Cisco Secure Cloud Analytics

ウェブフックとサービスの構成ガイド

目次

はじめに

概要

このガイドでは、Secure Cloud Analytics（以前の Stealthwatch Cloud）Web ポータルでウェブフックとサービスを構成する方法について説明します。サービスとウェブフックを使用すると、アラートが発行されたときに通知メッセージを送信できます。これは、サービスチケットの生成、スタッフへの通知、または自動修復の開始に使用できます。

構成オプション

構成されたすべてのサービスとウェブフックを表示するには、[設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] を選択します。

••• （[省略記号（Ellipsis）]）アイコン をクリックして、構成された各サービスまたはウェブフックの次のオプションにアクセスします。

- [配信ログ（Delivery Logs）]：送信時間、HTTP ステータスコード、メッセージを再送信するオプションなど、各サービスに送信されたメッセージに関する追加のコンテキストを提供します。
- [編集（Edit）]：サービスのメモや説明など、構成の詳細を更新します。
- [有効化/無効化（Enable/Disable）]：サービスへのメッセージの送信をオンまたはオフに切り替えます。
- [削除（Enable/Disable）]：サービスを Secure Cloud Analytics ポータルから削除します。

> SecureX Incident Manager サービスは、SecureX リボンがアクティブ化されたときに Secure Cloud Analytics によって自動的に作成されるため削除できません。

AWS S3 サービス

概要

このサービスは、Amazon S3 バケットにアラート通知メッセージを送信します。各メッセージは、一意の名前を持つ個別のファイルになります。このサービスを構成するには、AWS S3 バケットポリシーを編集して、Secure Cloud Analytics がオブジェクトをバケットに入れることを許可する必要があります。

AWS S3 バケットポリシーの編集

> この構成はパブリッククラウド用です。GovCloud を使用している場合は、アカウント ID が変更されます。詳細については、『 GovCloud Integration Guide』[英語] を参照してください。

1. AWS S3 コンソールにログインします。
2. [バケット(Buckets)] リストで、編集するバケットを選択します。
3. [アクセス許可(Permissions)] をクリックします。
4. [バケットポリシー(Bucket policy)] で、[編集(Edit)] をクリックします。
5. [ポリシー(Policy)] ボックスで、次を追加します。`<bucket>` は使用中のバケット名で置き換えます。

- 新しい権限を使用する場合：

```
{
 "Version": "2012-10-17",
 "Id": "ObsrvblWebhookPolicy",
 "Statement": [
 {
 "Sid": "ObsrvblWebhookStatement",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::757972810156:root"
 },
 "Action": "s3:PutObject",
 "Resource": "arn:aws:s3:::<bucket>/*"
 }
 ]
}
```

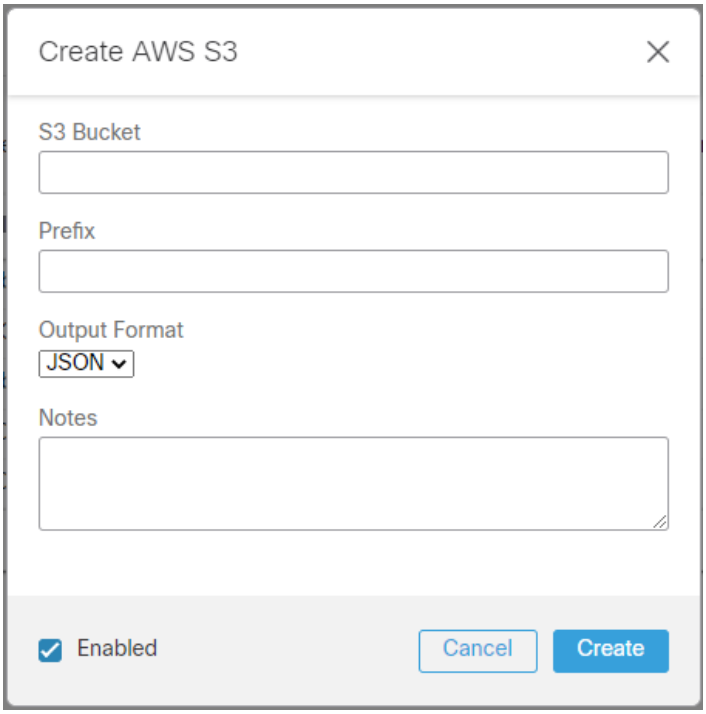
- 既存の権限を使用する場合：

```
{
 "Sid": "ObsrvblWebhookStatement",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::757972810156:root"
 },
 "Action": "s3:PutObject",
 "Resource": "arn:aws:s3:::<bucket>/*"
 }
```

6. ［変更を保存（Save changes）］をクリックします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [AWS S3] を選択します。[AWS S3 の作成(Create AWS S3)] ダイアログボックスが開きます。



4. [S3 バケット(S3 Bucket)] に名前を入力します。
5. 通知の配信先を制限する [プレフィックス(Prefix)] を入力します。
6. ドロップダウンリストで [出力フォーマット(Output Format)] を選択します。
7. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)] を入力します。
8. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
9. [作成(Create)] をクリックします。

AWS SNS サービス

概要

このサービスは、アラート通知メッセージを既存の Amazon Simple Notification Service（SNS）トピックに送信します。このサービスを構成するには、Secure Cloud Analytics によるトピックへの公開を許可するように SNS トピックのアクセスポリシーを編集する必要があります。

AWS SNS アクセスポリシーの編集

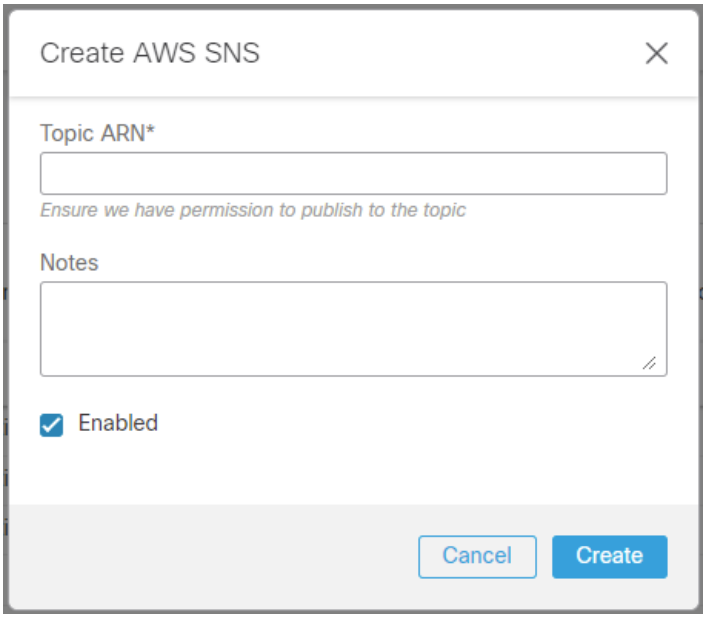
1. AWS SNS コンソールにログインします。
2. [トピック（Topics）] を選択し、編集するトピックを選択します。
3. [アクセスポリシー（Access policy）] タブを選択し、[編集（Edit）] をクリックします。
4. 以下を既存のポリシーに追加します。`<Topic ARN>` は、使用中のトピックの Amazon リソースネーム（ARN）で置き換えます。

```
{"Sid": "swc_publish",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::757972810156:role/site_role"
 },
 "Action": "sns:Publish",
 "Resource": "<Topic ARN>"
}
```

5. [レビュー（Review）] ページで、[変更を保存（Save changes）] をクリックします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [AWS SNS] を選択します。[AWS SNS の作成(Create AWS SNS)] ダイアログボックスが開きます。



4. 上記で使用した [トピック ARN(Topic ARN)] を入力します。
5. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
6. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
7. [作成(Create)] をクリックします。

AWS SQS サービス

概要

このサービスは、Amazon Simple Queue Service（SQS）にアラート通知メッセージを送信します。メッセージ本文は API JSON フォーマットに一致します。このサービスを構成するには、SQS 権限を編集して、Secure Cloud Analytics によるメッセージのキューへの送信を許可する必要があります。

AWS SQS 権限の編集

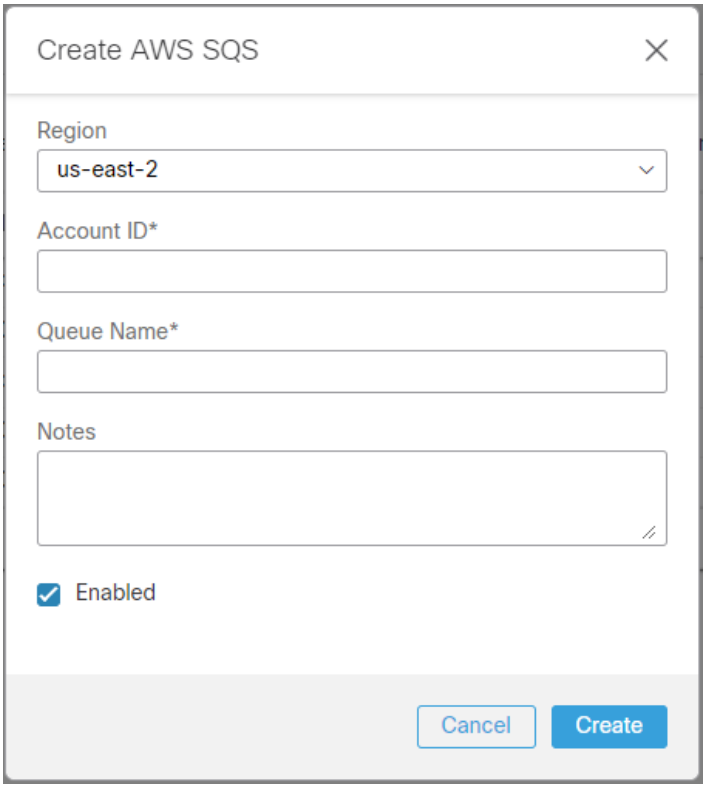
1. AWS SQS コンソールにログインします。
2. [キュー（Queues）] を選択します。
3. キューを選択し、[編集（Edit）] をクリックします。
4. [アクセスポリシー（Access policy）] セクションまでスクロールします。
5. 以下を既存のポリシーに追加します。`<SQS ARN>` は使用中の SQS の Amazon リソースネーム（ARN）で置き換えます。

```
{
 "Sid": "SCA_Publish",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::757972810156:root"
 },
 "Action": [
 "sqs:SendMessage",
 "sqs:GetQueueURL"
 ],
 "Resource": "<SQS ARN>"
 }
```

6. [保存（Save）] をクリックします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [AWS SQS] を選択します。[AWS SQS の作成(Create AWS SQS)] ダイアログボックスが開きます。



4. ドロップダウンリストから、AWS 展開の [リージョン(Region)] を選択します。
5. [アカウント ID(Account ID)] を入力します。
6. [キュー名(Queue Name)] を入力します。
7. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
8. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
9. [作成(Create)] をクリックします。

Azure Log Analytics

概要

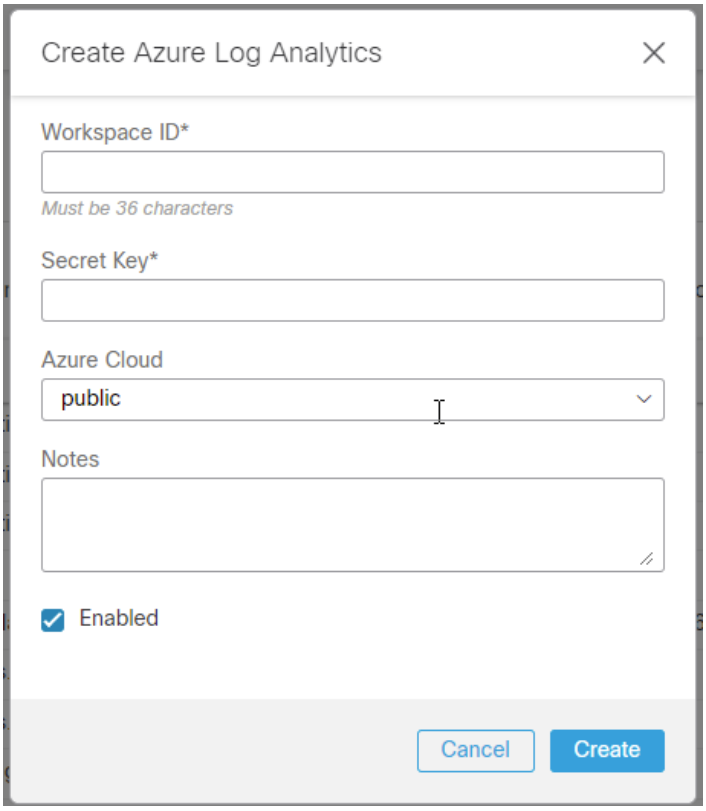
このサービスは、アラート通知メッセージを Azure Log Analytics ワークスペースに送信します。このサービスを構成するには、ワークスペース ID とキーが必要です。

Azure ワークスペースのログイン情報

1. Azure ポータルにサインインします。
2. 検索バーに「Log Analytics」と入力します。
3. [Log Analytics ワークスペース（Log Analytics workspaces）] を選択します。
4. [Log Analytics ワークスペース（Log Analytics workspaces）] のリストで、通知を送信するワークスペースを選択します。
5. [エージェント管理（Agents management）] を選択します。
6. [ワークスペース ID（Workspace ID）] と [プライマリキー（Primary key）] または [セカンダリキー（Secondary key）] をコピーします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [Azure Log Analytics] を選択します。[Azure Log Analytics の作成(Create Azure Log Analytics)] ダイアログ ボックスが開きます。



4. コピーした [ワークスペース ID(Workspace ID)] を入力します。
5. コピーした [秘密鍵(Secret Key)] を入力します。
6. ドロップダウンリストから [Azure Cloud] 展開タイプを選択します。
7. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
8. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
9. [作成(Create)] をクリックします。

DataDog

概要

このウェブフックは、アラート通知メッセージを DataDog に送信します。このサービスを構成するには、DataDog API キーを作成する必要があります。

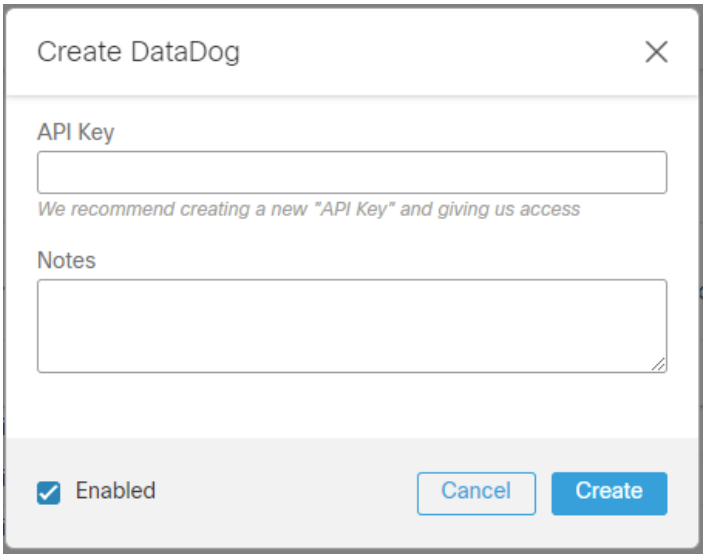
> 既存の API キーを使用する代わりに、新しい API キーを作成することを推奨します。

API キーの作成

1. DataDog コンソールにログインします。
2. [アカウント名（Account Name）] > [組織設定（Organization settings）] を選択します。
3. [API キー（API Key）] をクリックします。
4. [新しいAPI キー（New API key）] をクリックします。
5. キーの名前を入力します。
6. [API キーの作成（Create API key）] をクリックします。
7. キーはデフォルトでは非公開となります。紫色のボックスにカーソルを合わせて、[API キー（API key）] を表示しコピーします。

Secure Cloud Analytics へのウェブフックの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] を選択します。
3. [新しいウェブフック/サービスの追加（Add New Webhooks/Service）] > [DataDog] を選択します。[DataDog の作成（Create DataDog）] ダイアログボックスが開きます。



4. コピーした [API キー（API Key）] を入力します。
5. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ（Notes）]を入力します。

6. [有効（Enabled）] チェックボックスをオンにして、サービスを有効にします。
7. [作成（Create）] をクリックします。

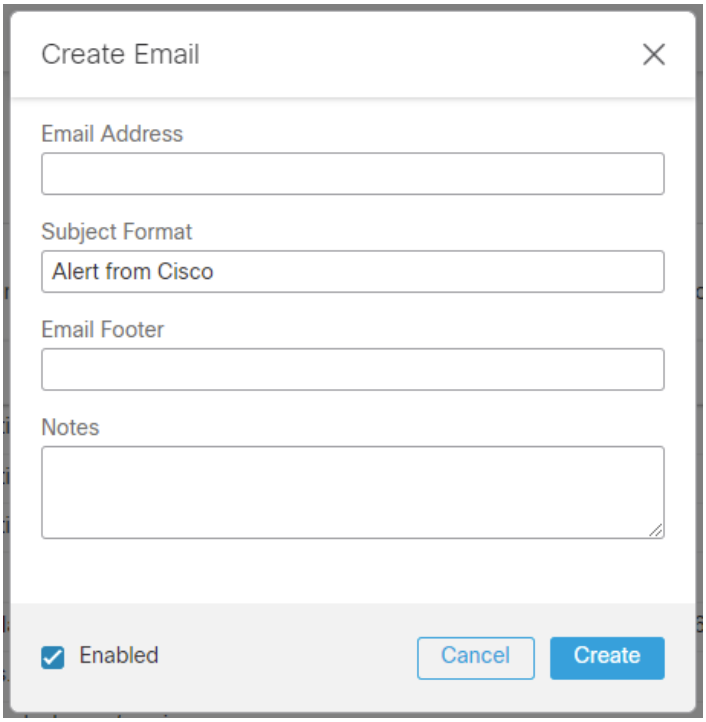
電子メール

概要

このサービスは、アラート通知を電子メールアドレスに送信します。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] を選択します。
3. [新しいウェブフック/サービスの追加（Add New Webhooks/Service）] > [電子メール（Email）] を選択します。[電子メールの作成（Create Email）] ダイアログボックスが開きます。



4. 受信者の [電子メールアドレス（Email Address）]を入力します。

5. [件名のフォーマット(Subject Format)]と[電子メールのフッター(Email Footer)]を更新します。次の表で説明されているように、そのアラートに固有の情報の電子メールにパラメータを追加できます。

パラメータ	定義
`${type}`	アラートタイプ
`${source_name}`	アラートを生成したエンティティの名前。
`${time}`	アラート生成の時刻
`${tags}`	アラートに関連付けられたタグ

6. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
7. [有効(Enabled)]チェックボックスをオンにして、サービスを有効にします。
8. [作成(Create)]をクリックします。

GCP PubSub

概要

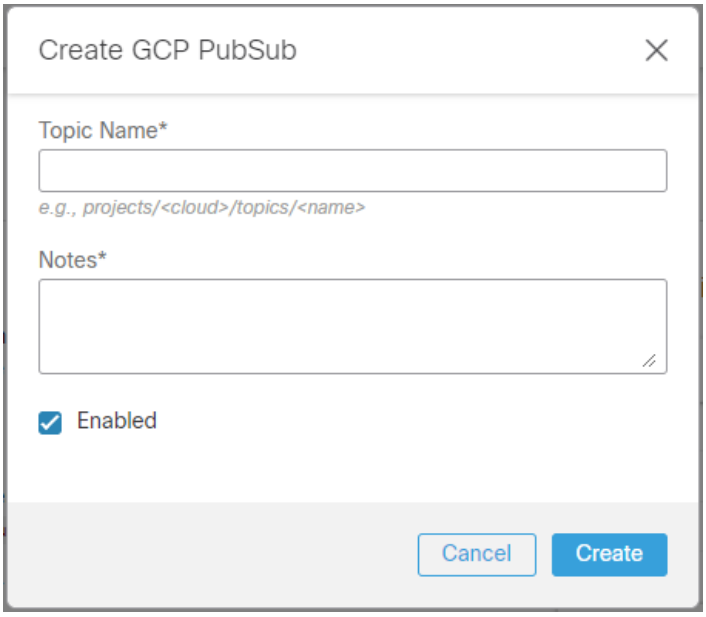
このサービスは、アラート通知メッセージを Google Cloud PubSub トピックに送信します。メッセージは API JSON フォーマットに一致します。このサービスを構成するには、トピックにメッセージを公開する権限を Secure Cloud Analytics に付与する必要があります。

GCP の権限

1. Google Cloud コンソールにログインします。
2. [Pub/Sub] > [トピック(Topics)] を選択します。
3. 編集するトピックを選択します。
4. [権限(Permissions)] タブで、[プリンシパルの追加(Add Principal)] をクリックします。
5. [アクセス権の付与(Grant access)] フォームに次の情報を入力します。
    - [プリンシパルの追加(Add principals)]: `service@swatch-cloud.iam.gserviceaccount.com`
    - [ロールの割り当て(Assign roles)]: `Pub/Sub Publisher`
6. [保存(Save)] をクリックします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] を選択します。
3. [新しいウェブフック/サービスの追加（Add New Webhooks/Service）] > [GCP PubSub] を選択します。[GCP PubSub の作成（Create GCP PubSub）] ダイアログボックスが開きます。



4. [トピック名（Topic Name）] を入力します。
5. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ（Notes）]を入力します。
6. [有効（Enabled）] チェックボックスをオンにして、サービスを有効にします。
7. [作成（Create）] をクリックします。

GCP ストレージ

概要

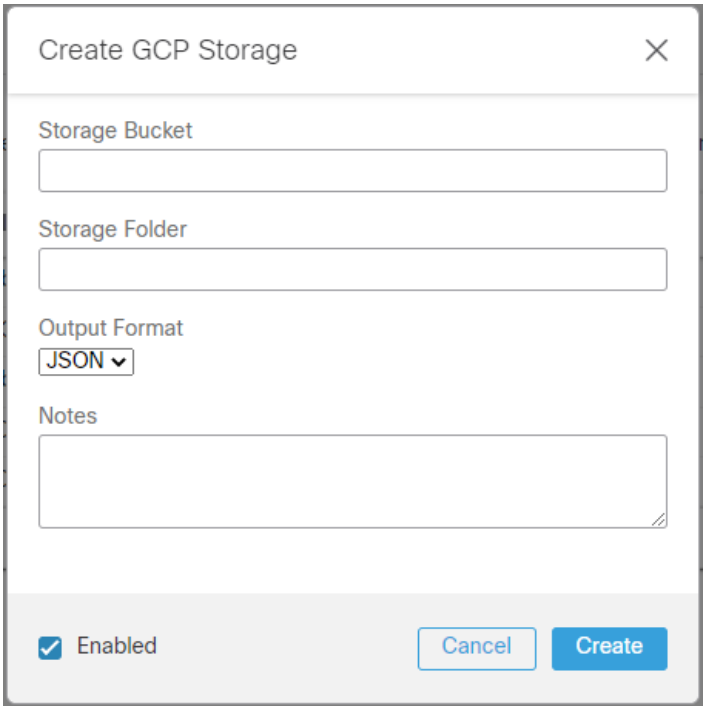
このサービスは、アラート通知メッセージを Google Cloud Storage バケットに送信します。各メッセージは、一意の名前を持つ個別のファイルになります。サービスを構成するには、バケットにストレージ オブジェクトを作成する権限を Secure Cloud Analytics に付与する必要があります。

GCP の権限

1. Google Cloud コンソールにログインします。
2. [クラウドストレージ(Cloud Storage)] > [バケット(Buckets)] を選択します。
3. 編集するバケットを選択します。
4. [権限(Permissions)] をクリックし、[プリンシパルの追加(Add Principal)] をクリックします。
5. [アクセス権の付与(Grant access)] フォームに次の情報を入力します。
    - [プリンシパルの追加(Add principals)]: `service@swatch-cloud.iam.gserviceaccount.com`
    - [ロールの割り当て(Assign roles)]: `Storage Object Creator`
6. [保存(Save)] をクリックします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [GCP ストレージ(GCP Storage)] を選択します。[GCP ストレージの作成(Create GCP Storage)] ダイアログボックスが開きます。



4. [ストレージバケット(Storage Bucket)] 名を入力します。
5. バケットにファイルが作成される [ストレージフォルダ(Storage Folder)] を入力します。
6. ドロップダウンリストで [出力フォーマット(Output Format)] を選択します。
7. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
8. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
9. [作成(Create)] をクリックします。

PagerDuty

概要

このサービスは、アラート通知メッセージを PagerDuty に送信します。このサービスを構成するには、Secure Cloud Analytics とやり取りする新しい API サービスを追加する必要があります。

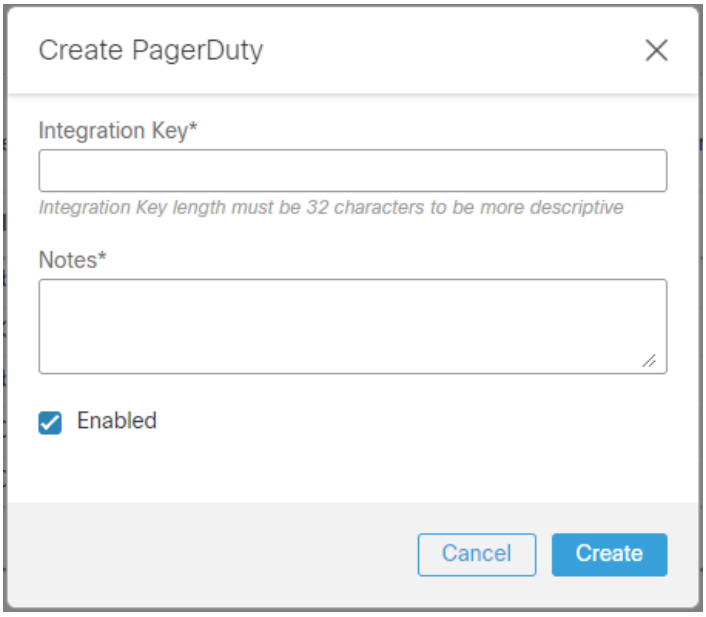
> トリガーイベントをサポートします。

統合キーの作成

1. PagerDuty にログインします。
2. [構成（Configuration）] > [サービス（Services）] を選択します。
3. [新しいサービスの追加（+Add New Service）] をクリックします。
4. サービスの [名前（Name）]と [説明（Description）] を入力します。
5. [統合設定（Integration Settings）] で、[API を直接使用する（Use our API directly）] を選択します。
6. [サービスの作成（Create Service）] をクリックします。
7. サービスの [統合（Integrations）] ページにリダイレクトされます。[統合キー（Integration Key）] をコピーします。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [PagerDuty] を選択します。[PagerDuty の作成(Create PagerDuty)] ダイアログボックスが開きます。



4. コピーした [統合キー(Integration Key)] を入力します。
5. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
6. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
7. [作成(Create)] をクリックします。

Slack

概要

このウェブフックは、アラート通知メッセージを Slack に送信します。このウェブフックを構成するには、Slack アプリとウェブフック URL を作成する必要があります。

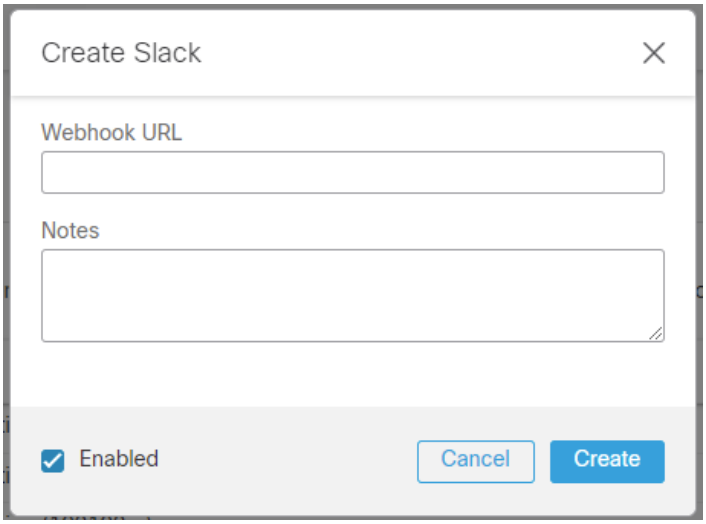
Slack の構成

1. https://api.slack.com/apps?new_app に移動します。
2. [アプリの作成(Create an App)] をクリックします。
3. 名前を入力し、メッセージを送信するワークスペースを選択します。
4. [アプリの作成(Create App)] をクリックします。
5. 作成後、新しいアプリの設定ページにリダイレクトされます。

   既存のアプリを使用している場合は、アプリの管理ダッシュボードを使用して設定をロードします。
6. [着信ウェブフック(Incoming Webhooks)] 機能を選択し、[着信ウェブフックのアクティブ化(Activate Incoming Webhooks)] トグルをクリックしてオンにします。設定ページが更新されます。
7. [新しいウェブフックをワークスペースに追加(Add New Webhook to Workspace)] をクリックします。
8. アプリの投稿先となるチャネルを選択し、[承認(Authorize)] をクリックします。
9. アプリの設定ページで、[ワークスペースのウェブフック URL(Webhook URLs for Your Workspace)] セクションの下に新しいエントリが表示されます。ウェブフック URL は次のようになります:`https://hooks.slack.com/services/NNNNNNN/`。
10. [ウェブフック URL(Webhook URL)] をコピーします。

Secure Cloud Analytics へのサービスの追加

1. Web ポータルにログインします。
2. [設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] を選択します。
3. [新しいウェブフック/サービスの追加（Add New Webhooks/Service）] > [Slack] を選択します。[Slack の作成（Create Slack）] ダイアログボックスが開きます。



4. コピーした [ウェブフック URL（Webhook URL）] を入力します。
5. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ（Notes）]を入力します。
6. [有効（Enabled）] チェックボックスをオンにして、サービスを有効にします。
7. [作成（Create）] をクリックします。

Splunk HEC

概要

このサービスは、モニタリングのためにアラート通知メッセージを Splunk HTTP イベントコレクタ（HEC）に送信します。このサービスを構成するには、Splunk HEC を作成し、HEC トークンを生成してから、HEC URI をアップロードする必要があります。

> Secure Cloud Analytics が通知を送信できるように、HEC に外部からアクセス可能であることを確認します。

Splunk の構成

HEC の有効化

> Splunk Cloud Platform に登録している場合、HEC はデフォルトで有効になっています。

イベントコレクタが HTTP 経由でイベントを受信できるようにするには、次の手順を実行します。

1. Splunk Enterprise コンソールにログインします。
2. [設定（Settings）] > [データ入力（Data Inputs）] を選択します。
3. [HTTP イベントコレクタ（HTTP Event Collector）] をクリックします。
4. [グローバル設定（Global Settings）] をクリックします。
5. [すべてのトークン（All Tokens）] トグルボタンで、[有効（Enabled）] を選択します。
6. （オプション）すべての HEC トークンで [デフォルトのソースタイプ（Default Source Type）] を選択します。ソースタイプを選択する前に、ドロップダウン リスト ボックスの上にあるテキスト フィールドにソースタイプの名前を入力することもできます。
7. （オプション）すべての HEC トークンで [デフォルトインデックス（Default Index）] を選択します。
8. （オプション）すべての HEC トークンで [デフォルト出力グループ（Default Output Group）] を選択します。
9. （オプション）展開サーバーを使用して HEC トークンの構成を処理するには、[展開サーバーを使用（Default Output Group）] チェックボックスをオンにします。
10. （オプション）HEC が HTTP ではなく HTTPS をリッスンして通信するようにするには、[SSL の有効化（Enable SSL）] チェックボックスをオンにします。
11. （オプション）HEC がリッスンする [HTTP ポート番号（HTTP Port Number）] フィールドに番号を入力します。

    > クライアントまたは HEC をホストする Splunk インスタンスのいずれかで、[HTTP ポート番号（HTTP Port Number）] フィールドで指定したポート番号をファイアウォールがブロックしていないことを確認します。

12. [保存（Save）] をクリックします。

HEC トークンの作成

HEC トークンを作成するには、次の手順を実行します。

1. Splunk Enterprise コンソールにログインします。
2. [設定(Settings)] > [データの追加(Settings)] を選択します。
3. [モニター(monitor)] をクリックします。
4. [HTTP イベントコレクタ(HTTP Event Collector)] をクリックします。
5. [名前(Name)] フィールドに、トークンの名前を入力します。
6. (オプション)[ソース名オーバーライド(Source name override)] フィールドに、この入力が生成するイベントのソース名を入力します。
7. (オプション)[説明(Description)] フィールドに、入力の説明を入力します。
8. (オプション) [出力グループ(Source name override)] フィールドで、既存のフォワーダ出力グループを選択します。
9. (オプション)このトークンのインデクサ確認応答を有効にする場合は、[インデクサ確認応答の有効化(Enable indexer acknowledgment)] チェックボックスをオンにします。
10. [次へ(Next)] をクリックします。
11. (オプション)HEC イベントのソースタイプとインデックスを確認します。
12. [レビュー(Review)] をクリックします。
13. エンドポイントのすべての設定が期待どおりであることを確認します。
14. すべての設定が期待通りの場合は、[送信(Submit)] をクリックします。それ以外の場合は、[<] をクリックして変更を加えます。
15. Splunk Web が表示するトークン値をコピーして、後で参照できるようにテキストエディタに貼り付けます。

HEC URI の決定

HEC 展開と Splunk サブスクリプションに基づいて、HEC の URI を決定します。

Splunk Enterprise

Splunk Enterprise に登録している場合:

1. 次の URI をコピーし、プレーンテキストエディタに貼り付けます。

   `<protocol>://<host>:<port>/services/collector`

2. HEC の作成時に SSL を有効にしたか無効にしたかに応じて、`<protocol>` を `http` または `https` で置き換えます。
3. プレーンテキストエディタで、`<host>` をホスト名で置き換えます。
4. プレーンテキストエディタで、`<port>` をポート番号で置き換えます。

Splunk Cloud（セルフサービス）

セルフサービスの Splunk Cloud に登録している場合：

1. 次の URI をコピーし、プレーンテキストエディタに貼り付けます。

   `https://input-<host>:8088/services/collector`

2. プレーンテキストエディタで、*<host>* をホスト名で置き換えます。

Splunk Cloud（マネージド）

マネージド Splunk Cloud に登録している場合：

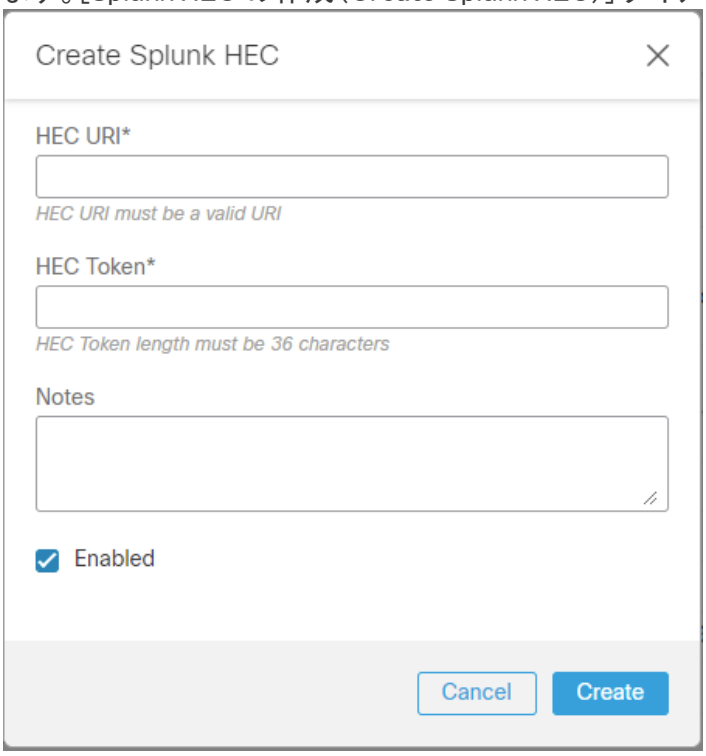
1. 次の URI をコピーし、プレーンテキストエディタに貼り付けます。

   `<protocol>://http-inputs-<host>:443/services/collector`

2. HEC の作成時に SSL を有効にしたか無効にしたかに応じて、*<protocol>* を `http` または `https` で置き換えます。
3. プレーンテキストエディタで、*<host>* をホスト名で置き換えます。

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] を選択します。
3. [新しいウェブフック/サービスの追加（Add New Webhooks/Service）] > [Splunk HEC] を選択します。[Splunk HEC の作成（Create Splunk HEC）] ダイアログボックスが開きます。



4. [HEC URI] を入力します。

5. コピーした [HEC トークン（HEC Token）] を入力します。
6. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ（Notes）]を入力します。
7. [有効（Enabled）] チェックボックスをオンにして、サービスを有効にします。
8. [作成（Create）] をクリックします。

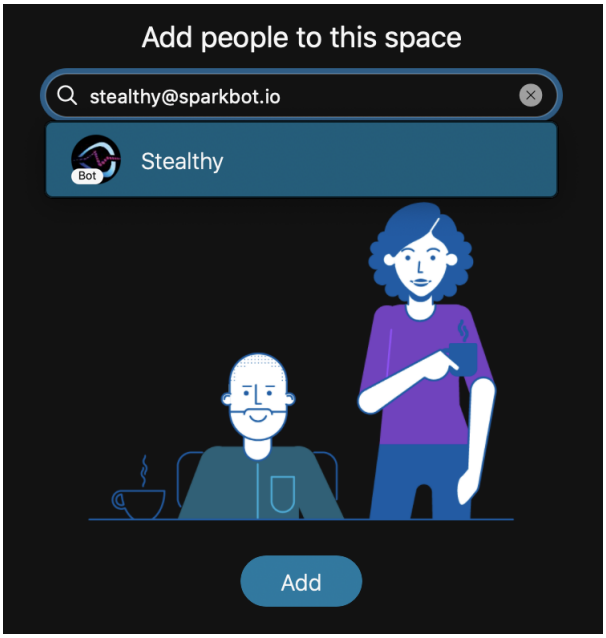
Webex アプリ

概要

このサービスは、アラート通知メッセージを Webex アプリスペースに送信します。このサービスを構成するには、スペース ID が必要で、さらに、Secure Cloud Analytics ボットをスペースに追加する必要があります。

Webex スペースの構成

1. Webex アプリで通知を送信するスペースを選択し、`stealthy@sparkbot.io` をスペースに追加します。



2. スペース ID をコピーします。これは、次のいずれかの方法を使用して見つけることができます。
   - Webex アプリスペースで（歯車）アイコンをクリックし、[スペースリンクをコピー（Copy space link）] を選択します。リンクをテキストエディタに貼り付けます。次のようになります：webexteams://im?space= space_id。
   - Webex アプリスペースで、スペース情報をクリップボードにコピーします。
     - Windows では、`Ctrl + Shift + K` を使用します。
     - Mac では、`Option + Command + K` を使用します。

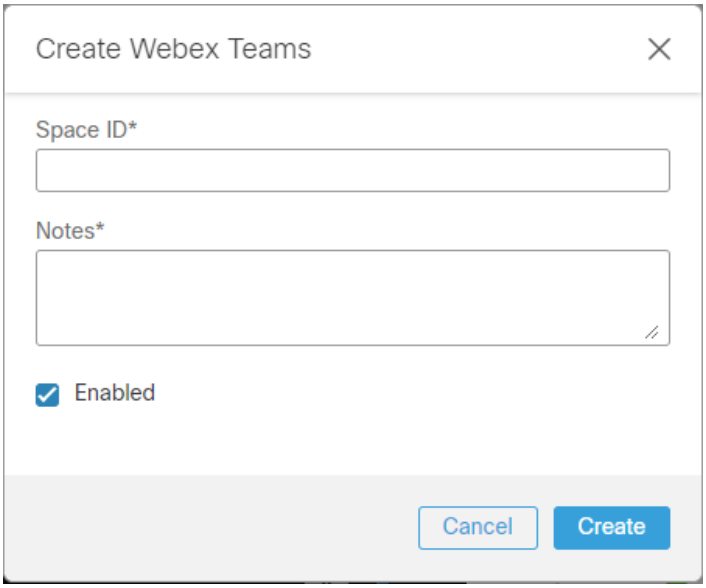
     スペース情報をテキストエディタに貼り付けると、次のようになります。

     ```
     Space name: My Space
     Space ID: 397538b0-7497-11ec-9fcb
     Space URI: webexteams://im?space=397538b0-7497-11ec-9fc
     ```

```
Space URI (markdown): [My Space]
(webexteams://im?space=397538b0-7497-11ec-9fc)
Participant count: 3
External participant count: 0
Conversation type: group
Actor role: Member
```

Secure Cloud Analytics へのサービスの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [Webex Teams] を選択します。[Webex Teams の作成(Create Webex Teams)] ダイアログボックスが開きます。



4. コピーした [スペース ID(Space ID)] を入力します。
5. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ(Notes)]を入力します。
6. [有効(Enabled)] チェックボックスをオンにして、サービスを有効にします。
7. [作成(Create)] をクリックします。

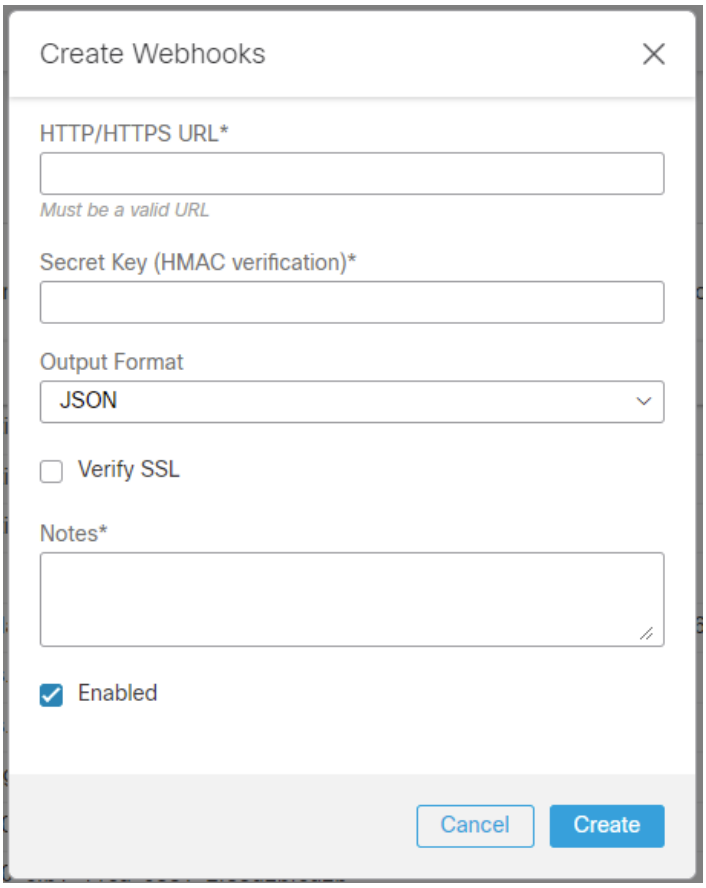
ウェブフック

概要

この汎用ウェブフックは、指定したウェブフック URL への `POST` リクエストとしてアラート通知を配信します。システムは、指定したウェブフック秘密鍵を使用して、`POST` リクエスト本文のハッシュベースのメッセージ認証コード(HMAC)ハッシュを生成します。`POST` リクエストのカスタム `X-OBSERVABLE-SIGNATURE` ヘッダーには、この HMAC ハッシュが含まれています。

Secure Cloud Analytics へのウェブフックの追加

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定(Settings)] > [ウェブフック/サービス(Webhooks/Services)] を選択します。
3. [新しいウェブフック/サービスの追加(Add New Webhooks/Service)] > [ウェブフック(Webhooks)] を選択します。[ウェブフックの作成(Create Webhooks)] ダイアログボックスが開きます。



4. [HTTP/HTTPS URL] フィールドにウェブフック URL を入力します。
5. [秘密鍵(HMAC 検証)(Secret Key (HMAC verification))] フィールドに秘密鍵を入力します。
6. ドロップダウンリストで [出力フォーマット(Output Format)] を選択します。
7. HTTPS ウェブフック URL を使用した場合は、[SSL の検証(Verify SSL)] を選択します。

8. アラート通知サービスのサマリーにテキストを表示する場合は、[メモ（Notes）]を入力します。
9. [有効（Enabled）] チェックボックスをオンにして、サービスを有効にします。
10. [作成（Create）] をクリックします。

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	2022 年 11 月 1 日	最初のバージョン

著作権情報