QRadar-integratie configureren met Umbrella Log Management en S3

Inhoud

Inleiding

In dit document wordt beschreven hoe u QRadar kunt configureren om logs in te nemen vanuit een AWS S3-emmer voor overkoepelend logboekbeheer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

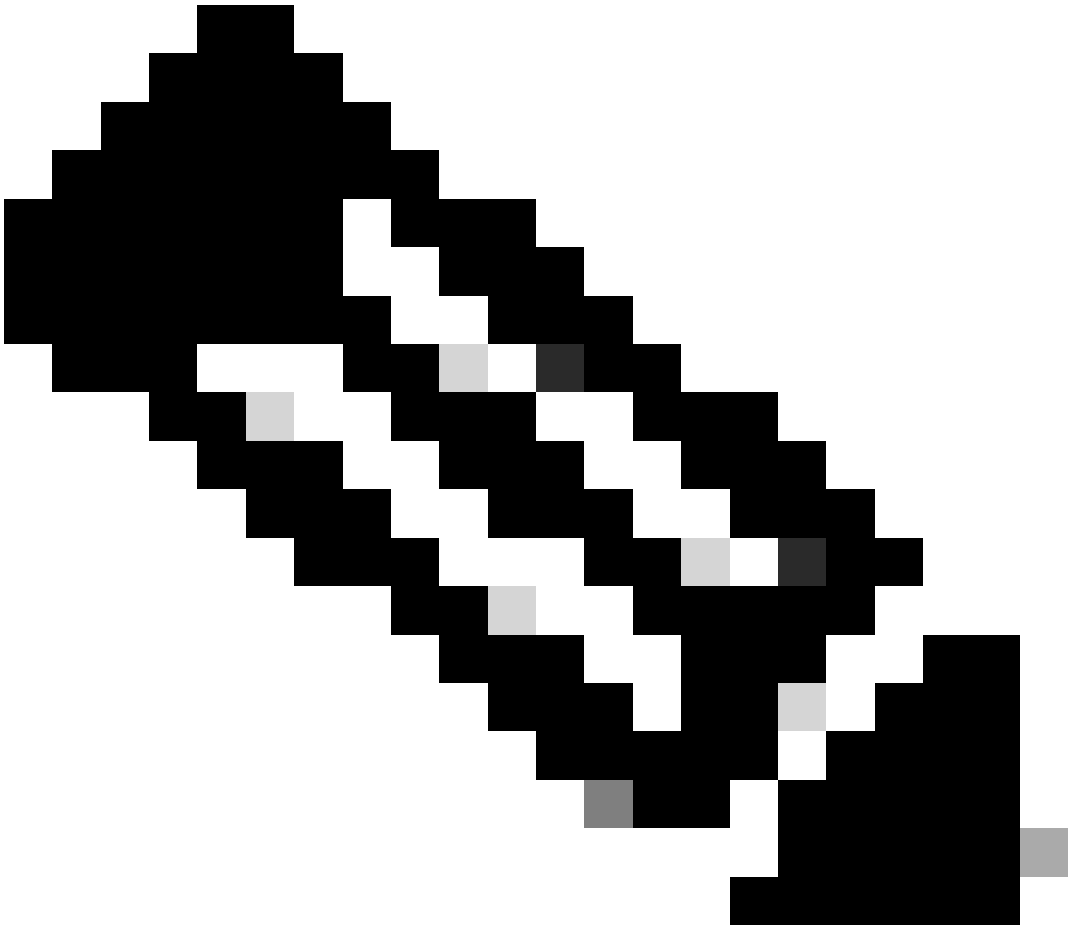
- In dit document wordt ervan uitgegaan dat uw Amazon AWS S3-emmer is geconfigureerd in Umbrella (Instellingen > Logbeheer) en groen wordt weergegeven met recente logs die zijn geüpload. Lees dit artikel voor meer informatie over het configureren van deze functie: Logboeken downloaden van Umbrella Log Management in AWS S3
- Naast de beheerdersrechten voor de QRadar-toestellen, de Amazon S3-configuratie en het Umbrella-dashboard, wordt in deze instructies ervan uitgegaan dat de QRadar-beheerder bekend is met het maken van LSX-bestanden (Log Source Extension).

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht



> Opmerking: de beste methode voor het configureren van QRadar voor gebruik met Cisco Umbrella is via de Cisco Cloud Security App. Ga alleen verder met deze methode als de app niet kan worden geconfigureerd.

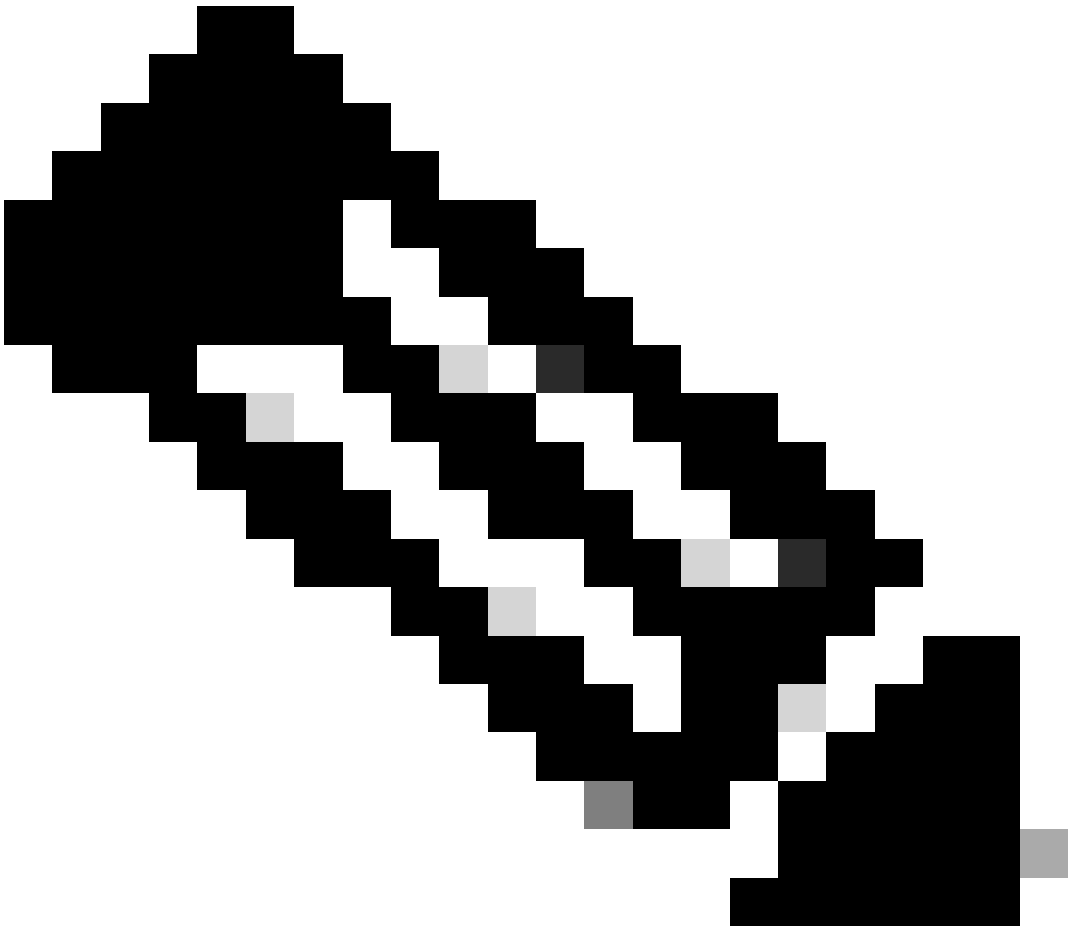
QRadar van IBM is een populaire SIEM voor log-analyse. Het biedt een krachtige interface voor

het analyseren van grote hoeveelheden gegevens, zoals de logs die door Cisco Umbrella worden geleverd voor het DNS-verkeer van uw organisatie.

In dit artikel wordt beschreven hoe u QRadar kunt instellen en uitvoeren, zodat het de logs uit uw S3-emmer kan halen en deze kan consumeren. Er zijn twee hoofdfasen:

- Configureer uw AWS S3-beveiligingsreferenties zodat QRadar toegang heeft tot de logs.
- Configureer QRadar zelf om naar uw emmer te wijzen.

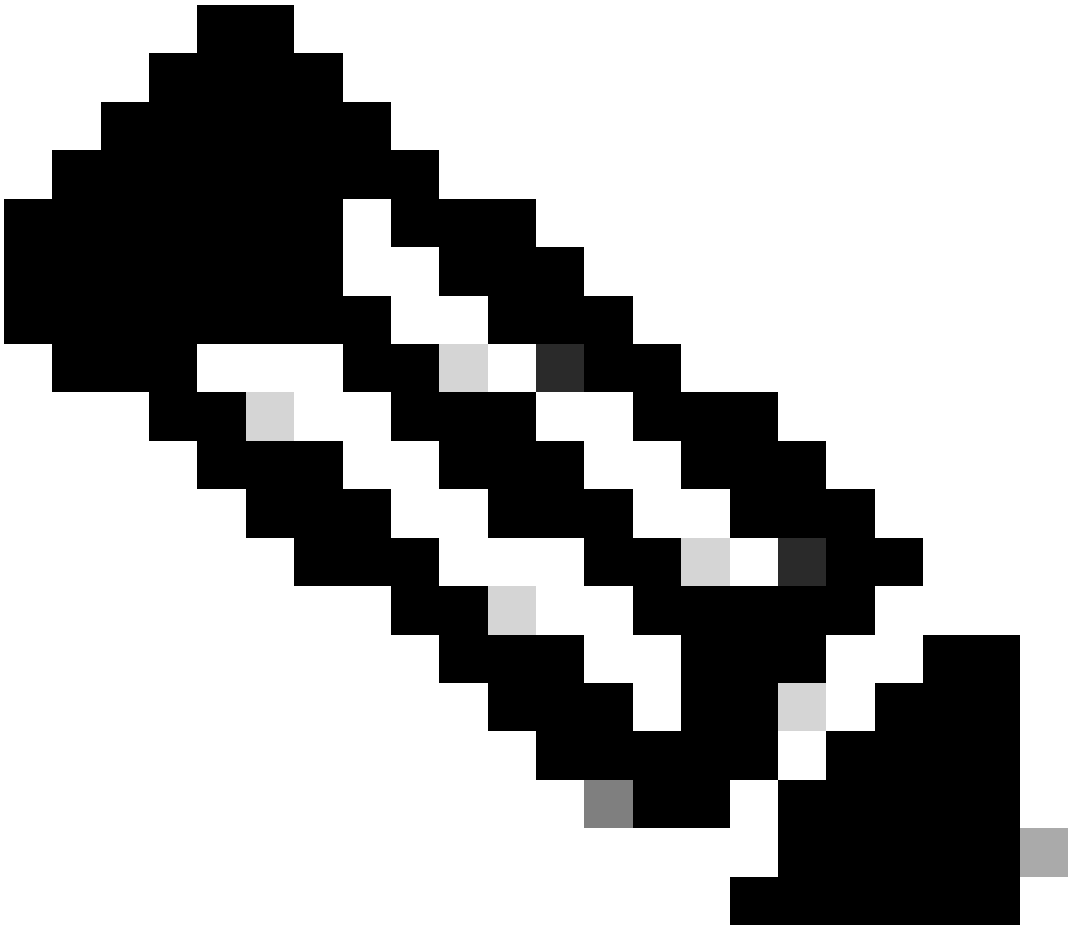
Als u de door Cisco beheerde S3-bucket gebruikt, gebruikt u deze instructies in het artikel Logboeken downloaden van Umbrella Log Management met behulp van de AWS CLI.



Opmerking: deze integratie is getest met zowel door de klant beheerde S3-emmers als door Cisco beheerde S3-emmers. De informatie die in dit artikel wordt besproken, is actueel vanaf dit schrijven (oktober 2019). Het kan veranderen op basis van de manier waarop QRadar en AWS Services interface. Dit document is een levend document. Als u feedback hebt of trucs of tips hebt gevonden die andere klanten kunnen helpen, neem dan contact op met Cisco Umbrella Support.

Ondersteuning voor QRadar moet afkomstig zijn van IBM, omdat Cisco niet in staat is om hardware of software van derden rechtstreeks te ondersteunen. Voor problemen met het aansluiten van uw Umbrella-dashboard op uw S3-emmer kan Cisco Umbrella ondersteuning bieden. Veel van de informatie in dit artikel is ook te vinden op de website van IBM.

Fase 1: Uw 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 (Logboeken downloaden van Umbrella Log Management in AWS S3). Als u deze stappen al hebt uitgevoerd, kunt u overslaan naar fase 2, hoewel u later de beveiligingsreferenties van uw IAM-gebruiker nodig hebt om QRadar naar uw emmer te verifiëren.

Stap 1

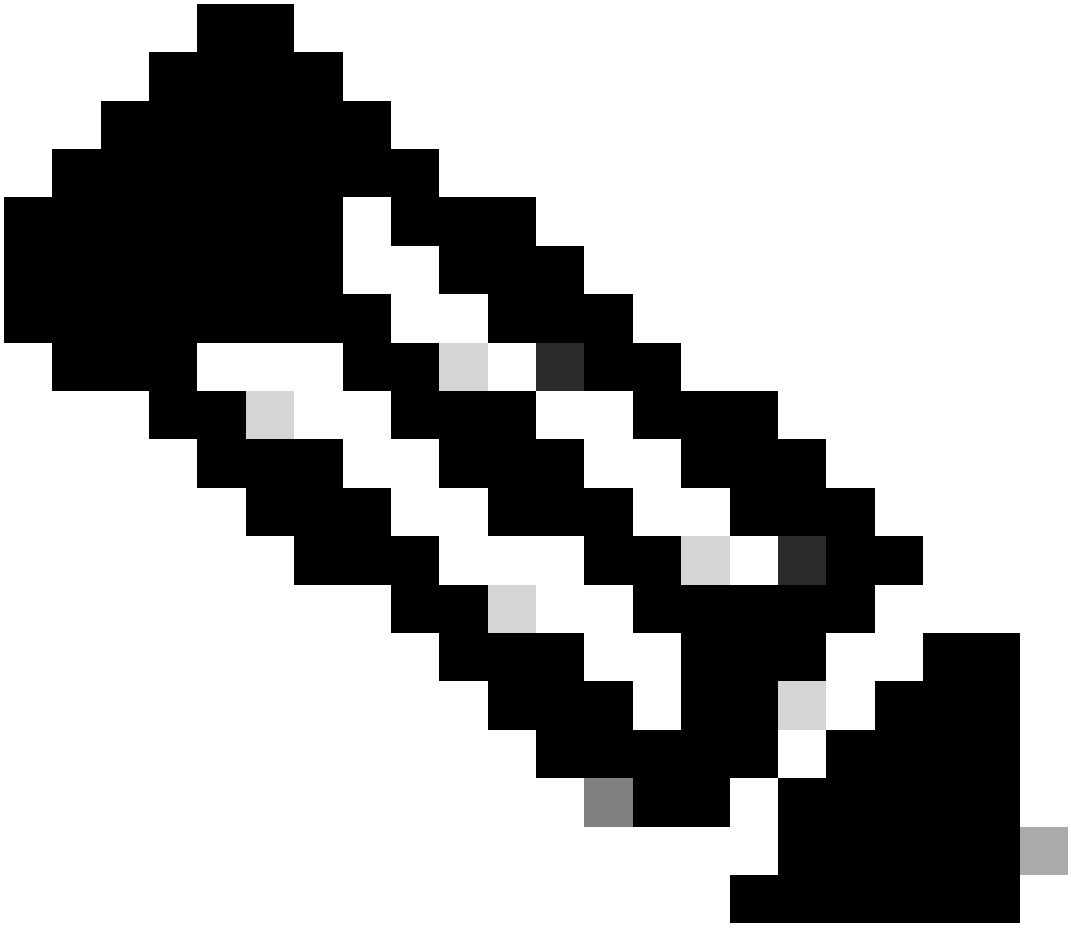
1. Voeg een toegangssleutel toe aan uw Amazon Web Services-account om externe toegang tot uw lokale tool mogelijk te maken en de mogelijkheid te bieden om bestanden in S3 te uploaden, downloaden en wijzigen:

1. Log in bij AWS.
2. Selecteer uw accountnaam in de rechterbovenhoek.
3. Selecteer in de vervolgkeuzelijst Beveiligingsreferenties.

2. U wordt vervolgens 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 hoofdaccount (bijvoorbeeld uw account) is 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 practices, lees de AWS documentatie.

Stap 2

1. Selecteer Aan de slag met IAM-gebruikers om een IAM-gebruiker te maken voor toegang tot uw S3-emmer U wordt vervolgens naar een scherm gebracht waar u een IAM-gebruiker kunt maken.
2. Selecteer Nieuwe gebruikers en vul de velden in.



Opmerking: de gebruikersaccount mag geen spaties bevatten.

3. Na het aanmaken van het gebruikersaccount krijgt u slechts één kans om twee kritieke stukjes informatie te verzamelen die uw Amazon User Security Credentials bevatten. Umbrella suggereert ten zeerste dat u deze downloadt 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 een notitie maakt van zowel uw toegangscode en geheime toegangscode omdat deze in een latere stap vereist zijn.

Stap 3

Voeg vervolgens een beleid toe voor uw IAM-gebruiker, zodat deze toegang heeft tot uw S3-emmer:

1. Selecteer de gebruiker die zojuist is gemaakt en blader omlaag door de eigenschappen van de gebruiker totdat u de knop Beleid toevoegen ziet.

2. Selecteer Beleid koppelen en voer vervolgens "s3" in het filter Beleidstype in. Dit geeft twee resultaten:

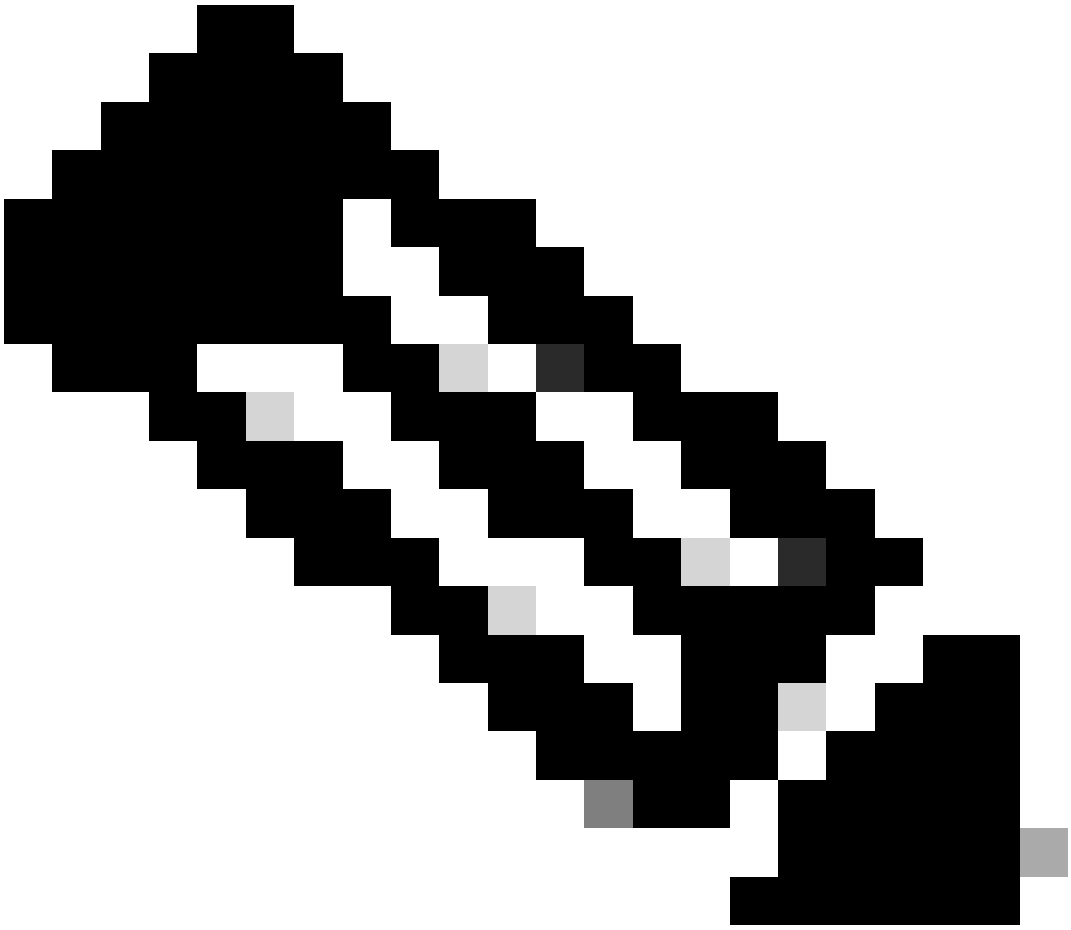
- AmazonS3FullAccess
- AmazonS3ReadOnlyAccess

3. Selecteer AmazonS3FullAccess en selecteer vervolgens Beleid voor bevestigen in de rechterbenedenhoek.

Fase 2: QRadar instellen om DNS-loggegevens uit uw S3-emmer te halen

QRadar maakt gebruik van de AWS CloudTrail-service, een webservice die AWS API-oproepen voor uw account registreert en logbestanden aan u levert.

Voordat QRadar toegang krijgt tot Amazon S3, voltooi deze procedure van IBM om het Amazon-servercertificaat te krijgen. Dit deel is moeilijk, dus zorg ervoor dat u de instructies precies invult.



Opmerking: bij het testen moet u de Firefox-browser gebruiken om dit te laten werken zoals verwacht.

Om het Amazon-servercertificaat te krijgen, moet u het certificaat in DER-indeling verplaatsen naar het juiste QRadar-apparaat. Het QRadar-toestel waarvoor het certificaat vereist is, is het toestel dat is toegewezen in het veld Target Event Collector in de Amazon AWS CloudTrail-logboekbron.

Voordat u begint

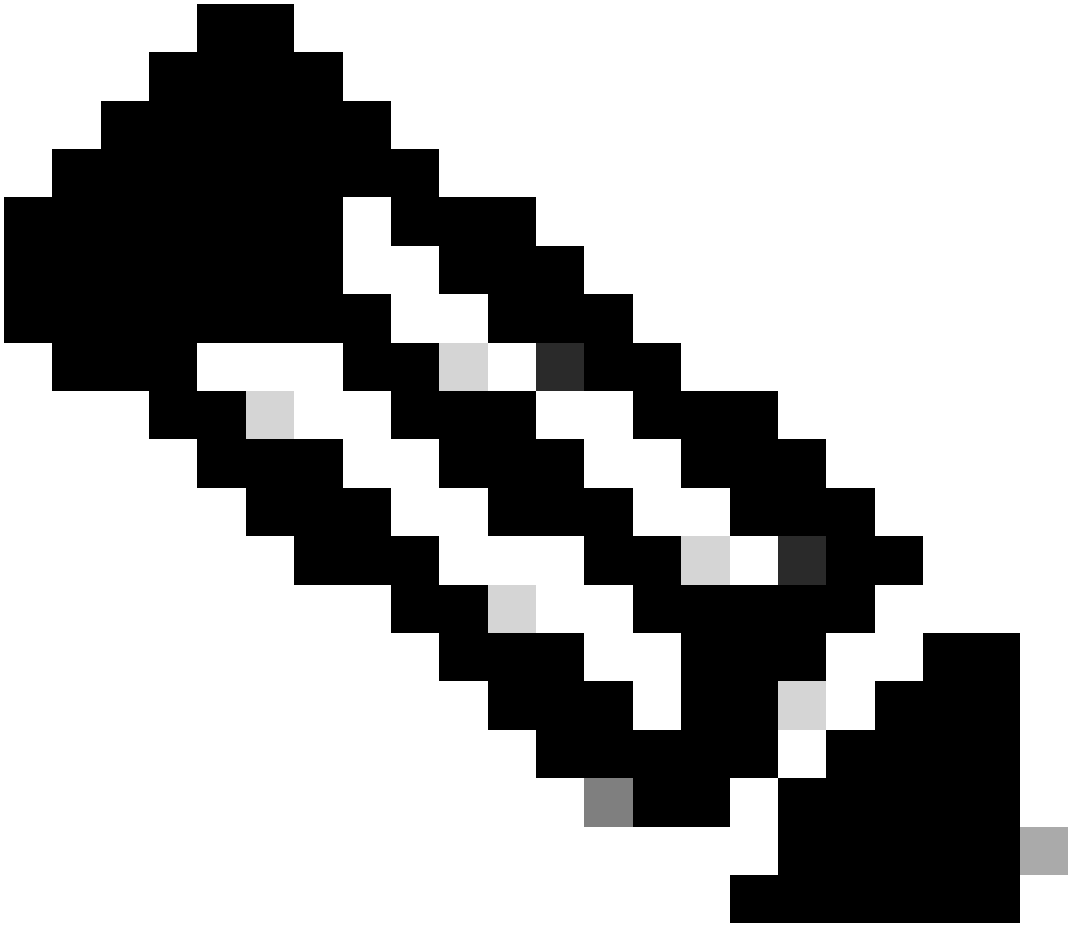
- Het certificaat moet in .DER-formaat zijn.
- De extensie .DER is hoofdlettergevoelig en moet hoofdlettergevoelig zijn.
- Als het certificaat in kleine letters wordt geëxporteerd, kan de logboekbron problemen ondervinden bij het verzamelen van gebeurtenissen.

Eerste stappen

1. Toegang tot uw AWS CloudTrail S3-emmer: `https://<bucketname>.s3.amazonaws.com`

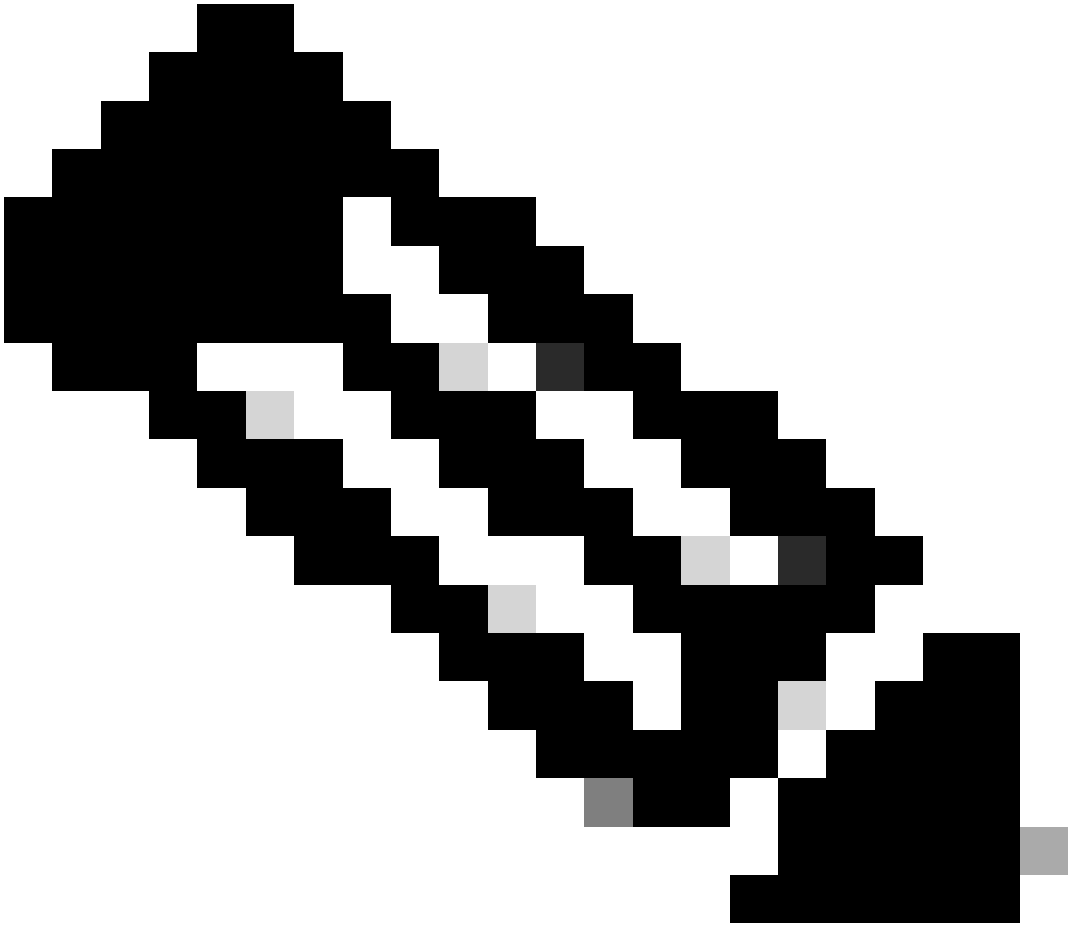
2. Gebruik Firefox om het SSL-certificaat van AWS te exporteren als een (.DER)-certificaat. Firefox kan het vereiste certificaat maken met de extensie .DER:

1. Selecteer het pictogram Site-identiteit (het vergrendelingspictogram in de adresbalk).
2. Selecteer Meer informatie > Certificaat weergeven en selecteer het tabblad Details.
3. Selecteer Exporteren om te exporteren in het certificaat .DER-formaat.



Opmerking: De .DER-extensie is hoofdlettergevoelig en moet hoofdletters zijn.

3. Kopieer het .DER-certificaat naar de directory /opt/QRadar/conf/trusted_certificates van het QRadar-toestel dat de Amazon AWS CloudTrail-logboekbron beheert. U kunt WinSCP gebruiken om het te kopiëren.



Opmerking: het QRadar-toestel dat de logboekbron beheert, wordt geïdentificeerd door het veld Target Event Collect in de Amazon AWS CloudTrail-logboekbron. Het QRadar-apparaat dat de Amazon AWS CloudTrail-logboekbron beheert, moet een kopie van het .DER-certificaat hebben in /opt/QRadar/conf/trusted_certificates.

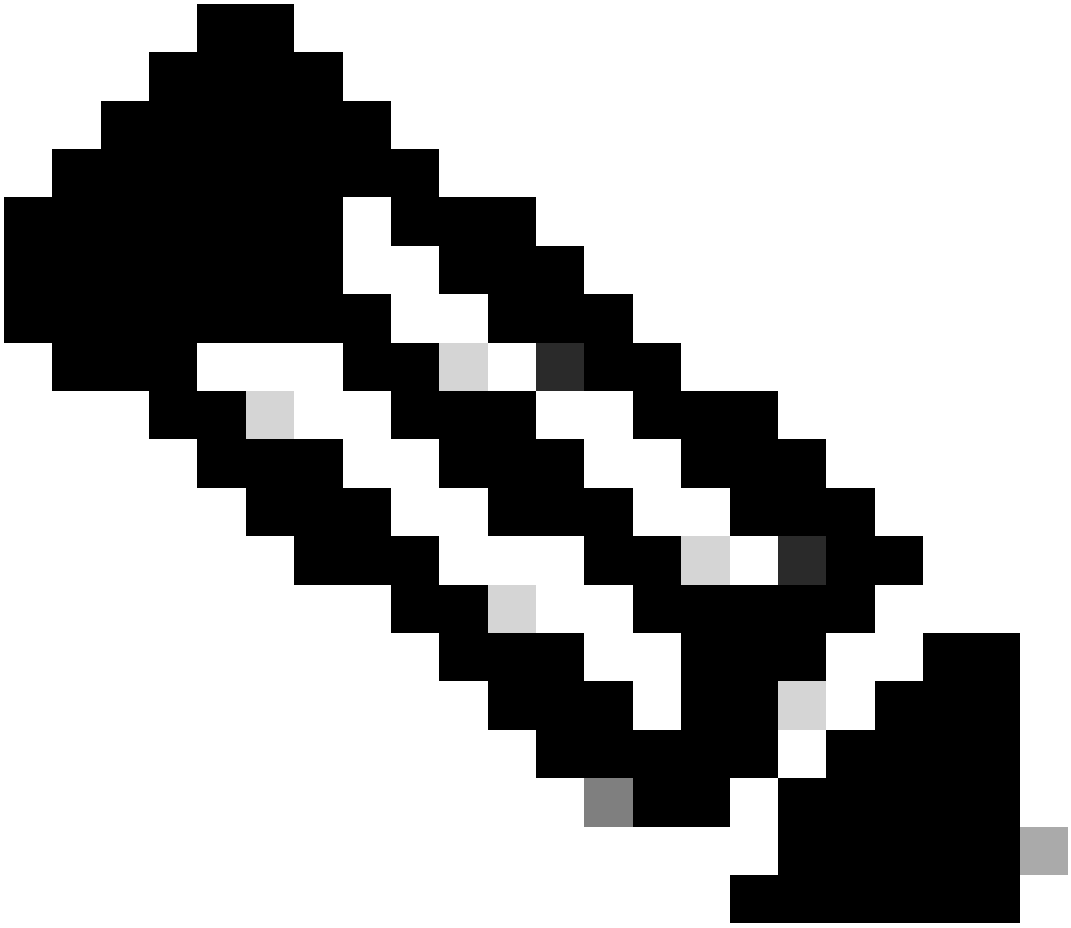
4. Meld u aan bij de gebruikersinterface van QRadar als Administratieve gebruiker.

5. Selecteer het tabblad Beheer.

6. Selecteer het pictogram Logbronnen.

7. Selecteer de logboekbron van Amazon AWS CloudTrail.

8. Selecteer in het navigatiemenu de optie Inschakelen/Uitschakelen om de Amazon AWS CloudTrail-logboekbron uit te schakelen en opnieuw in te schakelen.



Opmerking: wanneer een beheerder de logboekbron van uitgeschakeld naar ingeschakeld dwingt, kan het protocol verbinding maken met de Amazon AWS-bucket zoals gedefinieerd in de logboekbron. Een certificaatcontrole vindt dan plaats als onderdeel van de eerste communicatie.

9. Als u problemen blijft ondervinden, controleert u of het veld Logbronidentificatie de juiste Amazon AWS-bucketnaam bevat en of het pad naar de externe directory correct is in de logbronconfiguratie.

De QRadar-configuratie voltooien

1. Zorg er in QRadar voor dat al uw protocollen, DSM's en andere informatie up-to-date zijn. Selecteer het LogFileProtocol met deze configuraties (uw frequentie, starttijd, herhaling en andere informatie kan verschillen).

2. Voer op het tabblad Logbronnen een logbronnaam en een logbronbeschrijving in. Dit kan zijn wat je maar wilt.

3. Voer uw S3 Bucket Name, uw AWS Access Key, uw AWS Secret Key, en de Remote Directory (waarschijnlijk dnslogs, maar afhankelijk van uw installatie). Het toevoegen van een Logbron-ID zoals het jaar kan helpen bij het filteren, zodat alleen logs met "2019" erin worden getrokken.

4. Maak een LSX (Log Source Extension) die de Cisco Umbrella-gebeurtenissen kan ontleden. (Zo ziet het eruit na de import in QRadar.) Meer informatie over hoe u LSX precies kunt maken, vindt u op de website van IBM. Dit is slechts een voorbeeld. De gegevens die u uit de logboeken wilt halen, variëren afhankelijk van het gebruik.

5. Controleer nogmaals of uw AWS-toegangscode en AWS Secret-sleutel met succes zijn gekopieerd en in de logbronconfiguratie zijn geplakt.

6. Selecteer de GZIP-processor en een gebeurtenisgenerator van op RegEx gebaseerde multiline. De eenvoudigste manier om één gebeurtenis per regel te krijgen, is door een startpatroon van RegEx te gebruiken:

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}:\d{2}","
```

Zorg ervoor dat u de Logbronextensie en Gebruiksvoorwaarde selecteert en sla vervolgens de logboekbron op.

7. Voer een volledige implementatie uit in QRadar.

Uw logboekbron gebruikt vervolgens RestAPI om verbinding te maken met uw emmer met de referenties en sleutels die u hebt verstrekt en begint gebeurtenissen te trekken.

Aanvullende informatie

Bucket-logboekregistratie inschakelen

Om bucketlogging in te schakelen, leest u de AWS-documentatie en voltooit u de beschreven procedures. Logboekregistratie is standaard uitgeschakeld. Eenmaal ingeschakeld, bevindt zich een nieuwe map met de naam /logs in uw bucketroot om u de informatie van GETS, PUTS en DELETES te tonen.

De logboekcyclus beheren

Wanneer u S3 gebruikt, kunt u de levenscyclus van de gegevens in de emmer beheren om de tijdsduur te verlengen waarvoor u logs wilt bewaren. Afhankelijk van het doel waarvoor u het externe logboekbeheer gebruikt, kan de duur erg kort of erg lang zijn. U kunt bijvoorbeeld de logs na 24 uur eenvoudig downloaden uit de S3-emmer en ze offline opslaan, of de logs voor onbepaalde tijd in de cloud bewaren.

Standaard slaat Amazon de gegevens voor onbepaalde tijd op in een emmer, maar onbeperkte opslag verhoogt de kosten van het onderhoud van de emmer. Lees voor meer informatie over de levenscyclus van S3 de AWS-documentatie.

Om de levenscyclus van uw bucket te configureren:

1. Selecteer Eigenschappen **>** Levenscyclus.

2. Selecteer Regel toevoegen en Pas de regel toe op de hele emmer (of een submap als u deze als zodanig hebt geconfigureerd).

3. Selecteer een actie voor objecten, zoals Verwijderen of Archiveren, selecteer vervolgens de tijdsperiode en of u Glacier-opslag wilt gebruiken om uw Amazon-kosten te verlagen. (Glacier is "koude" offline opslag, die, hoewel langzamer toegankelijk, veel goedkoper is.)

Als u logboeken liever op een andere manier beheert (bijvoorbeeld op uw interne back-upoplossing), kunt u de logboeken eenvoudig downloaden van S3 en op een andere manier bewaren.

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.