

Splunk_TA_microsoft-IISがインストールされているとCPU使用率が高くなるユニバーサルフォワーダ

適用性

Splunk Enterpriseユニバーサルフォワーダ

説明

Splunk_TA_microsoft-IISを無効にするとCPU使用率が約70 %から約10 %に上昇するため、TAに問題が切り分けられました。

調査

識別方法：

a. ユニバーサルフォワーダには、次のアプリケーションがあります。

- OS名 Microsoft Windows Server 2008 R2 Enterprise
- バージョン 6.1.7601 Service Pack 1ビルド7601
- Splunk Universal Forwarder 7.2.0
- Splunk_TA_Windows 5.0.0
- Splunk_TA_microsoft-IIS 1.0.1

b. Splunk_TA_microsoft-IISの設定は次のとおりです。

```
[monitor://C:\inetpub\logs\LogFiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\inetpub\logs\LogFiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\inetpub\logs\logfiles\...\*.log]
disabled = false
```

```
sourcetype = ms:iis:auto  
index = iis[monitor://D:\IISLogs\...\*.log]  
disabled = false  
sourcetype = ms:iis:auto  
index = iis
```

c.上記の設定でSplunk_TA_microsoft-IISアドオンを有効にすると、CPU使用率が70 %になります。

d. 2点と3点を同じ位置に入力します。唯一の違いは、Windowsで無視されるパスの大文字と小文字の区別です。

解決方法

修正方法：

フォルダトラバーサル「..」はCPUリソースの束を盗むことでよく知られています。

Splunk_TA_microsoft-IISアドオンの公式ドキュメントでは、次の単一入力エントリを推奨しています。

[コンフィギュレーションファイルを使用して入力を設定する](#)

この問題を解決するには、4つの入力すべてを単一入力へのフォルダトラバーサルに置き換えます（暗黙的な再帰がtrueに等しい）。

```
[monitor://C:\inetpub\logs\LogFiles]  
whitelist = \.log$|\.LOG$  
disabled = false  
sourcetype = ms:iis:auto
```

\$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.confを変更してSplunkを再起動すると、CPU使用率は通常（10 %以下）のままになります。

関連リンク

[コンフィギュレーションファイルを使用して入力を設定する](#)

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。