

Probleem bij verzenden van e-mail vanuit Splunk - aangepaste waarschuwingsactie

toepasbaarheid

Splunk Enterprise Splunk Cloud

Beschrijving

Een nieuwe toepassing gemaakt om het afzenderadres voor waarschuwingen afkomstig van die specifieke toepassing te overschrijven.

Een lokaal .conf-bestand gemaakt voor de overschreven waarden in het volgende bestand:

```
/opt/splunk/etc/apps/<app_name>/local/alert_actions.conf
```

De inhoud is als volgt:

```
[email]  
from = Service Desk <servicedesk@your_domain.com>  
footer.text =
```

onderzoek

Maak een lab.

De configuratiebestanden gebruiken:

- [Opgeslagen zoekopdrachten.conf](#)
- [alert_actions.conf](#)

1. Creëer een waarschuwing.
2. Wijzig de e-mail in het veld 'van' op Splunk Web.
3. Wijzig het e-mailveld 'van' met de configuratiebestanden.

resolutie

Splunk moet de 'from' wijzigen op de waarschuwingsmelding in de Web-gebruikersinterface 'Serverinstellingen' en de CLI `alert_actions.conf`.

De juiste manier om het veld 'van' te wijzigen, is door de Web UI op de zoekkop te gebruiken:

Serverinstellingen > E-mailinstellingen > E-mailindeling > E-mails verzenden als

De wijziging is aangebracht op het zoekhoofd en werkte correct. Om de een of andere reden werd het veld 'van' niet direct geaccepteerd in de aangepaste app.

Zorg er altijd voor dat de waarschuwing op `savedsearches.conf` geen andere e-mailserver bevat die voorrang kan hebben op de e-mailserverset in `alert_actions.conf`

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.