

Server d'inoltro universale con utilizzo elevato della CPU quando è installato Splunk_TA_microsoft-IIS.

Applicabilità

Splunk Enterprise Universal Forwarder

Descrizione

Si è verificato un problema isolato per la scheda, quando la disabilitazione di Splunk_TA_microsoft-IIS fa sì che l'utilizzo della CPU passi a circa il 10% da circa il 70%.

Indagine

Come identificarlo:

a. Il server d'inoltro universale dispone delle seguenti app:

- Nome sistema operativo Microsoft Windows Server 2008 R2 Enterprise
- Versione 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. La configurazione di Splunk_TA_microsoft-IIS è la seguente:

```
[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. Dopo aver abilitato il componente aggiuntivo Splunk_TA_microsoft-IIS con la configurazione descritta in precedenza, l'utilizzo della CPU è pari al 70%.

d. I due e tre punti di input si trovano nella stessa posizione, l'unica differenza è rappresentata dalla distinzione tra maiuscole e minuscole per il percorso ignorato in Windows.

Risoluzione

Come risolvere il problema:

Visite cartelle "..." sono ben noti per rubare un mucchio di risorse CPU.

La documentazione ufficiale del componente aggiuntivo Splunk_TA_microsoft-IIS consiglia una voce con un solo input:

[Configurare gli input utilizzando i file di configurazione](#)

Per risolvere il problema, sostituire tutti e 4 gli input con l'attraversamento delle cartelle a un input singolo (ricorsivo implicito uguale a true):

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

Dopo aver modificato \$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.conf e riavviato Splunk, l'utilizzo della CPU rimarrà normale (~10%).

Collegamenti correlati

[Configurare gli input utilizzando i file di configurazione](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).