Cisco Secure Cloud Analytics

Microsoft Azure 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 Microsoft Azure 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、Microsoft Azure 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、Azure パブリック クラウド ネットワークからネットワーク セキュリティ グループ（NSG）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、動的エンティティモデリングを実行します。Secure Cloud Analytics は、Azure ストレージアカウントから直接 NSG フローログを消費し、アプリケーションを使用して追加のコンテキストを取得します。

Azure ユーザーロール

統合は、Azure Active Directory（AD）の**グローバル管理者**ロールとモニタリング対象のすべてのサブスクリプションに関する**所有者**ロールを持つユーザーとして設定することをお勧めします。それが不可能な場合は、Azure AD 管理者に問い合わせて、次のことを確認してください。

1. ユーザーがアプリケーション登録を作成できる：これはメンバーユーザーに対してデフォルトで許可されていますが、一部の Azure AD ではこれが無効になっている場合があります。これがゲストユーザーであるか、アプリケーション登録が無効になっている場合は、**アプリケーション開発者**ロールをユーザーに割り当てる必要があります。
2. モニタリング対象の各サブスクリプションについて、ユーザーが Azure リソース（認証、ネットワーク、ストレージアカウント、モニタリング）にアクセスできる：このためには、**ユーザーアクセス管理者**ロールと**コントリビュータ**ロールをユーザーに割り当てる必要があります。

詳細については、「**Secure Cloud Analytics 統合に必要な Azure 権限**」を参照してください。

bash スクリプトを使用したアクティブ化

シスコでは、設定手順を自動化する実験的な bash スクリプトを開発しました。

このスクリプトは Secure Cloud Analytics Web ポータルからダウンロードできます。
[設定（Settings）] > [（Integrations）] > [Azure] > [バージョン情報（About）] に移動します。

bash スクリプトを有効にするには、次の手順を実行します。

1. Azure ポータルにログインします。
2. 検索バーの横にあるコンソールアイコンをクリックして Azure Cloud Shell を起動します。[Bash] をクリックして bash コンソールを開きます。
3. [ファイルのアップロード/ダウンロード（Upload/Download files）] ボタンを使用してスクリプトをアップロードします。
4. bash azure_setup.sh でスクリプトを実行し、指示に従います。

- このスクリプトにより、スクリプトが検出できるすべてのサブスクリプションのモニタリングが有効になります。
- このスクリプトにより、指定された場所のすべてのネットワーク セキュリティ グループが、フローログを指定されたストレージアカウントに保存するようになります。

Azure の設定

フローログデータを生成して保存するように Azure を設定するには、次の手順を実行します。

- 少なくとも 1 つのリソースグループをモニターします。詳細については、「**Azure リソースグループの作成**」を参照してください。
- Azure AD の URL とサブスクリプション ID を取得します。詳細については、「**Azure Active Directory の URL とサブスクリプション ID の取得**」を参照してください。
- AD アプリケーションを作成し、そのアプリケーションへのアクセスを許可します。詳細については、「**Azure AD アプリケーションの作成**」と「**アプリケーションへのアクセスの許可**」を参照してください。
- フローログデータのストレージアカウントを作成し、SAS URL を生成します。詳細については、「**フローログデータを保存するための Azure ストレージアカウントの作成**」および「**Azure ストレージアカウントの共有アクセス署名 URL の生成**」を参照してください。
- Network Watcher を有効にして、Insights プロバイダーを登録し、フローログを有効にします。詳細については、「**Azure Network Watcher の有効化**」、「**Insights プロバイダーの登録**」、および「**Azure NSG フローログの有効化**」を参照してください。
- 実行されたアクティビティをさらに可視化する場合は、アクティビティログを保存するようにストレージアカウントを設定します。詳細については、「**Azure アクティビティ ログ ストレージの有効化**」を参照してください。

Azure リソースグループの作成

最初に、モニターする 1 つ以上のリソースグループがあることを確認します。既存のリソースグループを使用することも、新しいリソースグループを作成して、仮想マシンなどのリソースを追加することもできます。

1. Azure ポータルにログインします。
2. [リソースグループ（Resource Groups）] を選択します。
3. [追加（Add）] をクリックします。
4. [リソースグループ名（Resource group name）] を入力します。
5. [サブスクリプション（Subscription）] を選択します。
6. [リソースグループの場所（Resource group location）] を選択します。
7. [確認して作成（Review + create）] をクリックします。
8. [作成（Create）] をクリックします。

Azure Active Directory の URL とサブスクリプション ID の取得

Secure Cloud Analytics に Azure メタデータサービスへのアクセス権を提供するには、Azure Active Directory（AD）URL と Azure サブスクリプション ID を取得します。この情報を記録してください。このプロセスの最後に、この情報を Secure Cloud Analytics Web UI にアップロードして、Azure との統合を完了します。

1. Azure ポータルにログインします。
2. [Azure Active Directory] > [概要（Overview）] を選択します。
3. プライマリドメイン（例：example.onmicrosoft.com）をコピーして、プレーンテキストエディタに貼り付けます。これは Azure AD の URL です。

4. [サブスクリプション(Subscriptions)]を選択し、自分のサブスクリプションを選択します。
5. サブスクリプション ID をコピーし、プレーンテキストエディタに貼り付けます。

Azure AD アプリケーションの作成

Active Directory URL とサブスクリプション ID を取得したら、Secure Cloud Analytics がリソースグループからメタデータを読み取ることができるようにするアプリケーションを作成します。アプリケーションの作成が完了したら、アプリケーションキーをコピーします。

> Active Directory インスタンスごとに **1 つのアプリケーションのみ**を作成します。アプリケーションにロールを割り当てることで、Active Directory インスタンスの複数のサブスクリプションをモニターできます。詳細については、「**アプリケーションへのアクセスの許可**」を参照してください。

1. Azure ポータルにログインします。
2. [Azure Active Directory]、[アプリケーションの登録(App Registrations)]、[新規登録(New Registration)]の順に選択します。
3. [名前(Name)]フィールドに「`swc-reader`」と入力します。その他はデフォルトのままにします。
4. アプリケーション(クライアント)ID 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. [証明書と秘密(Certificates and Secrets)]>[新しいクライアント秘密(New Client Secret)]を選択します。
6. [説明(Description)]フィールドに「`SWC Reader`」と入力します。
7. [有効期日(Expires)]ドロップダウンで、適切な有効期日を選択するか、デフォルト値を受け入れます。
8. [追加(Add)]をクリックします。
9. アプリケーションキーの値をコピーし、プレーンテキストエディタに貼り付けます。

> このページから移動するとキーが表示されなくなるため、ここでアプリケーションキーをコピーします。

アプリケーションへのアクセスの許可

`swc-reader` アプリケーションを AD に登録した後、そのアプリケーションにモニタリングリーダーロールを割り当てます。これにより、リソースグループからメタデータを読み取れるようになります。モニターするサブスクリプションごとに次の手順を実行します。

1. Azure ポータルにログインします。
2. [サブスクリプション(Subscriptions)]を選択し、自分のサブスクリプションを選択します。
3. [アクセス制御(IAM)(Access control (IAM))]を選択します。
4. [追加(Add)]>[ロール割り当ての追加(Add role Assignment)]を選択します。
5. [ロール(Role)]ドロップダウンで[モニタリングリーダー(Monitoring Reader)]を選択します。
6. [アクセス権の割り当て先(Assign access to)]ドロップダウンで[ユーザー、グループ、またはサービスプリンシパル(User, group, or service principal)]を選択します。

7. [名前または電子メールアドレスで検索（Search by name or email address）] フィールドに「**swc-reader**」と入力します。
8. [保存（Save）] をクリックします。

フローログデータを保存するための Azure ストレージアカウントの作成

モニタリングリーダーロールを `swc-reader` アプリケーションに割り当てたら、フローログデータを保存するストレージアカウントを作成します。リソースグループと同じ場所にバイナリラージオブジェクト（BLOB）ストレージアカウントを作成します。

> リソースグループと同じ場所にあり、そこに BLOB を保存できる場合は、既存のストレージアカウントを再利用できます。

BLOB ストレージアカウントを作成したら、ファイアウォールルールでインターネットからストレージアカウントへのアクセスが許可されていることを確認します。これにより、Secure Cloud Analytics と Azure の展開を適切に統合できます。

BLOB ストレージアカウントの作成

1. Azure ポータルにログインします。
2. [ストレージアカウント（Storage Accounts）] を選択します。
3. [追加（Add）] をクリックします。
4. [サブスクリプション（Subscription）] を選択します。
5. モニターする [リソースグループ（Resource group）] を選択します。
6. [ストレージアカウント名（Storage account name）] を入力します。
7. 指定したリソースグループと同じストレージアカウントの [場所（Location）] を選択します。
8. [アカウントの種類（Account kind）] として [ストレージv2（汎用）（Storage v2 (general purpose)）] を選択します。
9. 組織の要件に基づいて、ドロップダウンから [レプリケーション（Replication）] オプションを選択します。
10. ストレージアカウント内で BLOB にアクセスする頻度に応じて、[ホット（Hot）] または [クール（Cool）] アクセス階層を選択します。
11. [確認して作成（Review + create）] をクリックします。
12. [作成（Create）] をクリックします。

BLOB ストレージアカウントへのインターネットアクセスの有効化

1. BLOB ストレージアカウントから、[ファイアウォールと仮想ネットワーク（Firewalls and virtual network）] 設定を選択します。
2. [すべてのネットワークからのアクセスを許可（Allow access from All Networks）] を選択し、変更を保存します。

Azure ストレージアカウントの共有アクセス署名 URL の生成

ストレージアカウントを作成した後、ストレージアカウントからフローログデータを取得する権限を Secure Cloud Analytics に許可するために、ストレージアカウントの共有アクセス署名（SAS）を生成します。次に、BLOB サービス SAS URL をコピーします。Secure Cloud Analytics は、BLOB サービスSAS URL を使用して、ストレージアカウントからフローログデータを取得します。

> SAS 権限には、設定に基づく時間制限があります。SAS 権限が期限切れの場合、Secure Cloud Analytics はストレージアカウントからフローログデータを取得できません。

1. Azure ポータルにログインします。
2. [その他のサービス（More Services）] > [ストレージ（Storage）] > [ストレージアカウント（Storage Accounts）] を選択します。
3. フローログデータを保存するように設定されたストレージアカウントを選択します。
4. [共有アクセス署名（Shared access signature）] を選択します。
5. [許可されるサービス（Allowed services）] フィールドで [BLOB（Blob）] を選択します。
6. [許可されるリソースタイプ（Allowed resource types）] フィールドで [サービス（Service）]、[コンテナ（Container）]、および [オブジェクト（Object）] を選択します。
7. [許可される権限（Allowed permissions）] で [読み取り（Read）] および [リスト（List）] を選択します。
8. 現在の時刻に対応する [開始時刻（Start time）] を入力します。
9. 現在の時刻から少なくとも 1 年に対応する [終了時刻（End time）] を入力します。
10. [許可されるプロトコル（Allowed protocols）] フィールドで [HTTPSのみ（HTTPS only）] を選択します。
11. [SASおよび接続文字列を生成（Generate SAS and connection string）] をクリックします。
12. BLOB サービス SAS URL をコピーし、プレーンテキストエディタに貼り付けます。

> IP に基づいてこのストレージアカウン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）] > [Azure] > [バージョン情報（About）] の順に選択すると、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。

Azure Network Watcher の有効化

BLOB ストレージ SAS URL を生成した後、リソースグループを含むリージョンで Network Watcher を有効にします（まだ有効にしていない場合）。Azure では、ネットワーク セキュリティ グループのフローログを有効にするために、Network Watcher が必要です。

1. Azure ポータルにログインします。
2. [Network Watcher] > [概要（Overview）] を選択します。
3. リージョンリストを選択して展開します。
4. リソースグループを含むリージョンのメニューを選択し、[Network Watcherの有効化（Enable Network Watcher）] を選択します。

Insights プロバイダーの登録

NSG フローログをアクティブ化する前に、`microsoft.insights` プロバイダーを有効にします。

1. Azure ポータルにログインします。
2. [サブスクリプション(Subscriptions)] に移動し、サブスクリプション名を選択します。
3. [設定(Settings)] > [リソースプロバイダー(Resource Providers)] の順にクリックします。
4. `microsoft.insights` プロバイダーを強調表示し、[登録(Register)] をクリックします。

Azure NSG フローログの有効化

Network Watcher を有効にした後、1 つ以上のネットワーク セキュリティ グループのネットワーク セキュリティ グループ(NSG)フローログを有効にします。これらのネットワーク セキュリティ グループは、モニターするリソースグループに対応している必要があります。

> BLOB ストレージアカウントは、NSG フローログの保持期間をサポートしていません。

1. Azure ポータルにログインします。
2. [Network Watcher] > [NSGフローログ(NSG flow logs)] の順に選択します。
3. ネットワーク セキュリティ グループを選択してフローログ設定ページを表示します。
4. [フローログのバージョン(Flow Logs version)] フィールドで [バージョン 2(Version 2)] を選択します。
5. 「**Azure ストレージアカウントの共有アクセス署名 URL の生成**」で SAS を設定した BLOB ストレージアカウントを選択します。
6. [トラフィック分析(Traffic Analytics)] ステータスとして [オフ(Off)] を選択します。

   > Secure Cloud Analytics では、トラフィック分析を有効にする必要はありませんが、この機能が必要な場合は有効にすることができます。

7. [保持日数(Retention (days))] フィールドにログの保持期間を入力します。
8. [保存(Save)] をクリックします。
9. フローロギングを有効にするネットワーク セキュリティ グループごとに、ステップ 2 ～ 8 を繰り返します。

Secure Cloud Analytics の Azure との設定

Secure Cloud Analytics Web ポータル UI に次の情報を入力して Azure との統合を完了します。

- Azure AD の URL
- サブスクリプション ID
- アプリケーション ID
- アプリケーションキー
- BLOB サービス SAS URL

Azure からフローログデータを取得するための 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)] > [Azure] > [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. Azure AD の URL を入力します。
5. Azure アプリケーション ID を入力します。
6. Azure アプリケーションキーを入力します。
7. ドロップダウンリストから [Azure Cloud] 環境を選択します。
8. [作成(Create)] をクリックします。
9. [ストレージアクセス(Storage Access)] をクリックします。
10. [新規統合(New Integration)] をクリックします。
11. [APIキー(API Key)] フィールドに **BLOB サービス SAS URL** を入力します。
12. [作成(Create)] をクリックします。
13. [サブスクリプション(Subscriptions)] を選択し、サブスクリプションがリストされていることを確認します。

Secure Cloud Analytics 統合に必要な Azure 権限

次の表に、Secure Cloud Analytics との統合のために Azure を設定するのに必要なロールメンバーシップの詳細を示します。

アクション	メンバーユーザー（ネイティブテナントメンバー）に必要な権限	ゲストユーザー（コラボレーションゲスト）に必要な権限
Azure リソースグループの作成	ストレージアカウントのコントリビュータロールにメンバーユーザーを追加する	ストレージアカウントのコントリビュータロールにゲストユーザーを追加する
Azure Active Directory の URL とサブスクリプション ID の取得	メンバーユーザーのデフォルト権限	AD URL を取得するためのゲストユーザーのデフォルト権限、サブスクリプション ID を取得するための Cognitive Services ユーザーロールへのゲストユーザーの追加
Azure AD アプリケーションの作成	AD アプリケーション登録を作成するためのメンバーユーザーのデフォルト権限、ユーザーがアプリケーション登録を作成した場合にクライアントシークレットを生成するためのメンバーユーザーのデフォルト権限	アプリケーション開発者ロールにゲストユーザーを追加する
アプリケーションへのアクセスの許可	ユーザーがアプリケーション登録を作成した場合は、メンバーユーザーのデフォルト権限	アプリケーション開発者ロールにゲストユーザーを追加する
フローログデータを保存するための Azure ストレージアカウントの作成	ストレージアカウントのコントリビュータロールにメンバーユーザーを追加する	ストレージアカウントのコントリビュータロールにゲストユーザーを追加する
Azure ストレージアカウントの共有アクセス署名 URL の生成	ストレージアカウントのコントリビュータロールにメンバーユーザーを追加する	ストレージアカウントのコントリビュータロールにゲストユーザーを追加する
Azure Network Watcher の有効化	ネットワーク コントリビュータ ロールにメンバーユーザーを追加する	ネットワーク コントリビュータ ロールにゲストユーザーを追加する
Azure NSG フローログの有効化	ネットワーク コントリビュータ ロールにメンバーユーザーを追加する	ネットワーク コントリビュータ ロールにゲストユーザーを追加する
Azure アクティビティログストレージの有効化	モニターリング コントリビュータ ロールにメンバーユーザーを追加する	モニターリング コントリビュータ ロールにゲストユーザーを追加する

ロールと権限の詳細については、Microsoft Azure のマニュアルで次の用語を検索してください。

- ゲストユーザーおよびメンバーユーザーの権限
- アプリケーション開発者ロール
- Cognitive Services ユーザーロール
- モニターリング コントリビュータ ロール
- ネットワーク コントリビュータ ロール
- ストレージ アカウント コントリビュータ ロール

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 12 月 6 日	最初のバージョン。
1.1	2019 年 3 月 20 日	ベータ版の記載を削除するために更新。
1.2	2019 年 11 月 1 日	アクティビティ ログ ストレージ情報と追加のロール情報について更新。
1.3	2019 年 1 月 10 日	フローログの保持設定を削除。
1.4	2020 年 8 月 26 日	BLOB ストレージアカウントのインターネットアクセス情報について更新。
1.5	2020 年 10 月 16 日	UI の更新に基づく更新。
1.6	2021 年 2 月 2 日	ストレージアカウントの作成方法を更新。
2.0	2021 年 11 月 3 日	製品のブランド名を更新。
3.0	2022 年 6 月 1 日	設定手順を再構成および更新。
4.0	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。
4.1	2023 年 1 月 11 日	「Azure アクティビティ ログ ストレージ」セクションを削除。

著作権情報