Cisco Secure Cloud Analytics

Amazon Web サービスの統合クイックスタートガイド

目次

パブリッククラウドのモニタリング Amazon Web Services 向けの設定

Cisco Secure Cloud Analytics パブリッククラウドのモニタリング（旧 Stealthwatch Cloud パブリック クラウド モニターリング）は、Amazon Web Services（AWS）向けの可視化、脅威特定、およびコンプライアンスサービスです。Secure Cloud Analytics は、AWS パブリック クラウド ネットワークから仮想プライベートクラウド（VPC）フローログなどのネットワークトラフィック データを取得します。次に、そのデータに対して分析を実行して脅威と侵害の兆候を検出することによって、ダイナミック エンティティ モデリングを実行します。Secure Cloud Analytics は、適切な権限を持つクロスアカウント IAM ロールを使用して、AWS アカウントから直接 VPC フロー ログを消費します。さらに、Secure Cloud Analytics は、追加のコンテキストとモニターリングのために、その他のデータ ソース（CloudTrail や IAM など）を消費することができます。

フローログを保存する **S3 バケット**と、これらのフローログを取り込む Secure Cloud Analytics を設定するには、次の手順を実行します。

1. AWS で、VPC の VPC フローロギングを有効にし、フローログのエクスポート先の S3 バケットを設定します。詳細については、「**S3 バケット フロー ログ データ ストレージの設定**」を参照してください。
2. AWS で、IAM アクセスポリシーと IAM ロールを設定して、Secure Cloud Analytics のフロー ログへのアクセスと取得を可能にします。詳細については、「**フローログデータにアクセスするための AWS 権限の設定**」および「**フローログデータにアクセスするための IAM ロールの設定**」を参照してください。
3. Secure Cloud Analytics Web ポータルの UI で、S3 バケットと IAM ロールを使用して構成を更新し、AWS フローログデータの取得を可能にします。詳細については、「**S3 バケットからフローログデータにアクセスするための Secure Cloud Analytics の設定**」を参照してください。

S3 バケット フロー ログ データ ストレージの設定

フローログデータを既存の S3 バケットに保存するか、フローログを有効にするときに新しい S3 バケットを作成できます。次に、フローログモニタリングのストレージコストを削減するために、不要になったフローログを削除するようにバケットを設定することをお勧めします。

> 複数の既存の VPC で VPC フローログを設定するには、設定を支援するスクリプト（https://github.com/obsrvbl-oss/aws-setup）を利用できます。AWS Cloudshell を使用してスクリプトを実行する方法の詳細については、https://docs.aws.amazon.com/cloudshell/latest/userguide/getting-started.html を参照してください。

S3 バケットの VPC への関連付け

1. AWS 管理コンソールにログインして、VPD ダッシュボードにアクセスします。
2. **使用している VPC** を選択します。
3. VPC を右クリックし、[フローログの作成（Create Flow Log）] を選択します。
4. [フィルタ（Filter）] ドロップダウンから、次のオプションのいずれかを選択します。
    - 許可された IP トラフィックと拒否された IP トラフィックの両方を記録するには、[すべて（All）] を選択し、Secure Cloud Analytics で両方のタイプのトラフィックを表示できるようにします。

- [許可(Accept)] を選択すると、許可された IP トラフィックのみが記録され、Secure Cloud Analytics には許可されたトラフィックのみが表示されます。

5. [宛先(Destination)] に [S3バケットに送信(Send to an S3 bucket)] を選択します。
6. フローログデータを保存する S3 バケット ARN を入力します。

> S3 バケットが存在しない場合は、変更をコミットした後に AWS によって作成されます。

7. [ログレコード形式(Log record format)] ペインで、[カスタム形式(Custom format)] を選択します。
8. [ログ形式(Log format)] ドロップダウンリストからすべての属性を選択します。
9. [作成(Create)] をクリックします。

> IP に基づいてこの S3 バケットへのアクセスを制限する場合は、関連する IP との通信が許可されていることを確認してください。Secure Cloud Analytics Web ポータルに移動し、[設定(Settings)] > [統合(Integrations)] > [AWS] > [バージョン情報(About)] を選択すると、Secure Cloud Analytics で使用されるパブリック IP のリストが表示されます。

コストを最小化するための S3 バケットの設定(推奨)

> 次の設定では、フローログを含むバケット内のすべてのオブジェクトが 1 日後に削除されます。Secure Cloud Analytics で使用するためにのみ VPC フローログをこのバケットに保存する場合は、この設定をお勧めします。

1. S3 の AWS コンソールにログインします。
2. [バケット(Buckets)] リストで、VPC フローログを保存するバケットの名前を選択します。
3. [管理(Management)] タブを選択します。
4. [ライフサイクルルール(Lifecycle rules)] セクションで、[ライフサイクルルールの作成(Create lifecycle rule)] をクリックします。
5. ライフサイクルルールの一意の名前を入力します(例:`Expire after 1 day`)。
6. ライフサイクルルールの範囲として、[このルールをバケット内のすべてのオブジェクトに適用する(This rule applies to all objects in the bucket)] を選択します。
7. [このルールがバケット内のすべてのオブジェクトに適用されることに同意する(I acknowledge that this rule will apply to all objects in the bucket)] チェックボックスをオンにします。
8. [ライフサイクルルールアクション(Lifecycle rule actions)] で、[以前のバージョンのオブジェクトを完全に削除(Permanently delete previous versions of objects)] を選択します。
9. [オブジェクトの非現行バージョンを完全に削除(Permanently delete noncurrent versions of objects)] で、[オブジェクトが非現行になってからの日数(Days after objects become noncurrent)] を 1 に設定します。
10. [ルールの作成(Create rule)] をクリックします。
11. [ライフサイクル設定(Lifecycle Configuration)] に戻り、作成したルールの横にあるオプションボタンをクリックし、[アクション(Actions)] ドロップダウンで [ルールの有効化(Enable rule)] をクリックします。

フローログデータにアクセスするための AWS 権限の設定

Secure Cloud Analytics Web に表示される JSON 構成を使用して、新しい IAM ポリシーを作成します。このポリシーには、Secure Cloud Analytics によるフローログデータへのアクセスを許可する権限が含まれています。

AWS クラウドポスチャを評価するには、AWS の IAM ポリシーに追加のアクセス許可を付与する必要があります。Secure Cloud Analytics の [AWSの概要（AWS About）] ページに、「`"Sid": "CloudCompliance"`」で始まる JSON オブジェクトの必要な権限が一覧表示されます。

Secure Cloud Analytics と AWS を初めて統合するお客様で、これらの追加の権限を付与したくない場合は、このオブジェクトを削除できますが、クラウドポスチャレポートは使用できなくなります。

フローログデータにアクセスする権限を持つポリシーの作成

1. Secure Cloud Analytics Web ポータルに管理者としてログインします。
2. [設定（Settings）] > [統合（Integrations）] > [AWS] > [情報（About）] を選択します。
3. AWS リソースにアクセスする手順を確認します。
4. ポリシードキュメントの JSON 設定をコピーし、プレーンテキストエディタに貼り付けます。
5. Secure Cloud Analytics で AWS Cloud ポスチャを評価するために必要な追加の権限について、`"Sid": "CloudCompliance"` で始まる JSON オブジェクトを確認します。次の選択肢があります。
    - これらの追加の権限を付与しない場合は、`"Sid": "CloudCompliance"` で始まる JSON オブジェクトを削除します。Secure Cloud Analytics で AWS クラウドポスチャを評価することはできなくなります。次の手順に進みます。
    - これらの追加の権限を付与して AWS クラウドポスチャを評価する場合は、次の手順に進みます。
6. AWS 管理コンソールにログインして、IAM ダッシュボードにアクセスします。
7. [ポリシー（Policies）] を選択します。
8. [ポリシーの作成（Create Policy）] をクリックします。
9. [JSON] タブを選択します。
10. プレーンテキストエディタからポリシーの JSON 設定をコピーし、JSON エディタに貼り付けます。
11. [ポリシーの確認（Review policy）] をクリックします。

    ポリシー検証ツールがエラーをスローした場合は、コピーして貼り付けたテキストを確認します。
12. [名前（Name）] フィールドに `swc_policy` と入力します。
13. `Secure Cloud Analytics` がイベントとログデータを読み取ることを許可するポリシーなどの [説明（Description）] を入力します。
14. [ポリシーの作成（Create Policy）] をクリックします。

フローログデータにアクセスするための IAM ロールの設定

IAM ポリシーを作成したら、Secure Cloud Analytics によるフローログデータへのアクセスを許可する IAM ロールを作成します。

フローログデータにアクセスする権限を持つ IAM ロールの設定

1. AWS 管理コンソールにログインして、IAM ダッシュボードにアクセスします。
2. [ロール(Role)] を選択します。
3. [ロールを作成(Create role)] を選択します。
4. [別のAWSアカウント(Another AWS account)] ロールタイプを選択します。
5. [アカウントID(Account ID)] フィールドに 757972810156 と入力します。
6. [外部IDが必要(Require external ID)] オプションを選択します。
7. 外部 ID として Secure Cloud Analytics のWeb ポータル名を入力します。

   > Web ポータル名は、`https://`**`portal-name`**`.obsrvbl.com` の形式でポータル URL に埋め込まれます。たとえば、Web ポータルの URL が `https://`**`example-client`**`.obsrvbl.com` の場合、外部 ID として **`example-client`** を入力します。URL 全体を入力すると、統合設定は失敗します。

8. [次へ:権限(Next: Permissions)] をクリックします。
9. 作成した `swc_policy` ポリシーを選択します。
10. [次へ:タギング(Next: Tagging)] をクリックします。
11. [次へ:レビュー(Next: Review)] をクリックします。
12. [ロール名(Role name)] として `swc_role` を入力します。
13. クロスアカウントアクセスを許可するロールなどの [説明(Description)] を入力します。
14. [ロールを作成(Create Role)] をクリックします。
15. ロール ARN をコピーし、プレーンテキストエディタに貼り付けます。

S3 バケットからフローログデータにアクセスするための Secure Cloud Analytics の設定

フローログの構成を完了するには、Secure Cloud Analytics Web ポータルで IAM ロールと S3 バケット名を入力し、S3 バケット名を追加するときに Secure Cloud Analytics によって提供される構成を使用して AWS で S3 バケットポリシーを変更します。

アカウントで VPC フローログを有効にしたばかりの場合は、10 分待ってから、フローログデータを取得するように Secure Cloud Analytics 設定してください。S3 バケットにログが含まれない、その **S3 パス**名を追加すると、エラーが返されることがあります。AWS は、約 10 分ごとに VPC フローログを生成します。

S3 バケットに保存されているフローログデータを取り込むための Secure Cloud Analytics の設定

1. Secure Cloud Analytics Web ポータルに管理者アカウントでログインします。
2. [設定(Settings)] > [統合(Integrations)] > [AWS] > [クレデンシャル(Credentials)] を選択します。
3. [新しいクレデンシャルの追加(Add New Credentials)] をクリックします。
4. 分かりやすい**名前**を入力します。

5. 保存したロール ARN をプレーンテキストエディタからコピーし、[ロールARN（Role ARN）] フィールドに貼り付けます。
6. [作成（Create）] をクリックします。
7. [設定（Settings）] > [統合（Integrations）] > [AWS] > [VPCフローログ（VPC Flow Logs）] を選択します。
8. [VPCフローログを追加（Add VPC Flowlog）] をクリックします。
9. [S3パス（S3 Path）] フィールドに、フローログデータを含む S3 バケットの名前を入力します。

   > 複数の設定済み S3 バケットを追加できます。Secure Cloud Analytics と AWS の統合には、1 つの IAM アクセス ポリシーとロールを設定する必要だけがあります。

10. S3 バケットの [クレデンシャル（Credentials）] を選択し、[設定手順（Setup Instructions）] をクリックします。

    S3 バケットパスとクレデンシャルを使用して更新されたバケットポリシー JSON 設定が表示されます。
11. 表示されたバケットポリシー JSON 設定をコピーし、プレーンテキストエディタに貼り付けます。

    > このブラウザウィンドウを開いたままにします。S3 バケットポリシーを設定した後、Secure Cloud Analytics Web ポータルの設定を完了します。

Secure Cloud Analytics がフローログデータを取り込むための S3 バケットポリシーの設定

1. AWS 管理コンソールにログインして、IAM ダッシュボードにアクセスします。
2. IAM ダッシュボードで、[ポリシー（Policies）] を選択します。
3. [ポリシーの作成（Create Policy）] をクリックします。
4. [JSON] タブを選択します。
5. プレーンテキストエディタからバケットポリシー JSON 設定をコピーし、ポリシーエディタに貼り付けて、既存のバケットポリシーを上書きします。
6. [ポリシーの確認（Review policy）] をクリックします。
7. ポリシーの [名前（Name）] を入力します。
8. 任意でポリシーの [説明（Description）] を入力します。
9. [ポリシーの作成（Create Policy）] をクリックします。
10. IAM ダッシュボードで、[ロール（Roles）] を選択します。
11. `swc_role` を選択します。
12. [権限（Permissions）] タブで、[ポリシーをアタッチ（Attach policies）] をクリックします。
13. ステップ 6 で入力したポリシー名を選択します。
14. [ポリシーをアタッチ（Attach policy）] をクリックします。
15. Secure Cloud Analytics Web ポータルで、入力した S3 バケットパスとログイン情報に対して [作成（Create）] をクリックします。

S3 バケットからフローログデータを取り込むための適切な権限がない場合、システムはエラーを表示します。サポートが必要な場合は、シスコサポートにポータル名と S3 バケット名をご連絡ください。

AWS との統合の確認

AWS の統合を完了すると、[設定(Settings)] メニューの [センサー(Sensors)] ページに、次の名前の新しい センサーが表示されます。

`AWS: S3-bucket-name`

このセンサーエントリには統合の健全性または S3 バケット名が表示されますが、センサーのページから直接設定することはできません。

AWS の構成を完了してからトラフィックとエンティティデータの表示が開始されるまでに最大 24 時間かかります。

AWS 統合の確認

1. Secure Cloud Analytics Web ポータルに管理者としてログインします。
2. [設定(Settings)] > [センサー(Sensors)] を選択します。ページに S3 バケット名が表示されていることを確認します。
3. [統合(Integrations)] > [AWS] > [権限(Permissions)] の順に選択します。表示された AWS 権限が期待どおりであることを確認します。

関連リソース

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html [英語] を参照してください。
- 60 日間の無料トライアルに登録するには、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html [英語] にアクセスしてください。
- ドキュメントリソースについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html [英語] を参照してください。
- Secure Cloud Analytics 初期導入ガイドなど、インストールおよびコンフィギュレーション ガイドについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html [英語] を参照してください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- Secure Cloud Analytics 無料トライアルの試用時に電子メールでケースを開く場合：
  swatchc-support@cisco.com

変更履歴

リビジョン	改訂日	説明
1.0	2018 年 3 月 7 日	最初のバージョン。
1.1	2019 年 5 月 30 日	S3 バケットの統合情報について更新。
1.2	2019 年 6 月 14 日	設定のマイナー更新。
1.3	2019 年 10 月 22 日	設定手順を更新。
1.4	2020 年 8 月 13 日	フローログのシンタクッス書式のレンダリングを修正。
1.5	2020 年 10 月 16 日	UI の更新に基づく更新、およびフローログ形式を明記。
1.6	2021 年 1 月 26 日	Secure Cloud Analytics ポスチャ管理の更新（必要な権限など）。
1.7	2021 年 2 月 18 日	UI 再構築のための更新。
2.0	2021 年 11 月 3 日	製品のブランド名を更新。
3.0	2022 年 8 月 1 日	「サポートへの問い合わせ」セクションを追加。 パブリック IP に関する注記を追加。 ドキュメントのタイトルを更新しました。
3.1	2023 年 1 月 20 日	「コストを最小化するための S3 バケットの設定」セクションを追加。

著作権情報