Logboeken downloaden van Umbrella Log Management in AWS S3

Inhoud

Inleiding

In dit document wordt beschreven hoe u logs kunt downloaden van het Umbrella Log Management in AWS S3.

Overzicht

Zodra u hebt ingesteld en getest dat Logboekbeheer in de Amazon S3 correct werkt, kunt u beginnen met het automatisch downloaden en opslaan van de logs in uw netwerkinfrastructuur, hetzij voor retentie of verbruik (of beide).

Om dit te doen, hebben we een aanpak geschetst met behulp van s3tools van http://s3tools.org. s3tools maakt gebruik van het s3cmd opdrachtregelhulpprogramma voor Linux of OS/X. Er zijn andere tools die een vergelijkbare functie voor Windows-gebruikers kunnen uitvoeren:

- Voor een opdrachtregelprogramma kunt u hier een klein uitvoerbaar opdrachtregelprogramma downloaden.
- Als u de voorkeur geeft aan een grafische interface, bekijk dan S3 Browser (https://s3browser.com/), hoewel we niet bespreken hoe deze te gebruiken omdat de grafische interface niet scriptable is om het proces te automatiseren. Dit artikel geeft u stappen om beide opdrachtregelgereedschappen in te stellen. U kunt de informatie in stap 1 gebruiken om de s3browser-applicatie te configureren als u dat wilt.

Begin met het downloaden van de tool voor het besturingssysteem dat u wilt gebruiken. Voorlopig behandelen we alleen s3cmd voor OS / X en Linux, hoewel de stappen om toegang te krijgen tot uw emmer en de gegevens te downloaden in feite hetzelfde zijn voor Windows.

Pak het installatieprogramma van s3tools hier.

Het installatieprogramma vereist niet dat u het programma installeert om de opdrachtregel uit te voeren, dus pak gewoon het pakket uit dat u hebt gedownload.

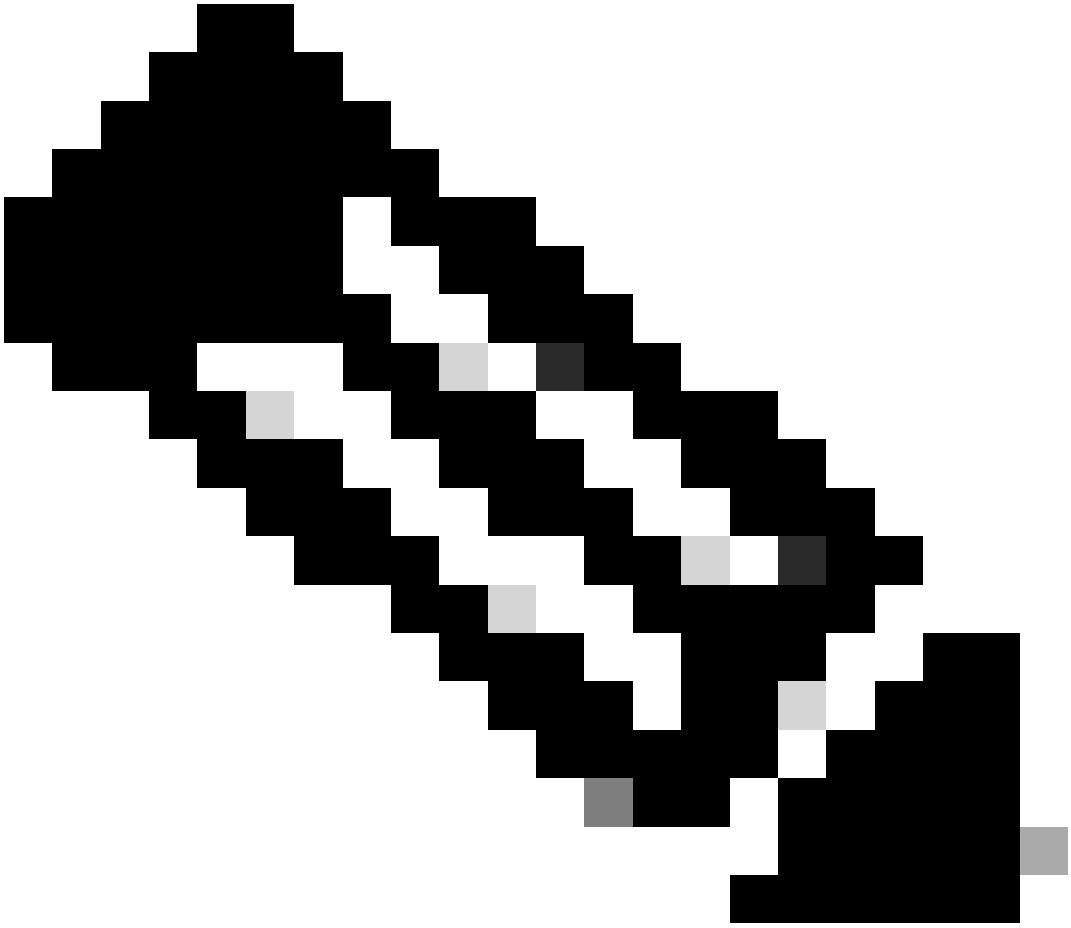
Fase 1: Uw beveiligingsreferenties configureren in AWS

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 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. Een prompt instrueert u om Amazon Best Practices te gebruiken en een AWS Identity and Access Management (IAM) -gebruiker 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.

Stap 2

1. Klik op Aan de slag met IAM-gebruikers om een IAM-gebruiker te maken met toegang tot uw S3-emmer. Navigeer naar een scherm waar u een IAM-gebruiker kunt maken.
2. Klik op Nieuwe gebruikers maken en vul de velden in.
3. Na het maken van het gebruikersaccount hebt u slechts één mogelijkheid 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 in een latere stap nodig hebben.



Opmerking: de gebruikersaccount mag geen spaties bevatten.

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 zou twee resultaten moeten tonen "AmazonS3FullAccess" en "AmazonS3ReadOnlyAccess".
3. Selecteer AmazonS3FullAccess en klik vervolgens op Beleid toevoegen.

Fase 2: Een tool configureren om DNS-logs uit de emmer te downloaden

s3cmd voor MacOS en Linux

1. Ga naar het pad dat u de s3cmd in de vorige fase hebt geëxtraheerd en typ uit Terminal:

```
./s3cmd --configure
```

   Dit moet u naar een prompt brengen waarin u wordt gevraagd uw beveiligingsreferenties te verstrekken:

Voer nieuwe waarden in of accepteer standaardinstellingen tussen haakjes met Enter.

Raadpleeg de gebruikershandleiding voor een gedetailleerde beschrijving van alle opties.

Toegangssleutel en geheime sleutel zijn uw identificatiegegevens voor Amazon S3. Laat ze leeg voor het gebruik van de env variabelen.

Toegangssleutel [UW TOEGANGSSLEUTEL]:

Secret Key [UW GEHEIME SLEUTEL]:

2. Vervolgens wordt u een reeks vragen gesteld over hoe u de toegang tot uw emmer wilt configureren. In dit geval stellen we geen coderingswachtwoord (GPG) in en gebruiken we geen HTTPS of een proxyserver. Als uw netwerk of voorkeuren verschillen, vult u de vereiste velden in:

Standaardgebied [VS]:

Coderingswachtwoord wordt gebruikt om uw bestanden te beschermen tegen lezen door onbevoegde personen tijdens de overdracht naar S3

Coderingswachtwoord:

Pad naar GPG-programma [Geen]:

Bij het gebruik van een beveiligd HTTPS-protocol is alle communicatie met Amazon S3-servers beveiligd tegen afluisteren door derden. Deze methode is

langzamer dan gewone HTTP en kan alleen worden benaderd met Python 2.7 of nieuwer

HTTPS-protocol gebruiken [No]:

Op sommige netwerken moet alle internettoegang via een HTTP-proxy verlopen.

Probeer het hier in te stellen als u niet rechtstreeks verbinding kunt maken met S3

Naam HTTP-proxyserver:

Nadat u netwerkspecifieke instellingen of een codering hebt ingevoerd, hebt u de kans om het volgende te bekijken:

Nieuwe instellingen:

Toegangssleutel: UW SLEUTEL

Geheime sleutel: UW GEHEIME SLEUTEL

Standaardregio: VS

Coderingswachtwoord:

Pad naar GPG-programma: Geen

HTTPS-protocol gebruiken: onwaar

Naam HTTP-proxyserver:

HTTP-proxyserverpoort: 0

Ten slotte wordt u gevraagd om te testen en, indien succesvol, de instellingen op te slaan:

Toegang testen met bijgeleverde referenties? [Y/n] y

Even geduld. Probeer alle emmers op te sommen...

Succes. Uw toegangssleutel en geheime sleutel werkten prima ��

Nu controleren of encryptie werkt...

Niet ingesteld. Laat maar.

Instellingen opslaan? [y/N]

Uitvoerbaar Windows-opdrachtregel (s3.exe)

Na het downloaden van de tool (https://s3.codeplex.com/releases/view/47595), kopieert u de .exe naar uw gewenste werkmap en typt u dit vanuit de opdrachtprompt, waarbij u uw toegangssleutel en geheim vervangt:

<#root>

s3 auth [

]

Voor meer informatie over de authenticatie syntaxis, lees hier.

Fase 3: Het testen van het downloaden van bestanden uit uw emmer

Stap 1: Test de download

s3cmd voor OS/X en Linux

Voer vanaf de terminal deze opdracht uit waarbij "my-organisatienaam-log-bucket" de naam is van uw bucket die al is geconfigureerd in het gedeelte Logbeheer van het Umbrella-dashboard. In dit voorbeeld wordt dit uitgevoerd vanuit de map die het uitvoerbare bestand s3cmd bevat en worden de bestanden op hetzelfde pad afgeleverd, maar deze kunnen worden gewijzigd:

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

Als er een verschil is tussen de bestanden in uw bucket en de bestanden in het bestemmingspad op de schijf, moet de synchronisatie de ontbrekende of bijgewerkte bestanden downloaden. Het eerste opgehaalde bestand moet het README-bestand zijn dat doorgaans wordt geüpload:

./S3CMD Sync S3://my-organization-name-log-bucket ./

S3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1 van 1]

1800 van 1800 100% in 0s 15,00 kB/s gedaan

Klaar. 1800 bytes gedownload in 1,0 seconden, 1800,00 B/s

Alle logbestanden die aanwezig zijn, worden ook gedownload. Het is aan jou of je een cron-taak wilt instellen om deze functie regelmatig te plannen, maar je moet nu in staat zijn om nieuwe of gewijzigde logbestanden in je bucket automatisch te downloaden naar een lokaal pad voor langdurige retentie.

Uitvoerbaar Windows-opdrachtregel (s3.exe)

Voer vanaf de opdrachtprompt deze opdracht uit waarbij 'my-organisatienaam-log-bucket' de naam is van uw bucket die al is geconfigureerd in het gedeelte Logbeheer van het Umbrella-dashboard. In dit voorbeeld worden alle bestanden in de bucket (gedefinieerd met de asterisk wildcard) gedownload naar de map \dnslogbackups\.

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

Voor meer informatie over de syntaxis voor deze opdracht, lees hier.

Stap 2: Automatiseer het downloaden

Zodra de syntaxis is getest en werkt zoals verwacht, kopieert u de instructies naar een scriptinstallatie voor een cron-taak (OS X / Linux) of een geplande taak (Windows) of gebruikt u een ander hulpmiddel voor taakautomatisering dat u tot uw beschikking hebt. Het is ook mogelijk om de tools te gebruiken om bestanden uit uw emmer te verwijderen nadat u ze hebt gedownload om ruimte vrij te maken in uw S3-exemplaar. We raden u aan om te kijken naar de documentatie voor de tool die u gebruikt om te zien wat het beste zou kunnen werken voor uw gegevensbewaringsbeleid.

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.