Protokolle von Umbrella Log Management in AWS S3 herunterladen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Protokolle von Umbrella Log Management in AWS S3 herunterladen.

Überblick

Wenn Sie das Log Management im Amazon S3 eingerichtet haben und testen, dass es korrekt funktioniert, können Sie die Logs automatisch herunterladen und in Ihrer Netzwerkinfrastruktur speichern, entweder zur Aufbewahrung oder zur Verwendung (oder beides).

Dazu haben wir einen Ansatz skizziert, der s3tools von http://s3tools.org verwendet. s3tools verwendet das s3cmd-Befehlszeilendienstprogramm für Linux oder OS/X. Es gibt andere Tools, die eine ähnliche Funktion für Windows-Benutzer ausführen können:

- Für ein Kommandozeilen-Tool können Sie hier eine kleine ausführbare Kommandozeilen-Datei herunterladen.
- Wenn Sie eine grafische Oberfläche bevorzugen, schauen Sie sich S3 Browser (https://s3browser.com/) an, obwohl wir nicht darauf eingehen, wie es zu verwenden ist, weil die grafische Oberfläche nicht skriptfähig ist, um den Prozess zu automatisieren. In diesem Artikel werden die Schritte zum Einrichten beider Befehlszeilentools beschrieben. Sie können die Informationen in Schritt 1 verwenden, um die s3browser-Anwendung zu

konfigurieren, wenn Sie es vorziehen.

Laden Sie zunächst das Tool für das Betriebssystem herunter, das Sie verwenden möchten. Für den Moment behandeln wir s3cmd für OS/X und Linux, obwohl die Schritte zum Zugriff auf Ihren Bucket und zum Herunterladen der Daten für Windows praktisch die gleichen sind.

Holen Sie sich den Installer von s3tools hier.

Der Installer erfordert nicht, dass Sie das Programm installieren, um die Kommandozeile auszuführen, also entpacken Sie einfach das heruntergeladene Paket.

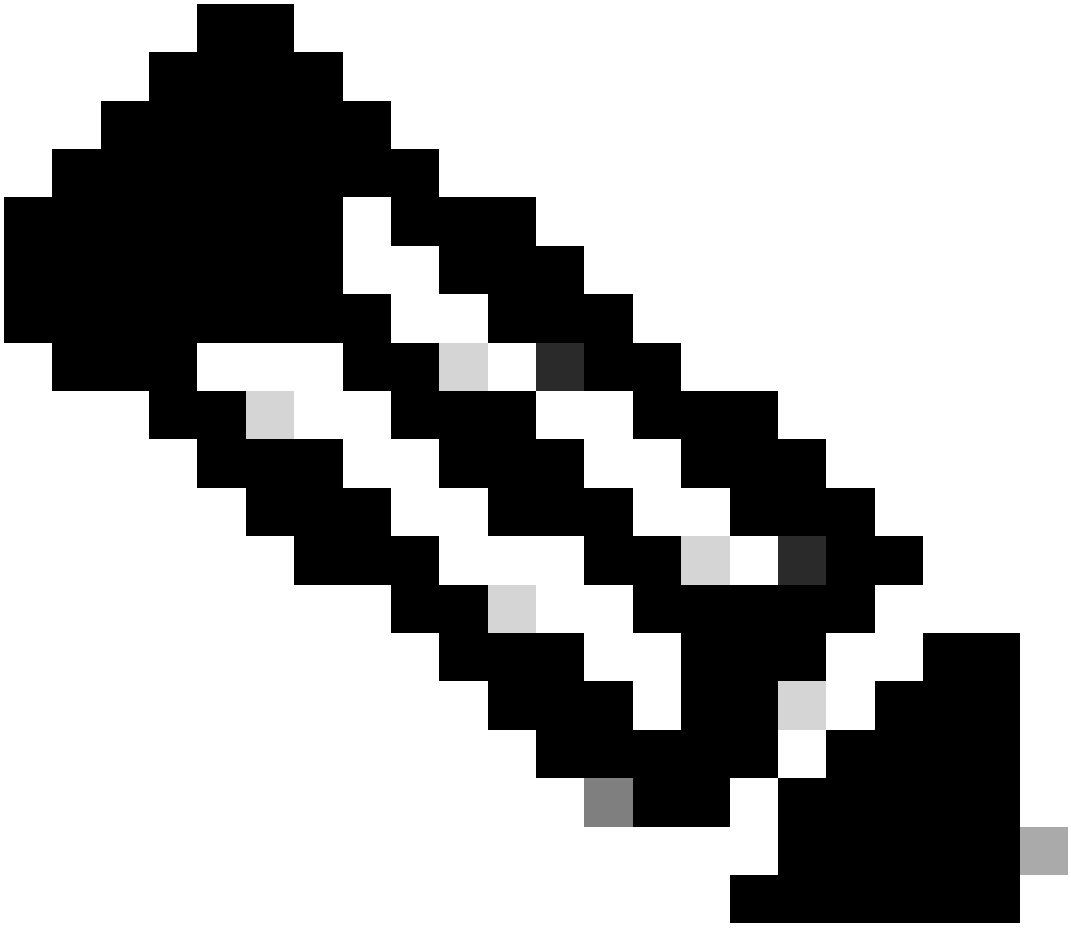
Phase 1: Konfigurieren Ihrer Sicherheitsanmeldeinformationen in AWS

Schritt 1

1. Fügen Sie Ihrem Amazon Web Services-Konto einen Zugriffsschlüssel hinzu, um den Remote-Zugriff auf Ihr lokales Tool und die Möglichkeit zum Hochladen, Herunterladen und Ändern von Dateien in S3 zu ermöglichen. Melden Sie sich bei AWS an, und klicken Sie in der oberen rechten Ecke auf Ihren Kontonamen. Wählen Sie im Dropdown-Menü die Option Security Credentials (Sicherheitsanmeldeinformationen).
2. Eine Eingabeaufforderung fordert Sie auf, Amazon Best Practices zu verwenden und einen AWS Identity and Access Management (IAM)-Benutzer zu erstellen. Im Wesentlichen stellt ein IAM-Benutzer sicher, dass das Konto, mit dem s3cmd auf Ihren Bucket zugreift, nicht das primäre Konto (z. B. Ihr Konto) für Ihre gesamte S3-Konfiguration ist. Durch die Erstellung individueller IAM-Benutzer für Personen, die auf Ihr Konto zugreifen, können Sie jedem IAM-Benutzer einen eindeutigen Satz von Sicherheitsanmeldeinformationen zuweisen. Sie können jedem IAM-Benutzer auch unterschiedliche Berechtigungen erteilen. Bei Bedarf können Sie die Berechtigungen eines IAM-Benutzers jederzeit ändern oder widerrufen.
   Weitere Informationen zu IAM-Benutzern und AWS-Best Practices finden Sie hier.

Schritt 2

1. Klicken Sie auf Erste Schritte mit IAM-Benutzern, um einen IAM-Benutzer mit Zugriff auf Ihre S3-Bucket zu erstellen. Navigieren Sie zu einem Bildschirm, auf dem Sie einen IAM-Benutzer erstellen können.
2. Klicken Sie auf Neue Benutzer erstellen, und füllen Sie die Felder aus.
3. Nach der Erstellung des Benutzerkontos haben Sie nur eine Möglichkeit, zwei wichtige Informationen mit Ihren Amazon User Security-Anmeldeinformationen zu erfassen. Es wird dringend empfohlen, diese über die Schaltfläche unten rechts herunterzuladen, um sie zu sichern. Sie sind nach dieser Phase der Einrichtung nicht mehr verfügbar. Notieren Sie sich sowohl Ihre Zugriffsschlüssel-ID als auch Ihren geheimen Zugriffsschlüssel, da wir sie in einem späteren Schritt benötigen.



Anmerkung: Das Benutzerkonto darf keine Leerzeichen enthalten.

Schritt 3

1. Als Nächstes fügen Sie eine Richtlinie für den IAM-Benutzer hinzu, damit dieser auf Ihren S3-Bucket zugreifen kann. Klicken Sie auf den soeben erstellten Benutzer, und scrollen Sie dann nach unten durch die Eigenschaften des Benutzers, bis die Schaltfläche Richtlinie anhängen angezeigt wird.
2. Klicken Sie auf Richtlinie anhängen, und geben Sie im Richtlinientyp-Filter 's3' ein. Es werden zwei Ergebnisse angezeigt: "AmazonS3FullAccess" und "AmazonS3ReadOnlyAccess".
3. Wählen Sie AmazonS3FullAccess aus, und klicken Sie dann auf Richtlinie anhängen.

Phase 2: Konfigurieren eines Tools zum Herunterladen von DNS-

Protokollen aus dem Bucket

s3cmd für MacOS und Linux

1. Gehen Sie zu dem Pfad, den Sie extrahiert haben s3cmd in der vorherigen Phase und aus Terminal, geben Sie ein:

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

Dadurch werden Sie aufgefordert, Ihre Sicherheitsanmeldeinformationen anzugeben:

Geben Sie mit der Eingabetaste neue Werte ein, oder übernehmen Sie die Standardwerte in Klammern.

Eine detaillierte Beschreibung aller Optionen finden Sie im Benutzerhandbuch.

Zugriffsschlüssel und Geheimschlüssel sind Ihre Kennungen für Amazon S3. Lassen Sie sie leer, um die env-Variablen zu verwenden.

Zugriffsschlüssel [IHR ZUGRIFFSSCHLÜSSEL]:

Geheimer Schlüssel [IHR GEHEIMER SCHLÜSSEL]:

2. Als Nächstes werden Ihnen eine Reihe von Fragen gestellt, wie Sie den Zugriff auf Ihren Bucket konfigurieren möchten. In diesem Fall richten wir kein Verschlüsselungskennwort (GPG) ein und verwenden weder HTTPS noch einen Proxy-Server. Wenn sich Ihr Netzwerk oder Ihre Einstellungen unterscheiden, füllen Sie die erforderlichen Felder aus:

Standardregion [US]:

Verschlüsselungskennwort wird verwendet, um Ihre Dateien vor dem Lesen durch unbefugte Personen während der Übertragung auf S3 zu schützen

Verschlüsselungskennwort:

Pfad zum GPG-Programm [Keine]:

Bei Verwendung des sicheren HTTPS-Protokolls ist die gesamte Kommunikation mit Amazon S3 Servern vor Abhörversuchen durch Drittanbieter geschützt. Diese Methode ist

langsamer als einfaches HTTP und kann nur mit Python 2.7 oder höher proximiert werden

HTTPS-Protokoll verwenden [Nein]:

In einigen Netzwerken muss der gesamte Internetzugang über einen HTTP-Proxy erfolgen.

Versuchen Sie, es hier einzustellen, wenn Sie keine direkte Verbindung mit S3 herstellen können.

HTTP-Proxy-Servername:

Nach der Eingabe netzwerkspezifischer Einstellungen oder einer Verschlüsselung können Sie Folgendes überprüfen:

Neue Einstellungen:

Zugriffsschlüssel: IHR SCHLÜSSEL

Geheimschlüssel: IHR GEHEIMSCHLÜSSEL

Standardregion: USA

Verschlüsselungskennwort:

Pfad zum GPG-Programm: None

HTTPS-Protokoll verwenden: Falsch

HTTP-Proxy-Servername:

HTTP-Proxy-Serverport: 0

Zuletzt werden Sie aufgefordert, die Einstellungen zu testen und bei Erfolg zu speichern:

Zugriff mit angegebenen Anmeldeinformationen testen? [J/N] J

Es wird versucht, alle Buckets aufzulisten...

Erfolg Ihr Zugriffsschlüssel und der geheime Schlüssel funktionierten einwandfrei ��

Überprüfen, ob die Verschlüsselung funktioniert ...

Nicht konfiguriert. Macht nichts.

Einstellungen speichern? [J/N]

Ausführbare Windows-Befehlszeilendatei (s3.exe)

Nachdem Sie das Tool heruntergeladen haben (https://s3.codeplex.com/releases/view/47595), kopieren Sie die EXE-Datei in Ihren bevorzugten Arbeitsordner, und geben Sie an der Eingabeaufforderung Folgendes ein. Ersetzen Sie dabei Zugriffsschlüssel und Schlüssel:

<#root>

```
s3 auth [
```

```
]
```

Weitere Informationen zur Authentifizierungssyntax finden Sie hier.

Phase 3: Testen des Downloads von Dateien aus Ihrem Bucket

Schritt 1: Testen des Downloads

s3cmd für OS/X und Linux

Führen Sie im Terminal den folgenden Befehl aus, wobei "my-organisation-name-log-bucket" der Name des Buckets ist, der bereits im Bereich Log Management des Umbrella Dashboards konfiguriert wurde. In diesem Beispiel wird dies von dem Ordner ausgeführt, der die ausführbare Datei s3cmd enthält, und die Dateien werden an denselben Pfad übermittelt, aber diese können geändert werden:

<#root>

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

Wenn es einen Unterschied zwischen den Dateien in Ihrem Bucket und den Dateien im Zielpfad auf der Festplatte gibt, sollte die Synchronisierung die fehlenden oder aktualisierten Dateien herunterladen. Die erste abgerufene Datei sollte die README-Datei sein, die normalerweise hochgeladen wird:

./s3cmd sync s3://my-organisation-name-log-bucket ./

s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1 von 1]

1800 von 1800 100% in 0s 15,00 kB/s fertig

Fertig. 1800 Byte in 1,0 Sekunden heruntergeladen, 1800,00 B/s

Alle vorhandenen Protokolldateien werden ebenfalls heruntergeladen. Es liegt an Ihnen, ob Sie einen Cron-Job festlegen möchten, um diese Funktion regelmäßig zu planen, aber Sie sollten jetzt in der Lage sein, automatisch neue oder geänderte Protokolldateien in Ihrem

Bucket auf einen lokalen Pfad herunterzuladen, um eine langfristige Aufbewahrung zu ermöglichen.

Ausführbare Windows-Befehlszeilendatei (s3.exe)

Führen Sie an der Eingabeaufforderung diesen Befehl aus, wobei "my-organisation-name-log-bucket" der Name des Buckets ist, der bereits im Bereich Protokollverwaltung des Umbrella Dashboards konfiguriert wurde. In diesem Beispiel werden alle Dateien in der Gruppe (definiert mit dem Platzhalter Sternchen) in den Ordner \dnslogbackups\ heruntergeladen.

<#root>

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

Weitere Informationen zur Syntax für diesen Befehl finden Sie hier.

Phase 2: Automatisierung des Downloads

Wenn die Syntax getestet wurde und wie erwartet funktioniert, kopieren Sie die Anweisungen in ein Skript, das einen Cron-Job (OS X/Linux) oder einen geplanten Task (Windows) konfiguriert, oder verwenden Sie ein anderes Tool zur Aufgabenautomatisierung, das Ihnen möglicherweise zur Verfügung steht. Es ist auch möglich, mit den Tools Dateien aus Ihrem Bucket zu entfernen, nachdem Sie sie heruntergeladen haben, um Speicherplatz in Ihrer S3-Instanz freizugeben. Wir empfehlen Ihnen, sich die Dokumentation für das von Ihnen verwendete Tool anzusehen, um herauszufinden, was am besten für Ihre Datenaufbewahrungsrichtlinie geeignet ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.