

# nullqueue regex ne fonctionne pas comme prévu

## Applicabilité

Splunk Enterprise

## Description

Nous avons plusieurs cas d'utilisation où nous implémentons ce modèle « Gardez des événements spécifiques et ignorez le reste ».

[https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep\\_specific](https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific)

Nous sommes tombés dans un cas où nous avons des transformations de file d'attente nulles définies comme ci-dessous dans nos indexeurs. Nous avons vérifié que cette expression régulière correspond à tous nos événements. XXX correspond ensuite au sous-ensemble d'événements que nous voulons conserver et envoyer à l'index <INDEX>.

Transformations :

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

Accessoires :

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

Cela n'a pas fonctionné. Nous n'avions rien dans <INDEX>. Ensuite, quand nous avons changé YYY regex en "REGEX=." ça a bien marché. Cependant, nous devrions être capables d'utiliser REGEX nullque avec regexp plus spécifique que "." quand il correspond réellement à tous les événements.

## Enquête

En comparant la conf de l'utilisateur avec la documentation, il a été remarqué que tous les diagrammes de travail ont commencé par un test catchall. Nous pouvons avoir plusieurs extractions de la catchall permettant à l'utilisateur d'être aussi granulaire avec la catchall en place.

[https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep\\_specific](https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific)

## Résolution

Configurez les propriétés et les transformations pour avoir la première transformation nullqueue avec un regex autre que ".". Puis une autre transformation avec un regex plus spécifique et un certain index et s'attendre à ce que les données aillent à cet index.

Transformations :

```
[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>
```

Accessoires :

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

## Liens connexes

Documentation Splunk

Conservez des événements spécifiques et ignorez le reste :

[https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep\\_specific](https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.