Configureer Splunk met een zelfbeheerde S3-emmer

Inhoud

Inleiding

In dit document wordt beschreven hoe u Splunk kunt configureren met een zelfbeheerde S3-emmer.

Overzicht

Splunk is een veelgebruikt instrument 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 het DNS-verkeer van uw organisatie.

Dit artikel schetst de basis van het krijgen van Splunk opgezet en uitgevoerd, zodat het in staat is om de logs uit uw S3 emmer te trekken en ze te consumeren. Er zijn twee hoofdfasen, een is om uw AWS S3-beveiligingsreferenties te configureren om Splunk toegang te geven tot de logs, en de tweede is om Splunk zelf te configureren om naar uw emmer te wijzen.

De documentatie voor de Splunk Add-on voor AWS S3 is hier, waarvan sommige letterlijk in dit document is gekopieerd. Voor specifieke vragen over de Splunk setup verwijzen wij u naar http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

Dit artikel bevat de volgende onderdelen:

- Voorwaarden
- Fase 1: Beveiligingsreferenties configureren in AWS (alleen zelfbeheerde emmer)

- Fase 2: Splunk instellen om DNS-loggegevens uit uw S3-emmer te trekken
    - Stap 1: Splunk instellen om DNS-loggegevens uit de zelfbeheerde S3-emmer te halen
- Fase 3: gegevensinvoer configureren voor Splunk

Voorwaarden

De Splunk Add-on voor Amazon Web Services ondersteunt deze platforms.

- AWS Linux
- RedHat
- Windows 2008R2, 2012R2

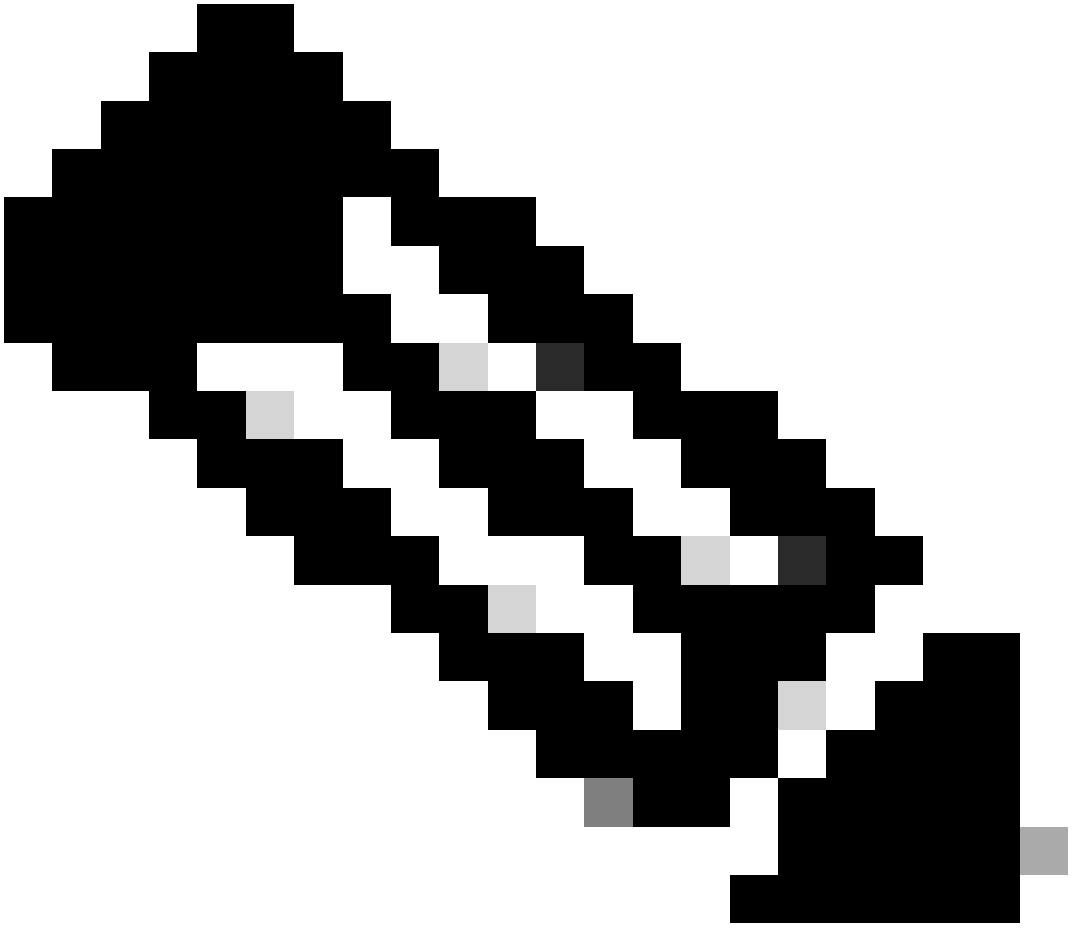
Splunk Enterprise-systeemvereisten

Omdat deze add-on wordt uitgevoerd op Splunk Enterprise, zijn alle systeemvereisten van Splunk Enterprise van toepassing. Zie de installatiehandleiding "Systeemvereisten" in de documentatie van Splunk Enterprise. Deze instructies zijn voor de Splunk Enterprise versie 6.2.1.

Paraplu-eisen

In dit document wordt ervan uitgegaan dat uw Amazon AWS S3-emmer is geconfigureerd in het Umbrella-dashboard (Beheer> Logbeheer) en groen wordt weergegeven met recente logs die zijn geüpload. Zie Cisco Umbrella Log Management in Amazon S3 voor meer informatie over logboekbeheer.

Fase 1: Beveiligingsreferenties configureren in AWS



Opmerking: deze stappen zijn dezelfde als die in het artikel worden beschreven waarin wordt beschreven hoe u een tool kunt configureren om de logs uit uw emmer te downloaden (Hoe: Logboeken downloaden van Cisco Umbrella Log Management in AWS S3). Als u deze stappen al hebt uitgevoerd, kunt u eenvoudig overslaan naar stap 2, hoewel u de beveiligingsreferenties van uw IAM-gebruiker nodig hebt om de Splunk-plug-in in uw emmer te verifiëren.

Stap 1

1. Voeg een toegangssleutel toe aan uw Amazon Web Services-account om externe toegang tot uw lokale tool mogelijk te maken en de mogelijkheid te bieden om bestanden in S3 te uploaden, downloaden en wijzigen. Meld u aan bij AWS en klik op uw accountnaam in de rechterbovenhoek. Kies in de vervolgkeuzelijst Beveiligingsreferenties.
2. U wordt gevraagd om Amazon Best Practices te gebruiken en een AWS Identity and Access Management (IAM) -gebruiker aan te maken. In wezen zorgt een IAM-gebruiker ervoor dat het account dat s3cmd gebruikt om toegang te krijgen tot uw bucket niet het primaire account is (bijvoorbeeld uw account) voor uw hele S3-configuratie. Door individuele IAM-

gebruikers te maken voor mensen die toegang hebben tot uw account, kunt u elke IAM-gebruiker een unieke set beveiligingsreferenties geven. U kunt ook verschillende machtigingen verlenen aan elke IAM-gebruiker. Indien nodig kunt u de machtigingen van een IAM-gebruiker op elk moment wijzigen of intrekken.
Voor meer informatie over IAM-gebruikers en AWS best practice, lees hier: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Stap 2

1. Maak een IAM-gebruiker om toegang te krijgen tot uw S3-emmer door op Aan de slag met IAM-gebruikers te klikken. U wordt naar een scherm gebracht waar u een IAM-gebruiker kunt maken.
2. Klik op Nieuwe gebruikers maken en vul de velden in. Houd er rekening mee dat de gebruikersaccount geen spaties kan bevatten.
3. Na het maken van het gebruikersaccount krijgt u slechts één kans om twee kritieke stukjes informatie te pakken die uw Amazon-gebruikersbeveiligingsreferenties bevatten. We raden u ten zeerste aan deze te downloaden met behulp van de knop rechtsonder om een back-up te maken. Ze zijn niet beschikbaar na deze fase in de setup. Zorg ervoor dat u zowel uw toegangscode als uw geheime toegangscode noteert, omdat we ze later nodig hebben bij het instellen van Splunk.

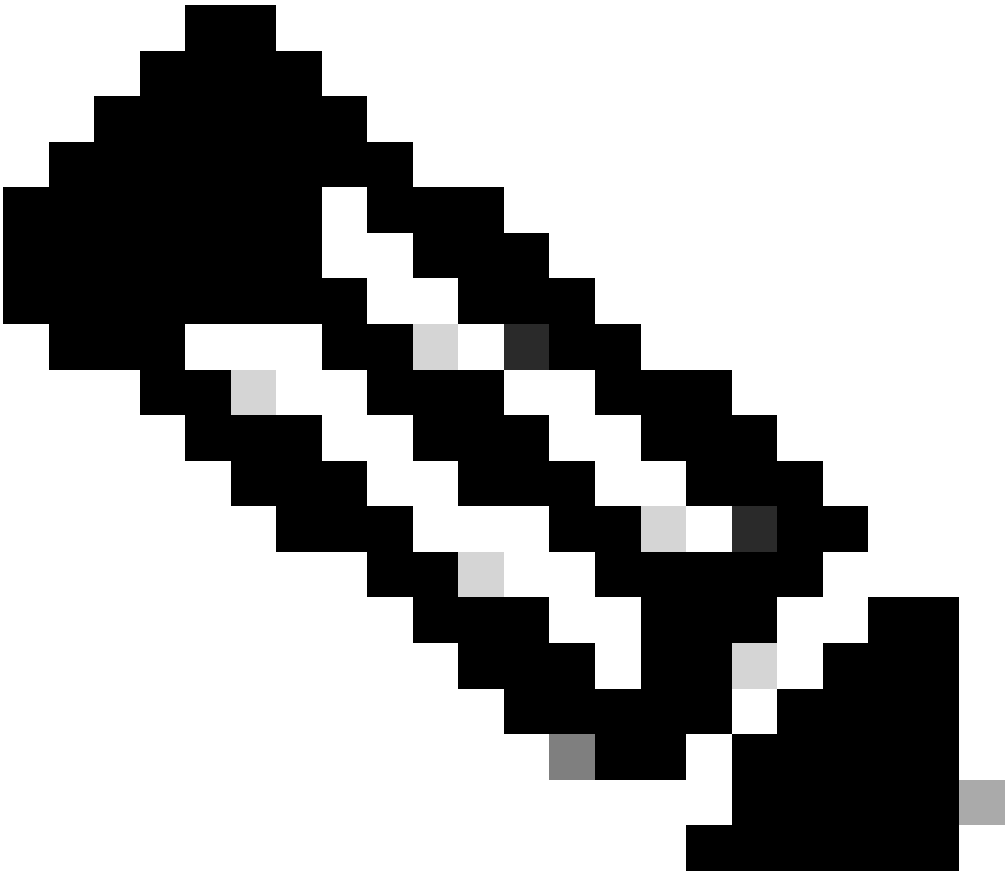
Stap 3

1. Vervolgens wilt u een beleid toevoegen voor uw IAM-gebruiker, zodat ze toegang hebben tot uw S3-emmer. Klik op de gebruiker die u zojuist hebt gemaakt en blader vervolgens omlaag door de eigenschappen van de gebruiker totdat u de knop Beleid toevoegen ziet.
2. Klik op Beleid bijvoegen en voer 's3' in het filter Beleidstype in. Dit toont twee resultaten: "AmazonS3FullAccess" en "AmazonS3ReadOnlyAccess".
3. Selecteer AmazonS3FullAccess en klik vervolgens op Beleid toevoegen.

Fase 2: Splunk instellen om DNS-loggegevens uit uw S3-emmer te trekken

Stap 1: Splunk instellen om DNS-loggegevens uit de zelfbeheerde S3-emmer te halen

1. Begin met het installeren van de "Splunk Add-on voor Amazon Web Services" naar uw Splunk instantie. Open je Splunk-dashboard en klik op Apps, of klik op Splunk Apps als het op je dashboard verschijnt. Eenmaal in de sectie Apps, typ "s3" in het zoekvenster om "Splunk Add-on for Amazon Web Services" te vinden en installeer de app.



Opmerking: u moet Splunk waarschijnlijk opnieuw starten tijdens de installatie. Zodra het is geïnstalleerd, ziet u Splunk Add-on voor AWS met de mapnaam 'Splunk_TA_aws' nu vermeld onder Apps.

2. Klik op Instellen om de app te configureren. Dit is het punt waarop u de beveiligingsreferenties van fase 1 in deze documentatie nodig hebt.
   Voor de installatie moeten de volgende velden worden ingevoerd:

   - Een vriendelijke naam - de naam die u gebruikt om naar deze integratie te verwijzen
   - Sleutel-ID van uw AWS-account (vanaf fase 1)
   - Uw wachtwoord (uw AWS-account Secret Key, ook vanaf stap 1)

U kunt ook lokale proxy-informatie instellen als het nodig is voor Splunk om AWS te bereiken, evenals het aanpassen van de logboekregistratie. Het setup-scherm ziet er als volgt uit:
3. Nadat u relevante informatie hebt toegevoegd, klikt u op Opslaan en de Splunk-invoegtoepassing voor Amazon Web Services is volledig geconfigureerd.

Fase 3: gegevensinvoer configureren voor Splunk

1. Vervolgens wilt u de gegevensinvoer configureren voor Amazon Web Services S3. Navigeer naar Instellingen > Gegevens > Gegevensinvoer en onder Lokale invoer ziet u nu een lijst met verschillende Amazon-ingangen, waaronder S3 onderaan de lijst.
2. Klik op AWS S3 om de invoer te configureren.
3. Klik op New (Nieuw).
4. U bent verplicht om deze informatie te verstrekken:

    - Voer een vriendelijke naam in voor uw S3-integratie.
    - Selecteer uw AWS-account van de dropdown. Dit is de vriendelijke naam die je in stap 1 hebt gegeven.
    - Selecteer uw S3-emmer in de vervolgkeuzelijst. Dit is de naam van de emmer zoals opgegeven in uw Umbrella-dashboard (Instellingen > Logbeheer).
    - Selecteer de naam van de S3-toets in de vervolgkeuzelijst. Elk item in uw bucket wordt vermeld, raden we u aan de directory op het hoogste niveau te kiezen \dns-logs\ , die alle bestanden en directory's eronder bevat.
    - Er zijn verschillende opties onder "Berichtensysteemconfiguratie", we raden aan deze te laten zoals ze zijn - standaardinstellingen.
    - Er zijn extra opties onder "Meer instellingen". Van belang is het "Source type", dat standaard aws: s3 is. We raden u aan dit ongewijzigd te laten, maar als u het wijzigt, verandert het filter voor uw logs in de zoekopdracht van wat wordt beschreven in stap 3 van deze instructies.

    Vul de gegevens in en uw gegevensinvoer ziet er als volgt uit:

4. Klik op Volgende om uw gegevens te voltooien.
   U wordt naar een scherm geleid dat aangeeft dat de invoer met succes is gemaakt

Stap 3

Voer een snelle zoekopdracht uit om te zien of uw gegevens correct worden geïmporteerd. Plak gewoon sourcetype="aws:s3" in het zoekvenster rechtsboven en selecteer vervolgens "Open sourcetype="aws:s3" in de zoekopdracht

Hiermee gaat u naar een scherm dat lijkt op het scherm waarop u de gebeurtenissen in de DNS-logs van uw organisaties ziet. De mobiele dienst Cisco Umbrella blokkeert sociale media op een iPhone. U kunt ook de bron van de bestandsnaam gebruiken om te filteren op een bepaalde batch logs.

Na dit punt blijft de cron-taak op de achtergrond worden uitgevoerd en worden de nieuwste sets uit logboekgegevens uit uw emmer gehaald.

Er is veel meer dat u met Splunk kunt doen dan wat in dit artikel is beschreven, en als u de kans hebt gehad om te experimenteren met het gebruik van deze gegevens in uw beveiligingsresponsprocedure, horen we graag van u. Stuur eventuele feedback, vragen of zorgen naar umbrella-support@cisco.com en verwijs naar dit artikel.

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.