

Monitor stanza werkt niet zoals verwacht.

toepasbaarheid

Splunk Enterprise

Beschrijving

Wanneer u bestanden probeert te controleren waarvan de namen niet veranderen, maar de inhoud wel, werkt Splunk niet zoals verwacht, bijvoorbeeld:

```
[monitor:///path/reports]
index = splunk_test
initCrcLength = 4096
ignoreOlderThan = 1d
disabled = 0
sourcetype = DiskUsage
```

onderzoek

Splunk is het indexeren van gegevens op basis van de tijdstempelcontext in het bestand en niet op het moment dat het bestand daadwerkelijk wordt gegenereerd, omdat het bestand datum-/tijdinformatie vastlegt op basis van de hostdetails van die specifieke tijdzone.

resolutie

Stel "DATETIME_CONFIG = CURRENT" in het bestand props.conf in, omdat de nieuwe logs die geïndexeerd zijn, de huidige tijd in de tijdstempel hebben, wat waarschijnlijk de tijd is waarop het bestand is gemaakt, de expediteur zal het bestand controleren en het vrijwel onmiddellijk doorsturen.

Voorbeeld:

```
$SPLUNK_HOME/etc/system/local/props.conf
[source::.../mylogs/*.log]
DATETIME_CONFIG = CURRENT
```

Gerelateerde links

Splunk-documentatie

Configuratie tijdstempelextractie:

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf?utm_source=answers&utm_medium=question&utm_term=props.conf&utm_campaign=refdoc#Timestamp_extraction_configuration

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.