

# Velden kunnen niet worden gezocht met "="

## toepasbaarheid

Splunk Enterprise Splunk Cloud

## Beschrijving

Splunk-versie: 7.0.13

Wanneer u een van de volgende velden probeert te doorzoeken door een tekenreeks te matchen:

- peul
- naamruimte
- container\_name
- container\_id

Zoals `container_id=aadd1`, geeft geen resultaten terug.

## onderzoek

Na enig onderzoek werd opgemerkt dat HEC-gegevens op deze configuratie worden geïndexeerd zonder enig configuratiebestand, maar voor een goed gebruik is enige configuratie nodig. De velden kunnen in feite doorzoekbaar zijn door in te stellen met de `::` teken (metagegevensvelden opgegeven), maar dit lost niet op dat ze niet kunnen worden gezocht met het teken `=`.

Om dit te laten werken, moeten verdere configuraties worden uitgevoerd bij het zoeken. Het lijkt erop dat bij het hebben van HEC-ingangen voor GCP-kubernetten de gebeurtenissen niet volledig zijn voorbereid om doorzoekbaar te zijn. Vooral de velden lijken niet geïndexeerd te blijven, wat deel uitmaakt van de ruwe gegevens, maar niet te worden gespecificeerd bij het zoeken naar het krijgen van gebeurtenissen.

## resolutie

Aangezien gebeurtenissen geen geïndexeerde configuratieparameters krijgen, moeten deze als volgt worden toegevoegd:

Voorbeeld: zoekkop

Bestand: `fields.conf`

Pad: \$SPLUNK\_HOME/etc/apps/zoeken/lokaal

Instelling: Voeg elk veld als een strofe toe met de parameter INDEXED=true als volgt.

```
[pod]
INDEXED=true[namespace]
INDEXED=true[container_name]
INDEXED=true[container_id]
INDEXED=true
```

Hierna moet de zoekkop opnieuw worden opgestart en hiermee kunnen nieuwe gebeurtenissen worden doorzocht met het =-teken.

## Gerelateerde links

### Splunk Antwoorden

Waarom moet ik metadata zoeken in een "velden" argument van een HEC met ':'?:

<https://answers.splunk.com/answers/635676/why-do-i-need-to-search-metadata-in-a-fields-argum.html>

### Externe links

Instellingen voor Kubernetes-logging:

<https://github.com/splunk/splunk-connect-for-kubernetes/tree/develop/helm-chart/splunk-kubernetes-logging>

## 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.