Integreer Splunk met Umbrella Log Management met S3 en Local Sync

Inhoud

Inleiding

In dit document wordt beschreven hoe u Splunk kunt configureren om DNS-verkeerslogboeken te analyseren vanuit een door Cisco beheerde S3-bucket.

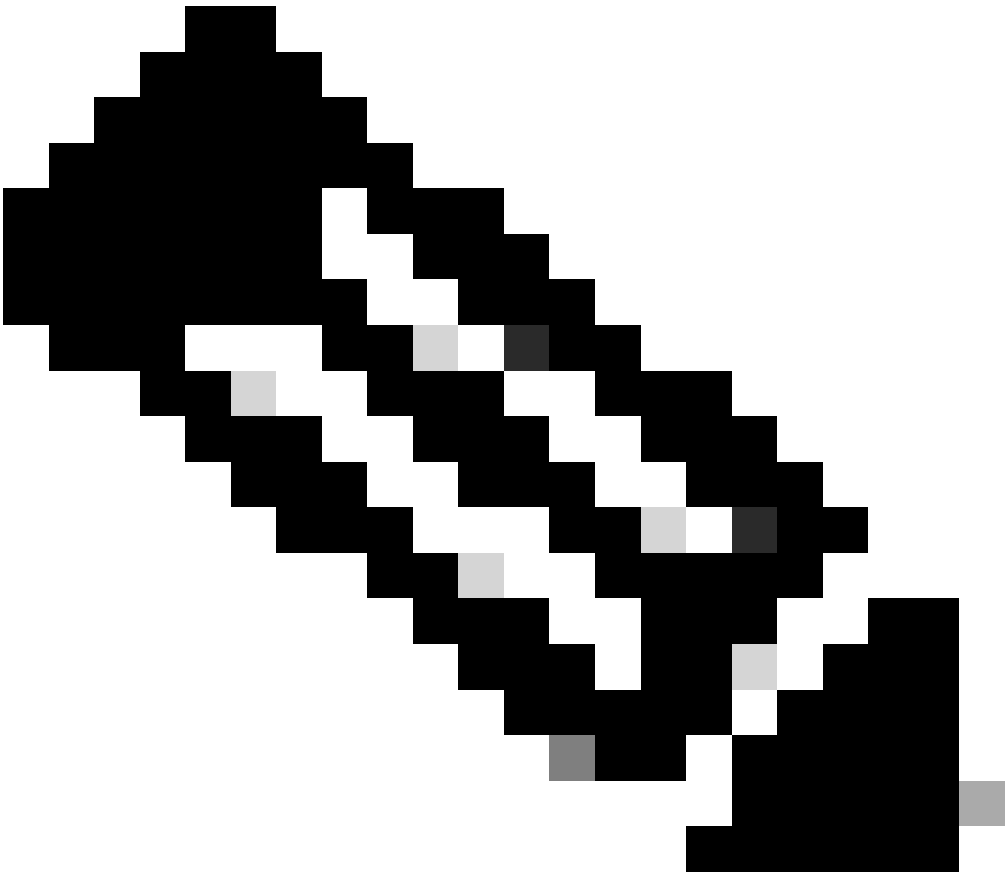
Overzicht

Splunk is een tool voor log-analyse. Het biedt een krachtige interface voor het analyseren van grote hoeveelheden gegevens, zoals de logs die door Cisco Umbrella worden geleverd voor uw DNS-verkeer. In dit artikel wordt beschreven hoe u:

- Stel uw Cisco-beheerde S3-emmer in uw dashboard in.
- Zorg ervoor dat aan de vereisten voor de AWS Command Line Interface (AWS CLI) is voldaan.
- Maak een cron-taak om bestanden uit de bucket op te halen en deze lokaal op uw server op te slaan.
- Configureer Splunk om te lezen uit een lokale directory.

Voorwaarden

- Download en installeer de AWS Command Line Interface (AWS CLI).
- Maak uw Cisco-beheerde S3-bucket.



Opmerking: bestaande Umbrella Insights- en Umbrella Platform-klanten kunnen via het dashboard toegang krijgen tot Logbeheer met Amazon S3. Logboekbeheer is niet beschikbaar in alle pakketten. Neem contact op met uw accountmanager als u geïnteresseerd bent in deze functie.

Een Cron-taak maken op de Splunk-server

1. Maak een shell-script met de naam **pull-umbrella-logs.sh** met de opgegeven inhoud, dat wordt uitgevoerd op een geplande cron-taak:

```
#!/bin/sh
cd <local data dir>
AWS_ACCESS_KEY_ID=<accesskey> AWS_SECRET_ACCESS_KEY=<secretkey> aws s3 sync <data path> .
```

Vervang de plaatsaanduidingen door uw werkelijke waarden:

-

: Directory op schijf om de gedownloade logbestanden op te slaan.

- : Toegangssleutel van het dashboard van de paraplu.
- : Geheime sleutel van het dashboard van de paraplu.
- : gegevenspad van de gebruikersinterface voor logboekbeheer (bijvoorbeeld s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/
).

2. Sla het shell-script op en stel de uitvoeringsmachtiging in. Het script moet eigendom zijn van root.

```
$ chmod u+x pull-umbrella-logs.sh
```

3. Voer het **pull-umbrella-logs.sh** script handmatig uit om te bevestigen dat het synchronisatieproces functioneel is. Volledige voltooiing is niet vereist; deze stap bevestigt dat referenties en scriptlogica correct zijn.

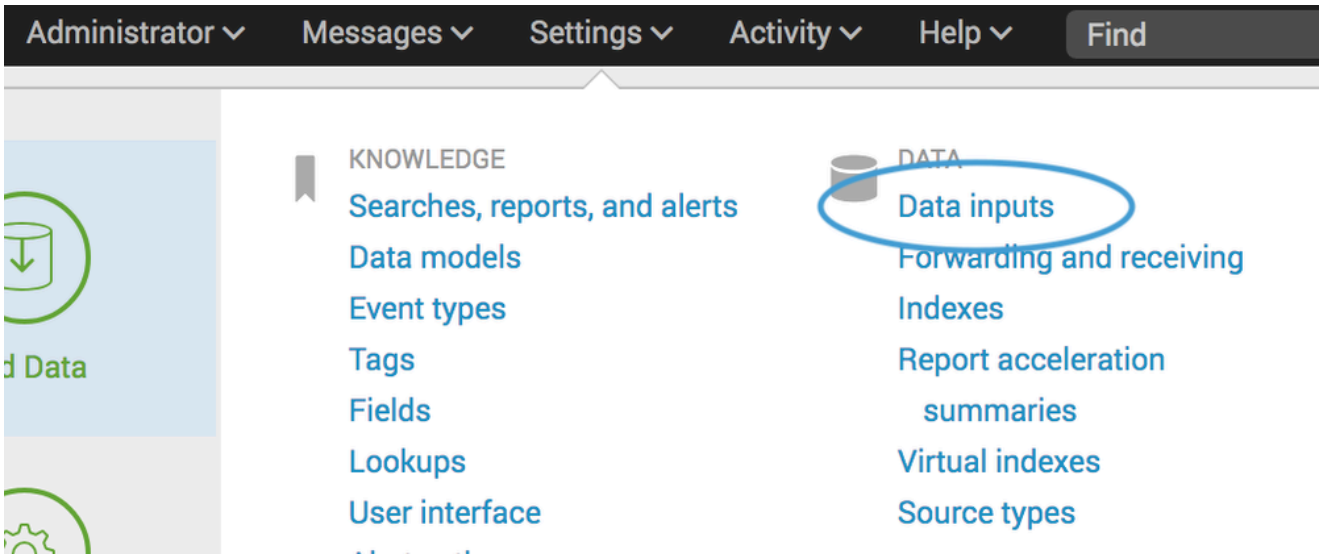
4. Voeg deze regel toe aan uw Splunk server crontab:

```
*/5 * * * * root root /path/to/pull-umbrella-logs.sh &2>1 >/var/log/pull-umbrella-logs.txt
```

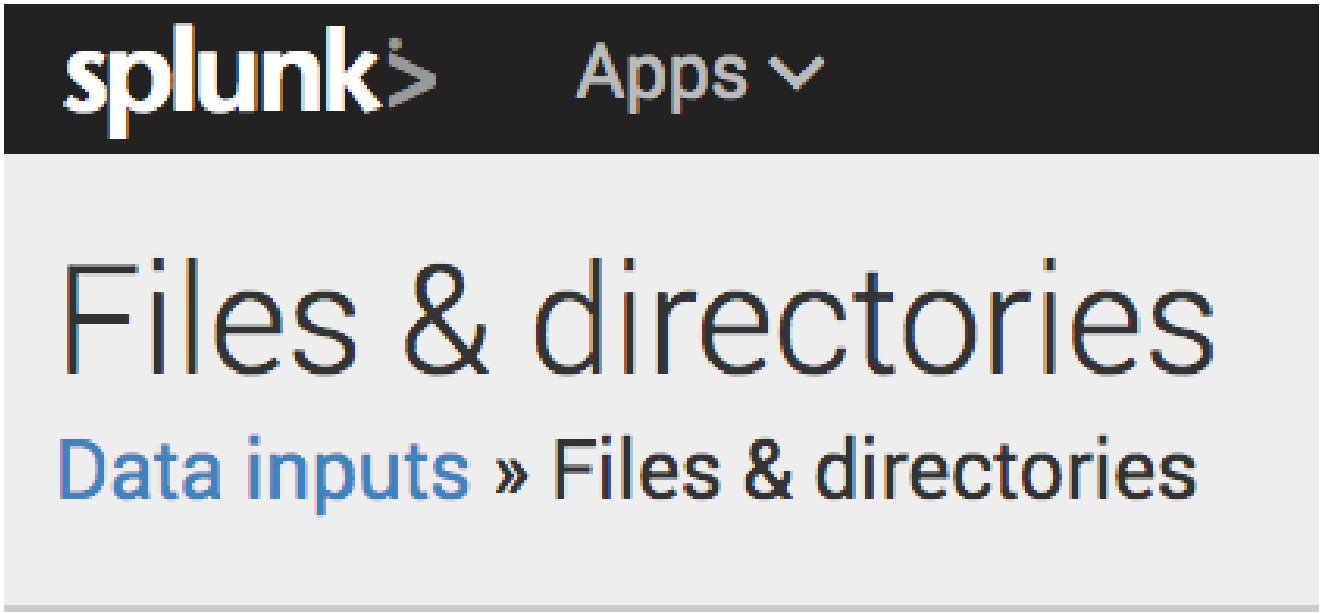
Zorg ervoor dat u de regel bewerkt om het juiste pad naar het script te gebruiken. Dit voert elke vijf minuten een synchronisatie uit. De S3-opslagdirectory wordt elke 10 minuten bijgewerkt en de gegevens blijven 30 dagen op de S3-opslag staan. Hierdoor blijven de twee synchroon lopen.

Splunk configureren om uit een lokale map te lezen

1. Navigeer in Splunk naar Instellingen > Gegevensinvoer > Bestanden en directory's en selecteer Nieuw.

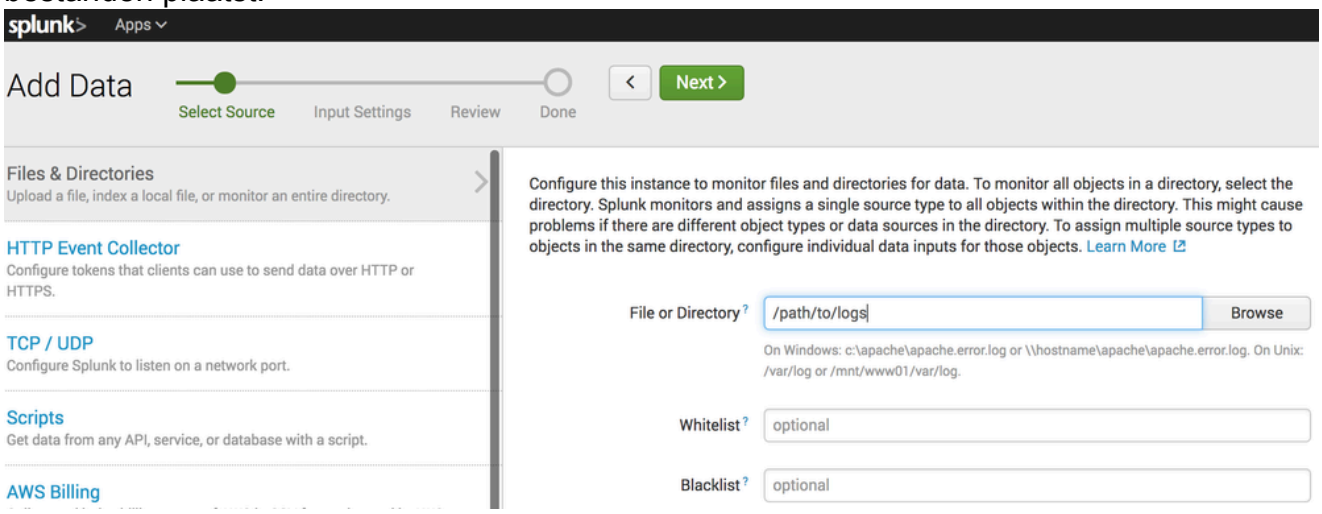


360002731126



360002731146

2. Geef in het veld Bestand of Directory de lokale map op waar de S3-synchronisatie bestanden plaatst.



360002731106

3. Klik op Volgende en voltooi de wizard met de standaardinstellingen.

Zodra er gegevens in de lokale directory zijn en Splunk is geconfigureerd, kunnen de gegevens beschikbaar zijn om te query en te rapporteren in Splunk.

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.