AWS S3のUmbrella Log Managementからのログのダウンロード

内容

はじめに

このドキュメントでは、AWS S3のUmbrella Log Managementからログをダウンロードする方法について説明します。

概要

Amazon S3のログ管理が正しく機能していることをセットアップし、テストしたら、保存または使用（あるいはその両方）のために、ネットワークインフラストラクチャ内でログのダウンロードと保存を自動的に開始することができます。

これを行うために、http://s3tools.orgからs3toolsを使用するアプローチの概要を説明しました。s3toolsは、LinuxまたはOS/X用のs3cmdコマンドラインユーティリティを使用します。Windowsユーザ用に、同様の機能を実現できるツールは他にもあります。

- コマンドラインツールの場合は、ここから小さなコマンドライン実行可能ファイルをダウンロードできます。
- グラフィカルインターフェイスを使用する場合は、S3ブラウザ(https://s3browser.com/)を確認してください。ただし、グラフィカルインターフェイスはプロセスを自動化するためのスクリプト可能ではないため、使用方法については説明していません。この記事では、両方のコマンドラインツールをセットアップする手順を説明します。必要に応じて、ステージ1の情報を使用してs3browserアプリケーションを設定できます。

まず、使用するオペレーティングシステムに対応したツールをダウンロードします。現時点では、バケットにアクセスしてデータをダウンロードする手順は事実上Windowsと同じですが、OS/XおよびLinux用のs3cmdについてのみ説明しています。

こちらのs3toolsからインストーラを取得します。

インストーラは、コマンドラインを実行するためにプログラムをインストールする必要がないため、単にダウンロードしたパッケージを抽出します。

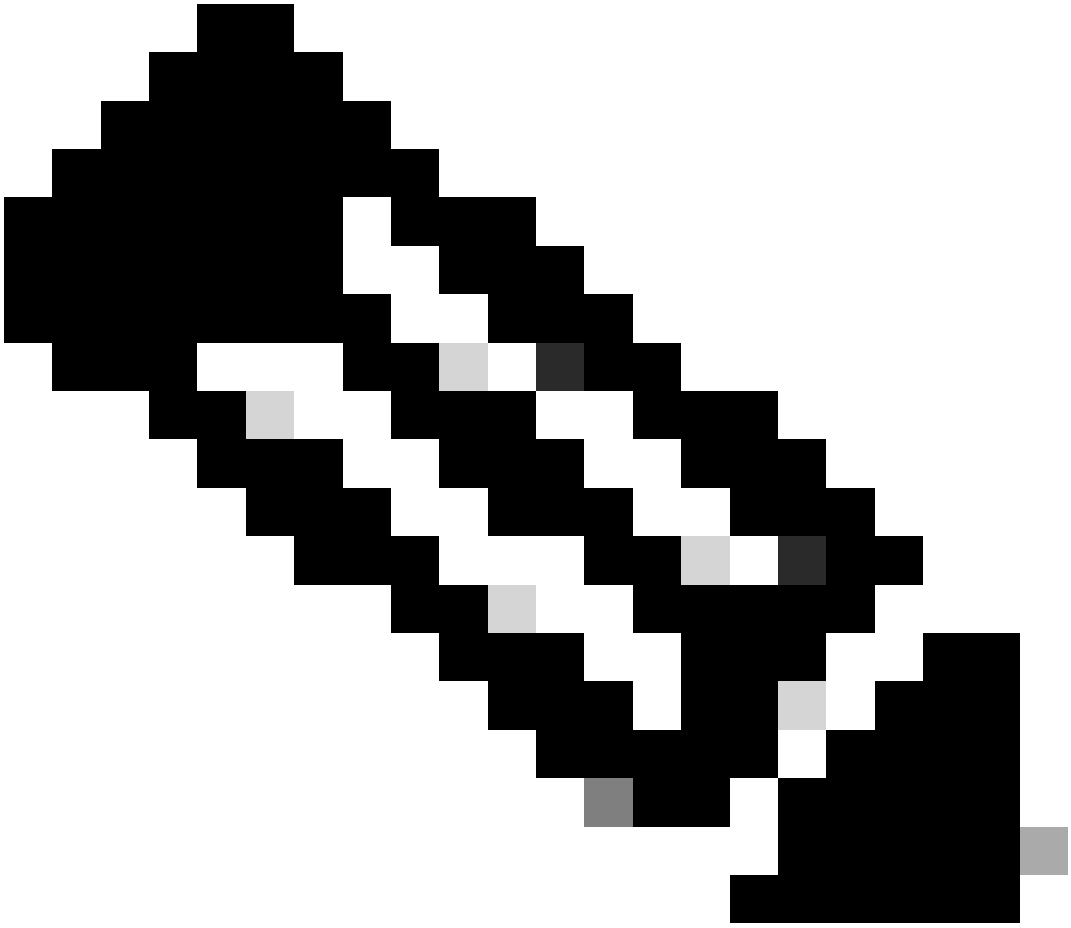
ステージ1: AWSでのセキュリティ認証情報の設定

手順 1

1. Amazon Web Servicesアカウントにアクセスキーを追加して、ローカルツールへのリモートアクセスを有効にし、S3でファイルをアップロード、ダウンロード、および変更できるようにします。AWSにログインし、右上隅にあるアカウント名をクリックします。ドロップダウンで、Security Credentialsを選択します。
2. プロンプトでは、Amazonのベストプラクティスを使用してAWS Identity and Access Management (IAM)ユーザーを作成するように指示されます。基本的に、IAMユーザーはs3cmdがバケットへのアクセスに使用するアカウントが、S3構成全体のプライマリアカウント（アカウントなど）ではないことを保証します。アカウントにアクセスするユーザー用に個別のIAMユーザーを作成することで、各IAMユーザーに一意のセキュリティ認証情報のセットを付与できます。各IAMユーザーに異なるアクセス許可を付与することもできます。必要に応じて、IAMユーザーのアクセス許可をいつでも変更または取り消すことができます。
   IAMユーザーとAWSのベストプラクティスの詳細については、ここを参照してください。

手順 2

1. Get Started with IAM Users をクリックして、S3バケットにアクセスできるIAMユーザを作成します。IAMユーザーを作成できる画面に移動します。
2. Create New Usersをクリックして、フィールドに入力します。
3. ユーザーアカウントを作成した後、Amazonユーザーセキュリティ認証情報を含む2つの重要な情報を取得する機会は1つだけです。これらをバックアップするには、右下のボタンを使用してダウンロードすることを強くお勧めします。セットアップのこの段階を過ぎると使用できなくなります。 アクセスキーIDとシークレットアクセスキーは、後の手順で必要になるため、両方をメモしておいてください。



注：ユーザアカウントにスペースを含めることはできません。

手順 3

1. 次に、IAMユーザーがS3バケットにアクセスできるようにポリシーを追加します。作成したばかりのユーザをクリックし、[Attach Policy]ボタンが表示されるまでユーザのプロパティをスクロールダウンします。
2. Attach Policyをクリックし、ポリシータイプのフィルタに「s3」と入力します。これにより、「AmazonS3FullAccess」と「AmazonS3ReadOnlyAccess」の2つの結果が表示されます。
3. AmazonS3FullAccessを選択し、Attach Policyをクリックします。

ステージ2：バケットからDNSログをダウンロードするためのツールの設定

MacOSおよびLinux用のs3cmd

1. 前の段階でs3cmdを抽出したパスに移動し、ターミナルから次のように入力します。

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

これにより、セキュリティクレデンシャルの入力を求めるプロンプトが表示されます。

新しい値を入力するか、[Enter]を使用して括弧で囲んだ既定値を受け入れます。

すべてのオプションの詳細については、ユーザマニュアルを参照してください。

アクセスキーとシークレットキーは、Amazon S3の識別子です。env変数を使用する場合は、空のままにします。

アクセスキー[アクセスキー]:

秘密キー[秘密キー]:

2. 次に、バケットへのアクセスの設定方法に関する一連の質問が表示されます。この場合、暗号化パスワード(GPG)は設定せず、HTTPSまたはプロキシサーバは使用しません。ネットワークまたは設定が異なる場合は、次の必須フィールドに入力します。

既定の地域[米国]:

暗号化パスワードは、S3への転送中に許可されていない人がファイルを読み取らないようにするために使用されます

暗号化パスワード：

GPGプログラムへのパス[なし]:

セキュアなHTTPSプロトコルを使用すると、Amazon S3サーバーとの通信はすべて、第三者による傍受から保護されます。このメソッドは

通常のHTTPより遅く、Python 2.7以降でのみプロキシできます

HTTPSプロトコルを使用[No]:

一部のネットワークでは、すべてのインターネットアクセスがHTTPプロキシを経由する必要があります。

S3に直接接続できない場合は、ここで設定してみてください

HTTPプロキシサーバー名：

ネットワーク固有の設定または暗号化を入力した後、次の項目を確認できます。

新しい設定

アクセスキー：自分のキー

秘密キー：秘密キー

デフォルトのリージョン：米国

暗号化パスワード：

GPGプログラムへのパス：なし

HTTPSプロトコルを使用： False

HTTPプロキシサーバー名：

HTTPプロキシサーバポート： 0

最後に、テストを行い、成功した場合は設定を保存するように求められます。

指定された資格情報でアクセスをテストしますか？[Y/n] y

すべてのバケットを一覧表示しています。しばらくお待ちください…

成功。アクセスキーと秘密キーは正常に動作しました��

暗号化が動作していることを確認しています…

Not configured.気にするなよ。

設定を保存しますか？[y/N]

Windowsコマンドライン実行可能ファイル(s3.exe)

ツール(https://s3.codeplex.com/releases/view/47595)をダウンロードした後、目的の作業フォルダに.exeをコピーし、コマンドプロンプトからアクセスキーとシークレットを入力します。

<#root>

```
s3 auth [


        ]
```

認証構文の詳細については、ここを参照してください。

ステージ3：バケットからのファイルのダウンロードのテスト

ステップ1：ダウンロードのテスト

OS/XおよびLinux用のs3cmd

ターミナルからこのコマンドを実行します。「my-organization-name-log-bucket」は、Umbrellaダッシュボードのログ管理部分ですでに設定されているバケットの名前です。この例では、s3cmd実行可能ファイルを含むフォルダから実行され、ファイルは同じパスに配信されますが、次のパスは変更できます。

<#root>

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

バケット内のファイルとディスク上の宛先パス内のファイルの間に違いがある場合は、失われたファイルまたは更新されたファイルが同期によってダウンロードされます。最初に取得するファイルは、通常アップロードされるREADMEファイルである必要があります。

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

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

1800の1800を0で100 %使用、15.00 kB/s実行

Done.1.0秒で1800バイトをダウンロード、1800.00 B/s

存在するログファイルもすべてダウンロードされます。この機能を定期的にスケジュールするようにcronジョブを設定する場合はユーザーの責任ですが、バケット内の新しいログファイルまたは変更されたログファイルをローカルパスに自動的にダウンロードして長期間保存することができます。

Windowsコマンドライン実行可能ファイル(s3.exe)

コマンドプロンプトから、このコマンドを実行します。「my-organization-name-log-bucket」は、Umbrellaダッシュボードのログ管理部分ですでに設定されているバケットの名前です。この例では、バケット内のすべてのファイル（アスタリスクのワイルドカードで定義されたファイル）が\dnslogbackups\フォルダにダウンロードされます。

<#root>

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

このコマンドの構文の詳細については、ここを参照してください。

ステップ2：ダウンロードの自動化

構文がテストされ、期待どおりに動作したら、cronジョブ(OS X / Linux)またはスケジュールされたタスク(Windows)のスクリプトセットアップに手順をコピーするか、自由に使用できる他のタスク自動化ツールを使用します。S3インスタンスの空き領域を確保するために、ダウンロードしたファイルをバケットから削除するツールを使用することもできます。データ保存ポリシーに最も適したツールについては、使用しているツールのドキュメントを参照することをお勧めします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。