

Cisco Unified SIP Proxy (CUSP) でのトレースログの有効化と収集

内容

[概要](#)

[トレースログの有効化](#)

[GUI を使用する場合](#)

[CLI を使用する場合](#)

[トレースログの収集](#)

[GUI を使用する場合](#)

[CLI を使用する場合](#)

[PFS \(パブリック・ ファイル・ システム \) から](#)

[SIPメッセージロギング](#)

[ログストレージ情報](#)

[CUSP 9.0以降](#)

[9.0より前のCUSPバージョン](#)

[CUSPバージョン10.2.1のログ収集](#)

[関連情報](#)

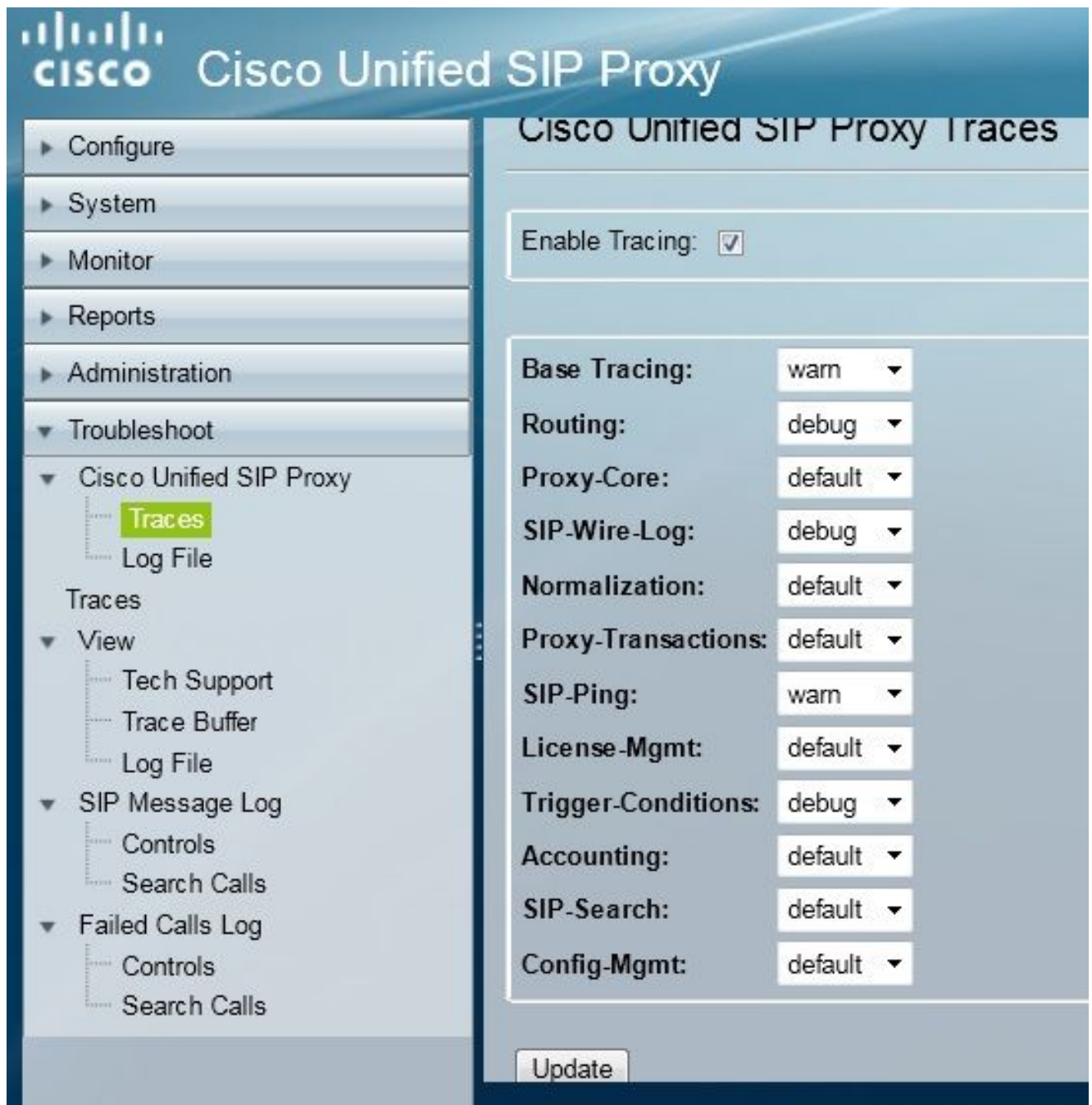
概要

このドキュメントでは、Cisco Unified SIP Proxy (CUSP) でトレース ログを有効化および収集するために使用できるさまざまなオプションについて説明します。トレースの有効化と収集は、GUI または CLI のいずれからでも実行できます。このドキュメントでは、それぞれの手順について詳しく説明します。

トレースログの有効化

GUI を使用する場合

1. CUSP GUI(<http://<CUSPモジュールのIPアドレス>/>)にログインします。
2. [Troubleshoot] < [Traces] に移動します。



3. [Enable Tracing] ボックスをオンにし、問題のトラブルシューティングに必要なコンポーネントを選択して、レベルをデバッグに設定します。
4. 必要な変更を行った後、[Update] をクリックします。

CLI を使用する場合

1. CUSPモジュールにアクセスし、CUSPモードに移行します。

```
Router#service-module sM 2/0 session
Trying 10.106.122.8, 2131 ... Open
CUSP# cusp
CUSP(cusp)#
```

2. トレースを有効にするには、**trace enable**コマンドを実行します。

```
CUSP(cusp)# trace enable
```

3. 必要なCUSPコンポーネントを選択し、トレースレベルをdebugに設定します。

```
MyCUSP-9(cusp)# trace level debug component ?
routing          Routing component
proxy-core       Proxy Core Component
sip-wire-log     SIP Wire Log Component
normalization    Normalization Component
proxy-transactions Proxy Transaction Layer Component
sip-ping         Servergroup SIP Ping Component
license-mgmt     License Management Component
trigger-conditions Trigger Conditions Component
accounting       Accounting Component
sip-search       SIP Search/Forking Component
config-mgmt      Configuration Management Component
```

4. 複数のコンポーネントのデバッグを有効にするには、前のコマンドを繰り返す必要があります。
5. 現在のトレース設定は、`show trace options`コマンドで表示できます。

```
MyCUSP-9(cusp)# show trace options
Trace is enabled.

Category                                     Level
root                                         warn
sip-wire-log                                 debug
sip-ping                                     warn
MyCUSP-9(cusp)#
```

トレースログの収集

GUIを使用する場合

1. CUSP GUIにログインします。
2. [Troubleshoot] > [Log File] に移動します。これにより、収集されたログが表示されます。ファイルを表示またはダウンロードできます。



注:CUSPバージョン8.5(5)以降では、GUIからログバッファをクリアするオプションが提供されています。CUSPのバージョンが8.5(5)より前の場合は、CLIを使用してログを手動でクリアする必要があります。

3. CLIでログをクリアするには、次のコマンドを入力します。

```
CUSP(cusp)# clear trace log
```

CLI を使用する場合

1. ログの内容を表示するには、次のコマンドを使用します。

```
MyCUSP-9(cusp)# show trace log ?
tail          Tail the log
<1-100000>    Dump specified number of lines from end of log
<cr>
|            Pipe output to another command
```

2. Ctrl+Cを押して、スクロールを中断します。
3. show trace log | pコマンドを発行して、トレース出力をページごとに表示します。

PFS (パブリック・ファイル・システム) から

トレースログを収集する別の方法があります。これは、CUSPが実行されているファイルシステムであるPFSから取得されます。PFSはFTPを使用してアクセスできます。

1. ユーザ名を作成し、このユーザにPFS権限を割り当てます。

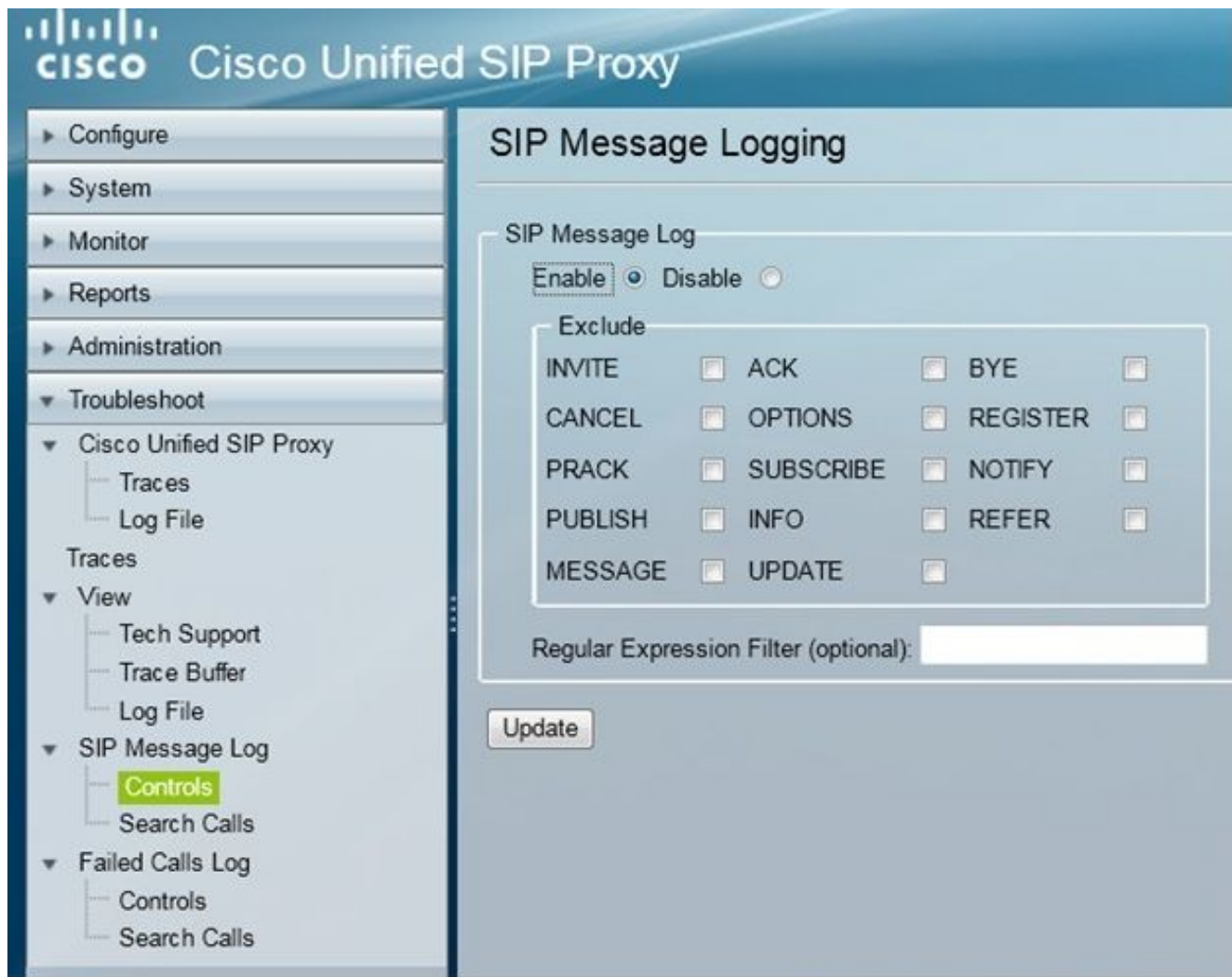
```
MyCUSP-9# conf t
Enter configuration commands, one per line. End with CNTL/Z.
MyCUSP-9(config)# username cisco create
MyCUSP-9(config)# exit
MyCUSP-9# username cisco password cisco
MyCUSP-9# username cisco group pfs-privusers
MyCUSP-9#
```

2. 前の手順で定義したクレデンシャルを使用して、このURLにアクセスします。トレースログを含む.logファイルをダウンロードできます。ftp://

SIPメッセージロギング

前のセクションで説明したトレースログとは別に、Session Initiation Protocol(SIP)メッセージログもCUSPで使用できます。このログには、CUSPで送受信されるSIPメッセージのみが表示されます。GUIからSIPメッセージログを有効にできます。

1. [Troubleshoot] > [SIP Message Logs] > [Controls] に移動します。



2. SIPメッセージログを表示するには、[Troubleshoot] > [SIP Message Logs] > [Search Calls] に移動します。

注：ルートテーブルや正規化など、CUSPによるSIP方式の処理方法を表示するには、トレースログが必要です。

ログストレージ情報

CUSP 9.0以降

CUSPバージョン9 (仮想CUSP) 以降では、ログバッファサイズを5 GBまで増やすことができます。このバージョンでは、ログとログファイルの数を保存するためにディスク領域をプロビジョニングできます。

ログサイズを5 GBに、ファイルカウントを500に設定する設定を次に示します。

```

MyCUSP-9# cusp
MyCUSP-9(cusp)# trace logsize 5000 filecount 500
MyCUSP-9(cusp)#
MyCUSP-9(cusp)# show trace size

Configured Log Size: 5000
Configured file Count: 500

Default Log Size is 200MB and File Count is 20

MyCUSP-9(cusp)# █

```

シスコでは、パフォーマンスを向上させるために、各ログファイルを10 MBにすることを推奨しています。

9.0より前のCUSPバージョン

古いバージョンのCUSPでは、ログバッファサイズは200 MBに設定されています。CUSP 8.5.8以降では、trace logsizeコマンドを使用して最大5 Gbまで増やすことができます。

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel8_5/cli_commands/cli_commands/cusp_exec_cmds.html#63802

CUSPバージョン10.2.1のログ収集

バージョン10.2.1では、ログローテーションにソフトウェアの制限があります。CUSPバージョン10.2.1でバッファがいっぱいになると、新しいログは書き込まれません。Cisco Bug ID [CSCvs47162](https://www.cisco.com/c/en/us/bug/CSCvs47162) この不具合修正については、『10.2.1v1リリースノート』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel10_2/releasenotes/cusprn102.html#Cisco_Concept.dita_4e7c4d6b-10ed-4bcf-901c-019500ba20c7

この問題は、10.2.1 v1以降のパッチで修正されています。

v1以降のバージョンへのアップグレードが完了したら、最新のログを収集するためにCLIまたはGUIのみを使用します。これは、SFTP (PFSユーザ) が最新のログに反映されないためです。

CLIによるログの収集 :

1. コマンド「show logs」を使用して、最新のログファイルを表示します

```

se-10-65-105-44# show logs

```

SIZE	LAST_MODIFIED_TIME	NAME
26552	Wed Aug 17 01:19:01 IST 2022	atrace.log
0	Tue Mar 22 15:55:16 IST 2022	pmessages.log
0	Mon Mar 07 11:19:04 IST 2022	yum.log
100618	Wed Aug 17 01:16:46 IST 2022	dmesg
14741	Wed Aug 17 01:16:55 IST 2022	boot.log
2078001	Mon Sep 05 13:32:34 IST 2022	messages.log

2. ファイルをSFTPサーバにコピーする

```
CUSP# copy log <logfilefilename> url sftp://<username>:<password>@<ftphost>/path/to/filename
```

GUIによるログの収集 :

CUSP GUI:[Troubleshoot] > [Cisco Unified SIP Proxy] > [Log File] > [Download Log File]

ユーザが新しいvCUSPをインストールし、バッファがいっぱいになる前にバージョン10.2.1v1以降にアップグレードすると、ログ収集メカニズムを使用してログを収集でき、問題が発生することはありません。

関連情報

- [CUSP 設定例](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)