

# Splunk ForwarderがSplunk Cloudにイベントを送信していません

## 適用性

Splunkクラウド

## 説明

SplunkフォワーダがSplunk Cloudにイベントを送信しなくなりました。これは、ユニバーサルフォワーダ、ヘビーフォワーダ、または中間フォワーディング層に影響を与える可能性があります。

splunkd.logに次のエラーが表示されます。

```
ERROR TcpOutputFd - Connection to host=1.22.122.222:9997 failed. sock_error = 104. SSL Error = No error
```

sock\_error = 104メッセージは、フォワーダがSplunk Cloud受信エンドポイントと通信しようとしたときに、TCP接続がリセットされたことを示します。

## 調査

影響を受けるフォワーダからSplunk Cloud入力エンドポイントへの基本的なネットワーク接続を確認します。

```
telnet inputs1.<stack_id>.splunkcloud.com 9997
```

telnet接続が成功すると、ポートが到達可能であることが確認されます。ただし、SSL/TLS接続

を完全に検証したり、中間ネットワークデバイスによってトラフィックがリセットされないことを確認したりすることはありません。

接続をさらに検証するには、影響を受けるフォワーダから次のコマンドのいずれかを実行します。

```
openssl s_client -connect inputs1.<stack_id>.splunkcloud.com:9997
```

または

```
$SPLUNK_HOME/bin/splunk cmd openssl s_client -connect inputs1.<stack_id>.splunkcloud.com
```

次の出力が返された場合は、接続がリセットされています。

```
CONNECTED(00000003)
write:errno=104
```

これにより、フォワーダは最初にTCP接続を確立できますが、SSL/TLSセッションが完了する前に接続が強制的に閉じられていることが確認できます。

また、影響を受けるフォワーダのフォワーディング設定 ( `outputs.conf` を含む ) をレビューし、フォワーダが正しい Splunk Cloud 受信エンドポイントおよびポートを使用していることを確認します。

## 解決方法

エラー104は「ECONNRESET」で、「Connection reset by peer」を意味します。これは、接続がTCPリセットパケットによって強制的に閉じられたことを示します。リセットは、宛先エンドポイントから送信される場合と、ファイアウォール、プロキシ、ロードバランサ、IDS/IPS、SSLインスペクションデバイス、ネットワークアプライアンスなどの中間ネットワークデバイスから送

信される場合があります。

影響を受けるフォワーダとSplunk Cloudの間の完全なネットワークパスを確認します。次の項目を確認します。

- Splunkクラウドの入力エンドポイントへの発信トラフィックは、ポート9997で許可されます。
- ファイアウォール、プロキシ、またはネットワークアプライアンスがTCPセッションをリセットしていません。
- SSLインスペクションがSplunkの転送接続を妨げることはありません。
- 最近のネットワーク、ファイアウォール、プロキシ、ルーティング、または証明書関連の変更が確認されます。
- Splunk Cloud Forwarderのアプリケーションと証明書は最新であり、正しく導入されています。
- 中間フォワーダはSplunk Cloudと通信でき、転送されたトラフィックをドロップまたはブロックしません。

ネットワーク、ファイアウォール、または証明書の設定を修正した後、必要に応じて該当するフォワーダを再起動するか、フォワーダが自動的に再接続できるようにします。次に、Splunk Cloudでイベントのインデックスが正常に作成されていることを確認します。

## 関連リンク

[Linux ARMおよびSplunk Cloud用ユニバーサルフォワーダ\(UFT\)の接続の問題 \( SSLエラー \)](#)

## 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。