

Hoog CPU-verbruik op Universal Forwarder

toepasbaarheid

Splunk Enterprise

Beschrijving

Een onverwachte activiteit van een Windows-hostproces dat de I/O-bewerkingen van Windows-gebeurtenissen afhandelt, is waargenomen waarbij het CPU-gebruik constant tussen 10% en 30% blijft. Gebruikers hebben geklaagd over degradatie van de eindpuntgebruikerservaring.

Opgemerkt wordt dat het splunk-PowerShell-proces voortdurend wordt uitgeschreven naar de open PowerShell-pijpleiding.

onderzoek

Het optreden van deze gebeurtenissen:

```
Event 4103CommandInvocation(Out-Null): "Out-Null"CommandInvocation(Out-Null): "Out-Null"
```

```
Event 4103CommandInvocation(Start-Sleep): "Start-Sleep"ParameterBinding(Start-Sleep): na
```

Deze constante 200 ms slaapstand en logboekregistratie zorgen ervoor dat de EventLog-service een hoge CPU verbruikt.

resolutie

De Splunk-bovenliggende PS1-code `$SPLUNK_HOME\bin\splunk-powershell.ps1` is gewijzigd op een paar machines door de volgende code te vervangen:

```
if($disposedNow -eq 0){start-sleep -m 200}
```

Met een hogere waarde, in onze test: 250000ms (~4 min)

Daarna was de CPU stabiel.

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.