

Nullqueue Regex werkt niet zoals verwacht

toepasbaarheid

Splunk Enterprise

Beschrijving

We hebben verschillende use cases waar we dit "Keep specific events and discard the rest" patroon implementeren.

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

We stuiten op een geval waarin we nulwachtrijtransformaties hadden zoals hieronder gedefinieerd in onze indexers. We hebben geverifieerd dat deze regex overeenkomt met al onze evenementen. Dan komt XXX overeen met de subset van gebeurtenissen die we willen bewaren en naar de index <INDEX> sturen.

Transformaties:

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

Rekwisieten:

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

Dit werkte niet. We hadden niets in de <INDEX>. Toen we YYY regex veranderden in "REGEX=." werkte het goed. We zouden echter in staat moeten zijn om REGEX nullque met meer specifieke regexp te gebruiken dan "." wanneer het daadwerkelijk overeenkomt met alle gebeurtenissen.

onderzoek

Vergelijking van het conf van de gebruiker met de documentatie werd opgemerkt dat alle werkende diagrammen begonnen met een catchall-test. We kunnen meerdere extracties uit de catchall hebben, waardoor de gebruiker net zo korrelig kan zijn met de catchall op zijn plaats.

resolutie

Stel rekvisieten en transformaties in om de eerste nullqueue-transformatie te hebben met enkele andere regex dan ".". Dan nog een transformatie met meer specifieke regex en wat index en verwacht dat de gegevens naar die index gaan.

Transformaties:

```
[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>
```

Rekvisieten:

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

Gerelateerde links

Splunk-documentatie

Houd specifieke gebeurtenissen bij en gooi de rest weg:

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

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.