

UCCEトレースログの設定と収集

内容

[概要](#)

[要件](#)

[トレース設定とログ収集](#)

[Finesse](#)

[Cisco Agent Desktop](#)

[Cisco Supervisor Desktop](#)

[CTIOSクライアントデスクトップ](#)

[PGのトレースとログに関するクライアント関連の問題](#)

[CAD同期サービスのデバッグ](#)

[CAD 6.0\(X\) RASCALサーバのデバッグ](#)

[チャットサーバのデバッグ](#)

[その他のPG関連のトレースとログ](#)

[CallManager PIMのトレースの有効化](#)

[CUCMでのトレースの有効化](#)

[Java Telephony Application Programming Interface\(JTAPI\)Gateway\(JGW\)を有効にする](#)

[アクティブ側でのCTIサーバ\(CTISVR\)トレースの有効化](#)

[トレースVRU PIMの有効化](#)

[両方のCTIOSサーバでCTIOSサーバトレースを有効にする](#)

[Active PGでOpen Peripheral Controller\(OPC\)トレースを有効にする](#)

[アクティブPGでのEagtpimトレースの有効化](#)

[Dumplogユーティリティを使用したログのプル](#)

[CVPサーバでのトレースの有効化](#)

[アウトバウンドダイヤラ関連のトレースおよびログ収集](#)

[プルログ](#)

[輸入業者について](#)

[キャンペーンマネージャ](#)

[ルータプロセスでのルータログの有効化](#)

[ルータのログのプル](#)

[ゲートウェイトレース\(SIP\)](#)

[CUSPトレース](#)

[トレースのためのCLIの使用](#)

[CLIの例](#)

概要

このドキュメントでは、クライアントの Cisco Unified Contact Center Enterprise (UCCE)、ペリフェラル ゲートウェイ (PG) サービス、Cisco Customer Voice Portal (CVP)、Cisco UCCE

アウトバウンド ダイアラ、Cisco Unified Communications Manager (CallManager) (CUCM)、および Cisco ゲートウェイでトレースを設定する方法について説明します。

要件

次の項目に関する知識があることが推奨されます。

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

トレース設定とログ収集

注：

このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \(登録ユーザ専用 \)](#) を使用してください。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

debug コマンドを使用する前に、「[デバッグ コマンドの重要な情報](#)」を参照してください。

Finesse

セキュアシェル(SSH)を使用してFinesseサーバにログインし、必要なログを収集するために次のコマンドを入力します。ログがアップロードされるSSH FTP(SFTP)サーバを特定するよう求められます。

ログ

インストールログ

デスクトップログ

サーバログ

プラットフォームTomcatログ

音声オペレーティングシステム(VOS)のインストールログ

コマンド

file get install desktop-install.log

file get activelog desktop recurs
compress

file get activelog

platform/log/servm*.* compress

file get activelog tomcat/logs

recurs compress

file get install install install.log

Cisco Agent Desktop

この手順では、デバッグファイルを作成して収集する方法について説明します。

1. エージェントコンピュータで、C:\Program Files\Cisco\Desktop\Config directory and open the Agent.cfg ファイルに移動します。
2. デバッグのしきい値をOFFからDEBUGに変更します。TRACEは、より深いレベルで使用できます。

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

3. Size=3000000 (6つのゼロ) であることを確認します。
4. 設定ファイルを保存します。
5. エージェントプログラムを停止します。
6. C:\Program Files\Cisco\Desktop\log directoryディレクトリ内のすべてのファイルを削除します。
7. エージェントプログラムを起動し、問題を再現します。
8. 次のデバッグファイルが作成され、C:\Program Files\Cisco\Desktop\logに配置されます。

```
agent0001.dbgctiosclientlog.xxx.log
```

Cisco Supervisor Desktop

この手順では、デバッグファイルを作成して収集する方法について説明します。

1. エージェントコンピュータで、C:\Program Files\Cisco\Desktop\Config directory and open the supervisor.cfg ファイルに移動します。
2. デバッグのしきい値をOFFからDEBUGに変更します。TRACEは、より深いレベルで使用できます。

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

3. Size=3000000 (6つのゼロ) であることを確認します。
4. 設定ファイルを保存します。
5. エージェントプログラムを停止します。

6. C:\Program Files\Cisco\Desktop\log directoryディレクトリ内のすべてのファイルを削除します。

7. エージェントプログラムを起動し、問題を再現します。supervisor0001.dbgという名前のデバッグファイルが作成され、C:\Program Files\Cisco\Desktop\logに配置されます。

CTIOSクライアントデスクトップ

CTIOSクライアントがインストールされているクライアントPCで、トレースを起動するためにRegedt32を使用します。次の設定を変更します。

Release	レジストリの場所	デフォルト値	Change
7.xより前のリリース	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0x07	値を0xffffに増やします
リリース7.x以降	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOSトレース	0x40000307	トラブルシューティング

デフォルト出力が作成され、c:\Program Files\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\install directoryディレクトリのCtiosClientLogという名前のテキストファイルに保存されます。

PGのトレースとログに関するクライアント関連の問題

CAD同期サービスのデバッグ

CAD Sync Serviceをデバッグするための設定を次に示します。

設定値	値
コンフィギュレーション ファイル	DirAccessSynSvr.cfg
既定の場所	C:\Program Files\Cisco\Desktop\config
一般的な問題	Threshold=DEBUG
出力ファイル	DirAccessSynSvr.log

CAD 6.0(X) RASCALサーバのデバッグ

CAD 6.0(X) RASCALサーバをデバッグするための設定を次に示します。

設定値	値
コンフィギュレーション ファイル	FCRasSvr.cfg
既定の場所	C:\Program Files\Cisco\Desktop\config
一般的な問題	範囲= 1 ~ 4、50、3000 ~ 8000
LDAP関連の問題 :	範囲= 4000 ~ 4999
LRM関連の問題 :	範囲= 1999 ~ 2000
データベース関連の問題	範囲= 50 ~ 59
出力ファイル	FCRasSvr.log、FCRasSvr.dbg
既定の場所	C:\Program Files\Cisco\Desktop\log

チャットサーバのデバッグ

チャットサーバをデバッグする設定は次のとおりです。

設定値	値
コンフィギュレーション ファイル	FCCServer.cfg
既定の場所	C:\Program Files\Cisco\Desktop\config
一般的な問題	Threshold=DEBUG
出力ファイル	FCCServer.log、FCCServer.dbg
既定の場所	C:\Program Files\Cisco\Desktop\log

その他のPG関連のトレースとログ

ログ収集に関しては、[Dumplogユーティリティを使用してログをプルする](#)を参照してください。

CallManager PIMのトレースの有効化

プロセスモニタリング(procmon)ユーティリティを使用して、トレースレベルをオンまたはオフにします。次のコマンドは、CallManagerペリフェラルインターフェイスマネージャ(PIM)トレースをオンにします。

```
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
```

このprocmonコマンドは、CallManager PIMトレースをオフにします。

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

CUCMでのトレースの有効化

この手順では、CUCMトレースをオンにする方法について説明します。

1. [Call Manager Unified Serviceability]に移動します。
2. [Trace/Configuration]を選択します。
3. [CM Services]を選択します。
4. [CTIManager (Active)]を選択します。
5. 右上の[SDL Configuration]を選択します。
6. SDLトレースの[Pretty Printを無効にする]以外をすべて有効にします。

7. ファイルの数とそのサイズはデフォルト値のままにします。

8. Real-Time Monitoring Tool(RTMT)で、Cisco Call ManagerとCisco Computer Telephony Integration(CTI)Managerを収集します。どちらもシステム診断インターフェイス(SDI)と信号分散層(SDL)のログがあります。

Java Telephony Application Programming Interface(JTAPI)Gateway(JGW)を有効にする

次のprocmonコマンドは、JGWトレースをオンにします。

```
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
```

procmon ipcc pg1a jgwコマンドの例を示します。

アクティブ側でのCTIサーバ(CTISVR)トレースの有効化

この手順では、アクティブ側でCTISVRトレースを有効にする方法について説明します。

1. HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a and b)\EMS\CurrentVersion\library\Processes\ctisvrを編集するには、レジストリエディタを使用します。
2. EMSTraceMask = f8を設定します。

トレースVRU PIMの有効化

注：コマンドでは大文字と小文字が区別されます。Voice Response Unit(VRU)PGは、Cisco CallManager(CCM)PGとは異なります。

次のprocmonコマンドは、VRU PIMのトレースをオンにします。

```
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
```

このprocmonコマンドは、VRU PIMトレースをオフにします。

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

両方のCTIOSサーバでCTIOSサーバトレースを有効にする

この手順では、両方のCTIOSサーバでトレースを有効にする方法について説明します。

1. 後で使用できるように、現在のトレースマスクをメモします。
2. HLKM >> Software\Cisco Systems
Inc.\ICM\<cust_inst>CTIOS\EMS\CurrentVersion\library\Processes\ctiosを編集するには、レジストリエディタを使用します。

3. Set:

- EMSTraceMask = 0x60A0F
- リリースに応じて、EMSTraceMaskを次のいずれかの値に設定します。
 - リリース6.0以前では0x0A0F
 - リリース7.0および7.1(1)の0x20A0F
 - リリース7.1(2)以降では0x60A0F

リリース7.0(0)を除くすべてのリリースでは、デフォルトのトレースマスクは0x3で、0x20003です。

トレースマスクの値が大きい (0xf以上) 場合、CTIOSサーバのパフォーマンスとコール完了率に大きな影響があります。問題をデバッグする場合にのみ、トレースマスクを高い値に設定します。必要なログを収集したら、トレースマスクをデフォルト値に戻す必要があります。

トラブルシューティングの目的で、CTIOSサーバのトレースマスクを次のように設定します。

- リリース6.0以前では0x0A0F
- リリース7.0および7.1(1)では0x20A0F
- リリース7.1(2)以降では0x60A0F

Active PGでOpen Peripheral Controller(OPC)トレースを有効にする

次のopctestコマンドは、アクティブなPGでOPCトレースをオンにします。

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

次に、ラボ環境の例を示します。

```
C:\Documents and Settings\ICMAdministrator>opctest /cust ccl /node pgl1
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
```

その他の例を次に示します。

```
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
```

アクティブPGでのEagtpimトレースの有効化

次のprocmonコマンドは、アクティブなPGでeagtpimトレースをオンにします。

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

次に、ラボ環境の例を示します。

```
C:\Documents and Settings\ICMAdministrator>procmon ccl pgl pml
>>>trace tp* /on
>>>trace precall /on
>>>trace *event /on
>>>trace csta* /on
>>>quit
```

Dumplogユーティリティを使用したログのプル

詳細は、『[Dumplogユーティリティの使用法](#)』を参照してください。次の例に示すように、**cdlog**コマンドを使用してlogfilesディレクトリに移動します。

```
c:\cdlog <customer_name> pgl !-- Or, pgXa to depending on the PG number (X)
```

```
c:\icm\<customer_name>\<PG#>\logfiles\
```

次の例は、出力をデフォルトファイルに配置する方法を示しています。いずれの場合も、**/of**を使用して、出力ファイルの特定の名前を定義できます。

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog pml /bt <HH:MM> /et <HH:MM> /ms /o
!-- This PIM example places output in a default pml.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> cgl
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サーバでのトレースの有効化

SIP

この手順では、Cisco SIP IP Phoneソフトウェアを使用してCVPサーバでトレースを有効にする方法について説明します。

1. コールサーバでCVP diagツール([http://localhost\(CallServer\):8000/cvp/diag](http://localhost(CallServer):8000/cvp/diag))に移動し、Session Initiation Protocol(SIP)スタックを取得します。
2. debugを使用して、com.dynamicsoft.Dslibs.DsUAlibsを追加します。
3. [設定]をクリックします。
4. **DEBUG/41**をクリックします。

H323

この手順では、H323ゲートウェイを使用するCVPサーバでトレースを有効にする方法について説明します。

1. コールサーバで、VBAAdminにログインします。
2. CVP Voice Browserで次のトレースを有効にします。

```
setcalltrace on  
setinterfacetrace on
```

コールサーバからのCVPログの取得

テスト期間の間、CVP *.logファイルとError.logファイルを収集します。これらのファイルはC:\Cisco\CVP\logs directory on both CVP serversディレクトリにあります。

これらはUnified CVPのログファイルの場所です。ここで、CVP_HOMEはUnified CVPソフトウェアがインストールされているディレクトリです。

ログのタイプ

コールサーバおよび/またはレポートサーバログ
操作コンソールログ
Voice XML(VXML)サーバログ
Simple Network Management Protocol(SNMP)エージェントログ
Unified CVP Resource Managerログ

場所

CVP_HOME\logs\
CVP_HOME\logs\OAMP\
CVP_HOME\logs\VXML\
CVP_HOME\logs\SNMP\
CVP_HOME\logs\ORM\

場所の例はC:\Cisco\CVPです。

VXMLサーバログ

配備されたAudiumアプリケーションなどのカスタム音声XMLアプリケーションでは、デバッグログをオンにできます。

C:\Cisco\CVP\VXMLServer\applications\APP_NAME\data\application\ directoryディレクトリの

settings.xml設定ファイルの<loggers>セクション (最後のセクション) に次の行を追加します。

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

実行時に、このロガーは詳細なVoiceXMLログを
\\Cisco\CVP\VXMLServer\applications\APP_NAME\MyDebuggerLogger directoryに出力します。

注： MyDebugLoggerから選択した任意の名前にsettings.xml設定ファイルでロガーの名前を変更できます。

アウトバウンドダイヤラ関連のトレースおよびログ収集

この手順では、アウトバウンドダイヤラ (通常はPGで見られます) のベースダイヤラプロセスログを増やす方法について説明します。

1. EMSDisplaytoScreen = 0であることを確認します。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialerを編集するには、レジストリエディタを使用します。
3. Set:
 - EMSTraceMask = 0xff
 - EMSUserData = ff (バイナリモードでは4つのf)
4. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialerを編集するには、レジストリエディタを使用します。
5. DebugDumpAllEvents = 1を設定します。

ブルログ

dumplogユーティリティを/icm/<instance>/dialer/logfilesディレクトリから実行します。

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

輸入業者について

この手順では、インポートプロセスログを増やす方法について説明します。

1. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Logger\EMS\CurrentVersion\Library\Processes\ balImportを編集するには、レジストリエディタを使用します。
2. Set:

- EMSTraceMask = 0xff
- EMSUserData = ff (バイナリモードでは4つのf)

3. dumplogユーティリティを/icm/<instance>/la/logfilesディレクトリから実行します。

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

キャンペーンマネージャ

この手順では、campaignmanagerプロセスログを増やす方法について説明します。

1. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Logger\EMS\CurrentVersion\Library\Processes\CampaignManagerを編集するには、レジストリエディタを使用します。

2. Set:

- EMSTraceMask = 0xff
- EMSUserData = ff (バイナリモードでは4つのf)

3. dumplogユーティリティを/icm/<instance>/la/logfilesディレクトリから実行します。

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

Avaya Communications Manager(ACD)PGで、opctestユーティリティを使用して、CallManagerとAvayaの両方で次の値を増やします。

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

この手順では、ctisvrプロセスのトレースを増やす方法について説明します。

1. HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvrを編集するには、レジストリエディタを使用します。

2. EMSTraceMask = f8を設定します。必要に応じて、値をf0のままにすることができます。

ルータプロセスでのルータログの有効化

次の手順では、ルータログを有効にする方法について説明します。

1. ルータで、[Start] > [Run]に移動し、**rttrace**と入力します。
2. 顧客名を入力します。

3. [Connect] をクリックします。

4. 次のオプションを選択します。

```
agentchangesrouterrequestsscriptselsNetworkVrutingtranslationroutequeueingcalltyperealtime
```

5. [Apply] をクリックします。

6. ユーティリティを終了します。

opctestリリース8.5の場合は、代わりにDiagnostic Framework Porticoを使用してください。

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

ルータのログのプル

テストの期間中にどちらかのルータからルータログを取得するには、`dumplog`ユーティリティを使用します。詳細については、「[Dumplogユーティリティの使用方法](#)」を参照してください。

次に、09:00:00 ~ 09:30:00 (24時間形式) の10/21/2011のログ要求の例を示します。次の出力は、C:/router_output.txtファイルに出力されます。

```
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
```

必要に応じて、トラブルシューティングのために出力ファイル(C:/router_output.txt)をシスコに送信します。

ゲートウェイトレース(SIP)

次のコマンドは、SIPを使用するCVPサーバのトレースをオンにします。

```
#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
```

注：実稼働Cisco IOS®ソフトウェアGWで変更を行うと、停止する可能性があります。

これは非常に堅牢なプラットフォームで、提供されたコール量で問題なく推奨されるデバッグを処理できます。ただし、シスコでは次のことを推奨しています。

- ログバッファではなく、すべてのログをsyslogサーバに送信します。

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

- debugコマンドを一度に1つずつ適用し、それぞれの後のCPU使用率を確認します。

```
show proc cpu hist
```

注：CPUの使用率が最大70～80%になると、パフォーマンス関連のサービスへの影響のリスクが大幅に増加します。したがって、GWが60%に達した場合は、追加のデバッグを有効にしないでください。

これらのデバッグを有効にします：

```
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
```

コールを発信して問題をシミュレートしたら、デバッグを停止します。

```
#undebug all
```

次の出力を収集します。

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

CUSPトレース

次のコマンドは、Cisco Unified SIP Proxy(CUSP)のSIPトレースをオンにします。

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

完了したら、必ずログオフをオフにしてください。

この手順では、ログを収集する方法について説明します。

1. CUSPでユーザを設定します (testなど)。
2. CUSPプロンプトで次の設定を追加します。

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

3. FTPでCUSP IPアドレスに接続します。前の手順で定義したユーザ名(test)とパスワードを使用します。
4. ディレクトリを/cusp/log/traceに変更します。
5. log_<filename>を取得します。

トレースのためのCLIの使用

UCCEリリース8以降では、ユニファイドシステムコマンドラインインターフェイス(CLI)を使用してトレースを収集できます。dumplogユーティリティと比較して、CLIはPGやRoggerなどの1台のサーバからログのセット全体を取得する非常に高速で効率的な方法です。

この手順では、問題の分析を開始する方法と、有効にするトレースを決定する方法について説明します。この例では、次のサーバからログを収集します。

- ルータA/ルータB
- LOGGER-A/LOGGER-B
- PGXA/PGXB
- すべてのCVPコールサーバ
- すべてのCVP VXML/メディアサーバ (存在する場合)

1. リストの各システムで、各サーバのUnified System CLIを開き、次のコマンドを実行します。
。

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

最初のmm-dd-yyyy:hh:mm文字列を、イベントの約15分前の日時に置き換えます。

2番目のmm-dd-yyyy:hh:mm文字列は、イベントが解決されてから約15分後の日付と時刻に置き換えます。イベントが引き続き発生する場合は、少なくとも15分集めてください。これにより、clioutputX.zipという名前のファイルが生成されます。ここで、Xは順番に次の番号です。

2. 各システムのWindowsアプリケーション/セキュリティ/システムログをカンマ区切り値(CSV)形式でエクスポートし、C:\Temp directoryディレクトリに保存します。
3. ステップ1のzipファイルにWindows CSVログを追加し、zipファイルの名前を次の形式に変更します。

<SERVERNAME>-SystCLILogs-EventOn-YYYYMMDD_HHMMSS.zip

4. 任意のエージェントPGで、C:\Program Files\Cisco\Desktop\logs every time the failure is seenディレクトリのログを収集します。ログを次の形式の名前のファイルに圧縮します。

<SERVERNAME>-CADLogs-EventOn-YYYYMMDD_HHMMSS.zip

CAD-Browser Edition(CAD-BE)またはCAD Web製品を使用している場合は、C:\Program Files\Cisco\Desktop\Tomcat\logs directoryフォルダからログを収集し、同じzipファイルに追加します。

いずれかのWindows 2008 x64製品で実行している場合、ログディレクトリはC:\Program Files (x86)\Cisco\Desktop\...にあります。

5. これらのファイルをサービスリクエストに添付するか、サイズが大きすぎて電子メールや添付ができない場合はFTPにアップロードします。
可能であれば、次の追加情報を収集します。

- イベントの開始時刻と終了時刻。
- イベントに含まれるANI/DNIS/AgentIDのサンプルがいくつかあります。イベントを表示するには、少なくとも1つの情報が必要です。
- イベントを取り囲む期間のRouteCallDetail(RCD)およびTerminationCallDetail(TCD)。RCDクエリは次のとおりです。

```
SELECT * FROM Route_Call_Detail WHERE DbDateTime > 'YYYY-MM-DD HH:MM:SS.MMM' and DbDateTime < 'YYYY-MM-DD HH:MM:SS.MMM'
```

```
TCDクエリは次のとおりです。  
SELECT * FROM Termination_Call_Detail WHERE DbDateTime > 'YYYY-MM-DD HH:MM:SS.MMM' and DbDateTime < 'YYYY-MM-DD HH:MM:SS.MMM'
```

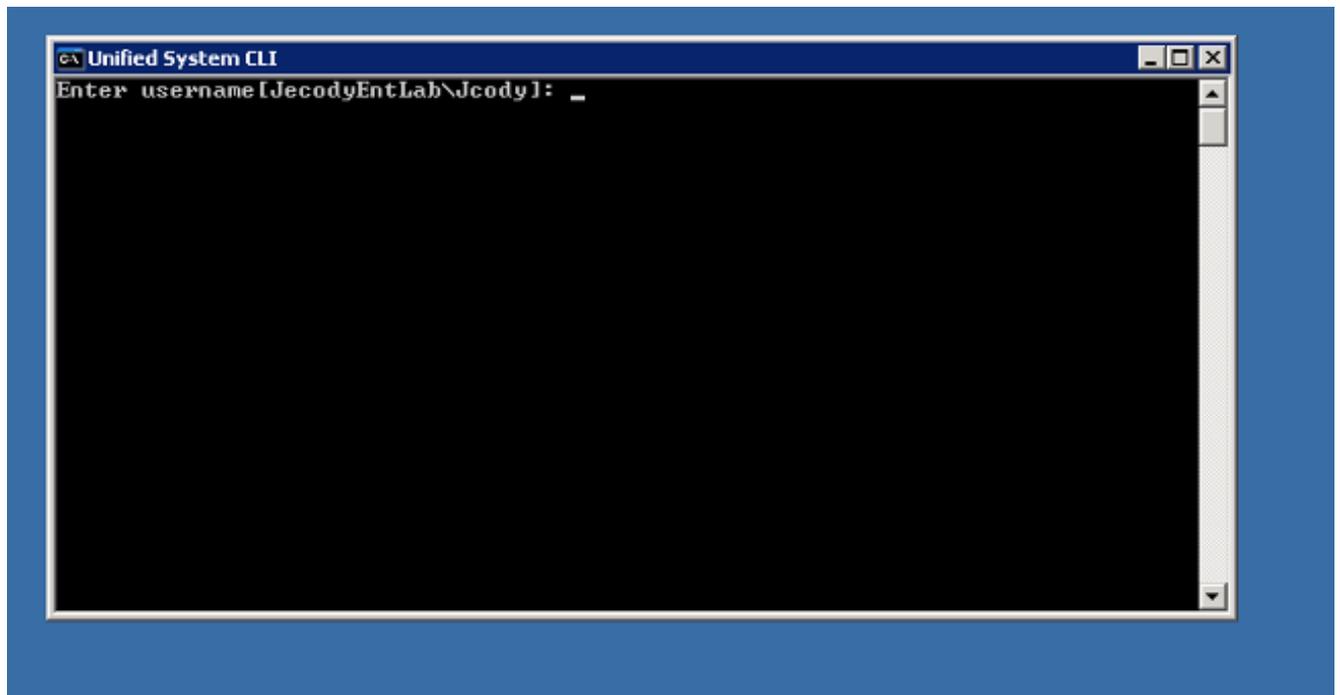
CLIの例

注：これらのアクションはシステムに影響を与える可能性があるため、この作業は業務時間外または遅い時間に行う場合があります。

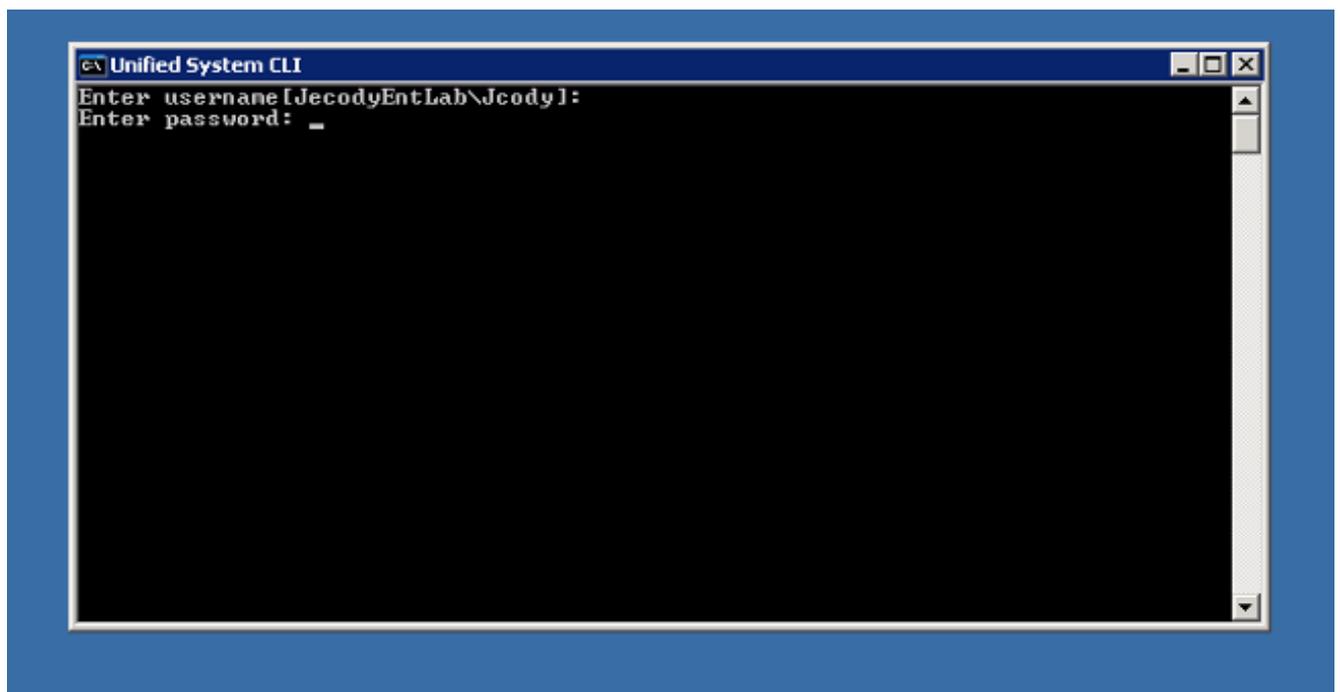
次の2つのツールがあります。診断フレームワークツールとシステムCLIツール。両方とも、デスクトップ上または各サーバのProgramsディレクトリ下のアイコンです。

この手順では、トレースにUnified System CLIを使用する方法について説明します。

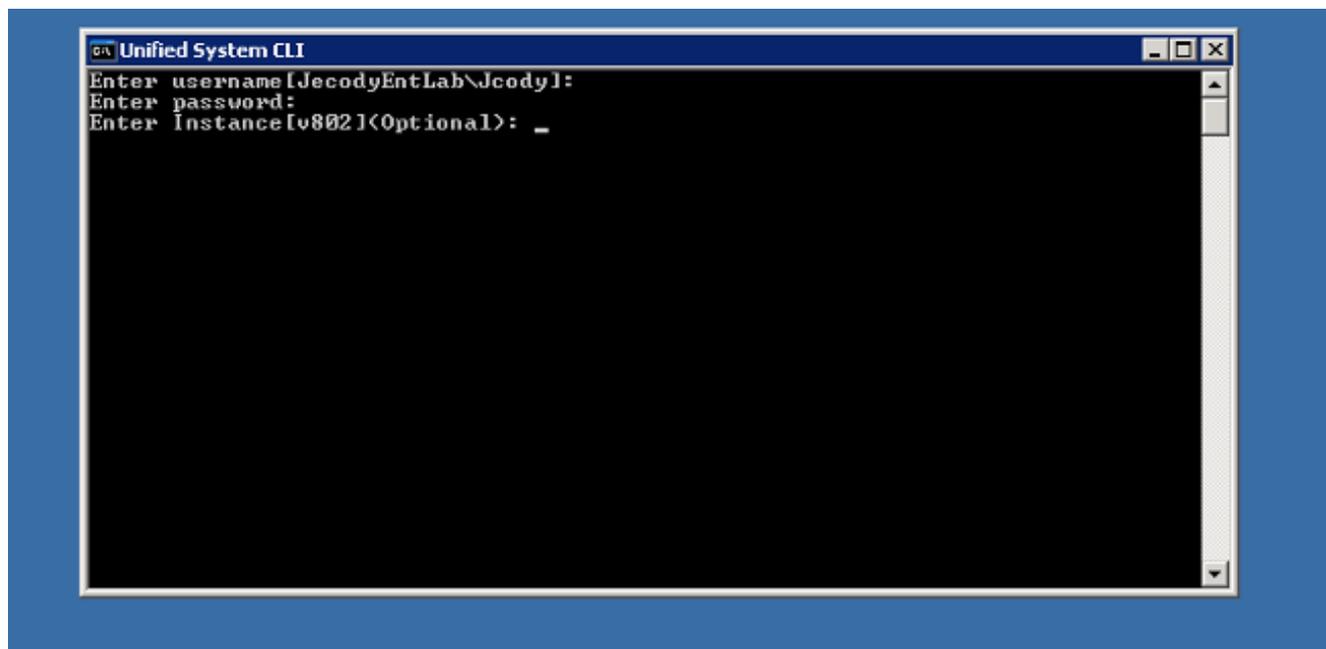
1. [Unified System CLI]アイコンをクリックし、ドメインとユーザ名でログインします。(この例では、ドメイン管理者は以前にログインしているため、CLIはドメイン(JcodyEntLab)とユーザ名(Jcody)をすでに認識しています。



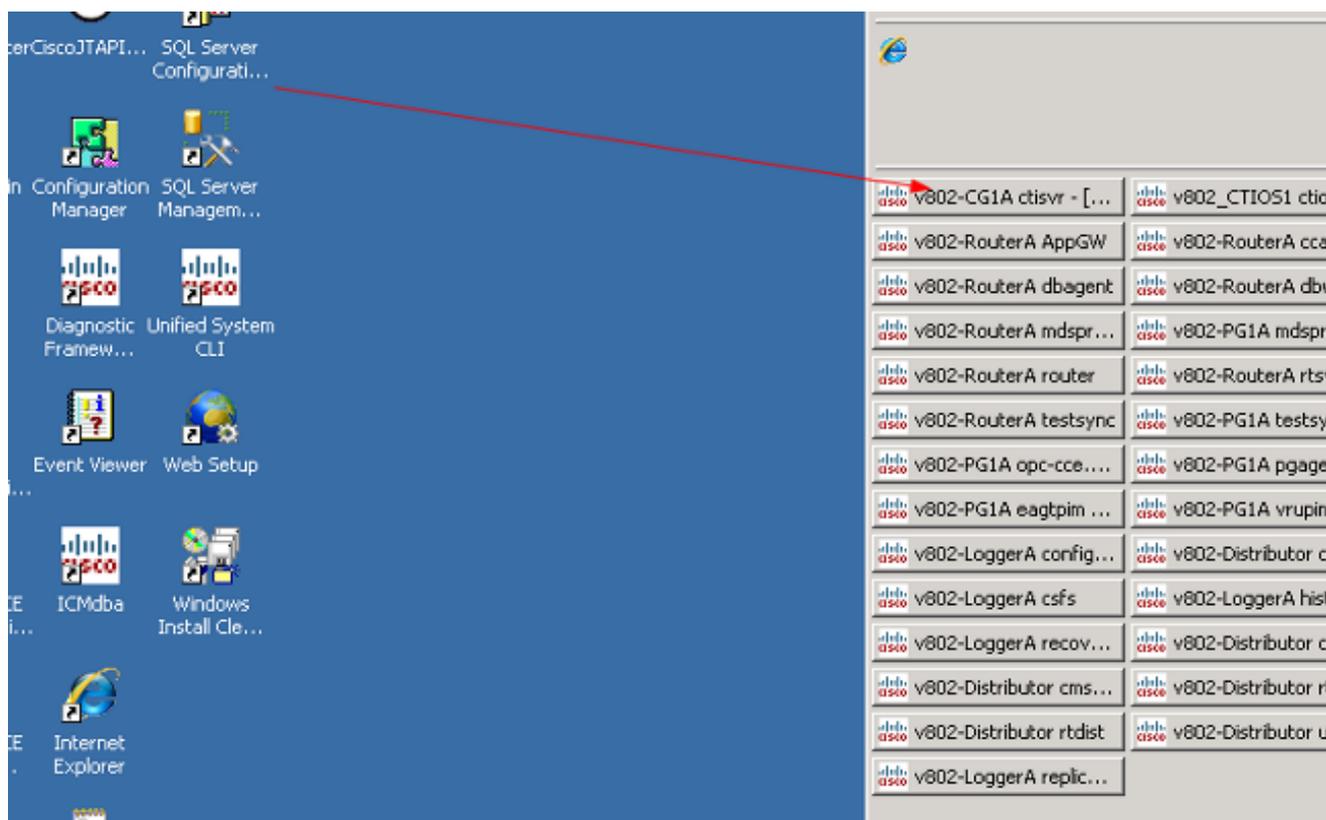
2. パスワードを入力します。



3. インスタンス名を入力します。この例では、これはv802です。いずれかのサービスでPGを調べます。インスタンス名は、サービス名の最初の部分です。



4. インスタンス名を見つける簡単な方法は、サーバで実行されているサービスを確認することです。



5. ウェルカムメッセージが表示されたら、次のコマンドを入力します。

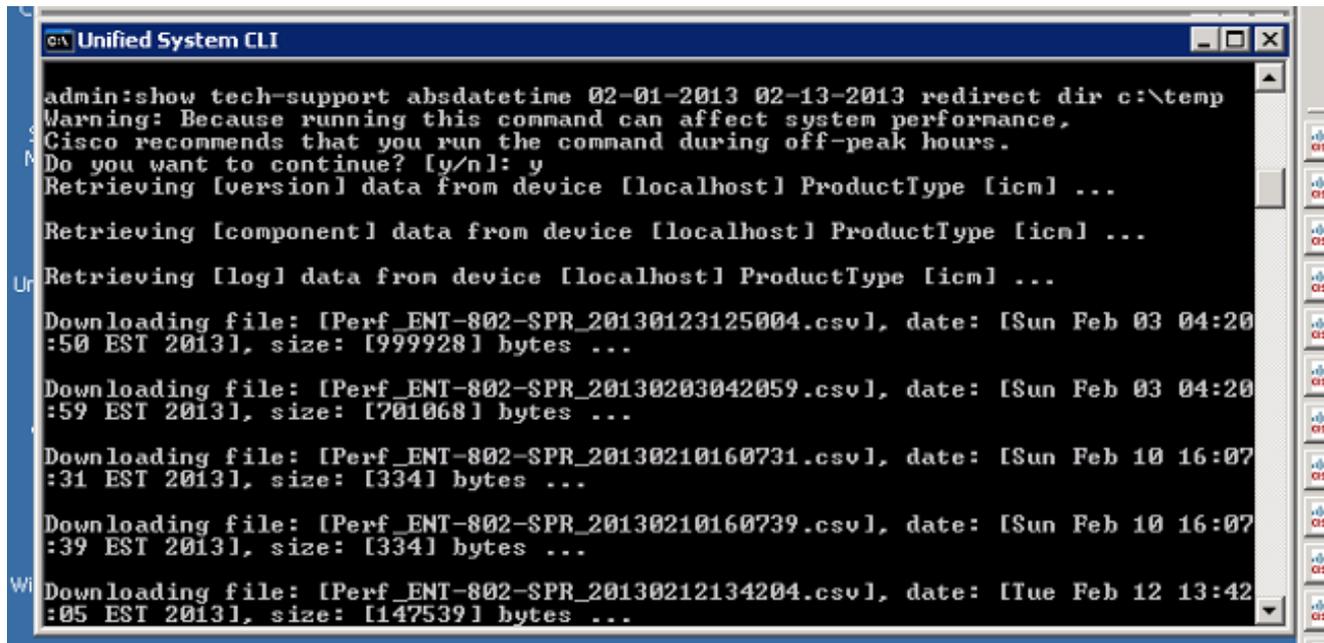
```
show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect dir c:\temp
```

最初のmm-dd-yyyy:hh:mm文字列を、イベントの約15分前の日時に置き換えます。

2番目のmm-dd-yyyy:hh:mm文字列は、イベントが解決されてから約15分後の日付と時刻に置き換えます。

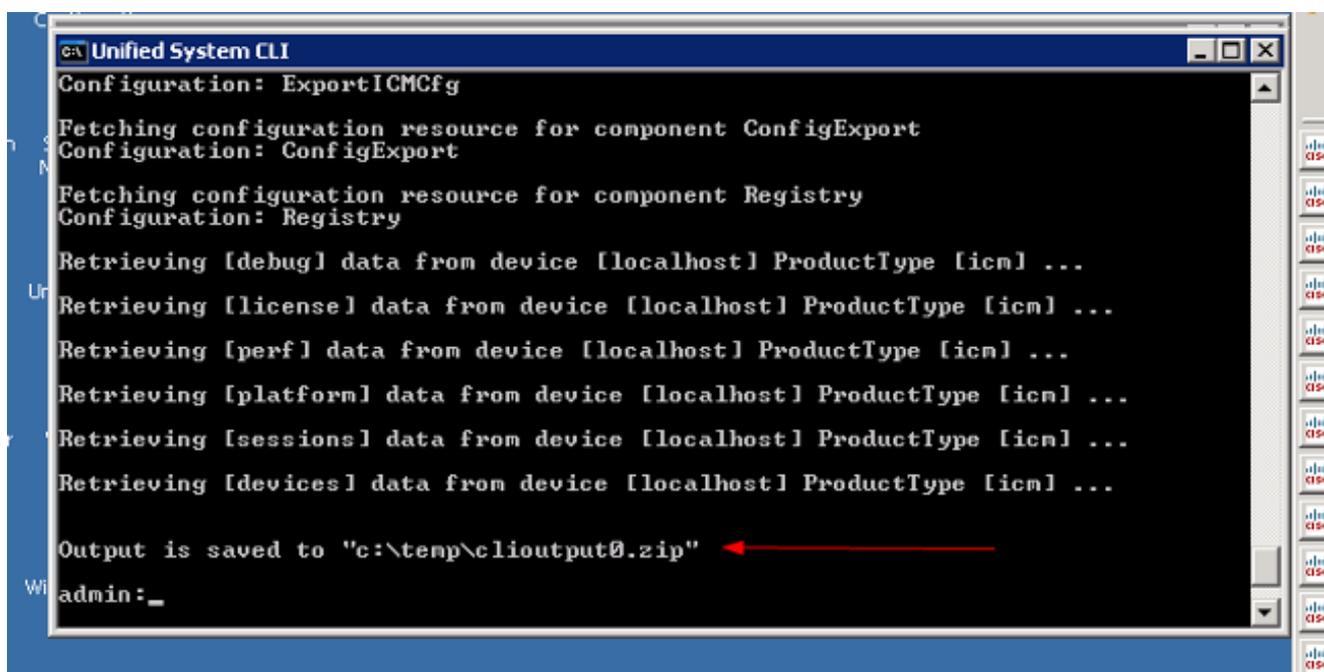
イベントが引き続き発生する場合は、少なくとも15分集めてください。

*clioutputX.zip*という名前のファイルが生成されます。ここで、*X*は次の番号です。



```
admin:show tech-support absdatetime 02-01-2013 02-13-2013 redirect dir c:\temp
Warning: Because running this command can affect system performance,
Cisco recommends that you run the command during off-peak hours.
Do you want to continue? [y/n]: y
Retrieving [version] data from device [localhost] ProductType [icm] ...
Retrieving [component] data from device [localhost] ProductType [icm] ...
Retrieving [log] data from device [localhost] ProductType [icm] ...
Downloading file: [Perf_ENT-802-SPR_20130123125004.csv], date: [Sun Feb 03 04:20:50 EST 2013], size: [999928] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130203042059.csv], date: [Sun Feb 03 04:20:59 EST 2013], size: [701068] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130210160731.csv], date: [Sun Feb 10 16:07:31 EST 2013], size: [334] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130210160739.csv], date: [Sun Feb 10 16:07:39 EST 2013], size: [334] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130212134204.csv], date: [Tue Feb 12 13:42:05 EST 2013], size: [147539] bytes ...
```

6. プロセスが完了したら、ディレクトリで*clioutputX.zip*ファイルを探します。



```
Configuration: ExportICMcfg
Fetching configuration resource for component ConfigExport
Configuration: ConfigExport
Fetching configuration resource for component Registry
Configuration: Registry
Retrieving [debug] data from device [localhost] ProductType [icm] ...
Retrieving [license] data from device [localhost] ProductType [icm] ...
Retrieving [perf] data from device [localhost] ProductType [icm] ...
Retrieving [platform] data from device [localhost] ProductType [icm] ...
Retrieving [sessions] data from device [localhost] ProductType [icm] ...
Retrieving [devices] data from device [localhost] ProductType [icm] ...
Output is saved to "c:\temp\clioutput0.zip"
admin: _
```

注：このファイルには、このサーバ上のすべてのサービスのすべてのUCCE関連ファイルが含まれるため、通常は非常に大きくなります。

7. 必要なログが1つだけの場合は、古いdumplogユーティリティを使用するか、Diagnostic Framework Porticoを使用する方が簡単です。

Unified ICM-CCE-CCH Diagnostic Framework Portico

Hostname: ENT-802-SPR.JecodyEntLab.com Address: 14.10.150.108

Commands:

- Alarm**
 - SetAlarms
 - GetAlarms
- Configuration**
 - ListConfigurationCategories
 - GetConfigurationCategories
- Inventory**
 - ListAppServers
- License**
 - GetProductLicense
- Log**
 - ListLogComponents
 - ListLogFiles
- Network**
 - GetNetStat
 - GetPConfig
 - GetTraceRoute
 - GetPing
- Performance**
 - GetPerformanceSummary

ListTraceFiles

Component: CTI Server 1A/clisvr

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%