CCEでのトレース設定と口グ収集

内容

はじめに

このドキュメントでは、Cisco Unified Contact Center Enterprise(CCE)でトレースを設定および収集する方法について説明します。

前提条件

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）
- Package Contact Center Enterprise(PCCE)
- Cisco Finesse

- Cisco Customer Voice Portal（CVP）
- Cisco Virtualized Voice Browser(VVB)
- Cisco Unified Border Element（CUBE）
- Cisco Unified Intelligence Center（CUIC）
- Cisco Unified Session Initiation Protocol(SIP)プロキシ(CUSP)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Finesseリリース12.5
- CVPサーバリリース12.5
- UCCE/PCCEリリース12.5
- Cisco VVBリリース12.5
- CUICリリース12.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

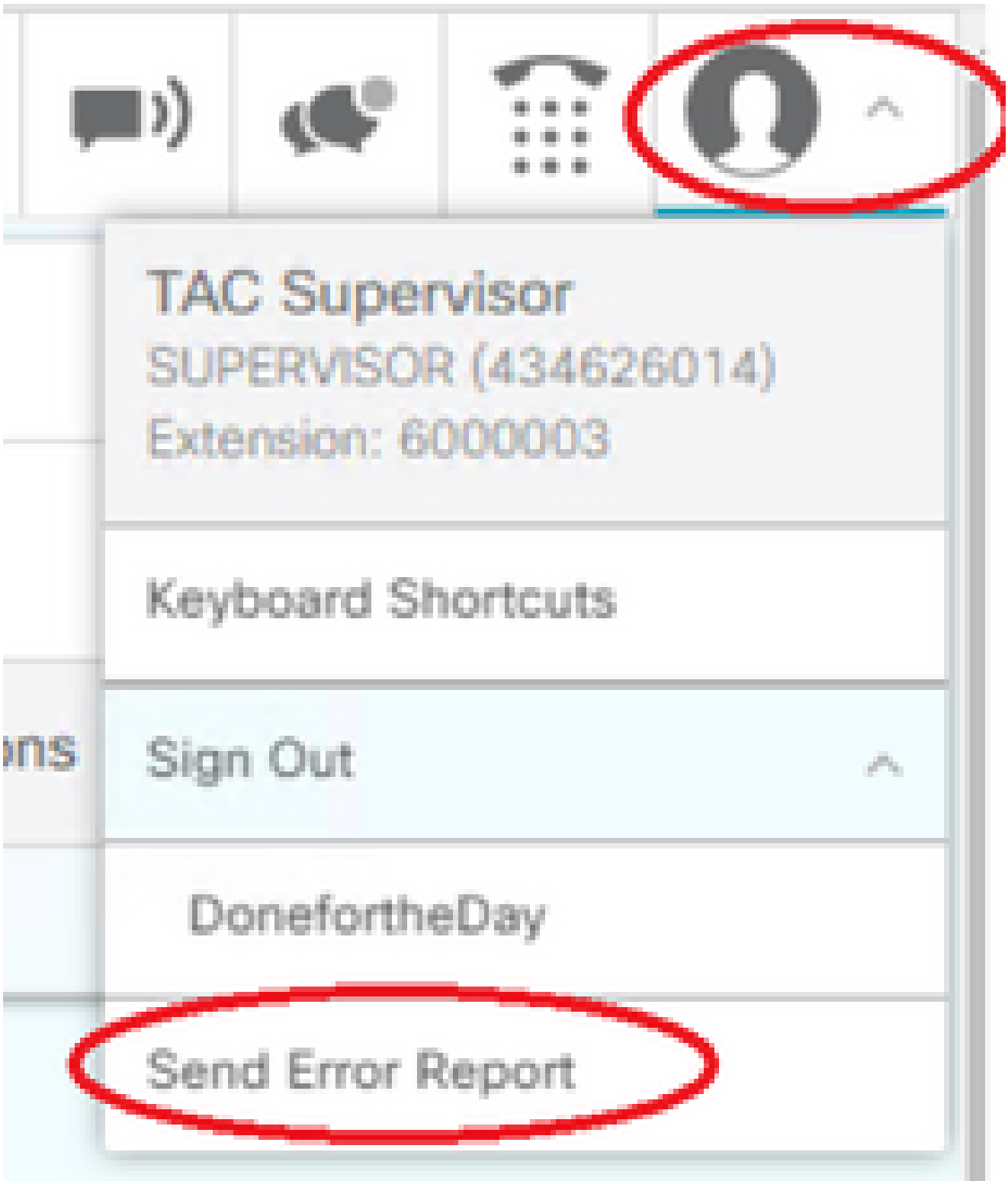
トレースの設定とFinesseログの収集

Finesseクライアント

Finesseクライアントログを収集するには、いくつかのオプションがあります。

オプション1：送信エラーレポートからクライアントログを収集する。

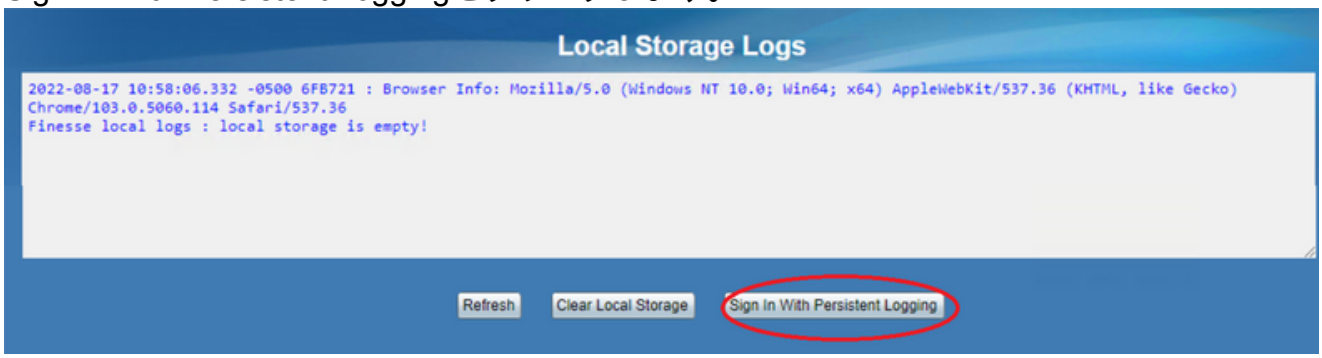
1. エージェントをログインします。
2. コールまたはメディアイベントの間に問題が発生した場合、エージェントに対して、Finesseデスクトップの右上隅にあるエラーレポートの送信リンクをクリックするように指示します。



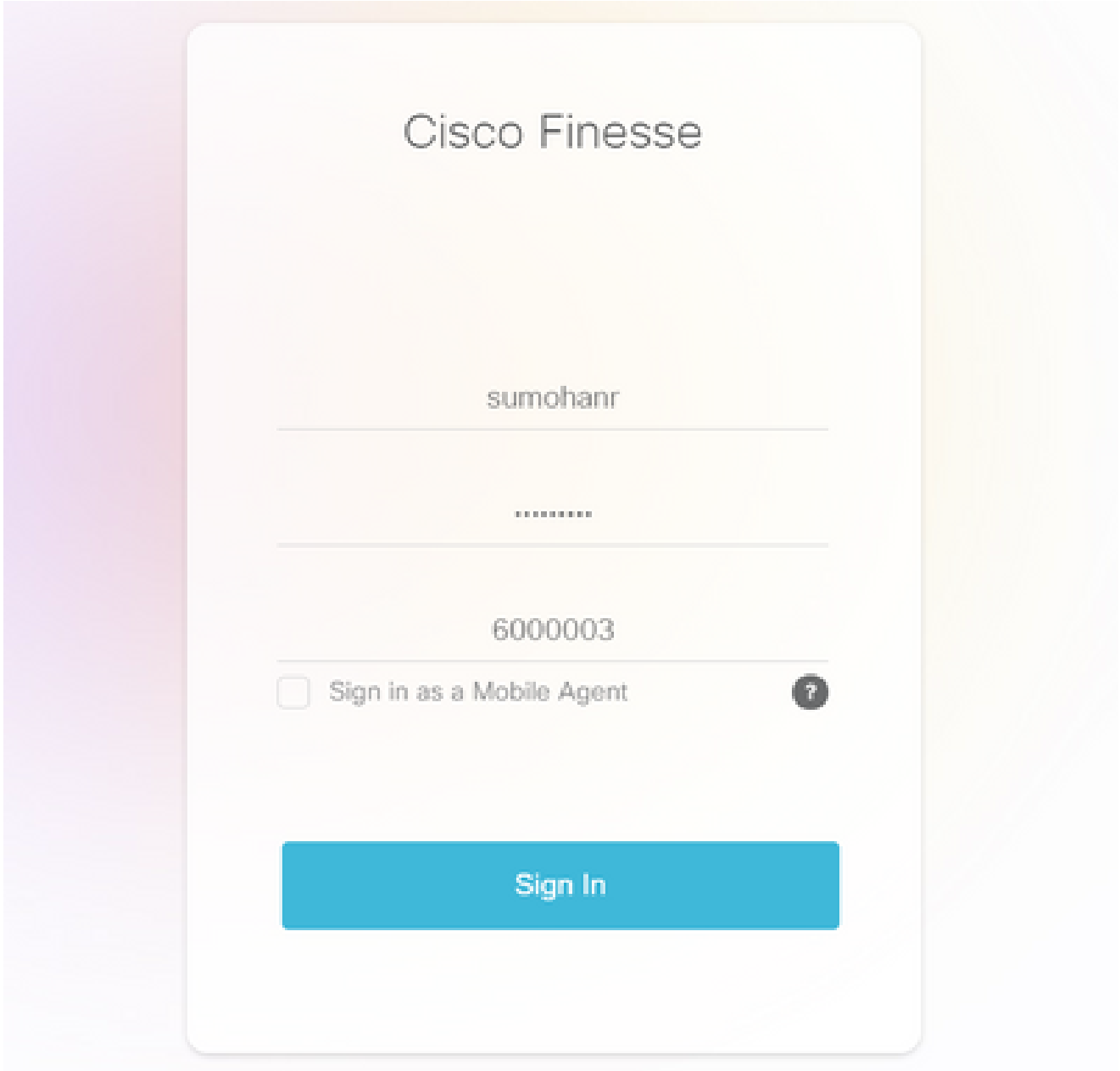
3. エージェントには「Logs Successfully Sent!」というメッセージが表示されます。
4. クライアントログがFinesseサーバに送信されます。https://x.x.x.x/finesse/logsに移動し、管理アカウントでログインします。
5. clientlogs/ ディレクトリの下でログを収集します。

オプション2：パーシステントロギングの設定

1. https://x.x.x.x:8445/desktop/locallog に移動します。
2. Sign In With Persistent Loggingをクリックします。



3. Cisco Finesseエージェントデスクトップのログインページが開きます。エージェントをログインします。

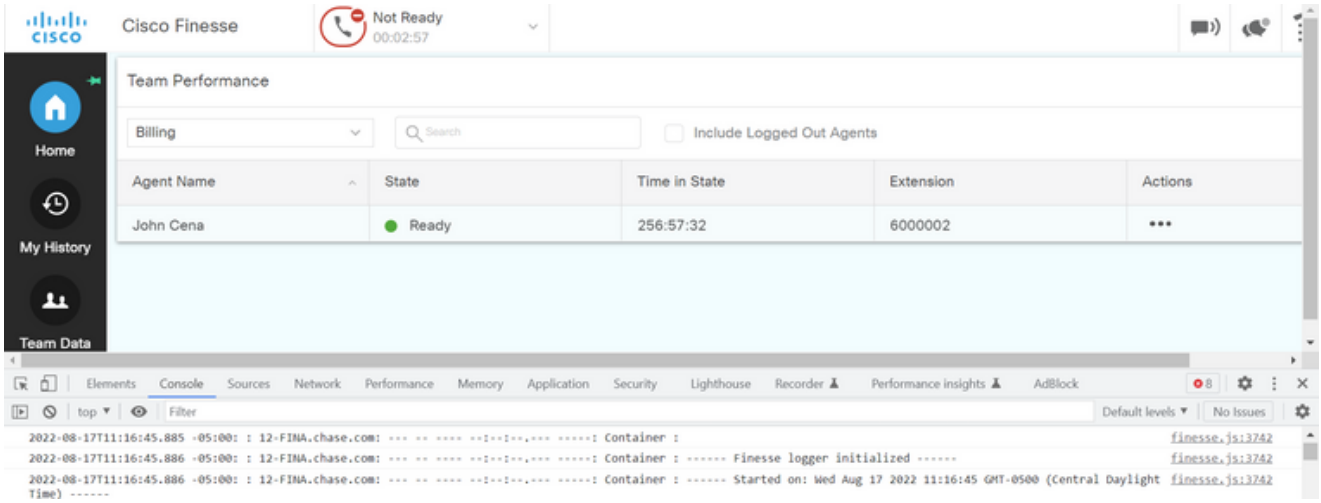


4. エージェントデスクトップの対話はすべて登録され、ローカルストレージログに送信されます。ログを収集するには、https://x.x.x.x:8445/desktop/locallogに移動し、内容をテキストフ

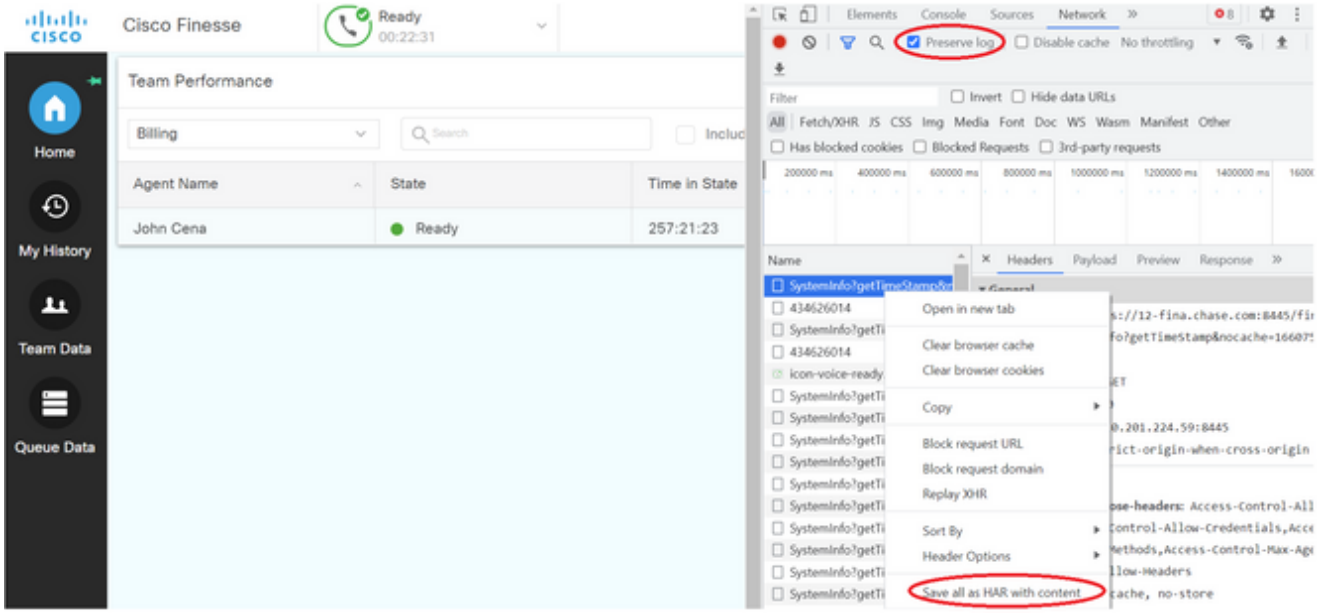
ァイルにコピーします。ファイルはSave、さらに分析するために必要です。

オプション3:Webブラウザコンソール

1. エージェントがログインしたら、F12キーを押してブラウザコンソールを開きます。
2. [Console] タブを選択します。
3. ブラウザコンソールでエラーを確認します。内容をテキストファイルにコピーしてsaveください。



4. Networkタブを選択し、Preserve logオプションにチェックマークを入れます。
5. 任意のネットワーク名イベントを右クリックし、「コンテンツを含むHAR」Saveを選択します。



Finesseサーバ

オプション1：ユーザインターフェイス(UI) - Webサービス（必須）および追加ログ

1. https://x.x.x.x/finesse/logsに移動し、管理アカウントでログインします。
2. ディレクトリwebservices/

3. 最後のWebサービスログを収集します。最後の解凍ファイルを選択します。たとえば、Desktop-Webservices.201X-..log.zipなどです。ファイルリンクをクリックすると、ファイルのオプションが表示saveされます。

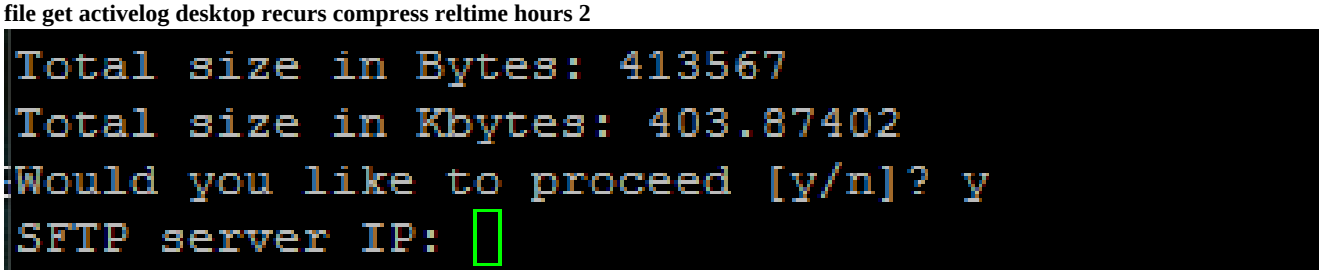
4. その他の必要なログを収集します（シナリオによって異なります）。たとえば、通知サービスの問題に対するopenfire、認証の問題に対するレルムログ、APIの問題に対するtomcatlogsなどがあります。

注：Cisco Finesseサーバのログを収集するには、セキュアシェル(SSH)およびセキュアファイル転送プロトコル(SFTP)を使用することをお勧めします。この方法では、Webサービスのログを収集できるだけでなく、Fippa、openfire、Realm、Clientlogsなどの追加のログも収集できます。

オプション2:SSHおよびSecure File Transfer Protocol(SFTP)経由 – 推奨オプション

1. SSHを使用してFinesseサーバにログインします。
2. 次のコマンドを入力して、必要なログを収集します。このコマンドは、ログを2時間収集します。ログのアップロード先のSFTPサーバを指定するように求められます。

file get activelog desktop recurs compress reltime hours 2



3. これらのログはSFTPサーバパス<IP address>\<date time stamp>\active_nnn.tgzに保存されます。nnnは長い形式のタイムスタンプです。
4. tomcat、Contextサービス、Servm、インストールログなどの追加のログを収集するには、『Cisco Finesseアドミニストレーションガイドリリース12.5(1)』の「ログ収集」セクションを参照してください。

トレースの設定とCVPおよびCVVBログの収集

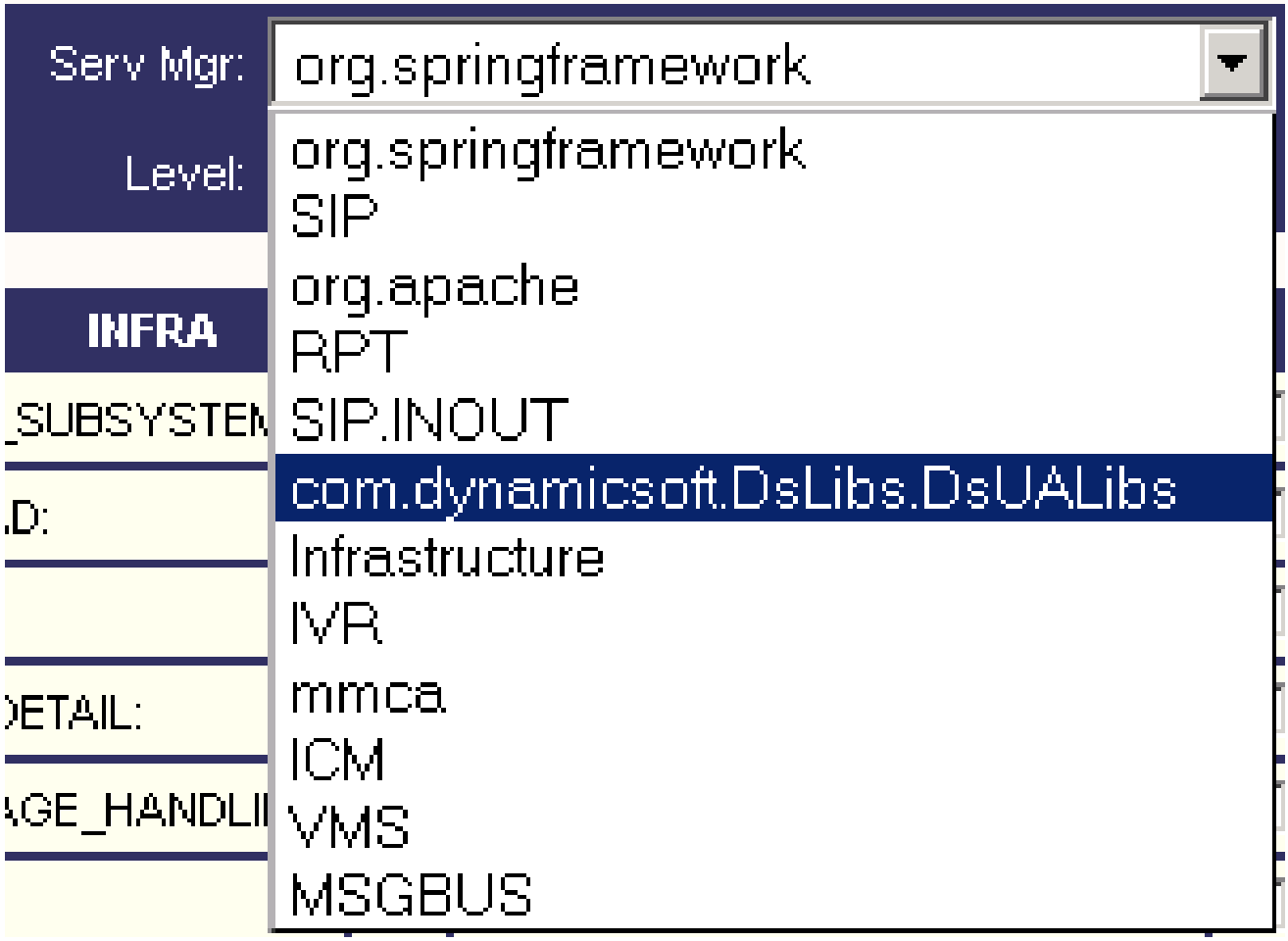
CVP コール サーバ

1. ほとんどの場合、CVP CallServerのデフォルトレベルのトレースで十分にトラブルシューティングできます。ただし、セッション開始プロトコル(SIP)メッセージの詳細を取得する必要がある場合は、SIPストラックトレースをデバッグレベルに設定する必要があります。

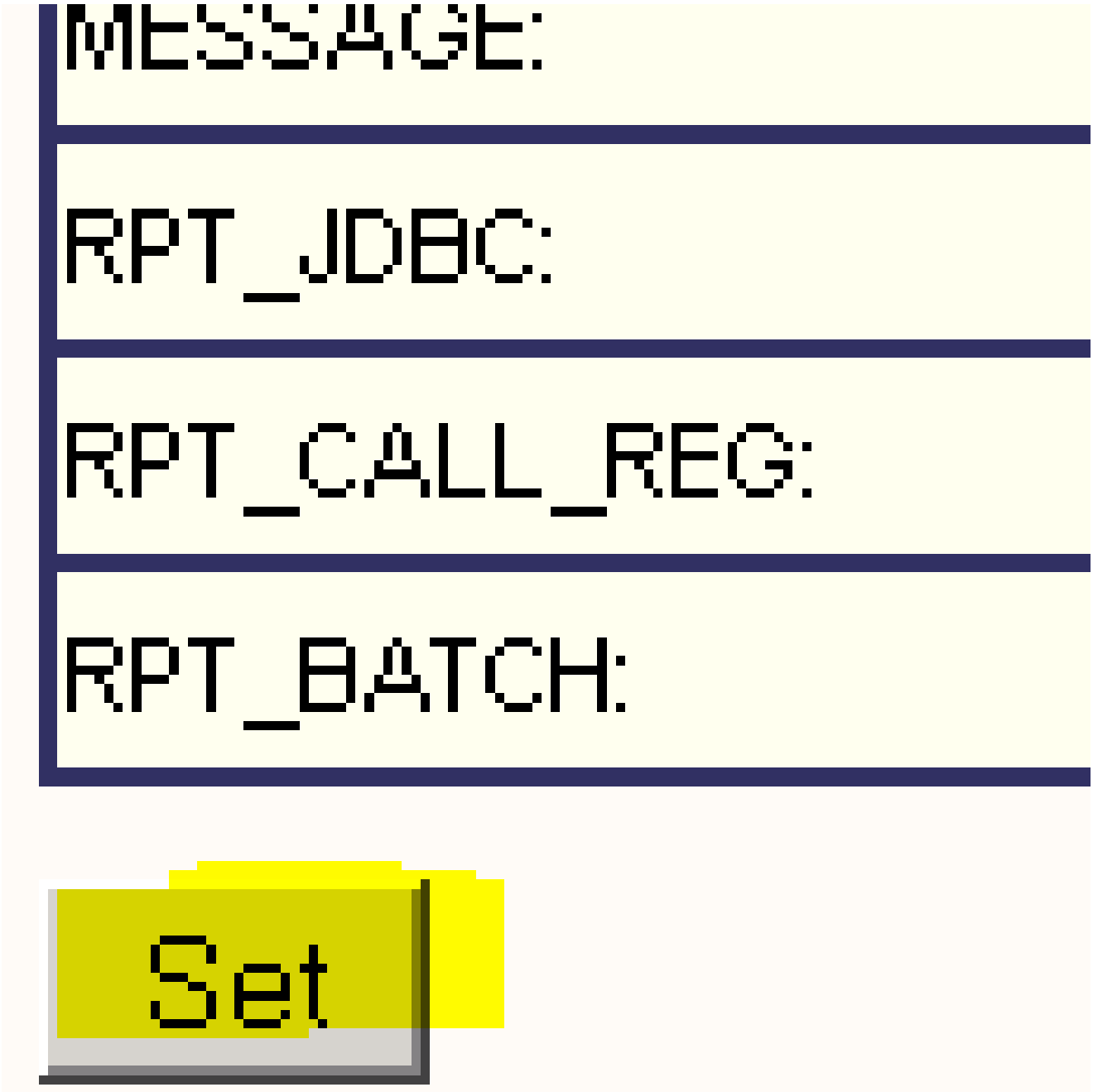
2. CVP CallServer Diag WebページURL http:/localhost:8000/cvp/diagに移動します。

> 注：このページには、CVP CallServerに関する有益な情報が表示され、特定のシナリオのトラブルシューティングに非常に役立ちます。

3. Servからcom.dynamicsoft.DsLibs.DsUALibsを選択します。左上隅のMgrドロップダウンメニュー



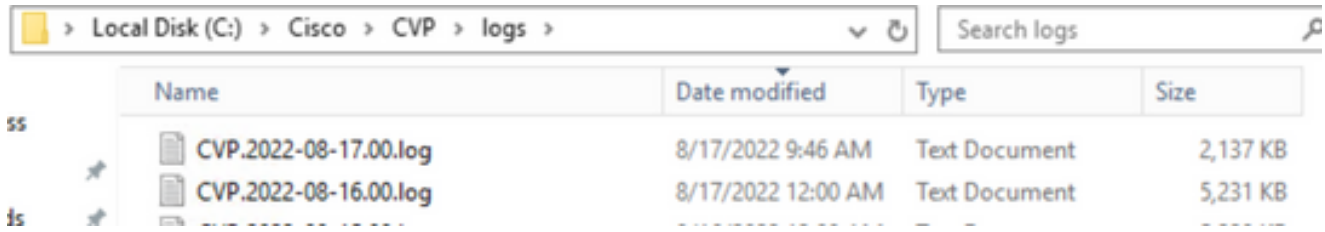
4. Setボタンをクリックします。



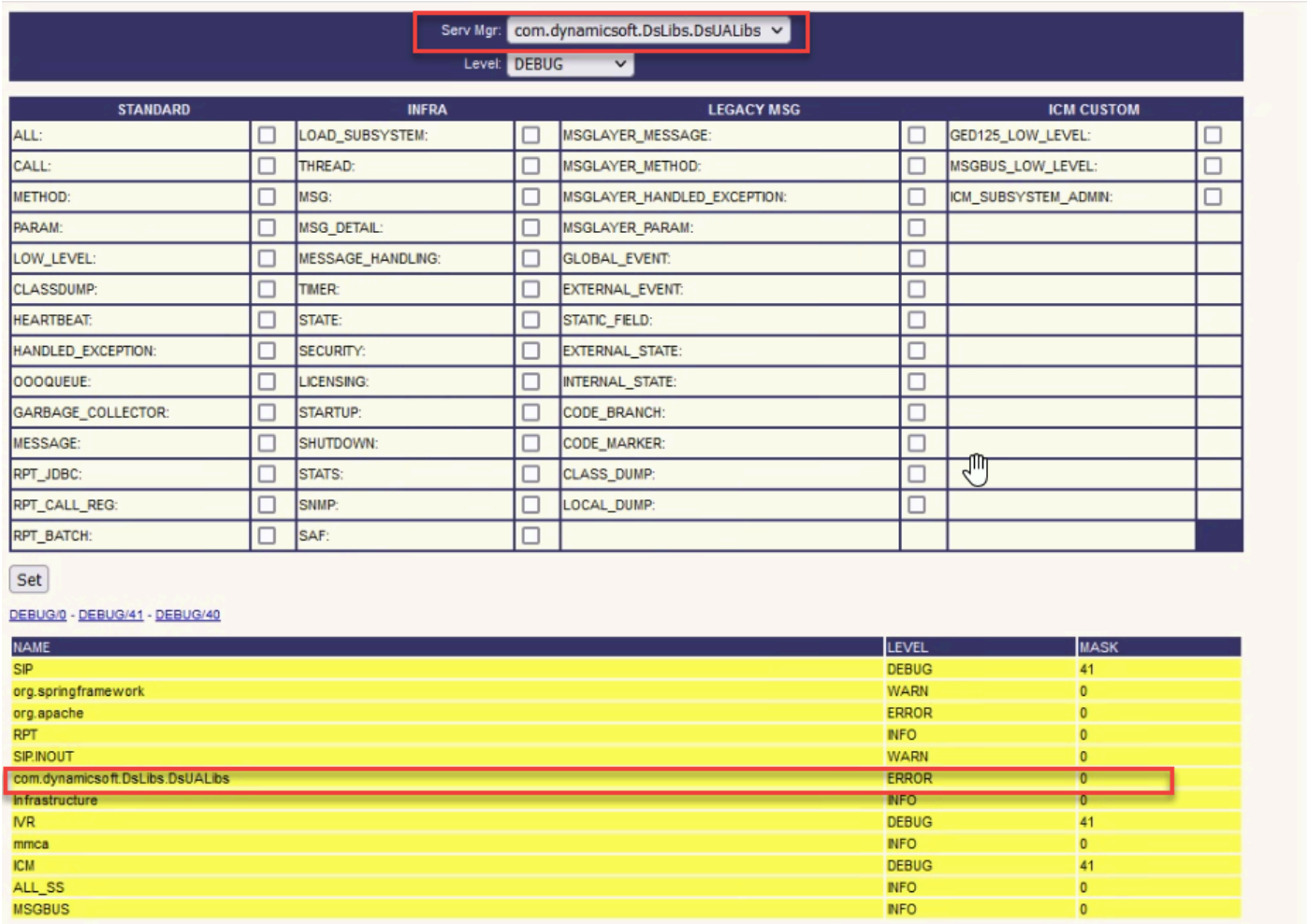
5. トレースウィンドウをスクロールダウンして、トレースのレベルが正しく設定されていることを確認します。デバッグ設定は次のとおりです。

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. 問題を再現する際には、C:\Cisco\CVP\logsからログを収集し、問題が発生した時刻に基づいてCVPログファイルを選択します。



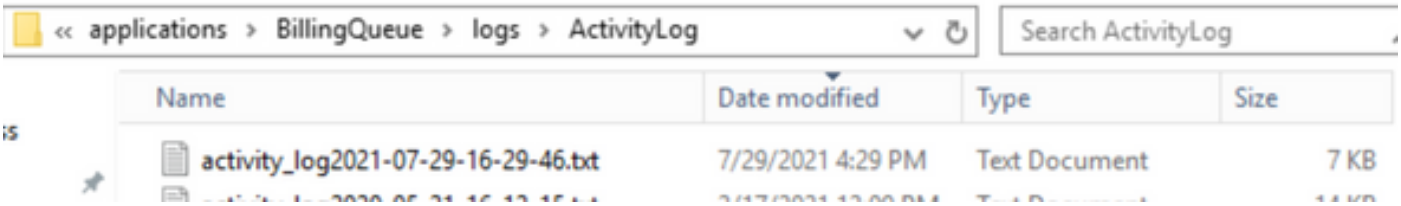
7.問題を再現したら、トレースをデフォルトレベルに復元します。Servから com.dynamicsoft.DsLibs.DsUALibsを選択します。左上隅にあるMgrドロップダウンメニューをクリックし、それをerrorに設定します。



CVP Voice XML(VXML)アプリケーション

非常にまれな状況で、VXMLサーバアプリケーションのトレースレベルを上げる必要があります。一方、シスコのエンジニアから要求されない限り、この値を増やすことは推奨されません。

VXMLサーバのアプリケーションログを収集するには、VXMLサーバの特定のアプリケーションディレクトリ(C:\Cisco\CVP\VXMLServer\applications\{name of application}\logs\ActivityLog\など)に移動し、アクティビティログを収集します。



CVP Operations and Administration Management Portal(OAMP)

ほとんどの場合、OAMPとORMのトレースのデフォルトレベルは、問題の根本原因を特定するのに十分です。ただし、トレースのレベルを上げる必要がある場合は、このアクションを実行する手順を次に示します。

1. バックアップ %CVP_HOME%\conf\oamp.properties

2. 編集 %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. 次に示すように、変更後にOPSConsoleServerを再起動します。

トレースレベル情報

トレースレベル	説明	ログ レベル	トレースマスク
0	製品インストールの既定値です。パフォーマンスへの影響は予測されていないか、または最小限です。	INFO	なし
1	パフォーマンスへの影響が少なく、詳細なトレースメッセージが少ない。	デバッグ	DEVICE_CONFIGURATION + (デバイス設定+) DATABASE_MODIFY +キー管理=0x01011000
2	パフォーマンスに中程度の影響を与える詳細なトレースメッセージ。	デバッグ	DEVICE_CONFIGURATION + (デバイス設定+) SYSLVL_CONFIGURATION + DATABASE_MODIFY +キー

トレースレベル	説明	ログ レベル	トレースマスク
			管理=0x05011000
3	パフォーマンスに大きな影響を与える詳細なトレースメッセージ	デバッグ	DEVICE_CONFIGURATION + (デバイス設定+) SYSLVL_CONFIGURATION + BULK_OPERATIONS + (一括操作) DATABASE_MODIFY +キー 管理=0x05111000
4	パフォーマンスへの影響が非常に大きい詳細なトレースメッセージ。	デバッグ	その他+ DEVICE_CONFIGURATION + (デバイス設定+) ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + (一括操作) BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY +キー DATABASE_SELECT +キー DATABASE_PO_INFO + 管理+ TRACE_METHODと TRACE_PARAM=0x17371000
5	最も詳細なトレースメッセージ。	デバッグ	その他+ DEVICE_CONFIGURATION + (デバイス設定+) ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + (一括操作) BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY +キー DATABASE_SELECT +キー DATABASE_PO_INFO + 管理+

トレースレベル	説明	ログ レベル	トレースマスク
			TRACE_METHODと TRACE_PARAM=0x17371006

Cisco Virtualized Voice Browser(CVVB)

CVVBでは、トレースファイルはCisco VVBコンポーネントサブシステムおよびステップからのアクティビティを記録するログファイルです。

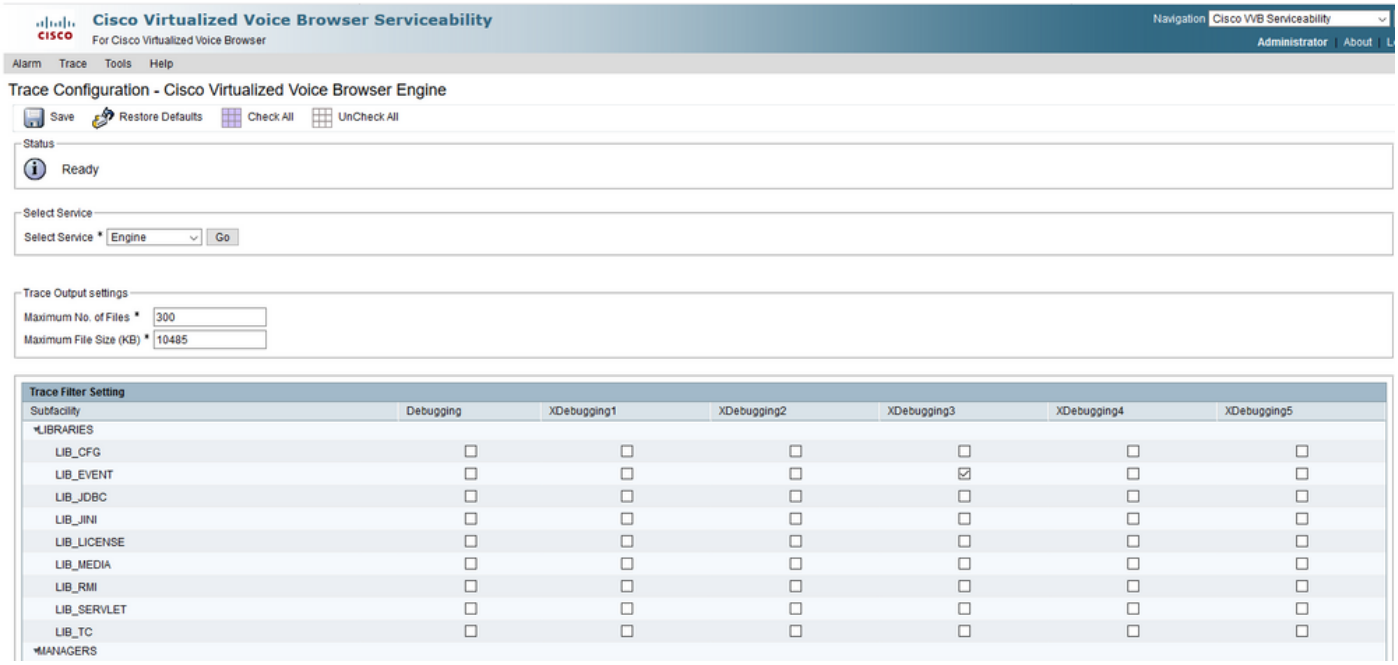
Cisco VVBには、次の2つの主要コンポーネントがあります。

- MADMログと呼ばれるCisco VVB「Administration」トレース
- MIVRログと呼ばれるCisco VVB「Engine」トレース

情報を収集するコンポーネントと、収集する情報のレベルを指定できます。

ログレベルの範囲：

- デバッグ：基本的なフローの詳細を次に示します
- XDebugging 5 – スタックトレースの詳細レベル



警告: Xdebugging5は、実稼働の読み込みシステムでは有効にしないでください。

収集する必要がある最も一般的なログはEngineです。CVVB Engineトレースのデフォルトレベルのトレースは、ほとんどの問題をトラブルシューティングするのに十分です。ただし、特定のシナリオのトレースレベルを変更する必要がある場合は、事前に定義されたシステムログプロファ

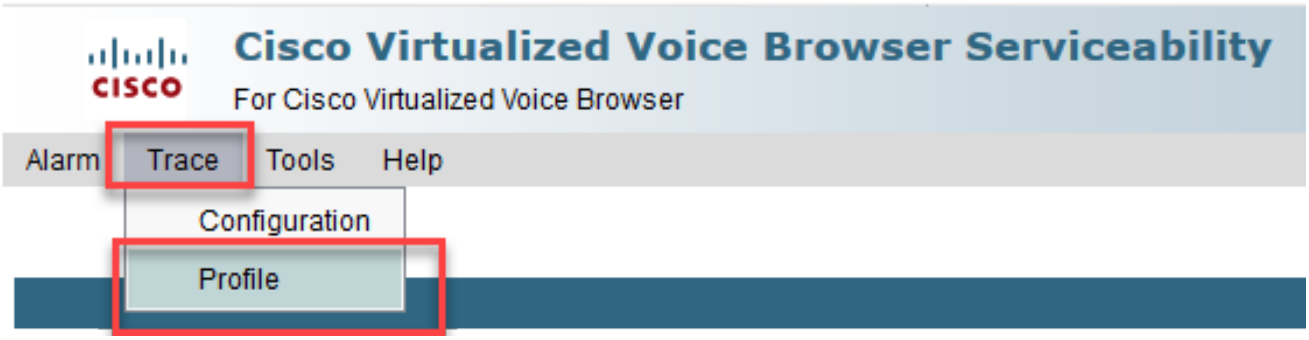
イルを使用することをお勧めします。

システムログプロファイル

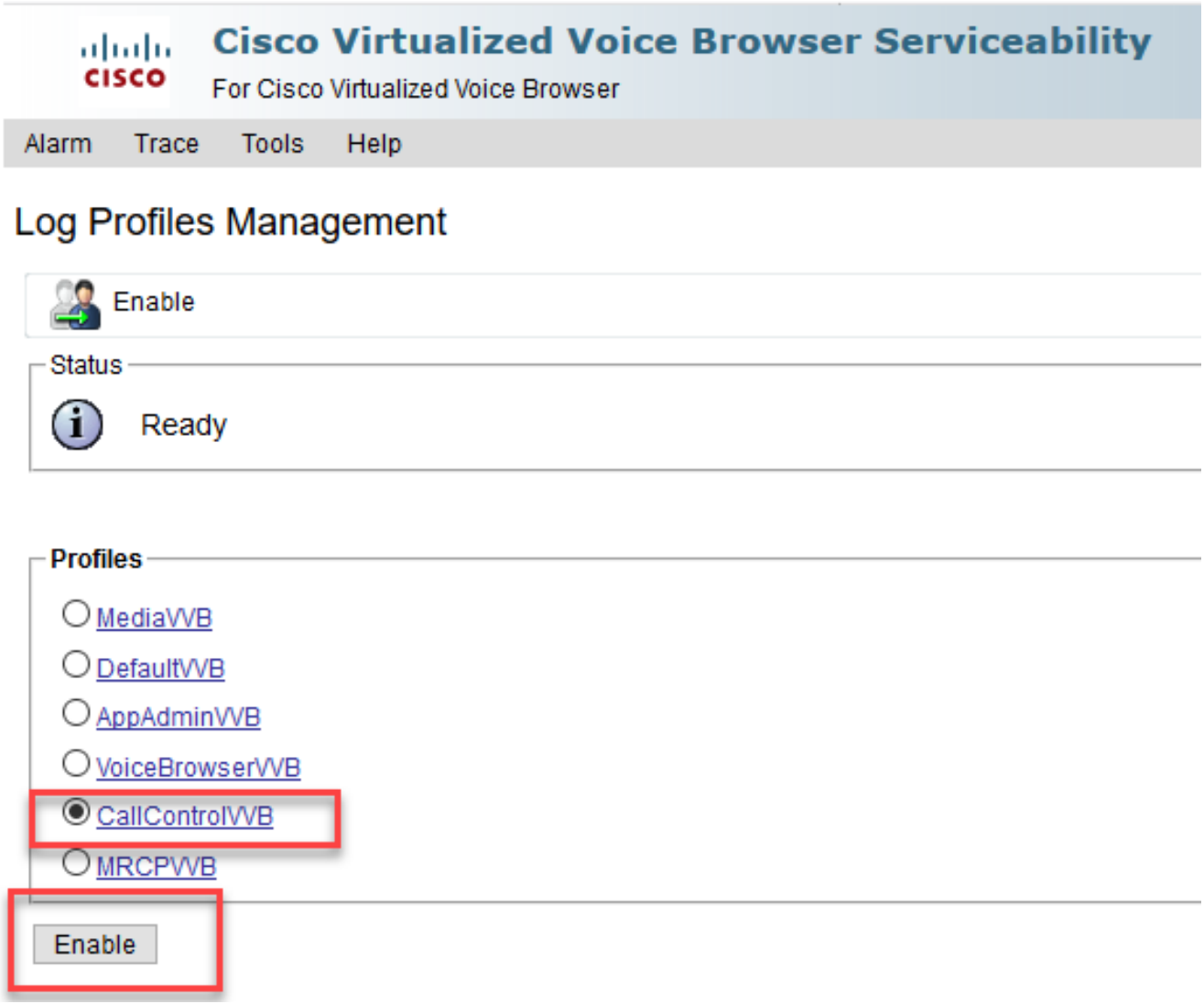
[名前(Name)]	このプロファイルをアクティブにする必要があるシナリオ
デフォルトVVB	汎用ログが有効になっています。
AppAdminVVB	AppAdmin、Cisco VVB Serviceability、およびその他のWebページを使用したWeb管理に関する問題
メディアVVB	メディア設定またはメディア送信の問題の場合。
音声ブラウザVVB	コールハンドルに関する問題の場合。
MRCPVVB	Cisco VVBインタラクションを伴うASR/TTSの問題の場合。
コール制御VVB	SIP信号に関連する問題については、ログで公開されています。

1. CVVBのメインページ(https://X.X.X.X/uccxservice/main.htm)を開き、Cisco VVB Serviceabilityページに移動します。管理アカウントでログインします

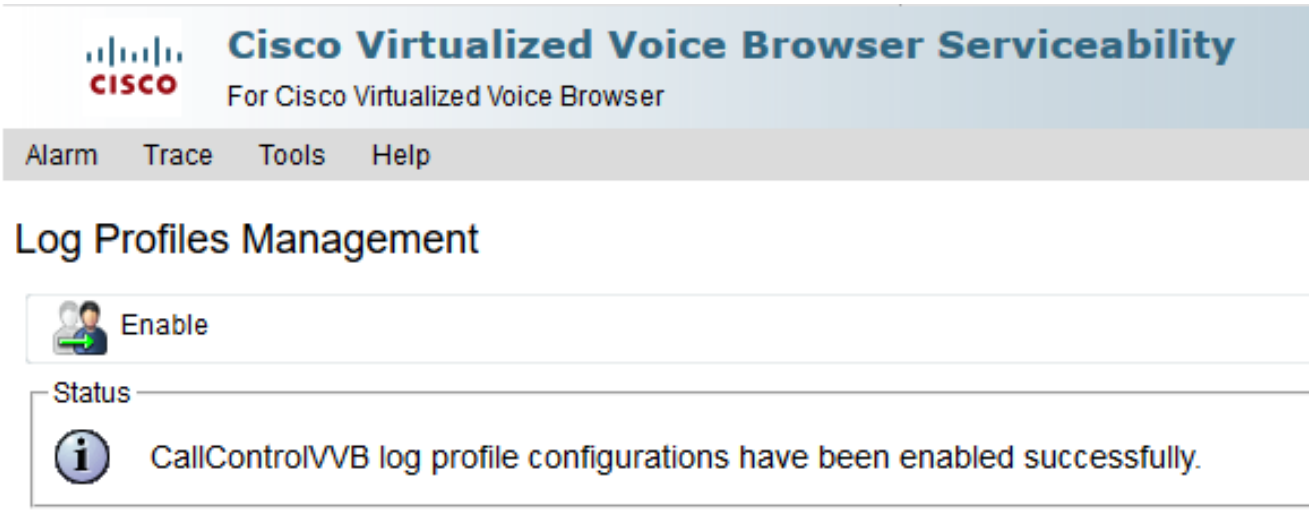
2. 選択 Trace -> Profileを選択します。



3. 特定のシナリオに対して有効にするプロファイルにチェックマークを入れて、Enableボタンをクリックします。たとえば、SIP関連の問題に対してはプロファイルCallControlVVBを有効にし、自動音声認識と音声合成(ASR/TTS)インタラクションに関連する問題に対してはMRCPVVBを有効にします。



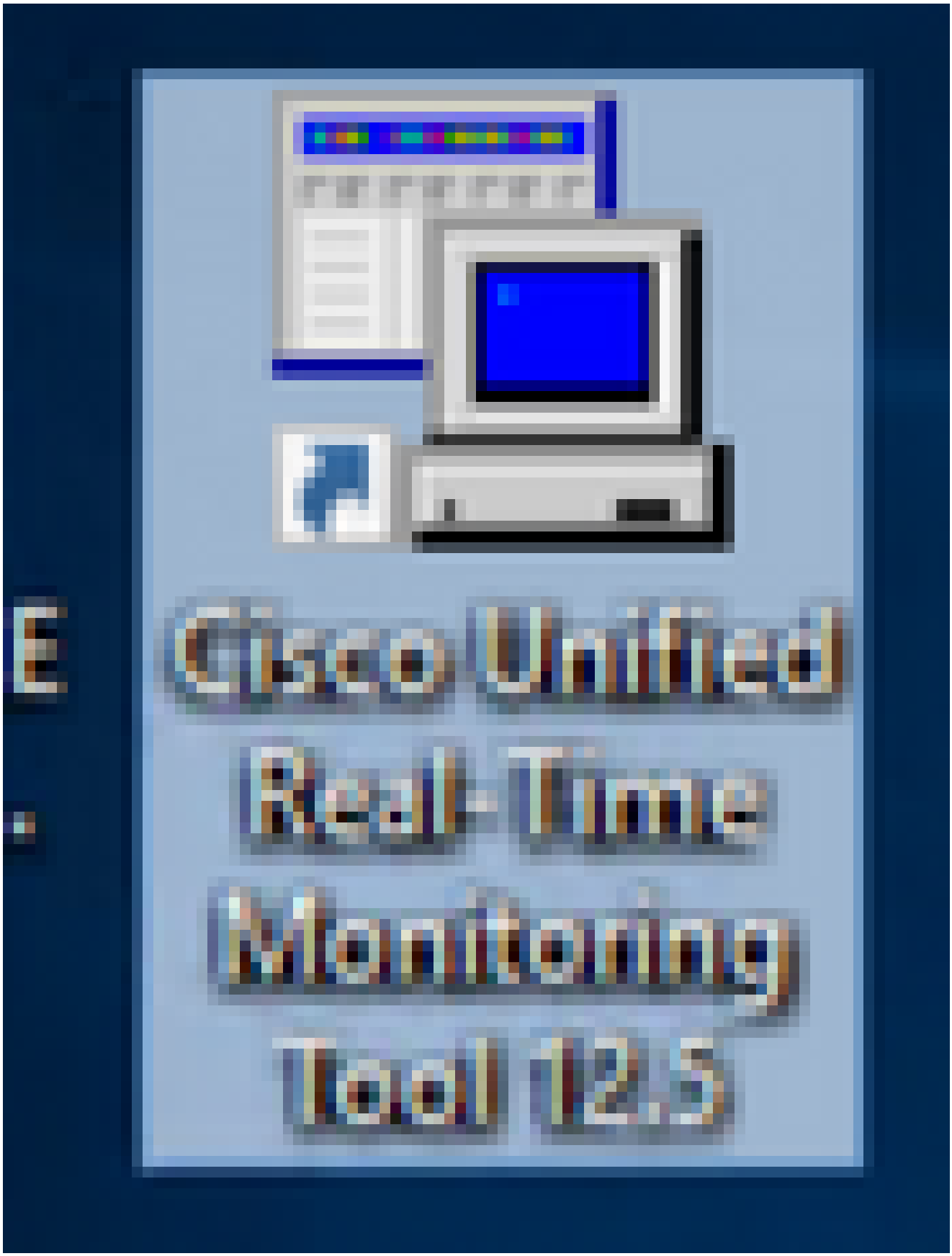
4. enableボタンをクリックすると、成功したことを示すメッセージが表示されます。



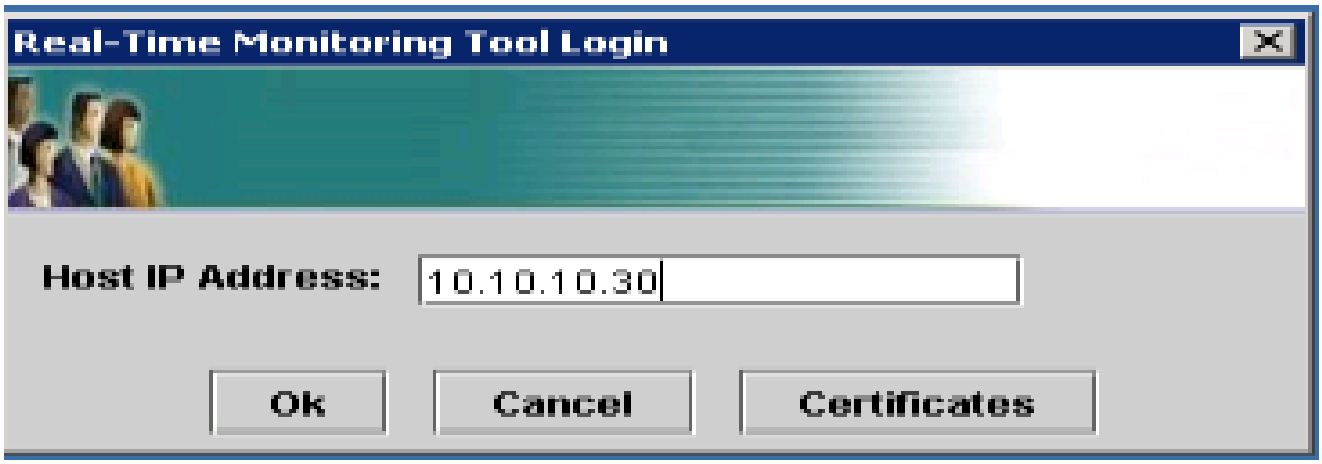
5. 問題が再現されたら、ログを収集します。ログを収集するには、CVVBに付属しているReal Time Monitor Tool(RTMT)を使用します。

6. デスクトップのCisco Unified Real-Time Monitoring Toolアイコンをクリックします（必要に

応じて、CVVBからこのツールをダウンロードします）。

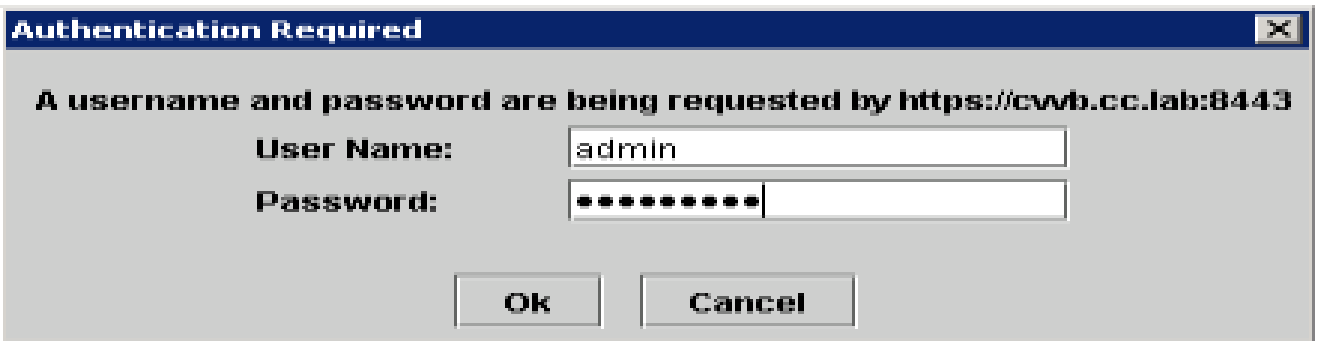


7. VVBのIPアドレスを指定して、OKをクリックします。



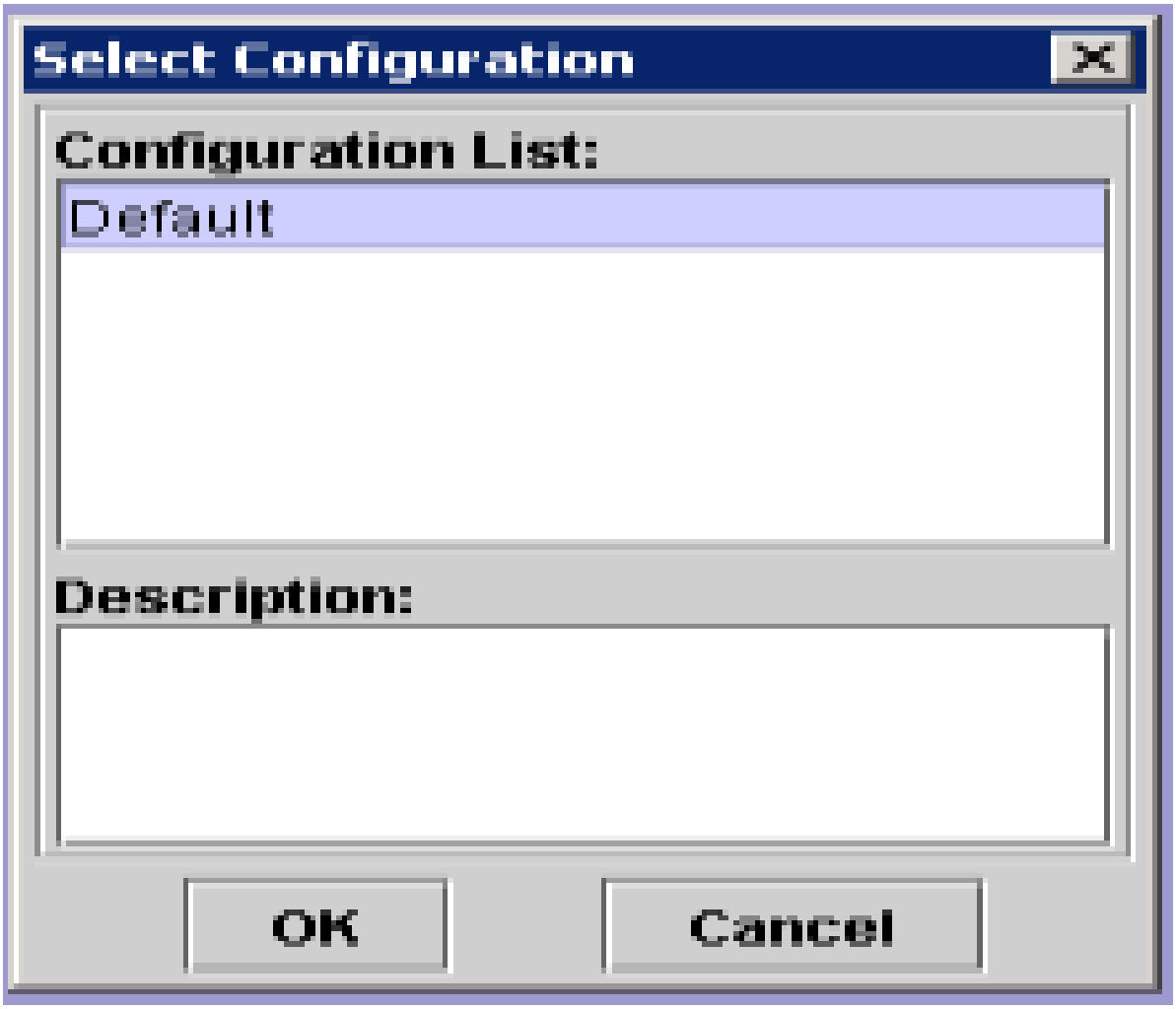
8. 表示された証明書情報を受け入れます

9. クレデンシャルを入力し、OKをクリックします。



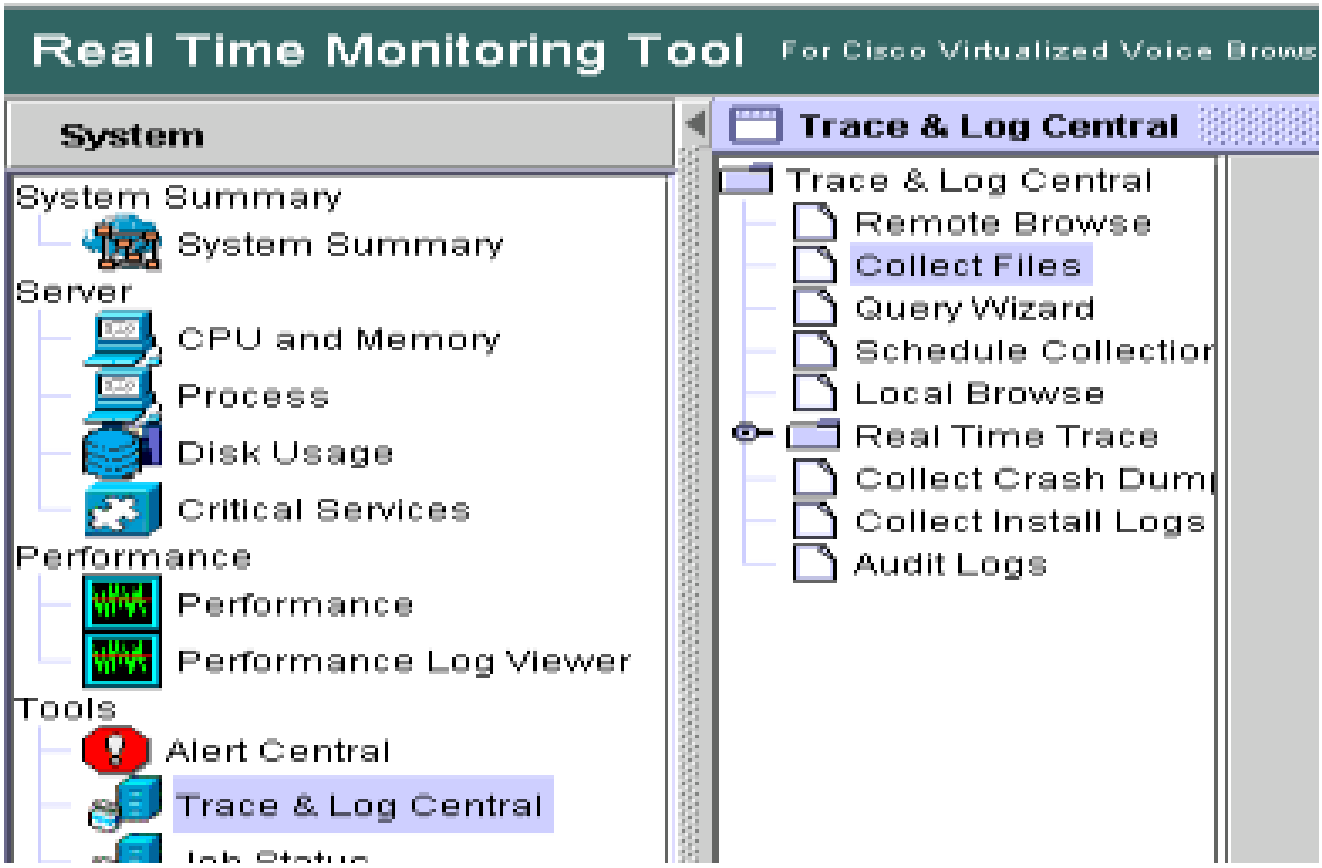
10. TimeZone エラーが表示された場合は、Yesボタンをクリックした後でRTMTを閉じることができます。RTMTツールを再起動してください。

11. デフォルト設定を選択したままで、OKをクリックします。

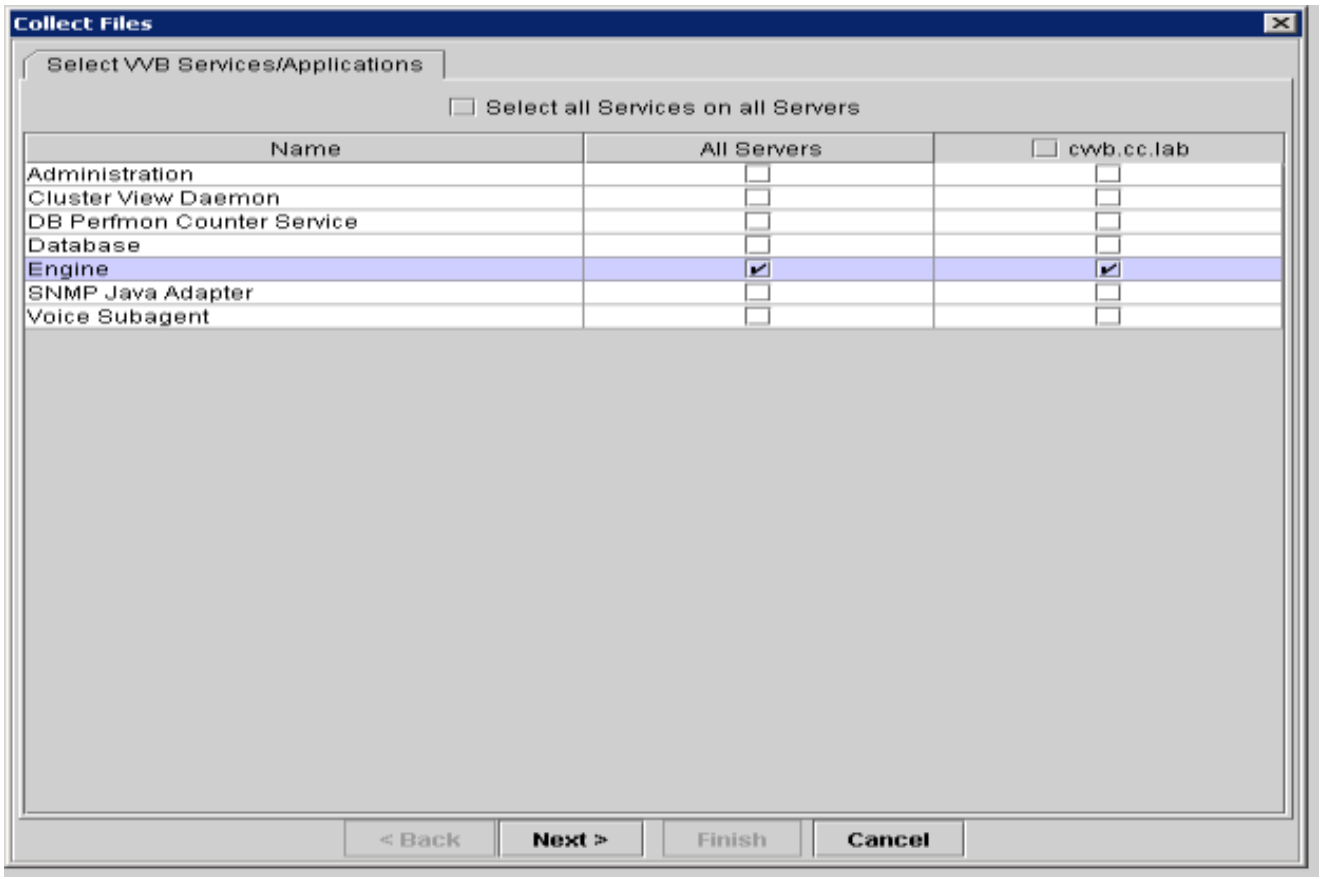


を参照。

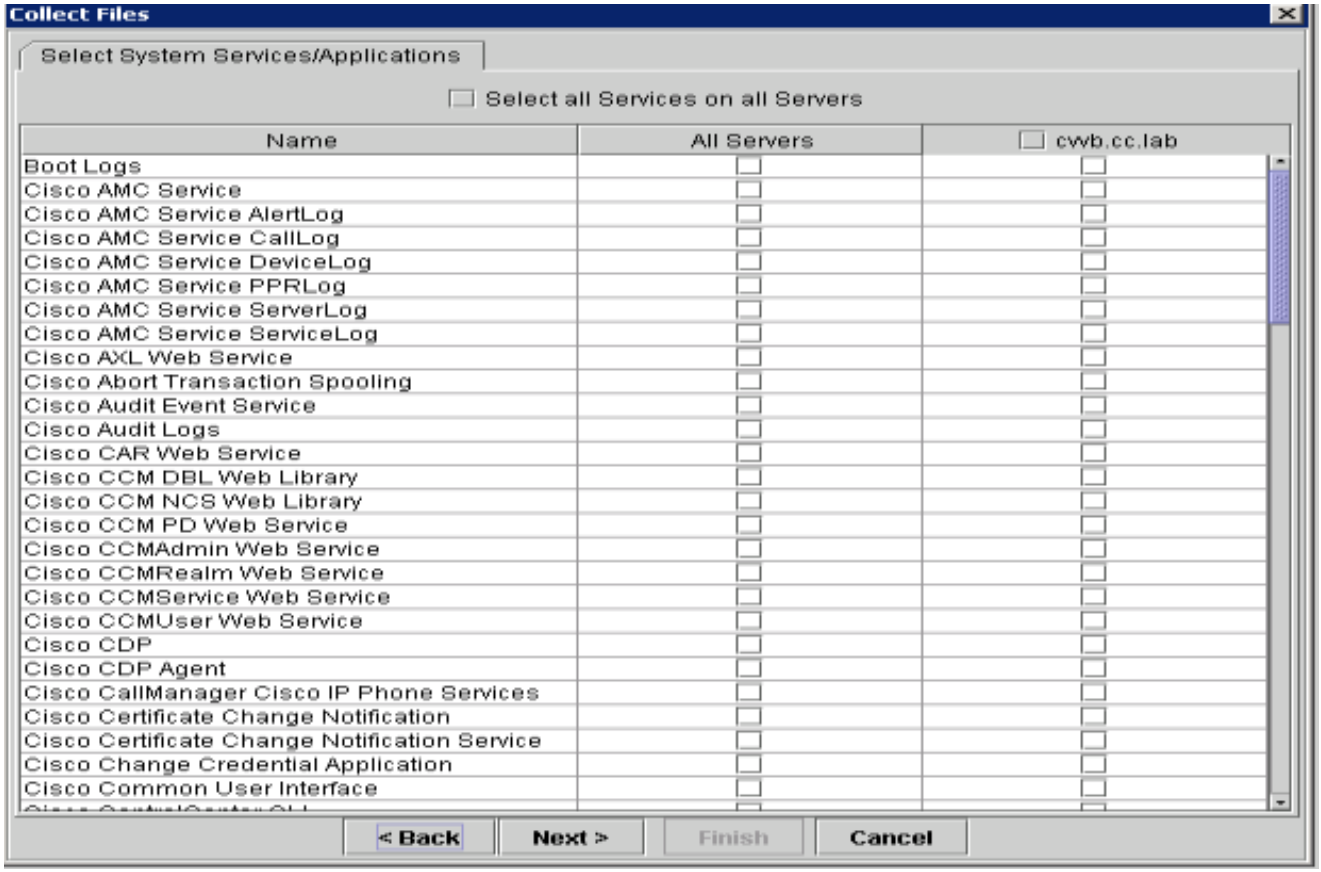
12. Trace & Log Centralを選択し、Collect Filesをダブルクリックします。



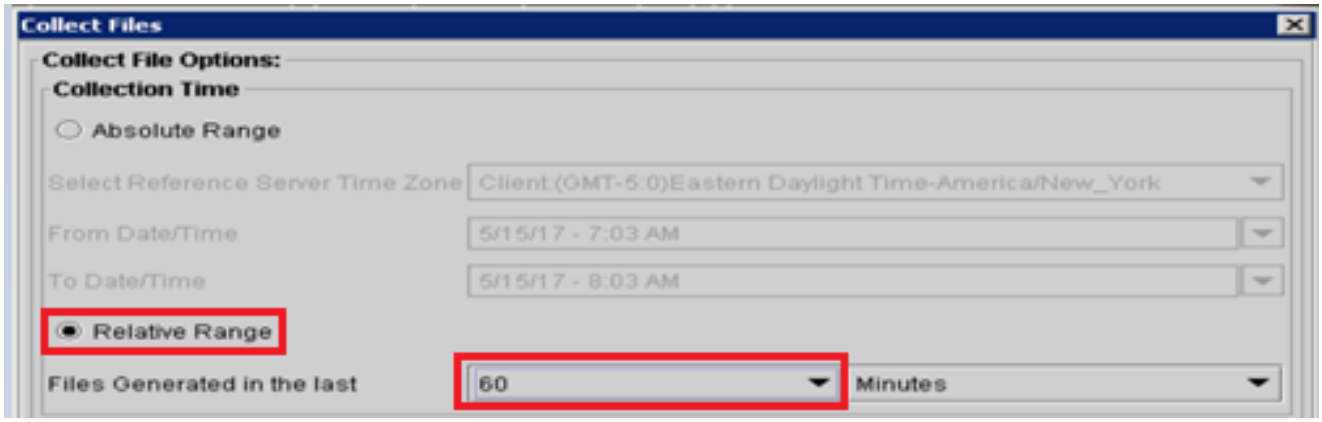
13. 新しく開いたウィンドウでEngineを選択し、Nextをクリックします。



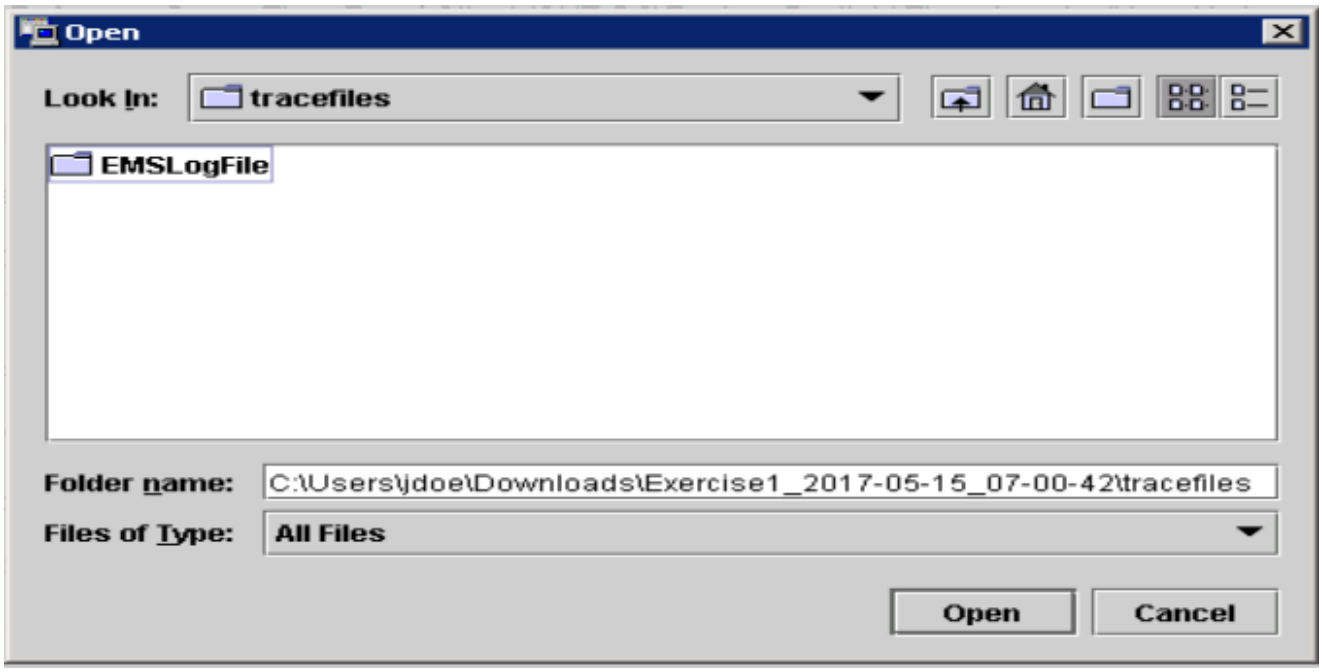
14. 次のウィンドウで再度Nextをクリックします。



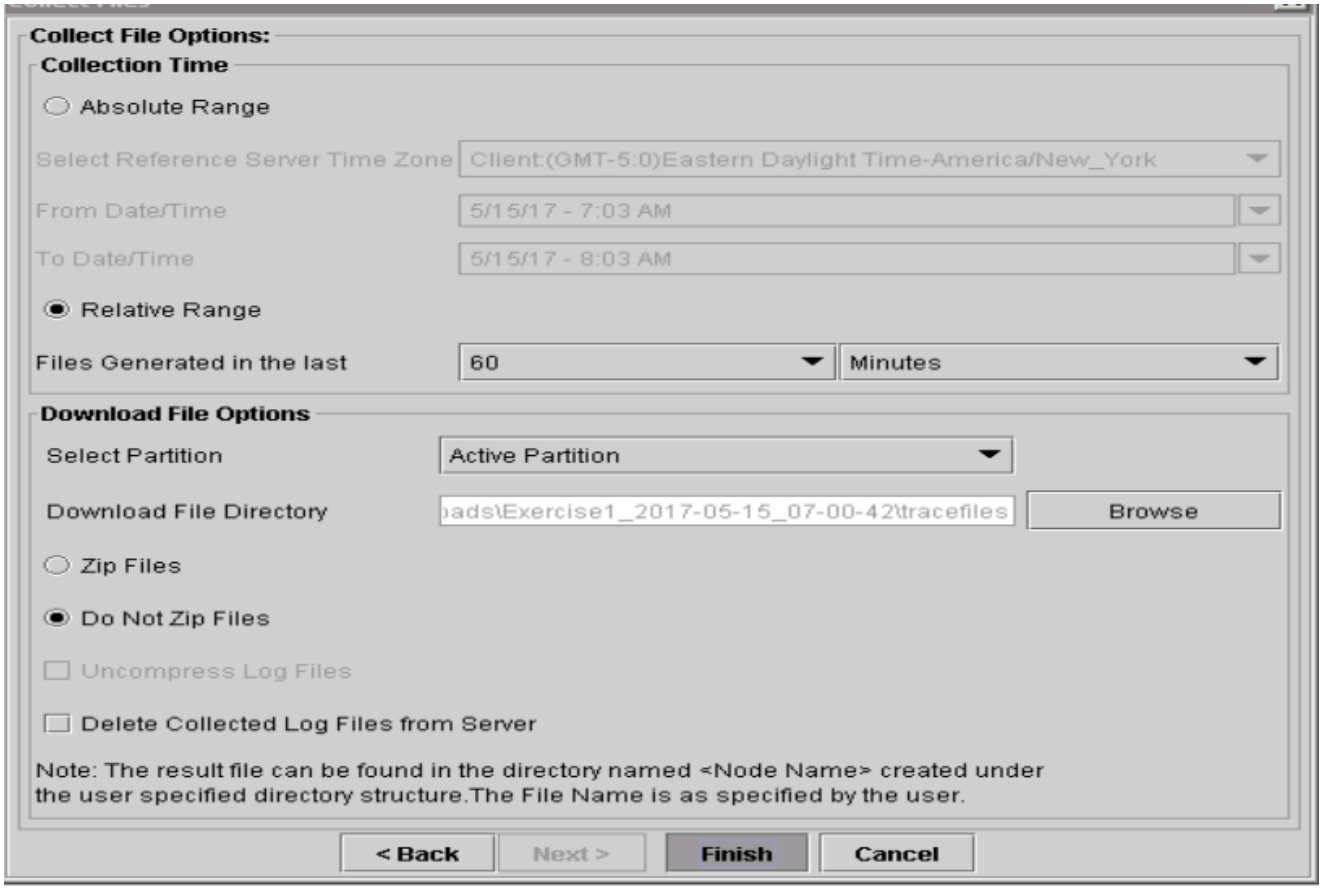
15. Relative Rangeを選択し、不正コールの時間をカバーする時間を選択していることを確認します。



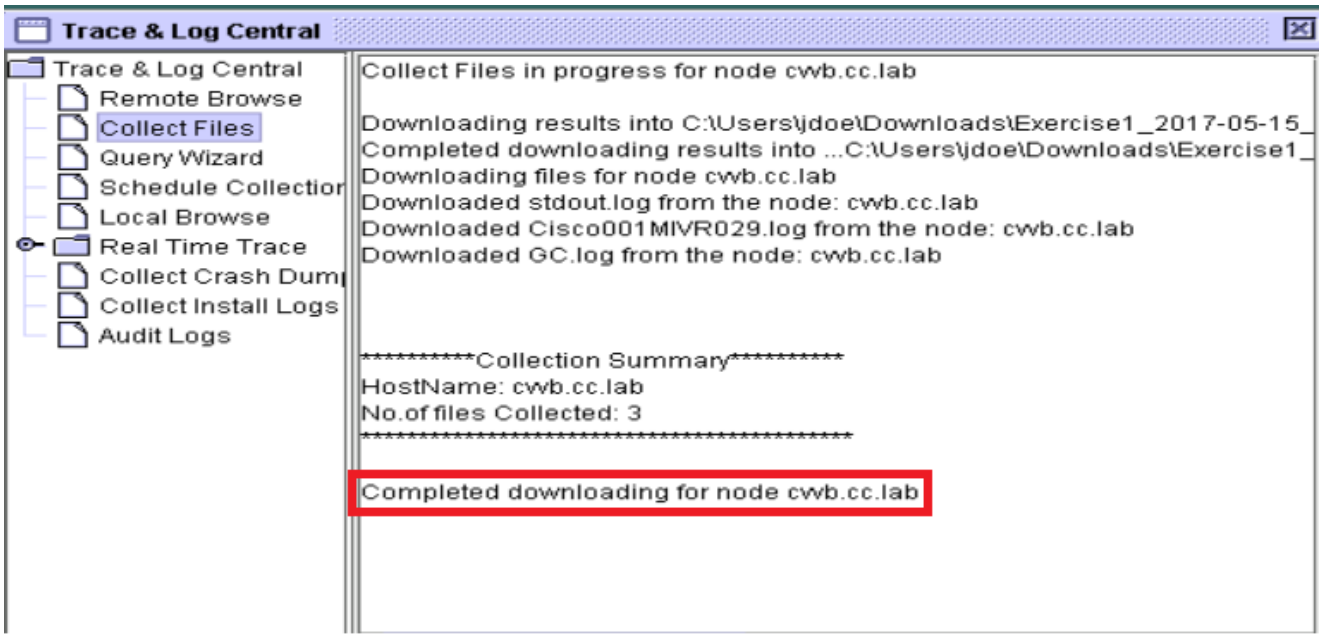
16. Download File OptionsでBrowseをクリックし、ファイルを保存するディレクトリを選択して、Open$_{save}$をクリックします。



17. すべてを選択したら、Finishボタンをクリックします。



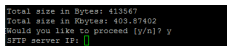
18. これにより、ログファイルが収集されます。RTMTに確認メッセージが表示されるまで待ちます。



19. トレースが保存されているフォルダに移動します。

20. 必要なのはエンジンログだけです。ファイルを見つけるには、\<time stamp>\uccx\log\MIVRフォルダに移動します。

オプション2:SSHおよびSFTP経由 – 推奨オプション

1. セキュアシェル(SSH)を使用してVVBサーバにログインします。
2. 次のコマンドを入力して、必要なログを収集します。ログが圧縮され、ログのアップロード先のSFTPサーバを指定するように求められます。 **file get activelog /uccx/log/MIVR/*** 
3. これらのログはSFTPサーバパス<IP address>\<date time stamp>\active_nnn.tgz（nnnは長い形式のタイムスタンプ）に保存されます。

CUBEおよびCUSPのトレースと収集ログの設定

CUBE(SIP)

1. ログタイムスタンプを設定し、ロギングバッファを有効にします。

```
#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
```

⚠ 警告：実稼働のCisco IOS®ソフトウェアゲートウェイに変更を加えると、サービスが

停止する可能性があります。

2. これは、提供されたコール量で問題なく推奨デバッグを処理できる非常に堅牢なプラットフォームです。ただし、シスコでは次のことを推奨しています。
   - すべてのログをロギングバッファではなくsyslogサーバに送信します。

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

   - debugコマンドを1つずつ適用し、その後でCPU使用率を確認します。

```
show proc cpu hist
```

警告:CPUのCPU使用率が最大70 ~ 80 %になると、パフォーマンスに関連するサービスへの影響のリスクが大幅に高まります。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。

3. これらのデバッグを有効にします：

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

4. 問題を再現します。
5. トレースを無効にします。

```
#undebug all
```

6. ログを収集します。

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

CUSP

1. CUSPで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
```

2. 問題を再現します。
3. 作業が完了したら、ロギングをオフにします。

ログの収集

1. CUSPでユーザを設定します（例：test）。
2. CUSPプロンプトでこの設定を追加します。

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

3. CUSP IPアドレスにFTP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。

トレースの設定とUCCEログの収集

シスコでは、Diagnostis Framework PorticoまたはSystem CLIツールを使用してトレースレベルを設定し、トレースを収集することを推奨しています。

注：診断フレームワークのPorticoおよびSystem CLIの詳細については、『Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1)』の「診断ツール」の章を参照してください。

ほとんどのUCCEシナリオをトラブルシューティングする際に、デフォルトのトレースレベルで十分な情報が得られない場合は、必要なコンポーネントでトレースレベルを3に設定します（一部の例外を除く）。

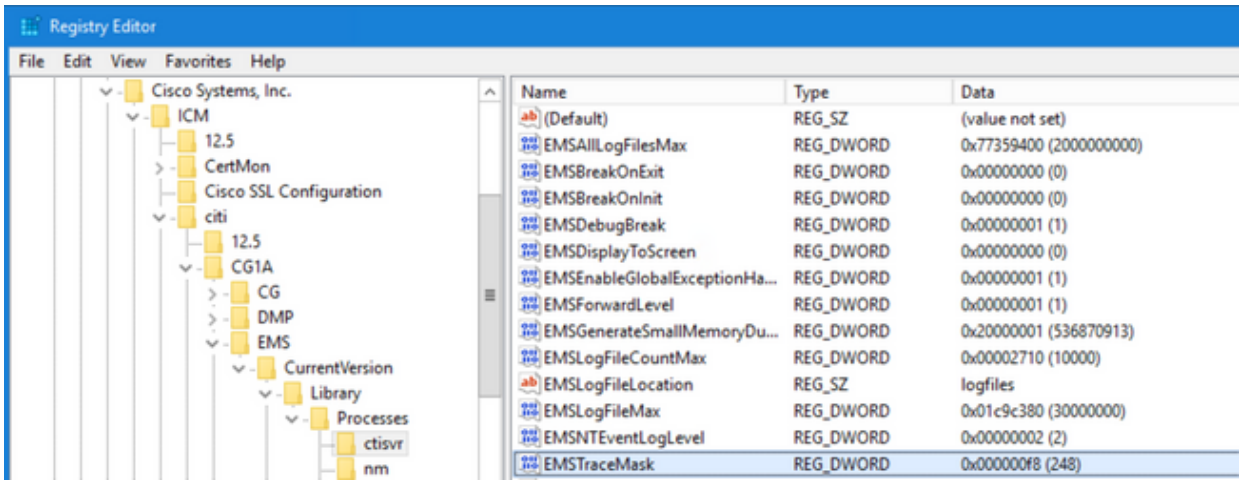
注：詳細については、『Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1)』の「Trace Level」の項を参照してください。

たとえば、発信ダイヤラの問題をトラブルシューティングする場合、ダイヤラがビジーであれば、トレースレベルをレベル2に設定する必要があります。

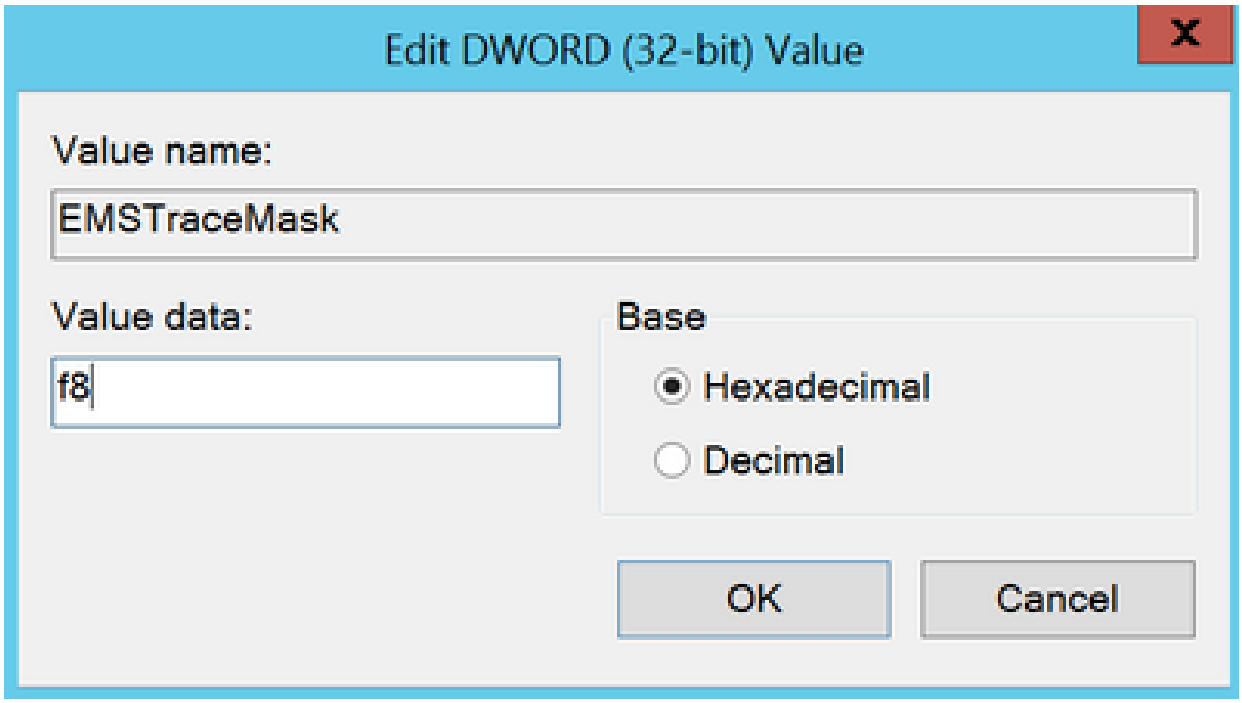
CTISVR(CTISVR)については、レベル2およびレベル3はシスコが推奨する正確なレジストリレベルを設定しません。CTISVRの推奨トレースレジストリは0XF8です。

1. UCCE Agent PGで、レジストリエディタ(Regedit)を開きます。

2. HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a and b)\EMS\CurrentVersion\library\Processes\ctisvrに移動します。



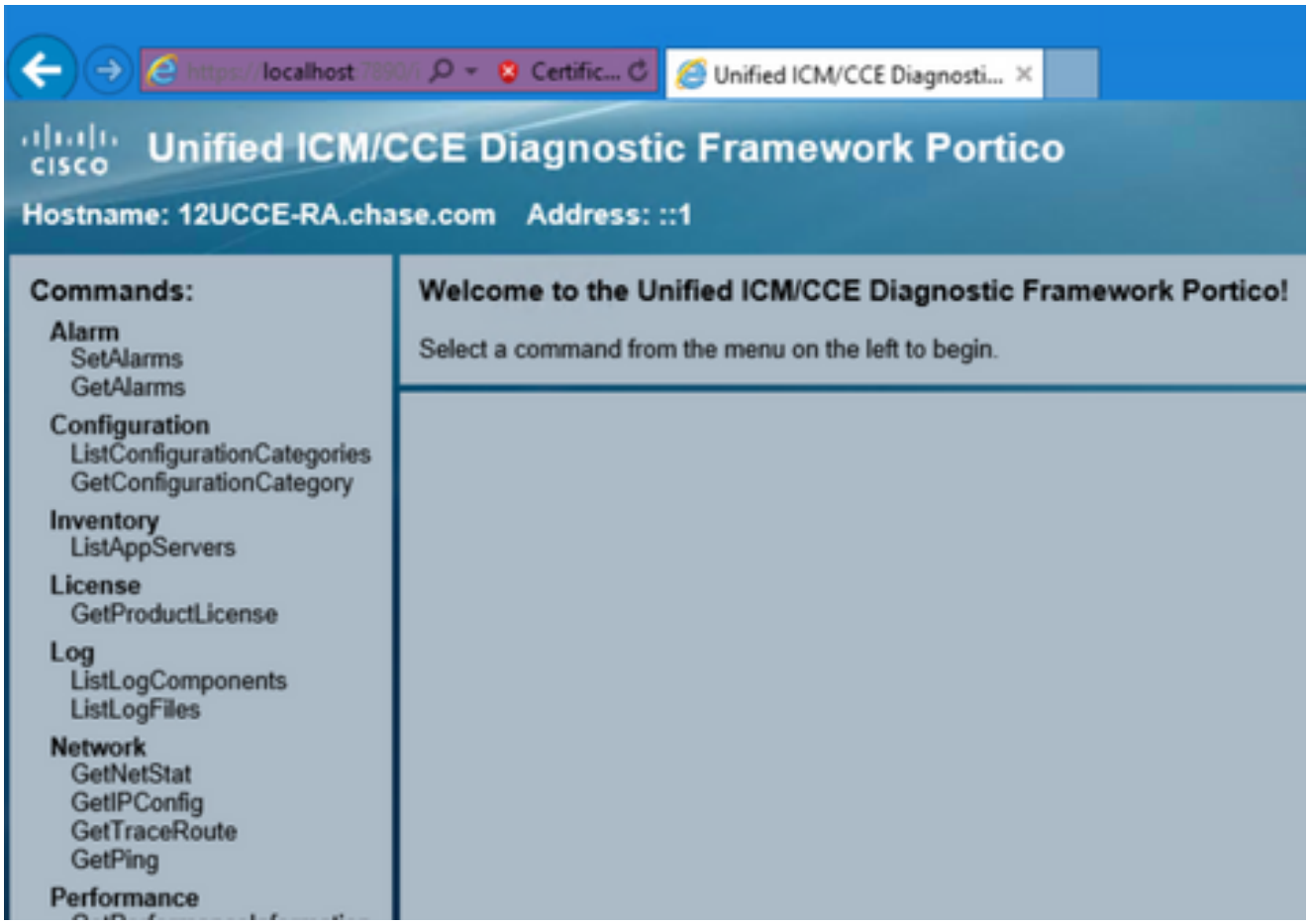
3. EMSTraceMaskをダブルクリックし、値をf8に設定します。



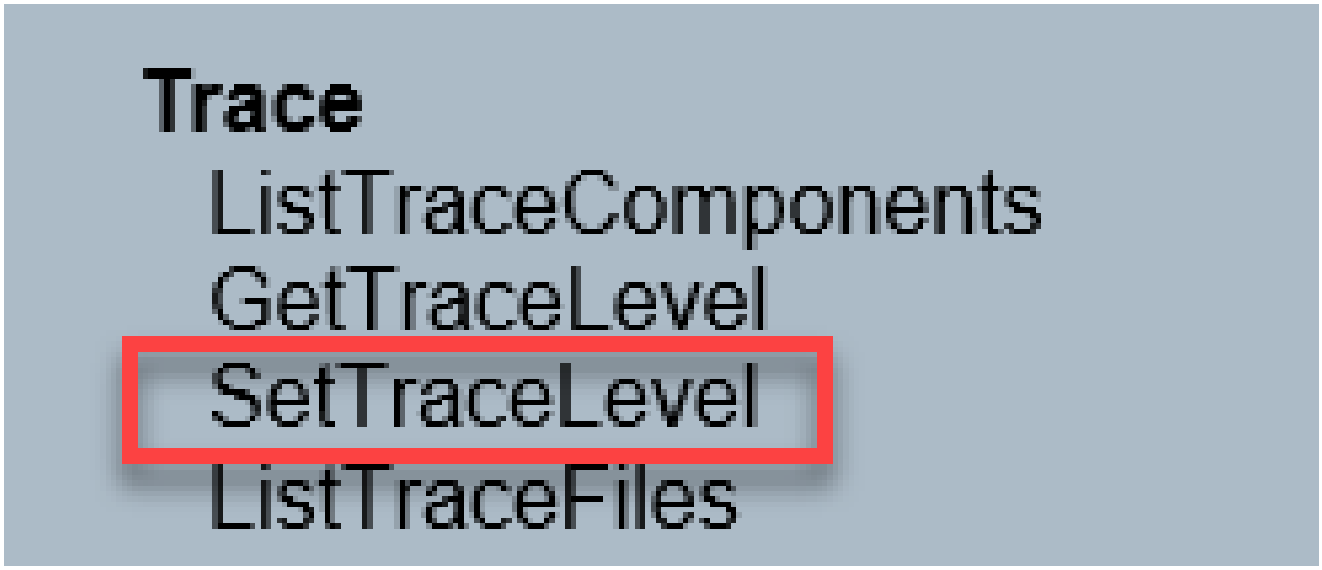
4. Okをクリックして、レジストリエディタを閉じます。次に、UCCEコンポーネントトレースを設定する手順を示します（例としてRTRプロセスを使用します）。

SetTraceレベル

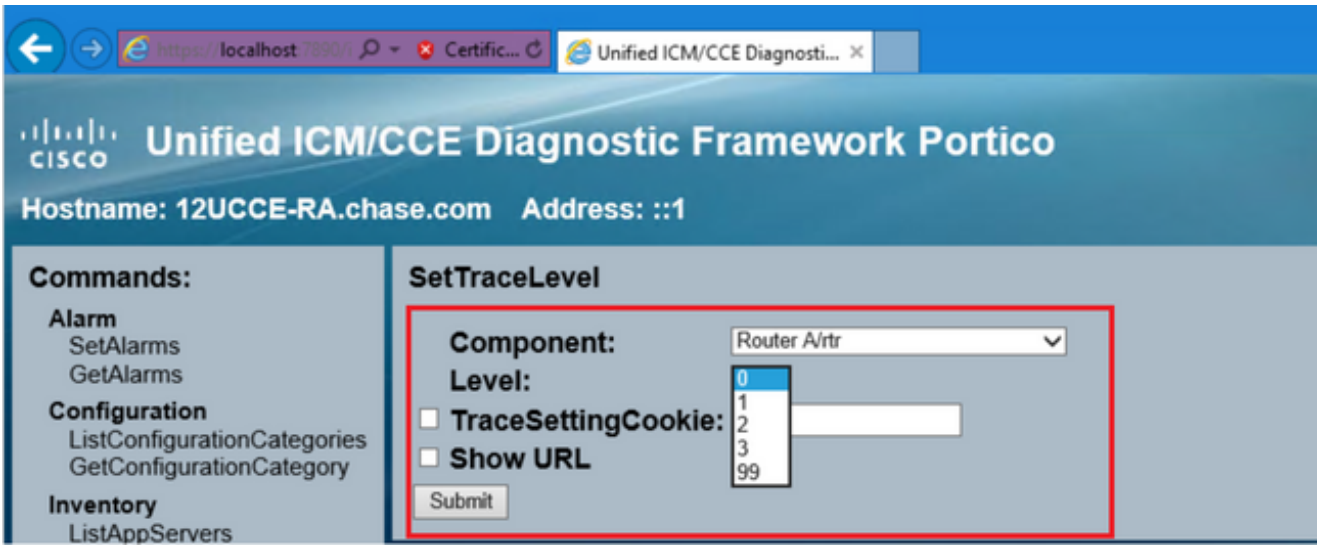
1. トレースを設定する必要があるサーバからDiagnostic Framework Porticoを開き、管理者ユーザとしてログインします



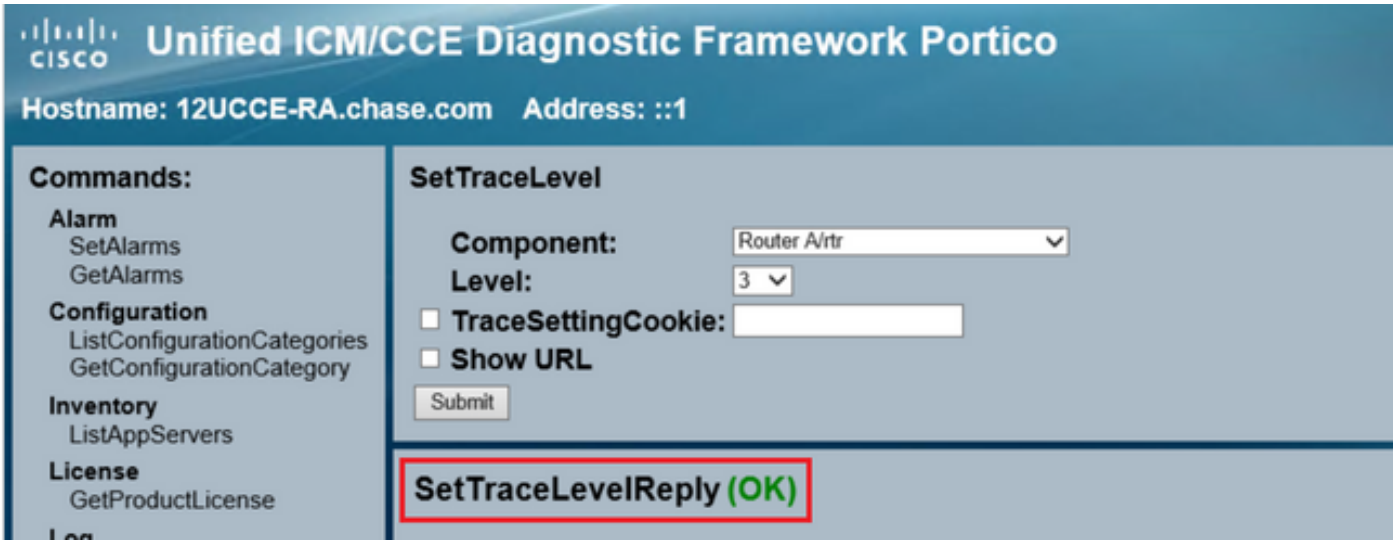
2. Commandsセクションで、Traceに移動し、 SetTraceLevelです。



3. SetTraceLevelウィンドウで、コンポーネントとレベルを選択します。



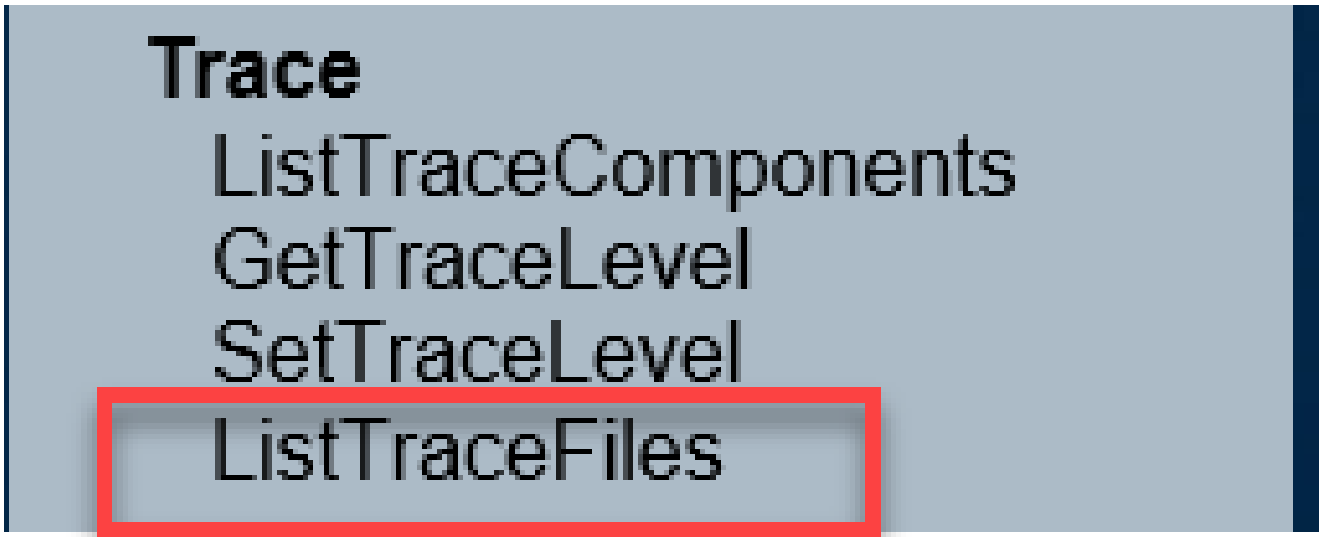
4. [Submit] をクリックします。完了すると、OKメッセージが表示されます。



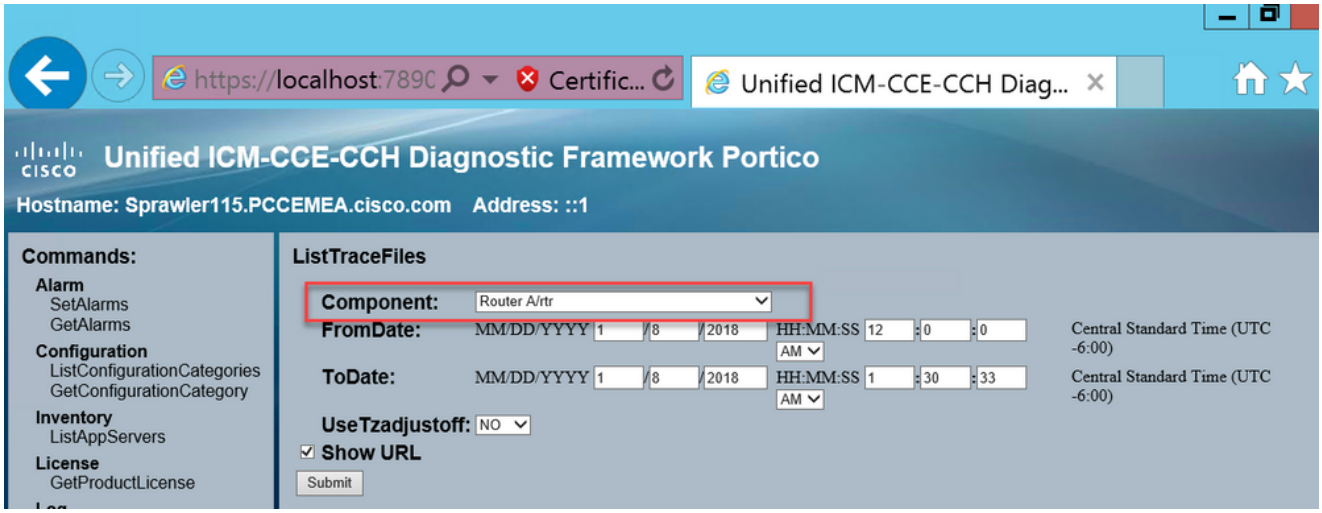
警告：問題を再現する際は、トレースレベルをレベル3に設定してください。問題が再現されたら、トレースレベルをデフォルトに設定します。レベル2とレベル3は低レベルのトレースを設定するため、JTAPIGWトレースを設定する場合は特に注意が必要です。これにより、パフォーマンスに影響が及ぶ可能性があります。非実稼働時またはラボ環境では、JTAPIGWでレベル2またはレベル3を設定します。

ログ収集

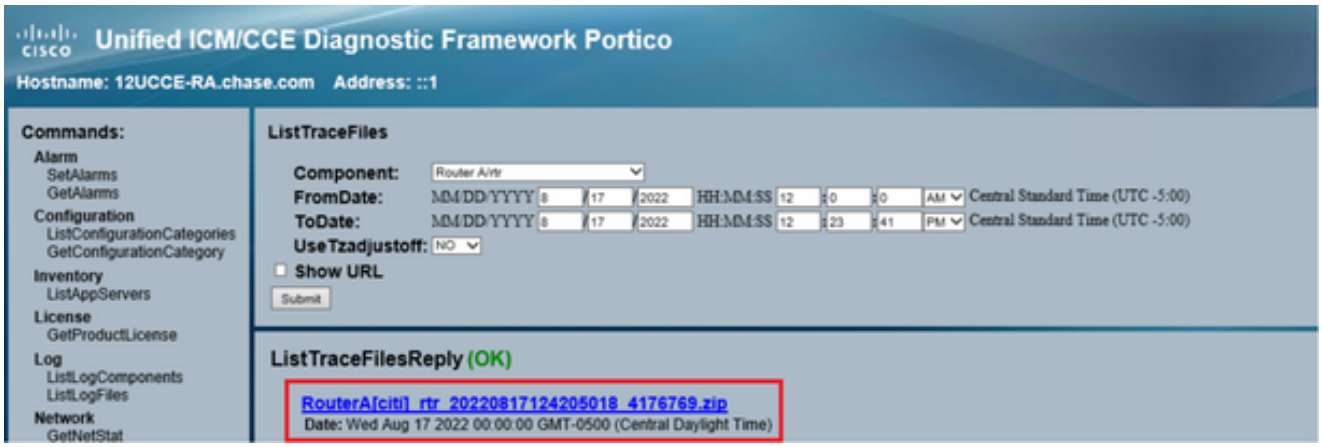
1. Diagnostic Framework PorticoのCommandsセクションでTraceに移動し、ListTraceFileを選択します。



2. ListTraceFileウィンドウで、Component、FromDate、およびToDateを選択します。Show URLボックスにチェックマークを入れてから、Submitをクリックします。



3. 要求が完了すると、ZIPログファイルのリンクを含むOKメッセージが表示されます。

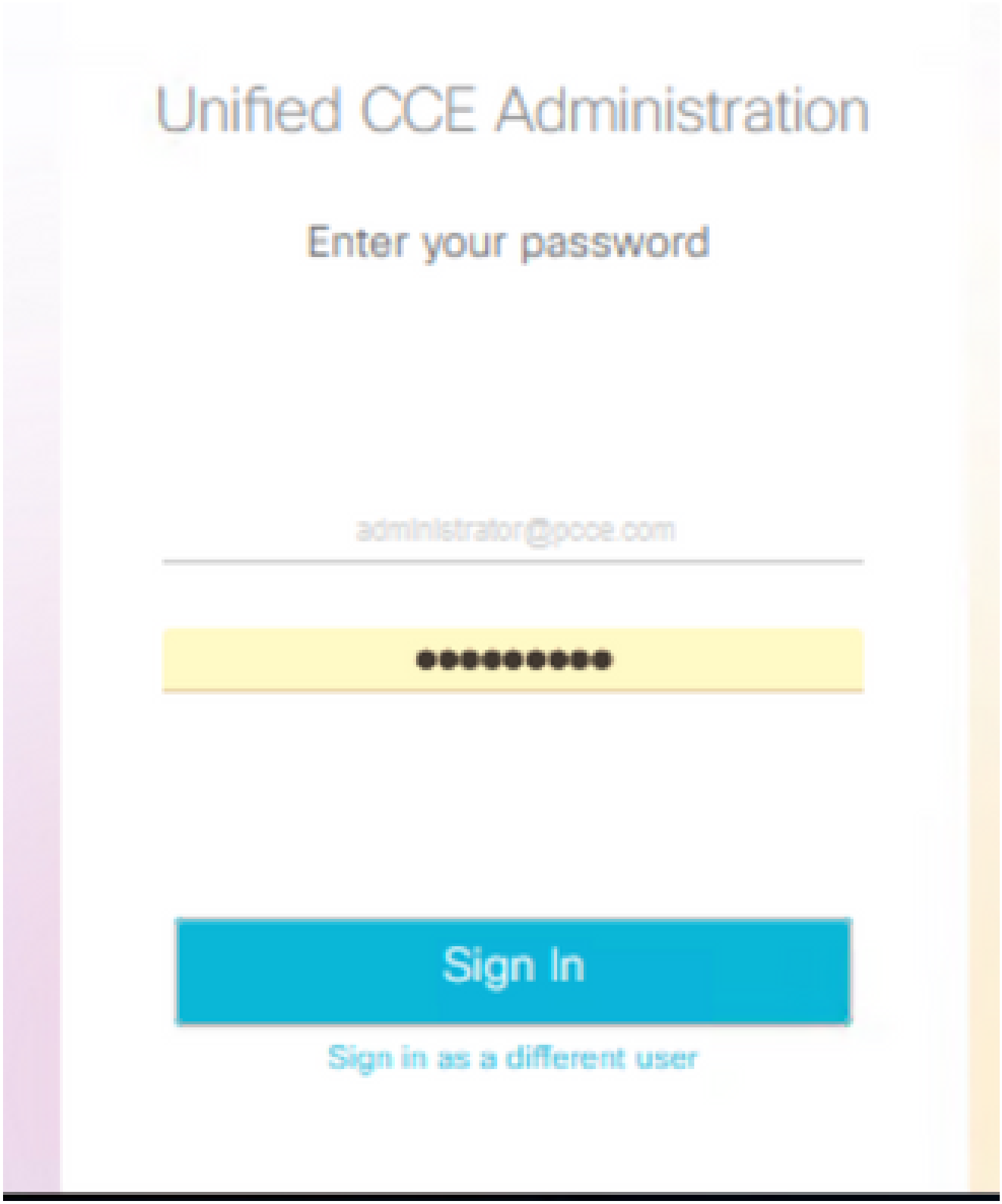


4. ZIPファイルのリンクをクリックしsave、選択した場所のファイルをクリックします。

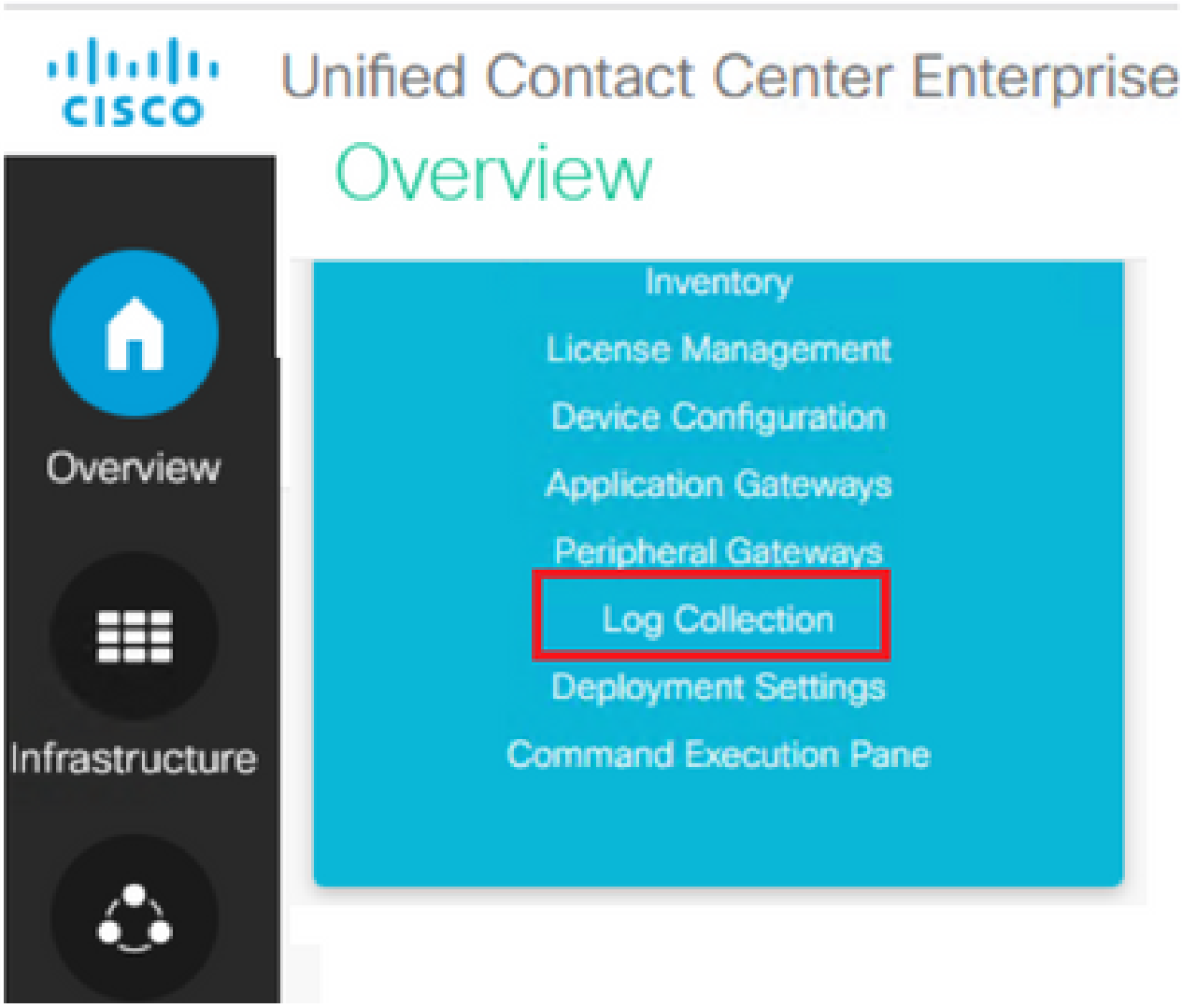
トレースの設定とPCCEログの収集

PCCEには、トレースレベルを設定する独自のツールがあります。ログを有効にして収集する方法としてDiagnostic Framework PorticoまたはシステムCLIが推奨されるUCCE環境には適用されません。

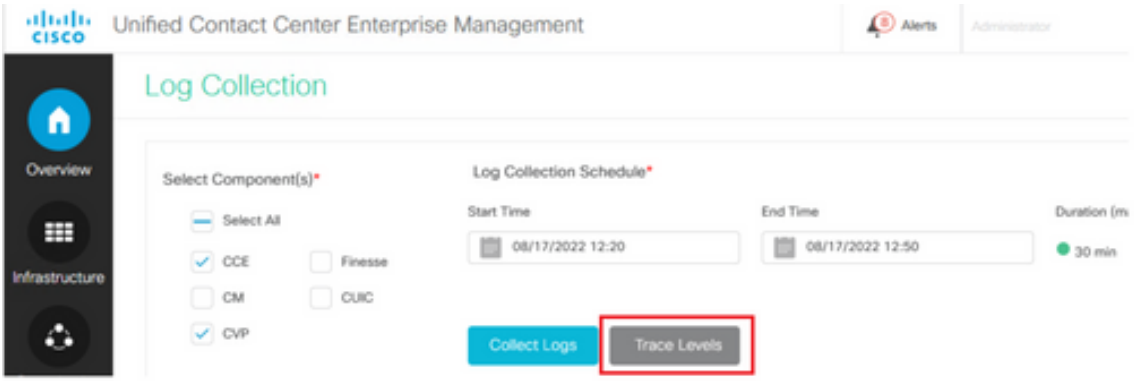
1. PCCE AWサーバからUnified CCE Web Administrationツールを開き、Administratorアカウントにログインします。



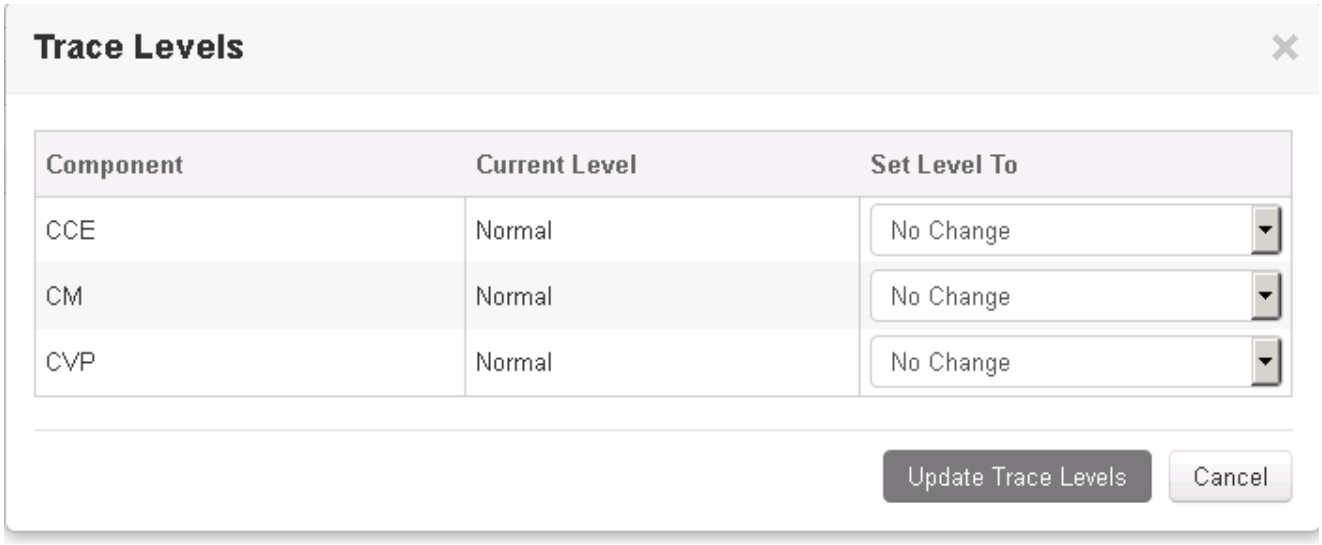
2. Overview->Infrastructure Settings->Log Collectionの順に選択し、Log Collectionページを開きます。



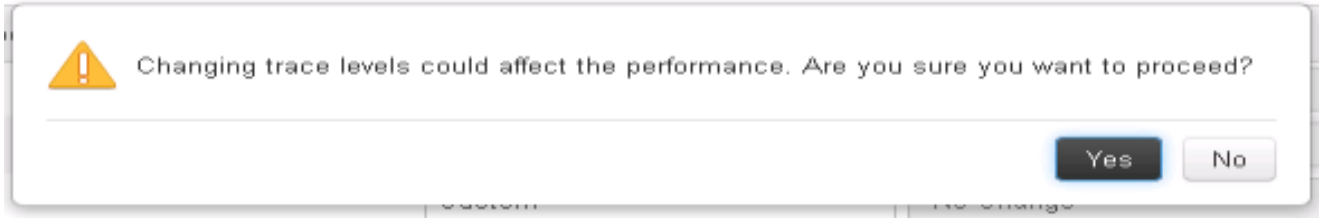
3. Log CollectionページでTrace Levelsをクリックすると、Trace Levelsダイアログボックスが開きます。



4. CCEでトレースレベルをDetailedに設定し、CMとCVPについてはNo Changeのままにして、 トレースレベルを更新します。



5. Yesをクリックして、警告を確認します。



6. 問題が再現されたら、Unified CCE Administrationを開き、System >に戻ります ログ収集。
7. ComponentsペインでCCEとCVPを選択します。
8. 適切なログ収集時間を選択します (デフォルトは最後の30分) 。
9. Collect Logsをクリックし、ダイアログ警告でYesをクリックします。ログコレクションが開始されます。完了するまで数分待ちます。

10. 完了したら、Actions列のDownloadボタンをクリックして、すべてのログが含まれるzipファイルをダウンロードします。Save zipファイルは適切な場所にあります。

トレースの設定とCUIC/ライブデータ/IDSログの収集

SSHによるログのダウンロード

1. CUIC、LD、およびIDSのSSHコマンドライン(CLI)にログインします。
2. CUIC関連のログを収集するには、コマンドを実行します。

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関連のログを収集するには、コマンドを実行します。

file get activelog livedata/logs/*.*

4. IdS関連のログを収集するには、コマンドを実行します。

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

5. これらのログはSFTPサーバパス<IP address>\<date time stamp>\active_nnn.tgzに保存されます。nnnは長い形式のタイムスタンプです。

RTMTによるログのダウンロード

1. OAMPページからRTMTをダウンロードします。https://<HOST ADDRESS>/oampにログインします。ここで、HOST ADDRESSはサーバのIPアドレスです。

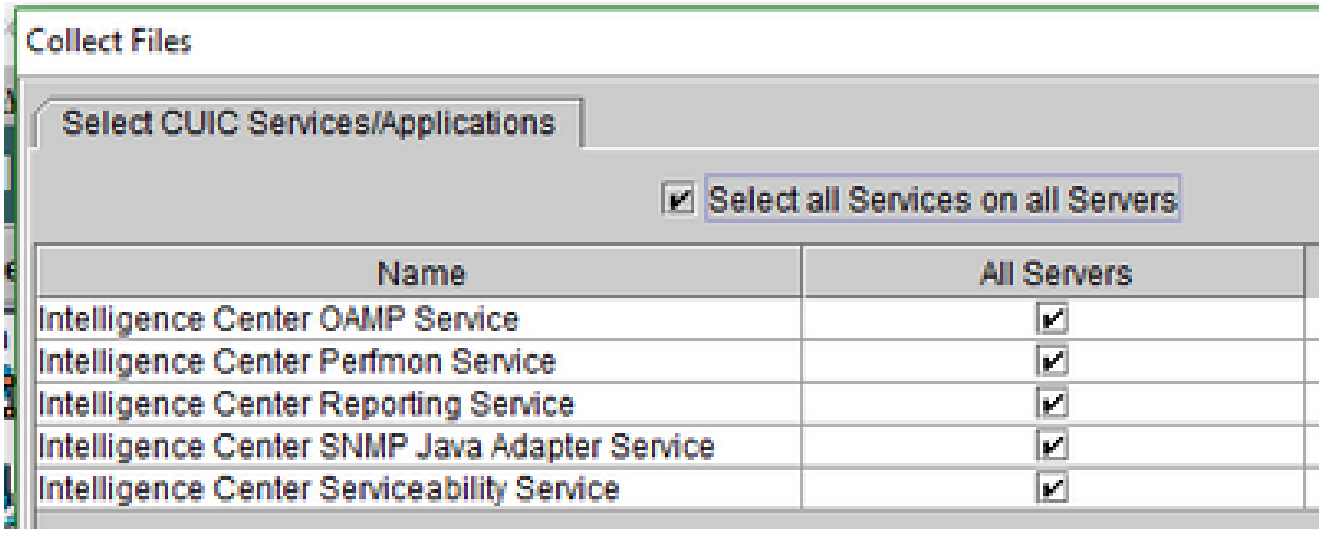
2. Tools > RTMT plugin downloadの順に移動します。プラグインをダウンロードしてインストールします。

3. RTMTを起動し、管理者クレデンシャルでサーバにログインします。

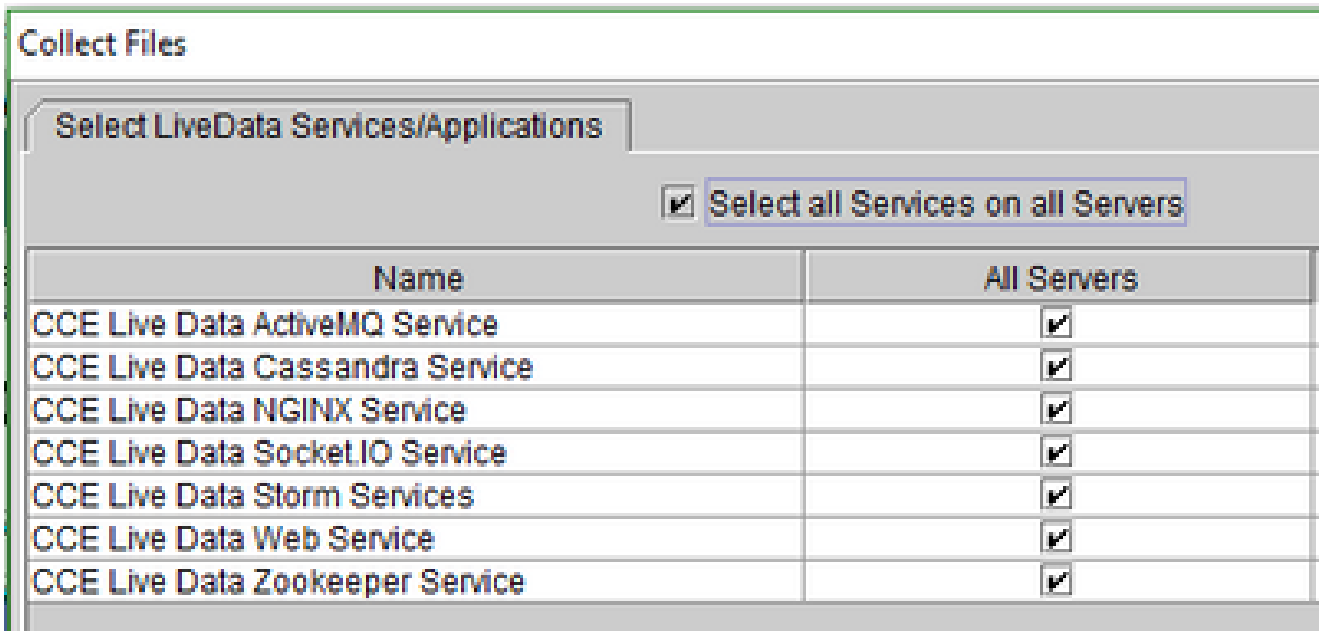
4. Trace and Log Centralをダブルクリックし、次にCollect Filesをダブルクリックします。

5. 特定のサービスに関する次のタブが表示されます。CUIC、LD、およびIDSのすべてのサービス/サーバを選択する必要があります。

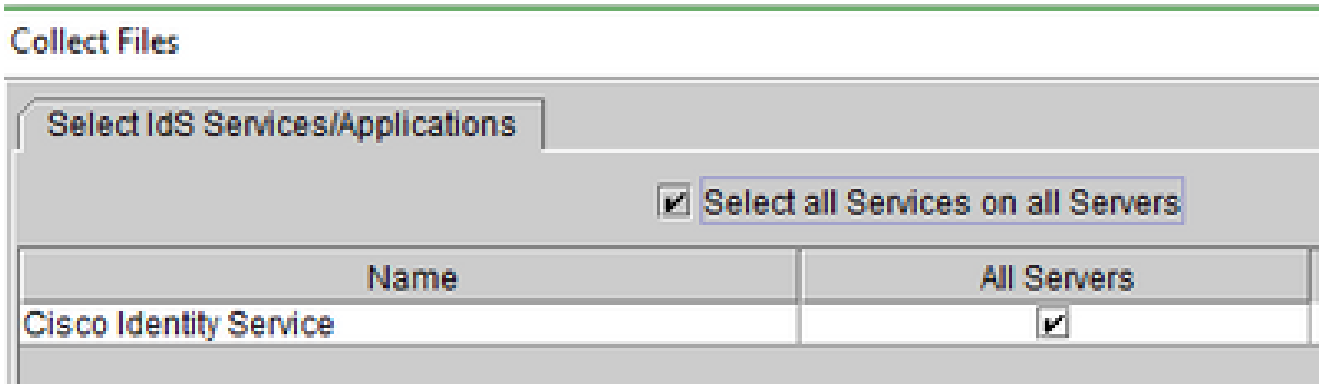
CUICの場合：



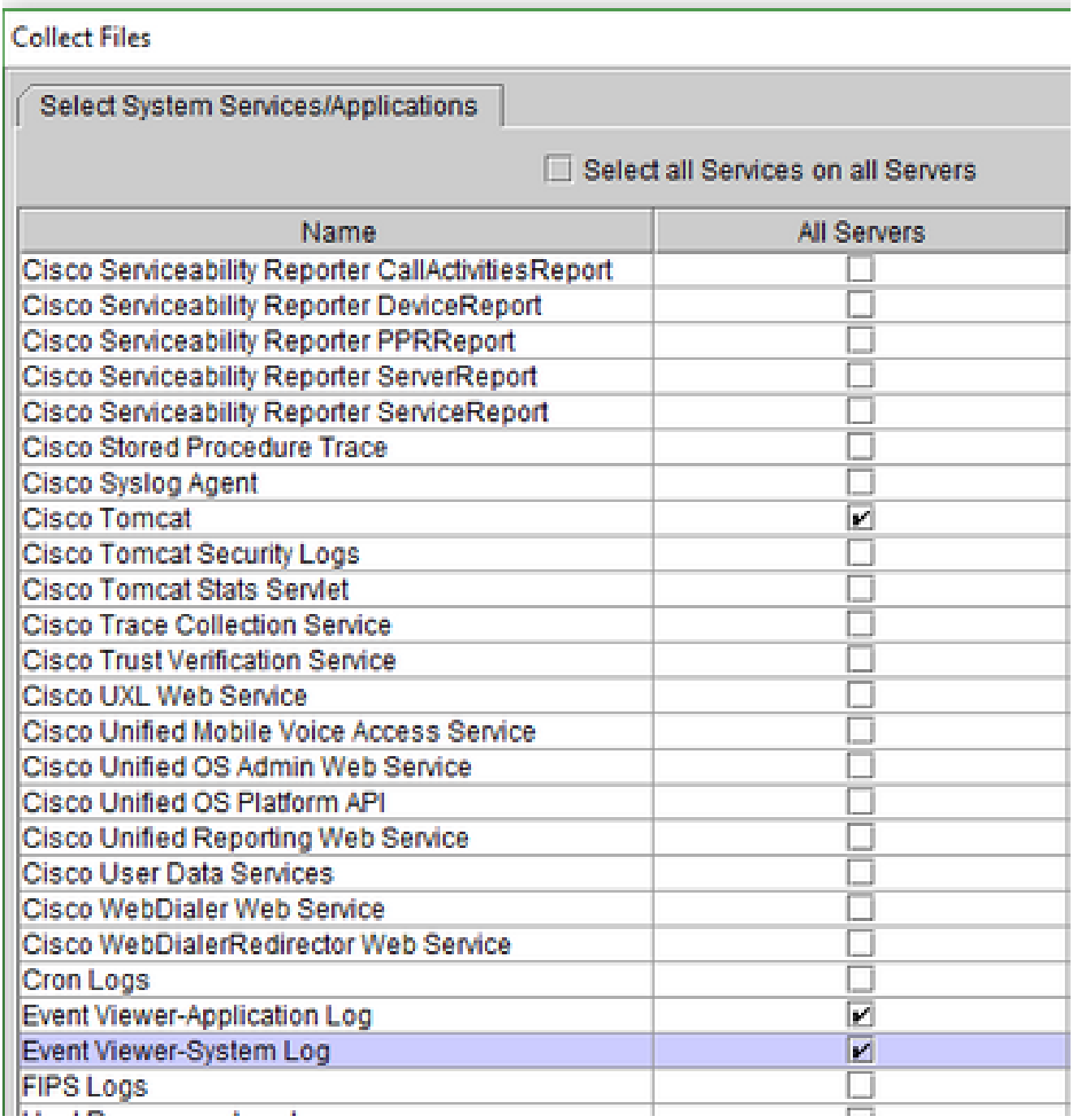
LDの場合：



IDSの場合



Platformサービスの場合は、一般にTomcatとイベントビューアのログを選択することをお勧めします。

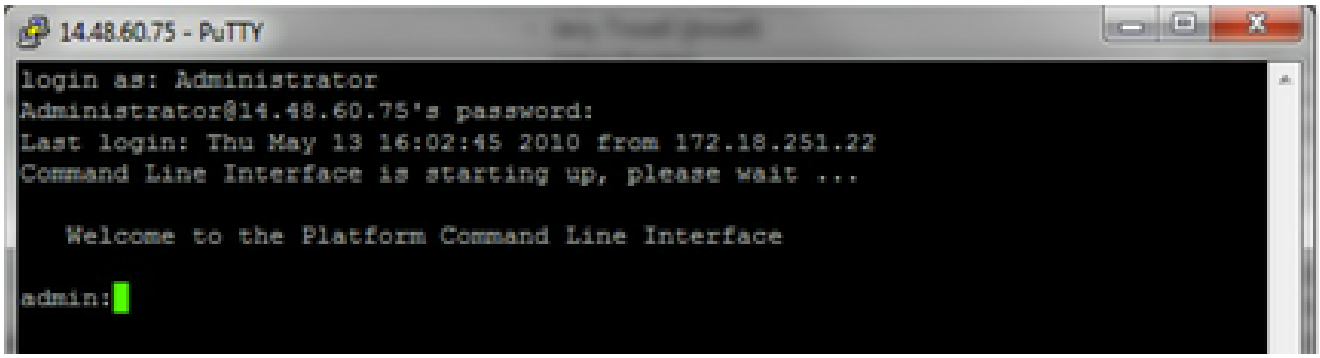


6. ログを表示するには、宛先フォルダと一緒に日付と時刻を選択saveします。

VoSでのパケットキャプチャ(Finesse、CUIC、VVB)

1. キャプチャの開始

   キャプチャを開始するには、プラットフォーム管理者アカウントで認証するVOSサーバへのSSHセッションを確立します。

2. 

1a.コマンド構文

コマンドは次utils network captureのとおりです。構文は次のとおりです。

<#root>

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

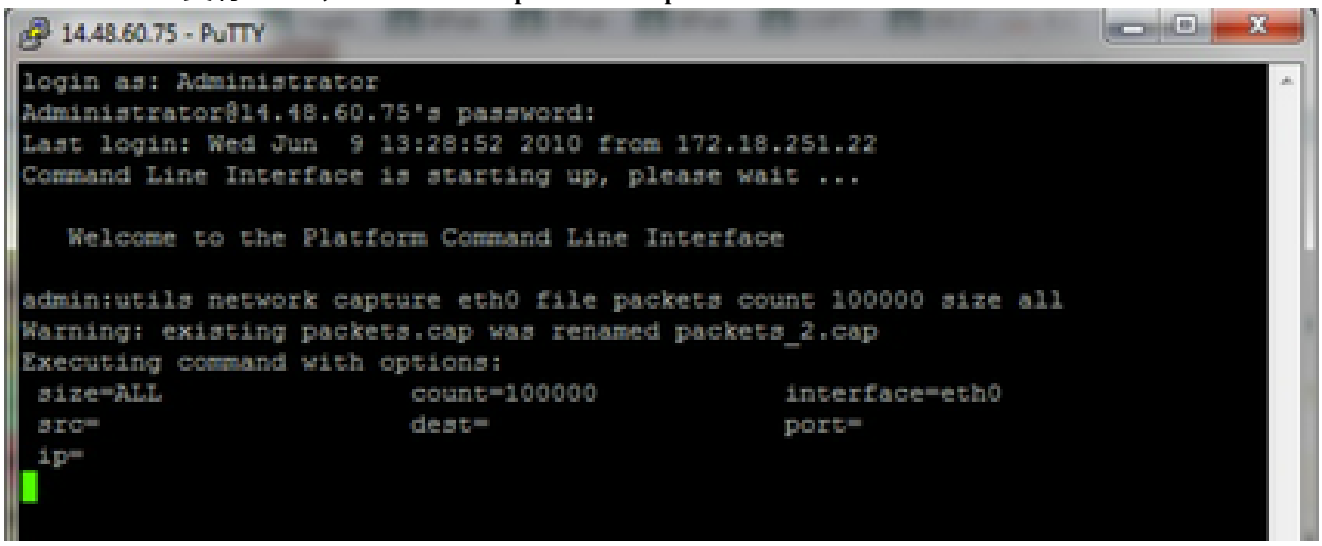
Note: The file is saved in platform/cli/fname.cap

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.すべてのトラフィックのキャプチャ

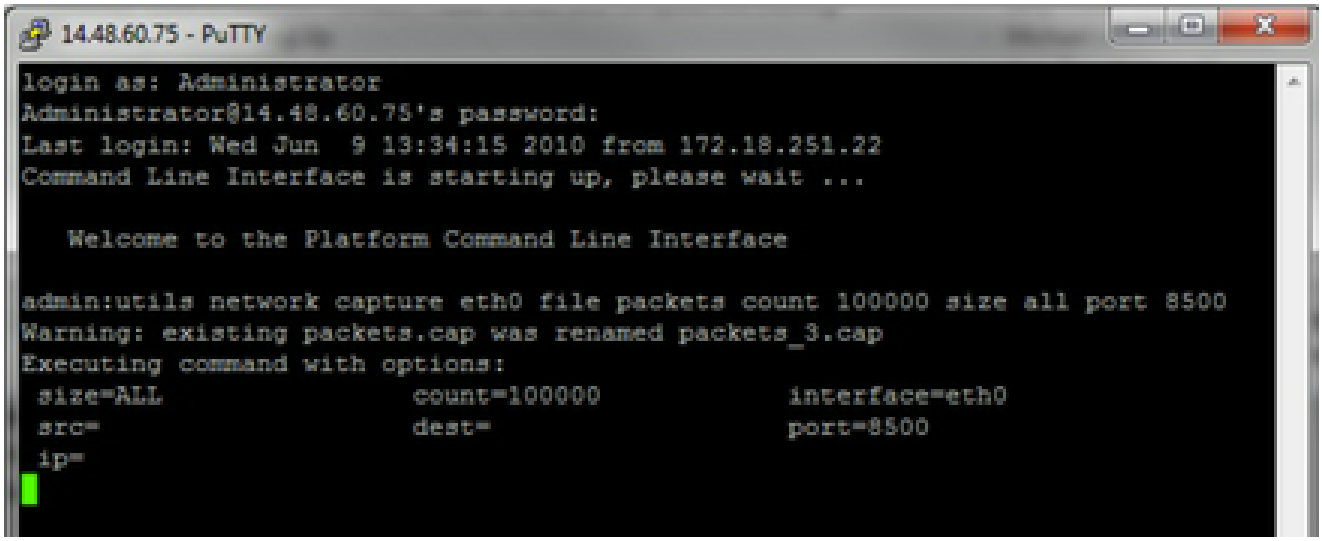
一般的なキャプチャでは、packets.capという名前のキャプチャファイルに、すべてのサイズのすべてのパケットとすべてのアドレスのパケットを収集できます。 これを行うには、admin CLIで実行します **utils network capture eth0 file packets count 100000 size all**



1c.ポート番号に基づくキャプチャ

Cluster Managerの通信の問題をトラブルシューティングするには、ポートオプションを使用して、特定のポート(8500)に基づいてキャプチャすることを推奨します。

各ポートで通信を必要とするサービスの詳細については、該当するバージョンの各コンポーネントの『TCPおよびUDPポートの使用ガイド』を参照してください。

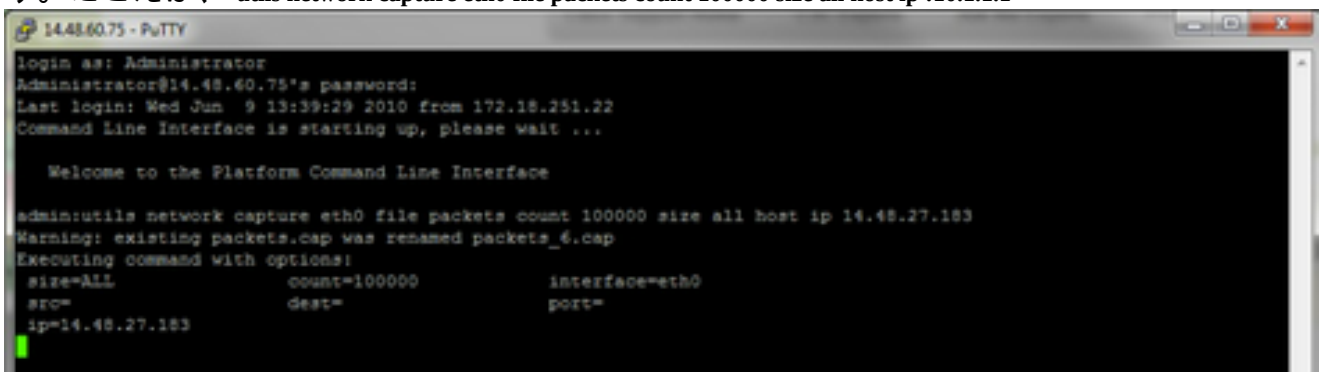


1d。ホストに基づくキャプチャ

VOSおよび特定のホストに関する問題をトラブルシューティングするには、「host」オプションを使用して、特定のホストとの間で送受信されるトラフィックをフィルタリングする必

要があります。

特定のホストを除外する必要がある場合もあります。この場合は、IPの前に「!」を付けます。たとえば、 **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

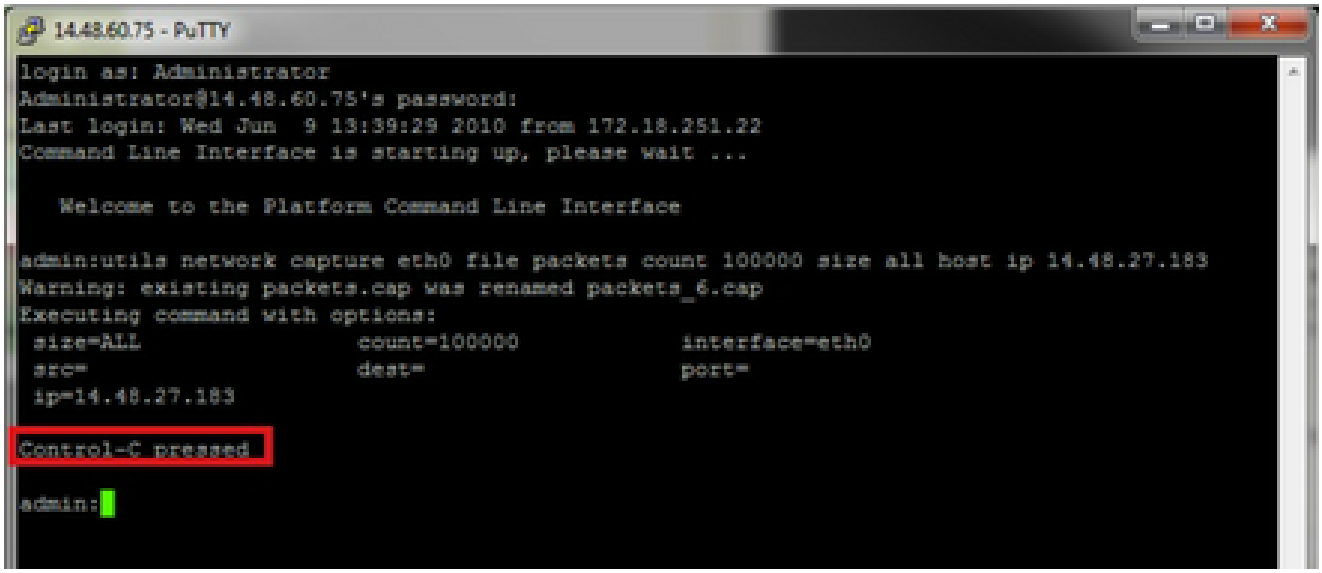


3. 問題の症状を再現する

   必要なパケットがキャプチャに含まれるように、問題の症状または状態を再現するためにキャプチャが開始されている間。問題が断続的に発生する場合は、キャプチャを長時間実行する必要があります。キャプチャが終了した場合、バッファがいっぱいになったことが原因です。キャプチャを再開すると、以前のキャプチャの名前が自動的に変更され、以前のキャプチャが失われなくなります。キャプチャが長期間必要な場合は、スイッチでモニタセッションを使用して、ネットワークレベルでキャプチャします。

4. キャプチャの停止

   キャプチャを停止するには、Controlキーを押したままキーボードのCキーを押します。これにより、キャプチャプロセスが終了し、キャプチャダンプに新しいパケットが追加されなくなります。

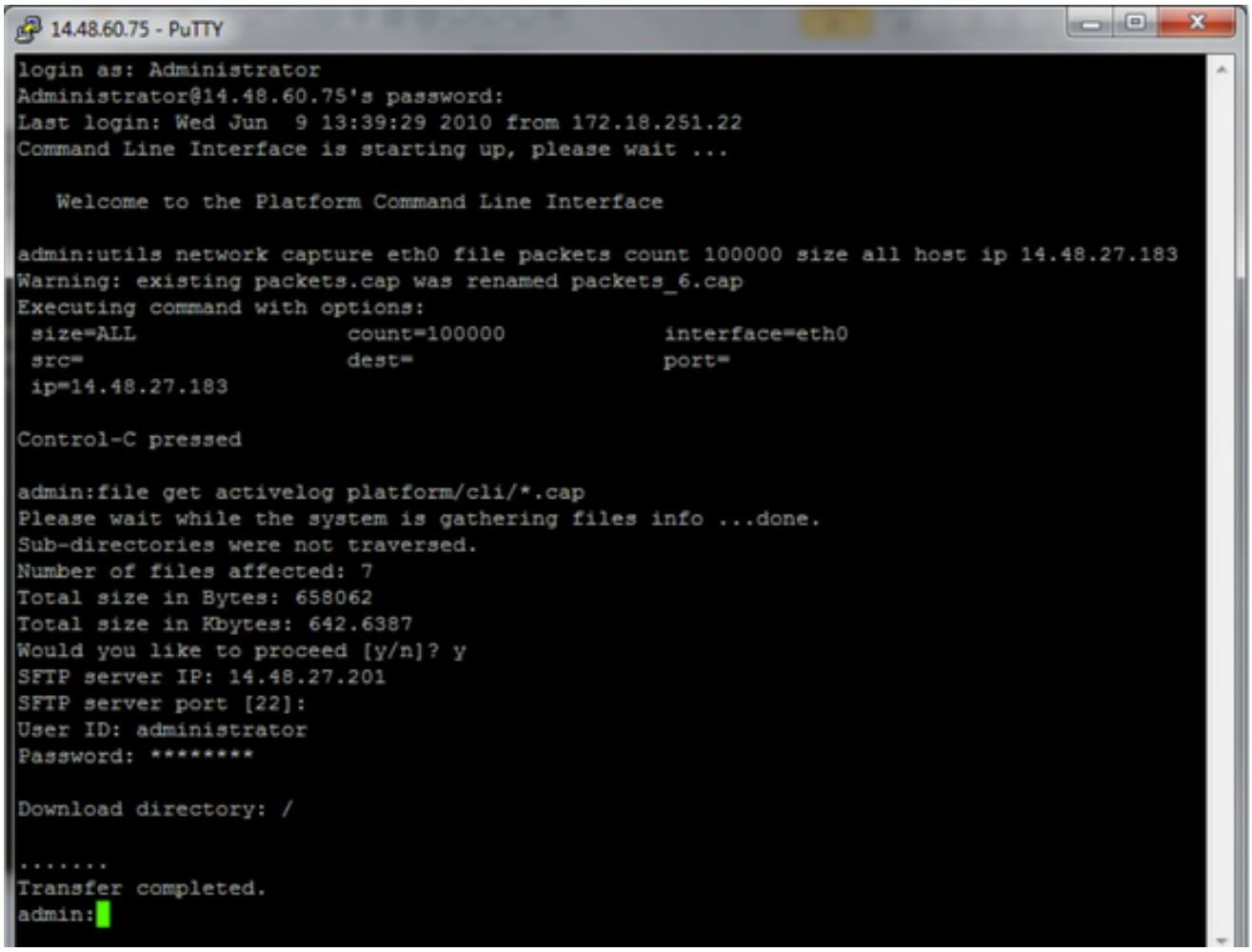
5. 

   これが完了すると、サーバの「activelog platform/cli/」にキャプチャファイルが保存されます

6. サーバからキャプチャを収集します
   キャプチャファイルは、サーバの「activelog platform/cli/」の場所に保存されます。CLIを使

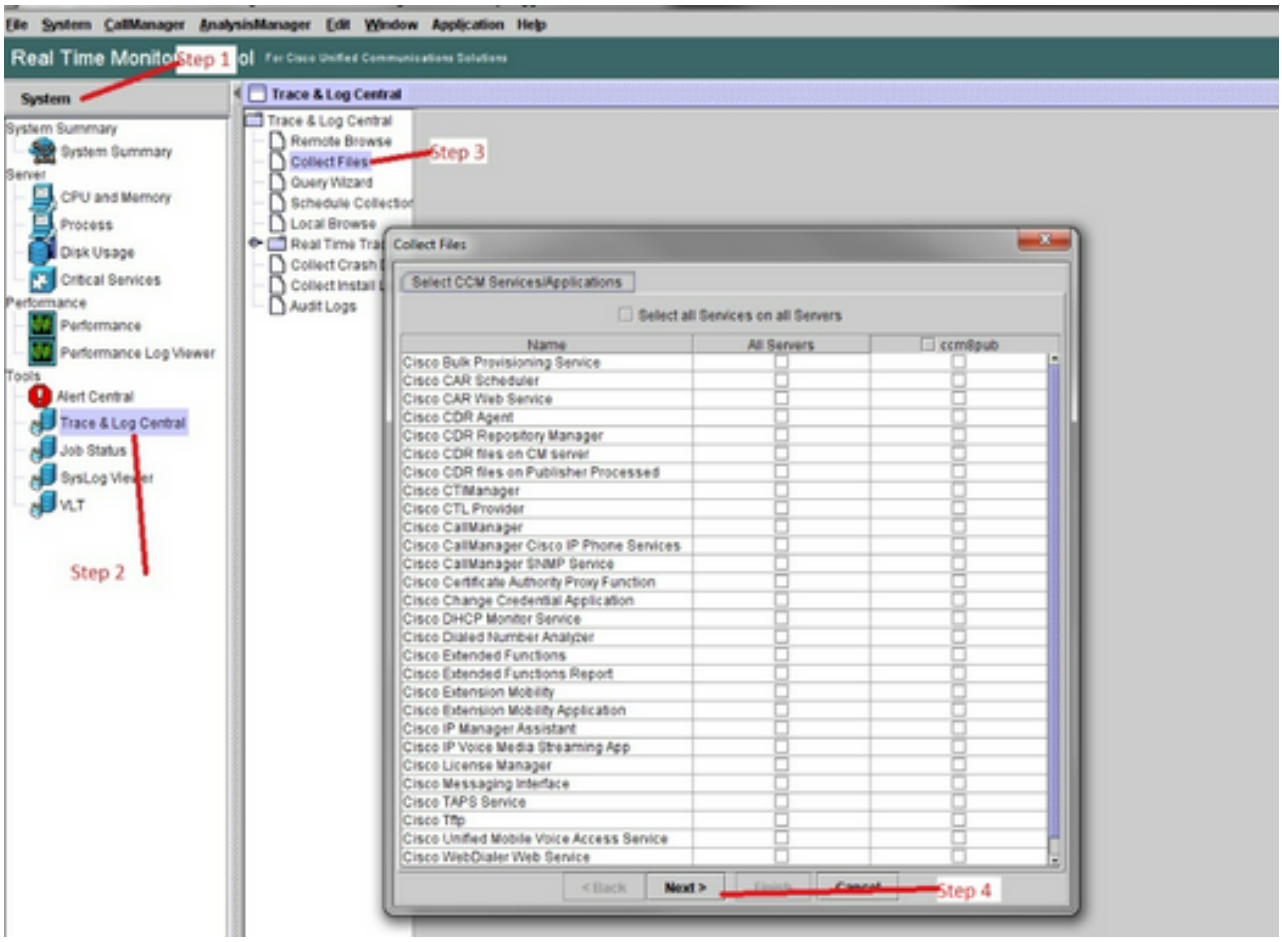
用して、SFTPサーバまたはRTMTを使用するローカルPCにファイルを転送できます。

4a.CLIを使用したSFTPサーバへのキャプチャファイルの転送
コマンドを使用**file get activelog platform/cli/packets.cap**して、SFTPサーバにpackets.capファイルを収集します。
または、サーバに保存されているすべての.capファイルを収集するには、「file get activelog platform/cli/*.cap」を使用します
最後に、SFTPサーバのIP/FQDN、ポート、ユーザ名、パスワード、およびディレクトリ情報を入力します。

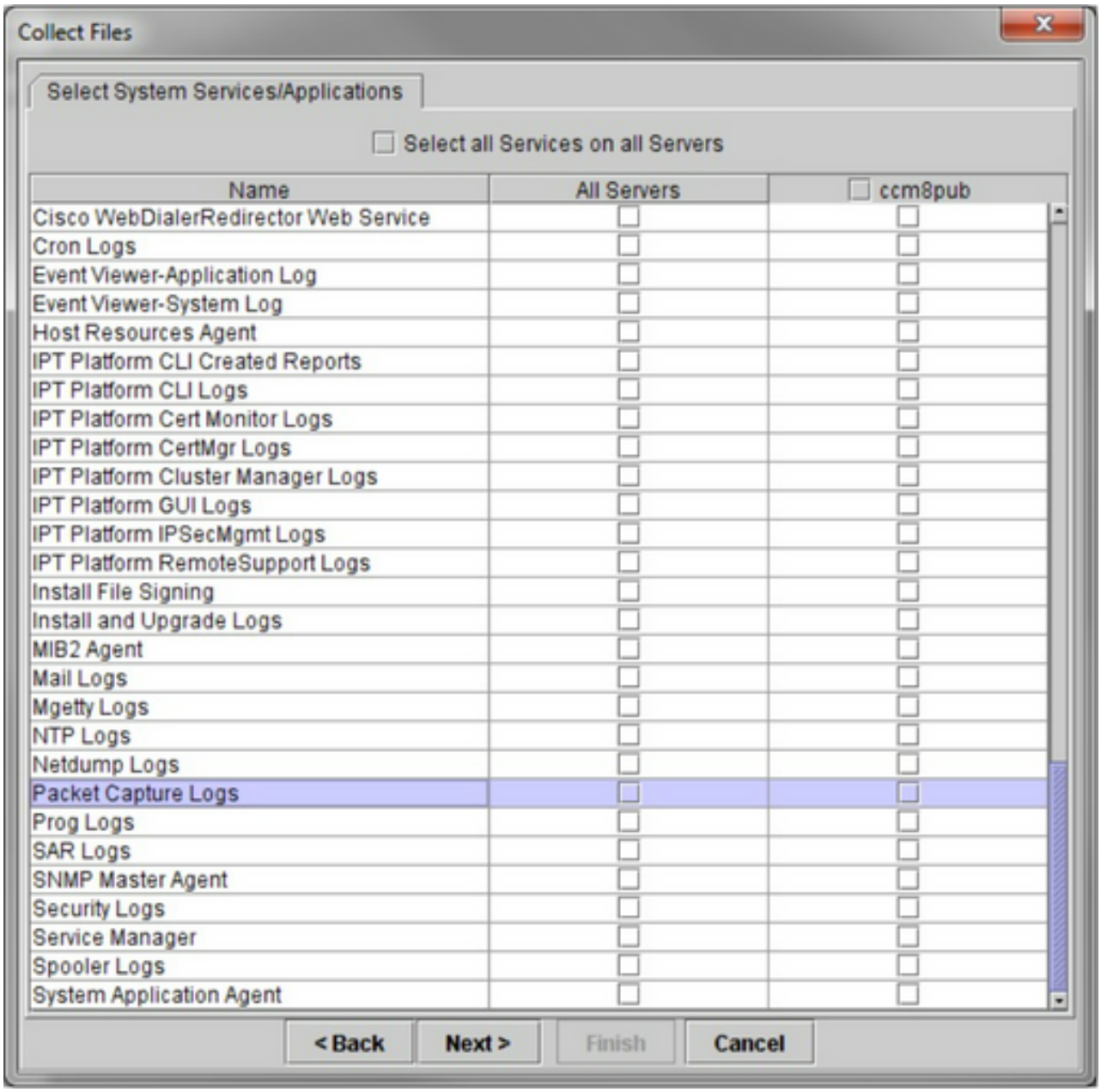


CLIは、SFTPサーバへのファイル転送の成功または失敗を示します。

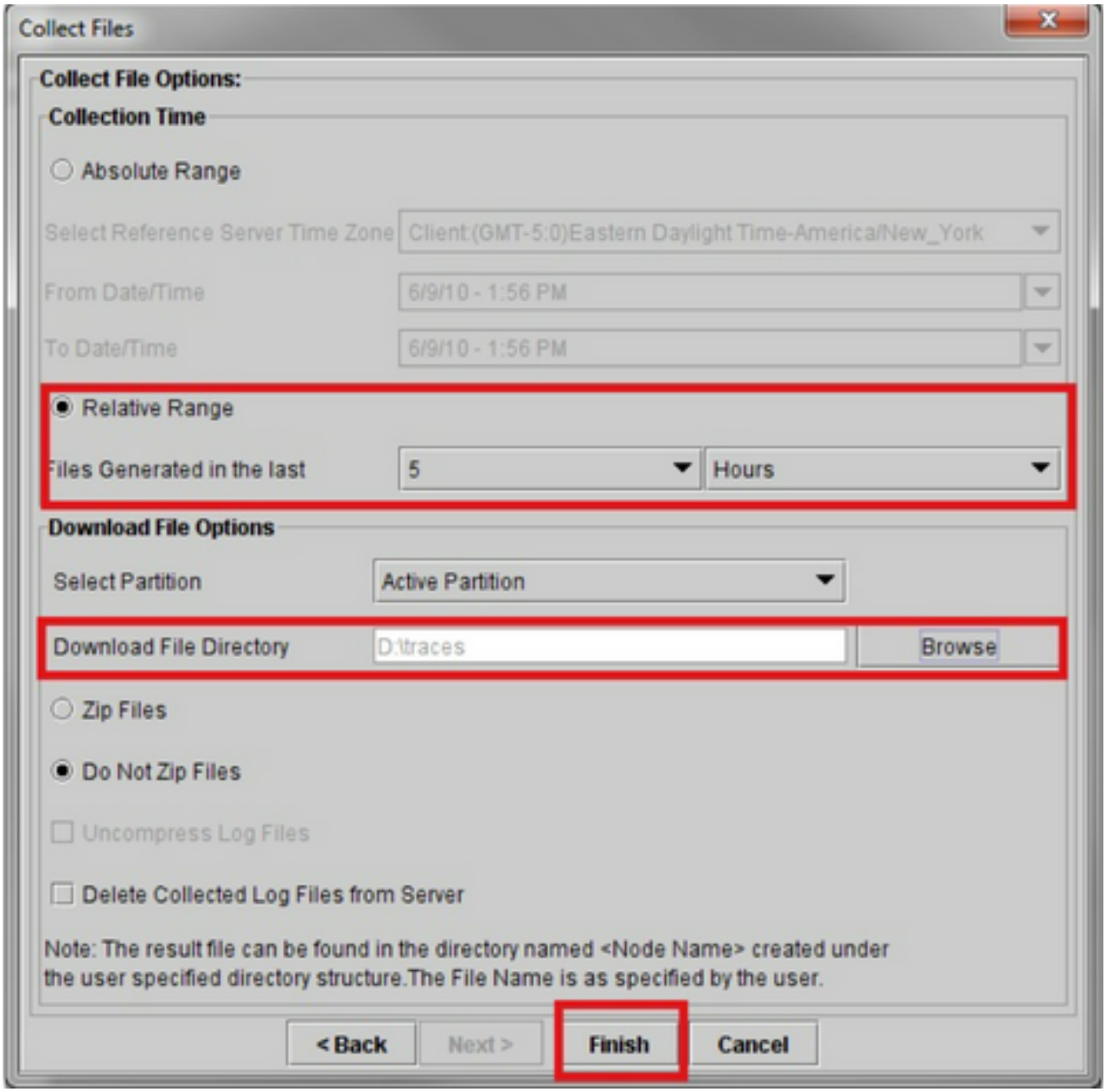
4b.RTMTを使用して、キャプチャファイルをローカルPCに転送します。
RTMTを起動します。ローカルPCにインストールされていない場合は、VOS Administrationページから適切なバージョンをインストールし、Applications->Pluginsメニューに移動します。
System、Trace & Log Centralの順にクリックし、Collect Filesをダブルクリックします。 最初のメニューでNextをクリックします。



2番目のメニューで、キャプチャが実行されたサーバのパケットキャプチャログのチェックボックスを選択し、Nextをクリックします。



最後の画面で、キャプチャが実行された時間範囲と、ローカルPC上のダウンロードディレクトリを選択します。



RTMTはこのウィンドウを閉じ、ファイルの収集に進み、指定された場所のローカルPCにファイルを保存します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。