Cisco Secure Cloud Analytics

Microsoft Azure 向けパブリック クラウド モニターリング クイック スタート ガイド

目次

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

フローログデータを生成して保存し、Secure Cloud Analytics がそのフローログデータを取り込むように Azure を設定するには、次の手順を実行します。

- Azure で、少なくとも 1 つのリソースグループをモニターする必要があります。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 で、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。
- Azure で、AD アプリケーションを作成し、アプリケーションにロールを関連付けます。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 Azure ロールの割り当て**」を参照してください。
- Azure で、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。
- Azure で、Network Watcher と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**」および「**Azure NSG フローログの有効化**」を参照してください。
- Azure で、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。
- Secure Cloud Analytics で、AD URL、サブスクリプション ID、アプリケーション ID とキー、および BLOB サービス SAS URL を含む Azure クレデンシャルとフローログのストレージ情報をアップロードします。詳細については、「**Secure Cloud Analytics Azure との統合**」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。

リソースグループの作成：

はじめる前に

- Azure ポータルにログインします。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

手順

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

AD URL とサブスクリプション ID の取得:

はじめる前に

- Azure ポータルにログインします。

手順

1. [Azure Active Directory] > [概要(Overview)]を選択します。
2. AD 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。
3. [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。
4. 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

AD 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 Azure ロールの割り当て**」を参照してください。

AD アプリケーションの作成:

はじめる前に

- Azure ポータルにログインします。

手順

1. [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。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

2. [名前(Name)] に `swc-reader` と入力します。
3. [リダイレクトURI(Redirect URI)] ドロップダウンから [Web] を選択します。
4. デフォルトの [サポートされているアカウントタイプ(Supported Account Types)] の選択は変更しないでください。
5. リダイレクト URI として `https://obsrvbl.com/azure-api/swc-reader` と入力します。
6. [登録(Register)] をクリックします。
7. アプリケーション 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。
8. [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。
9. [説明(Description)] に `SWC Reader`と入力します。
10. [有効期日(Expires)] ドロップダウンから [期限なし(Never expires)] を選択します。
11. **[保存(Save)]**をクリックします。
12. 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 Azure ロールの割り当て

`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ネットワーク コントリビュータ ロールとモニターリング 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。

AD アプリケーションへのロールの割り当て:

はじめる前に

- Azure ポータルにログインします。

手順

1. [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。
2. [アクセス制御(IAM) (Access control (IAM))] を選択します。
3. [追加(Add)] > [ロール割り当ての追加(Add role Assignment)] を選択します。
4. [ネットワーク コントリビュータ ロール(Network Contributor Role)] を選択します。
5. [アクセス権の割り当て先(Assign access to)] ドロップダウンから Azure AD のユーザー、グループ、またはサービスプリンシパルを選択します。
6. [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` と入力して選択します。
7. **[保存(Save)]**をクリックします。
8. [追加(Add)] > [ロール割り当ての追加(Add role Assignment)] を選択します。
9. [モニターリングリーダーロール(Monitoring Reader Role)] を選択します。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

10. [アクセス権の割り当て先(Assign access to)]ドロップダウンから Azure AD のユーザー、グループ、またはサービスプリンシパルを選択します。
11. ドロップダウンから `swc-reader` アプリケーションを選択します。
12. **[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

ネットワーク コントリビュータ ロールとモニター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:

はじめる前に

- Azure ポータルにログインします。

手順

1. [ストレージアカウント(Storage Accounts)]を選択します。
2. [追加(Add)]をクリックします。
3. [サブスクリプション(Subscription)]を選択します。
4. モニターする[リソースグループ(Resource group)]を選択します。
5. [ストレージアカウント名(Storage account name)]を入力します。
6. 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。
7. [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。
8. 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。
9. 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。
10. [確認して作成(Review + create)]をクリックします。
11. [作成(Create)]をクリックします。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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：

手順

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。

SAS URL の生成：

はじめる前に

- Azure ポータルにログインします。

手順

1. [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。
2. 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。
3. [共有アクセス署名（Shared access signature）] を選択します。
4. [許可されるサービス（Allowed services）] で [BLOB] を選択します。
5. [許可されるリソースタイプ（Allowed resource types）] 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。
6. [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。
7. 現在の時刻に対応する [開始時刻（Start time）] を入力します。
8. 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。
9. [許可されるプロトコル（Allowed protocols）] で [HTTPS] を選択します。
10. [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。
11. 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。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

Network Watcher の有効化：

はじめる前に

- Azure ポータルにログインします。

手順

1. [Network Watcher] > [概要（Overview）] を選択します。
2. リージョンリストを選択して展開します。
3. 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。

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 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。

フローロギングの有効化：

はじめる前に

- Azure ポータルにログインします。

手順

1. [Network Watcher] > [NSGフローログ（NSG Flow Logs）] を選択します。
2. ネットワーク セキュリティ グループを選択します。
3. [ステータス（Status）] で [オン（On）] を選択します。
4. [フローログバージョン2（Flow Logs 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. **[保存（Save）]**をクリックします。
8. 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 ～ 7 を繰り返します。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Azure アクティビティログストレージの有効化

Secure Cloud Analytics には、サブスクリプションレベルのイベントに対する追加の可視性とセキュリティ検出機能があります。この機能を有効にするには、アクティビティログのストレージアカウントへのエクスポートを設定します。

アクティビティログをストレージアカウントにエクスポート:

手順

1. Azur eポータルから、[モニター(Monitor)] > [アクティビティログ(Activity Log)] > [診断設定(Diagnostic Settings)] の順に選択します。
2. バナーをクリックして、[アクティビティログのエクスポート(Export activity log)] ブレードを起動します。
3. 表示されるブレードで、次を指定します。
    - ドロップダウンから [サブスクリプション(Subscription)] を選択します。
    - ドロップダウンからエクスポートする [リージョン(Regions)] を選択します。
    - [レガシーエクスペリエンス(Legacy experience)] を選択します。
    - [ストレージアカウントへエクスポート(Export to storage account)] を選択します。
    - 設定したストレージアカウントを選択します。
    - [保持日数(Retention (days))] で 7 を選択します。
4. **[保存(Save)]**をクリックします。

Secure Cloud Analytics Azure との統合

フローロギングを設定したら、Secure Cloud Analytics Web 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(Application 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:

はじめる前に

- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。
- AD の URL とサブスクリプション ID の詳細については、「**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。
- アプリケーション ID とキーの詳細については、「**Azure AD アプリケーションの作成**」を参照してください。
- BLOB サービス SAS URL の詳細については、「**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。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

手順

1. [設定（Settings）] > [統合（Integrations）] > [Azure] > [クレデンシャル（Credentials）] を選択します。
2. [新しいクレデンシャルの追加（Add New Credentials）] をクリックします。
3. Azure AD の URL を入力します。
4. Azure アプリケーション ID を入力します。
5. Azure アプリケーションキーを入力します。
6. [作成（Create）] をクリックします。
7. [ストレージアクセス（Storage Access）] をクリックします。
8. [新規統合（New Integration）] をクリックします。
9. [APIキー（API Key）] フィールドに **BLOB サービス SAS URL** を入力します。
10. [作成（Create）] をクリックします。
11. [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。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 Azure ロールの割り当て	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

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

その他のリソースおよびサポート

さらにサポートが必要な場合は、support@obsrvbl.com まで電子メールでお問い合わせください。

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 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 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 を参照してください。
- Secure Cloud Analytics 無料トライアルのガイドなど、インストールおよび設定ガイドについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html を参照してください。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。（1721R）

© 2022 Cisco Systems, Inc. and/or its affiliates.
All rights reserved.