Gecentraliseerd beheer van overkoepelende logboeken met de S3-service van Amazon voor MSP-, MSSP- en Multi-org-klanten

Inhoud

Inleiding

Dit document beschrijft gecentraliseerd Umbrella-logboekbeheer met de S3-service van Amazon voor MSP-, MSSP- en multi-org-klanten.

Overzicht

De MSP-, MSSP- en Multi-org-consoles hebben de mogelijkheid om de DNS-, URL- en IP-logs van uw klanten offline op te slaan in cloudopslag. De opslag bevindt zich in Amazon S3 en nadat de logs zijn geüpload, kunnen ze worden gedownload en bewaard om nalevingsredenen of beveiligingsanalyse.

Deze documentatie helpt u deze functie te begrijpen, deze in te stellen in zowel uw Umbrella-dashboard als uw Amazon S3-console en verschillende configuratieopties uit te voeren, waaronder de tijdsduur dat u wilt dat de logs in S3 worden bewaard.

Umbrella voor MSP, MSSP en Multi-Org hebben allemaal de mogelijkheid om de verkeersactiviteitslogs van de kinderorganisaties van de console te uploaden en die logs in de cloud op te slaan. Amazon's AWS S3 (Simple Storage Service) is de service die logboeken archiveert en soms wordt aangeduid als offline opslag of als islog-retentie

Het archiveren van logs kan om verschillende redenen nuttig zijn, afhankelijk van uw behoefte. Voor sommige mensen kunnen de geëxporteerde en gearchiveerde logs worden geïmporteerd in data-analyse of forensische beveiligingstools, zoals SIEM's. Voor anderen kan een archief van activiteitenlogboeken nuttig zijn voor forensische gegevensverwerking in het geval van een beveiligingsincident of personeelsdossiers.

AWS S3 slaat logs op in een gecomprimeerd (gzip) archief in CSV-formaat. Omdat logboeken elke tien minuten worden geüpload, is er een minimale vertraging van tien minuten tussen netwerkverkeer dat van uw netwerk komt, geregistreerd door Umbrella en vervolgens beschikbaar gesteld om te downloaden van S3.

Het orgID-nummer van de console

Elke klantorganisatie uploadt hun logs afzonderlijk, met behulp van het orgID-nummer van de console om elke klant aan een map toe te wijzen. De functie kan ook per klant / per organisatie worden in- of uitgeschakeld.

Twee soorten Umbrella Log Management

Logbeheer wordt uitgevoerd door het uploaden van logs naar wat wordt genoemd een isbucketit is (in wezen een map binnen AWSit iss S3 omgeving). Er zijn twee manieren om een emmer te hosten voor uw Umbrella-logs:

- Beheerd, beheerd en betaald door u, de beheerder van het bedrijf.
- Beheerd, beheerd en betaald door Cisco Umbrella.

Er zijn voor- en nadelen aan het hebben van Cisco om uw S3-bucket te beheren.

De voordelen van Cisco voor het beheren van uw bucket:

- Zeer eenvoudig in te stellen. Het duurt slechts een paar minuten en daarna is het zeer eenvoudig te beheren.
- Cisco bucket-management is inbegrepen in uw licentiekosten met Umbrella, waardoor de service effectief gratis is. Hoewel het goedkoop is om je eigen emmer te hebben, kunnen de overheadkosten van het beheren van een andere rekening onbetaalbaar zijn.

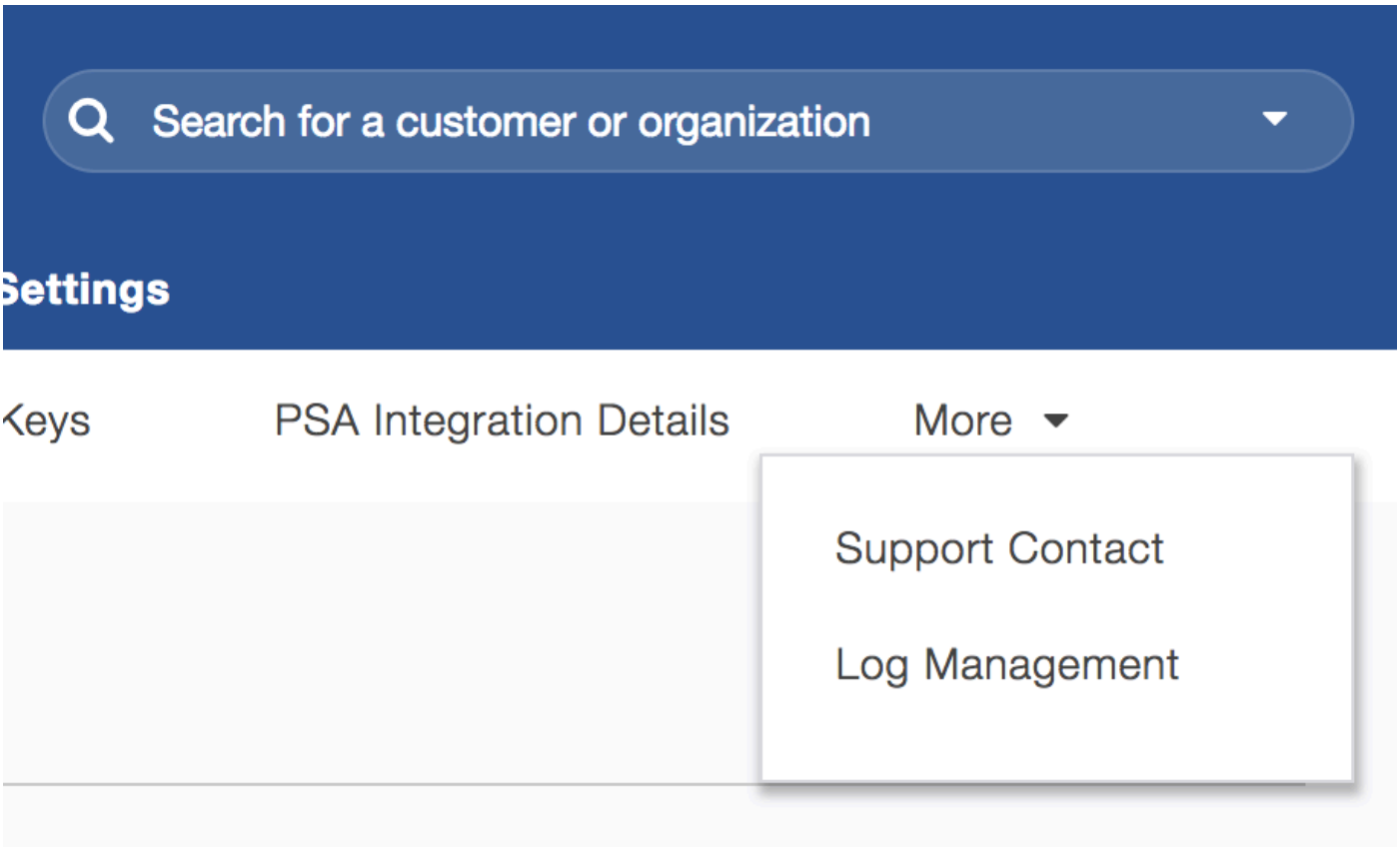
De voordelen van het zelf beheren van een S3-exemplaar:

- Er is geen beperking op hoe lang gegevens offline kunnen worden opgeslagen. Cisco beperkt offline opslag tot maximaal 30 dagen.
- U kunt alles aan uw emmer toevoegen, inclusief logbestanden van Umbrella, zodat de emmer ook door andere toepassingen kan worden gebruikt.
- U kunt rechtstreeks ondersteuning krijgen van Amazon voor geavanceerde configuratiehulp, zoals automatisering of hulp bij de opdrachtregel.

Voor de meeste klanten zijn de kosten van het onderhouden van een emmer erg goedkoop, maar kunnen ze lastig blijken te zijn.

Aan de slag

De functie Logbeheer is te vinden in de console onder Instellingen > Logbeheer (u kunt op de vervolgkeuzelijst klikken).



115012963103

Een zelfbeheerde S3-emmer configureren

Voorwaarden

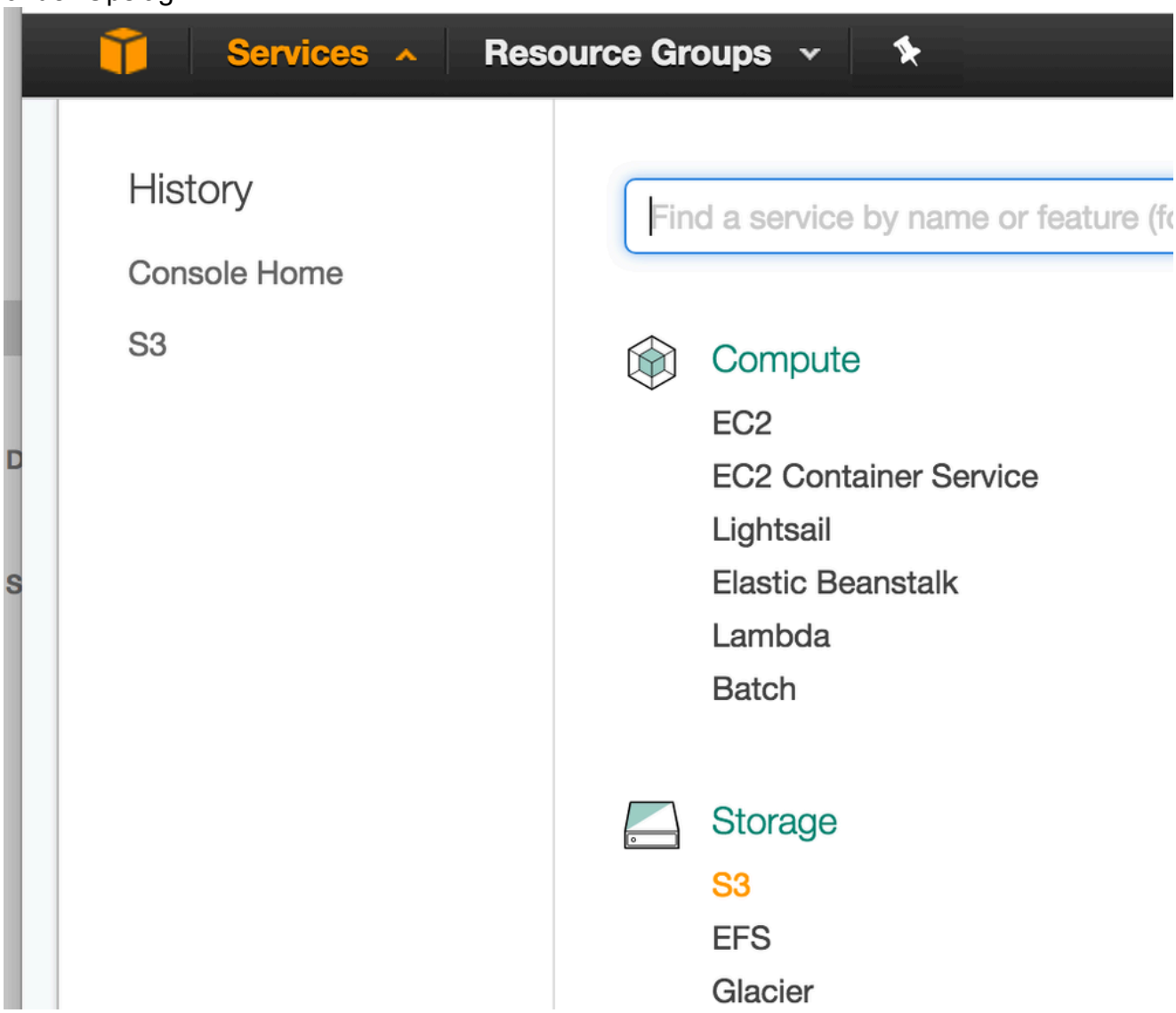
Om logboeken te archiveren, moet u aan de volgende vereisten voldoen:

- Volledige administratieve toegang tot de Cisco Umbrella MSP, MSSP of Multi-org Console.
- Een aanmelding bij Amazon AWS-service (https://aws.amazon.com/console/). Als je geen account hebt, biedt Amazon gratis aanmelding voor S3. Ze hebben echter een creditcard nodig voor het geval uw gebruik groter is dan het gebruik van het gratis abonnement.
- Een bucket geconfigureerd in Amazon S3 voor logboekopslag. Zie de volgende sectie voor instructies over het configureren en instellen van de Amazon S3-emmer.

Het opzetten van uw Amazon S3 Bucket

1. Begin door u aan te melden bij de AWS-console en selecteer "S3" in de lijst met opties

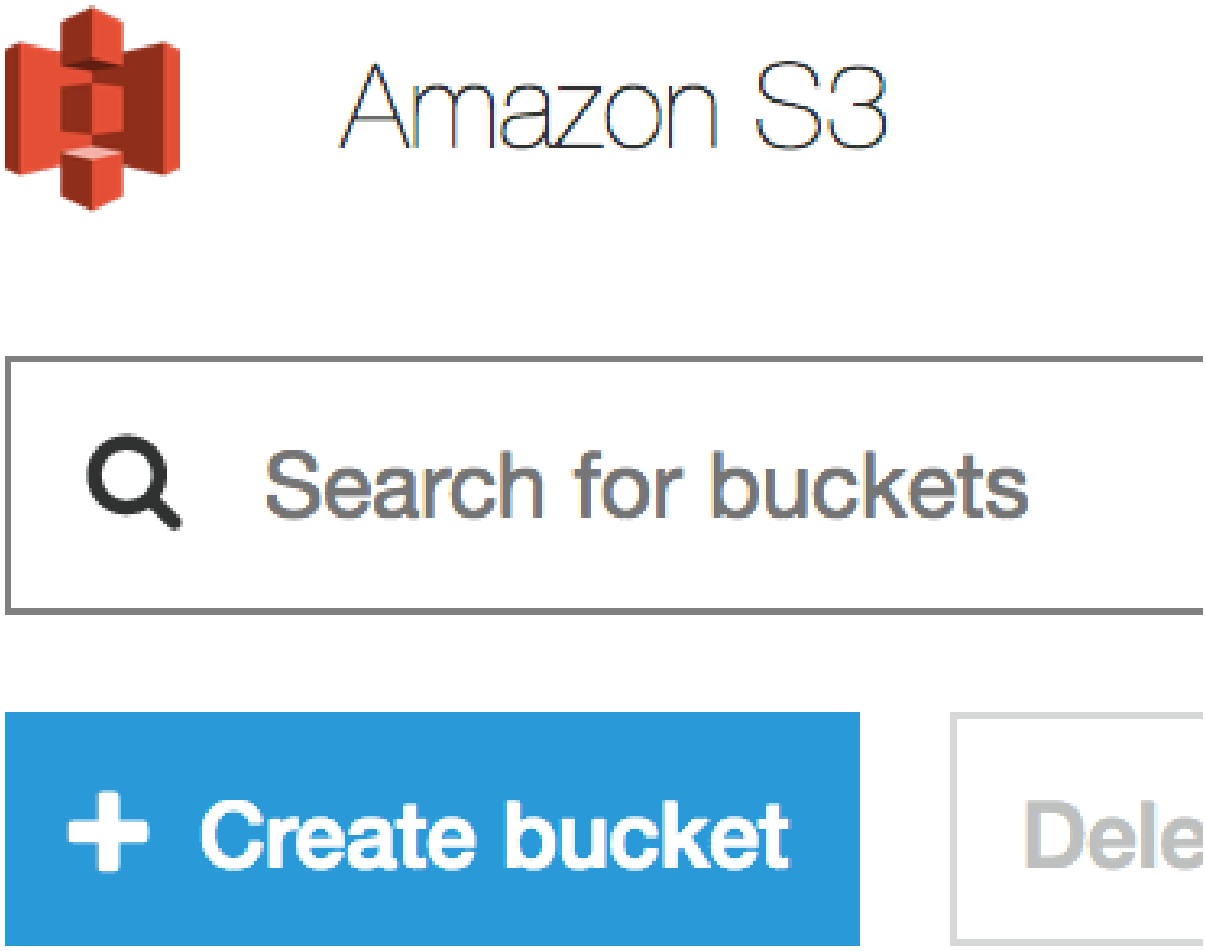
onder Opslag.



115012842106

2. U ziet een introductiescherm dat u verwelkomt in het Amazon Simple Storage System

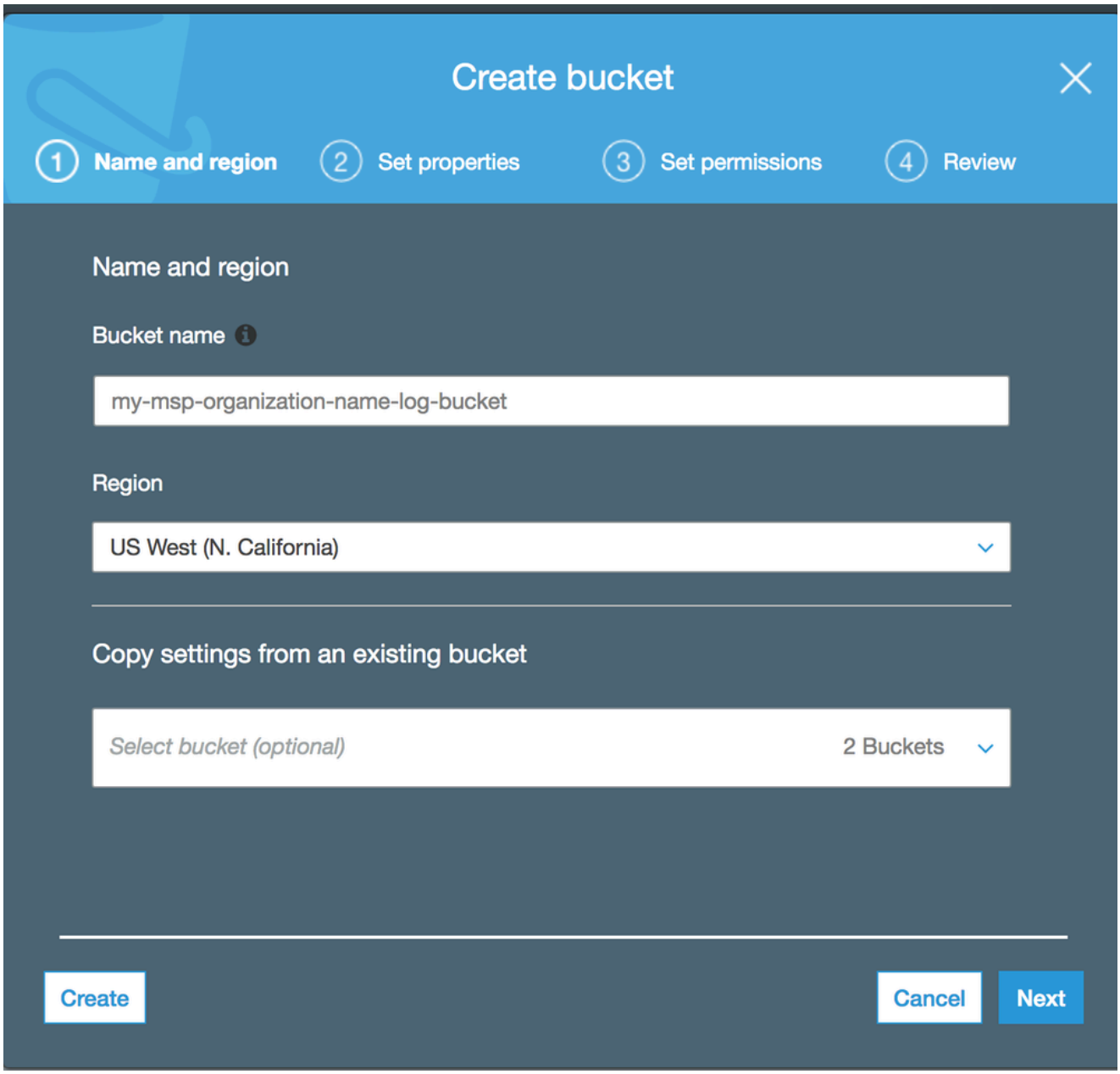
3. Als je nog geen bucket hebt, wil je er een maken. Klik op de knop Bucket maken



115012842326

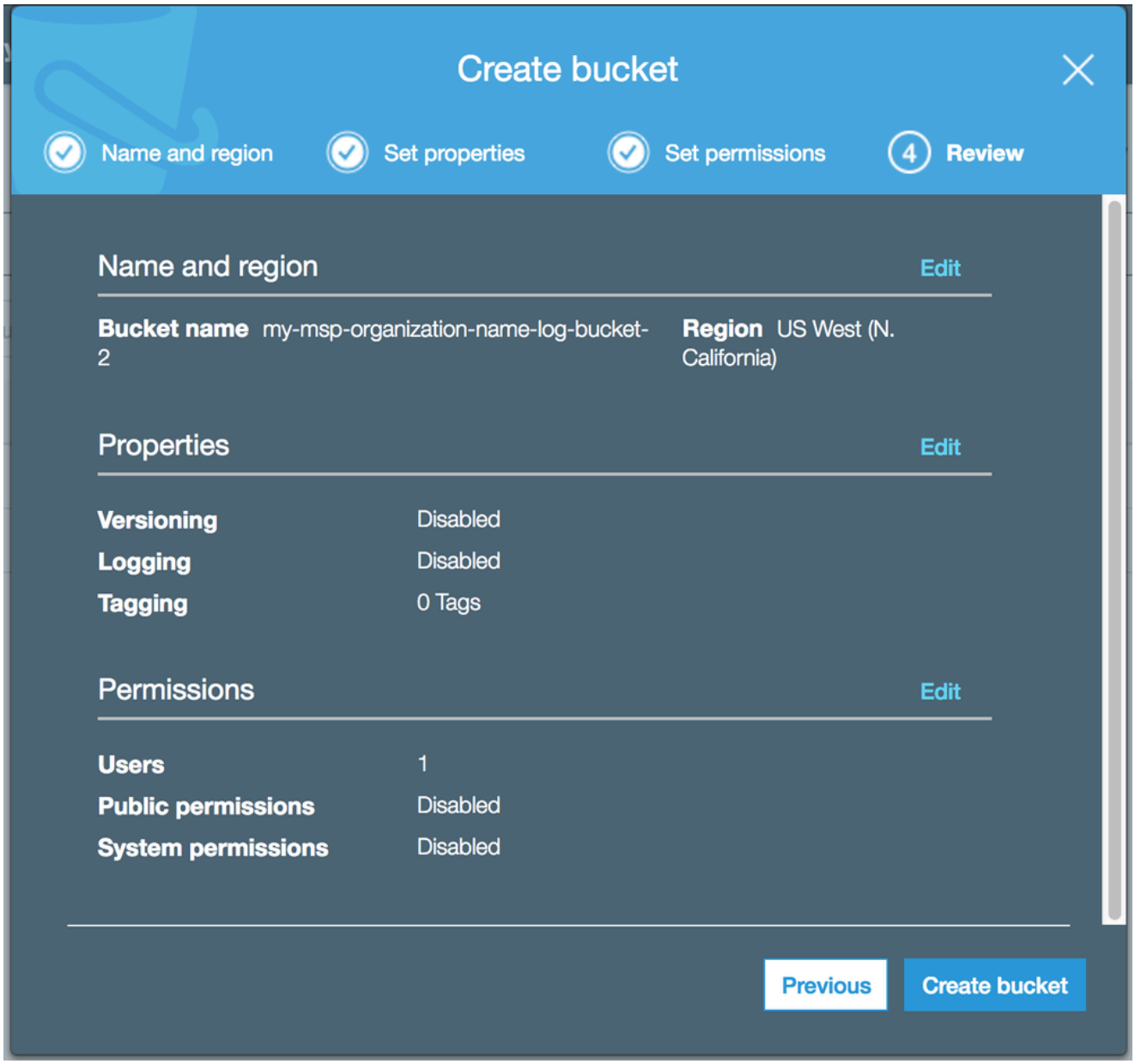
.

4. Begin met het invoeren van een Bucket Name
   De naam van de emmer moet universeel uniek zijn, niet alleen voor uw AWS of uw paraplu, maar voor alle Amazon AWS. Het gebruik van iets persoonlijks, zoals "mijn-organisatienaam-log-bucket" kan u helpen de vereiste voor universeel unieke bucketnaam te omzeilen. De naam van de bucket mag alleen kleine letters gebruiken en mag geen spaties of perioden bevatten en moet voldoen aan de DNS-naamgevingsconventies. Voor meer informatie over naamsbeperkingen, lees hier. Voor meer informatie over het maken van buckets, inclusief naamgeving, lees hier.



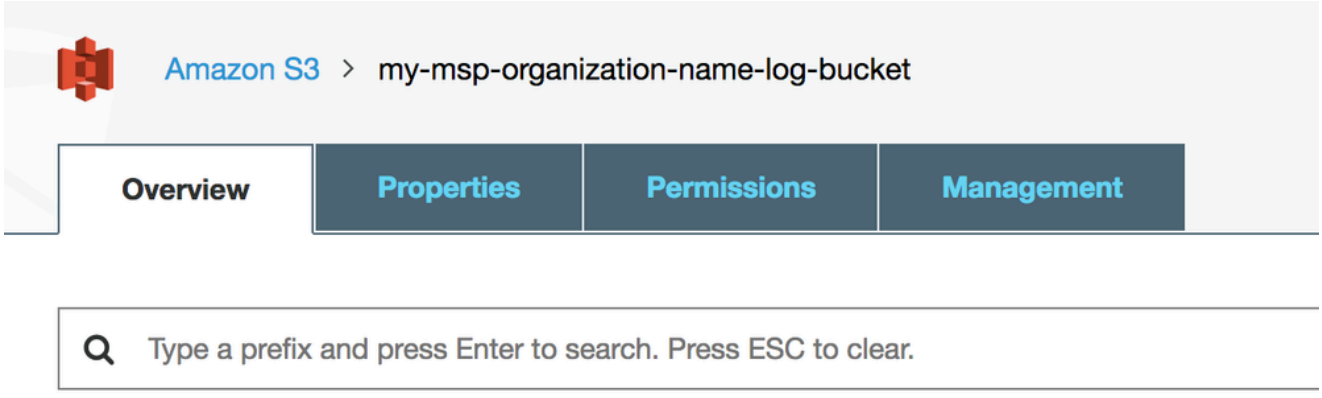
115013010503

5. Selecteer de regio die het beste werkt voor uw locatie en klik op Maken. Kopieer de instellingen niet van een andere emmer
6. Klik in de stap "Eigenschappen instellen" op Volgende. Deze kunnen later worden aangepast
7. Klik in de stap "Rechten instellen" op Volgende. We gaan de machtigingen later opnieuw bekijken om de emmer voor uploaden in te stellen
8. Voltooi het controleproces en klik op Emmer maken



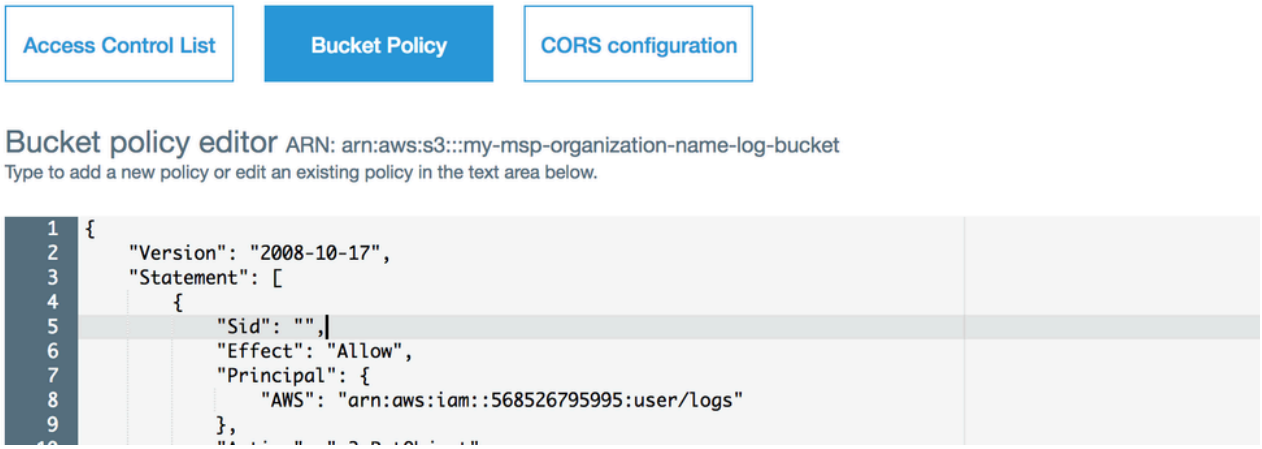
115012842686

9. Vervolgens moet u de emmer configureren om uploads van de Umbrella Service te accepteren. In S3 wordt dit een bucket policy genoemd. Klik op de naam van uw nieuw geconfigureerde emmer en selecteer vervolgens het tabblad Rechten boven aan de interface



115012842906

10. Selecteer Bucket Policy en vervolgens wordt u gevraagd om in de bucket te plakken



115012843006

11. Kopieer en plak de onderstaande JSON-tekenreeks, die het bucketbeleid bevat, naar een teksteditor of plak deze gewoon in het venster. Vervang uw exacte bucketnaam waar bucketname hieronder wordt gespecificeerd. Als u dit niet doet, verschijnt er een foutmelding

{
"Version": "2008-10-17",
"Verklaring": [
{
"SID": "",
"Effect": "Toestaan",
"Opdrachtgever": {
"AWS": "arn:aws:iam::568526795995:user/logs"
}
"Actie": "s3: PutObject",
"Resource": "arn:aws:s3::bucketname/*"
}
{
"SID": "",
"Effect": "Deny",
"Opdrachtgever": {
"AWS": "arn:aws:iam::568526795995:user/logs"
}
"Actie": "s3: GetObject",
"Resource": "arn:aws:s3::bucketname/*"
}

{
"SID": "",
"Effect": "Toestaan",
"Opdrachtgever":

{ "AWS": "arn:aws:iam::568526795995:user/logs" }

,
"Actie": "s3: GetBucketLocation",
"Resource": "arn:aws:s3::bucketname"
}

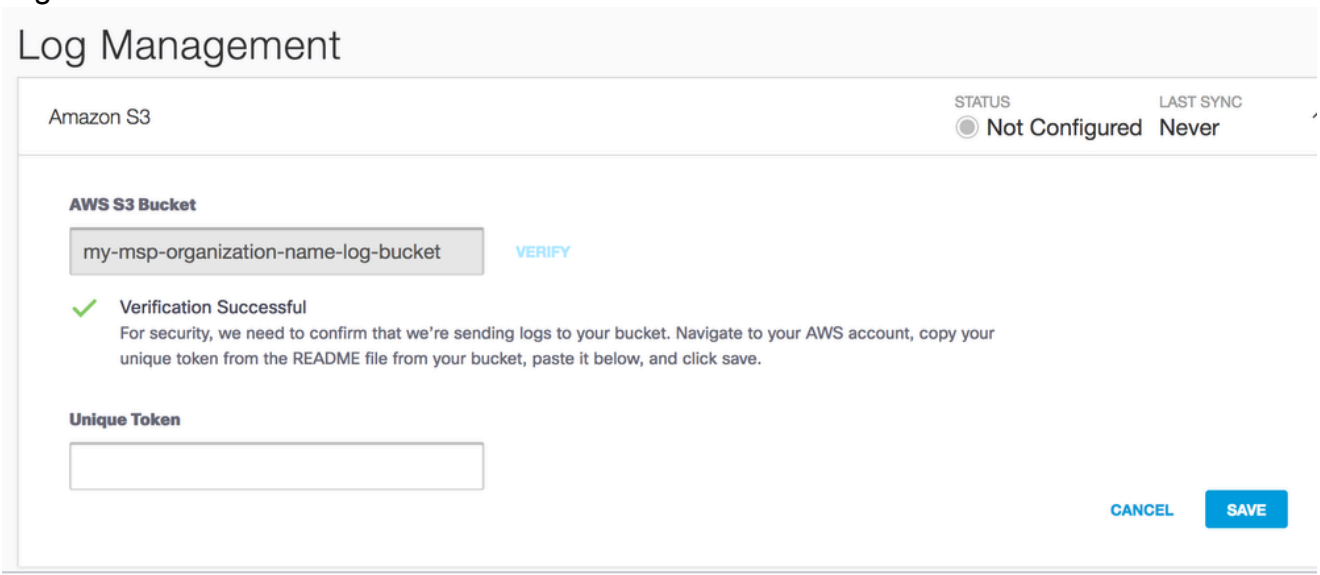
{
"SID": "",
"Effect": "Toestaan",
"Opdrachtgever": {
"AWS": "arn:aws:iam::568526795995:user/logs"
}
"Actie": "s3: ListBucket",
"Resource": "arn:aws:s3::bucketname"
}
]
}

12. Klik op Opslaan om deze wijziging te bevestigen

Uw Amazon S3-emmer verifiëren

Stap 1:

1. Ga terug naar je Umbrella Console en navigeer naar Instellingen > Logbeheer
2. Klik op "Amazon S3" om het venster uit te vouwen
3. Typ of plak in het veld Bucketnaam de exacte bucketnaam die u in S3 hebt gemaakt en klik op Verifiëren
   U ontvangt een bevestigingsbericht in uw dashboard dat aangeeft dat de emmer met succes is geverifieerd.



115012847146

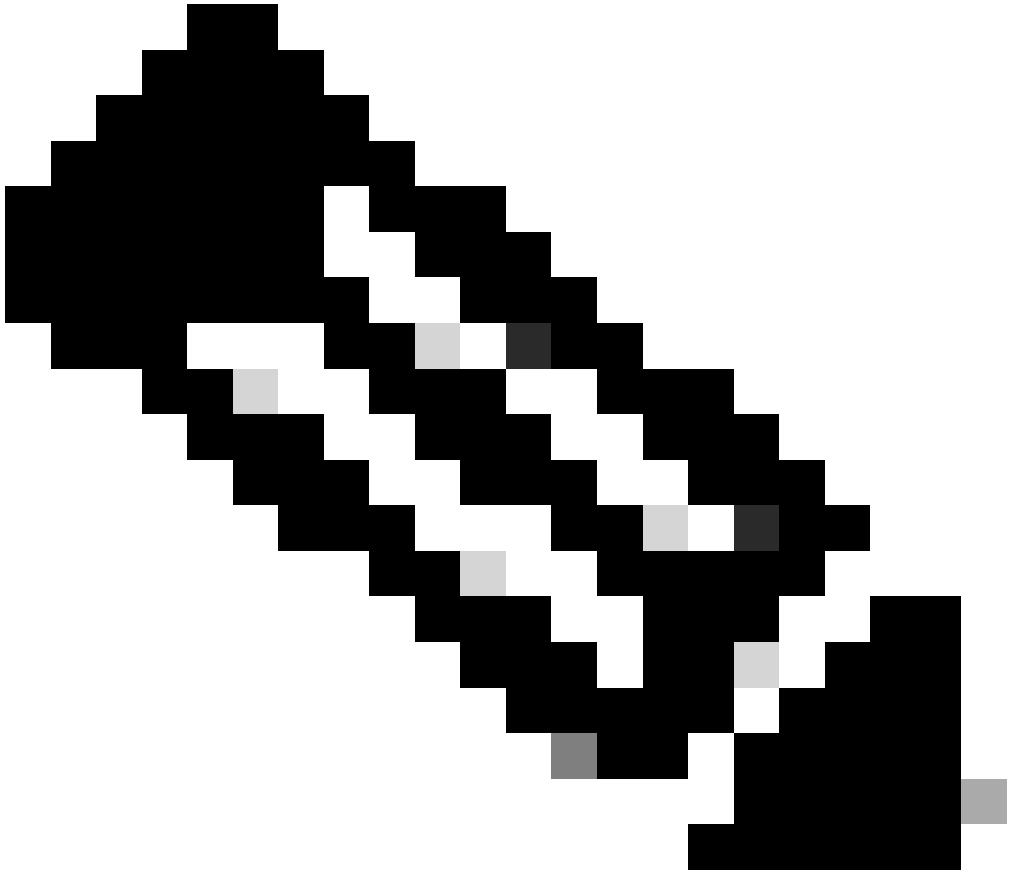
Als u een fout ontvangt die aangeeft dat uw bucket niet kon worden geverifieerd, controleert u de syntaxis van de bucketnaam opnieuw en bekijkt u de configuratie. Als er problemen blijven

bestaan, kunt u een kwestie openen bij onze ondersteuningsafdeling

Stap 2:

Als secundaire voorzorgsmaatregel om ervoor te zorgen dat de juiste emmer is opgegeven, vraagt Umbrella u om een unieke activeringstoken in te voeren. De activeringstoken kan worden verkregen door uw S3-emmer opnieuw te bekijken. Als onderdeel van het verificatieproces werd een bestand met de naam README_FROM_UMBRELLA.txt geüpload van Umbrella naar uw Amazon S3-emmer en wordt daar weergegeven.

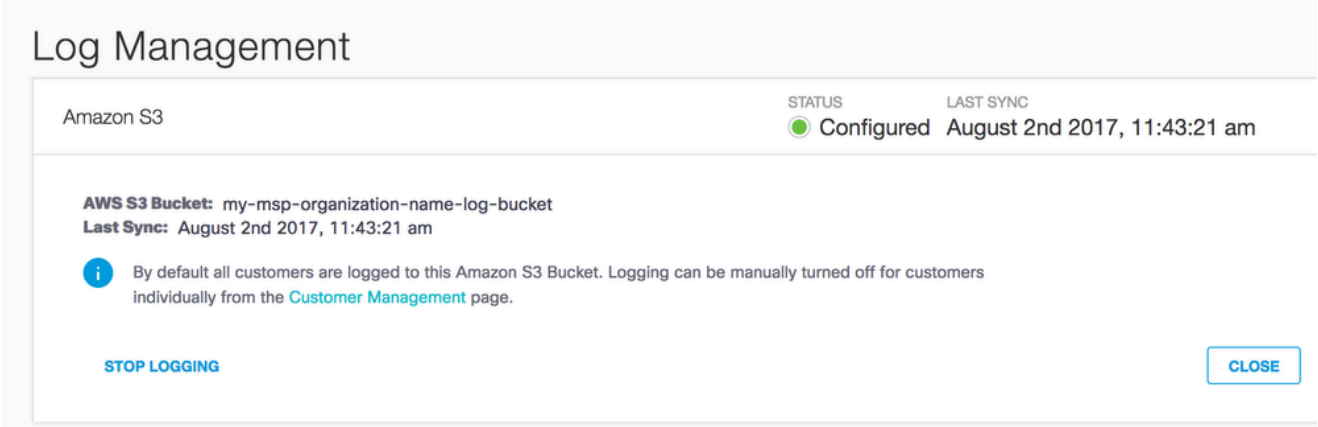
1. Download het readme-bestand door erop te dubbelklikken en open het vervolgens in een teksteditor. In het bestand is er een uniek token dat uw S3-emmer aan uw Umbrella-dashboard bindt



Opmerking: Mogelijk moet u uw S3-emmer in de browser vernieuwen om het README-bestand te zien nadat het is geüpload.

2. Ga terug naar het Umbrella-dashboard en plak de token in het veld met het label "Unique token" en klik vervolgens op Opslaan. Op dit moment is de configuratie voltooien. Klik op de naam van Amazon S3 in het gedeelte Logbeheer om uw configuratie te

bekijken



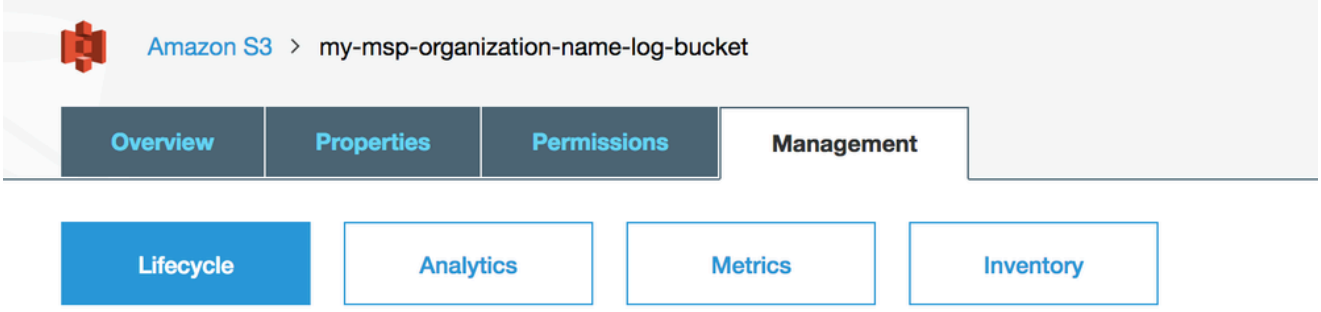
115012848126

De levenscyclus van het logboek 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 de reden waarom u het externe logbeheer 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. Voor meer informatie over de levenscyclus van S3, lees hier.

Om de levenscyclus van uw bucket te configureren:

1. Selecteer Beheer en klik op levenscyclus



115012848246

2. Klik op Regel toevoegen en vervolgens op Regel toepassen 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. (Gletsjer is het iscoldit is off-line opslag, die hoewel langzamer toegankelijk, goedkoper is.)

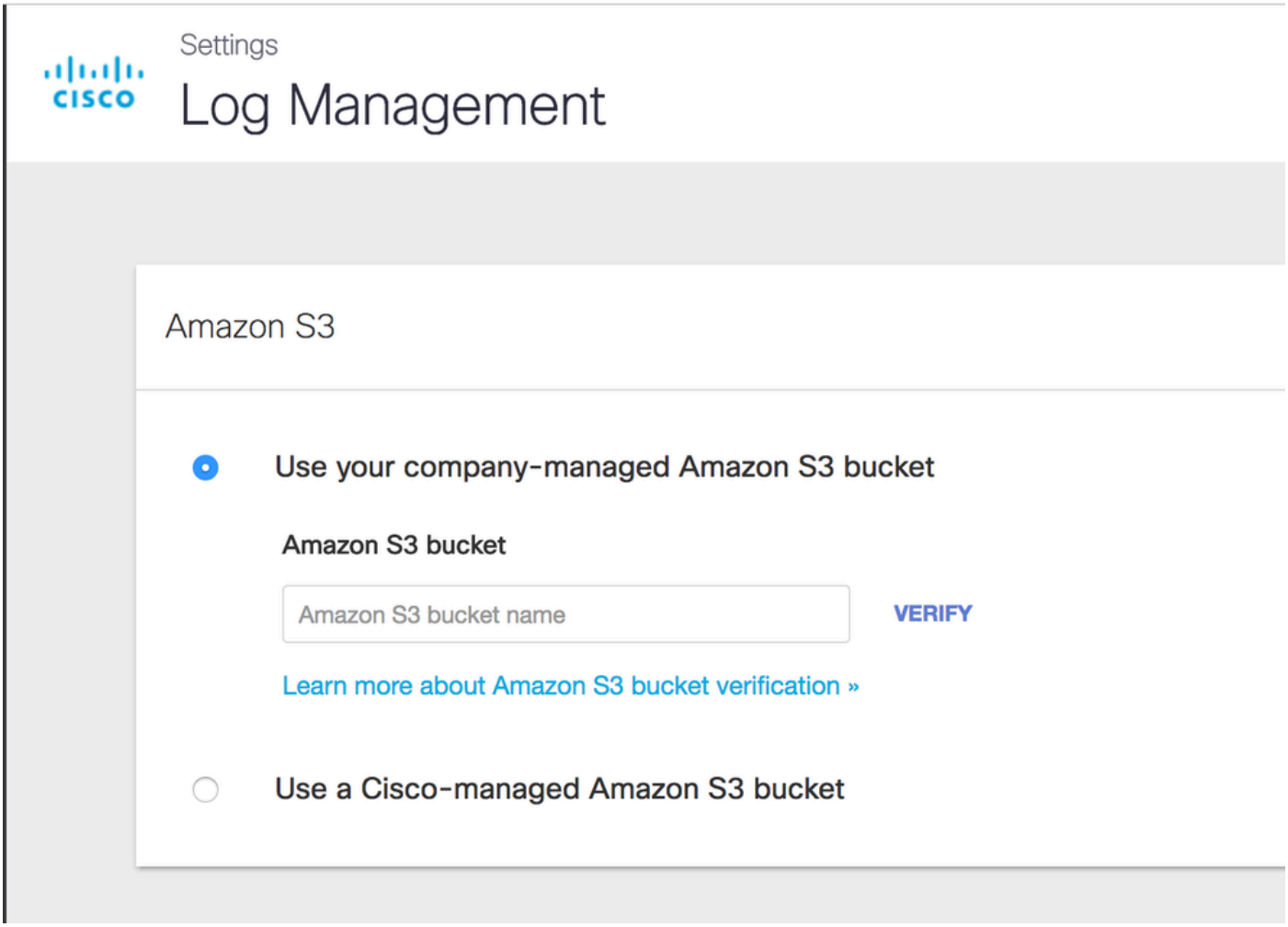
4. Als u logs liever met een andere methode beheert (zoals uw interne back-upoplossing), kunt u de logs eenvoudig downloaden van S3 en ze op een andere manier bewaren en vervolgens uw retentietijd instellen op een paar dagen.

Een door Cisco beheerde S3-bucket configureren

Navigeer naar Instellingen > Logboekbeheer in uw Umbrella-dashboard.

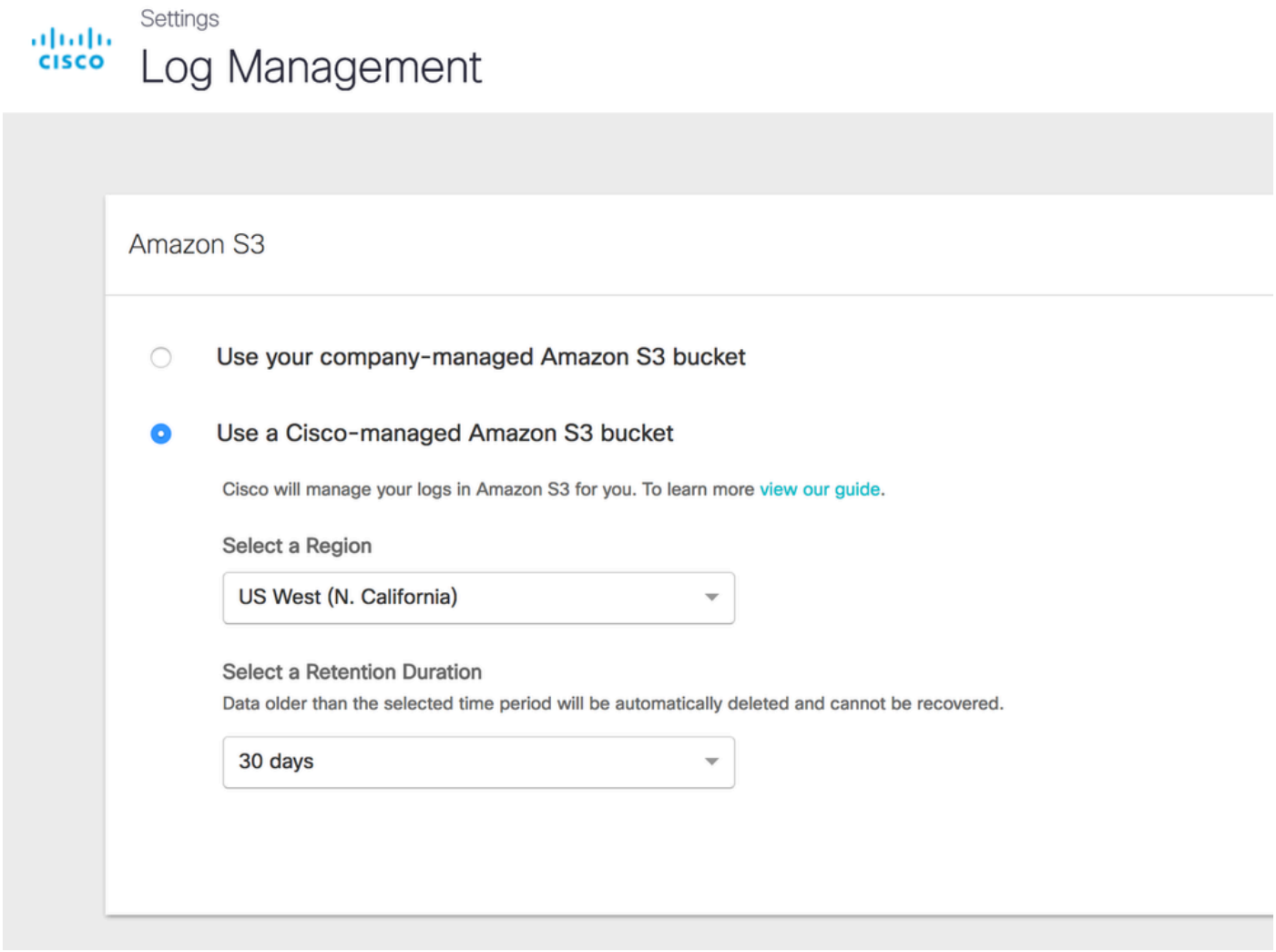
Er zijn twee opties:

- Gebruik uw door het bedrijf beheerde Amazon S3-emmer
- Gebruik een door Cisco beheerde Amazon S3-bucket



25231151138964

Kies "Gebruik een door Cisco beheerde Amazon S3-emmer" en u krijgt twee nieuwe opties: "Selecteer een regio" en "Selecteer een retentieduur".



25231151158036

Selecteer een regio

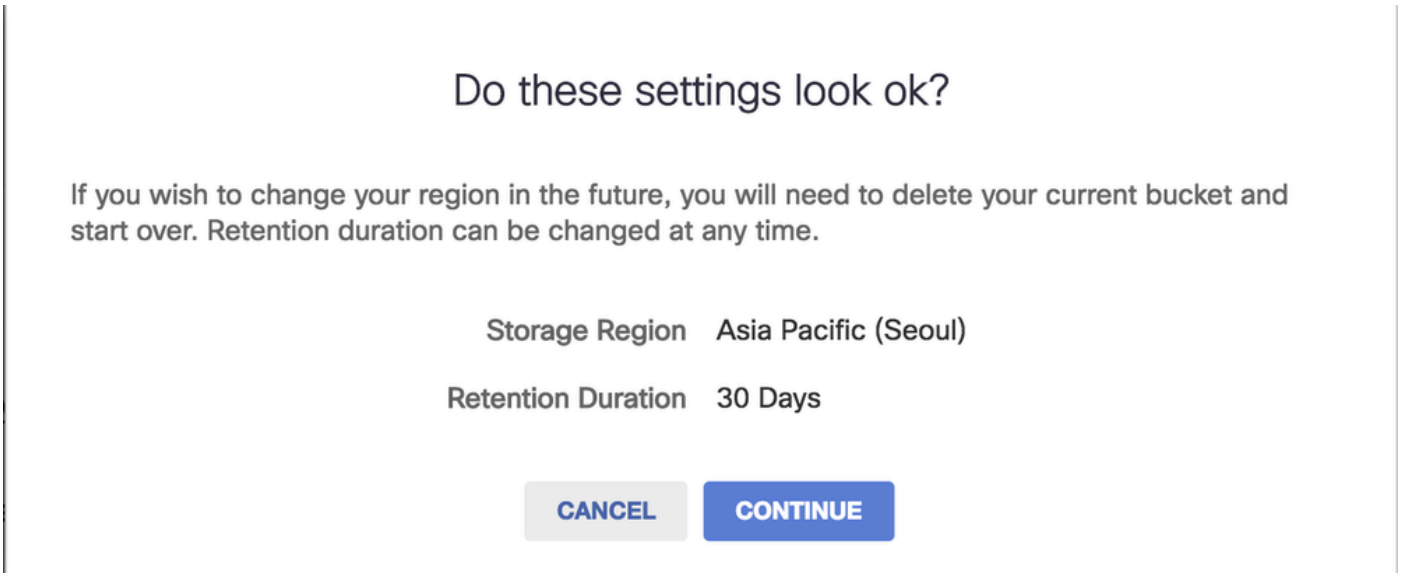
Regionale eindpunten zijn belangrijk om de latentie bij het downloaden van logs naar uw servers te minimaliseren. De vermelde regio's komen overeen met de regio's die beschikbaar zijn in Amazon S3, maar niet alle regio's zijn beschikbaar. China staat niet op de lijst.

Kies de regio die het dichtst bij u in de buurt is van de drop-down. Als u uw regio in de toekomst wilt wijzigen, moet u uw huidige instellingen verwijderen en opnieuw beginnen.

Selecteer een retentieduur

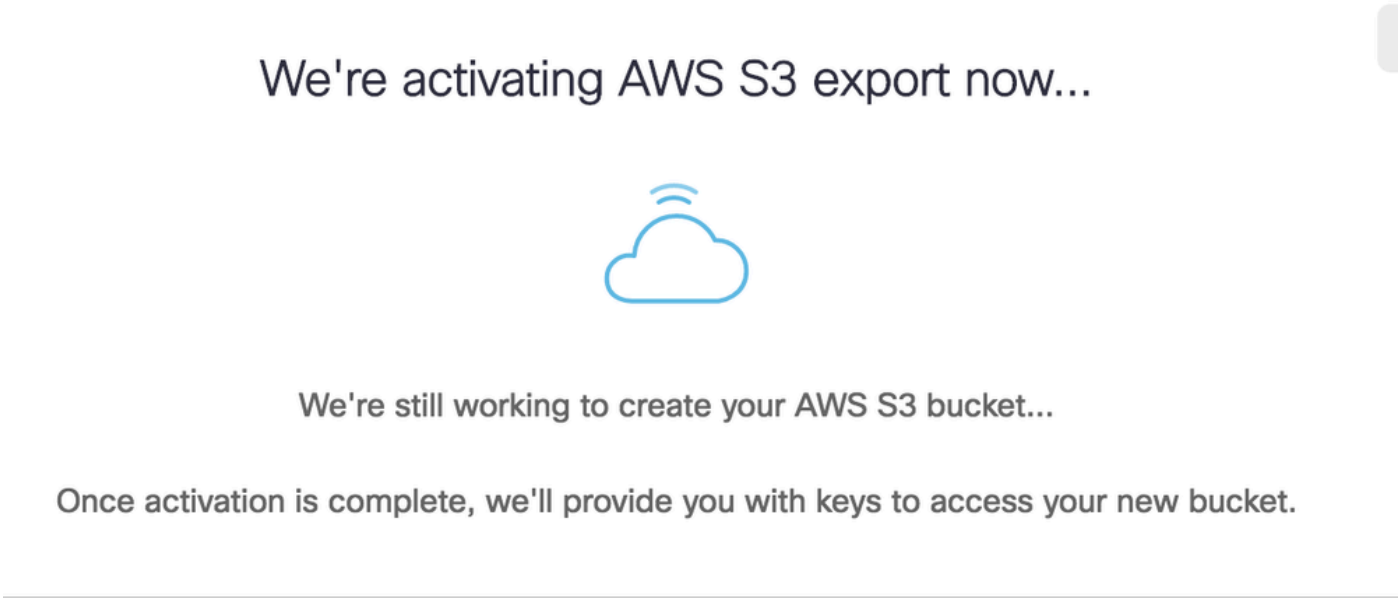
De bewaartermijn is 7, 14 of 30 dagen. Na de geselecteerde periode worden alle gegevens gewist en kunnen ze niet worden opgehaald, wat er ook gebeurt. We raden een kortere periode aan als uw innamecyclus regelmatig is. De bewaartermijn kan op een later tijdstip worden gewijzigd.

Nadat u uw selecties hebt gemaakt, klikt u op Volgende en wordt u gevraagd uw regio en duur te bevestigen



25231181211796

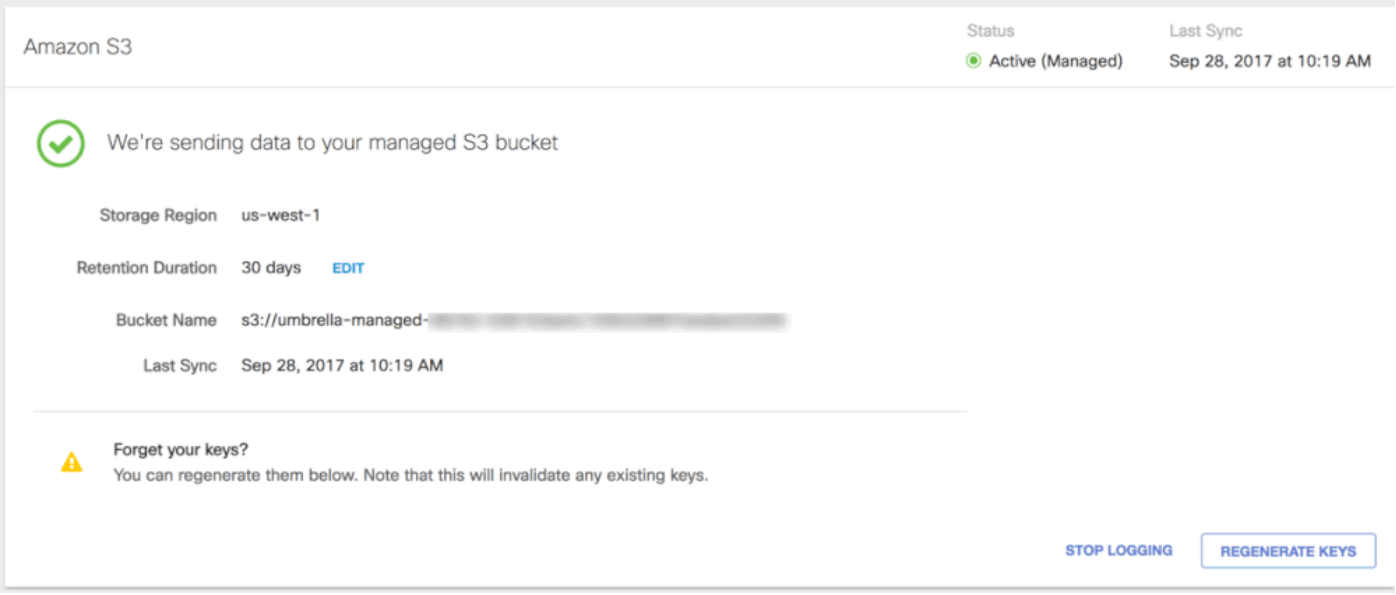
Zodra u ermee akkoord gaat om door te gaan, ontvangt u een activeringsmelding.



25231181218708

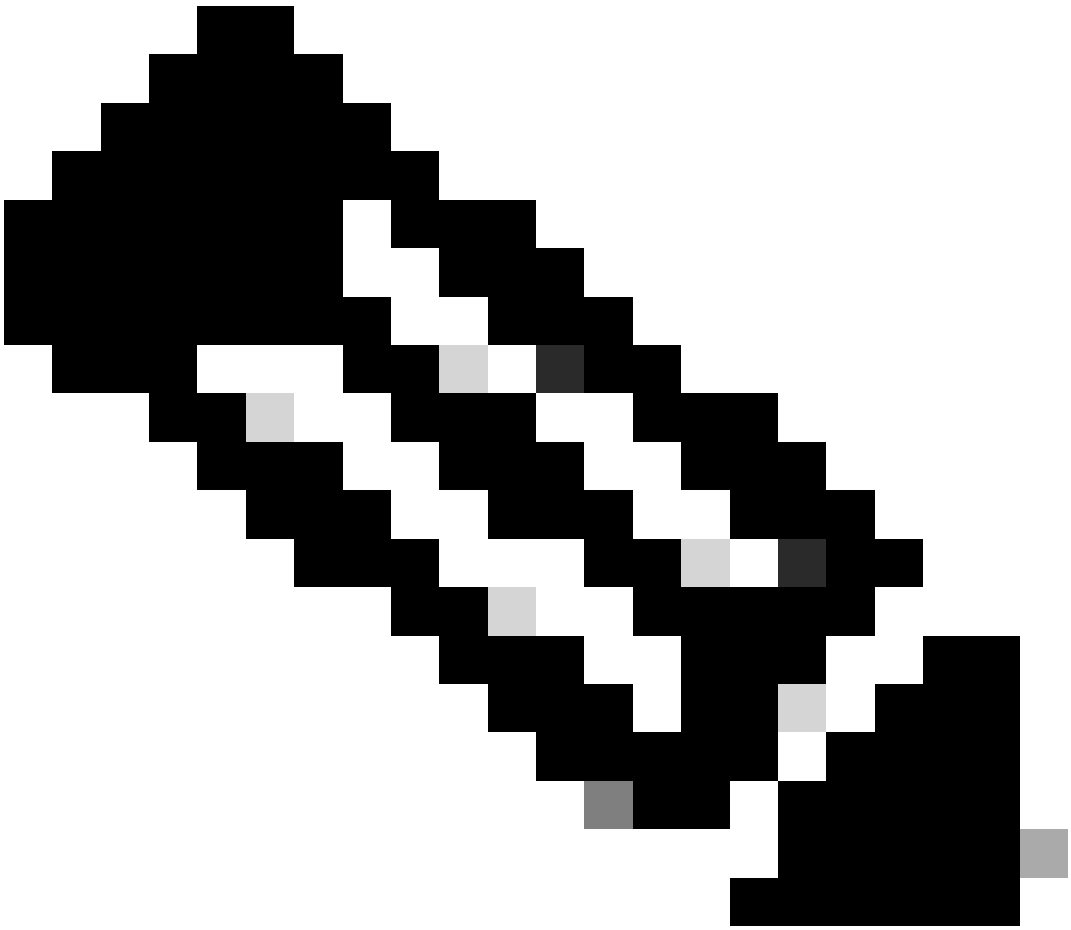
U ontvangt dan een toegangssleutel en een geheime sleutel. U moet accepteren (klik op "Heb het!") omdat dit de enige keer is dat u een van de sleutels te zien krijgt. De toegangs- en geheime sleutels zijn vereist om toegang te krijgen tot uw emmer en uw logs te downloaden.

Ten slotte ziet u het overzichtsscherm met de configuratie en, het belangrijkste, uw bucketnaam.



25231181228180

U kunt het inloggen op uw gemak in- of uitschakelen.



Opmerking: Cisco blijft logs opschonen op basis van de geselecteerde bewaarduur, zelfs als de logboekregistratie is uitgeschakeld.

Opties voor postconfiguratie

Fouten bij uploaden van logboek

In het geval van het niet uploaden van logs van Cisco Umbrella naar uw S3-emmer, is er een aflossingsvrije periode van vier uur waarin de service elke 20 minuten opnieuw wordt geprobeerd. Na vier uur wordt een zaak geopend met ons ondersteuningsteam, dat een onderzoek start naar de oorzaak van het probleem en proactief contact met u opneemt om u op de hoogte te stellen van het probleem.

Geüploade logs en opmaak controleren

Logboeken worden in intervallen van tien minuten geüpload van de Paraplu-logboekwachtrij naar de S3-emmers. Na het voltooien van de configuratie wordt het eerste log binnen twee uur naar uw S3-bucket geüpload, hoewel het proces meestal onmiddellijk of bijna onmiddellijk is. Voor het uploaden van iets zijn echter nieuw gegenereerde logboekgegevens nodig, dus als u dit in een testomgeving probeert, moet u ervoor zorgen dat netwerkgegevens worden vastgelegd in de zoekactiviteit.

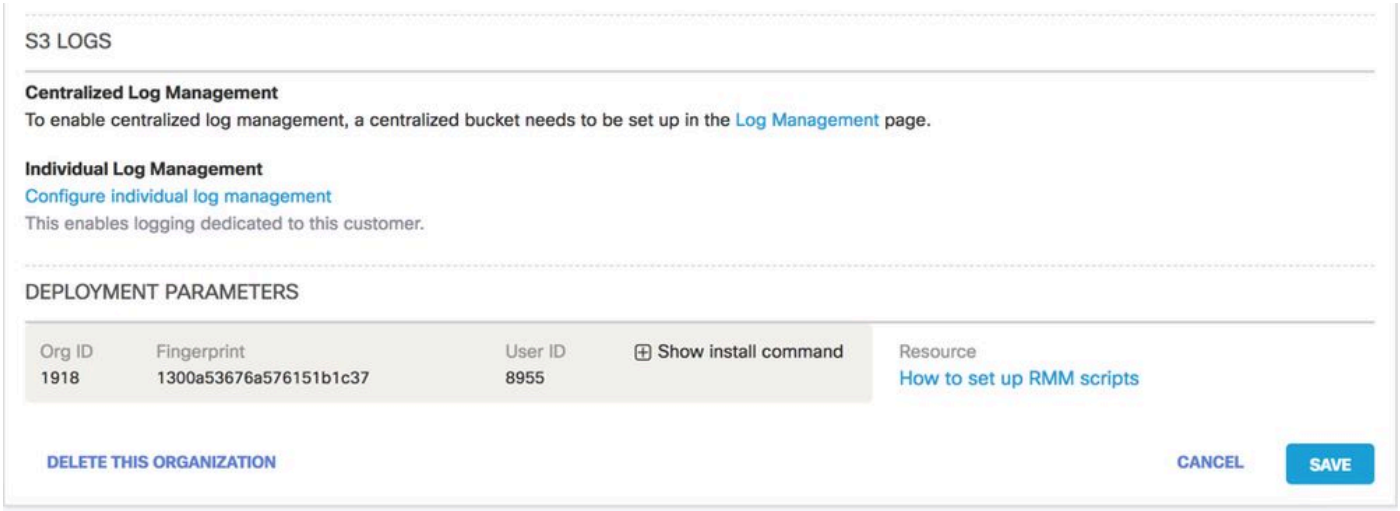
Als u wilt controleren of alles werkt, wordt de tijd voor de laatste synchronisatie in het dashboard van de paraplu bijgewerkt en worden er logs weergegeven in uw S3-emmer.

Binnen uw emmer wordt elke klant of organisatie gelabeld met hun organisatie-ID, dus de mappenstructuur is:

```
Amazon S3/<bucket-name>/<orgID>/<subfolder>
```

<bucket-name> is uw bucket-naam, <orgID> is uw organisatie-id, en <submap> zijn ofwel dnslogs, proxylogs of iplogs, afhankelijk van de soorten logs binnen.

Voor MSP- en MSSP-klanten komt de orgID overeen met die in Klantinstellingen onder elk klantdetail in het gedeelte Implementatieparameters. Multi-org-klanten kunnen de orgID verzamelen door in te loggen op elke afzonderlijke suborganisatie en de orgID op te nemen in de browser-URL: (https://dashboard.umbrella.com/o/####/).



360002271623

Momenteel is de loginversie voor de MSP-, MSSP- en Multi-org-klanten versie 1.1. De logs worden weergegeven in een GZIP-indeling en worden geüpload naar S3-emmers in de juiste submap met deze naamgevingsindeling:

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

<submap> is DNS-logs, proxylogs of iPlogs, afhankelijk van de typen logs in. **<xxxx>** is een willekeurige tekenreeks van vier alfanumerieke tekens die voorkomt dat dubbele bestandsnamen worden overschreven.

Voorbeeld:

```
dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz
```

Als u binnen 10 minuten geen logs in uw emmer ziet, neem dan contact op met ondersteuning met de stappen die u tot nu toe hebt ondernomen.

Zodra logs verschijnen, raden we aan de gegevens te bekijken door de inhoud van de eerste paar log-uploads die worden ontvangen, uit te pakken om ervoor te zorgen dat de gegevens zichtbaar zijn in een teksteditor (of zelfs Microsoft Excel, vaak de standaard voor .CSV). Voor informatie over welke elk veld in het log staat, lees hier.

Als een log-upload van Cisco Umbrella naar uw S3-emmer mislukt, is er een respijtperiode van vier uur waarin de service elke 20 minuten opnieuw wordt geprobeerd. Na vier uur opent zich een zaak binnen ons Support-team, die een onderzoek begint naar de oorzaak van het probleem en proactief contact met u opneemt om u op de hoogte te stellen van het probleem.

Logboekregistratie inschakelen op basis van gegevens per klant

Out of the box is deze functie ingeschakeld voor alle klanten, tenzij anders aangegeven. De functie kan worden uitgeschakeld voor individuele klanten, wat handig is als u verschillende serviceniveaus hebt voor klanten die de functie wel hebben. Dit is onder de instellingen van elke klant in de console. De schermafbeelding in de vorige sectie toont de schakelaar om het uit te schakelen.

Het is ook mogelijk om IAM-gebruikers in Amazon te maken en die IAM-gebruikers toe te wijzen aan individuele of iris-submappen van de emmer. Hiermee kunt u een eindgebruiker toegang geven tot hun logs, maar alleen tot hun logs.

Logboeken downloaden, het formaat begrijpen en Splunk / QRadar-integratie

Om de logs te downloaden voor retentie of verbruik, zijn er een paar benaderingen voor het downloaden van de DNS-logs van S3. We hebben hier een artikel gemaakt waarin een paar benaderingen van dit probleem worden geschetst.

U kunt ook een paar vragen hebben over de logindeling en hoe deze enigszins verschilt van de logs die worden weergegeven in het Umbrella-dashboard. Lees dit artikel voor meer informatie over de indeling van het geëxporteerde logboek.

Ten slotte is een van de belangrijkste toepassingen voor het exporteren van DNS-logs integratie met SIEM-tools. Hoewel de configuratie voor een SIEM bij het omgaan met logs zoals deze vaak kan komen neer op een beheerder is het persoonlijke voorkeuren, hebben we een aantal richtlijnen voor de meest populaire SIEMs.

Voor meer informatie over het instellen van de Splunk plug-in voor Amazon AWS S3 en Umbrella, lees hier.

Voor informatie over het configureren van IBM QRadar om logs van Amazon S3 te trekken en deze te verteren, lees hier.

Hoe groot zijn S3-logs?

De grootte van uw S3-logs is afhankelijk van het aantal gebeurtenissen dat plaatsvindt, afhankelijk van het volume van uw DNS-verkeer.

U kunt het logformaat voor de S3 Logging hier vinden.

Het voorbeelditem is 220 bytes, maar de grootte van elke logregel varieert op basis van een aantal items (lengte van de domeinnaam, aantal categorieën, enz.). Ervan uitgaande dat elke logregel 220 bytes is, zouden een miljoen verzoeken 220 MB zijn.

Om een schatting te krijgen van het aantal DNS-query's dat elke dag wordt gezien:

1. Navigeer in het Umbrella-dashboard naar Rapportage > Activiteit zoeken.
2. Voer onder Filters een rapport uit van de afgelopen 24 uur en klik op het pictogram CSV exporteren.
3. Open het gedownloade .csv bestand. Het aantal rijen (min één voor de header) is het aantal DNS-query's per dag; vermenigvuldig dat met 220 bytes om de schatting voor één dag te krijgen.

In termen van kosten, hoewel het variabel is, vinden we dat zelfs onze meest volumineuze klanten slechts een paar dollar per maand aan de service besteden. De ene kost is gekoppeld aan opslagtijd en de andere is gekoppeld aan het downloaden van gegevens van S3 naar uw omgeving. Neem contact op met Amazon voor meer informatie.

Zoals met al onze functies, willen we graag weten wat u denkt, vooral rond SIEM-integraties of eventuele aanvullende vragen die het in deze documentatie niet behandelt. Mocht je feedback hebben, laat het ons weten!

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.