

CUE에서 추적 데이터 설정 및 수집

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[추적 개요](#)

[AIM\(Advanced Integration Module\)과 NM\(Network Module\) 비교](#)

[추적 구성](#)

[추적 데이터 수집](#)

[추적 버퍼 작업](#)

[저장된 추적 로그 파일](#)

[FTP 서버로 추적](#)

[JTAPI 추적](#)

[추적 해제](#)

[기본 추적 다시 활성화](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Unity Express(CUE)의 추적 기능에 대한 개요를 제공합니다. Trace는 Cisco Unity Express의 디버그 기능으로 다양한 문제를 해결하는 데 사용됩니다. 추적 기능이 활성화되면 시스템 성능에 부정적인 영향을 미칠 수 있습니다. 이 문제로 인해 Cisco는 [Cisco 기술 지원](#)의 요청에서만 추적을 활성화하여 특정 문제에 대한 정보를 수집하는 것을 권장합니다. Lab의 시스템 또는 유지 보수 윈도우의 경우 추적 기능을 사용하여 Cisco Unity Express 동작을 트러블슈팅하고 이해할 수 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 CLI(Command-Line Interface)를 통해 Cisco Unity Express의 관리 및 사용에 대해 기본적으로 잘 알고 있는 것을 권장합니다.

사용되는 구성 요소

이 기능을 사용하려면 Cisco Unity Express 버전 1.0 이상이 필요합니다. 통합 방법(Cisco CallManager 또는 Cisco CallManager Express)은 중요하지 않습니다. 모든 샘플 구성 및 화면 출력은 Cisco Unity Express 버전 1.1.1에서 가져옵니다.

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

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

[추적 개요](#)

Cisco IOS® Software에 익숙한 사람들은 CLI와 강력한 디버그 기능에 익숙하지 않을 것입니다. Cisco Unity Express에는 기능과 비슷하지만 몇 가지 중요한 차이점이 있는 툴이 있습니다. Cisco Unity Express에서 **debug** 명령이 없습니다. 대신 **trace** 명령이 있습니다. 추적 기능은 메모리에 커널 버퍼 내에 메시지를 기록하는 진단 기능입니다. 이 메모리 공간은 최대 10MB까지 가능하며 로컬 추적 파일(atrace.log)에 주기적으로(구성된 경우), 외부 FTP 서버의 파일에 기록되거나 둘 다에 기록됩니다.

참고: atrace.log 파일 및 FTP 서버에 로깅된 추적 데이터는 일반 텍스트로 표시되지 않습니다. 진단을 위해서는 Cisco 기술 지원 센터로 데이터를 보내야 합니다.

Cisco Unity Express 모듈에 기록된 각 파일(atrace.log 및 messages.log 및 기타)을 외부 FTP 서버에 수동으로 복사할 수 있습니다.

Cisco Unity Express는 Cisco IOS Software의 syslog와 유사한 로그 기능도 지원합니다. 이러한 메시지는 운영 체제 및 다른 레벨로 분류되는 다른 애플리케이션 소스에서 온 것입니다. Cisco Unity Express의 다른 파일(messages.log)에 기록되는 정보, 경고, 오류 및 치명적 메시지입니다. 또한 외부 syslog 서버 및 Cisco Unity Express의 콘솔에 쓸 수 있습니다.

CUE 모듈이 외부 syslog 서버에 INFO 메시지를 기록하도록 하려면 CUE 모듈에서 다음 명령을 실행합니다.

```
CUE> config t
    CUE(config)>log server
```

기본적으로 치명적 메시지만 AIM에 기록됩니다. 대부분의 일반적인 문제에서는 messages.log 파일과 오류에 대한 추적 정보가 필요합니다.

Cisco Technical Support에서 특정 추적을 수집하도록 지시하는 경우 활성화해야 할 특정 추적 및 캡처 방법에 동의해야 합니다. 예를 들어 실시간 추적을 사용하거나 추적 메모리 버퍼를 보거나 FTP 서버에서 추적 데이터를 캡처할 수 있습니다.

[AIM\(Advanced Integration Module\)과 NM\(Network Module\) 비교](#)

Cisco Unity Express에는 AIM과 NM이라는 두 가지 하드웨어 모델이 있습니다. 추적 기능에는 두 가지 중요한 차이점이 있습니다.

AIM	NM
atrace.log 파일은 기본적으로 비활성화되어 있습니다. log trace local enable 명령을 시작하고 log trace local disable 명령을 실행하여 중지합니다.	atrace.log 파일은 기본적으로 활성화되어 있습니다. 외부 서버로의 추적도 지원됩니다.
atrace.log의 최대 크기는 10MB입니다.	atrace.log의 최대 크기는 100MB입니다.
atrace.log 파일이 가득 차면 래핑되지 않습니다.	atrace.log 파일이 꽉 차면 래핑됩니다.

추적 데이터를 활성화하고 보는 방법은 이 문서의 뒷부분에서 자세히 설명합니다. AIM은 기본적으로 Flash 자체에 추적 정보를 저장하지 않습니다. 또한 추적 데이터를 위한 내부 스토리지 용량이 활성화된 경우 훨씬 제한됩니다. 이는 AIM의 내부 컴팩트 플래시 카드의 수명이 이 카드에 발급된 쓰기 수와 관련이 있기 때문입니다. 지속적으로 흔적을 쓰는 것은 수명을 크게 줄여줍니다.

참고: **log trace local disable** 명령과 최대 크기에 도달한 AIM에서 atrace.log 파일을 다시 시작하려면 구성 모드에서 **log trace local enable** 명령을 실행합니다. 이렇게 하면 원래 atrace.log 파일이 제거되고 새 파일이 시작됩니다.

로그 기능에는 다음과 같은 중요한 차이점도 있습니다.

AIM	NM
Fatal 메시지만 기본적으로 messages.log 파일에 기록됩니다. 모든 메시지를 보려면 컨피그레이션 모드에서 명령 로그 콘솔 정보 를 실행합니다.	모든 메시지 범주가 messages.log 파일에 기록됩니다.

추적 구성

주의: Cisco Unity Express의 추적 구성은 시스템 성능에 부정적인 영향을 미칠 수 있습니다. 특히 활성화된 로컬 로그 파일에 쓸 때 그렇습니다. 여기에는 프롬프트 지연, DTMF(Dual-Tone Multifrequency) 톤 응답 시간, 녹음 또는 재생된 오디오의 품질 문제가 포함될 수 있습니다. 추적을 주의하여 구성합니다.

추적 컨피그레이션은 추적 메모리 버퍼에 기록되는 메시지 유형을 제어합니다. 이 10MB 버퍼는 항상 래핑되므로 최신 추적 정보가 표시됩니다. 시스템은 활동 레벨이 다르기 때문에 이 추적 버퍼가 다루는 기간을 알 수 없습니다. 그러나 구성된 경우 버퍼가 로컬 atrace.log 파일 또는 FTP 서버에 기록됩니다.

Cisco Unity Express CLI에서만 추적을 구성할 수 있습니다. 활성화된 현재 추적을 보려면 **show trace** 명령을 실행합니다.

예를 들면 다음과 같습니다.

```
vnt-3745-44a#service-module service-Engine 4/0 session
Trying 172.18.106.66, 2129 ... Open
vnt-nm-cue#
vnt-nm-cue#show trace
```

MODULE	ENTITY	SETTING
ccn	Engine	00000001
ccn	LibLdap	00000001
ccn	SubsystemAppl	00000001
ccn	ManagerAppl	00000001
ccn	ManagerChannel	00000001
ccn	SubsystemJtapi	00000001
ccn	SubsystemSip	00000001
ccn	StackSip	00000001
ccn	SubsystemHttp	00000001
ccn	VbrowserCore	00000001
ccn	SubsystemCmt	00000001
ccn	LibMedia	00000001
ccn	ManagerContact	00000001
ccn	StepCall	00000001
ccn	StepMedia	00000001
config-ccn	sip-subsystem	00000001
config-ccn	jtapi-subsystem	00000001
config-ccn	sip-trigger	00000001
config-ccn	jtapi-trigger	00000001
config-ccn	http-trigger	00000001
config-ccn	group	00000001
config-ccn	application	00000001
config-ccn	script	00000001
config-ccn	prompt	00000001
config-ccn	miscellaneous	00000001
voicemail	database	0000008f
voicemail	mailbox	0000003f
voicemail	message	0000002f
webInterface	initwizard	00000001

vnt-nm-cue#

NM 및 AIM 모두에 대한 기본 추적 설정입니다. AIM은 기본적으로 이러한 추적의 출력을 아무 곳에도 저장하지 않습니다. 대부분의 일반적인 트러블슈팅에서는 이러한 추적 수준만으로도 충분합니다. 최근에 문제가 발생한 경우 추적 메모리 버퍼에 일부 기록이 있을 수 있습니다.

추적을 활성화하려면 **trace module entity activity** 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
vnt-nm-cue#trace ccn subsystemsip dbug
```

다음은 CUE 1.1.1용 모듈입니다.

```
vnt-nm-cue#trace ?
```

```
BackupRestore Module
all          Every module, entity and activity
ccn         Module
config-ccn  Module
dns         Module
superthread Module
udppacer    Module
voicemail   Module
webInterface Module
```

각 모듈에는 많은 엔티티가 있습니다. 활동 레벨은 다소 다릅니다(일반적으로 모듈에서 모듈로). 일반적으로 모든 엔티티에는 최소한 디버그(DBUG로 입력됨)와 모든 활동 수준이 있습니다. 일반적으로 디버그 활동 수준이면 충분합니다.

trace module entity activity 명령은 원하는 모든 모듈 및 엔티티에 대한 추적이 활성화될 때까지 여러 번 실행할 수 있습니다.

어떤 흔적을 설정하든 상관없다.다시 로드한 후 시스템은 기본 추적 레벨로 돌아갑니다.이러한 기본 설정을 변경하여 리부팅을 유지하려면 **log trace boot** 명령을 실행해야 합니다.

추적 데이터 수집

모든 추적이 구성되면 데이터가 메모리 버퍼에 기록됩니다.그런 다음 메시지가 수신될 때 실시간으로 표시할 수도 있고 이벤트 또는 테스트가 발생한 후 버퍼를 볼 수도 있습니다.

추적 버퍼 작업

메모리 기반 추적 버퍼는 추적을 검사하는 첫 번째 위치 중 하나입니다.실시간으로 볼 수 있으므로 추적 메시지가 들어오는 대로 표시됩니다.대안으로 메모리 버퍼의 전체 또는 일부를 표시하고 검사할 수 있습니다.

실시간 추적

실시간 추적은 제어된 시스템에서 문제를 해결할 때 특히 유용합니다(동시 통화가 많지 않거나 시스템이 아직 프로덕션 중이 아닌 경우). 추적 출력 줄은 종종 줄 바꿈되며 정보는 거의 항상 읽을 수 있는 것보다 빠르게 스크롤되므로 실시간 추적을 켜기 전에 콘솔 출력을 텍스트 파일에 기록합니다.이를 통해 나중에 텍스트 편집기에서 정보를 볼 수 있습니다.예를 들어 Microsoft 하이퍼터미널에서는 **Transfer > Capture Text**를 선택한 다음 캡처 파일을 지정할 수 있습니다.

실시간 추적 기능은 시스템에 가장 큰 영향을 미칩니다.주의해서 사용하십시오.

실시간 추적 정보를 보려면 **show trace buffer tail** 명령을 실행합니다.예를 들면 다음과 같습니다.

```
vnt-nm-cue>show trace buffer tail
Press <CTRL-C> to exit...
295 06/22 10:39:55.428 TRAC TIMZ 1 EST EDT 18000
2019 06/22 11:20:15.164 ACCN SIPL 0 receive 1098 from 172.18.106.66:54948
2020 06/22 11:20:15.164 ACCN SIPL 0 not found header for Date
2020 06/22 11:20:15.164 ACCN SIPL 0 not found header for Supported
2020 06/22 11:20:15.164 ACCN SIPL 0 not found header for Min-SE
2020 06/22 11:20:15.165 ACCN SIPL 0 not found header for Cisco-Guid
2020 06/22 11:20:15.165 ACCN SIPL 0 not found header for Remote-Party-ID
2020 06/22 11:20:15.165 ACCN SIPL 0 not found header for Timestamp
2020 06/22 11:20:15.165 ACCN SIPL 0 not found header for Call-Info
2020 06/22 11:20:15.165 ACCN SIPL 0 not found header for Allow-Events
2020 06/22 11:20:15.166 ACCN SIPL 0 -----
INVITE sip:18999@172.18.106.88:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.106.66:5060;branch=z9hG4bK1678
From: "Caller1" <sip:201@172.18.106.66>;tag=23F5B364-22C9
To: <sip:18999@172.18.106.88>
Date: Tue, 22 Jun 2004 15:20:14 GMT
Call-ID: 7E86EC94-C39611D8-AF50DA50-D3EDBBC9@172.18.106.66
Supported: 100rel,timer
Min-SE: 1800
Cisco-Guid: 2092538615-3281392088-2941114960-3555572681
...
```

이 정보는 Cisco IOS Software 디버그 출력과 비슷하게 스크롤됩니다.한 가지 차이점은 **Control-C** 키 조합만 눌러 중지하면 된다는 것입니다.

추적 메모리 버퍼 표시

메모리의 추적 버퍼 크기는 최대 10MB입니다. 몇 가지 명령줄 매개 변수는 다음과 같습니다.

```
vnt-nm-cue>show trace buffer ?
<cr>
containing    Only display events matching a regex pattern
long          Show long format
short         Show short format
tail          Wait for events and print them as they occur
|             Pipe output to another command
```

대부분의 경우 사용해야 하는 유일한 옵션은 **show trace buffer long**입니다. 출력이 한 번에 한 페이지씩 표시되도록 페이지 지정 키워드를 끝에 추가할 수 있습니다. 긴 형식에는 많은 오류 및 반환 코드에 대한 확장 텍스트가 포함되지만 짧은 형식에는 16진수 코드만 포함될 수 있습니다. 일반적으로 터미널 프로그램의 캡처 기능을 사용하여 모든 항목을 가져온 다음 텍스트 편집기에서 Find 함수를 사용하여 특정 항목을 검색하는 것이 더 쉽지만 특정 오류 조건만 검색해야 하는 경우 *containing* 키워드가 유용합니다. 정규식 매개 변수를 사용하여 출력을 디스플레이로 필터링할 수 있습니다.

참고: *containing* 키워드로 특정 통화 또는 포트 번호를 검색할 수 없습니다.

```
vnt-nm-cue>show trace buffer long paged
2029 06/24 17:48:40.479 ACCN SIPL 0 receive 1096 from 172.18.106.66:49255
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Date
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Supported
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Min-SE
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Cisco-Guid
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Remote-Party-ID
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Timestamp
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Call-Info
2030 06/24 17:48:40.480 ACCN SIPL 0 not found header for Allow-Events
2030 06/24 17:48:40.481 ACCN SIPL 0 -----
INVITE sip:18900@172.18.106.88:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.106.66:5060;branch=z9hG4bK1128
From: "Caller1" <sip:201@172.18.106.66>;tag=2FA6AE58-20E5
To: <sip:18900@172.18.106.88>
Date: Thu, 24 Jun 2004 21:48:40 GMT
Call-ID: 16EEB21C-C55F11D8-BF05DA50-D3EDBBC9@172.18.106.66
Supported: 100rel,timer
Min-SE: 1800
Cisco-Guid: 384701940-3311342040-3204635216-3555572681
User-Agent: Cisco-SIPGateway/IOS-12.x
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE,
NOTIFY, INFO, UPDATE, REGISTER
CSeq: 101 INVITE
Max-Forwards: 6
```

clear trace 명령을 실행하여 추적 메모리 버퍼를 지웁니다. 대부분의 문제 해결 상황에서는 수집할 추적을 설정하고, **clear trace** 명령을 실행하여 버퍼를 지우고, 추적을 수집할 작업을 다시 생성한 다음 **show trace buffer long** 명령의 출력을 캡처할 수 있습니다. 이 방법은 재현할 수 있는 문제에 대한 추적을 수집하는 가장 효과적인 방법입니다.

저장된 추적 로그 파일

NM 및 AIM(활성화된 경우)에서 추적은 `atrace.log` 파일에 기록됩니다. `show logs` 명령은 사용 가능한 모든 로그 파일을 표시합니다.

```
vnt-nm-cue>show logs
dmesg
```

```
syslog.log
atrace.log
atrace.log.prev
klog.log
messages.log
messages.log.prev
root_javacore828.1087272313.txt
tomcat_javacore1094.1087272313.txt
workflow_javacore1096.1087272313.txt
```

중요한 파일은 atrace.log 및 messages.log입니다.messages.log 파일에는 모든 시스템 메시지가 포함되어 있습니다(AIM의 경우 Fatal 및 Error 메시지만 포함). 특히 AIM에서 messages.log 파일이 기록 정보를 포함하는 유일한 로그 파일인 경우가 있습니다._javacore 파일은 시스템을 다시 시작할 때 작성되며 일반적으로 다른 파일(dmesg, syslog.log, klog.log)만큼 중요하지 않습니다. atrace.log.prev 및 messages.log.prev 파일도 중요합니다(있는 경우). 이전 버전의 atrace.log 및 messages.log입니다.예를 들어 atrace.log 파일이 가득 차면 atrace.log.prev에 복사되고 새 atrace.log 파일이 시작됩니다.이전 atrace.log.prev가 대체되고 정보가 손실됩니다.

각 파일은 FTP 서버에 개별적으로 복사해야 합니다.

atrace.log 파일은 큰 파일(NM에서는 최대 100MB, AIM에서는 10MB)이므로 일반적으로 FTP 서버에 복사하려고 합니다.copy log 명령은 이 용도로 사용됩니다.이 예에서는 FTP 사용자 이름(jdoe) 및 비밀번호(mybass)가 URL의 일부입니다.

```
vnt-nm-cue>copy log atrace.log url ftp://jdoe:mybass@172.18.106.10/cue/atrace.log
% Total      % Received % Xferd  Average Speed           Time         Curr.
              Dload  Upload Total    Current  Left      Speed
100 1387k    0      0 100 1387k      0 4476k 0:00:00 0:00:00 0:00:00 6104k
```

참고: atrace.log 파일은 일반 텍스트 파일이 아닙니다.진단을 위해서는 Cisco 기술 지원 센터로 보내야 합니다.

Cisco Unity Express 모듈 자체에서 저장된 로그 파일을 볼 수도 있습니다.그러나 일반 텍스트에서 파일이 제대로 변환되지 않으므로 atrace.log 파일에 대해서는 이 옵션을 사용하지 않는 것이 좋습니다.다음은 messages.log 파일을 사용하는 예입니다.

```
cue-3660-41a#show log name messages.log
#!/bin/cat
19:46:08 logmgr: BEGIN FILE
19:46:08 logmgr: START
<45>Feb 26 19:46:08 localhost syslog-ng[134]: syslog-ng version 1.6.0rc1 starting
<197>Feb 26 19:46:08 localhost syslog-ng:      INFO startup.sync syslog-ng arrived
phase online
<197>Feb 26 19:46:10 localhost err_handler:      INFO Recovery Recovery startup :CUE
Recovery Script started.
<197>Feb 26 19:46:10 localhost err_handler:      INFO Recovery Recovery LDAPVerify
Verifying LDAP integrity
...
```

참고: show log name 명령으로 로그 파일을 표시할 때 Control-C 키 조합을 눌러 명령 출력을 중단합니다.그렇게 한 후 프롬프트로 돌아가려면 몇 초가 걸립니다.

Cisco Unity Express에 저장된 atrace.log 파일에 대해 show trace store 명령(또는 show trace store-prev 명령)을 실행합니다.

```
vnt-nm-cue>show trace store ?
<cr>
```

```
containing    Only display events matching a regex pattern
long          Show long format
short        Show short format
tail         Wait for events and print them as they occur
|            Pipe output to another command
```

```
vnt-nm-cue>show trace store long paged
```

```
236 02/26 14:46:24.029 TRAC TIMZ 0 UTC UTC 0
236 02/26 14:46:24.031 TRAC TIMZ 0 UTC UTC 0
885 06/04 13:14:40.811 WFSP MISC 0 WFSysdbLimits::WFSysdbLimits hwModuleType=NM
885 06/04 13:14:40.812 WFSP MISC 0 WFSysdbProp::getProp
885 06/04 13:14:40.812 WFSP MISC 0 keyName = limitsDir
str = /sw/apps/wf/ccnapps/limits
885 06/04 13:14:40.819 WFSP MISC 0 WFSysdbProp::getNodeXml
885 06/04 13:14:40.819 WFSP MISC 0 WFSysdbProp::getProp
885 06/04 13:14:40.820 WFSP MISC 0 keyName = limits
str =
885 06/04 13:14:40.822 WFSP MISC 0 WFSysdbProp::getNodeXml(str, str)
885 06/04 13:14:40.822 WFSP MISC 0 WFSysdbProp::getProp
885 06/04 13:14:40.822 WFSP MISC 0 keyName = app
str =
```

추적 버퍼를 메모리에 표시할 때 긴 형식이 중요합니다. **show trace store long** 명령을 실행합니다. 이 정보는 `atrace.log` 파일의 맨 처음 부분부터 제공됩니다. 이 파일은 NM에서 최대 100MB 또는 AIM에서 10MB까지 가능합니다. `containing` 키워드는 특정 이벤트를 검색해야 하는 경우 경우에 유용합니다.

참고: AIM의 `atrace.log` 파일이 최대 크기로 증가하면 로그 파일에 추적을 로깅하지 않습니다. 추적 로깅을 다시 시작하려면 다음 명령을 실행합니다.

```
VNT-AIM-CUE1>configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
VNT-AIM-CUE1(config)>log trace local disable
```

```
VNT-AIM-CUE1(config)>log trace local enable
```

참고: 이 명령은 이전 `atrace.log` 파일을 제거하고 새 파일을 시작합니다.

[FTP 서버로 추적](#)

특히 AIM에서 대량의 데이터를 추적하는 가장 좋은 방법은 FTP 서버에 직접 정보를 로깅하는 것입니다. 오프라인 추적은 성능에 미치는 영향이 가장 적습니다. 이는 컨피그레이션 모드에서 수행됩니다.

참고: Cisco Unity Express 시스템이 AIM인 경우 이 명령이 필요합니다. 네트워크 모듈은 기본적으로 정보 레벨 이상을 기록합니다.

```
vnt-nm-cue(config)>log console info
```

참고: 공간 이유로 이 명령이 두 번째 행으로 내려갔습니다.

```
vnt-nm-cue(config)>log trace server url
```

```
ftp://172.18.106.10/path/ username jdoe password mypass
```

참고: Cisco Unity Express 버전 7.x를 사용하는 경우 이전 명령을 `로그 추적 서버 url "ftp://172.18.106.10/path/" 사용자 이름 jdoe 비밀번호 mypass`로 사용합니다.

참고: FTP 서버로 로그를 보낼 때 **로그 추적 서버 활성화도** 구성해야 합니다.

```
vnt-nm-cue(config)>log trace server enable
```

참고: 시스템은 FTP 서버의 지정된 경로에 파일을 생성합니다.지정된 디렉토리에 파일을 만들고 수정할 수 있는 권한이 있어야 하며, 이 권한이 있어야 합니다.파서는 사용자 이름과 비밀번호를 추출합니다. 이 비밀번호는 컨피그레이션 파일 자체에 암호화된 것으로 나타납니다(**show running-config**).

참고: FTP 서버에 로깅된 추적 파일은 일반 텍스트 파일이 아닙니다.진단을 위해서는 Cisco 기술 지원 센터로 보내야 합니다.

JTAPI 추적

JTAPI 추적은 Cisco Unity Express의 다른 추적 기능과 별개입니다.Cisco CallManager 환경에만 적용됩니다.현재 활성화된 JTAPI 추적을 보려면 **show ccn trace jtapi** 명령을 실행합니다.

참고: 기본적으로 모든 JTAPI 추적은 비활성화되어 있습니다.

```
VNT-AIM-CUE1>show ccn trace jtapi
```

```
Warning: 0
Informational: 0
Jtapi Debugging: 0
Jtapi Implementation: 0
CTI Debugging: 0
CTI Implementation: 0
Protocol Debugging: 0
Misc Debugging: 0
```

모든 추적을 활성화하려면 다음 명령을 실행합니다.

```
VNT-AIM-CUE1>ccn trace jtapi debug all
```

You will have to reload the system for your changes to take effect

```
VNT-AIM-CUE1>ccn trace jtapi informational all
```

You will have to reload the system for your changes to take effect

```
VNT-AIM-CUE1>ccn trace jtapi warning all
```

You will have to reload the system for your changes to take effect

```
VNT-AIM-CUE1>show ccn trace jtapi
```

```
Warning: 1
Informational: 1
Jtapi Debugging: 1
Jtapi Implementation: 1
CTI Debugging: 1
CTI Implementation: 1
Protocol Debugging: 1
Misc Debugging: 1
```

시스템을 다시 로드합니다.여기에 표시된 동일한 **ccn 추적 명령**을 실행하여 나중에 이 명령을 비활성화합니다.그러나 각 명령 앞에 **no 키워드**를 입력합니다.예를 들어, **ccn trace jtapi debug all**을 실행하지 않습니다.이는 특히 AIM에서 기억해야 할 중요한 단계입니다.이 단계를 수행하지 않으면 잠재적인 성능이 저하되고 AIM에서 콤팩트 플래시 카드의 수명이 줄어듭니다.

다시 로드한 후 시스템은 CiscoJtapi1.log 및 CiscoJtapi2.log 파일(첫 번째 파일이 가득 찬 경우)을 쓰기 시작합니다.

show log name CiscoJtapi1.log 명령을 실행하면 Cisco Unity Express에서 이러한 로그를 볼 수 있습니다. 로그 파일을 FTP 서버에 복사한 다음 오프라인으로 정보를 보려면 **copy log CiscoJtapi1.log url ftp://user:passwd@ftpservipaddr/** 명령을 실행합니다.

추적 해제

no trace module entity activity CLI 명령을 사용하여 추적을 해제할 수 있습니다. 확실하지 않은 경우 모든 항목을 해제하기 위해 추적을 모두 실행할 수 없습니다.

또한 추적 설정을 그대로 두고 컨피그레이션 모드에서 **no log trace local enable** 명령을 사용하여 추적 파일 쓰기를 비활성화할 수 있습니다. AIM에서는 과도한 쓰기가 내부 플래시 카드의 수명을 줄여주기 때문에 이 옵션을 권장합니다. 예를 들면 다음과 같습니다.

```
vnt-nm-cue>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vnt-nm-cue(config)>no log trace local enable
vnt-nm-cue(config)>
```

FTP 서버에 대한 추적을 비활성화하려면 다음 명령을 실행합니다.

```
vnt-nm-cue>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vnt-nm-cue(config)>log trace server disable
vnt-nm-cue(config)>
```

기본 추적 다시 활성화

특정 문제를 해결할 때 특정 추적만 활성화하는 것이 합리적입니다. 완료되면 기본 추적 설정을 다시 활성화하는 것이 좋습니다. **no trace all** 명령을 사용하여 모든 추적을 비활성화하면 됩니다. 다음으로, 다음 명령을 Cisco Unity Express CLI에 붙여넣어 기본 추적을 활성화합니다(컨피그레이션 모드가 아님).

```
trace ccn engine debug
trace ccn libldap debug
trace ccn subsystemappl debug
trace ccn managerappl debug
trace ccn managerchannel debug
trace ccn subsystemjtapi debug
trace ccn subsystemsip debug
trace ccn stacksip debug
trace ccn subsystemhttp debug
trace ccn vbrowsercore debug
trace ccn subsystemcmt debug
trace ccn libmedia debug
trace ccn managercontact debug
trace ccn stepcall debug
trace ccn stepmedia debug
trace config-ccn sip-subsystem debug
trace config-ccn jtapi-subsystem debug
trace config-ccn sip-trigger debug
trace config-ccn jtapi-trigger debug
trace config-ccn http-trigger debug
trace config-ccn group debug
trace config-ccn application debug
```

```
trace config-ccn script debug
trace config-ccn prompt debug
trace config-ccn miscellaneous debug
trace voicemail database query
trace voicemail database results
trace voicemail database transaction
trace voicemail database connection
trace voicemail database execute
trace voicemail mailbox login
trace voicemail mailbox logout
trace voicemail mailbox send
trace voicemail mailbox save
trace voicemail mailbox receive
trace voicemail mailbox delete
trace voicemail message create
trace voicemail message dec
trace voicemail message delete
trace voicemail message get
trace voicemail message inc
trace webinterface initwizard init
```

관련 정보

- [음성 기술 지원](#)
- [음성 및 통합 커뮤니케이션 제품 지원](#)
- [Cisco IP 텔레포니 문제 해결](#)
- [기술 지원 및 문서 - Cisco Systems](#)