Cisco Secure Cloud Analytics

GovCloud 統合ガイド

目次

はじめに

Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）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 モニタリング） on GovCloud は、Amazon Web Services（AWS）GovCloud 向けの可視化、脅威の特定、およびコンプライアンスサービスです。Secure Cloud Analytics on GovCloud 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 テレメトリを消費します。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 on GovCloud 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 GovCloud 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 on GovCloud は、追加のコンテキストとモニタリングのために、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。

> E メール通知、ドメインネームシステム（DNS） 解決、フロントエンドの静的アセットなどの一部のサービスは、AWS パブリック クラウド インフラストラクチャを通じて提供されます。

次の点に注意してください。

- Secure Cloud Analytics は現在 FedRAMP 認定を取得していません。
- Secure Cloud Analytics on GovCloud 展開では、AWS GovCloud アカウント、オンプレミスネットワーク、GCP 展開、および Azure 展開を監視できます。Secure Cloud Analytics on GovCloud 展開では、AWS パブリック クラウド アカウントを監視できません。AWS パブリッククラウド展開を監視する場合は、Secure Cloud Analytics無料トライアル にサインアップしてください。
- Secure Cloud Analytics on GovCloud は Cisco Secure サインオンをサポートしていません。お客様は、ローカルアカウントを使用して Secure Cloud Analytics on GovCloud ポータルにアクセスします。

> これらの機能に関心がある場合は、シスコサポートにお問い合わせください。そのようなお問い合わせは、シスコが将来のリリースでこれらの機能を優先順位付けするうえで役立ちます。

Secure Cloud Analytics on GovCloud を使用するには：

- Secure Cloud Analytics on GovCloud AWS Marketplace トライアルページ [英語] に移動して、Secure Cloud Analytics on GovCloud の 60 日間無料トライアルにサインアップします。
- Secure Cloud Analytics on GovCloud と AWS GovCloud 展開を統合するには、Secure Cloud Analytics on GovCloud パブリック クラウド モニタリングの統合を参照してください。必要に応じて、Secure Cloud Analytics on GovCloud Cisco Secure Cloud Analytics プライベートネットワークのモニタリング（旧 Stealthwatch Cloud プライベート ネットワーク モニタリング）の展開を参照して、Cisco Secure Cloud Analytics センサー（旧 Stealthwatch Cloud センサー）を Secure Cloud Analytics on GovCloud ポータルに追加します。
- Secure Cloud Analytics on GovCloud ポータルの使用方法については、Secure Cloud Analytics on GovCloud ポータルに関する注意事項を参照してください。

無料トライアルのサインアップ

AWS Marketplace から Secure Cloud Analytics on GovCloud の 60 日間無料トライアルをリクエストできます。トライアルページには、Secure Cloud Analytics on GovCloud のさまざまな機能と課金情報の詳細が一覧されます。

Secure Cloud Analytics on GovCloud の統合

Secure Cloud Analytics on GovCloud の無料トライアルにサインアップしたら、Secure Cloud Analytics on GovCloud ポータルを AWS GovCloud 展開と統合できます。Secure Cloud Analytics for Amazon Web Services Quick Start Guide [英語] の手順に従いますが、次の点が異なります。

- Secure Cloud Analytics on GovCloud ポータル URL には **.gov** が含まれます (`https://`*`portal-name`*`.gov.obsrvbl.com`)。含まれていない場合は、シスコサポートにお問い合わせください。
- Secure Cloud Analytics on GovCloud ポータルは、AWS パブリッククラウド展開ではなく、AWS GovCloud 展開とのみ統合できます。
- S3 バケット、ロール、ポリシーを含むすべての AWS オブジェクトを AWS GovCloud 展開内に作成します。AWS パブリッククラウド展開内でこれらのオブジェクトのいずれかを作成すると、Secure Cloud Analytics on GovCloud 統合が失敗します。
- フローログデータを保存するように S3 バケットを設定する場合、**S3 バケットの ARN** は **aws-us-gov** パーティションに属し、AWS GovCloud 展開内にある必要があります。
- フローログデータへアクセスするための Secure Cloud Analytics 権限を許可する AWS ポリシーを設定する場合は、Secure Cloud Analytics on GovCloud ポータル UI でポリシードキュメントを参照してください。
- フローログデータにアクセスするための IAM ロールを設定する場合:
    - Secure Cloud Analytics on GovCloud 統合の**アカウント ID** は `523133480950` です。
    - 外部 ID の Secure Cloud Analytics on GovCloud Web ポータル名は、`https://`**`portal-name`**`.gov.obsrvbl.com` の形式でポータル URL に組み込まれています。たとえば、Web ポータル URL が `https://`**`example-client`**`.gov.obsrvbl.com` の場合は、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。

Secure Cloud Analytics on GovCloud 展開

Secure Cloud Analytics の GovCloud でホストされるインスタンスは、オンプレミスネットワークを監視できます。ローカル ネットワーク テレメトリを収集するには、オンプレミスセンサーを展開します。センサー Installation [英語] の手順に従いますが、次の点が異なっています。

- センサーと外部インターネット間のトラフィックを許可するファイアウォールルールを設定する場合、Secure Cloud Analytics on GovCloud ではリモートトラブルシューティング オプションがサポートされません。リモートトラブルシューティング アプライアンスの IP アドレス（54.83.42.41:22/TCP）からセンサーへのインバウンドトラフィックを許可しないでください。
- センサーを展開した後、Web ポータルを設定してセンサーを追加する前に、GovCloud 固有のホストで `config.local` 構成ファイルを更新してから、センサーを再起動する必要があります。詳細については、次の手順を参照してください。

Secure Cloud Analytics on GovCloud 固有のホストに接続するようにセンサーを設定する：

手順

1. SSH 経由で管理者としてセンサーにログインします。
2. コマンドプロンプトで「`sudo nano opt/obsrvbl-ona/config.local`」と入力して Enter キーを押し、構成ファイルを編集します。
3. 次の行をファイルの下部に追加します。

   ```
   OBSRVBL_HOST=https://sensor.us-gov.gov.obsrvbl.com
   ```

4. Ctrl+0 を押して変更を保存します。
5. Ctrl+X を押して終了します。
6. コマンドプロンプトで「`sudo service obsrvbl-ona restart`」を入力し、Enter を押して Secure Cloud Analytics サービスを再起動します。

次の作業

- Secure Cloud Analytics on GovCloud ポータル UI で構成を続行して、センサーを追加します。

Secure Cloud Analytics on GovCloud ポータルに関する注意事項

Secure Cloud Analytics on GovCloud ポータルは、次の点で Secure Cloud Analytics ポータルとは異なります。

- Secure Cloud Analytics on GovCloud は Cisco Secure サインオンをサポートしていません。ローカルユーザーアカウントは、Secure Cloud Analytics on GovCloud ポータルにアクセスするために使用されます。
- Secure Cloud Analytics on GovCloud ポータル URL には **.gov** が含まれます (`https://`*`portal-name`*`.gov.obsrvbl.com`)。
- Secure Cloud Analytics on GovCloud ポータルは、AWS パブリッククラウド展開ではなく、AWS GovCloud 展開と統合できます。
- Cisco Security Analytics and Logging の Secure Cloud Analytics on GovCloud との統合は**サポートされていません**。CSAL の詳細については、https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html [英語] を参照してください。
- Secure Cloud Analytics on GovCloud は AWS 関連のウェブフックをサポートしています。ただし、ウェブフックを介して送信されるデータには機密情報が含まれている可能性があるため、Secure Cloud Analytics on GovCloud でこれらのウェブフックを使用することは**推奨しません**。
- クロスアカウントロールの Secure Cloud Analytics アカウント番号は `523133480950` です。

さらに、次の点に注意してください。

- GCP、Azure、Kubernetes、Meraki、Umbrella の Secure Cloud Analytics on GovCloud との統合がサポートされています。ただし、組織のセキュリティポリシーをチェックして、これが組織のガイドラインとベストプラクティスに違反していないことを確認してください。
- Secure Cloud Analytics on GovCloud は、他のすべてのウェブフックをサポートします。ただし、ウェブフックを介して送信されるデータには機密情報が含まれている可能性があるため、Secure Cloud Analytics on GovCloud でこれらのウェブフックを使用することは**推奨しません**。

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	2020 年 4 月 13 日	初版
2.0	2021 年 11 月 3 日	製品のブランド名を更新。
2.1	2022 年 8 月 2 日	「サポートへの問い合わせ」セクションを追加。

著作権情報