

nullqueue regex non funziona come previsto

Applicabilità

Splunk Enterprise

Descrizione

Abbiamo diversi casi di utilizzo in cui implementiamo questo modello "Mantieni eventi specifici ed elimina il resto".

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

Si è verificato un caso in cui negli indicizzatori erano presenti trasformazioni di coda nulle definite di seguito. Abbiamo verificato che questo regex corrisponde a tutti i nostri eventi. XXX corrisponde quindi al sottoinsieme di eventi che si desidera mantenere e inviare all'indice <INDEX>.

Trasformazioni:

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

Proprietà:

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

Questo non ha funzionato. Non c'è nulla in <INDEX>. Poi quando abbiamo cambiato YYY regex in "REGEX=" ha funzionato bene. Tuttavia, dovremmo essere in grado di REGEX nullque con regex più specifico che "." quando corrisponde effettivamente a tutti gli eventi.

Indagine

Confrontando la configurazione dell'utente con la documentazione, è stato notato che tutti i diagrammi funzionanti iniziavano con un test catchall. Possiamo avere più estrazioni dal catchall che permettono all'utente di essere così granulari con il catchall in posizione.

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

Risoluzione

Impostare le proprietà e le trasformazioni in modo che abbiano la prima trasformazione nullqueue con alcuni regex diversi da ".". Poi un'altra trasformazione con regex più specifico e qualche indice e si aspetta che i dati vanno a quel indice.

Trasformazioni:

```
[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>
```

Proprietà:

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

Collegamenti correlati

Documentazione relativa a Splunk

Mantieni eventi specifici ed elimina il resto:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).