

Encaminhador Universal com Alta Utilização de CPU quando Splunk_TA_microsoft-IIS está Instalado.

Aplicabilidade

Encaminhador Universal Corporativo Splunk

Descrição

O problema foi isolado do TA, quando a desabilitação do Splunk_TA_microsoft-IIS faz com que o uso da CPU vá para ~10% de ~70%.

Investigação

Como identificá-lo:

a. O encaminhador universal tem os seguintes aplicativos:

- Nome do SO Microsoft Windows Server 2008 R2 Enterprise
- Versão 6.1.7601 Service Pack 1 Build 7601
- Encaminhador Universal Splunk 7.2.0
- Splunk_TA_windows 5.0.0
- Splunk_TA_microsoft-IIS 1.0.1

b. A configuração de Splunk_TA_microsoft-IIS é a seguinte:

```
[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. Após habilitar o complemento Splunk_TA_microsoft-IIS com a configuração acima, o uso da CPU vai para 70%.

d. As entradas dois e três apontam para o mesmo local, a única diferença é a distinção entre maiúsculas e minúsculas para o caminho ignorado no Windows.

Resolução

Como corrigi-lo:

Travessias de pasta "..." são conhecidos por roubar vários recursos da CPU.

A documentação oficial do complemento Splunk_TA_microsoft-IIS recomenda uma entrada com uma entrada:

[Configurar entradas usando os arquivos de configuração](#)

Para corrigir o problema, substitua todas as 4 entradas com passagem de pasta para uma entrada única (recursivo implícito é igual a verdadeiro):

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

Após modificar \$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.conf e reiniciar o Splunk, o uso da CPU permanecerá normal (~10%).

Links relacionados

[Configurar entradas usando os arquivos de configuração](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.