

nullqueue regex não está funcionando conforme esperado

Aplicabilidade

Empresa Splunk

Descrição

Temos vários casos de uso em que implementamos esse padrão "Mantenha eventos específicos e descarte o restante".

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specifi

Esbarramos em um caso em que tínhamos transformações de fila nula definidas abaixo em nossos indexadores. Verificamos que este regex corresponde a todos os nossos eventos. Em seguida, XXX corresponde ao subconjunto de eventos que queremos manter e enviar para o índice <INDEX>.

Transformações:

```
[YYY]
REGEX = .*LogName=Security.*
DEST_KEY = queue
FORMAT = nullQueue[XXX]
REGEX=(?msi)^EventCode=(<NUMBERS IN A REGEX>)
DEST_KEY = _MetaData:Index
FORMAT = <INDEX>
```

Suplementos:

```
[WinEventLog:Security]
TRANSFORMS-set=YYY, XXX
```

Isso não funcionou. Não tínhamos nada em <INDEX>. Então quando mudamos YYY regex para "REGEX=" funcionou bem. No entanto, devemos ser capazes de REGEX nullque com regexp mais específico do que "." quando ele realmente coincide com todos os eventos.

Investigação

Comparando a conferência do usuário com a documentação, observou-se que todos os diagramas de trabalho começaram com um teste de chamada. Podemos ter várias extrações do

catchall, permitindo que o usuário seja tão granular com o catchall no lugar.

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific

Resolução

Configure props e transformações para ter a primeira transformação nullqueue com algum regex diferente de ".". Em seguida, outra transformação com regex mais específico e algum índice e espera que os dados vão para esse índice.

Transformações:

```
[XXX]
REGEX = .
DEST_KEY = queue
FORMAT = nullQueue[YYY]
REGEX=(?msi)^EventCode=(<NUMBERS IN A REGEX>)
DEST_KEY = _MetaData:Index
FORMAT = <INDEX>[ZZZ]
REGEX= <LOG NAME REGEX>
DEST_KEY = _MetaData:Index
FORMAT = <DIFFERENT INDEX>
```

Suplementos:

```
[WinEventLog:Security]
TRANSFORMS-set=XXX, YYY, ZZZ
```

Links relacionados

Documentação do Splunk

Manter eventos específicos e descartar o restante:

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific

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.