

Universal Forwarder met hoog CPU-gebruik wanneer Splunk_TA_microsoft-IIS is geïnstalleerd.

toepasbaarheid

Splunk Enterprise Universal Forwarder

Beschrijving

Probleem was om de TA te isoleren, wanneer het uitschakelen van de Splunk_TA_microsoft-IIS het CPU-gebruik naar ~10% laat gaan van ~70%.

onderzoek

Hoe het te identificeren:

a. De universele forwarder heeft de volgende apps:

- Naam besturingssysteem Microsoft Windows Server 2008 R2 Enterprise
- Versie 6.1.7601 Service Pack 1 Build 7601
- Splunk Universal Forwarder 7.2.0
- Splunk_TA_windows 5.0.0
- Splunk_TA_microsoft-IIS 1.0.1

b. De configuratie van Splunk_TA_microsoft-IIS is als volgt:

```
[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. Na het inschakelen van de Splunk_TA_microsoft-IIS add-on met de bovenstaande configuratie, gaat het CPU-gebruik naar 70%.

d. Invoer twee en drie wijzen naar dezelfde locatie, het enige verschil is de hoofdlettergevoeligheid voor het pad genegeerd in Windows.

resolutie

Hoe het te repareren:

Folder Traversals "..." staan erom bekend dat ze een hoop CPU-bronnen stelen.

De officiële documentatie van de Splunk_TA_microsoft-IIS-add-on beveelt een vermelding met één invoer aan:

[Invoer configureren met de configuratiebestanden](#)

Als u het probleem wilt oplossen, vervangt u alle 4 ingangen door mapverkeer door een eenmalige invoer (impliciet recursief is gelijk aan true):

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

Na het wijzigen van \$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.conf en het opnieuw opstarten van Splunk, blijft het CPU-gebruik normaal (~10%).

Gerelateerde links

[Invoer configureren met de configuratiebestanden](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.