

安装Splunk_TA_microsoft-IIS时具有高CPU使用率的通用转发器。

适用范围

Splunk企业通用转发器

描述

问题被隔离到TA，当禁用Splunk_TA_microsoft-IIS时，CPU使用率从~70%升至约10%。

调查

如何识别：

a.通用转发器具有以下应用：

- OS名称Microsoft Windows Server 2008 R2 Enterprise
— 版本6.1.7601 Service Pack 1 Build 7601
- Splunk通用转发器7.2.0
- Splunk_TA_windows 5.0.0
- Splunk_TA_microsoft-IIS 1.0.1

b.Splunk_TA_microsoft-IIS的配置如下：

```
[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.使用上述配置启用Splunk_TA_microsoft-IIS加载项后，CPU使用率将变为70%。

d.向同一位置输入两点和三点的区别是Windows中忽略的路径区分大小写。

分辨率

如何修复：

文件夹遍历“.....”窃取一堆CPU资源是众所周知的。

Splunk_TA_microsoft-IIS附加官方文档建议输入一条信息：

[使用配置文件配置输入](#)

要解决此问题，请使用单输入的文件夹遍历替换所有4个输入（隐式递归等于true）：

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

修改\$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.conf并重新启动Splunk后，CPU使用率将保持正常（约10%）。

相关链接

[使用配置文件配置输入](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。