トラフィックのタイプ

有効にすると、トラフィックがルールにヒットするたびにトラフィックログが生成されます。これらのログインタラクションは、送信元 IP アドレスと宛先 IP アドレス、ポート番号、使用されたプロトコルなど、着信および発信トラフィックに関する情報を記録します。ログはネットワークの監査に非常に有益であり、アクティビティをモニターしたり、潜在的なセキュリティ侵害を調査したり、ファイアウォールの状況を監視したりできます。トラフィックの可視性はいつでも有効にできますが、クラウドサービスプロバイダーのアカウントをオンボーディングし、ゲートウェイポリシーを割り当てた直後にトラフィックを有効にすることを強くお勧めします。

トラフィックの可視性を有効にするプロセスは、クラウドアカウントタイプごとに異なりますが、通常は、クラウドアカウントのリージョン、モニターする VPC/VNet、ネットワーク セキュリティ グループ、ログ用のクラウド ストレージ アカウントといったアカウント特性を識別する必要があります。

簡単セットアップウィザードを使用してアカウントをオンボーディングしていない場合、または簡単セットアップウィザードからトラフィックの可視性を有効にしていない場合は、次のログを有効にすることを強くお勧めします。

- NSG フローログ
- VPC フローログ
- DNS ログ
- Route53 クエリロギング。

（注） フローとイベントのログをダウンロードできます。[時間範囲（Time Range）] セクションで時間範囲を選択し、ダウンロードアイコンをクリックします。1 つのインスタンスで最大 10,000 件の記録がダウンロードされます。より多数の記録セットをダウンロードするには、この手順を繰り返す必要があります。

- DNS ログの有効化 （2 ページ）
- VPC フローログの有効化 （4 ページ）

DNS ログの有効化

AWS：DNS ログの有効化

前のセクションで CloudFormation テンプレートからスタックを作成するときに S3 バケットを指定した場合、route53 クエリログの宛先として機能する S3 バケットがテンプレートによって作成されます。DNS クエリログ用にモニターされる VPC は、手動で追加する必要があります。

手順

ステップ 1 AWS コンソールで、Route53 クエリロギングに移動します。

ステップ 2 テンプレートによって作成された [クエリロガー（Query Logger）] を選択します。テンプレートで指定されたプレフィックス名を持つロガーを探します。

ステップ 3 トラフィックのインサイトを取得するすべての VPC を選択し、[追加（Add）] をクリックします。

1. [クエリが記録されたVPC（VPCs that query is logging for）] セクションで、[VPCのクエリを記録（Log query for VPCs）] または [VPCの追加（Add VPC）] をクリックします。
2. すべての VPC を選択し、[選択（Choose）] をクリックします。

GCP：DNS ログの有効化

GCP DNS クエリを有効にするには、次の手順に従います。

手順

ステップ 1 GCP コンソールで VPC ネットワークに移動します。

ステップ 2 Google Cloud Shell を開き、次のコマンドを実行します。

```
gcloud dns policies create POLICY_NAME --networks=NETWORK --enable-logging
```

ステップ 3 [クラウドストレージ（Cloud Storage）] セクションに移動し、ストレージバケットを作成します。ストレージバケットの作成時には、すべてをデフォルトのままにすることができます。

（注）
DNS ログと VPC ログの両方で同じクラウドストレージバケットを共有できます。

ステップ 4 [ログルート（Logs Route）] セクションに移動します。

ステップ 5 [シンクを作成（Create Sink）] をクリックします。

ステップ 6 シンク名を指定します。

ステップ 7 シンクサービスの [クラウドストレージバケット（Cloud Storage bucket）] を選択します。

ステップ 8 上記で作成したクラウドストレージバケットを選択します。

ステップ 9 [シンクに含めるログの選択（Choose logs to include in Sink）] セクションに、`resource.type="dns_query"` という文字列を入力します。

以下の手順は、GCP の VPC フローログで言及されているものと同じです。クラウドストレージバケットを共有している場合は、以下の手順は 1 回のみ実行する必要があります。

ステップ 10 [シンクを作成（Create Sink）] をクリックします。

ステップ 11 **[IAMロール（IAM）]** > **[ロール（Roles）]**に移動します。

ステップ 12 次の権限を持つカスタムロールを作成します：**storage.buckets.list**。

ステップ 13 次の権限を持つ別のカスタムロールを作成します：

storage.buckets.get storage.objects.get storage.objects.list。

ステップ 14 Multicloud Defense Controller 用に作成されたサービスアカウントに両方のカスタムロールを追加します。2 番目のカスタムロールを追加する場合は、次の条件を入力します。

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
 "storage.googleapis.com/Object") &&
resource.name.startsWith('projects/_/buckets/<cloud storage name>')
```

ステップ 15 [パブ/サブ（Pub/Subs）]に移動します。

ステップ 16 [トピックを作成（Create Topic）] をクリックします。

ステップ 17 トピック名を入力し、[作成（create）] をクリックします。

ステップ 18 [サブスクリプション（Subscriptions）] をクリックします。作成したトピックに対してサブスクリプションが作成されたことがわかります。

ステップ 19 サブスクリプションを編集します。

ステップ 20 [配信（Delivery ）] タイプを [プッシュ（Push）] に変更します。

ステップ 21 [プッシュ（Push）] を選択したら、エンドポイント URL に `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage` と入力します。テナント名は Multicloud Defense によって割り当てられます。テナント名を表示するには、Multicloud Defense Controller に移動し、ユーザー名をクリックします。

ステップ 22 **[更新（Update）]**をクリックします。

ステップ 23 Google Could Schell を開き、次のコマンドを実行してクラウドストレージの通知を作成します：`gsutil notification create -t <TOPIC_NAME\> -f json gs://<BUCKET_NAME>`。

Azure：DNS ログ

Azure では現在、DNS ログを公開していません。Multicloud Defense Controller は、このクラウド サービ スプロバイダーのログを有効にできません。

VPC フローログの有効化

AWS：VPC フローログの有効化

前のセクションで CloudFormation テンプレートからスタックを作成するときに S3 バケットを指定した場合、VPC フローログの宛先として機能する S3 バケットがテンプレートによって作成されます。フローログは、VPC ごとに有効にする必要があります。

AWS VPC フローログを有効にするには、次の手順に従います。

手順

ステップ 1 AWS コンソールで、[VPC] セクションに移動します。
ステップ 2 VPC を選択し、その VPC の [フローログ（Flow Logs）] タブを選択します。
ステップ 3 フィルタには [すべて（All）] を選択します。
ステップ 4 宛先として [S3バケットに送信（Send to an Amazon S3 bucket）] を選択します。
ステップ 5 CloudFormation テンプレートスタックの出力からコピーした S3 バケット ARN を入力します。
ステップ 6 ログ記録形式として [カスタム形式（Custom Format）] を選択します。
ステップ 7 [ログ形式（Log Format）] ドロップダウンからすべてのフィールドをセレクトします。
ステップ 8 [フローログの作成（Create Flow Log）] をクリックします。

GCP：VPC フローログの有効化

GCP VPC フローログを有効にするには、次の手順に従います。

手順

ステップ 1 GCP コンソールで、[VPCネットワーク（VPC Network）] に移動します。
ステップ 2 VPC フローログを有効にするには、[サブネット（Subnet）] を選択します。
ステップ 3 フローログが [オン（On）] になっていることを確認します。オフになっている場合は、[編集（Edit）] オプションをクリックし、フローログをオンにします。
ステップ 4 フローログを有効にするすべてのサブネットで、フローログをオンにします。
ステップ 5 [クラウドストレージ（Cloud Storage）] セクションに移動し、ストレージバケットを作成します。ストレージバケットの作成時には、すべてをデフォルトのままにすることができます。

（注）
DNS ログと VPC ログの両方で同じクラウドストレージバケットを共有できます。

ステップ 6 [ログルート（Logs Route）] セクションに移動します。

ステップ 7 [シンクを作成（Create Sink）] をクリックします。

ステップ 8 シンクの名前を入力します。

ステップ 9 シンクサービスの [クラウドストレージバケット（Cloud Storage bucket）] を選択します。

ステップ 10 上記で作成したクラウドストレージバケットを選択します。

ステップ 11 [シンクに含めるログの選択（Choose logs to include in Sink）] セクションに、`logName:(projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows)` という文字列を入力します。

クラウドストレージバケットを共有している場合は、この手順の残りのステップは 1 回のみ実行する必要があります。

ステップ 12 [シンクを作成（Create Sink）] をクリックします。

ステップ 13 **[IAMロール（IAM）]** > **[ロール（Roles）]**に移動します。

ステップ 14 次の権限を持つカスタムロールを 1 つ作成します：`storage.buckets.list`。

ステップ 15 次の権限を持つカスタムロールを 1 つ作成します：`storage.buckets.get storage.objects.get storage.objects.list`。

ステップ 16 Multicloud Defense Controller 用に作成されたサービスアカウントに両方のカスタムロールを追加します。2 番目のカスタムロールを追加する場合は、次の条件を入力します。

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
"storage.googleapis.com/Object") && resource.name.startsWith('projects/_/buckets/<cloud
storage name>')
```

ステップ 17 [パブ/サブ（Pub/Subs）]に移動します。

ステップ 18 [トピックを作成（Create Topic）] をクリックします。

ステップ 19 トピック名を入力し、[作成（create）] をクリックします。

ステップ 20 [サブスクリプション（Subscriptions）] をクリックします。ステップ 18 で作成したトピックのサブスクリプションが作成されます。

ステップ 21 [編集（Edit）] をクリックしてサブスクリプションを編集します。

ステップ 22 [配信（Delivery ）] タイプを [プッシュ（Push）] に変更します。

ステップ 23 エンドポイント URL に `https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage` と入力します。

Multicloud Defense は、テナント名を自動的に割り当てます。テナント名を確認するには、Multicloud Defense Controller に移動し、ユーザー名をクリックします。

ステップ 24 **[更新（Update）]**をクリックします。

ステップ 25 Google Could Schell を開き、次のコマンドを実行します：`gsutil notification create -t <TOPIC_NAME> -f json gs://<BUCKET_NAME>`。

Azure：NSG フローログの有効化

Azure VPC フローログを有効にするには、次の手順に従います。

手順

ステップ 1 Azure ポータルの [リソースグループ（Resource Groups）] セクションに移動します。

ステップ 2 [作成（Create）] ボタンをクリックします。

ステップ 3 サブスクリプションを選択し、この新しいリソースグループの名前を指定します。

ステップ 4 [リージョン（Region）] を選択します。（例：（US）米国東部）。

ステップ 5 [確認して作成（Review + create）] ボタンをクリックします。

ステップ 6 [ストレージアカウント（Storage accounts）] セクションに移動し、[作成（Create）] ボタンをクリックします。

ステップ 7 作成した [サブスクリプション（Subscription）] と [リソース（Resource）] グループを選択します。

ステップ 8 [リージョン（Region）] ではリソースグループと同じリージョンを選択します。

ステップ 9 ストレージアカウントの名前を指定します。

[冗長性（Redundancy）] をローカル冗長ストレージ（LRS）にすることは**できない**ことに注意してください。

ステップ 10 [確認して作成（Review + create）] ボタンをクリックします。これにより、NSG フローログが保存されるストレージアカウントが作成されます。

ステップ 11 [サブスクリプション（Subscription）] セクションに移動し、最近作成されたサブスクリプションを見つけます。

ステップ 12 [リソースプロバイダー（Resource Providers）] に移動します。

ステップ 13 `microsoft.insights` プロバイダーと `Microsoft.EventGrid` プロバイダーが登録されていることを確認します。登録されていない場合は、[登録（Register）] ボタンをクリックします。

ステップ 14 [Network Watcher] セクションに移動します。

ステップ 15 [追加（Add）] をクリックし、NSG フローログを有効にするリージョンを追加します。

ステップ 16 **[Network Watcher]** > **[NSGフローログ（NSG flow logs）]**の順に選択します。

ステップ 17 NSG フローログを有効にする NSG で、フローログを作成します。上記で作成したストレージアカウントを指定します。[保持日数（Retention days）] を 30 日に設定します。

ステップ 18 作成したストレージアカウントに移動し、[イベント（Events）] をクリックします。

ステップ 19 [イベントサブスクリプション（Event Subscription）] をクリックします。

ステップ 20 このイベントサブスクリプションの名前を入力します。

ステップ 21 上記で作成したリソースグループを選択します。

ステップ 22 [システムトピック名（System Topic Name）] を入力します。

ステップ 23 [イベントのフィルタタイプ（Filter to Event Types）] では、デフォルト値は [BLOBが作成（Blob Created）] および [BLOBが削除（Blob Deleted）] です。

ステップ 24 [エンドポイントタイプ（Endpoint Type）] では、[Webフック（Web Hook）] を選択します。

ステップ 25 [エンドポイントの選択（Select an endpoint）] リンクをクリックします。

サブスクライバのエンドポイントは `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant_name>/azure` です。テナント名は

Multicloud Defense によって割り当てられます。Multicloud Defense Controller のユーザー名をクリックすると、テナント名を見つけることができます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。