Aktivieren und Erfassen von Ablaufverfolgungsprotokollen im Cisco Unified SIP-Proxy (CUSP)

Inhalt

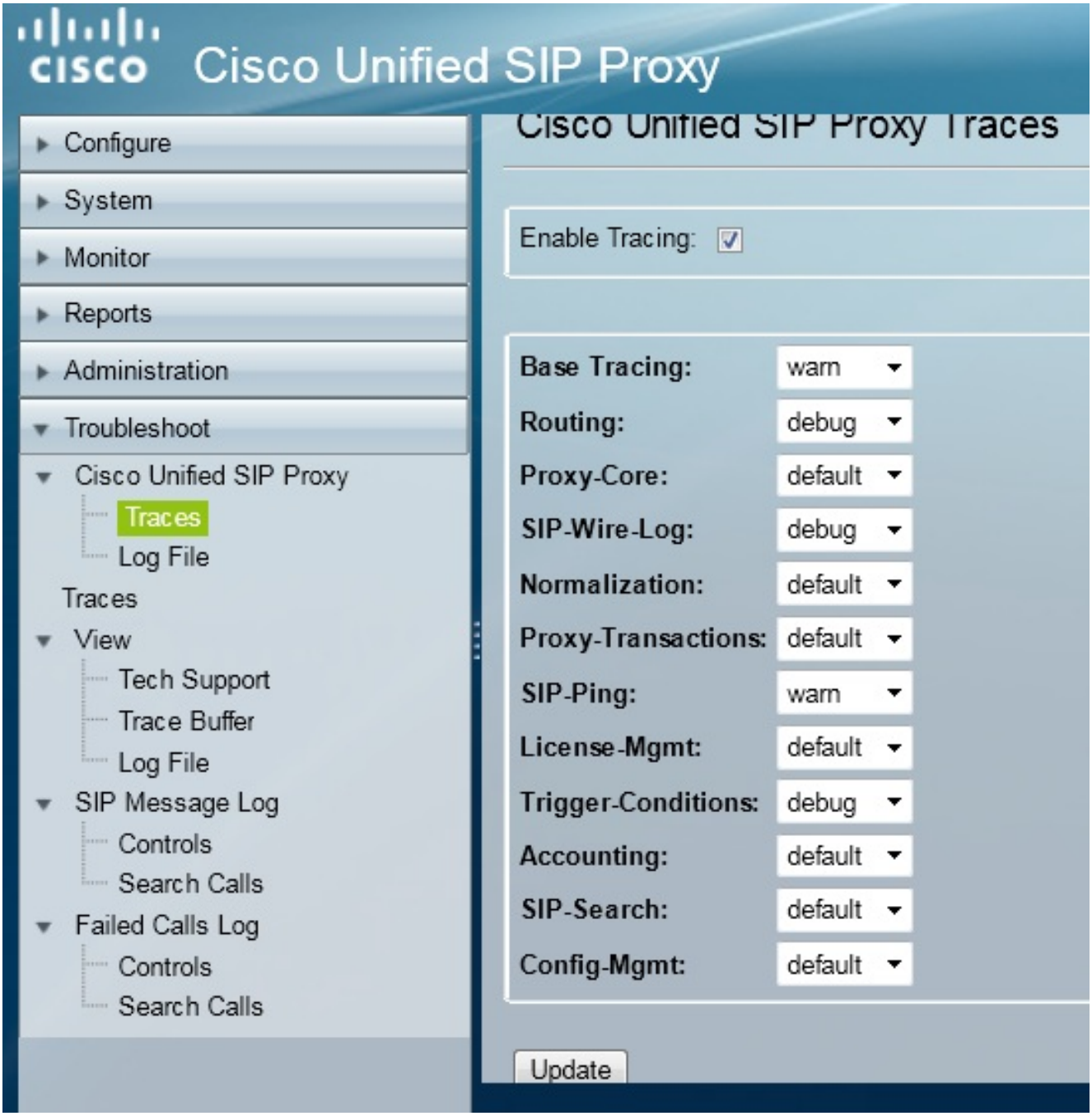
Einführung

In diesem Dokument werden die verschiedenen in Cisco Unified SIP Proxy (CUSP) verfügbaren Optionen zum Aktivieren und Erfassen von Ablaufverfolgungsprotokollen beschrieben. Ablaufverfolgungen können entweder über die GUI oder die CLI aktiviert und erfasst werden. In diesem Dokument werden die einzelnen Schritte ausführlich erläutert.

Trace-Protokolle aktivieren

Über die Benutzeroberfläche

1. Melden Sie sich bei der CUSP-GUI an (http://<IP-Adresse des CUSP-Moduls>/).
2. Navigieren Sie zu **Fehlerbehebung < Ablaufverfolgungen**.



3. Aktivieren Sie das Kontrollkästchen **Ablaufverfolgung aktivieren**, und wählen Sie dann die erforderliche(n) Komponente(n) aus, um das Problem zu beheben, und legen Sie die Debugstufe fest.
4. Klicken Sie nach Durchführung der erforderlichen Änderungen auf **Aktualisieren**.

Über die CLI

1. Öffnen Sie das CUSP-Modul, und wechseln Sie in den CUSP-Modus.

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

2. Um die Ablaufverfolgung zu aktivieren, führen Sie den Befehl **trace enable aus**:

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

3. Wählen Sie die erforderliche CUSP-Komponente aus, und legen Sie die Ablaufverfolgungsebene zum Debuggen fest.

```
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. Sie müssen den vorherigen Befehl wiederholen, um das Debuggen für mehrere Komponenten zu aktivieren.

5. Sie können die aktuelle Ablaufverfolgungseinstellung mithilfe des Befehls **Ablaufverfolgungsoptionen anzeigen**.

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

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

Trace Log Collection

Über die Benutzeroberfläche

1. Melden Sie sich bei der CUSP-GUI an.

2. Navigieren Sie zu **Fehlerbehebung > Protokolldatei**. Es werden die gesammelten Protokolle angezeigt. Sie können die Datei entweder anzeigen oder herunterladen.

Hinweis: CUSP Version 8.5(5) und höher bieten die Option, den Protokollpuffer aus der GUI zu löschen. Wenn die CUSP-Version älter ist als Version 8.5(5), müssen die Protokolle manuell über die CLI gelöscht werden.

3. Um die Protokolle mit der CLI zu löschen, geben Sie den folgenden Befehl ein:

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

Über die CLI

1. Verwenden Sie diesen Befehl, um den Inhalt des Protokolls anzuzeigen:

```
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. Drücken Sie **STRG+C**, um das Scrollen zu unterbrechen.
3. Verwenden des **Ablaufverfolgungsprotokolls anzeigen | p-Befehl**, um die Ablaufverfolgungsausgabe seitenweise anzuzeigen.

Über das öffentliche Dateisystem (PFS)

Es gibt eine andere Möglichkeit, die Ablaufverfolgungsprotokolle zu sammeln. Dies stammt vom PFS, dem Dateisystem, auf dem CUSP ausgeführt wird. Der Zugriff auf PFS erfolgt über FTP.

1. Erstellen Sie einen Benutzernamen, und weisen Sie diesem Benutzer die PFS-Berechtigung zu.

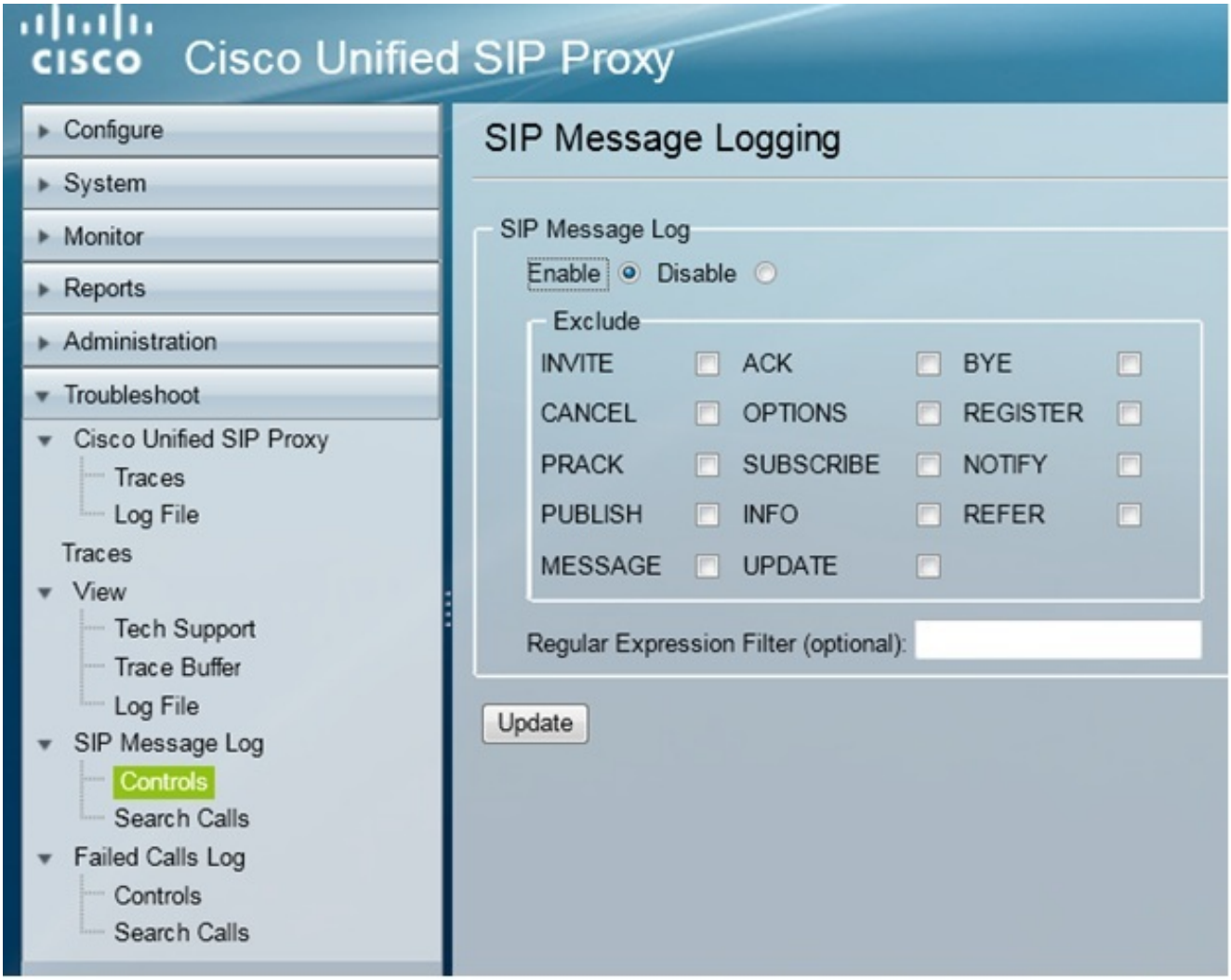
```
MyCUSP-9# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MyCUSP-9(config)# username cisco create
MyCUSP-9(config)# exit
MyCUSP-9# username cisco password cisco
MyCUSP-9# username cisco group pfs-privusers
MyCUSP-9#
```

2. Greifen Sie mit den im vorherigen Schritt definierten Anmeldeinformationen auf diese URL zu. Sie können **.log-**Dateien herunterladen, die das Ablaufverfolgungsprotokoll enthalten. ftp://<IP von CUSP>/cusp/log/trace/

SIP-Nachrichtenprotokollierung

Neben den in den vorherigen Abschnitten erwähnten Ablaufverfolgungsprotokollen sind auch SIP-Nachrichtenprotokolle (Session Initiation Protocol) in CUSP verfügbar. Dieses Protokoll zeigt nur die SIP-Meldungen an, die beim CUSP eingehen und von dort ausgehen. Sie können SIP-Nachrichtenprotokolle über die Benutzeroberfläche aktivieren.

1. Navigieren Sie zu **Problembehandlung > SIP-Nachrichtenprotokolle > Steuerelemente**.



2. Um die SIP-Nachrichtenprotokolle anzuzeigen, navigieren Sie zu **Troubleshoot > SIP Message Logs > Search Calls**.

   Hinweis: Um anzuzeigen, wie CUSP die SIP-Methoden verarbeitet, z. B. die Routentabellen und die Normalisierung, sind Ablaufverfolgungsprotokolle erforderlich.

Protokollspeicherinformationen

CUSP 9.0 und höher

In CUSP Version 9 (Virtual CUSP) und höher kann die Größe des Protokollpuffers auf bis zu 5 GB erhöht werden. In dieser Version können Sie Speicherplatz bereitstellen, um Protokolle und die Anzahl der Protokolldateien zu speichern.

Die folgende Konfiguration legt die Protokollgröße auf 5 GB und die Dateianzahl auf 500 fest.

```
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)#
```

Cisco empfiehlt, dass jede Protokolldatei 10 MB groß sein sollte, um die Leistung zu verbessern.

CUSP-Versionen vor 9.0

In älteren Versionen von CUSP ist die Größe des Protokollpuffers auf 200 MB festgelegt, und es ist nicht vorgesehen, die Puffergröße des Ablaufverfolgungsprotokolls und die Anzahl der Dateien zu ändern.

Zugehörige Informationen

- CUSP-Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems