Cisco Secure Cloud Analytics

Google Cloud Platform 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 Google Cloud Platform 向けのパブリック クラウド モニターリング設定

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、Google Cloud Platform（GCP）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。Cisco 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 データを取り込みます。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。Cisco Secure Cloud Analytics は、適切な権限を持つクロスアカウント IAM サービス アカウントを使用して、GCP アカウントから直接 VPC フロー ログを消費します。

単一 GCP プロジェクトの設定

単一プロジェクトのフローログデータを生成して保存し、Cisco Secure Cloud Analytics がそのデータを取り込むように GCP を設定するには、次の手順を実行します。

1. GCP で、フローログおよびその他のデータを表示し、JSON クレデンシャルを保存するための適切な権限を持つサービスアカウントを設定します。詳細については、「**VPC フローログを表示するためのサービスアカウントの構成**」を参照してください。
2. GCP で、メトリック収集のためのフローロギングと Stackdriver Monitoring API を有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の構成**」を参照してください。
3. Cisco Secure Cloud Analytics Web ポータル UI で、サービスアカウントの JSON クレデンシャルをアップロードします。詳細については、「**JSON ログイン情報のアップロード**」を参照してください。

高スループットの GCP 環境がある場合は、必要に応じて Pub/Sub を構成するとフローログデータを Cisco Secure Cloud Analytics に配信できます。

> 統合が GCP Stackdriver API の割り当てを超えたり、フローデータが削除されたりしないように、Pub/Sub を構成することを強くお勧めします。

1. 導入が高スループットであるかどうかを判断します。詳細については、「**高スループット環境の特定**」を参照してください。
2. フローログデータを取り込むための Pub/Subトピックと、フローログデータを配信するトピックの Pub/Sub サブスクリプションを設定します。詳細については、「**GCP Pub/Sub サブスクリプションの作成**」を参照してください。

複数の GCP プロジェクトの設定

複数プロジェクトのフローログデータを生成して保存し、Cisco Secure Cloud Analytics がそのデータを取り込むように GCP を設定するには、次の手順を実行します。

1. GCP で、フローログおよびその他のデータを表示し、JSON クレデンシャルを保存するための適切な権限を持つサービスアカウントを設定します。単一サービスアカウントを使用するように追加のプロジェクトを設定します。詳細については、「**VPC フローログを表示するためのサービスアカウントの構成**」を参照してください。
2. GCP で、サービスアカウントを使用する追加のプロジェクトを設定します。詳細については、「**複数のプロジェクトの VPC フローログを表示するための単一サービスアカウントの設定**」を参照してください。
3. GCP で、メトリック収集のためのフローロギングと Stackdriver Monitoring API を有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の構成**」を参照してください。
4. Cisco Secure Cloud Analytics Web ポータル UI で、サービスアカウントの JSON クレデンシャルをアップロードします。詳細については、「**JSON ログイン情報のアップロード**」を参照してください。

高スループットの GCP 環境がある場合は、必要に応じて Pub/Sub を構成するとフローログデータを Cisco Secure Cloud Analytics に配信できます。

> 統合が GCP Stackdriver API の割り当てを超えたり、フローデータが削除されたりしないように、Pub/Sub を構成することを強くお勧めします。

1. 導入が高スループットであるかどうかを判断します。詳細については、「**高スループット環境の特定**」を参照してください。
2. フローログデータを取り込むための Pub/Subトピックと、フローログデータを配信するトピックの Pub/Sub サブスクリプションを設定します。詳細については、「**GCP Pub/Sub サブスクリプションの作成**」を参照してください。
3. 追加のプロジェクト向けに、追加の Pub/Sub トピックとサブスクリプションを設定します。詳細については、「**Pub/Sub トピックおよびサブスクリプションの設定**」を参照してください。

VPC フローログを表示するためのサービスアカウントの構成

IAM サービスアカウントを設定するには、Cisco Secure Cloud Analytics用の情報を収集するために必要な権限を持つカスタムロールを作成します。次に、サービスアカウントを作成し、カスタムロールを含む複数のロールを関連付けます。GCP は、秘密キー情報を使用してアカウントを作成します。秘密キーを安全な場所に保存します。

1. GCP コンソールで、[IAM と管理(IAM & Admin)] > [IAM] > [サービスアカウント(Service Accounts)] を選択します。
2. [サービスアカウントの作成(Create Service Account)] をクリックします。
3. [サービスアカウント名(Service Account Name)] フィールドに `logs-viewer` と入力します。Cloud コンソールは、この名前に基づいてサービスアカウント ID を生成します。必要に応じて ID を編集します。後で ID を変更することはできません。
4. [作成して続行(Create and Continue)] をクリックします。
5. [ロールの選択(Select a role)] ドロップダウンをクリックし、[ログビューア(Logs Viewer)] ロールを選択します。
6. [別のロールの追加(Add Another Role)] をクリックします。
7. 新しい [ロールの選択(Select a role)] ドロップダウンをクリックし、[コンピューティングビューア(Compute Viewer)] ロールを選択します。
8. 手順 6 と 7 を繰り返して、[モニタリングビューア(Monitoring Viewer)] ロールと [Pub/Sub サブスクライバ(Pub/Sub Subscriber)] ロールを追加します。
9. (オプション)クラウドポスチャ分析の場合は、手順 6 と 7 を繰り返して、[セキュリティ センター サービス エージェント(Security Center Service Agent)] ロールと [セキュリティレビューア(Security Reviewer)] ロールを追加します。
10. [続行(Continue)] をクリックします。
11. [キーの作成(Create Key)] をクリックします。
12. [キータイプ(Key type)] として [JSON] を選択し、[作成(Create)] をクリックします。

    > ⚠ 生成される JSON 秘密キー ファイルにはアカウントが VPC フロー ログにアクセスするために必要な情報が含まれているので、ファイルを安全な場所に保存してください。

13. JSON 秘密キーを保存したら、[閉じる(Close)] をクリックします。
14. [完了(Done)] をクリックします。

> ⓘ GCP 環境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ます。Cisco Secure Cloud Analytics Web ポータルに移動し、[設定(Settings)] > [統合(Integrations)] > [GCP] > [バージョン情報(About)] を選択すると、Cisco 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。

次の作業

- **単一プロジェクト**をモニターする場合は、展開でフローロギングを有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の構成**」を参照してください。
- **複数のプロジェクト**をモニターする場合は、展開でフローロギングを有効にする前に、サービスアカウントを追加の各プロジェクトに関連付けます。詳細については、「**複数のプロジェクトの VPC フローログを表示するための単一サービスアカウントの設定**」を参照してください。

複数のプロジェクトの VPC フローログを表示するための単一サービスアカウントの設定

GCP 展開で**複数のプロジェクトをモニターする**場合は、単一サービスアカウントを使用してプロジェクトをモニターできます。モニターする各プロジェクトのクラウドリソースマネージャ API を有効にし、作成したサービスアカウントの電子メールアドレスおよび適切なロール権限をそのプロジェクトに追加します。

サービスアカウントの電子メールアドレスの検索

1. GCP コンソールで、[IAM と管理（IAM & Admin）] > [IAM] を選択します。
2. 新しいサービスアカウントの編集アイコンをクリックします。
3. [メンバー（Member）] の次の形式の電子メールアドレスをコピーし、プレーンテキストエディタに貼り付けます。

   `[account-name]@[project-id].[gcp-info].com`

追加プロジェクトに対する Stackdriver Monitoring API の有効化

1. GCP コンソールで、[API とサービス（APIs & Services）] > [ライブラリ（Library）] を選択します。
2. プロジェクトの [選択（Select）] をクリックします。
3. [クラウドリソースマネージャAPI（Cloud Resource Manager API）] を検索し、[クラウドリソースマネージャAPI（Cloud Resource Manager API）] を選択して、[有効（Enable）] をクリックします。

追加プロジェクトへのサービスアカウントの追加

1. GCP コンソールで、[IAM と管理（IAM & Admin）] > [IAM] を選択します。
2. [プロジェクト（Project）] ドロップダウンから追加のプロジェクトを選択します。
3. [追加（Add）] をクリックします。
4. プレーンテキストエディタからメンバーサービスアカウントの電子メールアドレスをコピーし、[新しいメンバー（New members）] フィールドに貼り付けます。
5. [ロールを選択（Select a role）] ドロップダウンをクリックします。Enter を押して、[ログビューア（Logs Viewer）] ロールを選択します。
6. [別のロールの追加（Add Another Role）] をクリックします。
7. 新しい [ロールを選択（Select a role）] ドロップダウンをクリックします。Enter を押して、[計算ビューア（Compute Viewer）] ロールを選択します。

8. 手順 6 と 7 を繰り返して、[モニタリングビューア（Monitoring Viewer）] ロールと [Pub/Sub サブスクライバ（Pub/Sub Subscriber）] ロールを追加します。
9. （オプション）クラウドポスチャ分析の場合は、手順 6 と 7 を繰り返して、[セキュリティ センター サービス エージェント（Security Center Service Agent）] ロールと [セキュリティレビューア（Security Reviewer）] ロールを追加します。
10. [保存（Save）] をクリックします。
11. 追加プロジェクトごとにステップ 2 ～ 9 を繰り返します。

次の作業

- 展開でフローロギングを有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の構成**」を参照してください。

VPC フローログを生成して権限を有効化するための GCP の構成

サービスアカウントを設定したら、サブネットごとに GCP 展開でフローロギングを有効にした後で、Cisco Secure Cloud Analytics による取り込みを可能にします。その後、Stackdriver Monitoring API を有効にして、さまざまな GCP メトリックを収集します。

VPC フロー ログを生成するための GCP サブネットの構成

1. GCP コンソールから、[VPC ネットワーク(VPC network)] を選択します。
2. サブネットを選択します。
3. [編集(Edit)] をクリックします。
4. [フローログ(Flow logs)] から [オン(On)] を選択します。
5. [保存(Save)] をクリックします。設定するサブネットごとにステップ 1 ～ 4 を繰り返します。

Stackdriver Monitoring API の有効化(推奨)

Cisco Secure Cloud Analytics この権限を GCP Cloud 関数呼び出し回数の急増アラートに使用して統合の正常性とステータスをモニターします。

1. GCP コンソールで、API を有効にするクラウドプロジェクトを選択し、[API とサービス(APIs & Services)] ページに移動します。
2. [APIとサービスの有効化(Enable APIs and Service)] をクリックします。
3. 検索フィールドに、**Monitoring** と入力して [Stackdriver Monitoring API] を選択します。
4. API が有効になっていない場合は、[有効(Enable)] をクリックします。
5. [保存(Save)] をクリックします。

次の作業

- 保存した JSON クレデンシャルを Cisco Secure Cloud Analytics ポータルにアップロードします。詳細については、を参照してください。詳細については、「**JSON ログイン情報のアップロード**」を参照してください。

JSON ログイン情報のアップロード

構成を完了するには、JSON サービスアカウントのログイン情報を Cisco Secure Cloud Analytics Web ポータルの UI にアップロードします。

1. サイト管理者として Cisco Secure Cloud Analytics Web ポータルにログインします。
2. [設定（Settings）] > [統合（Integrations）] > [GCP] > [クレデンシャル（Credentials）] を選択します。
3. [クレデンシャル ファイルのアップロード（Upload Credentials File）] をクリックし、JSON クレデンシャル ファイルを選択します。

次の作業

- 高スループット環境かどうかを確認し、そうである場合は、Pub/Sub がフローログデータを取り込むように構成します。

高スループット環境の特定

高スループット環境でのフローデータの送信を保証するため、Pub/Sub トピックとサブスクリプションを設定できます。VCP フローデータが GCP によって課されるロギング読み取り制限を超える場合は、GCP Pub/Sub コレクションが理想的であり、大規模な GCP 展開では強く推奨されます。

GCP ロギングクォータの確認

既存のログベースの GCP 統合で GCP のロギング制限を超えているかどうかを確認するには、次の手順を実行します。

1. https://console.cloud.google.com/apis/api/logging.googleapis.com/quotas にログインします。
2. プロジェクトを選択します。
3. *Quota exceeded errors count (1 min) – Read requests per minute* を検索します。クオータを超過している場合、GCP Pub/Sub の詳細については、「**GCP Pub/Sub サブスクリプションの作成**」を参照してください。

GCP Pub/Sub サブスクリプションの作成

GCP 展開のトラフィックスループットが高い場合は、フローログデータ配信用に Pub/Sub を設定することを推奨します。フローログデータの取り込み用に Pub/Sub を設定するには、プライマリプロジェクト ID を取得し、ログエクスポートシンクを作成してから、トピックの Pub/Sub サブスクリプションを作成します。

GCP プロジェクト ID の検索

1. GCP コンソールで、[リソースの管理（Manage resources）] を選択します。
2. プライマリプロジェクトを選択し、プロジェクト **ID** をコピーします。
3. プロジェクト ID をテキストエディタに貼り付けます。

プロジェクト用の GCP ログエクスポートシンクの作成

1. GCP コンソールで、[Stackdriver ロギング（Stackdriver Logging）] > [ログルータ（Logs Router）] を選択します。
2. [シンクを作成（Create Sink）] をクリックします。
3. ログエントリの上にある [ラベルまたはテキスト検索によるフィルタ（Filter by label or text search）] ドロップダウンフィールドから、[高度なフィルタに変換（Convert to advanced filter）] を選択します。
4. 次をコピーし、プレーンテキストエディタに貼り付けます。

```
                    resource.type="gce_subnetwork"
logName="projects/MY_PROJECT_
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

5. `MY_PROJECT_NAME` をプロジェクト ID に置き換えます。
6. 更新されたテキストをコピーし、[ラベルまたはテキスト検索によるフィルタ（Filter by label or text search）] フィールドに貼り付け、既存のテキストを上書きします。
7. [シンクを編集（Edit Sink）] ペインの [シンク名（Sink Name）] フィールドに `vpc_flows-sink` と入力します。
8. [シンクサービス（Sink Service）] ドロップダウンから [Pub/Sub] を選択します。
9. [シンクの宛先（Sink Destination）] ドロップダウンから [新しいクラウドPub/Subトピックの作成（Create new Cloud Pub/Sub topic）] を選択します。
10. [名前（Name）] フィールドに `vpc_flows-topic` と入力し、[作成（Create）] をクリックします。
11. [シンクを作成（Create Sink）] をクリックします。

プロジェクト用の GCP Pub/Sub サブスクリプションの作成

1. GCP コンソールで、[Pub/Sub] > [トピック(Topics)] を選択します。
2. `vpc_flows-topic` のコンテキストメニューから [サブスクリプションを作成(Create Subscription)] を選択します。
3. [サブスクリプション名(Subscription Name)] フィールドに `swc_subscription` と入力します。
4. [配信タイプ(Delivery Type)] で [プル(Pull)] を選択します。
5. [確認期限(Acknowledgment Deadline)] フィールドに `600` 秒と入力します。
6. [メッセージ保持期間(Message Retention Duration)] フィールドに `2` 時間と入力します。
7. [確認応答メッセージの保持(Retain Acknowledged Messages)] をオフにします。
8. [作成(Create)] をクリックします。

次の作業

- **複数のプロジェクト**をモニターしている場合は、追加プロジェクトごとに、Pub/Sub トピックとサブスクリプションを設定します。詳細については、「**Pub/Sub トピックおよびサブスクリプションの設定**」を参照してください。

Pub/Sub トピックおよびサブスクリプションの設定

GCP 展開で複数のプロジェクトをモニターする場合は、プライマリプロジェクトの Pub/Sub を設定した後、プライマリプロジェクト ID を参照する追加プロジェクトごとに、ログエクスポートシンクと Pub/Sub サブスクリプションを作成します。

追加プロジェクト用の GCP ログエクスポートシンクの作成

1. GCP コンソールで、プライマリプロジェクト以外のプロジェクトを選択します。
2. [Stackdriverロギング(Stackdriver Logging)] > [ログルータ(Logs Router)] を選択します。
3. [シンクを作成(Create Sink)] をクリックします。
4. ログエントリの上にある [ラベルまたはテキスト検索によるフィルタ(Filter by label or text search)] ドロップダウンフィールドから、[高度なフィルタに変換(Convert to advanced filter)] を選択します。
5. 次をコピーし、プレーンテキストエディタに貼り付けます。

```
                    resource.type="gce_subnetwork"
logName="projects/MY_PROJECT_
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

6. `MY_PROJECT_NAME` を**プライマリ**プロジェクト ID に置き換えます。
7. 更新されたテキストをコピーし、[ラベルまたはテキスト検索によるフィルタ(Filter by label or text search)] フィールドに貼り付け、既存のテキストを上書きします。
8. [シンクの編集(Edit Sink)] ペインで、[シンク名(Sink Name)] フィールドに `vpc_flows-sink` と入力します。
9. [シンク名(Sink Name)] フィールドに `vpc_flows-sink` と入力します。

10. [シンクサービス（Sink Service）] ドロップダウンから [Pub/Sub] を選択します。
11. [シンクの宛先（Sink Destination）] ドロップダウンから [新しいクラウドPub/Subトピックの作成（Create new Cloud Pub/Sub topic）] を選択します。
12. [名前（Name）] フィールドに `vpc_flows-topic` と入力し、[作成（Create）] をクリックします。
13. [シンクを作成（Create Sink）] をクリックします。
14. 追加のプロジェクトごとにステップ 1 ～ 13 を繰り返します。

追加プロジェクト用の GCP Pub/Sub サブスクリプションの作成

1. GCP コンソールで、プライマリプロジェクト以外のプロジェクトを選択します。
2. [Pub/Sub] > [トピック（Topics）] を選択します。
3. `vpc_flows-topic` のコンテキストメニューから [サブスクリプションを作成（Create Subscription）] を選択します。
4. [サブスクリプション名（Subscription Name）] フィールドに `swc_subscription` と入力します。
5. [配信タイプ（Delivery Type）] で [プル（Pull）] を選択します。
6. [確認期限（Acknowledgment Deadline）] フィールドに `600` 秒と入力します。
7. [メッセージ保持期間（Message Retention Duration）] フィールドに `2` 時間と入力します。
8. [確認応答メッセージの保持（Retain Acknowledged Messages）] をオフにします。
9. [作成（Create）] をクリックします。

   追加のプロジェクトごとにステップ 1 ～ 9 を繰り返します。

関連リソース

Cisco 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。
- Cisco 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
- Cisco 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	2022 年 8 月 29 日	最初のバージョン

著作権情報