Netzwerkmitschnitt

SIP-Pakete aufzeichnen (erweitert)

Datenschutzhinweis:
SIP-Pakete können personenbezogene und andere sensible Daten enthalten. Stimmen Sie die Verwendung von SIP-Aufzeichnungen vorab mit dem zuständigen **Datenschutzbeauftragten** ab. Senden Sie uns entsprechende Dateien **nie unaufgefordert**. Der UCware Support teilt Ihnen mit, welche Maßnahmen vor bzw. während der Aufzeichnung erforderlich sind.

In diesem Artikel erfahren Sie, wie Sie SIP-Pakete gezielt für einzelne Endpunkte und/oder anhand spezieller Kriterien aufzeichnen können. Ein solcher Mitschnitt (SIP-Trace) ist insbesondere zur Diagnose und Behebung von Verbindungsproblemen erforderlich.

Dabei haben Sie zwei Möglichkeiten:

- über sngrep:

Diese Methode erfasst nur unverschlüsselte Pakete. Das gleichnamige Werkzeug muss aus den Ubuntu-Paketquellen nachinstalliert werden.

- direkt im Asterisk:

Diese Methode erfasst auch verschlüsselte Pakete. Das erforderliche Modul **res_pjsip_logger** ist Bestandteil der UCware-Installation.

Hinweis:
Alternativ können Sie im Admin-Client einen vollständigen Mitschnitt **aller** ein- und ausgehenden SIP-Pakete erstellen. Lesen Sie dazu den Artikel SIP-Pakete aufzeichnen (Admin-Client).

SIP-Trace über sngrep

Hinweis:
Dieser Abschnitt beschränkt sich auf die Darstellung grundlegender Funktionen. Weitere Hilfe zur Benutzung erhalten Sie mit `F1` oder auf GitHub.

Installation

Um **sngrep** auf dem UCware Server bereitzustellen, gehen Sie wie folgt vor:

1. Greifen Sie per SSH auf den UCware Server zu.
2. Lesen Sie die Paketquellen neu ein:

```
sudo apt update
```

3. Installieren Sie das Paket **sngrep**:

```
sudo apt install sngrep
```

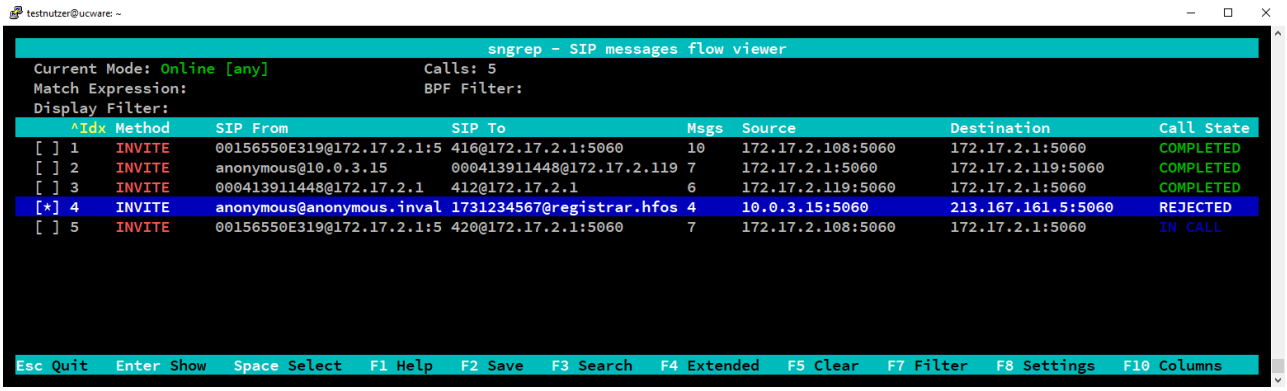
Verbindungsübersicht anzeigen

Um **sngrep** auszuführen, gehen Sie wie folgt vor:

1. Greifen Sie per SSH auf den UCware Server zu.
2. Starten Sie **sngrep**:

```
sudo sngrep -c
```

Die Option `-c` schränkt die folgende Verbindungsübersicht auf Anrufe ein:



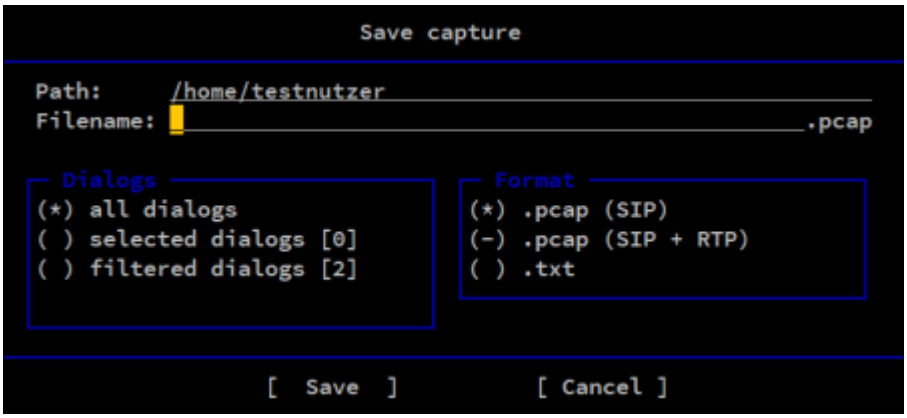
Alternativ können Sie `sngrep` mit den folgenden Optionen ausführen:

Option	Ergebnis
–leer–	Zeigt **alle** SIP-Verbindungen in der Übersicht.
`-d enp0s3`	Zeigt nur die Verbindungen über das angegeben Netzwerkinterface.
`-I /path/to/file.pcap`	Zeigt gespeicherte Verbindungsdetails aus der angegebenen Datei.

Verbindungsdetails speichern

Um Details zu einer oder mehreren Verbindungen zu speichern, gehen Sie wie folgt vor:

1. Wählen Sie in der Übersicht mit `↓` `↑` die gewünschten Einträge und markieren Sie diese mit `Leertaste`.
   Wenn Sie alle angezeigten Verbindungen speichern möchten, ist dieser Schritt nicht erforderlich.
2. Rufen Sie den **Speichern**-Dialog mit `F2` auf.



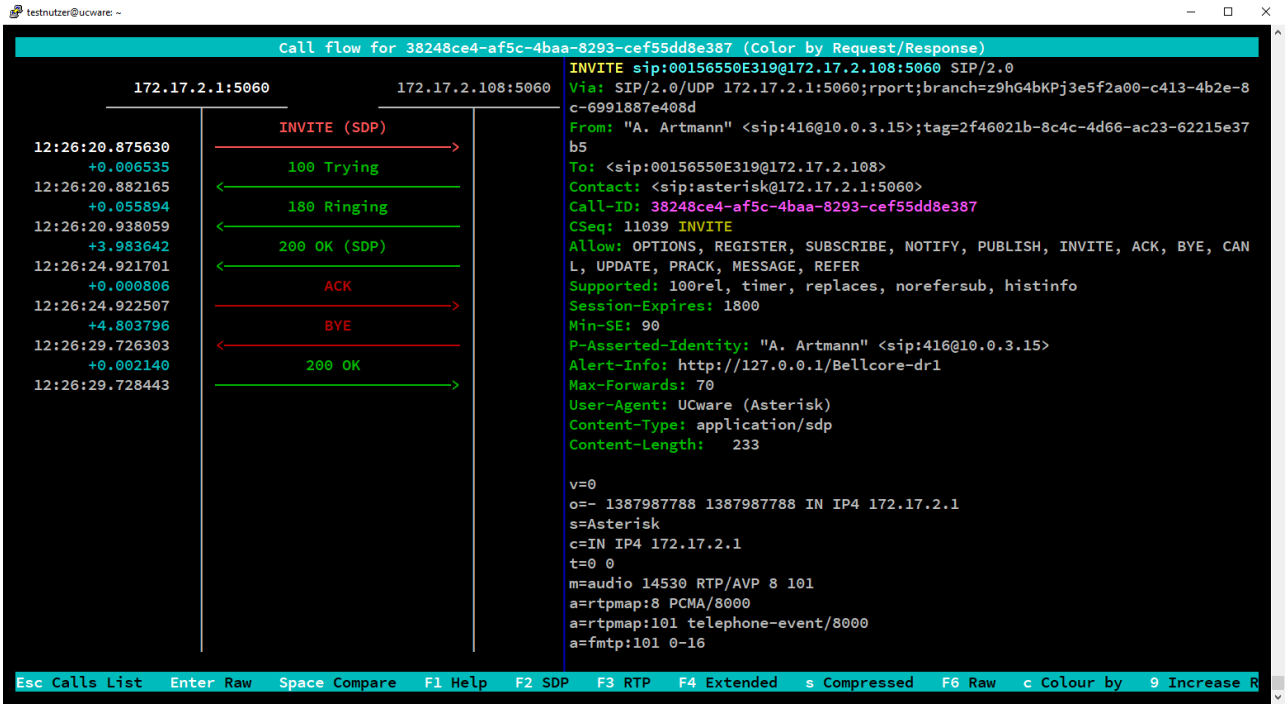
3. Wählen Sie unter **Dialogs** aus, ob **sngrep** alle oder nur bestimmte Verbindungen speichern soll.
4. Wenn der Support kein anderes Dateiformat anfordert, wählen Sie `.pcap (SIP)`.
5. Vervollständigen Sie alle weiteren Angaben und bestätigen Sie mit **Save**.

Datenschutzhinweis:
Löschen Sie nicht mehr benötigte SIP-Aufzeichnungen umgehend.

Verbindungsdetails anzeigen

Um Details zu einer oder mehreren Verbindungen anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Übersicht mit ↓ ↑ den gewünschten Eintrag und drücken Sie Enter.



2. Um Details zu einzelnen Paketen der Verbindung anzuzeigen wählen Sie diese mit ↓ ↑ aus.

SIP-Trace direkt im Asterisk

Verbindungsdetails anzeigen

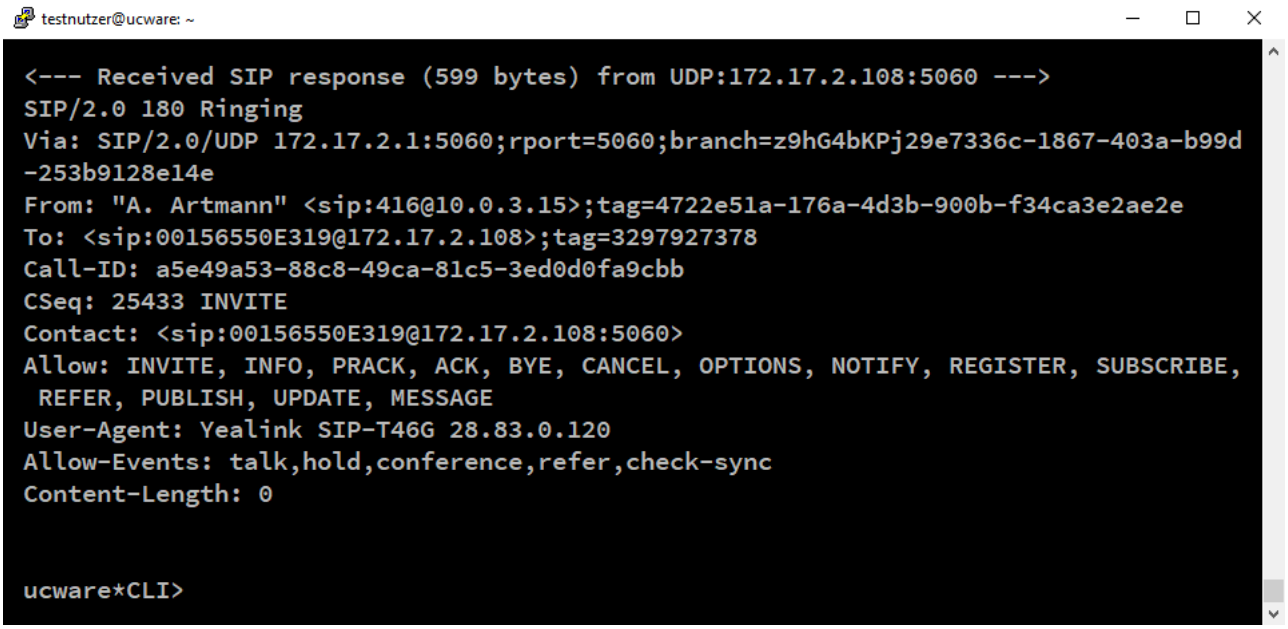
Um die Verbindungen von bzw. zu einem bestimmten Endgerät anzuzeigen, gehen Sie wie folgt vor:

1. Ermitteln Sie bei Bedarf unter **Provisionierung > Geräte** die IP-Adresse des gewünschten Endgeräts.
2. Greifen Sie per SSH auf den UCware Server zu.
3. Rufen Sie die Asterisk-Kommandozeile auf:

```
sudo asterik -r
```

4. Starten Sie das Logging für den gewünschten Endpunkt:

```
pjsip set logger host [IP-Adresse]
```



Alternativ können Sie auch die Verbindungen **aller** Endpunkte loggen:

```
pjsip set logger on
```

5. Um das Logging zu beenden, geben Sie den folgenden Befehl ein:

```
pjsip set logger off
```

Verbindungsdetails speichern

Um Details zu einer oder mehreren Verbindungen zu speichern, gehen Sie wie folgt vor:

1. Zeigen Sie die gewünschten Verbindungen wie oben beschrieben an.
2. Starten Sie das Logging in die gewünschte Datei:

```
pjsip set logger pcap /path/to/file.pcap
```

3. Finalisieren Sie die Datei, indem Sie das Logging beenden:

```
pjsip set logger off
```

Datenschutzhinweis:
Löschen Sie nicht mehr benötigte SIP-Aufzeichnungen umgehend.

From:
https://wiki.ucware.com/ - **UCware-Dokumentation**

Permanent link:
https://wiki.ucware.com/adhandbuch/system/sip_trace/erweitert

Last update: **17.01.2024 11:23**