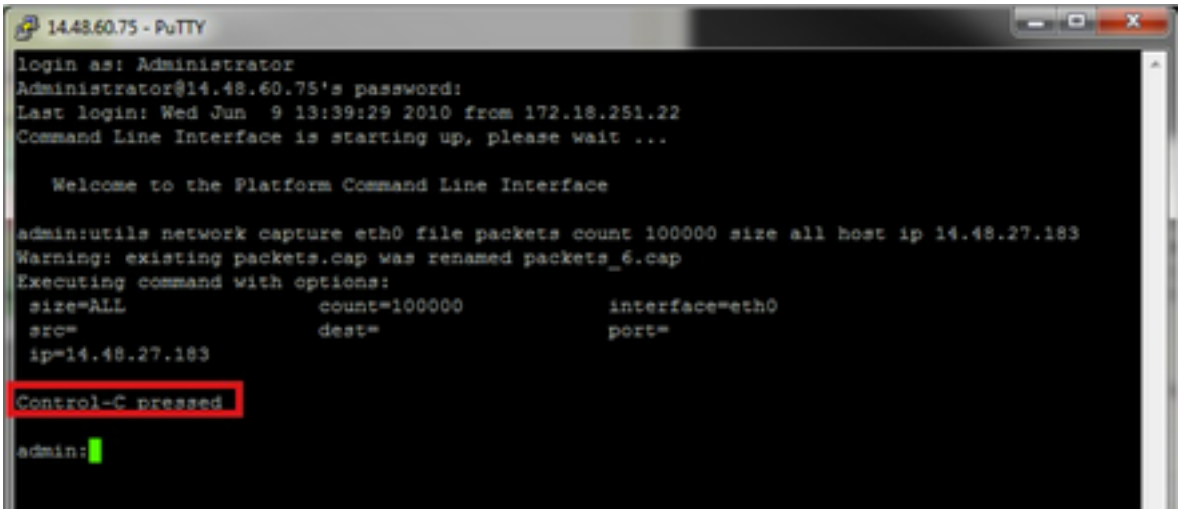
1d. 호스트 기반 캡처

VOS 및 특정 호스트의 문제를 해결하려면 'host' 옵션을 사용하여 특정 호스트에서 나가고 들어오는 트래픽을 필터링해야 할 수 있습니다.

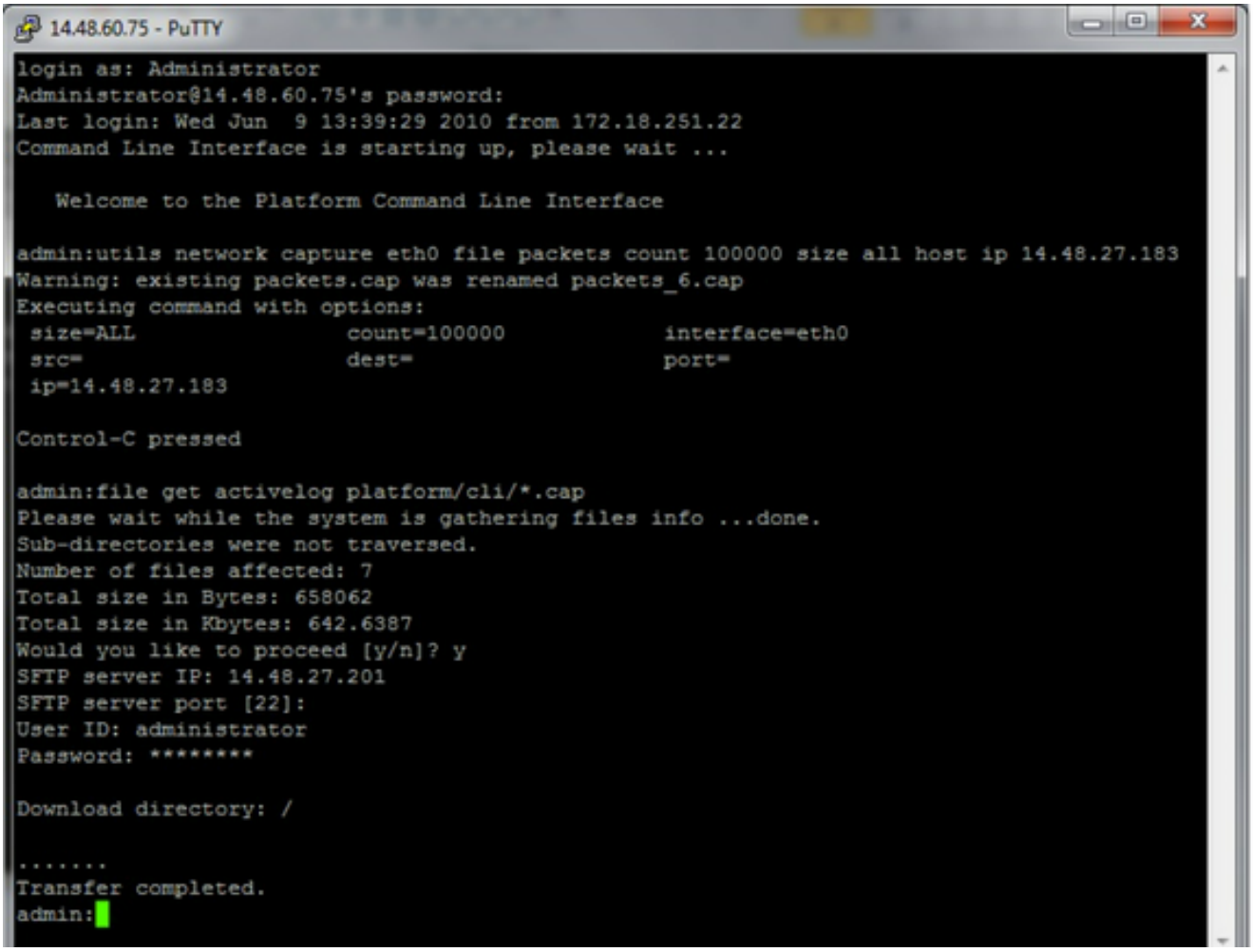
특정 호스트를 제외해야 할 수도 있으며, 이 경우에는 "!"를 사용합니다. 있습니다 예를 들면 **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

3. 문제 증상 재현 캡처가 시작되는 동안 필요한 패킷이 캡처에 포함되도록 문제 증상이나 상태

를 재현합니다. 문제가 간헐적으로 발생하는 경우 장기간 캡처를 실행해야 할 수 있습니다. 캡처가 끝나면 버퍼가 채워져서 캡처를 다시 시작하고 이전 캡처가 손실되지 않도록 이전 캡처의 이름이 자동으로 변경됩니다. 장기간 캡처가 필요한 경우 스위치에서 모니터 세션을 사용하여 네트워크 레벨에서 캡처합니다.

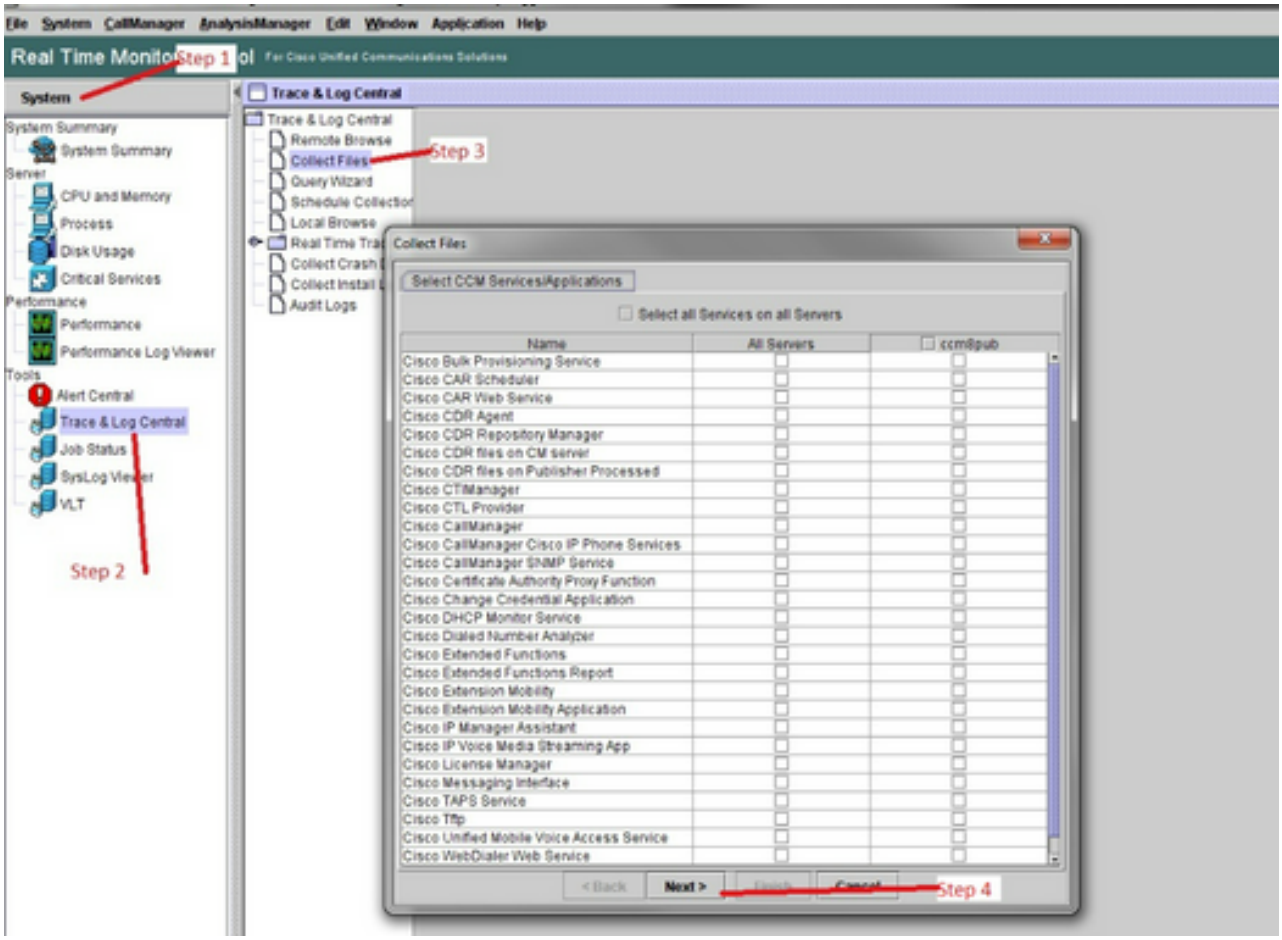
4. 캡처 중지 캡처를 중지하려면 **Ctrl** 키를 누르고 키보드에서 **C**를 누릅니다. 그러면 캡처 프로세스가 종료되고 캡처 덤프에 새 패킷이 추가되지 않습니다.
5. 

이 작업이 완료되면 캡처 파일은 'activelog platform/cli/' 위치에 서버에 저장됩니다
6. 서버에서 캡처 수집
캡처 파일은 서버의 "activelog platform/cli/" 위치에 저장됩니다. CLI를 통해 SFTP 서버로 또는 RTMT를 사용하여 로컬 PC로 파일을 전송할 수 있습니다. 4a. CLI를 통해 캡처 파일을 SFTP 서버로 전송
다음 명령을 사용하여 **file get activelog platform/cli/packets.cap** SFTP 서버에 packets.cap 파일을 수집합니다.
또는 서버에 저장된 모든 .cap 파일을 수집하려면 'file get activelog platform/cli/*.cap을 사용합니다
마지막으로 SFTP 서버 IP/FQDN, 포트, 사용자 이름, 비밀번호 및 디렉토리 정보를 입력합니다.

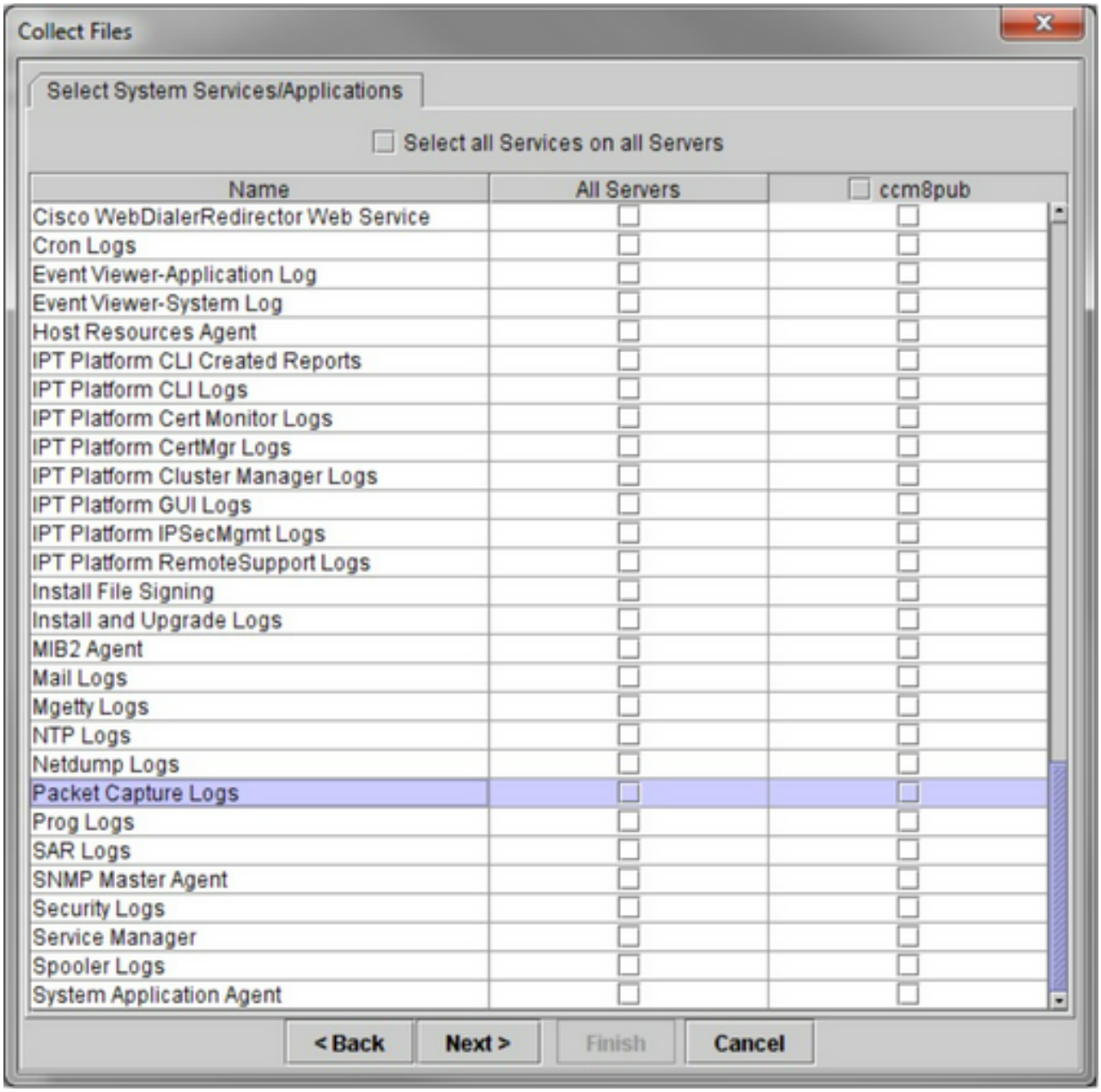


CLI는 SFTP 서버로의 파일 전송의 성공 또는 실패를 나타냅니다.

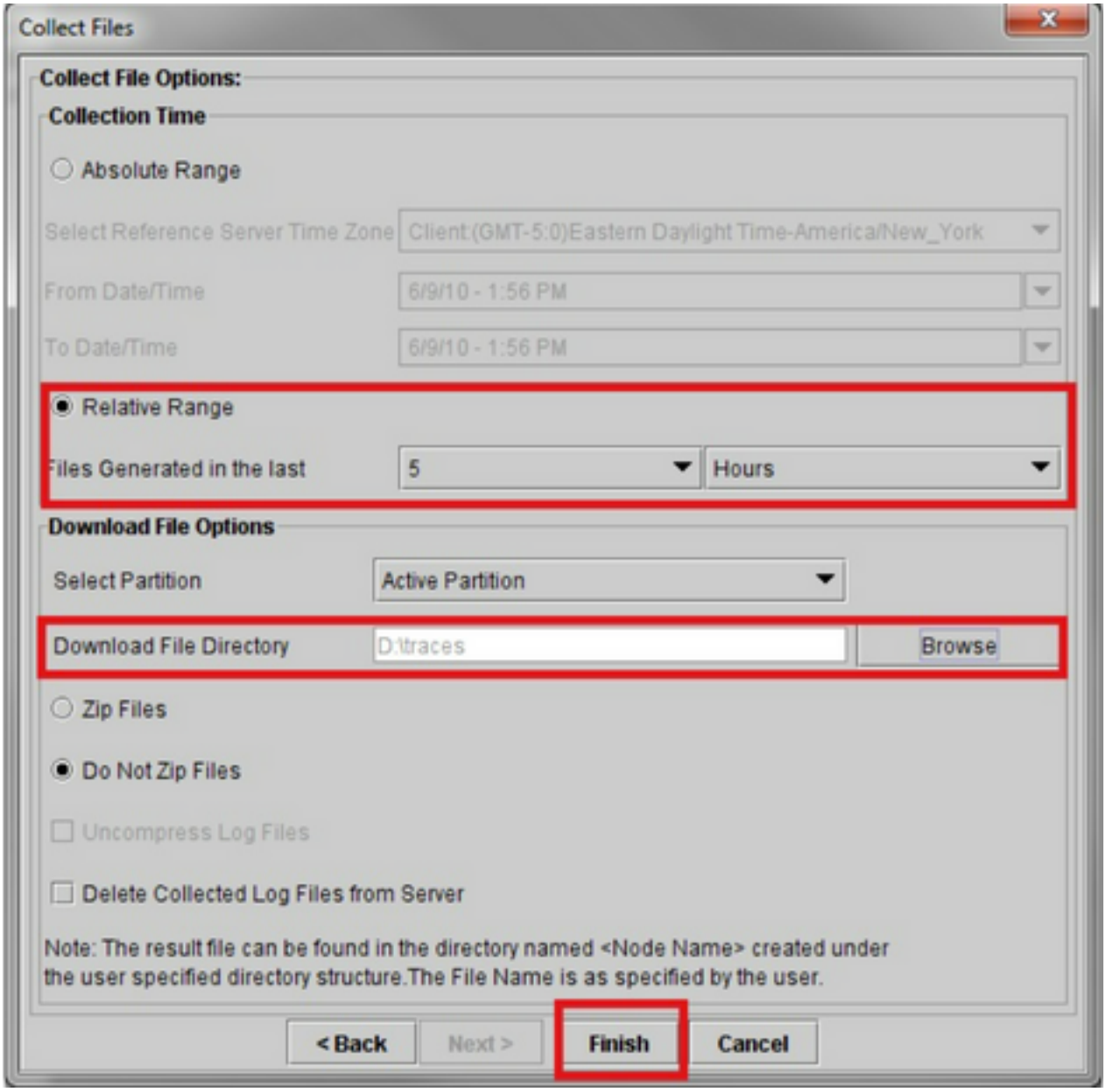
4b. RTMT를 사용하여 캡처 파일을 로컬 PC로 전송합니다.
RTMT를 시작합니다. 로컬 PC에 설치되지 않은 경우 VOS Administration(VOS 관리) 페이지에서 적절한 버전을 설치하고 Applications(애플리케이션) **->Plugins(플러그인) 메뉴로** 이동합니다.
System(**시스템**), **Trace & Log Central(추적 및 로그 센트럴)**을 차례로 클릭한 다음 Collect Files(**파일 수집)를** 두 번 클릭합니다. 첫 번째 **메뉴**에서 다음을 클릭합니다.



두 번째 메뉴에서 캡처가 수행된 서버의 **Packet Capture Logs(패킷 캡처 로그)** 확인란을 선택하고 **Next(다음)**를 클릭합니다.



마지막 화면에서 캡처가 수행된 시간 범위와 로컬 PC의 다운로드 디렉토리를 선택합니다.



RTMT는 이 창을 닫고 파일을 수집하고 지정된 위치에 로컬 PC에 저장합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.