Umbrella Log ManagementおよびS3を使用したQRadar統合の設定

内容

はじめに

このドキュメントでは、Umbrella口グ管理のためにAWS S3バケットから口グを取り込むようにQRadarを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

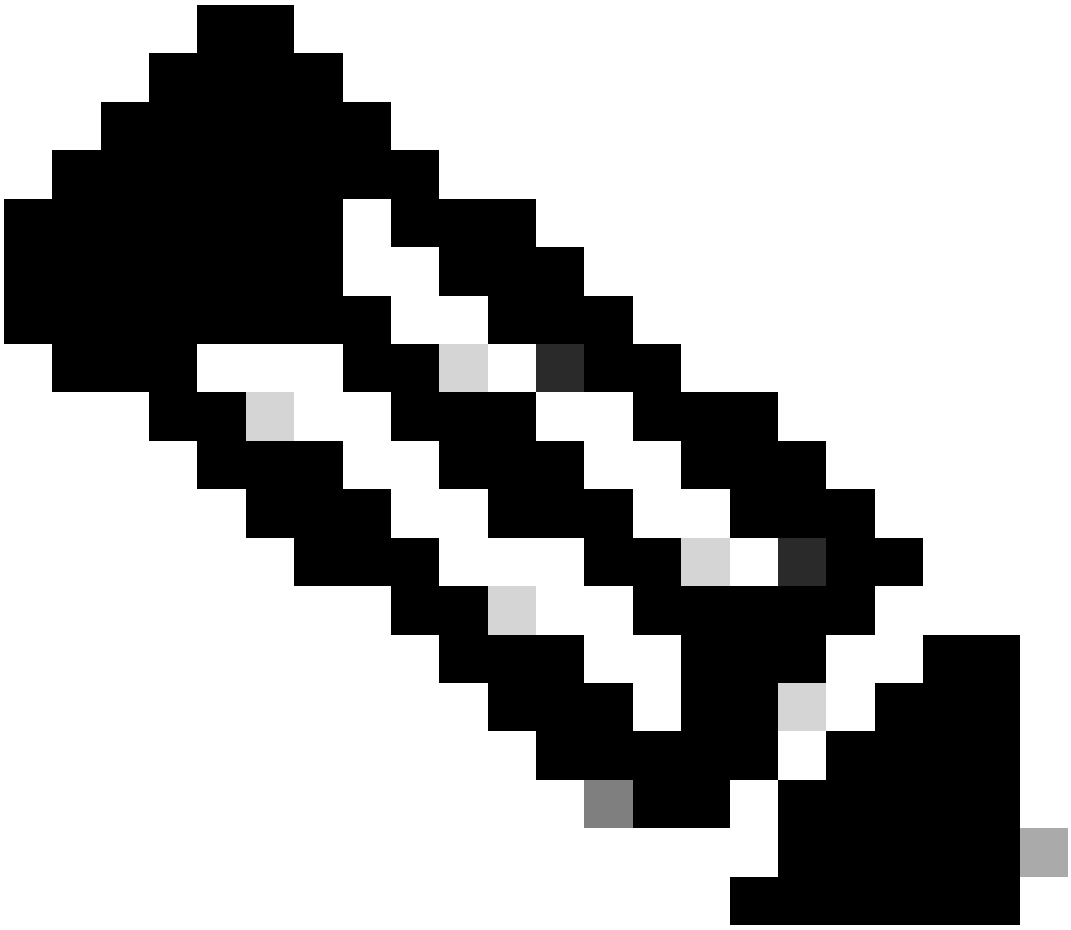
- このドキュメントでは、Amazon AWS S3バケットがUmbrella(Settings > Log Management)に設定され、最新の口グがアップロードされて緑色で表示されていることを前提としています。この機能を設定する方法の詳細については、「AWS S3のUmbrella Log Managementからの口グのダウンロード」を参照してください。
- QRadarアプライアンス、Amazon S3構成、Umbrellaダッシュボードに対する管理者権限に加えて、これらの手順は、QRadar管理者がLSX (Log source Extension)ファイルの作成に精通していることを前提としています。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要



注:Cisco Umbrellaで使用するQRadarを設定する最良の方法は、Cisco Cloud Securityアプリケーションを使用することです。アプリを構成できない場合のみ、この方法を続行してください。

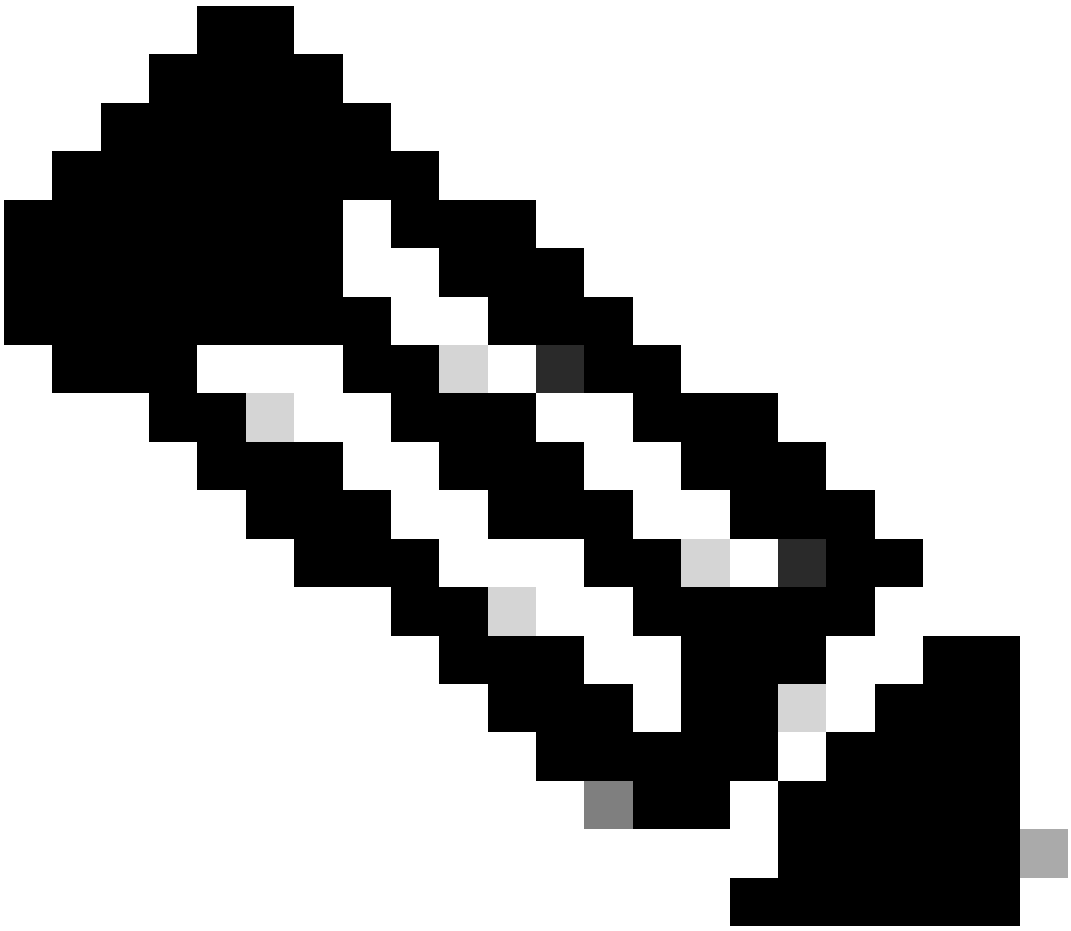
IBMのQRadarは、ログ分析用の一般的なSIEMです。Cisco Umbrellaが組織のDNSトラフィック

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、QRadarをセットアップして実行し、S3バケットからログをプルして消費できるようにする方法について説明します。次の2つの主要な段階があります。

- AWS S3セキュリティ認証情報を設定して、QRadarがログにアクセスできるようにします。
- バケットを指すようにQRadar自体を設定します。

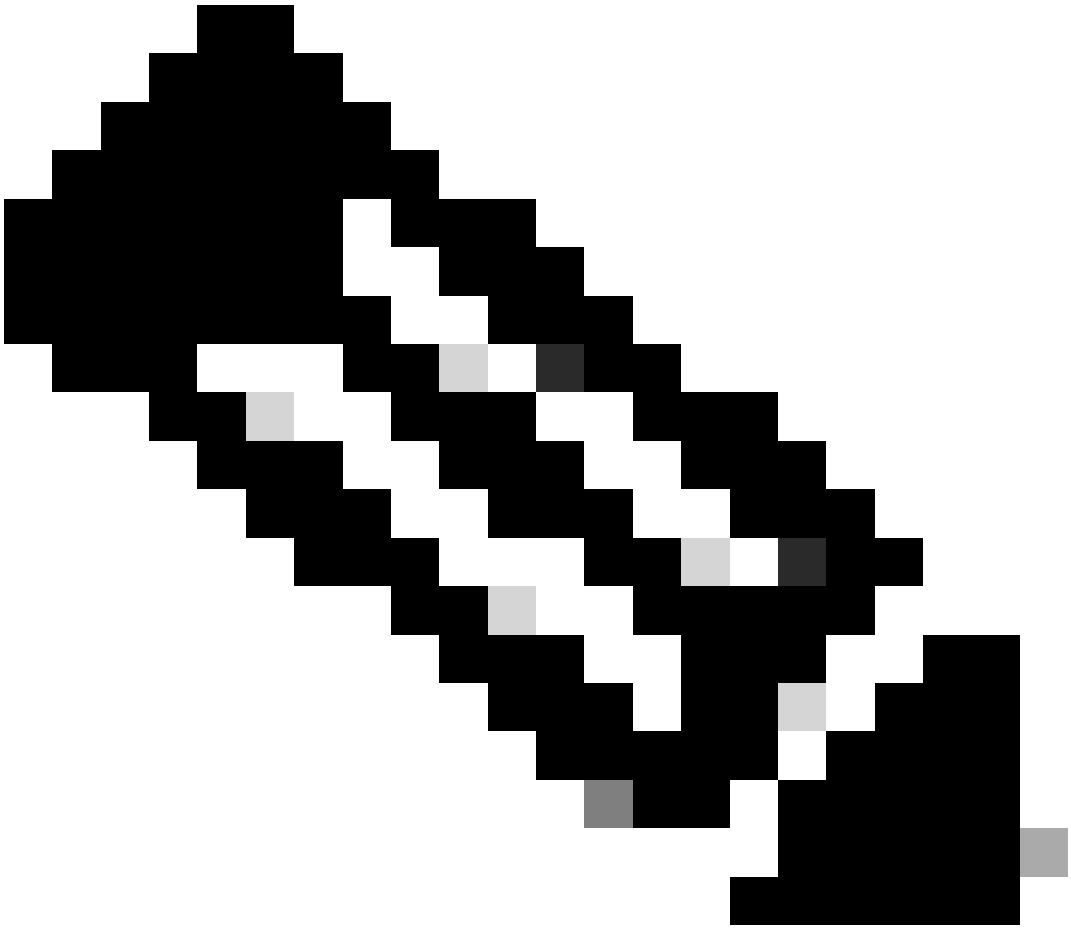
シスコが管理するS3バケットを使用している場合は、「AWS CLIを使用したUmbrellaログ管理からのログのダウンロード」の記事を参照してください。



注：この統合は、顧客管理S3バケットとシスコ管理S3バケットの両方でテストされています。この記事で説明されている情報は、この文書（2019年10月）の時点のものです。QRadarとAWSサービスインターフェイスの方法に基づいて変更できます。 この書類は生きた書類だ。フィードバックがある場合、または他のお客様に役立つ可能性があるテクニックやヒントが見つかった場合は、Cisco Umbrellaサポートにお問い合わせください。

QRadarは、サードパーティ製のハードウェアやソフトウェアを直接サポートしていないため、IBMのサポートが必要です。Umbrellaダッシュボードを S3バケットに接続する際に問題が発生した場合は、Cisco Umbrellaがサポートを提供します。この記事に記載されている情報の多くは、IBMのWebサイトでも入手できます。

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(AWS S3のUmbrella Log Managementからログをダウンロードする)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。 これらの手順をすでに実行している場合は、ステージ2にスキップできます。ただし、後でIAMユーザーのセキュリティ認証情報を使用してQRadarをバケットに認証する必要があります。

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

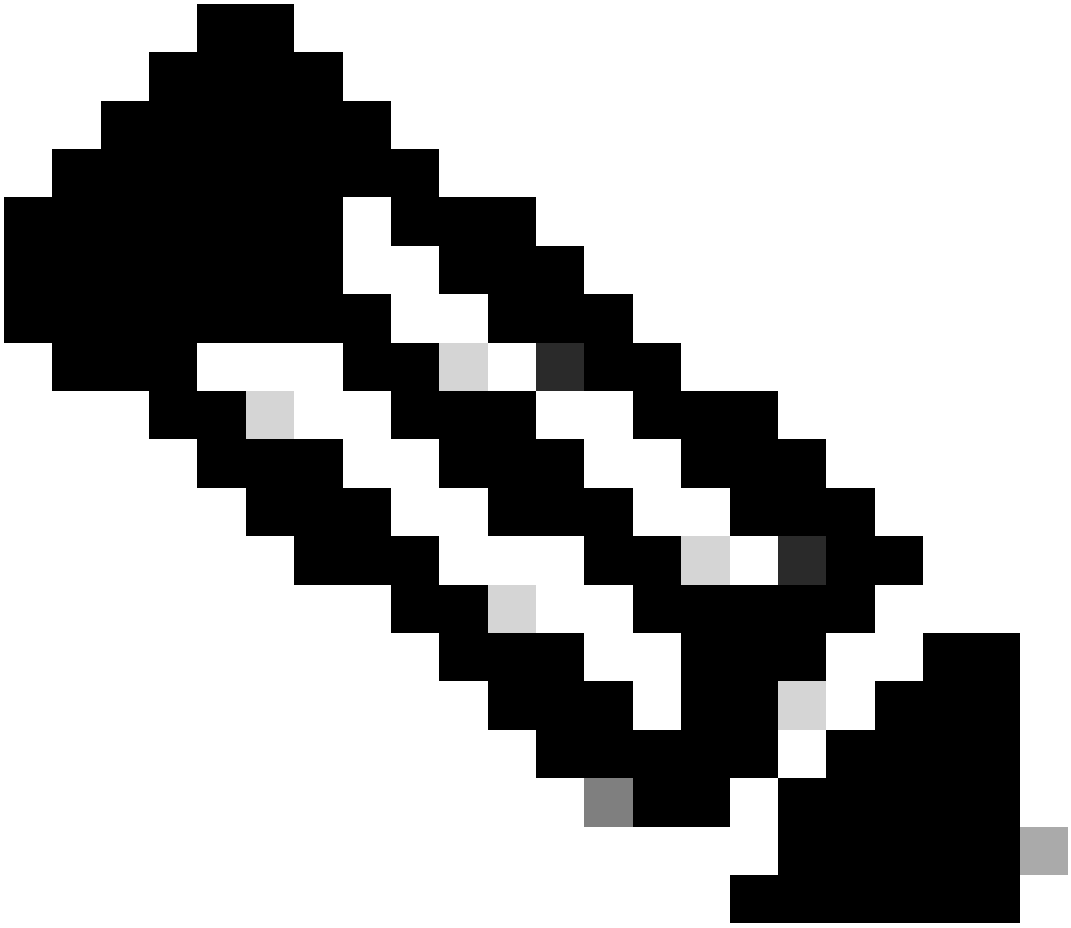
クセスを許可し、S3でファイルをアップロード、ダウンロード、および変更できるようにします。

1. AWSにログインします。
2. 右上隅にあるアカウント名を選択します。
3. ドロップダウンで、Security Credentialsを選択します。

2. その後、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構成全体のマスターアカウント（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、AWSのドキュメントを参照してください。

手順 2

1.「IAMユーザーについて始める」を選択してIAMユーザーを作成し、S3バケットにアクセスします。次に、IAMユーザーを作成できる画面が表示されます。
2.「新規ユーザー」を選択し、フィールドに入力します。



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。

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。 Umbrellaでは、右下のボタンを使用してこれらをダウンロードしてバックアップすることを強く推奨しています。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。

手順 3

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。

1. 作成したばかりのユーザを選択し、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を選択し、ポリシータイプのフィルタに「s3」と入力します。次の2つの結果が表

示されます。

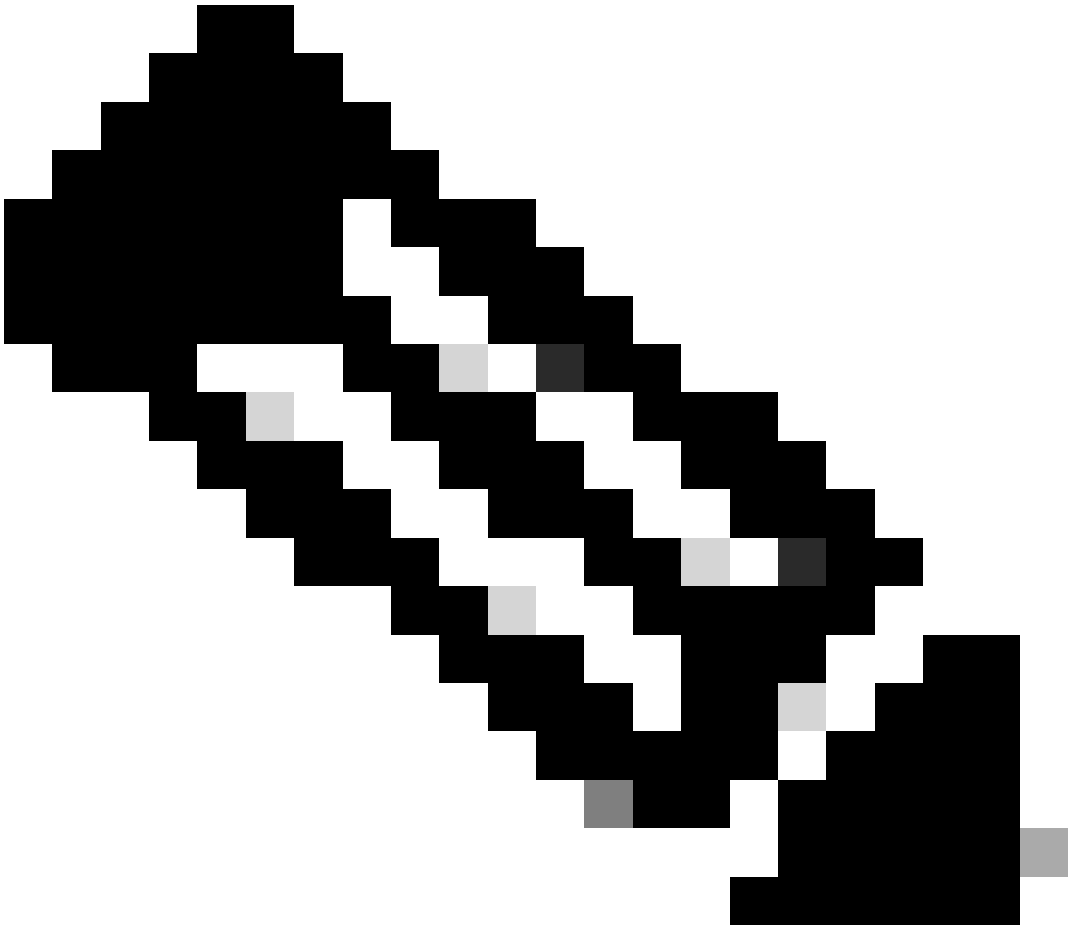
- AmazonS3FullAccess
- AmazonS3ReadOnlyAccess

3. AmazonS3FullAccessを選択し、右下隅にあるAttach Policyを選択します。

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QRadarのセットアップ

QRadarは、アカウントのAWS API呼び出しを記録し、ログファイルを配信するウェブサービスであるAWS CloudTrailサービスを利用します。

QRadarがAmazon S3にアクセスする前に、IBMから次の手順を実行してAmazonサーバー証明書を取得します。この部分は難しいので、必ず正確に指示に従ってください。



注：テストでは、これが期待どおりに動作するように、Firefoxブラウザを使用する必要

があります。

Amazonサーバー証明書を取得するには、DER形式の証明書を適切なQRadarアプライアンスに移動する必要があります。証明書を必要とするQRadarアプライアンスは、Amazon AWS CloudTrailログソースのTarget Event Collectorフィールドに割り当てられているアプライアンスです。

はじめる前に

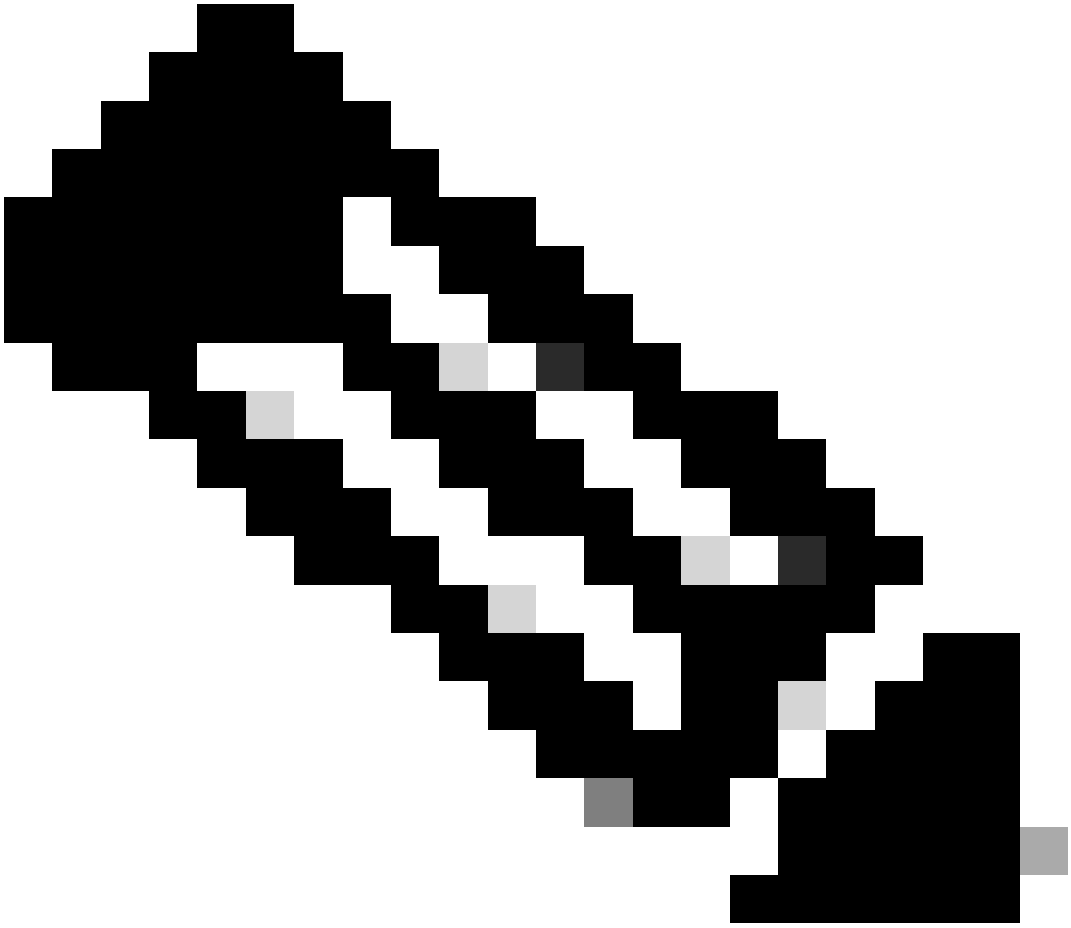
- 証明書は.DER形式である必要があります。
- 拡張子.DERは大文字と小文字が区別され、大文字にする必要があります。
- 証明書を小文字でエクスポートすると、ログソースでイベント収集の問題が発生する可能性があります。

最初のステップ

1. AWS CloudTrail S3バケットにアクセスします： `https://<bucketname>.s3.amazonaws.com`

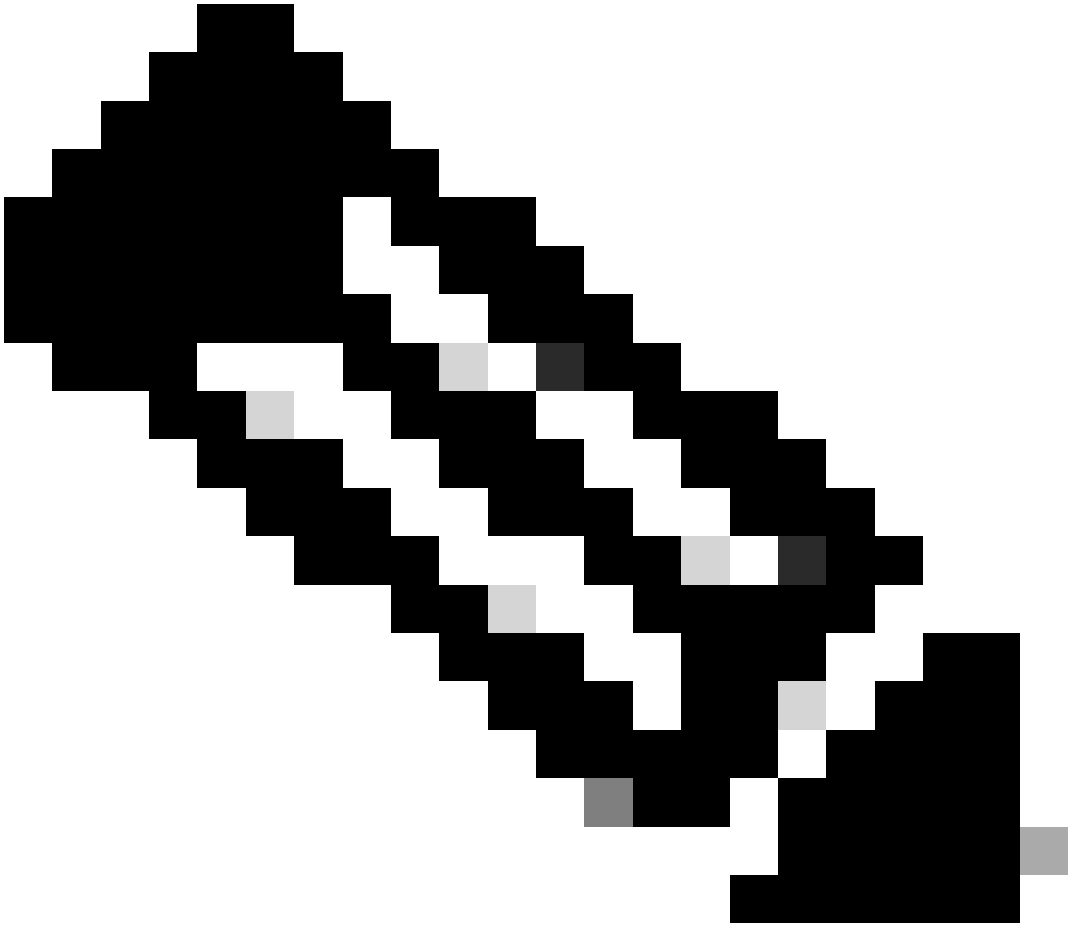
2. Firefoxを使用して、SSL証明書を(.DER)証明書としてAWSからエクスポートします。Firefoxでは、.DER拡張子を使用して必要な証明書を作成できます。

    1. Site Identityアイコン（アドレスバーのロックアイコン）を選択します。
    2. More Information > View Certificateの順に選択し、Detailsタブを選択します。
    3. Exportを選択して、証明書の.DER形式でエクスポートします。



注:.DER拡張子は大文字と小文字が区別され、大文字にする必要があります。

3. .DER証明書を、Amazon AWS CloudTrailログソースを管理するQRadarアプライアンスの/opt/QRadar/conf/trusted_certificatesディレクトリにコピーします。WinSCPを使用してコピーできます。



注：ログソースを管理するQRadarアプライアンスは、Amazon AWS CloudTrailログソースのTarget Event Collectフィールドで識別されます。Amazon AWS CloudTrailログソースを管理するQRadarアプライアンスは、/opt/QRadar/conf/trusted_certificatesに.DER証明書のコピーを保持している必要があります。

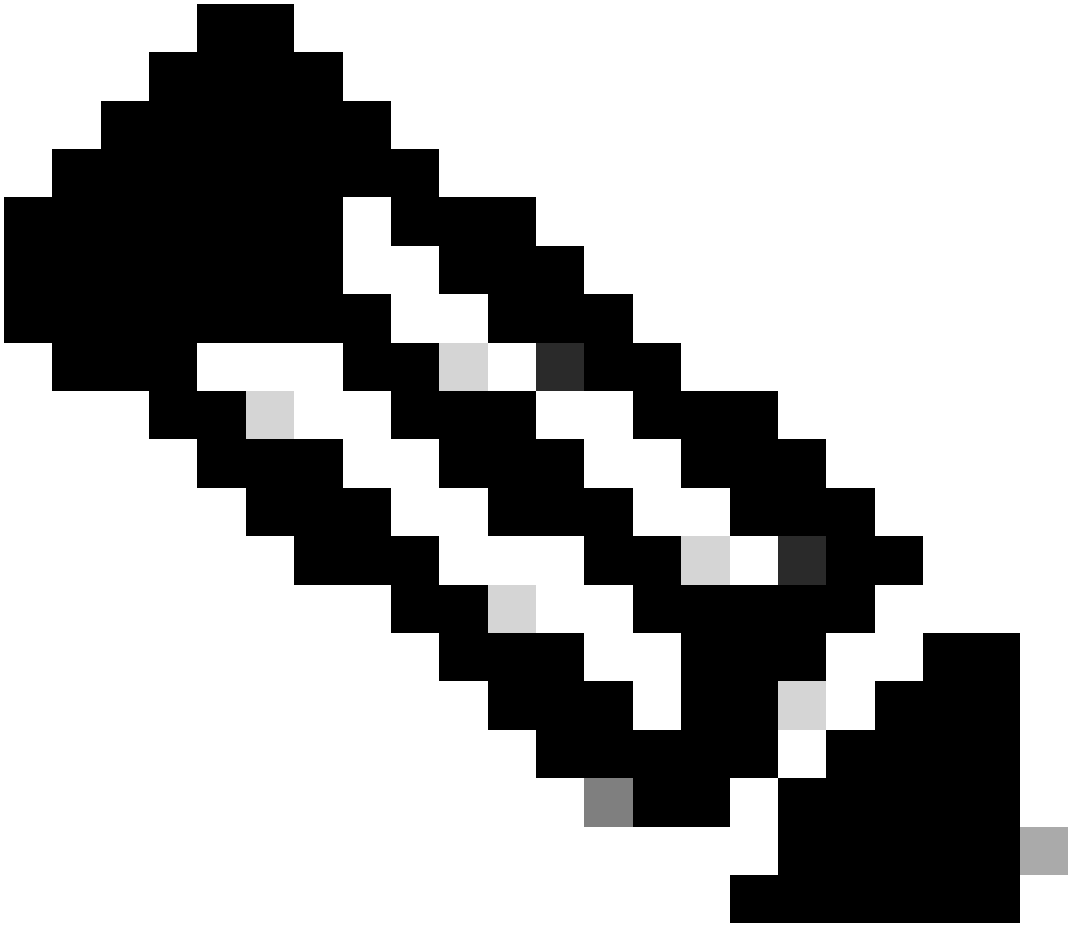
4. 管理ユーザーとしてQRadarユーザー・インタフェースにログインします。

5. Adminタブを選択します。

6. 「ログ・ソース」アイコンを選択します。

7. Amazon AWS CloudTrail ログソースを選択します。

8. ナビゲーションメニューから[Enable/Disable]を選択して無効にし、Amazon AWS CloudTrailログソースを再度有効にします。



注：管理者がログソースを無効から有効に強制的に設定すると、プロトコルはログソースで定義されているとおりにAmazon AWSバケットに接続できます。その後、最初の通信の一部として証明書チェックが行われます。

---

9. 問題が解決しない場合は、ログソース識別子フィールドに正しいAmazon AWSバケット名が含まれていることと、ログソースコンフィギュレーションのリモートディレクトリパスが正しいことを確認してください。

QRadar設定の完了

1. QRadarでは、すべてのプロトコル、DSM、その他の情報が最新であることを確認してください。次の設定でLogFileProtocolを選択します（頻度、開始時刻、繰り返しなどの情報は異なる場合があります）。

2.「ログ・ソース」タブで、「ログ・ソース名」と「ログ・ソースの説明」を入力します。これらは何でも好きなものでよい。

3.S3バケット名、AWSアクセスキー、AWSシークレットキー、およびリモートディレクトリ（おそらくdnslogsですが、設定によって異なります）を入力します。 年などのログソースIDを追加すると、フィルタリングに役立ち、「2019」を含むログのみが抽出されます。

4. Cisco Umbrellaイベントを解析できるLSX(Log Source eXtension)を作成します。（QRadarにインポートした後の状態です）。 LSXを正確に作成する方法の詳細については、IBM Webサイトを参照してください。これは単なる例です。ログから取得するデータは、ユースケースによって異なります。

5. AWSアクセスキーとAWSシークレットキーが正常にコピーされ、ログソースコンフィギュレーションに貼り付けられていることを再確認します。

6. GZIPプロセッサとRegEx Based Multilineのイベントジェネレータを選択します。行ごとに1つのイベントを取得する最も簡単な方法は、次の開始パターンRegExを使用することです。

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}","")
```

必ずLog Source Extension and Use Conditionを選択してから、ログソースを保存してください。

7. QRadarで完全展開を実行します。

次に、ログソースはRestAPIを使用して、指定したクレデンシャルとキーでバケットに接続し、イベントの取得を開始します。

追加情報

バケットロギングの有効化

バケットロギングを有効にするには、AWSのドキュメントを読み、記載されている手順を実行します。デフォルトでは、ロギングは無効になっています。有効にすると、/logsという名前の新しいフォルダがバケットルートに存在し、GETS、PUTS、およびDELETESの情報が表示されます。

ログサイクルの管理

S3を使用している場合は、バケット内のデータのライフサイクルを管理して、ログを保持する期間を延長できます。外部ログ管理を使用している目的に応じて、期間は非常に短いか非常に長い可能性があります。たとえば、24時間後にS3バケットからログをダウンロードしてオフラインで保存したり、ログをクラウドに無期限で保持したりできます。

デフォルトでは、Amazonはデータを無期限にバケットに保存しますが、無制限のストレージはバケットの維持コストを増加させます。S3ライフサイクルの詳細については、AWSのドキュメントを参照してください。

バケットのライフサイクルを構成する手順は、次のとおりです。

1. Properties > Lifecycleの順に選択します。

2. Add a Ruleを選択してから、Apply the Ruleをバケット全体（またはサブフォルダとして設定し

た場合はサブフォルダ）に適用します。

3.「オブジェクトに対するアクション」で「削除」や「アーカイブ」などを選択し、期間と、Glacierストレージを使用してAmazonコストを削減するかどうかを選択します。（Glacierは「コールド」オフラインストレージで、アクセスに時間がかかりますが、はるかに安価です）。

ログを別の方法（内部バックアップソリューションなど）で管理する場合は、S3からログをダウンロードし、別の方法で保存することができます。

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。