Splunkがsplunkd.logの「Too many open files in system」メッセージによりクラッシュする

適用性

Splunkエンタープライズ

説明

splunkd.logの「 Too many open files in system」メッセージが原因で、Splunkが断続的にクラッシュします。

splunkd.logのログの例：

```
ERROR ProcessRunner - child's last words: ^@^@^@^@cannot create a pipe: Too many open fi
ERROR ProcessRunner - parent/child protocol error: read reply from child "s" (ASCII 0x73
ERROR ProcessRunner - parent/child protocol error: read reply from child "t" (ASCII 0x74
ERROR ProcessRunner - parent/child protocol error: read reply from child "e" (ASCII 0x65
ERROR ProcessRunner - parent/child protocol error: read reply from child "m" (ASCII 0x6D
FATAL ProcessRunner - Unexpected EOF from process runner child!
```

調査

システムレベルで開いているファイルをチェックすると、クラッシュのたびに8kに近い開いているファイルが示され、開いているファイルのハード制限は4096から64000に増加しました。開いているファイルの ulimit値は、次のように splunkd.logに反映されます。

```
INFO  ulimit - Limit: open files: 64000 files
INFO  ulimit - Limit: open files: 64000 files
```

Splunkは、開いているファイルの8k近くでクラッシュし続けます。

「file-max」はカーネルレベルでチェックされました。この場合は、カーネルレベルで強制される最大ファイル記述子(FD)である8192に設定されています。この値を確認するには、次のコマンドを使用します。

```
$ cat /proc/sys/fs/file-max
8192
```

解決方法

この問題を解決するには、file-maxを増やす必要があります。次のコマンドを使用します。

```
sysctl -w fs.file-max=64000
```

システムを再起動します。

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。