

A estrofe do monitor não está funcionando conforme esperado.

Aplicabilidade

Empresa Splunk

Descrição

Ao tentar monitorar arquivos cujos nomes não mudam, mas o conteúdo muda, o Splunk não está funcionando conforme esperado, por exemplo:

```
[monitor:///path/reports]
index = splunk_test
initCrcLength = 4096
ignoreOlderThan = 1d
disabled = 0
sourcetype = DiskUsage
```

Investigação

O Splunk está indexando dados com base no contexto de timestamp no arquivo e não no momento em que o arquivo é realmente gerado, já que o arquivo captura informações de data/hora com base nos detalhes do host daquele fuso horário específico.

Resolução

Defina "DATETIME_CONFIG = CURRENT" no arquivo props.conf, porque os novos logs indexados terão a hora atual no timestamp, que provavelmente será a hora em que o arquivo foi criado, o encaminhador monitorará o arquivo e o encaminhará quase instantaneamente.

Exemplo:

```
$SPLUNK_HOME/etc/system/local/props.conf
[source::.../mylogs/*.log]
DATETIME_CONFIG = CURRENT
```

Links relacionados

Documentação do Splunk

Configuração de extração de carimbo de data/hora:

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf?utm_source=answers&utm_medium=question&utm_term=props.conf&utm_campaign=refdoc#Timestamp_extraction_configuration

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.