# 自己管理S3バケットによるSplunkの設定

## 内容



## はじめに

このドキュメントでは、セルフマネージドS3バケットでSplunkを設定する方法について説明します。

## 概要

Splunkは、ログ分析のための一般的なツールです。Cisco Umbrellaが組織のDNSトラフィック用に提供するログなど、大量のデータを分析するための強力なインターフェイスを提供します。

この記事では、S3バケットからログを取得して使用できるように、Splunkをセットアップして実行する基本的な方法について説明します。2つの主要な段階があります。1つはAWS S3セキュリティクレデンシャルを設定してSplunkがログにアクセスできるようにすること、もう1つはSplunk自体がバケットを指すように設定することです。

AWS S3用Splunkアドオンのドキュメントはここにあります。一部のドキュメントは逐語的にこのドキュメントにコピーされています。Splunkのセットアップに関する具体的な質問については、http://docs.splunk.com/Documentation/AddOns/latest/AWS/Descriptionを参照してください。

この記事には、次のセクションがあります。

- 前提条件
- ステージ1: AWSでのセキュリティ認証情報の設定（自己管理バケットのみ）
- ステージ2:S3バケットからDNSログデータをプルするためのSplunkのセットアップ
  - ステップ1：自己管理されたS3バケットからDNSログデータをプルするためのSplunkのセットアップ

- ステージ3:Splunkのデータ入力の設定

# 前提条件

アマゾンウェブサービス用Splunkアドオンは、これらのプラットフォームをサポートします。

- AWS Linux
- RedHat
- Windows 2008R2、2012R2

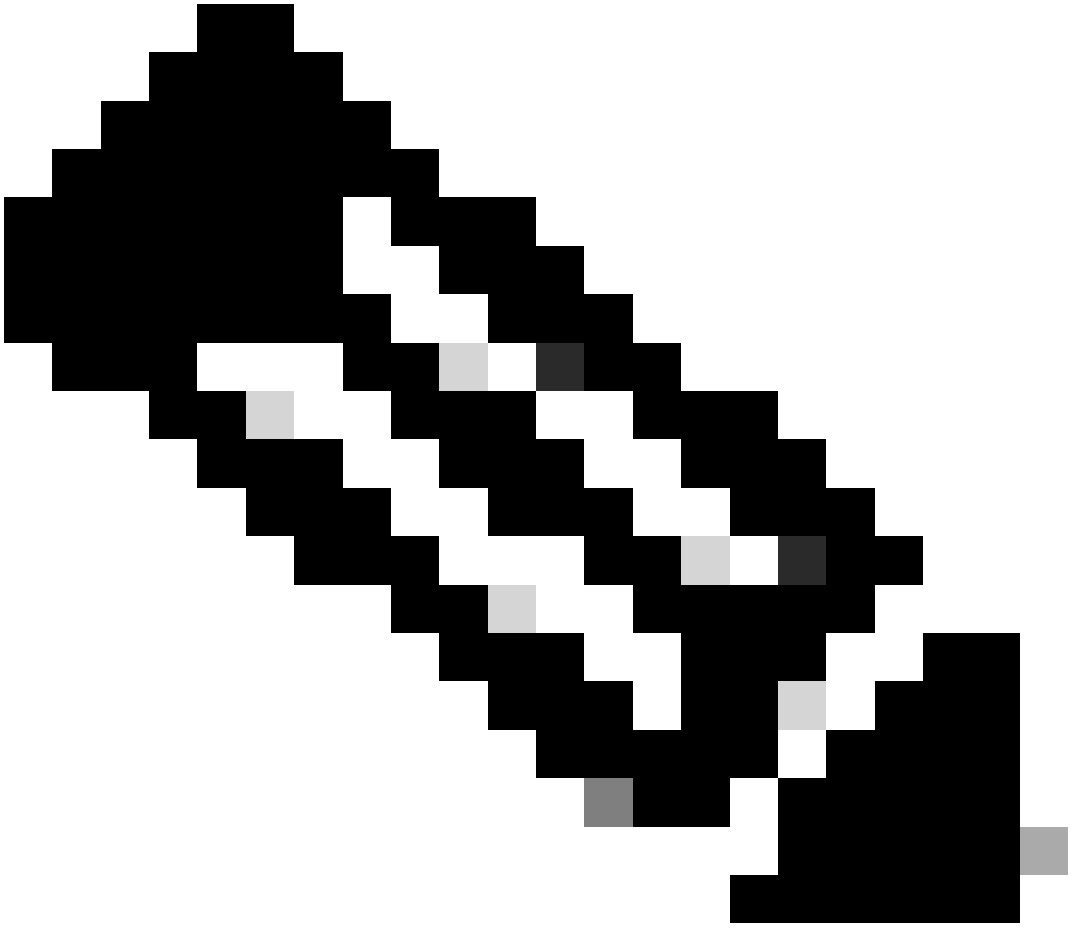
## Splunk Enterpriseのシステム要件

このアドオンはSplunk Enterpriseで実行されるため、Splunk Enterpriseのすべてのシステム要件が適用されます。Splunk Enterpriseのマニュアルの「システム要件」を参照してください。Splunk Enterpriseバージョン6.2.1用の手順を次に示します。

## 包括的な要件

このドキュメントでは、Amazon AWS S3バケットがUmbrellaダッシュボード(Admin> Log Management)で設定され、最近のログがアップロードされて緑色で表示されていることを前提としています。ログ管理の詳細については、「Amazon S3でのCisco Umbrella口グ管理」を参照してください。

# ステージ1: AWSでのセキュリティ認証情報の設定



注：これらの手順は、バケットからログをダウンロードするようにツールを設定する方法について説明する記事で概説されている手順と同じです（方法： AWS S3のCisco Umbrella口グ管理からのログのダウンロード）。 これらの手順をすでに実行している場合は、手順2に進むだけで済みます。ただし、バケットに対してSplunkプラグインを認証するには、IAMユーザからのセキュリティ認証情報が必要です。

## 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許可し、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. 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求められます。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ベストプラクティスの詳細については、
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html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するためのIAMユーザを作成します。 IAMユーザーを作成できる画面が表示されます。
2. Create New Usersをクリックしてから、先に進んでフィールドに入力します。ユーザーアカウントにスペースを含めることはできません。
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が1つだけ与えられます。 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、後でSplunkをセットアップするときに必要になるので、両方をメモしておいてください。

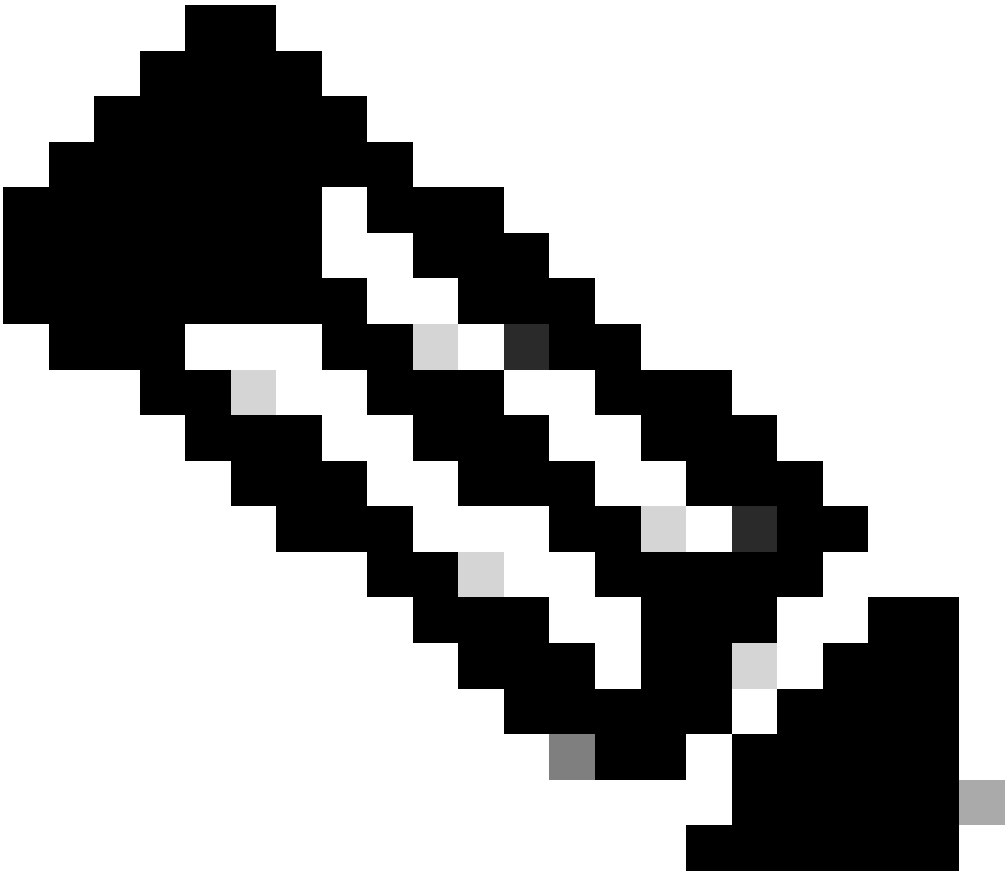
### 手順 3

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:S3バケットからDNSログデータをプルするためのSplunkのセットアップ

### 手順1：自己管理されたS3バケットからDNSログデータをプルするためのSplunkのセットアップ

1. まず、Splunkインスタンスに「Amazon Web Services用Splunkアドオン」をインストールします。Splunkダッシュボードを開き、アプリケーションをクリックします。ダッシュボードにSplunkアプリケーションが表示されたら、それをクリックします。「アプリケーション」セクションで、検索ウィンドウに「s3」と入力して「Splunk Add-on for Amazon Web Services」を検索し、アプリケーションをインストールします。



注：インストール中にSplunkを再起動する必要がある場合があります。
インストールが完了すると、AWS用Splunkアドオンのフォルダ名「
Splunk_TA_aws」がアプリケーションの下に表示されます。

2. Set upをクリックして、アプリケーションを設定します。ここで、このドキュメントのステージ1のセキュリティ認証情報が必要になります。
この設定では、次のフィールドを入力する必要があります。

- フレンドリ名：この統合を参照するために使用する名前
- AWSアカウントのキーID（ステージ1から）
- パスワード（ステージ1のAWSアカウントの秘密キー）

また、SplunkがAWSに到達するために必要な場合は、ローカルプロキシ情報を設定したり、ロギングを調整したりできます。セットアップ画面は次のようになります。
3. 関連情報を追加したら、Saveをクリックします。これでAmazon Web Services用Splunkアドオンが完全に設定されました。

# ステージ3:Splunkのデータ入力の設定

1. 次に、アマゾンウェブサービスS3のデータ入力を設定します。Settings > Data > Data Inputsの順に移動すると、Local Inputsの下に、リストの下部にS3を含むさまざまなAmazon入力のリストが表示されます。
2. AWS S3をクリックして入力を設定します。
3. [New] をクリックします。
4. 次の情報を入力する必要があります。

    - S3統合のフレンドリ名を入力します。
    - お客様の ドロップダウンからAWSアカウントを選択します。これは、手順1で指定したフレンドリ名です。
    - ドロップダウンからS3バケットを選択します。これは、Umbrellaダッシュボード ( 「設定」 >「ログ管理」 ) で指定したバケット名です。
    - ドロップダウンからS3キー名を選択します。バケット内のすべての項目が表示されます。トップレベルのディレクトリ\dns-logs\を選択することをお勧めします。このディレクトリには、その下にあるすべてのファイルとディレクトリが含まれています。
    - 「メッセージシステムの設定」にはいくつかのオプションがあります。デフォルト設定のままにしておくことをお勧めします。
    - 「詳細設定」の下に追加オプションがあります。 特に「Source type」はデフォルトでaws:s3です。この設定は変更しないことをお勧めしますが、変更した場合は、検索内のログのフィルタがこれらの手順のステップ3で説明した内容から変更されます。

    詳細を入力すると、データ入力は次のようになります。

4. Nextをクリックして詳細を確定します。
    入力が正常に作成されたことを示す画面が表示されます

## 手順 3

クイック検索を実行して、データが正しくインポートされているかどうかを確認します。右上の検索ウィンドウにsourcetype="aws:s3"を貼り付け、検索で「Open sourcetype="aws:s3"」を選択するだけです

これにより、組織のDNSログからのイベントを表示する画面と同様の画面が表示されます。ここでは、Cisco Umbrellaモバイルサービスがiphoneのソーシャルメディアをブロックしています。また、ファイル名のソースを使用して、特定のログのバッチに対してフィルタリングを行うこともできます。

この時点を過ぎると、バックグラウンドのcronジョブが実行を続け、バケットのログ情報から最新のセットをプルダウンします。

Splunkを使用することで、この記事で説明した以外にも多くのことができるようになります。セキュリティ対応手順でこのデータを試してみたことがあれば、ぜひ連絡してください。フィードバック、ご質問、懸念事項がありましたら、umbrella-support@cisco.comまでメールでお問い合わせください。また、こちらの記事も参考にしてください。

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。