

ユニバーサルフォワーダがSplunkインデクサにデータを転送していません

適用性

ユニバーサルフォワーダ

説明

\$SPLUNK_HOME/etc/system/local/outputs.confの誤設定により、Splunk Universal Forwarderが予期したとおりにデータを転送しません。

調査

ユニバーサルフォワーダの\$SPLUNK_HOME/var/log/splunk/splunkd.logに次のエラーメッセージが表示されます。

```
'09-06-2019 10:53:39.389 -0400 ERROR TcpOutputProc - LightWeightForwarder/UniversalForwa
```

解決方法

このエラーメッセージは、\$SPLUNK_HOME/etc/system/local/outputs.confファイルで次の設定を行うことで解決できます。

```
[tcpout]defaultGroup = <target_group>, <target_group>, ...
* A comma-separated list of one or more target group names, specified later in [tcpout:<
* The forwarder sends all data to the specified groups.
* If you don't want to forward data automatically, don't set this setting.
* Can be overridden by an inputs.conf '_TCP_ROUTING' setting, which in turn can be overr
* Starting with version 4.2, this setting is no longer required.
```

```
[tcpout:<target_group>]server = [<ip>|<servername>]:<port>, [<ip>|<servername>]:<port>,
```

- * A comma-separated list of one or more systems to send data to over a TCP socket.
- * Required if the 'indexerDiscovery' setting is not set.
- * Typically used to specify receiving Splunk systems, although you can use it to send data to other systems.
- * For each system you list, the following information is required:
 - a. The IP address or server name where one or more systems are listening.
 - b. The port on which the syslog server is listening.

outputs.confのその他の例については、次を参照してください。

[outputs.conf.example \(出力例 \)](#)

[outputs.confを使用してフォワーダを設定します](#)

設定後、ファイルを保存し、\$SPLUNK_HOME/binから次のコマンドを実行してSplunkを再起動します。

```
./splunk restart
```

関連リンク

[outputs.conf.example \(出力例 \)](#)

[outputs.confを使用してフォワーダを設定します](#)

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。