Cisco Security Analytics and Logging

Security Analytics and Logging（SaaS）について

Cisco Security Analytics and Logging（SAL）を使用すると、すべての Firepower Threat Defense（FTD）デバイスからの接続イベント、侵入イベント、ファイルイベント、マルウェアイベント、およびセキュリティ インテリジェンス イベント、および ASA からのすべての syslog イベントと NetFlow Secure Event Logging（NSEL）イベントをキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging ）] ページから表示できます。このページでイベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。

これらのイベントをキャプチャ後、追加のライセンスを使用して、CDO から、プロビジョニングされた Cisco Secure Cloud Analytics ポータルをクロス起動できます。Cisco Secure Cloud Analytics は、イベントとネットワークフローデータの動作分析を実行することでネットワークの状態を追跡する Software as a Service（SaaS）ソリューションです。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報を送信元から収集することによって、トラフィックに関する観測内容が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。Cisco Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Cisco Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

用語に関する注 : このドキュメントでは、Cisco Security Analytics and Logging が Cisco Secure Cloud Analytics ポータル（Software as a Service（SaaS）製品）で使用されている場合、この統合は Cisco Security Analytics and Logging（SaaS）または SAL（SaaS）と呼ばれています。

ASA の Security Analytics and Logging（SAL SaaS）について

Security Analytics and Logging（SaaS）を使用すると、すべての syslog イベントと NetFlow Secure Event Logging（NSEL）を ASA からキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging ）] ページから確認できます。このページでイベントをフィルタリングして確認し、ネットワークでトリガー

されているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

Logging Analytics and Detection パッケージ（旧 **Firewall Analytics and Logging** パッケージ）を使用すると、システムは Cisco Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、行動モデリング分析を使用して Cisco Secure Cloud Analytics の観測値とアラートを生成できます。**Total Network Analytics and Monitoring** パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、プロビジョニングされた Cisco Secure Cloud Analytics ポータルを CDO からクロス起動できます。

CDO イベントビューアでの ASA イベントの表示方法

Syslog イベントと NSEL イベントは、ロギングが ASA で有効になっていて、ネットワークトラフィックがアクセス制御ルールの基準に一致するときに生成されます。イベントが Cisco Cloud に保存されたら、CDO で表示できます。

複数の Secure Event Connector（SEC）をインストールし、任意のデバイスでルールによって生成されたイベントを、syslog サーバーであるかのように任意の SEC に送信できます。SEC はイベントを Cisco Cloud に転送します。同じイベントをすべての SEC に転送しないでください。Cisco Cloud に送信されるイベントを複製すると、日次取り込み率が不必要に高くなります。

Syslog および NSEL イベントが Secure Event Connector を介して ASA から Cisco Cloud に送信される方法

Logging and Troubleshooting の基本ライセンスでは、ASA イベントが Cisco Cloud に到達する方法は次のとおりです。

1. ユーザー名とパスワードを使用して、ASA を CDO に導入準備します。
2. ASA を設定して、syslog および NSEL イベントを、syslog サーバーであるかのいように任意の SEC に転送し、デバイスでのロギングを有効にします。
3. SEC は、イベントが保存されている Cisco Cloud にイベントを転送します。
4. CDO は、設定したフィルタに基づいて、Cisco Cloud からのイベントをイベントビューアに表示します。

Logging Analytics and Detection または **Total Network Analytics and Monitoring** ライセンスでは、次のことも発生します。

1. Cisco Secure Cloud Analytics は、Cisco Cloud に保存されている ASA syslog イベントに分析を適用します。
2. 生成された観測値とアラートには、CDO ポータルに関連付けられた Cisco Secure Cloud Analytics ポータルからアクセスできます。
3. CDO ポータルから、Cisco Secure Cloud Analytics ポータルをクロス起動して、観察値とアラートを確認できます。

ソリューションで使用されるコンポーネント

Secure Device Connector（SDC）：SDC は CDO を ASA に接続します。ASA のログイン情報は SDC に保存されます。詳細については、Secure Device Connector（SDC）を参照してください。

Secure Event Connector（SEC）：SEC は、ASA からイベントを受信し、Cisco Cloud に転送するアプリケーションです。Cisco Cloud に転送されたイベントは、CDO の [イベントロギング] ページで確認したり、Cisco Secure Cloud Analytics で分析したりできます。使用環境に応じて、SEC は Secure Device Connector（ある場合）にインストールされます。または、ネットワーク内で維持する独自の CDO コネクタ仮想マシンにインストールされます。詳細については、Secure Event Connector （59 ページ）を参照してください。

適応型セキュリティアプライアンス（ASA）：ASA はアドオンモジュールとの統合サービスに加え、高度なステートフルファイアウォールおよびVPNコンセントレータ機能を提供します。ASA は、複数のセキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを1つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール オペレーション、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。

Cisco Secure Cloud Analytics は、動的エンティティモデリングを ASA イベントに適用し、この情報に基づいて検出を生成します。これにより、ネットワークから収集されたテレメトリの詳細な分析が可能になり、ネットワークトラフィックの傾向を特定し、異常な動作を調べることができます。**Logging Analytics and Detection** または **Total Network Analytics and Monitoring** ライセンスをお持ちの場合は、このサービスを利用できます。

ライセンシング

このソリューションを設定するには、次のアカウントとライセンスが必要です。

- **Cisco Defense Orchestrator**。CDO テナントが必要です。
- **Secure Device Connector**。Secure Device Connector 用の個別のライセンスはありません。
- **Secure Event Connector**。Secure Event Connector 用の個別のライセンスはありません。
- **Secure Logging Analytics（SaaS）**。「Security Analytics and Logging ライセンスの表」を参照してください。
- **適応型セキュリティアプライアンス（ASA）**。基本ライセンス以上。

Security Analytics and Logging ライセンス

Security Analytics and Logging（SaaS）を実装するには、次のいずれかのライセンスを購入する必要があります。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Logging and Troubleshooting	• ライブフィードと履歴ビューの両方で、CDO 内の ASA イベントとイベントの詳細を表示します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの ASA 展開。 • ASA イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。
Logging Analytics and Detection（旧 **Firewall Analytics and Monitoring**）	**Logging and Troubleshooting** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析をイベントに適用します。 • イベントデータに基づいて Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの ASA 展開 • ASA イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Total Network Analytics and Monitoring	**Logging Analytics and Detection** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析を ASA イベント、オンプレミスのネットワークトラフィック、およびクラウドベースのネットワークトラフィックに適用します。 • ASA イベントデータ、Cisco Secure Cloud Analytics センサーによって収集されたオンプレミスのネットワークトラフィックのフローデータ、および Cisco Secure Cloud Analytics に渡されるクラウドベースのネットワークトラフィックの組み合わせに基づいて、Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの ASA 展開 • イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • ネットワークトラフィックのフローデータをクラウドに渡すための少なくとも 1 つの Cisco Secure Cloud Analytics センサーバージョン 4.1 以降の展開、または、ネットワークトラフィックのフローデータを Cisco Secure Cloud Analytics に渡すためのクラウドベースと統合された Cisco Secure Cloud Analytics の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

データプラン

Cisco Cloud が導入準備された ASA から毎日受け取るイベント数を反映したデータプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。Logging Volume Estimator

ツールを使用して、日次取り込み率を推定でき、率が変化すると、データプランを更新できます。

データプランは、1 GB の日次ボリューム単位で、1 年、3 年、または 5 年の期間で利用できます。データプランの詳細については、Secure Logging Analytics（SaaS）発注ガイド [英語] を参照してください。

（注） Security Analytics and Logging ライセンスとデータプランがある場合、その後は別のライセンスを取得するだけで済み、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで済み、別の Security Analytics and Logging ライセンスを取得する必要はありません。

30 日間の無料トライアル

CDO にログインし、**[モニタリング（Monitoring）]** > **[イベントロギング（Event Logging）]** タブに移動して、30 日間のリスクフリーのトライアルをリクエストできます。30 日間のトライアルが終了したら、Secure Logging Analytics（SaaS）発注ガイド [英語] の手順に従って、Cisco Commerce Workspace（CCW）からサービスを継続するために必要なイベントデータボリュームを注文できます。

次のステップ

「ASA デバイスに安全なロギング分析（SaaS）を導入する」に移動します。

ASA デバイスに安全なロギング分析（SaaS）を導入する

はじめる前に

- 「ASA の Security Analytics and Logging（SAL SaaS）について」で以下について確認してください。
  - Cisco Cloud へのイベントの送信方法
  - ソリューションに含まれるアプリケーション
  - 必要なライセンス
  - 必要なデータプラン
- すでにマネージドサービスプロバイダーまたは CDO セールス担当者に問い合わせて CDO テナントを作成しました。
- Secure Device Connector（SDC）を確認してください。SDC を使用して CDO を ASA に接続することは「ベストプラクティス」と考えられますが、必須ではありません。

- ネットワークで SDC を展開する場合、次のいずれかの方法を使用してインストールできます。
  - 「CDO の VM イメージを使用した Secure Device Connector の展開」を使用して、CDO の準備された VM イメージを使用して SDC をインストールします。これが推奨される最も簡単な SDC の展開方法です。
  - 「独自の VM イメージを使用して Secure Device Connector を展開する」を使用します。
- Secure Event Connector をインストールする、任意の ASA から、テナントに導入準備された任意の SEC にイベントを送信できます。
- アカウントのユーザー向けに二要素認証を設定しました。

Cisco Security Analytics and Logging（SaaS）の導入と Secure Event Connector を介した Cisco Cloud へのイベント送信のワークフロー

1. 上の「はじめる前に」を参照し、環境が適切に設定されていることを確認してください。
2. ユーザー名とパスワードを使用して ASA デバイスの導入準備 を行います。
3. コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
4. CDO マクロを使用して ASA デバイスの NSEL を設定する
5. CDO にイベントが表示されていることを確認します。ナビゲーションバーから、[モニターリング（Monitoring）] > [イベントロギング（Event Logging）] を選択します。ライブイベントを表示するには、[ライブ] タブをクリックします。
6. [Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、次のセクション「**Cisco Secure Cloud Analytics を使用したイベントの分析**」に進みます。

Cisco Secure Cloud Analytics を使用したイベントの分析

[Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、先行するステップに加えて、次の手順を実行します。

1. Cisco Secure Cloud Analytics ポータルのプロビジョニング （80 ページ）。
2. [Total Network Analytics and Monitoring] ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開します。「総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （82 ページ）」を参照してください。
3. Cisco シングルサインオンのログイン情報に関連付ける Secure Cloud Analytics ユーザーアカウントを作成するようにユーザーに勧めます。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）」を参照してください。

4. CDO から Secure Cloud Analytics をクロス起動し、FTD イベントから生成される Secure Cloud Analytics アラートをモニターします。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）」を参照してください。

CDO からのクロス起動による Cisco Secure Cloud Analytics アラートの確認

[Firewall Analytics and Monitoring] ライセンスまたは [Total Network Analytics and Monitoring] ライセンスにより、CDO から Secure Cloud Analytics をクロス起動して、FTD イベントから生成されるアラートを確認できます。

詳細については、次の項目を参照してください。

- CDO へのサインイン
- Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）
- Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング
- ファイアウォールイベントに基づくアラートの使用

Secure Event Connector に関する問題のトラブルシューティング

ステータス情報とロギング情報の収集については、次のトラブルシューティングトピックを使用してください。

- Secure Event Connector 導入準備エラーのトラブルシューティング
- イベントロギングのトラブルシューティング ログ ファイル
- Secure Event Connector の状態を把握するためのヘルスチェックの使用

ワークフロー

「Security and Analytics Logging イベントを使用したトラブルシューティング」では、Cisco Security Analytics and Logging から生成されたイベントを使用して、ユーザーがネットワークリソースにアクセスできなかった原因を特定する方法について説明しています。

「ファイアウォールイベントに基づくアラートの使用」も参照してください。

CDO マクロを使用した Cisco Cloud への ASA Syslog イベントの送信

「コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信」で説明されているすべてのコマンドを使用する CDO マクロを作成し、同じバッチのすべての ASA でそのマクロを実行することにより、すべての ASA を設定してイベントを Cisco Cloud に送信します。

CDO のマクロツールを使用すると、CLI コマンドのリストを作成し、コマンドシンタックスの要素をパラメータに変換してから、コマンドのリストを保存して、複数回使用できるようにすることができます。マクロは、一度に複数のデバイスで実行することもできます。

実証済みのマクロを使用すると、デバイス間の設定の一貫性が促進され、コマンド ライン インターフェイスの使用時に発生する可能性のあるシンタックスエラーが防止されます。

先に進む前に、以下のトピックを参照して、マクロの使用方法を把握してください。この記事では、最終的なマクロの作成についてのみ説明します。

- デバイス管理用の CLI マクロ
- CLI マクロの作成
- CLI マクロの実行
- CLI マクロの編集
- CLI マクロの削除

ASA セキュリティ分析とロギング（SaaS）マクロを作成する

次の手順では、ASA CLI コマンドとマクロ形式の 2 種類の形式があります。ASA CLI コマンドは、ASA の構文表記法に従うように記述されています。マクロの表記法については、「CLI マクロの作成」で説明されています。

開始する前に、マクロを作成しながらコマンドの説明を読むことができるように、別ウィンドウで「コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信」を開き、この手順と並行して読めるようにしてください。

（注） ASA にロギング設定がすでに存在する場合、CDO からマクロを実行しても、最初に既存のログ設定がすべてクリアされるわけではありません。その代わり、CDO マクロで定義された設定は、既存の設定があればそれにマージされます。

ステップ 1 プレーンテキストエディタを開き、以下の手順とオプションに基づいて、マクロに変換するコマンドのリストを作成します。CDO は、マクロに記述された順序でコマンドを実行します。一部のコマンドには、{{parameters}} に変換する値が含まれます。これは、マクロの実行時に入力することになります。

ステップ 2 SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定します。

logging host コマンドを使用して、メッセージ送信先の syslog サーバーとして SEC を指定します。テナントに導入準備した SEC のいずれかにイベントを送信できます。

logging host コマンドは、イベント送信先の TCP または UDP ポートを指定します。どのポートを使用するかを判断するには、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

logging host*interface_nameSEC_IP_address* { **tcp/port** | **udp/port** }

syslog イベントを SEC に送信するために使用するプロトコルに応じて、このコマンドを 2 つの異なるマクロのいずれかに変換します。

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

（任意）TCP を使用する場合、次のコマンドをマクロのコマンドリストに追加できます。パラメータは必要としません。

logging permit-hostdown

ステップ 3　syslog サーバに送信する syslog メッセージを指定します。

logging trap コマンドを使用して、syslog サーバーに送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

SEC に送信されるイベントを重大度レベルで定義する場合は、コマンドを次のマクロに変換します。

logging trap {{severity_level}}

メッセージリストの一部であるイベントのみを SEC に送信する場合は、コマンドを次のマクロに変換します。

logging trap {{message_list_name}}

前のステップで **logging trap message_list** コマンドを選択した場合は、メッセージリスト内で syslog を定義する必要があります。マクロを作成しながらコマンドの説明を読むことができるように、「カスタムイベント リストの作成」を開いておきます。次のコマンドで開始します。

logging list*name* {**level***level* [**class***message_class*] | **message***start_id* [*-end_id*]}

次に、これを次のバリエーションに分割します。

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

最後のバリエーションでは、メッセージパラメータ{{syslog_range_or_number}} は、単一の syslog ID（106023）または範囲（302013-302018）として入力できます。メッセージリストを作成するには、1 つまたは複数のコマンドバリエーションを任意の行数で使用します。単一のマクロでは、同じ名前のすべてのパラメータが、入力した同じ値を使用することに注意してください。CDO は、空のパラメータを含むマクロを実行しません。

重要　マクロでは、**logging list** コマンドは **logging trap** コマンドの前に置く必要があります。最初にリストを定義すると、**logging trap** コマンドでそれを使用できます。下のサンプルマクロを参照してください。

ステップ 4　（任意）**syslog timestamp** を追加します。 ASA 上の syslog メッセージから生じたメッセージに日付と時刻を追加する場合は、このコマンドを追加します。タイムスタンプの値は **SyslogTimestamp** フィールドに表示されます。このコマンドをコマンドのリストに追加します。パラメータは必要としません。

logging timestamp

（注） バージョン 9.10(1) 以降、ASA は、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションを提供します。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

.

ステップ 5 **（任意）非 EMBLEM 形式の syslog メッセージにデバイス ID を含めます。**マクロを作成しながらコマンドの説明を読むことができるように、「非 EMBLEM 形式の syslog メッセージにデバイス ID を含める」を開いておきます。次は、マクロのベースとなる CLI コマンドです。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text*}

次に、これを次のバリエーションに分割します。

logging device-id cluster-id

logging device-id context-name

logging device-id hostname

logging device-id ipaddress {{interface_name}} **system**

logging device-id string {{text_16_char_or_less}}

ステップ 6 **ロギングを有効にします。**次のコマンドをそのままマクロに追加します。パラメータはありません。

logging enable

ステップ 7 マクロの最終行に **write memory を追加しないでください。**その代わりに、 **show running-config logging** コマンドを追加して、ロギングコマンドを ASA のスタートアップコンフィギュレーションにコミットする前に、入力したロギングコマンドの結果を確認します。

show running-config logging

ステップ 8 設定の変更が行われたことを確認したら、**write memory** コマンド用に別のマクロを作成して、または CDO の一括コマンド ライン インターフェイス機能を使用して、設定したすべてのデバイスにマクロを使用してコマンドを発行できます。

write memory

ステップ 9 **（任意）アクセス制御ルール「許可」イベントのロギングを有効化します。**コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信手順で説明されているこのステップは、このマクロには含まれていません。代わりに CDO GUI で実行されます。

ステップ 10 マクロを保存します。

例

1 つのマクロに結合されるコマンドのリストのサンプルを次に示します。

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
```

```
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

（注） 特定のさまざまな syslog ID または範囲を追加するための logging list コマンドがいくつかあります。{{syslog_range_or_number_X}} パラメータには、数値またはその他の差別化要因が必要です。そうしないと、マクロが入力されたときにそれらの値はすべて同じになります。また、すべてのパラメータに値が指定されていない場合には、CDO はマクロを実行しないことに注意してください。そのため、マクロには実行するコマンドのみが含まれるようにしてください。すべての syslog ID を同じリストに含める必要があるため、event_list_name は各行で同じままです。

次のタスク

マクロの実行

ASA セキュリティ分析とロギングマクロを作成して保存したら、マクロを実行して ASA syslog イベントを Cisco Cloud に送信します。

コマンドラインインターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信

この手順では、ASA の syslog イベントを Secure Event Connector（SEC）に転送してから、ロギングを有効にする方法について説明します。以下の手順では、ワークフローの完了に必要な事柄のみを説明します。ASA でロギングを設定できるすべての方法の広範な説明については、『ASDM ブック 1：Cisco ASA シリーズ ASDM コンフィギュレーション ガイド（一般的な操作）』または『CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』のいずれかのモニターリングに関する章を参照してください。

ASA コマンドのサポート制限

CDO では、次の syslog コマンドまたはメッセージの形式はまだサポートされていません。

- syslog の EMBLEM 形式
- Secure Syslog

ASA の CDO コマンド ライン インターフェイス

この手順に含まれるすべてのタスクでは、ASA の CDO のコマンド ライン インターフェイスで作業します。コマンド ライン インターフェイスのページを開くには、次の手順を実行します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、ロギングを有効にする ASA を選択します。

ステップ 4 右側の [デバイスアクション] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 5 [コマンド ライン インターフェイス（Command Line Interface）] タブをクリックします。プロンプトで以下に説明するコマンドを入力する準備ができました。

すべてのコマンドを入力したら、[送信（Send）] をクリックします。CDO の CLI インターフェイスは ASA への直接接続なので、コマンドはデバイスの実行構成に即座に書き込まれます。ASA のスタートアップ コンフィギュレーションに変更を書き込むには、さらに `write memory` コマンドを発行する必要があります。

ASA syslog イベントの Secure Event Connector への転送

導入準備した Secure Event Connector（SEC）の 1 つに ASA syslog イベントを転送し、ログを有効にするには、次の手順で以下のタスクを完了する必要があります。

ステップ 1 SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定します。

ステップ 2 すべてのログの重大度レベル、または SEC に送信する syslog イベントのリストを決定します。

ステップ 3 ロギングを有効にします。

ステップ 4 ASA のスタートアップ コンフィギュレーションに変更を保存します。

CLI を使用した Cisco Cloud への ASA Syslog イベントの送信

ステップ 1 **SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定する**

ASA から Cisco Cloud に syslog イベントを送信する場合、ユーザーは SEC が外部の syslog サーバーであるかのように SEC に転送し、SEC はメッセージを Cisco Cloud に転送します。

syslog メッセージを SEC に送信するには、次の手順を実行します。

1. TCP または UDP を使用して、SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように ASA を設定します。SEC は、IPv4 アドレスまたは IPv6 アドレスを使用できます。TCP ポートと UDP ポートのいずれかにイベントを送信します。どのポートを使用するかを判断するには、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

   logging host コマンドシンタックスの例を次に示します。

   logging host *interface_name SEC_IP_address* [[**tcp/port**] | [**udp/port**]]

   例：

   ```
    > logging host mgmt 192.168.1.5 tcp/10125
   > logging host mgmt 192.168.1.5 udp/10025
   > logging host mgmt 2002::1:1 tcp/10125
   > logging host mgmt 2002::1:1 udp/10025
   ```

   - **interface_name** 引数は、syslog サーバーへのメッセージの送信元である ASA インターフェイスを指定します。SDC との通信にすでに使用されているのと同じ ASA インターフェイスを介して、syslog メッセージを SDC に送信するのが「ベストプラクティス」です。
   - **SEC_IP_address** 引数には、SEC がインストールされている VM の IP アドレスが含まれている必要があります。
   - キーワードと引数のペア **tcp/port** または **udp/port** は、TCP プロトコルと関連するポート、または UDP プロトコルと関連するポートのいずれかを使用して、syslog メッセージが送信されるように指定します。UDP または TCP のいずれかを使用して syslog サーバにデータを送信するようにASA を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

     TCP を指定すると、ASA は syslog サーバーの障害を検出し、セキュリティ保護として ASA 経由の新しい接続をブロックします。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、手順 b を参照してください。UDP を指定すると、syslog サーバーが動作しているかどうかにかかわらず、ASA は引き続き新しい接続を許可します。有効なポート値

     （注） ASA メッセージを 2 台の別個の syslog サーバーに送信する場合は、もう一方の syslog サーバーの適切なインターフェイス、IP アドレス、プロトコル、およびポートを使用して、2 番目の logging host コマンドを実行できます。

2. （オプション）TCP 経由で SEC にイベントを送信し、SEC がダウンしているものの、ASA のログキューがいっぱいである場合、新しい接続はブロックされます。新しい接続は、syslog サーバーがバックアップされ、ログ キューがいっぱいでなくなった後に再度許可されます。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、次のコマンドを使用して、TCP 接続された syslog サーバーがダウンしたときに新しい接続をブロックする機能を無効にします。

   logging permit-hostdown

   例：

   ```
    > logging permit-hostdown
   ```

ステップ 2 次のコマンドを使用して、**syslog サーバーに送信する syslog メッセージを指定します。**

logging trap { severity_level | message_list }

例：

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASAは、重大度が 3、2、および 1 の syslog メッセージを送信します。

message_list 引数は、カスタムイベントリストを作成した場合、そのリストの名前に置き換えられます。カスタムイベントリストの指定に必要な操作は、そのリストにある syslog メッセージを Secure Event Connector に送信することだけです。上記の例では、asa_syslogs_to_cloud がイベントリストの名前です。

message_list を使用すると、Cisco Cloud に送信する syslog メッセージを明確に指定できるため、費用を節約できます。

message_list を作成するには、カスタム イベント リストの作成を参照してください。データの取り込みとストレージのコストの詳細については、「データストレージプラン」を参照してください。

ステップ 3 （オプション）syslog タイムスタンプの追加

logging timestamp コマンドを使用して、ASA での syslog メッセージの発信日時をメッセージに追加します。タイムスタンプの値は **SyslogTimestamp** フィールドに表示されます。

例：

```
> logging timestamp
```

（注） バージョン 9.10(1) 以降、ASA は、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションを提供します。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
 src interface :src IP/src port to dest IP/dest port.
```

ステップ 4 （オプション）非 EMBLEM 形式の Syslog メッセージにデバイス ID を含める

デバイス ID は、特定の ASA から送信されたすべての syslog メッセージを簡単に区別できるように、syslog メッセージに挿入できる識別子です。詳細については、「非 EMBLEM 形式の syslog メッセージにデバイス ID を含める」を参照してください。

ステップ 5 （オプション）アクセス制御ルール「許可」イベントのロギングの有効化

アクセス制御ルールによってリソースへのアクセスが拒否されると、イベントが自動的にログに記録されます。アクセス制御ルールによってリソースへのアクセスが許可されたときに生成されたイベントもログに記録する場合は、アクセス制御ルールのロギングをオンにして、重大度タイプを設定する必要があります。個々のネットワークアクセス制御ルールのロギングをオンにする方法については、「ログルールアクティビティ」を参照してください。

（注） アクセス制御ルール「許可」イベントでのロギングを有効にすると、購入したデータプランはイベントの毎日の取り込み率に基づいているため、データの消費量が増大します。

ステップ 6 ロギングの有効化

コマンドプロンプトで、「logging enable」と入力します。ASA では、個々のルールではなく、デバイス全体に対してロギングが有効になります。

例：

```
> logging enable
```

（注）　現時点では、CDO はセキュアロギングの有効化をサポートしていません。

ステップ 7　スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、「write memory」と入力します。ASA では、個々のルールではなく、デバイス全体に対してロギングが有効になります。

例：

```
> write memory
```

関連情報：

- SDC 仮想マシンへの Secure Event Connector のインストール （60 ページ）
- CDO イメージを使用して SEC をインストールする

カスタム イベント リストの作成

ASA syslog イベントを Cisco Cloud に送信するときに、次のいずれかの方法を使用してカスタムイベントリストを作成します。

- コマンド ライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- CDO マクロを使用した Cisco Cloud への ASA Syslog イベントの送信

次の 3 つの基準に基づいて、message_list とも呼ばれるイベントリストを作成できます。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（syslog サーバーや Secure Event Connector など）に送信するカスタムイベントリストを作成するには、次の手順を実行します。

ステップ 1　[デバイスとサービス] ページで、[デバイス] タブをクリックします。

ステップ 2　適切なタブをクリックして、syslog メッセージをカスタムイベントリストに含める ASA を選択します。

ステップ 3　[デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 4　次のコマンドシンタックスを使用して、**logging list** コマンドを ASA に発行します。

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id* [*-end_id*] }

name 引数には、リストの名前を指定します。キーワードと引数のペア **level** *level* により、重大度が指定されます。キーワードと引数のペア **class** *message_class* により、特定のメッセージクラスが指定されます。キーワードと引数のペア **message** *start_id* [*-end_id*] により、個々の syslog メッセージ番号または番号の範囲が指定されます。

（注） 重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベント リスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベントリスト名は使用しないでください。

- **重大度に基づいてイベントリストに syslog メッセージを追加します。**たとえば重大度を 3 に設定すると、ASAは、重大度が 3、2、および 1 の syslog メッセージを送信します。

  例：

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- **他の基準に基づいて syslog メッセージをイベントリストに追加します。**

  前回の手順で使用したものと同じコマンドを入力し、既存のメッセージ リストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

  - ID が 302013 ～ 302018 の範囲の syslog メッセージ。
  - 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
  - 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての HA クラス syslog メッセージ。

    例：

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    （注） syslogメッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

ステップ 5 スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、「**write memory**」と入力します。

例：

```
> write memory
```

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

非 EMBLEM 形式の syslog メッセージにデバイス ID を含めるように ASA を設定できます。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。この手順は、次の手順によって参照されます。

- コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- CDO マクロを使用した Cisco Cloud への ASA Syslog イベントの送信

このデバイス ID は、[イベントロギング] ページに表示される syslog イベントの SensorID フィールドに反映されます。

ステップ 1 デバイス ID を割り当てる syslog メッセージが属す ASA を選択します。

ステップ 2 [デバイスアクション] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

ステップ 3 次のコマンドシンタックスを使用して、デバイスに **logging device-id** コマンドを発行します。

logging device-id { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **string***text* }

例：

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

context-name キーワードは、現在のコンテキストの名前を装置 ID として使用することを示します（マルチ コンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**システム**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注） ASA クラスタでは、選択したインターフェイスのプライマリユニットの IP アドレスが常に使用されます。

Cluster-id キーワードは、デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

hostname キーワードは、ASA のホスト名をデバイス ID として使用することを指定します。

ipaddress *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。

string *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

ステップ 4　スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、**write memory** と入力します。

例：

```
> write memory
```

ASA デバイス向け NetFlow Secure Event Logging（NSEL）

ASA からの基本的な Syslog メッセージには、ASA によって報告されたイベントが脅威を示しているかどうかを Secure Cloud Analytics が判断するために必要な多くのデータが不足しています。Netflow Secure Event Logging（NSEL）は、そのデータを Secure Cloud Analytics に提供します。

「フローは、ネットワークデバイスを通過する、いくつかの共通プロパティを持つ一方向のパケットシーケンスとして定義されます。これらの収集されたフローは、外部デバイスである NetFlow コレクタにエクスポートされます。ネットワークフローは非常に細分化されています。たとえば、フローレコードには IP アドレス、パケット数とバイト数、タイムスタンプ、サービスのタイプ（ToS）、アプリケーションポート、入出力インターフェイスなどの詳細が含まれます。」[1]

Cisco ASA では、NetFlow バージョン 9 サービスがサポートされています。ASA の NSEL の導入は、フロー内の重要なイベントを示すレコードだけをエクスポートするステートフルな IP フローのトラッキング方式を提供します。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。

このドキュメントでは、CDO マクロを使用して ASA に NetFlow を設定するための簡単なアプローチについて説明します。『Cisco NetFlow Implementation Guide』には、ASA に NetFlow を設定することに関する非常に詳細な説明が記載されており、このコンテンツに付随する貴重なリソースとなっています。

次の作業

「CDO マクロを使用して ASA デバイスの NSEL を設定する」に進みます。

関連記事

1. （『Cisco Systems NetFlow サービス エクスポート バージョン 9』。インターネット技術特別委員会、ネットワーク ワーキング グループ、Request for Comments（RFC）：3954、2004 年 10 月、B. Claise 編集。https://www.ietf.org/rfc/rfc3954.txt）

CDO マクロを使用して ASA デバイスの NSEL を設定する

ASA は、NetFlow Secure Event Logging（NSEL）を使用して詳細な接続イベントデータをレポートします。この接続イベントデータ（双方向フロー統計を含む）に Stealthwatch Cloud 分析を適用できます。この手順では、ASA デバイスで NSEL を設定し、NSEL イベントをフローコレクタに送信する方法について説明します。このケースでは、フローコレクタは Secure Event Connector（SEC）です。

この手順では、**Configure NSEL** マクロを参照します。

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

クラスマップの一般名、グローバルポリシーに追加されたクラスマップなど、すべてのデフォルト値が入力された Configure NSEL マクロの例を次に示します。これらの手順を完了すると、マクロは次のようになります。

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

はじめる前に

次の情報を用意します。

- CDO マクロを初めて使用する場合は、次のトピックをお読みください。
  - デバイスの管理用 CLI マクロ
    - CLI マクロの編集
    - CLI マクロの実行

- ASA からデータを受け取る SEC の IPv4 アドレス
- SEC にデータを送信する ASA のインターフェイス
- NetFlow イベントの転送に使用する UDP ポート番号「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索 （58 ページ）」を参照してください。
- ASA グローバルポリシーの名前を決定する （29 ページ）

ワークフロー

CDO マクロを使用して ASA デバイスの NSEL を設定するには、次のワークフローに従います。各手順に従う必要があります。

1. [NSELの設定（Configuring NSEL）] マクロを開く （22 ページ）。
2. NSEL メッセージの宛先と SEC に送信される間隔の定義 （23 ページ）。
3. SEC に送信される NSEL イベントを定義するクラスマップの作成 （24 ページ）。
4. NSEL イベントのポリシーマップの定義 （25 ページ）。
5. 冗長な Syslog メッセージの無効化 （26 ページ）。
6. マクロのレビューと送信 （27 ページ）。

次の作業

[NSELの設定（Configuring NSEL）] マクロを開く （22 ページ）に移動して、前述のワークフローを開始します。

[NSELの設定（Configuring NSEL）] マクロを開く

始める前に

これは長いワークフローの最初の部分です。開始する前に CDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ） を参照してください。

ステップ 1 [デバイスとサービス] ページで、[デバイス] タブをクリックします。

ステップ 2 適切なデバイスタイプのタブをクリックし、NetFlow セキュアイベントロギング（NSEL）を設定する ASA を選択します。

ステップ 3 [デバイスアクション] ペインで、[コマンドライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 4 マクロスター  をクリックして、使用可能なマクロのリストを表示します。

ステップ 5 マクロのリストから、[NSELの設定（Configuring NSEL）] を選択します。

ステップ 6 [マクロ（Macro）] ボックスで、[パラメータの表示（View Parameters）] をクリックします。

次のタスク

NSEL メッセージの宛先と SEC に送信される間隔の定義 （23 ページ） に進みます。

NSEL メッセージの宛先と SEC に送信される間隔の定義

NSEL メッセージは、テナントに導入準備した SEC のいずれかに送信できます。以下の手順では、このセクションのマクロを参照しています。

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）を参照してください。

ステップ 1 **flow-export destination** コマンドは、NetFlow パケットの送信先のコレクタを定義します。この場合、SEC に送信します。次のパラメータのフィールドに入力します。

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{SEC_IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{SEC_NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

ステップ 2 **flow-export template timeout-rate** コマンドは、テンプレートレコードがすべての設定された出力先に送信される間隔を指定します。

- **{{timeout_rate_in_mins}}**：テンプレートが再送信されるまでの分数を入力します。60 分の値を使用することをお勧めします。SEC はテンプレートを処理しません。数字を大きくすると、SEC へのトラフィックが減少します。

ステップ 3 **flow-export delay flow-create** コマンドは、flow-create イベントの送信を指定した秒数遅らせます。この値は、推奨されるアクティブタイムアウト値と一致し、ASA からエクスポートされるフローイベントの数を減らします。この場合、NSEL イベントが最初に CDO に表示されるのは、接続の終了時または接続の作成

から 55 秒以内のいずれか早い方となると考えてください。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。

- **{{delay_flow_create_rate_in_secs}}**：flow-create イベントの送信間の遅延秒数を入力します。55 秒の値を使用することをお勧めします。

ステップ 4 **flow-export active refresh-interval** コマンドは、長時間フローのステータスの更新が ASA から送信される頻度を定義します。有効な値は 1 ～ 60 分です。[フロー更新間隔（Flow Update Interval）] フィールドで、**flow-export active refresh-interval** を **flow-export delay flow-create interval** よりも少なくとも 5 秒長く設定すると、flow-update イベントが flow-creation イベントの前に表示されなくなります。

- **{{refresh_interval_in_mins}}**：**値を 1 分にすることをお勧めします。**有効な値は 1 ～ 60 分です。

次のタスク

SEC に送信される NSEL イベントを定義するクラスマップの作成 （24 ページ） に進みます。

SEC に送信される NSEL イベントを定義するクラスマップの作成

マクロ内の次のコマンドは、クラス内のすべての NSEL イベントをグループ化し、そのクラスを Secure Event Connector（SEC）にエクスポートします。以下の手順では、このセクションのマクロを参照しています。

```
class-map {{flow_export_class_name}}
match {{add_this_traffic_to_class_map}}
```

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）を参照してください。

ステップ 1 **class-map** コマンドは、SEC にエクスポートされる NSEL トラフィックを識別するクラスマップに名前を付けます。

- **{{flow-export-class-name}}**：クラスマップの名前を入力します。名前の長さは最大 40 文字です。名前「class-default」と、「_internal」または「_default」で始まる名前はすべて予約されています。すべてのタイプのクラスマップで同じ名前空間が使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。

ステップ 2 クラスマップに関連付けられる（一致する）トラフィックを識別します。**{{add_this_traffic_to_class_map}}** の値として、次のいずれかのオプションを選択します。

- **{{add_this_traffic_to_class_map}}** フィールドに **any** と入力します。NSEL トラフィックのすべてのトラフィックタイプが監視されます。**値「any」を使用することをお勧めします。**
- **{{add_this_traffic_to_class_map}}** フィールドに **access-list** ***name-of-access-list*** と入力します。作成したアクセスリストに関連付けられたすべてのトラフィックが関連付けられます。詳細については、Cisco

ASA NetFlow 実装ガイド [英語] の「Configure Flow-Export Actions Through Modular Policy Framework」を参照してください。

次のタスク

NSEL イベントのポリシーマップの定義 （25 ページ）に進みます。

NSEL イベントのポリシーマップの定義

このタスクでは、前のタスクで作成したクラスに NetFlow エクスポートアクションを割り当て、そのクラスを新しいポリシーマップに割り当てます。以下の手順では、このセクションのマクロを参照しています。

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）を参照してください。

ステップ 1 **policy-map** コマンドは、ポリシーマップを作成します。次のタスクでは、このポリシーマップをグローバルポリシーに関連付けます。

- **{{global_policy_map_name}}**：ポリシーマップの名前を入力します。ファイアウォールの既存のグローバルポリシーがある場合は、その名前を使用することをお勧めします。グローバルポリシーのデフォルト名は **global_policy** です。ASA グローバルポリシーの名前を決定する新しいポリシーマップを作成し、『Cisco ASA NetFlow 実装ガイド』の「モジュラ ポリシー フレームワークを使用した flow-export アクションの設定」に従ってグローバルに適用すると、残りの検査ポリシーは非アクティブ化されます。

ステップ 2 **class** コマンドでは、SEC に送信される NSEL イベントを定義するクラスマップの作成 （24 ページ）で作成したクラスマップの名前が継承されます。

ステップ 3 **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} コマンドは、フローコレクタ（この場合は SEC）に送信する必要があるイベントタイプを定義します。

- **{{event-type}}**：event_type キーワードは、フィルタリングされるサポートされているイベントの名前です。値「all」を使用することをお勧めします。
- **{{SEC_IPv4_address}}**：これは SEC の IPv4 アドレスです。その値は、NSEL メッセージの宛先と SEC に送信される間隔の定義 （23 ページ）で入力した値から継承されます。

次のタスク

冗長な Syslog メッセージの無効化 （26 ページ） に進みます。

冗長な Syslog メッセージの無効化

以下の手順では、このセクションのマクロを参照しています。コマンドを変更する必要はありません。

logging flow-export-syslogs disable

NetFlow でフロー情報をエクスポートできるようにすると、次の表に記載されている syslog メッセージが冗長になります。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージをディセーブルにすることをお勧めします。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギングタイプ間が時系列順になる保証はありません。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
106100	アクセス制御ルール（ACL）が発生するたびに生成されます。	1：フローが作成されました（ACL がフローを許可した場合）。 3：フローが拒否されました（ACL がフローを拒否した場合）。	0：ACL がフローを許可した場合。 1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。	3：フローが拒否されました。	1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
106023	**access-group** コマンドによってインターフェイスに接続された ACL によってフローが拒否された場合。	3：フローが拒否されました。	1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
302013、302015、302017、302020	TCP、UDP、GRE、および ICMP 接続の作成。	1：フローが作成されました。	0：無視します。
302014、302016、302018、302021	TCP、UDP、GRE、および ICMP 接続のティアダウン。	2：フローが削除されました。	0：無視します。 > 2000：フローが切断されました。
313001	デバイスへの ICMP パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
710003	デバイスインターフェイスへの接続の試行が拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

冗長なsyslogメッセージを無効にしない場合は、このマクロを編集して、次の行のみを削除できます。

logging flow-export-syslogs disable

後に NetFlow 関連の Syslog メッセージの無効化と再有効化の手順を実行することで、個別の syslog メッセージを有効化または無効化できます。

マクロのレビューと送信

始める前に

この手順は、より大きなワークフローの一部です。始める前に、「CDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）」を参照してください。

ステップ 1 マクロのフィールドに入力したら、[確認] をクリックして、コマンドを ASA への送信前に確認します。

ステップ 2 コマンドへの応答に問題がなければ、[送信（Send）] をクリックします。

ステップ 3 コマンドを送信した後で、「一部のコマンドが実行構成に変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。

- [ディスクへの書き込み（Write to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行構成のその他の変更がデバイスのスタートアップ構成に保存されます。

• [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

CDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ） で説明されている
ワークフローが完了しました。

ASA から NetFlow Secure Event Logging（NSEL）構成を削除する

この手順では、Secure Event Connector（SEC）を NSEL フローコレクタとして指定する ASA で NetFlow Secure Event Logging（NSEL）の構成を削除する方法について説明します。この手順では、「CDO マクロを使用して ASA デバイスの NSEL を設定する」で説明されているマクロを元に戻します。

この手順では、このマクロを **DELETE NSEL** と呼びます。

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

DELETE-NSEL マクロを開く

ステップ 1 [デバイスとサービス] ページで、[デバイス] タブをクリックします。

ステップ 2 適切なデバイスタイプのタブをクリックし、NetFlow セキュアイベントロギング（NSEL）の設定を削除する ASA を選択します。

ステップ 3 [デバイスアクション] ペインで、[コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 4 マクロスター  Macros をクリックして、使用可能なマクロのリストを表示します。

ステップ 5 マクロのリストで、[DELETE-NSEL] を選択します。

ステップ 6 [マクロ（Macro）] ボックスで、[パラメータの表示（View Parameters）] をクリックします。

マクロに値を入力して No コマンドを完成させる

ASA CLI では、コマンドの「no」形式を使用してそのコマンドを削除します。マクロのフィールドに入力して、コマンドの「no」形式を完成させます。

ステップ 1 policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}**：policy-map 名の値を入力します。

ステップ 2 no class {{flow_export_class_name}}

- **{{flow_export_class_name}}**：class-map 名の値を入力します。

ステップ 3 no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}**：class-map 名の値は、上記の手順から継承されます。

ステップ 4 no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

ステップ 5 no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}**：flow-export template のタイムアウトレートを入力します。

ステップ 6 no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}**：flow-export delay flow-create のレートを入力します。

ステップ 7 no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}**：flow-export active refresh-interval の間隔を入力します。

ASA グローバルポリシーの名前を決定する

ASA のグローバルポリシーの名前を決定するには、次の手順に従います。

ステップ 1 [デバイスとサービス] ページで、グローバルポリシーの名前を検索するデバイスを選択します。
ステップ 2 [デバイスアクション] ペインで、[>_コマンドリファレンス（>_Command Reference）] を選択します。
ステップ 3 コマンド ライン インターフェイス ウィンドウのプロンプトで、次のように入力します。

show running-config service-policy

以下の例の出力では、global_policy はグローバルポリシーの名前です。

例：

> **show running-config service-policy**

service-policy global_policy global

NSEL データフローのトラブルシューティング

CDO マクロを使用して ASA デバイスの NSEL を設定するしたら、次の手順を使用して、NSEL イベントが ASA から Cisco Cloud に送信されていること、および Cisco Cloud がそれらのイベントを受信していることを確認します。

NSEL イベントを Secure Event Connector（SEC）に送信してから Cisco Cloud に送信するように ASA を設定すると、データはすぐには流れないことに注意してください。ASA で NSEL 関連のトラフィックが生成されていると仮定すると、最初の NSEL パケットが到着するまでに数分かかることがあります。

（注） このワークフローは、「flow-export counters」コマンドと「capture」コマンドを単純に使用して NSEL データフローをトラブルシューティングする方法を示しています。これらのコマンドの使用法の詳細については、CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーションガイド（一般的な操作）[英語] および Cisco ASA NetFlow 実装ガイド [英語] の「Monitoring NSEL」を参照してください。

次のタスクを実行します。

- NetFlow パケットが SEC に送信されていることを確認する
- NetFlow パケットが Cisco Cloud 受信されていることを確認する

NSEL イベントが SEC に送信されたことを確認する

次の 2 つのコマンドのいずれかを使用して、NSEL パケットが SEC に送信されていることを確認します。

- flow-export counters
- capture

「flow-export counters」コマンドは、送信中の flow-export パケットと NSEL エラーをチェックするために使用します。

- ASA が NSEL イベントを SEC に送信するように設定されていることを確認してください。「CDO マクロを使用して ASA デバイスの NSEL を設定する」を参照してください。
- SEC IP アドレスは、NSEL イベントのフローコレクタアドレスです。テナントに複数の SEC を導入準備している場合は、正しい IP アドレスを使用していることを確認してください。
- NetFlow イベントの転送に使用する UDP ポート番号を検索します。「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。
- ASA でそこから NSEL イベントを送信するための推奨インターフェイスは管理インターフェイスです。お使いのインターフェイスとは異なる場合があります。

CDO のコマンドライン インターフェイスを使用して、NSEL に設定した ASA にこれらのコマンドを送信します。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切な [デバイス] タブをクリックし、NSEL イベントを SEC に送信するように設定した ASA を選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ペインで、[コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 5 `clear flow-export counters` コマンドを実行して、フローエクスポートカウンタをリセットします。これにより、エクスポートフローカウンタがクリアされてゼロになるため、新しいイベントの発生を簡単に知ることができます。

例：

```
> clear flow-export counters

Done!
```

ステップ 6 show flow-export counters コマンドを実行して、NSEL パケットの宛先、送信されたパケットの数、およびエラーを確認します。

例：

```
>show flow-export counters

destination: management 209.165.200.225 10425

Statistics:

packets sent 25000

エラー：

block allocation errors 0

invalid interface 0

template send failure 0

no route to collector 0

source port allocation 0
```

上記の出力では、宛先行は、NSEL イベントの送信元の ASA のインターフェイス、SEC の IP アドレス、SEC のポート 10425 を示しています。また、25000 のパケットが送信されたことも示しています。

エラーがなく、パケットが送信されている場合は、以下の「NetFlow パケットが Cisco Cloud 受信されていることを確認する」にスキップしてください。

エラーの説明：

- [ブロック割り当てエラー（block allocation errors）]：ブロック割り当てエラーを受け取った場合、ASA によってフローエクスポーターにメモリが割り当てられていません。

- 回復処置：Cisco Technical Assistance Center（TAC）に連絡してください。

- [無効なインターフェイス（invalid interface）]：NSELイベントをSECに送信しようとしていますが、フローエクスポート用に定義したインターフェイスがそれを行うように設定されていないことを示します。
  - 回復処置：NSEL の設定時に選択したインターフェイスを確認します。管理インターフェイスを使用することをお勧めします。お使いのインターフェイスが異なる場合があります。

- [テンプレート送信失敗（template send failure）]：NSEL を定義するためのテンプレートが正しく解析されませんでした。
  - 回復処置：Defense Orchestrator サポートに連絡してください。

- [コレクタへのルートがない（no route to collector）]：ASA から SEC へのネットワークルートがないことを示します。
  - 回復処置：
    - NSEL を設定したときに SEC に使用した IP アドレスが正しいことを確認してください。
    - SEC のステータスがアクティブで、最近のハートビートが送信されていることを確認します。「SDC に到達不能」を参照してください。
    - Secure Device Connector のステータスがアクティブで、最近のハートビートが送信されていることを確認します。

- [送信元ポートの割り当て（source port allocation）]：ASAにポート不良がある可能性を示しています。

「capture」コマンドを使用して、ASAからSECに送信されたNSELパケットをキャプチャする

- ASA が NSEL イベントを SEC に送信するように設定されていることを確認してください。「CDO マクロを使用して ASA デバイスの NSEL を設定する」を参照してください。
- SEC IP アドレスは、NSEL イベントのフローコレクタアドレスです。テナントに複数の SEC を導入準備している場合は、正しい IP アドレスを使用していることを確認してください。
- NetFlowイベントの転送に使用するUDPポート番号を検索します。「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。
- ASA でそこから NSEL イベントを送信するための推奨インターフェイスは管理インターフェイスです。お使いのインターフェイスとは異なる場合があります。

CDO のコマンドライン インターフェイスを使用して、NSEL に設定した ASA にこれらのコマンドを送信します。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切な [デバイスタイプ] タブをクリックし、NSEL イベントを SEC に送信するように設定した ASA を選択します。

ステップ 4 右側の [デバイスアクション] ペインで、[コマンドライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 5 コマンドウィンドウで、以下の [キャプチャ（capture）] コマンドを実行します。

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

引数の説明

- *capture_name* は、パケットキャプチャの名前です。
- *interface_name* は、NSEL パケットが ASA から送信されるインターフェイスの名前です。
- *IP_of_SEC* は、SEC VM の IP アドレスです。
- *NetFlow_port* は、NSEL イベントが送信されるポートです。

これにより、パケットキャプチャが開始されます。

ステップ 6 キャプチャされたパケットを表示するには、**show capture** コマンドを実行します。

> show capture*capture_name*

ここで、*capture_name* は、前の手順で定義したパケットキャプチャの名前です。

キャプチャの時刻、パケットの送信元の IP アドレス、IP アドレス、およびパケットの送信先ポートを示す出力の例を次に示します。この例では、192.168.25.4 は SEC の IP アドレスであり、ポート 10425 は NSEL イベントを受信する SEC 上のポートです。

6 パケットがキャプチャされました

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

ステップ 7 パケットキャプチャを手動で停止するには、**capture stop** コマンドを実行します。

> capture *capture_name***stop**

ここで、*capture_name* は、前の手順で定義したパケットキャプチャの名前です。

NetFlow パケットが Cisco Cloud 受信されていることを確認する

はじめる前に

ASA から NSEL イベントが送信されていることを確認します。

ライブ NSEL イベントの確認

ライブイベントと履歴イベントの両方を確認します。

この手順では、過去 1 時間以内に Cisco Cloud が受信した NSEL イベントをフィルタ処理します。

ステップ 1 CDO の左側のメニューバーで、**[モニターリング（Monitoring）]** > **[イベントロギング]** を選択します。
ステップ 2 [ライブ（Live）] タブをクリックします。
ステップ 3 イベントフィルタを開いた状態でピン留めします。
ステップ 4 [ASAイベント（ASA Event）] セクションで、[NetFlow] がオンになっていることを確認します。
ステップ 5 [センサーID] フィールドで、NSEL イベントを送信するために設定した ASA の IPアドレスを入力します。
ステップ 6 フィルタの一番下の [NetFlowイベントを含める（Include NetFlow Events）] がオンになっていることを確認します。

NSEL のイベント履歴の確認

この手順では、指定した時間枠内に Cisco Cloud が受信した NSEL イベントをフィルタリングします。

ステップ 1 CDO で、左側のメニューバーにある **[モニタリング（Monitoring）]** > **[イベントロギング]** を選択します。
ステップ 2 [履歴（Historic）] タブをクリックします。
ステップ 3 イベントフィルタを開いた状態でピン留めします。
ステップ 4 [ASAイベント（ASA Event）] セクションで、[NetFlow] がオンになっていることを確認します。
ステップ 5 CDO が NSEL イベントを受信したことがあるかどうかを確認するために、時間を十分にさかのぼって [開始時刻（Start time）] を設定します。
ステップ 6 [センサーID] フィールドで、NSEL イベントを送信するために設定した ASA の IPアドレスを入力します。
ステップ 7 フィルタの一番下の [NetFlowイベントを含める（Include NetFlow Events）] がオンになっていることを確認します。

ASA イベント タイプ

イベントロギングページでのイベントの検索とフィルタリング場合、イベントタイプのリストから選択できますこれらのイベントタイプは、syslog ID のグループを表します。次の表は、どの ASA イベントタイプにどの syslog ID が含まれるかを示しています。特定の syslog ID の詳細については、『Cisco ASA シリーズ Syslog メッセージガイド』で検索できます。

一部の syslog イベントには、追加の属性「EventName」があります。属性:値のペアでフィルタ処理することにより、EventName 属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。「Syslog イベントの EventName 属性」を参照してください。

ASA デバイス向け NetFlow Secure Event Logging（NSEL） は、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの NetFlow イベント ID は、『Cisco ASA NetFlow 実装ガイド』で定義されています。

フィルタ名（Filter Name）	対応する Syslog イベントまたは NetFlow イベント
AAA	109001-109035 113001-113027
BotNet	338001-338310
フェールオーバー	101001-101005、102001、103001-103007、104001-104004、105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	106001、106007、106012、106013、106015、106016、106017、106020、106021、106022、106023、106025、106027 Firewall Denied イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。

フィルタ名（Filter Name）	対応する Syslog イベントまたは NetFlow イベント
Firewall Traffic	106001-106100、108001-108007、110002-110003 201002-201013、209003-209005、215001 302002-302304、302022-302027、303002-303005、313001-313008、317001-317006、324000-324301、337001-337009 400001-400050、401001-401005、406001-406003、407001-407003、408001-408003、415001-415020、416001、418001-418002、419001-419003、424001-424002、431001-431002、450001 500001-500005、508001-508002 607001-607003、608001-608005、609001-609002、616001 703001-703003、726001 Firewall Traffic イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。
IPSec VPN	402001-402148、602102-602305、702304-702307
NAT	201002-201013、202001-202011、305005-305012
SSL VPN	716001-716060、722001-722053、723001-723014、724001-724004、725001-725015
NetFlow	0、1、2、3、5

関連情報：

- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性 （105 ページ）
- Syslog イベントの EventName 属性

解析済みの ASA Syslog イベント

解析済みの syslog イベントは、他の syslog イベントよりも多くのイベント属性を含んでおり、特定の解析済みフィールドの検索を可能にします。SEC は、指定したすべての ASA イベントを Cisco Cloud に転送しますが、解析されるのは以下の表の syslog メッセージのみです。すべての解析済みの Syslog イベントは、識別しやすいように EventType が斜体で表示されます。

syslog ID	syslog カテゴリ	syslog メッセージの目的
106015	ファイアウォール	州外 TCP の拒否を表します。
106023	ファイアウォール	実際の IP パケットが ACL によって拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。
106100	アクセスリスト/ユーザーセッション	パケットは ACL によって許可または拒否されました。
113019	ユーザー認証（User Authentication）	クリティカルな AnyConnect
302013、302015、302017、302020	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302014, 302016, 302018, 302021	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302020 ～ 302021	ユーザ セッション	ICMP セッションの確立と解除。
305006	ユーザーセッション/NAT および PAT	NAT 接続の失敗
305011 ～ 305014	ユーザーセッション/NAT および PAT	NAT 確立/解除関連
313001、313008	IP スタック	ボックスへの接続が拒否されたことを表します。
414004	システム（System）	クリティカルな AnyConnect
609001 ～ 609002	ファイアウォール	ネットワーク状態コンテナは、ゾーンに接続されたホスト **ip-address** 用に予約済み/削除済みでした。
710002、710004、710005	ユーザ セッション	ボックスへの接続の失敗
710003	ユーザ セッション	ボックスへの接続が拒否されたことを表します。

syslog ID	syslog カテゴリ	syslog メッセージの目的
746012、746013	ユーザ セッション	クリティカルな AnyConnect

syslog の詳細な説明については、『Cisco ASA Series Syslog Messages』を参照してください。

関連情報：

- コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- イベントロギングページでのイベントの検索とフィルタリング

Cisco Secure Firewall Cloud Native 向け Secure Logging and Analytics（SaaS）

Secure Analytics and Logging（SaaS）を使用すると、Cisco Secure Firewall Cloud Native からすべての syslog イベントと NetFlow Secure Event Logging（NSEL）をキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging）] ページから確認できます。このページでイベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

Logging Analytics and Detection パッケージ（旧 **Firewall Analytics and Logging** パッケージ）を使用すると、システムは Cisco Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、行動モデリング分析を使用して Cisco Secure Cloud Analytics の観測値とアラートを生成できます。**Total Network Analytics and Monitoring** パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、CDO から、プロビジョニングされた Secure Cloud Analytics ポータルを相互起動できます。

CDO イベントビューアでの Cisco Secure Firewall Cloud Native イベントの表示方法

Syslog イベントと NSEL イベントは、ロギングが Cisco Secure Firewall Cloud Native で有効になっていて、ネットワークトラフィックがアクセス制御ルールの基準に一致するときに生成されます。イベントが Cisco Cloud に保存されたら、CDO で表示できます。

複数の Secure Event Connector（SEC）をインストールし、任意のデバイスでルールによって生成されたイベントを、syslog サーバーであるかのように任意の SEC に送信できます。SEC はイベントを Cisco Cloud に転送します。同じイベントをすべての SEC に転送しないでください。Cisco Cloud に送信されるイベントを複製すると、日次取り込み率が不必要に高くなります。

Syslog および NSEL イベントが Secure Event Connector を介して Cisco Secure Firewall Cloud Native から Cisco Cloud に送信される方法

Logging and Troubleshooting の基本ライセンスでは、Cisco Secure Firewall Cloud Native イベントが Cisco Cloud に到達する方法は次のとおりです。

1. クラスタエンドポイント、名前空間、およびトークンを使用して、Cisco Secure Firewall Cloud Native を CDO に導入準備します。.
2. Cisco Secure Firewall Cloud Native を設定して、syslog および NSEL イベントを、syslog サーバーであるかのように任意の SEC に転送し、デバイスでのロギングを有効にします。
3. SEC は、イベントが保存されている Cisco Cloud にイベントを転送します。
4. CDO は、設定したフィルタに基づいて、Cisco Cloud からのイベントをイベントビューアに表示します。

Logging Analytics and Detection または **Total Network Analytics and Monitoring** ライセンスでは、次のことも発生します。

1. Cisco Secure Cloud Analytics は、Cisco Cloud に保存されている Cisco Secure Firewall Cloud Native syslog イベントに分析を適用します。
2. 生成された観測値とアラートには、CDO ポータルに関連付けられた Cisco Secure Cloud Analytics ポータルからアクセスできます。
3. CDO ポータルから、Cisco Secure Cloud Analytics ポータルをクロス起動して、観察値とアラートを確認できます。

ソリューションで使用されるコンポーネント

Secure Device Connector（SDC）：SDC は、CDO を Cisco Secure Firewall Cloud Native に接続します。Cisco Secure Firewall Cloud Native のログイン情報は SDC に保存されます。詳細については、Secure Device Connector（SDC）を参照してください。

Secure Event Connector（SEC）：SEC は、Cisco Secure Firewall Cloud Native からイベントを受信し、Cisco Cloud に転送するアプリケーションです。Cisco Cloud に転送されたイベントは、CDO の [イベントロギング] ページで確認したり、Cisco Secure Cloud Analytics で分析したりできます。使用環境に応じて、SEC は Secure Device Connector（ある場合）にインストールされます。または、ネットワーク内で維持する独自の CDO コネクタ仮想マシンにインストールされます。詳細については、Secure Event Connector （59 ページ）を参照してください。

Cisco Secure Firewall Cloud Native：Cisco Secure Firewall Cloud Native は、Kubernetes（K8s）オーケストレーションを使用して、シスコの業界をリードするセキュリティをクラウド ネイティブ フォーム ファクタ（CNFW）にシームレスに拡張し、拡張性と管理性を実現します。Amazon Elastic Kubernetes Service（Amazon EKS）を使用すると、AWS クラウドで Kubernetes アプリケーションを柔軟に開始、実行、スケーリングできます。Amazon EKS は、可用性が高く安全なクラスタを提供し、パッチ適用、ノードのプロビジョニング、更新などの主要なタスクを自動化するのに役立ちます。

Cisco Secure Cloud Analytics は動的エンティティモデリングを Cisco Secure Firewall Cloud Native イベントに適用し、この情報に基づいて検出を生成します。これにより、ネットワークから収集されたテレメトリの詳細な分析が可能になり、ネットワークトラフィックの傾向を特定し、異常な動作を調べることができます。**Logging Analytics and Detection** または **Total Network Analytics and Monitoring** ライセンスをお持ちの場合は、このサービスを利用できます。

ライセンシング

このソリューションを設定するには、次のアカウントとライセンスが必要です。

- **Cisco Defense Orchestrator**。CDO テナントが必要です。
- **Secure Device Connector**。Secure Device Connector 用の個別のライセンスはありません。
- **Secure Event Connector**。Secure Event Connector 用の個別のライセンスはありません。
- **Secure Logging Analytics（SaaS）**。「Security Analytics and Logging ライセンスの表」を参照してください。
- **Cisco Secure Firewall Cloud Native**。基本ライセンス以上。

Security Analytics and Logging ライセンス

Security Analytics and Logging（SaaS）を実装するには、次のいずれかのライセンスを購入する必要があります。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Logging and Troubleshooting	• ライブフィードと履歴ビューの両方で、CDO 内の Cisco Secure Firewall Cloud Native イベントとイベントの詳細を表示します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの Cisco Secure Firewall Cloud Native 展開。 • Cisco Secure Firewall Cloud Native イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Logging Analytics and Detection（旧 **Firewall Analytics and Monitoring**）	**Logging and Troubleshooting** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析をイベントに適用します。 • イベントデータに基づいて Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの Cisco Secure Firewall Cloud Native 展開。 • Cisco Secure Firewall Cloud Native イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

ライセンス名	提供される機能	利用可能なライセンス期間	機能の前提条件
Total Network Analytics and Monitoring	**Logging Analytics and Detection** の機能に加えて、以下の機能 • 動的エンティティモデリングと行動分析を Cisco Secure Firewall Cloud Native イベント、オンプレミスのネットワークトラフィック、およびクラウドベースのネットワークトラフィックに適用します。 • Cisco Secure Firewall Cloud Native イベントデータ、Cisco Secure Cloud Analytics センサーによって収集されたオンプレミスのネットワークトラフィックのフローデータ、および Cisco Secure Cloud Analytics に渡されるクラウドベースのネットワークトラフィックの組み合わせに基づいて、Cisco Secure Cloud Analytics でアラートを開き、CDO イベントビューアからクロス起動します。	• 1 年 • 3 年 • 5 年	• CDO • ソフトウェアバージョン 9.6 以降を実行しているオンプレミスの Cisco Secure Firewall Cloud Native 展開。 • イベントを Cisco Cloud に渡すための 1 つ以上の SEC の展開。 • ネットワークトラフィックのフローデータをクラウドに渡すための少なくとも 1 つの Cisco Secure Cloud Analytics センサーバージョン 4.1 以降の展開、または、ネットワークトラフィックのフローデータを Cisco Secure Cloud Analytics に渡すためのクラウドベースと統合された Cisco Secure Cloud Analytics の展開。 • 新たにプロビジョニングされたか、または既存の Cisco Secure Cloud Analytics ポータル。

データプラン

導入準備された Cisco Secure Firewall Cloud Native から Cisco Cloud が毎日受け取るイベント数を反映したデータプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。Logging Volume Estimator ツールを使用して、日次取り込み率を推定でき、率が変化すると、データプランを更新できます。

データプランは、1 GB の日次ボリューム単位で、1 年、3 年、または 5 年の期間で利用できます。データプランの詳細については、Secure Logging Analytics（SaaS）発注ガイド [英語] を参照してください。

（注） Security Analytics and Logging ライセンスとデータプランがある場合、その後は別のライセンスを取得するだけで済み、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで済み、別の Security Analytics and Logging ライセンスを取得する必要はありません。

30 日間の無料トライアル

CDO にログインし、**[モニタリング（Monitoring）]** > **[イベントロギング]** タブに移動して、30 日間のリスクフリーのトライアルをリクエストできます。30 日間のトライアルが終了したら、Secure Logging Analytics（SaaS）発注ガイド [英語] の手順に従って、Cisco Commerce Workspace（CCW）からサービスを継続するために必要なイベントデータボリュームを注文できます。

次のステップ

に進みます。 Secure Firewall Cloud Native のセキュアロギング分析（SaaS）の導入 （43 ページ）

Secure Firewall Cloud Native のセキュアロギング分析（SaaS）の導入

はじめる前に

- 「Cisco Secure Firewall Cloud Native 向け Secure Logging and Analytics（SaaS） （38 ページ）」を参照して、次の点を確認してください。
  - Cisco Cloud へのイベントの送信方法
  - ソリューションに含まれるアプリケーション
  - 必要なライセンス
  - 必要なデータプラン
- すでにマネージドサービスプロバイダーまたは CDO セールス担当者に問い合わせて CDO テナントを作成しました。

- を確認してください。SDC を使用して CDO を Secure Firewall Cloud Native に接続することは「ベストプラクティス」と考えられますが、必須ではありません。

  Secure Device Connector（SDC）を確認してください。SDC を使用して CDO を Secure Firewall Cloud Native に接続することは「ベストプラクティス」と考えられますが、必須ではありません。
- ネットワークで SDC を展開する場合、次のいずれかの方法を使用してインストールできます。
  - 「CDO の VM イメージを使用した Secure Device Connector の展開」を参照し、CDO で準備した VM イメージを使用して SDC をインストールします。これが推奨される最も簡単な SDC の展開方法です。
  - 自身の VM 上での Secure Device Connector の展開 を使用します。
- Secure Event Connector をインストールする、任意の Secure Firewall Cloud Native から、テナントに導入準備された任意の SEC にイベントを送信できます。
- アカウントのユーザー向けに二要素認証を設定しました。

Cisco Security Analytics and Logging（SaaS）の展開と Secure Event Connector を介した Cisco Cloud へのイベント送信のワークフロー

1. 上の「はじめる前に」を参照し、環境が適切に構成されていることを確認してください。
2. クラスタエンドポイント、名前空間、およびトークンを使用して、Secure Firewall Cloud Native デバイスを導入準備します。
3. Secure Firewall Cloud Native Syslog イベントの Cisco Cloud への送信 （46 ページ）。
4. Cisco Secure Firewall Cloud Native デバイス向け NSEL の設定 （49 ページ）。
5. CDOにイベントが表示されていることを確認します。ナビゲーションバーから、[モニターリング（Monitoring）] > [イベントロギング（Event Logging）] を選択します。ライブイベントを表示するには、[ライブ] タブをクリックします。
6. [Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、次のセクション「**Cisco Secure Cloud Analytics を使用したイベントの分析**」に進みます。

Cisco Secure Cloud Analytics を使用したイベントの分析

[Firewall Analytics and Monitoring] ライセンスや [Total Network Analytics and Monitoring] ライセンスがある場合は、先行するステップに加えて、次の手順を実行します。

1. Cisco Secure Cloud Analytics ポータルのプロビジョニング （80 ページ）。
2. [Total Network Analytics and Monitoring] ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開します。「総合的なネットワーク分析

およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （82 ページ）」を参照してください。

3. Cisco Single Sign-On ログイン情報に関連付ける Secure Cloud Analytics ユーザーアカウントを作成するようにユーザーに勧めます。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）」を参照してください。

4. CDO から Secure Cloud Analytics をクロス起動し、FTD イベントから生成される Secure Cloud Analytics アラートをモニタします。「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）」を参照してください。

CDO からのクロス起動による Cisco Secure Cloud Analytics アラートの確認

Firewall Analytics and Monitoring ライセンスまたは **Total Network Analytics and Monitoring** ライセンスにより、CDO から Secure Cloud Analytics をクロス起動して、FTD イベントから生成されるアラートをモニタできます。

詳細については、次の項目を参照してください。

- CDO へのサインイン
- Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）
- Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング
- ファイアウォールイベントに基づくアラートの使用

Secure Event Connector に関する問題のトラブルシューティング

ステータス情報とロギング情報の収集については、次のトラブルシューティングトピックを使用してください。

- Secure Event Connector 導入準備のトラブルシューティング
- イベントロギングのトラブルシューティング ログ ファイル
- Secure Event Connector の状態を把握するためのヘルスチェックの使用

ワークフロー

「Security and Analytics Logging イベントを使用したトラブルシューティング」では、Cisco Security Analytics and Logging から生成されたイベントを使用して、ユーザーがネットワークリソースにアクセスできなかった原因を特定する方法について説明しています。

「ファイアウォールイベントに基づくアラートの使用」も参照してください。

Secure Firewall Cloud Native Syslog イベントの Cisco Cloud への送信

この手順では、Secure Firewall Cloud Native の syslog イベントを Secure Event Connector（SEC）に転送してから、ロギングを有効にする方法について説明します。以下の手順では、ワークフローの完了に必要な事柄のみを説明します。

（注） コマンドは、ファイアウォールの構成ファイルに入力する必要があります。

始める前に

注目 この手順は、デバイスの構成ファイルのシンタックスに精通している上級ユーザーを対象としています。この手法では、Defense Orchestrator に保存されている構成ファイルのコピーに直接変更を加えます。そのため、変更を加える前に、既存のデバイス設定をバックアップすることをお勧めします。必要に応じて、バックアップ設定を復元できます。

1. ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
2. [デバイス] タブをクリックします。
3. 適切なデバイスタイプタブをクリックし、設定を変更する Secure Firewall Cloud Native デバイスを選択します。
4. 右側の [管理（Management] ペインで、[設定（Configuration）] をクリックします。
5. [ダウンロード（Download）] をクリックします。

ステップ 1 [デバイスの設定（Device Configuration）] タブで、[編集] をクリックします。

ステップ 2 構成ファイルで、「snmp-server-config」に先立つ任意の場所に新しいCRDエントリを作成し、以下で説明するコマンドを入力します。

コマンド

```
########## CRD ### name: entry-name, order: order-number, generation: 1 ##########
           logging enable
           logging timestamp
           logging trap {severity_level | message_list}
           logging list name {level level [class message_class] | message start_id[-end_id]}
           logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]
           logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]
           logging permit-hostdown
```

例

```
########## CRD ### name: syslog-events, order: 4, generation: 3 ##########
           logging enable
           logging timestamp
           logging list sfcn_syslogs_to_cloud level critical
           logging list sfcn_syslogs_to_cloud level warnings class ha
```

```
logging list sfcn_syslogs_to_cloud message 302013-302018
logging trap sfcn_syslogs_to_cloud
logging host outside 192.168.1.5 17/10125
logging host outside 192.168.1.5 6/10025
logging permit-hostdown
```

- **entry-name**：CRD エントリの名前を指定します。名前に下線「_」を使用しないでください。
- **order-number**：コマンドを任意の順に実行する順序を指定します。構成ファイルで使用されている最大の番号の前にある一意の番号である必要があります。
- **logging enable**：個々のルールではなく、デバイス全体に対してロギングが有効になります。注：現時点では、CDO はセキュアロギングの有効化をサポートしていません。
- **logging timestamp**：logging timestamp コマンドを使用して、syslog メッセージがファイアウォールで発信された日付と時刻をメッセージに追加します。タイムスタンプの値は、SyslogTimestamp フィールドに表示されます。
- **logging trap** {severity_level | message_list}：

  次のコマンドを使用して、syslog サーバーに送信する syslog メッセージを指定します。

  例：

  ```
  logging trap 3
            logging trap sfcn_syslogs_to_cloud
  ```

  重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、SFCN は、重大度が 3、2、および 1 の syslog メッセージを送信します。

  message_list 引数は、カスタムイベントリストを作成した場合、そのリストの名前に置き換えられます。カスタムイベントリストの指定に必要な操作は、そのリストにある syslog メッセージを Secure Event Connector に送信することだけです。上記の例では、sfcn_syslogs_to_cloud がイベントリストの名前です。

  message_list を使用すると、Cisco Cloud に送信する syslog メッセージを明確に指定できるため、費用を節約できます。

- **logging list** *name* {**level** *level* [class message_class] | **message** start_id[-end_id]}

  このコマンドシンタックスを使用して、ファイアウォールに **logging list** コマンドを発行します。

  name 引数には、リストの名前を指定します。level level キーワードと引数のペアは、重大度を指定します。キーワードと引数のペア **class** *message_class* により、特定のメッセージクラスが指定されます。キーワードと引数のペア **message** start_id [-end_id] により、個々の syslog メッセージ番号または番号の範囲が指定されます。

  他の基準に基づいて syslog メッセージをイベントリストに追加します。

  前回の手順で使用したものと同じコマンドを入力し、既存のメッセージリストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

  - ID が 302013 ～ 302018 の範囲の syslog メッセージ。
  - 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。

- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての HA クラス syslog メッセージ。

（注） syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

- **logging host** interface_name SEC_IP_address [[tcp/port] | [udp/port]]
- **logging host** interface_name SEC_IP_address [[tcp/port] | [udp/port]]

TCP または UDP を使用して、SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように Secure Firewall Cloud Native を設定します。SEC は、IPv4 アドレスまたは IPv6 アドレスを使用できます。TCP ポートと UDP ポートのいずれかにイベントを送信します。どのポートを使用するかを判断するには、「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]

logging host コマンドシンタックスの例を次に示します。

```
logging host outside 192.168.1.5 tcp/10125
          logging host outside 192.168.1.5 udp/10025
          logging host outside 2002::1:1 tcp/10125
          logging host outside 2002::1:1 udp/10025
```

interface_name 引数は、syslog サーバーへのメッセージの送信元である Secure Firewall Cloud Native インターフェイスを指定します。SDC との通信に使用されるのと同じ Secure Firewall Cloud Native インターフェイスから、SEC に syslog メッセージを送信するのが「ベストプラクティス」です。

SEC_IP_address 引数には、SEC がインストールされている VM の IP アドレスが含まれている必要があります。

キーワードと引数のペア **tcp/port** または **udp/port** は、TCP プロトコルと関連するポート、または UDP プロトコルと関連するポートのいずれかを使用して、syslog メッセージが送信されるように設定します。UDP または TCP のいずれかを使用して syslog サーバーにデータを送信するように Secure Firewall Cloud Native を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

TCP を指定すると、Secure Firewall Cloud Native は syslog サーバーの障害を検出し、セキュリティ保護として、Secure Firewall Cloud Native 経由の新しい接続をブロックします。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、手順 b を参照してください。UDP を指定すると、syslog サーバーが動作しているかどうかにかかわらず、Secure Firewall Cloud Native は引き続き新しい接続を許可します。

（注） Secure Firewall Cloud Native メッセージを 2 台の別個の syslog サーバーに送信する場合は、もう一方の syslog サーバーの適切なインターフェイス、IP アドレス、プロトコル、およびポートを使用して、2 番目の logging host コマンドを実行できます。

- **logging permit-hostdown**

  （オプション）TCP 経由で SEC にイベントを送信し、SEC がダウンしているものの、Secure Firewall Cloud Native のログキューがいっぱいである場合、新しい接続はブロックされます。新しい接続は、syslog サーバーがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。

TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、このコマンドを使用して、TCP 接続された syslog サーバーがダウンしたときに新しい接続をブロックする機能を無効にします。

ステップ 3 [保存（**Save**）] をクリックします。

ステップ 4 設定の変更をファイアウォールに展開します。

Cisco Secure Firewall Cloud Native デバイス向け NetFlow セキュアイベントロギング（NSEL）

Secure Firewall Cloud Native からの基本的な Syslog メッセージには、 Secure Firewall Cloud Native によって報告されたイベントが脅威を示しているかどうかを Cloud Cisco Secure Cloud Analytics が判断するために必要な多くのデータが不足しています。Netflow Secure Event Logging（NSEL）は、そのデータを Secure Cloud Analytics に提供します。

「フローは、ネットワークデバイスを通過する、いくつかの共通プロパティを持つ一方向のパケットシーケンスとして定義されます。これらの収集されたフローは、外部デバイスである NetFlow コレクタにエクスポートされます。ネットワークフローは非常に細分化されています。たとえば、フローレコードには IP アドレス、パケット数とバイト数、タイムスタンプ、タイプオブサービス（ToS）、アプリケーションポート、入出力インターフェイスなどの詳細が含まれます。」1

Secure Firewall Cloud Native では、NetFlow バージョン 9 サービスがサポートされています。Secure Firewall Cloud Native の NSEL を実装することで、フロー内の重要なイベントを示すレコードだけをエクスポートする、ステートフルな IP フローのトラッキング方式が可能となります。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。

このドキュメントでは、 構成ファイル内の一連のコマンドを使用して、Secure Firewall Cloud Native デバイスに NetFlow を設定する簡単な方法について説明します。『Cisco NetFlow Implementation Guide』には、Secure Firewall Cloud Native に NetFlow を設定することに関する非常に詳細な説明が記載されており、このコンテンツに付随する貴重なリソースとなっています。

Cisco Secure Firewall Cloud Native デバイス向け NSEL の設定

Secure Firewall Cloud Native デバイスは、NetFlow Secure Event Logging（NSEL）を使用して詳細な接続イベントデータをレポートします。この接続イベントデータ（双方向フロー統計を含む）に Cisco Secure Cloud Analytics を適用できます。この手順では、Secure Firewall Cloud Native デバイスで NSEL を設定し、それらの NSEL イベントをフローコレクタに送信する方法について説明します。このケースでは、フローコレクタは Secure Event Connector（SEC）です。

この手順では、ファイアウォールの構成ファイルに入力する一連のコマンドに言及します。

ステップ 1 [デバイスの設定（Device Configuration）] タブで、[編集（Edit）] をクリックします。

ステップ 2 構成ファイルで、「snmp-server-config」に先立つ任意の場所に新しいCRDエントリを作成し、以下で説明するコマンドを入力します。

コマンド

```
########## CRD ### name: entry-name, order: order-number, generation: 1 ##########
flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
    flow-export template timeout-rate {{timeout_rate_in_mins}}
    flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
    flow-export active refresh-interval {{refresh_interval_in_mins}}
    class-map {{flow_export_class_name}}
         match {{add_this_traffic_to_class_map}}
    policy-map {{global_policy_map_name}}
         class {{flow_export_class_name}}
              flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
    service-policy {{global_policy_map_name}} global
    logging flow-export-syslogs disable
    show run flow-export
    show run policy-map {{global_policy_map_name}}
    show run class-map {{flow_export_class_name}}
```

クラスマップの一般名、および global_policy に追加されたクラスマップなど、すべてのデフォルト値が入力された例を次に示します。

```
########## CRD ### name: nsel-config, order: 5, generation: 1 ##########
    flow-export destination outside {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
    flow-export template timeout-rate 60
    flow-export delay flow-create 55
    flow-export active refresh-interval 1
    class-map flow_export_class_map
         match any
    policy-map global_policy
         class flow_export_class_map
              flow-export event-type all destination {{SEC_IPv4_address}}
    service-policy global_policy global
    logging flow-export-syslogs disable
    show run flow-export
    show run policy-map global_policy
    show run class-map flow_export_class_map
```

ステップ 3 [保存（Save）] をクリックします。

ステップ 4

NSEL メッセージの宛先と SEC に送信される間隔の定義

NSELメッセージは、テナントに導入準備したSECのいずれかに送信できます。以下の手順では、このセクションのマクロを参照しています。

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）を参照してください。

ステップ 1 **flow-export destination** コマンドは、NetFlow パケットの送信先のコレクタを定義します。この場合、SEC に送信します。次のパラメータのフィールドに入力します。

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{SEC_IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{SEC_NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

ステップ 2 **flow-export template timeout-rate** コマンドは、テンプレートレコードがすべての設定された出力先に送信される間隔を指定します。

- **{{timeout_rate_in_mins}}**：テンプレートが再送信されるまでの分数を入力します。60 分の値を使用することをお勧めします。SEC はテンプレートを処理しません。数字を大きくすると、SEC へのトラフィックが減少します。

ステップ 3 **flow-export delay flow-create** コマンドは、flow-create イベントの送信を指定した秒数遅らせます。この値は、推奨されるアクティブタイムアウト値と一致し、ASA からエクスポートされるフローイベントの数を減らします。この場合、NSEL イベントが最初に CDO に表示されるのは、接続の終了時または接続の作成から 55 秒以内のいずれか早い方となると考えてください。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。

- **{{delay_flow_create_rate_in_secs}}**：flow-create イベントの送信間の遅延秒数を入力します。55 秒の値を使用することをお勧めします。

ステップ 4 **flow-export active refresh-interval** コマンドは、長時間フローのステータスの更新が ASA から送信される頻度を定義します。有効な値は 1 ～ 60 分です。[フロー更新間隔（Flow Update Interval）] フィールドで、**flow-export active refresh-interval** を **flow-export delay flow-create interval** よりも少なくとも 5 秒長く設定すると、flow-update イベントが flow-creation イベントの前に表示されなくなります。

- **{{refresh_interval_in_mins}}**：**値を 1 分にすることをお勧めします。**有効な値は 1 ～ 60 分です。

次のタスク

SEC に送信される NSEL イベントを定義するクラスマップの作成 （24 ページ） に進みます。

SEC に送信される NSEL イベントを定義するクラスマップの作成

マクロ内の次のコマンドは、クラス内のすべてのNSELイベントをグループ化し、そのクラスを Secure Event Connector（SEC）にエクスポートします。以下の手順では、このセクションのマクロを参照しています。

```
class-map {{flow_export_class_name}}
match {{add_this_traffic_to_class_map}}
```

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）を参照してください。

ステップ 1 **class-map** コマンドは、SEC にエクスポートされる NSEL トラフィックを識別するクラスマップに名前を付けます。

- **{{flow-export-class-name}}**：クラスマップの名前を入力します。名前の長さは最大 40 文字です。名前「class-default」と、「_internal」または「_default」で始まる名前はすべて予約されています。すべてのタイプのクラスマップで同じ名前空間が使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。

ステップ 2 クラスマップに関連付けられる（一致する）トラフィックを識別します。**{{add_this_traffic_to_class_map}}** の値として、次のいずれかのオプションを選択します。

- **{{add_this_traffic_to_class_map}}** フィールドに **any** と入力します。NSEL トラフィックのすべてのトラフィックタイプが監視されます。**値「any」を使用することをお勧めします。**
- **{{add_this_traffic_to_class_map}}** フィールドに **access-list *name-of-access-list*** と入力します。作成したアクセスリストに関連付けられたすべてのトラフィックが関連付けられます。詳細については、Cisco ASA NetFlow 実装ガイド [英語] の「Configure Flow-Export Actions Through Modular Policy Framework」を参照してください。

次のタスク

NSEL イベントのポリシーマップの定義 （25 ページ）に進みます。

NSEL イベントのポリシーマップの定義

このタスクでは、前のタスクで作成したクラスに NetFlow エクスポートアクションを割り当て、そのクラスを新しいポリシーマップに割り当てます。以下の手順では、このセクションのマクロを参照しています。

```
policy-map {{global_policy_map_name}}
class {{flow_export_class_name}}
flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
```

始める前に

この手順は、より大きなワークフローの一部です。始める前にCDO マクロを使用して ASA デバイスの NSEL を設定する （21 ページ）を参照してください。

ステップ 1 **policy-map** コマンドは、ポリシーマップを作成します。次のタスクでは、このポリシーマップをグローバルポリシーに関連付けます。

- **{{global_policy_map_name}}**：ポリシーマップの名前を入力します。ファイアウォールの既存のグローバルポリシーがある場合は、その名前を使用することをお勧めします。グローバルポリシーのデフォルト名は **global_policy** です。ASA グローバルポリシーの名前を決定する新しいポリシーマップを作成し、『Cisco ASA NetFlow 実装ガイド』の「モジュラ ポリシー フレームワークを使用した flow-export アクションの設定」に従ってグローバルに適用すると、残りの検査ポリシーは非アクティブ化されます。

ステップ 2 **class** コマンドでは、SEC に送信される NSEL イベントを定義するクラスマップの作成 （24 ページ）で作成したクラスマップの名前が継承されます。

ステップ 3 **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} コマンドは、フローコレクタ（この場合は SEC）に送信する必要があるイベントタイプを定義します。

- **{{event-type}}**：event_type キーワードは、フィルタリングされるサポートされているイベントの名前です。値「all」を使用することをお勧めします。
- **{{SEC_IPv4_address}}**：これは SEC の IPv4 アドレスです。その値は、NSEL メッセージの宛先と SEC に送信される間隔の定義 （23 ページ）で入力した値から継承されます。

次のタスク

冗長な Syslog メッセージの無効化 （26 ページ） に進みます。

冗長な Syslog メッセージの無効化

以下の手順では、このセクションのマクロを参照しています。コマンドを変更する必要はありません。

logging flow-export-syslogs disable

NetFlow でフロー情報をエクスポートできるようにすると、次の表に記載されている syslog メッセージが冗長になります。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージをディセーブルにすることをお勧めします。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギングタイプ間が時系列順になる保証はありません。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
106100	アクセス制御ルール（ACL）が発生するたびに生成されます。	1：フローが作成されました（ACLがフローを許可した場合）。 3：フローが拒否されました（ACLがフローを拒否した場合）。	0：ACL がフローを許可した場合。 1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
106015	最初のパケットがSYNパケットではなかったため、TCPフローが拒否されました。	3：フローが拒否されました。	1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
106023	**access-group** コマンドによってインターフェイスに接続されたACLによってフローが拒否された場合。	3：フローが拒否されました。	1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
302013、302015、302017、302020	TCP、UDP、GRE、および ICMP 接続の作成。	1：フローが作成されました。	0：無視します。
302014、302016、302018、302021	TCP、UDP、GRE、およびICMP接続のティアダウン。	2：フローが削除されました。	0：無視します。 > 2000：フローが切断されました。
313001	デバイスへの ICMP パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
710003	デバイスインターフェイスへの接続の試行が拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

冗長なsyslogメッセージを無効にしない場合は、このマクロを編集して、次の行のみを削除できます。

logging flow-export-syslogs disable

後に NetFlow 関連の Syslog メッセージの無効化と再有効化の手順を実行することで、個別の syslog メッセージを有効化または無効化できます。

ASA グローバルポリシーの名前を決定する

ASA のグローバルポリシーの名前を決定するには、次の手順に従います。

ステップ 1 [デバイスとサービス] ページで、グローバルポリシーの名前を検索するデバイスを選択します。

ステップ 2 [デバイスアクション] ペインで、[>_コマンドリファレンス（>_Command Reference）] を選択します。

ステップ 3 コマンド ライン インターフェイス ウィンドウのプロンプトで、次のように入力します。

show running-config service-policy

以下の例の出力では、global_policy はグローバルポリシーの名前です。

例：

> **show running-config service-policy**

service-policy global_policy global

ASA イベント タイプ

イベントロギングページでのイベントの検索とフィルタリング場合、イベントタイプのリストから選択できますこれらのイベントタイプは、syslog ID のグループを表します。次の表は、どの ASA イベントタイプにどの syslog ID が含まれるかを示しています。特定の syslog ID の詳細については、『Cisco ASA シリーズ Syslog メッセージガイド』で検索できます。

一部の syslog イベントには、追加の属性「EventName」があります。属性:値のペアでフィルタ処理することにより、EventName 属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。「Syslog イベントの EventName 属性」を参照してください。

ASA デバイス向け NetFlow Secure Event Logging（NSEL） は、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの NetFlow イベント ID は、『Cisco ASA NetFlow 実装ガイド』で定義されています。

フィルタ名（**Filter Name**）	対応する **Syslog** イベントまたは **NetFlow** イベント
AAA	109001-109035 113001-113027
BotNet	338001-338310

フィルタ名（**Filter Name**）	対応する **Syslog** イベントまたは **NetFlow** イベント
フェールオーバー	101001-101005、102001、103001-103007、104001-104004、105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	106001、106007、106012、106013、106015、106016、106017、106020、106021、106022、106023、106025、106027 Firewall Denied イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。
Firewall Traffic	106001-106100、108001-108007、110002-110003 201002-201013、209003-209005、215001 302002-302304、302022-302027、303002-303005、313001-313008、317001-317006、324000-324301、337001-337009 400001-400050、401001-401005、406001-406003、407001-407003、408001-408003、415001-415020、416001、418001-418002、419001-419003、424001-424002、431001-431002、450001 500001-500005、508001-508002 607001-607003、608001-608005、609001-609002、616001 703001-703003、726001 Firewall Traffic イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。
IPSec VPN	402001-402148、602102-602305、702304-702307
NAT	201002-201013、202001-202011、305005-305012
SSL VPN	716001-716060、722001-722053、723001-723014、724001-724004、725001-725015

フィルタ名（Filter Name）	対応する Syslog イベントまたは NetFlow イベント
NetFlow	0、1、2、3、5

関連情報：

- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性 （105 ページ）
- Syslog イベントの EventName 属性

解析済みの ASA Syslog イベント

解析済みの syslog イベントは、他の syslog イベントよりも多くのイベント属性を含んでおり、特定の解析済みフィールドの検索を可能にします。SEC は、指定したすべての ASA イベントを Cisco Cloud に転送しますが、解析されるのは以下の表の syslog メッセージのみです。すべての解析済みの Syslog イベントは、識別しやすいように EventType が斜体で表示されます。

syslog ID	syslog カテゴリ	syslog メッセージの目的
106015	ファイアウォール	州外 TCP の拒否を表します。
106023	ファイアウォール	実際の IP パケットが ACL によって拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。
106100	アクセスリスト/ユーザーセッション	パケットは ACL によって許可または拒否されました。
113019	ユーザー認証（User Authentication）	クリティカルな AnyConnect
302013、302015、302017、302020	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302014, 302016, 302018, 302021	ユーザ セッション	TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。
302020 ～ 302021	ユーザ セッション	ICMP セッションの確立と解除。
305006	ユーザーセッション/NAT および PAT	NAT 接続の失敗

syslog ID	syslog カテゴリ	syslog メッセージの目的
305011 ～ 305014	ユーザーセッション/NAT および PAT	NAT 確立/解除関連
313001、313008	IP スタック	ボックスへの接続が拒否されたことを表します。
414004	システム（System）	クリティカルな AnyConnect
609001 ～ 609002	ファイアウォール	ネットワーク状態コンテナは、ゾーンに接続されたホスト **ip-address** 用に予約済み/削除済みでした。
710002、710004、710005	ユーザ セッション	ボックスへの接続の失敗
710003	ユーザ セッション	ボックスへの接続が拒否されたことを表します。
746012、746013	ユーザ セッション	クリティカルな AnyConnect

syslog の詳細な説明については、『Cisco ASA Series Syslog Messages』を参照してください。

関連情報：

- コマンドライン インターフェイスを使用した Cisco Cloud への ASA syslog イベントの送信
- イベントロギングページでのイベントの検索とフィルタリング

SecureLoggingAnalytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索

Secure Logging Analytics（SaaS）を使用すると、ご使用の ASA デバイスまたは FTD デバイスから、Secure Event Connector（SEC）上の特定の UDP、TCP、または NSEL ポートにイベントを送信できます。その後、SEC はそれらのイベントを Cisco Cloud に転送します。

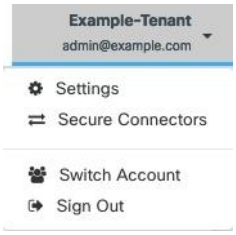
まだ使用されていないポートの場合、SEC はそれらのポートを使用してイベントを受信できるようにします。Secure Logging Analytics（SaaS）のマニュアルでは、機能を設定するときにポートを使用することが推奨されています。

- TCP：10125
- UDP：10025
- NSEL：10425

すでに使用されているポートの場合は、Secure Logging Analytics（SaaS）を設定する前に、SEC デバイスの詳細を調べて、イベントの受信に実際に使用しているポートを特定します。

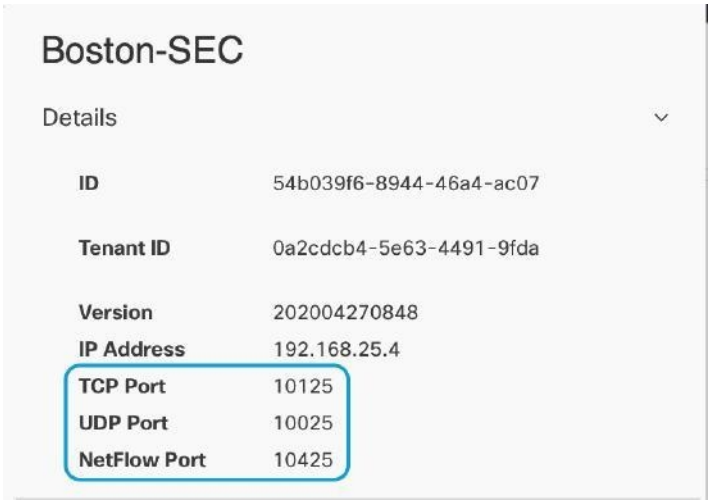
SEC が使用するポート番号を見つけるには、次の手順を実行します。

ステップ 1 CDO の任意のページで [アカウント（Account）] メニューを開き、[セキュアコネクタ（Secure Connectors）] を選択します。



ステップ 2 [セキュアコネクタ（Secure Connectors）] ページで、イベントを送信する SEC を選択します。

ステップ 3 [詳細] ペインに、イベントの送信先となる TCP、UDP、および NetFlow（NSEL）ポートが表示されます。



Secure Event Connector

Secure Event Connector（SEC）は、Security Analytics and Logging SaaS ソリューションのコンポーネントです。ASA や FTD デバイスからイベントを受信し、Cisco Cloud に転送します。イベントは CDO の [イベントロギング] ページに表示されます。管理者はこのページまたは Cisco Secure Cloud を使用してイベントを分析できます。

SEC は、ネットワークに展開された Secure Device Connector、またはネットワークに展開された独自の CDO コネクタ仮想マシンにインストールします。

Secure Event Connector ID

Cisco Technical Assistance Center（TAC）などの CDO サポートと連携する場合、SEC の ID が必要になる場合があります。この ID は、CDO の [セキュアコネクタ（Secure Connectors）] ページで確認できます。SEC ID を確認するには、次の手順を実行します。

1. ユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。
2. 確認する SEC をクリックします。
3. SEC ID は、[詳細] ペインの [テナントID（ Tenant ID）] の上に表示されている ID です。

関連情報：

- ASA の Security Analytics and Logging（SAL SaaS）について
- SDC 仮想マシンへの Secure Event Connector のインストール （60 ページ）
- VM イメージを使用した SEC のインストール
- VM イメージを使用した SEC のインストール
- Secure Event Connector の削除
- Cisco Security Analytics and Logging（SaaS）をプロビジョニング解除する

Secure Event Connector をインストールする

Secure Event Connector（SEC）は、SDC の有無にかかわらず、テナントにインストールできます。

SEC は Secure Device Connector（あれば）と同じ仮想マシンにインストールすることも、ネットワーク内で維持管理している独自の CDO コネクタ仮想マシンにインストールすることもできます。

各インストールケースについて説明している次のトピックを参照してください。

- VM イメージを使用した SEC のインストール （70 ページ）
- CDO イメージを使用して SEC をインストールする （64 ページ）

SDC 仮想マシンへの Secure Event Connector のインストール

Secure Event Connector（SEC）は、ASA および FTD デバイスからイベントを受信し、それらをシスコクラウドに転送します。CDO は [イベントロギング] ページにイベントを表示し、管理者はそこで、または Cisco Secure Cloud Analytics を使用してイベントを分析できます。

SEC は Secure Device Connector（あれば）と同じ仮想マシンにインストールすることも、ネットワーク内で維持管理している独自の CDO コネクタ仮想マシンにインストールすることもできます。

この記事では、SDC と同じ仮想マシンに SEC をインストールする方法について説明します。他にも SEC をインストールする場合は、CDO イメージを使用して SEC をインストールする（64 ページ） または VM イメージを使用した SEC のインストール （70 ページ） を参照してください。

始める前に

- Cisco Security and Analytics Logging の **Logging and Troubleshooting** ライセンスを購入します。または、Cisco Security and Analytics を最初に試す場合は、CDO にログインし、メインナビゲーションバーで [モニタリング（Monitoring）] > [イベントロギング] を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。また、**Logging Analytics and Detection** および **Total Network Analytics and Monitoring** ライセンスを購入して、Secure Cloud Analytics をイベントに適用することもできます。
- SDC がインストールされていることを確認します。SDC をインストールする必要がある場合は、次のいずれかの手順に従います。
  - CDO の VM イメージを使用して Secure Device Connector を展開する
  - 独自の VM を使用して Secure Device Connector を展開する

（注） オンプレミスの SDC を独自の VM にインストールした場合は、イベントが到達できるようにするために作成した VM にインストールされた SDC および CDO コネクタの追加設定が必要です。

- SDC が CDO と通信していることを確認します。
  1. CDO で開いている任意のページから、ページの右上隅にあるユーザー名の下にあるメニューをクリックして、Secure Connectors のページを開きます。
  2. SEC をインストールする前に、SDC の最後のハートビートが 10 分以内であったこと、および SDC のステータスがアクティブであることを確認してください。
- システム要件：SDC を実行している仮想マシンに追加の CPU とメモリを割り当てます。
  - CPU：SEC 用に**追加**の 4 つの CPU を割り当て、CPU の合計が 6 つとなるようにします。
  - メモリ：SEC 用に**追加**の 8 GB のメモリを割り当てて、メモリの合計が 10 GB となるようにします。

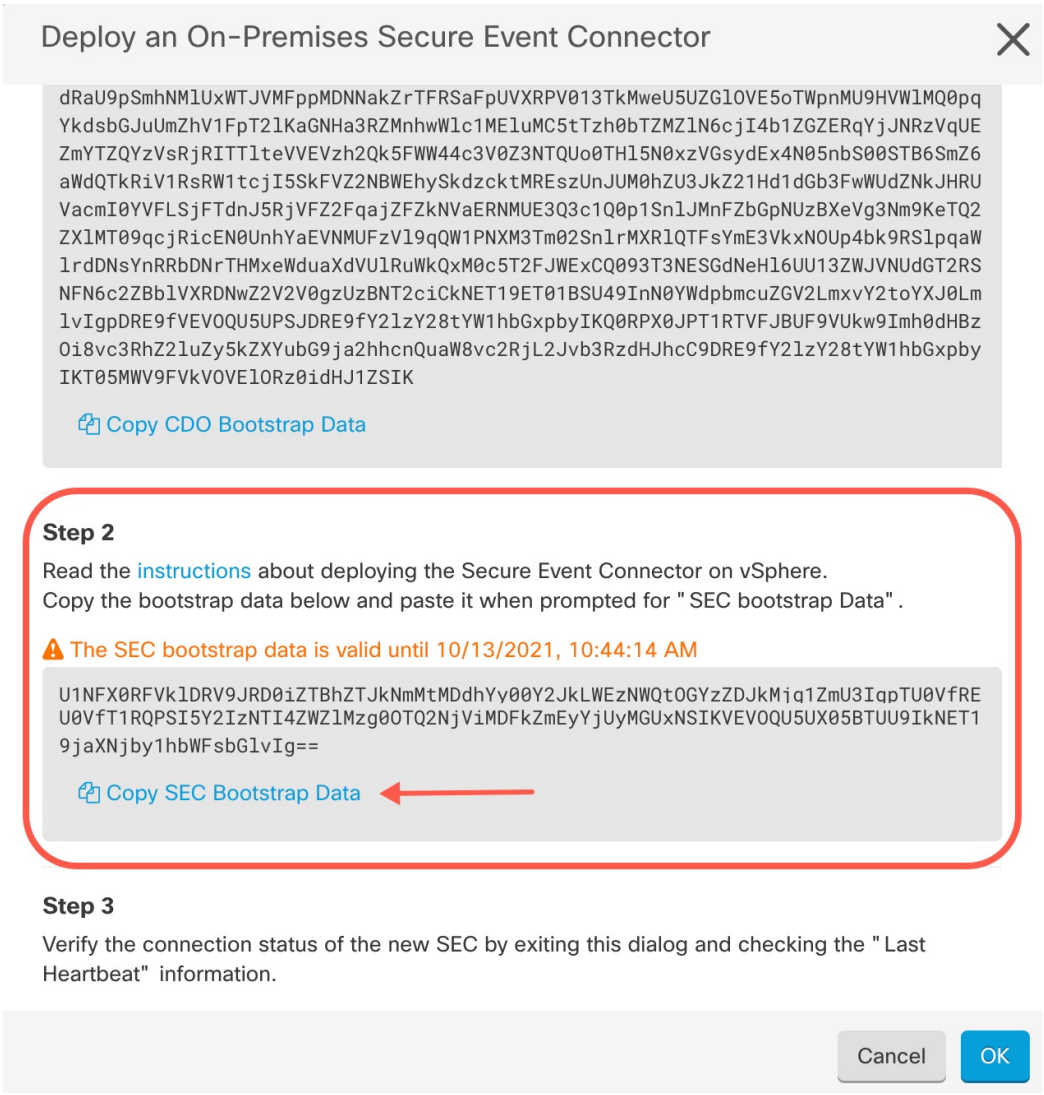
    SEC に対応するように VM の CPU とメモリを更新したら、VM の電源を入れ、[セキュアコネクタ（Secure Connectors）] ページに SDC が「アクティブ」状態であることが示されていることを確認します。

ステップ 1 CDO にログインします。

ステップ 2 [ユーザー（user）]メニューをクリックし、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 3 青色のプラスボタンをクリックし、[Secure Event Connector] をクリックします。

ステップ 4 ウィザードのステップ 1 をスキップして、ステップ 2 に進みます。ウィザードのステップ 2で、 [SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。



ステップ 5 ターミナルウィンドウを開き、SDC に「cdo」ユーザーとしてログインします。

ステップ 6 ログインしたら、「sdc」ユーザーに切り替えます。パスワードの入力を求められたら、「cdo」ユーザーのパスワードを入力します。これらのコマンドの例を次に示します。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

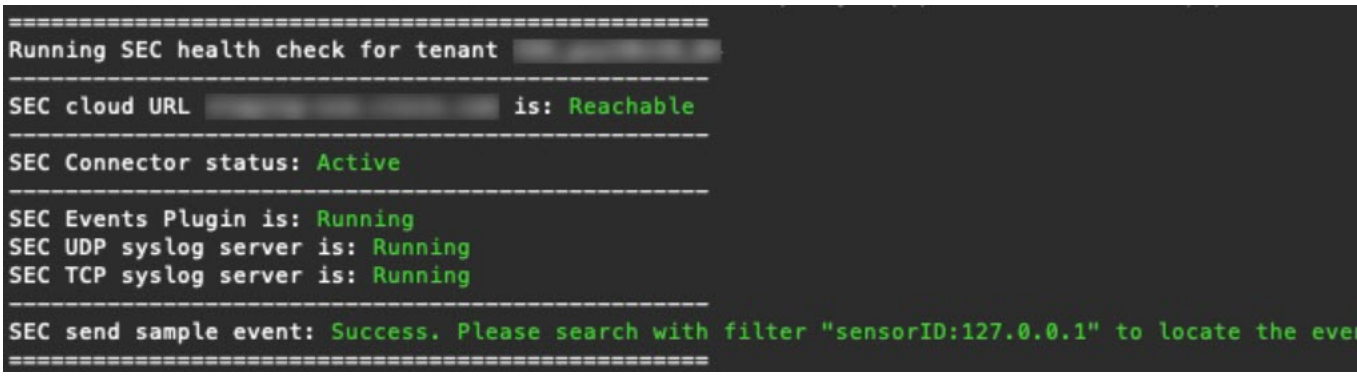
ステップ 7 プロンプトで、**sec.sh setup** スクリプトを実行します。

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

ステップ 8 プロンプトの最後に、手順4でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。



登録に失敗したことや SEC の導入準備に失敗したことを示すメッセージを受け取った場合は、「Secure Event Connector 導入準備のトラブルシューティング」を参照してください。

ステップ 9 SDC と SEC が実行されている VM に追加の構成が必要かどうかを判断します。

- SDC を独自の仮想マシンにインストールした場合は、作成した VM にインストールされた SDC および CDO コネクタの追加設定 （75 ページ） を続行します。
- CDO イメージを使用して SDC をインストールした場合は、「次に行う作業」に進みます。

次のタスク

ASA デバイスに安全なロギング分析（SaaS）を導入する （7 ページ） に戻ります。

関連情報：

- Secure Device Connector のトラブルシュート
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング
- Secure Event Connector の登録失敗のトラブルシューティング

CDO イメージを使用して SEC をインストールする

Secure Event Connector（SEC）は、ASA と FTD からのイベントを Cisco Cloud に転送するため、ライセンスに応じて、[イベントロギング] ページでイベントを表示し、Stealthwatch Cloud で調査できます。

テナントに複数の Secure Event Connector（SEC）をインストールし、インストールした任意の SEC に ASA および FTD からイベントを送信できます。複数の SEC を使用すると、さまざまな場所に SEC をインストールし、Cisco Cloud にイベントを送信する作業を分散できます。

SEC のインストールは、2 つの部分からなるプロセスです。

1. CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール （64 ページ） インストールする SEC ごとに 1 つの CDO コネクタが必要です。CDO コネクタは、Secure Device Connector（SDC）とは異なります。
2. CDO コネクタ仮想マシンへの Secure Event Connector のインストール （76 ページ）。

（注） 独自の VM を作成して CDO コネクタを作成する場合は、「作成した VM にインストールされた SDC および CDO コネクタの追加設定」を参照してください。

次に行う作業：

CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール （64 ページ） に進みます。

CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール

始める前に

- Cisco Security and Analytics Logging と **Logging and Troubleshooting** ライセンスに加えて、**Logging Analytics and Detection** と **Total Network Analytics and Monitoring** ライセンスを購入すると、イベントに Stealthwatch Cloud 分析を適用できます。

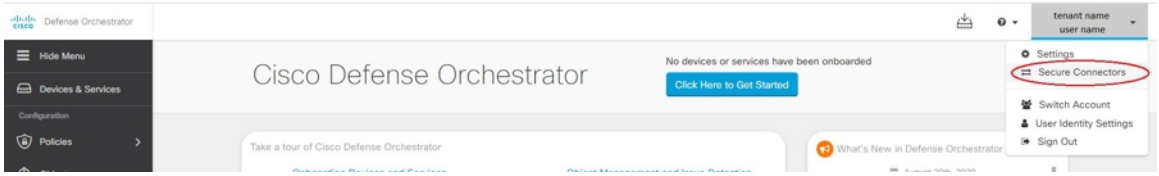
  Security Analytics and Logging のトライアル版をリクエストする場合は、CDO にログインし、メインナビゲーションバーで **[モニタリング（Monitoring）][イベントロギング]** を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。

- CDO は、厳密な証明書チェックを必要とし、CDO コネクタとインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、CDO コネクタと CDO の間のトラフィックの検査を無効にします。
- **このプロセスでインストールされる CDO コネクタには TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。**
- **CDO コネクタで適切なネットワークアクセスを確保するには、「**Secure Device Connector を使用した Cisco Defense Orchestrator への接続**」を参照してください。**

- CDO は、vSphere Web クライアントまたは ESXi Web クライアントを使用した CDO コネクタ VM OVF イメージのインストールをサポートしています。
- CDO は、VM vSphere デスクトップクライアントを使用した CDO コネクタ VM OVF イメージのインストールをサポートしていません。
- ESXi 5.1 ハイパーバイザ。
- CDO コネクタと SEC のみをホストすることを目的した VM のシステム要件は以下のとおりです。
  - VMware ESXi ホストには 4 つの vCPU が必要です。
  - VMware ESXi ホストには 8 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 64GB のディスク容量が必要です。
- インストールを開始する前に、次の情報を収集します。
  - CDO コネクタ VM に使用する静的 IP アドレス。
  - インストールプロセス中に作成する **root** ユーザーと **cdo** ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- CDO Connector 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。

ステップ 1 CDO コネクタを作成する CDO テナントにログオンします。

ステップ 2 [アカウント（Account）] メニューをクリックし、[セキュアコネクタ（Secure Connectors）] を選択します。



ステップ 3 青色のプラスボタンをクリックし、[Secure Event Connector] をクリックします。

ステップ 4 手順 1 で [CDOコネクタVMイメージのダウンロード（Download the CDO Connector VM image）] をクリックします。これは、SEC をインストールする特別なイメージです。最新のイメージを確実に使用するために、常に CDO コネクタ VM をダウンロードしてください。

ステップ 5 .zip ファイルからすべてのファイルを抽出します。これらは、次のようなものです。

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

ステップ 6 vSphere Web クライアントを使用して、管理者として VMware サーバーにログオンします。

（注） VM vSphere デスクトップクライアントは使用しないでください。

ステップ 7 プロンプトに従って、OVF テンプレートからオンプレミスの CDO コネクタ仮想マシンを展開します（テンプレートを展開するには、.ovf、.mf、および .vdk ファイルが必要です）。

ステップ 8 セットアップが完了したら、VM の電源を入れます。

ステップ 9 新しい CDO コネクタ VM のコンソールを開きます。

ステップ 10 **cdo** ユーザーとしてログインします。デフォルトのパスワードは `adm123` です。

ステップ 11 プロンプトで、`sudo sdc-onboard setup` と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

ステップ 12 プロンプトで、cdo ユーザーのデフォルトのパスワード（`adm123`）を入力します。

ステップ 13 プロンプトに従って、**root** ユーザーの新しいパスワードを作成します。

ステップ 14 プロンプトに従って、**cdo** ユーザーの新しいパスワードを作成します。

ステップ 15 プロンプトに従って、Cisco Defense Orchestrator ドメイン情報を入力します。

ステップ 16 CDO コネクタ VM に使用する静的 IP アドレスを入力します。

ステップ 17 CDO コネクタ VM がインストールされているネットワークのゲートウェイ IP アドレスを入力します。

ステップ 18 CDO コネクタの NTP サーバーのアドレスまたは FQDN を入力します。

ステップ 19 プロンプトで、Docker ブリッジの情報を入力するか、該当しない場合は空白のままにして、Enter キーを押します。

ステップ 20 入力内容を確定します。

ステップ 21 「Would you like to setup the SDC now?」というプロンプトで、**n** を入力します。

ステップ 22 **cdo** ユーザーとしてログインして、CDO コネクタへの SSH 接続を作成します。

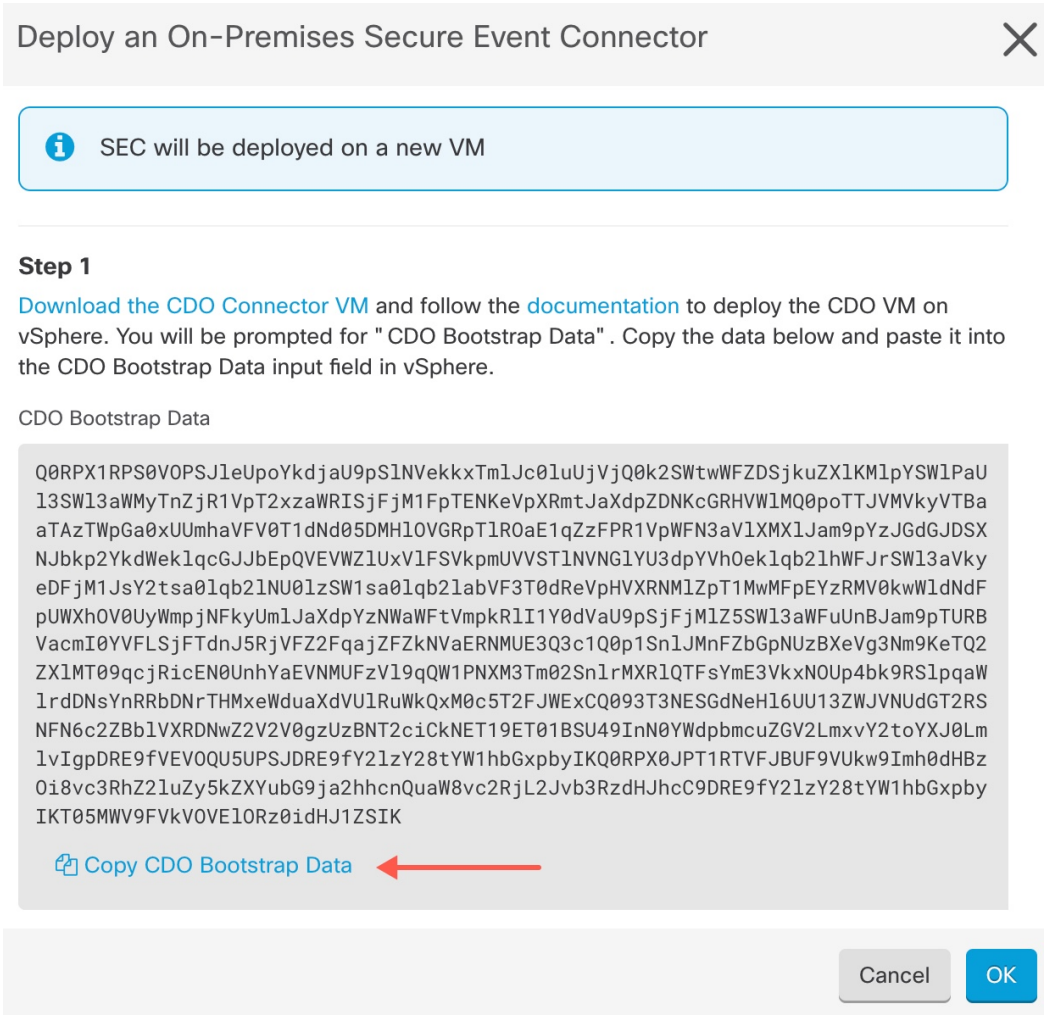
ステップ 23 プロンプトで、**`sudo sdc-onboard bootstrap`** と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

ステップ 24 プロンプトで、cdo ユーザーのパスワードを入力します。

ステップ 25 プロンプトで、CDO に戻り、CDO ブートストラップデータをコピーして、SSH セッションに貼り付けます。CDO ブートストラップデータをコピーするには、次の手順を実行します。

1. CDO にログインします。
2. ユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。
3. 導入準備を開始した Secure Event Connector を選択します。ステータスが「Onboarding」と表示されます。
4. [アクション] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。
5. ダイアログボックスのステップ 1 で、CDO ブートストラップデータをコピーします。



ステップ 26 「Would you like to update these settings?」というプロンプトで、**n** を入力します。

ステップ 27 CDO の [オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] ダイアログに戻り、[OK] をクリックします。[セキュアコネクタ（Secure Connectors）] ページで、Secure Event Connector が黄色の導入準備状態であることを確認できます。

次のタスク

CDO コネクタ VM への Secure Event Connector のインストール （68 ページ） に進みます。

CDO コネクタ VM への Secure Event Connector のインストール

始める前に

CDO VM イメージを使用して Secure Event Connector をサポートするための CDO コネクタのインストール （64 ページ） に記載があるように、CDO コネクタ VM がインストールされている必要があります。

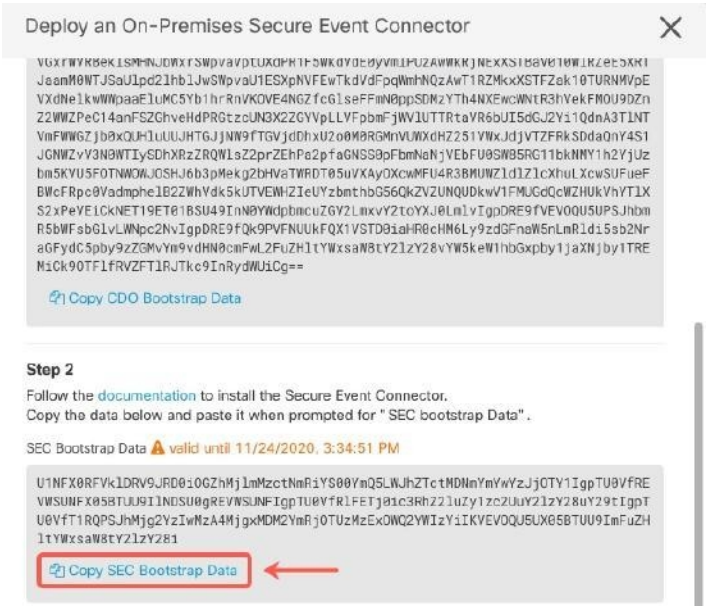
ステップ 1 CDO にログインします。

ステップ 2 [ユーザー（user）] メニューをクリックし、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 3 上記で導入準備した CDO コネクタを選択します。セキュアコネクタテーブルでは、これはセキュアイベントコネクタと呼ばれ、「導入準備」ステータスのままである必要があります。

ステップ 4 右側の [アクション] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

ステップ 5 ウィザードの**ステップ 2**で、 [SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。



ステップ 6 CDO コネクタへの SSH 接続を作成し、**cdo** ユーザーとしてログインします。

ステップ 7 ログインしたら、**sdc** ユーザーに切り替えます。パスワードの入力を求められたら、「cdo」ユーザーのパスワードを入力します。これらのコマンドの例を次に示します。

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

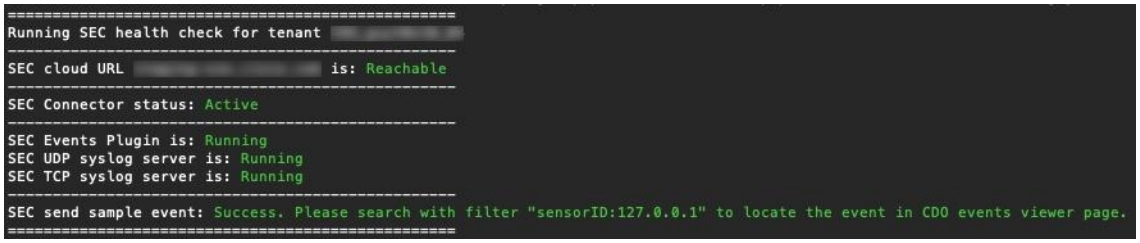
ステップ 8 プロンプトで、sec.sh セットアップスクリプトを実行します。

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

ステップ 9 プロンプトの最後に、手順 4 でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。



登録に失敗したことや SEC の導入準備に失敗したことを示すメッセージを受け取った場合は、次を参照してください： SEC オンボーディング失敗のトラブルシューティング

成功メッセージを受け取った場合は、CDO に戻り、[オンプレミス セキュア イベント コネクタの展開（Deploy an ON-Premise Secure Event Connector）] ダイアログボックスで [完了（Done）] をクリックします。

ステップ 10 「**次のステップ**」に進みます。 "

次のタスク

ASA デバイスに安全なロギング分析（SaaS）を導入する （7 ページ） に戻ります。

関連情報：

- Secure Device Connector のトラブルシュート
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング

VM イメージを使用した SEC のインストール

Secure Event Connector（SEC）は、ASA と FTD からのイベントを Cisco Cloud に転送するため、ライセンスに応じて、[イベントロギング] ページでイベントを表示し、Stealthwatch Cloud で調査できます。

テナントに複数の Secure Event Connector（SEC）をインストールし、インストールした任意の SEC に ASA および FTD からイベントを送信できます。複数の SEC を使用すると、さまざまなリージョンに SEC をインストールし、Cisco Cloud にイベントを送信する作業を分散できます。

独自の VM イメージを使用した複数の SEC のインストールは、3 つの部分からなるプロセスです。次の各手順を実行する必要があります。

1. VM イメージを使用して SEC をサポートするための CDO コネクタのインストール （70 ページ）
2. 作成した VM にインストールされた SDC および CDO コネクタの追加設定 （75 ページ）を使用して、VM の追加の設定手順をいくつか実行します。
3. CDO コネクタ仮想マシンへの Secure Event Connector のインストール

（注） CDO コネクタに CDO VM イメージを使用する方法は、CDO コネクタをインストールする最も簡単で正確な推奨される方法です。その方法を使用する場合は、CDO イメージを使用して SEC をインストールする （64 ページ）を参照してください。

次に行う作業：

VM イメージを使用して SEC をサポートするための CDO コネクタのインストール （70 ページ）に進みます。

VM イメージを使用して SEC をサポートするための CDO コネクタのインストール

CDO コネクタ VM は、SEC をインストールする仮想マシンです。CDO コネクタの唯一の目的は、Cisco Security Analytics and Logging（SaaS）のお客様向けに SEC をサポートすることです。

始める前に

- Cisco Security and Analytics Logging と **Logging and Troubleshooting** ライセンスに加えて、**Logging Analytics and Detection** と **Total Network Analytics and Monitoring** ライセンスを購入すると、イベントに Secure Cloud Analytics を適用できます。

  Security Analytics and Logging のトライアル版をリクエストする場合は、CDO にログインし、メインナビゲーションバーで **[モニタリング（Monitoring）][イベントロギング（Event Logging）]** を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。

- CDO は、厳密な証明書チェックを必要とし、CDO コネクタとインターネット間の Web プロキシやコンテンツプロキシをサポートしていません。
- **CDO コネクタには TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。**
- **CDO コネクタで適切なネットワークアクセスを確保するには、「**Secure Device Connector を使用した Cisco Defense Orchestrator への接続**」を参照してください。**
- vCenter Web クライアントまたはr ESXi Web クライアントを使用してインストールされた VMware ESXi ホスト。

（注） vSphere デスクトップクライアントを使用したインストールはサポートしていません。

- ESXi 5.1 ハイパーバイザ。
- Cent OS 7 ゲスト オペレーティング システム。
- CDO コネクタと SEC のみをホストするための VM のシステム要件は以下のとおりです。
  - CPU：SEC 用に 4 つの CPU を割り当てます。
  - メモリ：SEC 用に 8 GB のメモリを割り当てます。
  - ディスク領域：64 GB
- この手順を実行するユーザーは、Linux 環境の操作と **vi** ビジュアルエディタによるファイルの編集に慣れている必要があります。
- CDO コネクタを CentOS 仮想マシンにインストールする場合は、Yum セキュリティパッチを定期的にインストールすることをお勧めします。Yum の更新を取得するための設定に応じて、ポート 443 だけでなくポート 80 でもアウトバウンドアクセスを開く必要がある場合があります。また、更新をスケジュールするために yum-cron または crontab も設定する必要があります。セキュリティ運用チームと連携して、Yum の更新を取得するためにセキュリティポリシーを変更する必要があるかどうかを判断します。
- インストールを開始する前に、次の情報を収集します。
  - CDO コネクタに使用する静的 IP アドレス。
  - インストールプロセス中に作成する **root** ユーザーと **cdo** ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - CDO コネクタアドレスが存在するネットワークゲートウェイの IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- CDO Connector 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。

- **始める前に**：手順内のコマンドは、コピーして端末ウィンドウに貼り付けるのではなく入力するようにしてください。一部のコマンドに含まれる「n ダッシュ」は、カットアンドペーストのプロセスで「m ダッシュ」として適用される場合があり、コマンドが失敗する原因となります。

ステップ 1 [Secure Device Connector] ページで、青いプラスボタン  をクリックし、[Secure Event Connector] を選択します。

ステップ 2 表示されたリンクを使用して、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] ウィンドウの手順 2 で SEC ブートストラップデータをコピーします。

ステップ 3 少なくともこの手順の前提条件に記載されているメモリ、CPU、およびディスク容量を備えた CentOS 7 仮想マシン（http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso）をインストールします。

ステップ 4 インストールしたら、CDO コネクタの IP アドレス、サブネットマスク、ゲートウェイの指定など、ネットワークの基本設定を行います。

ステップ 5 DNS（ドメインネームサーバー）を設定します。

ステップ 6 NTP（ネットワーク タイム プロトコル）サーバーを設定します。

ステップ 7 CDO コネクタの CLI と簡単にやり取りできるように、CentOS に SSH サーバーをインストールします。

ステップ 8 Yum の更新を実行し、**open-vm-tools**、**nettools**、および **bind-utils** パッケージをインストールします。

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

ステップ 9 **AWS CLI パッケージ**をインストールします（https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html を参照）。

（注） `--user` フラグは使用しないでください。

ステップ 10 **Docker CE パッケージ**をインストールします（https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce を参照）。

（注） 「リポジトリを使用したインストール」方法を使用します。

ステップ 11 Docker サービスを開始し、起動時に開始できるようにします。

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

ステップ 12 **cdo** と **sdc** の 2 つのユーザーを作成します。cdo ユーザーは、管理機能を実行するためにログインするユーザーです（つまり root ユーザーを直接使用する必要はありません）。sdc ユーザーは、CDO コネクタの docker コンテナを実行するユーザーです。

```
[root@sdc-vm ~]# useradd cdo
 [root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

ステップ 13 cdo ユーザーのパスワードを設定します。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

ステップ 14 cdo ユーザーを「wheel」グループに追加し、管理者（sudo）権限を付与します。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
 [root@sdc-vm ~]#
```

ステップ 15 Docker がインストールされると、ユーザーグループが作成されます。CentOS/Docker のバージョンに応じて、「docker」または「dockerroot」と呼ばれます。/etc/group ファイルでどのグループが作成されたかを確認したら、sdc ユーザーをそのグループに追加します。

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

ステップ 16 `/etc/docker/daemon.json` ファイルが存在しない場合は作成し、以下の内容を入力します。作成したら、docker デーモンを再起動します。

（注） 「group」キーに入力したグループ名が、ステップ 15と一致していることを確認してください。

```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

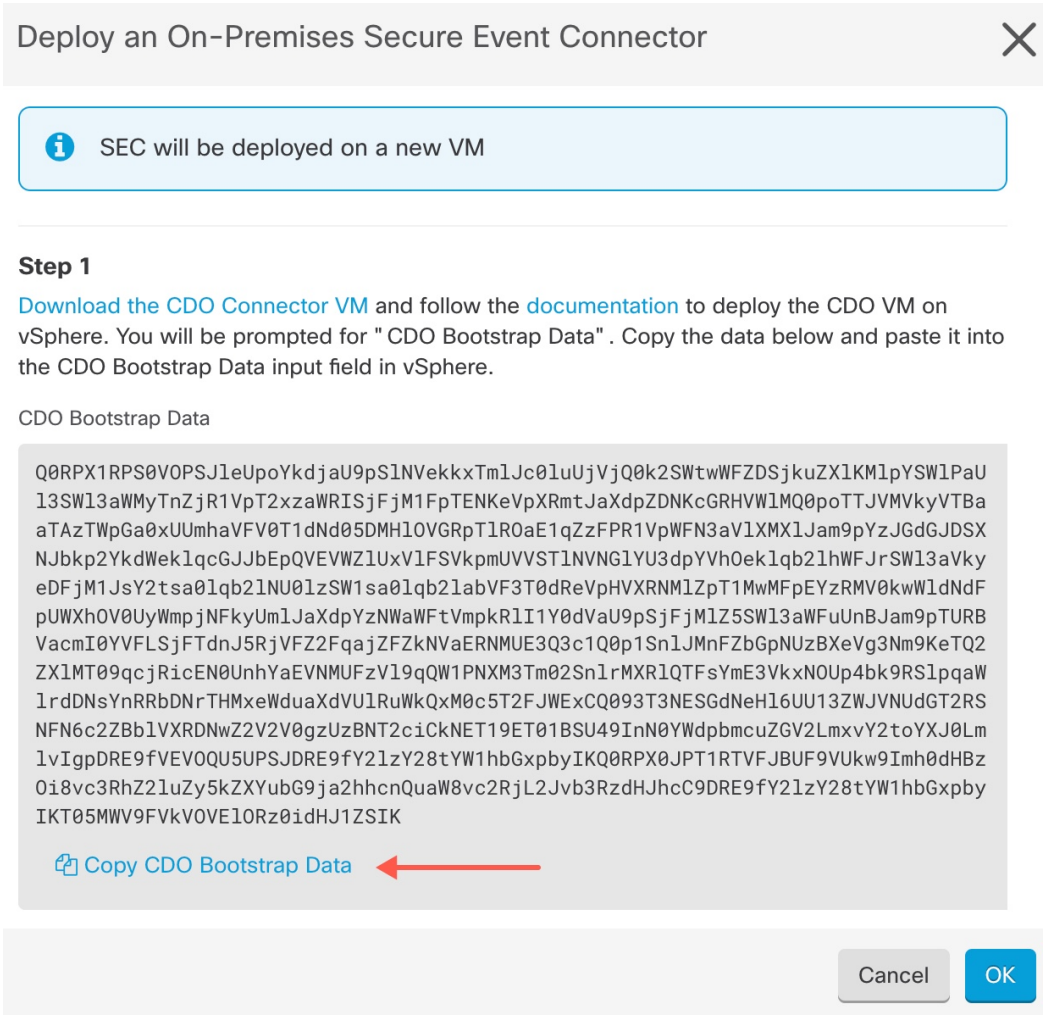
ステップ 17 現在 vSphere コンソールセッションを使用している場合は、SSH に切り替えて、**cdo** ユーザーでログインします。ログインしたら、**sdc** ユーザーに切り替えます。パスワードの入力を求められたら、**cdo** ユーザーのパスワードを入力します。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

ステップ 18 ディレクトリを **/usr/local/cdo** に変更します。

ステップ 19 **bootstrapdata** という新しいファイルを作成し、展開ウィザードの手順1 のブートストラップデータを、このファイルに貼り付けます。[保存（Save）] をクリックしてファイルを保存します。[vi] または [nano]

を使用してファイルを作成できます。



ステップ 20 ブートストラップデータはbase64でエンコードされていますので、暗号解読化して**extractedbootstrapdata**というファイルにエクスポートします。

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

catコマンドを実行して暗号解読化したデータを表示します。コマンドおよび暗号解読化したデータは次のようになります。

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

ステップ 21 以下のコマンドを実行して、暗号解読化したブートストラップデータの一部を環境変数にエクスポートします。

```
 [sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
[sdc@sdc-vm ~]$
```

ステップ 22 CDO からブートストラップバンドルをダウンロードします。

```
 [sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

ステップ 23 CDO コネクタ tarball を展開し、bootstrap_sec_only.sh ファイルを実行して CDO コネクタパッケージをインストールします。

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

次のタスク

作成した VM にインストールされた SDC および CDO コネクタの追加設定 （75 ページ） に進みます。

作成した VM にインストールされた SDC および CDO コネクタの追加設定

CDO コネクタを独自の CentOS 7 仮想マシンにインストールした場合は、イベントが SEC に到達できるように、次の付加的な設定手順の**いずれか**を実行する必要があります。

- CentOS 7 VM での firewalld サービスの無効化この設定は、シスコが提供する SDC VM の設定と一致します。
- firewalld サービスの実行を許可し、ファイアウォールルールを追加して、イベントトラフィックが SEC に到達できるようにします。 （76 ページ）。この手順では、インバウンドイベント トラフィックを許可するためのより詳細なアプローチが示されます。

CentOS 7 VM での firewalld サービスの無効化

1. SDC VM の CLI に「cdo」ユーザーとしてログインします。

2. firewalld サービスを停止してから、続く VM の再起動時に無効のままになっていることを確認します。プロンプトが表示されたら、**cdo** ユーザーのパスワードを入力します。

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker サービスを再起動して、Docker 固有のエントリをローカルファイアウォールに再挿入します。

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. CDO コネクタ仮想マシンへの Secure Event Connector のインストール （76 ページ）に進みます。

firewalld サービスの実行を許可し、ファイアウォールルールを追加して、イベントトラフィックが SEC に到達できるようにします。

1. SDC VM の CLI に「cdo」ユーザーとしてログインします。
2. ローカル ファイアウォール ルールを追加して、設定した TCP、UDP、または NSEL ポートから SEC への着信トラフィックを許可します。SEC で使用されるポートについては、「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。プロンプトが表示されたら、**cdo** ユーザーのパスワードを入力します。コマンドの例を次に示します。別のポート値の指定が必要になる場合があります。

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. firewalld サービスを再起動して、新しいローカルファイアウォールルールをアクティブかつ持続的なものにします。

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. CDO コネクタ仮想マシンへの Secure Event Connector のインストール （76 ページ） に進みます。

CDO コネクタ仮想マシンへの Secure Event Connector のインストール

始める前に

次の 2 つのタスクを実行します。

- VM イメージを使用して SEC をサポートするための CDO コネクタのインストール （70 ページ）
- 作成した VM にインストールされた SDC および CDO コネクタの追加設定 （75 ページ）

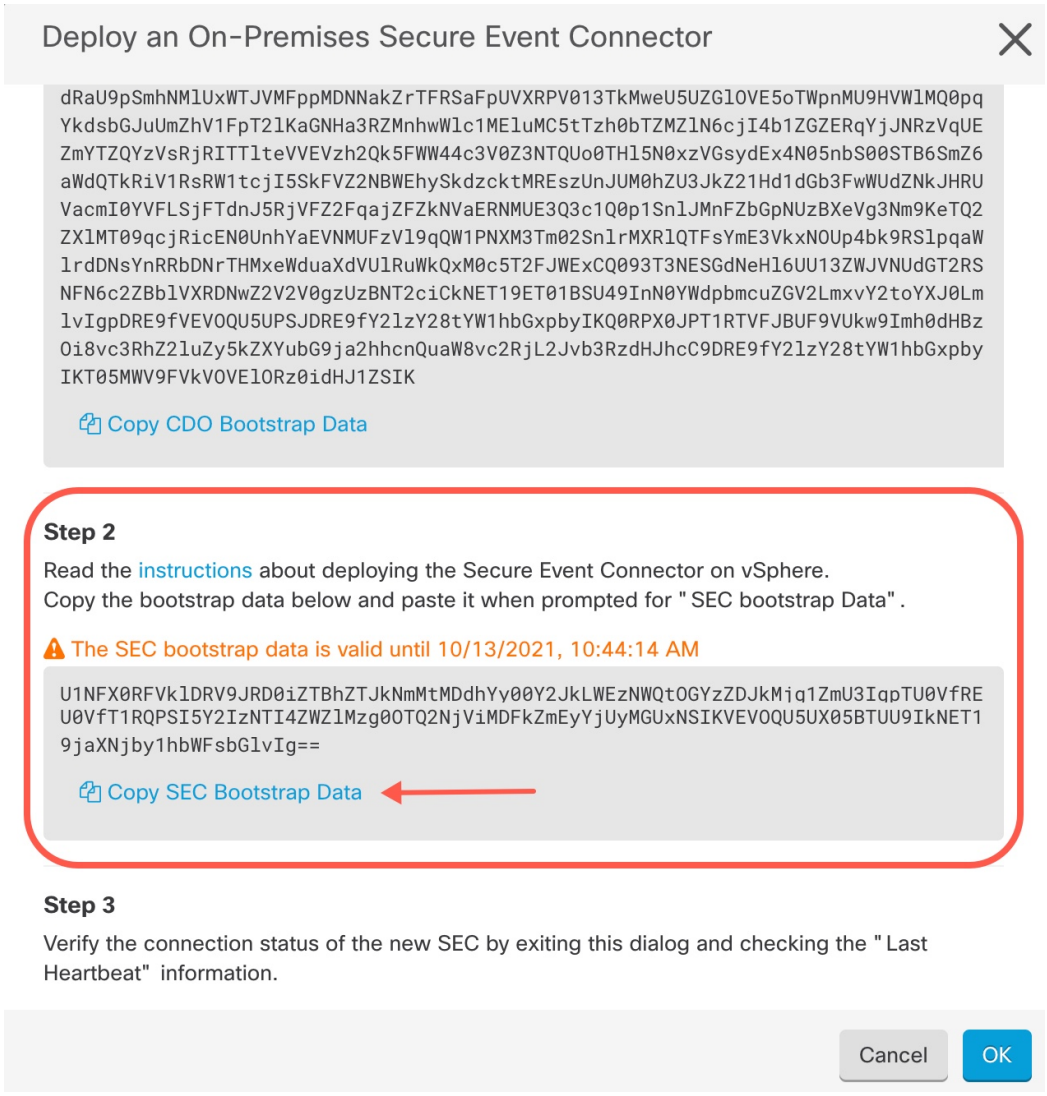
ステップ 1 CDO にログインします。

ステップ 2 [ユーザー（user）] メニューをクリックし、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 3 上記の前提条件の手順を使用してインストールした CDO コネクタを選択します。[セキュアコネクタ（Secure Connectors）] テーブルでは、「Secure Event Connector」と呼ばれます。

ステップ 4 右側の [アクション] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

ステップ 5 ウィザードの**ステップ 2**で、[SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。



ステップ 6 SSH を使用してセキュアコネクタに接続し、**cdo** ユーザーとしてログインします。

ステップ 7 ログインしたら、**sdc** ユーザーに切り替えます。パスワードの入力を求められたら、「cdo」ユーザーのパスワードを入力します。これらのコマンドの例を次に示します。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

ステップ 8 プロンプトで、sec.sh セットアップスクリプトを実行します。

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

ステップ 9 プロンプトの最後に、手順 4 でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。

```
================================================
Running SEC health check for tenant [redacted]
------------------------------------------------
SEC cloud URL [redacted] is: Reachable
------------------------------------------------
SEC Connector status: Active
------------------------------------------------
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
------------------------------------------------
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
================================================
```

登録に失敗したことや SEC の導入準備に失敗したことを示すメッセージを受け取った場合は、「Secure Event Connector 導入準備のトラブルシューティング」を参照してください。

成功メッセージを受け取った場合は、[オンプレミスのSecure Event Connectorの展開（Deploy an ON-Premise Secure Event Connector）] ダイアログボックスで [完了（Done）] をクリックします。VM イメージへの SEC のインストールは完了です。

ステップ 10 「**次の作業**」に進みます。

次のタスク

この手順に戻って、SAL SaaS の実装を続行します：ASA デバイスに安全なロギング分析（SaaS）を導入する （7 ページ）

関連情報：

- Secure Device Connector のトラブルシュート
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング
- SEC 登録失敗のトラブルシューティング

Cisco Security Analytics and Logging（SaaS）をプロビジョニング解除する

Cisco Security Analytics and Logging（SaaS）の有料ライセンスの有効期限が切れた場合、90 日間の猶予期間があります。この猶予期間中に有料ライセンスを更新した場合は、サービスが中断されません。

更新せずに 90 日間の猶予期間が経過すると、お客様のデータはすべて消去されます。[イベントロギング] ページから ASA や FTD イベントを表示することも、ダイナミック エンティティ モデリングの動作分析を ASA、FTD イベント、およびネットワークフローデータに適用することもできなくなります。

Secure Event Connector の削除

警告：この手順により、Secure Event Connector が Secure Device Connector から削除されます。これを行うと、Secure Logging Analytics（SaaS）を使用できなくなります。この操作は元に戻せません。質問や懸念事項がある場合は、このアクションを実行する前に CDO サポートまでお問い合わせください。

Secure Device Connector から Secure Event Connector を削除するには、次の 2 段階のプロセスを実行します。

1. CDO からの SEC の削除。
2. SDC からの SEC ファイルの削除。

次に行う作業：CDO からの SEC の削除を続行します。

CDO からの SEC の削除

始める前に

Secure Event Connector の削除 （79 ページ）を参照してください。

ステップ 1 CDO にログインします。

ステップ 2 アカウントメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 3 デバイスタイプが [Secure Event Connector] の行を選択します。

警告 ：慎重に操作してください。Secure Device Connector を選択しないでください。

ステップ 4 [アクション] ペインで、[削除] をクリックします。

ステップ 5 [OK] をクリックして、Secure Event Connector を削除することを確認します。

次のタスク

SDC からの SEC ファイルの削除 （79 ページ） に進みます。

SDC からの SEC ファイルの削除

この項目は、SDC から Secure Event Connector を削除する 2 つの部分から成る手順の 2 番目の部分です。開始する前に「Secure Event Connector の削除 （79 ページ）」を参照してください。

ステップ 1 仮想マシンのハイパーバイザを開き、SDC のコンソールセッションを開始します。

ステップ 2 SDC ユーザーに切り替えます。

```
[cdo@tenant toolkit]$sudo su sdc
```

ステップ 3 プロンプトで、次のいずれかのコマンドを入力します。

- 独自のテナントのみを管理している場合：

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
```

- 複数のテナントを管理する場合は、テナント名の先頭に CDO_ を追加してください。次に例を示します。

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
```

ステップ 4 SEC ファイルの削除を確定します。

Cisco Secure Cloud Analytics ポータルのプロビジョニング

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

Logging Analytics and Detection ライセンスまたは **Total Network Analytics and Monitoring** ライセンスを購入した場合、Secure Event Connector（SEC）を展開して設定した後、Secure Cloud Analytics ポータルを CDO ポータルに関連付けて、Secure Cloud Analytics アラートを表示する必要があります。ライセンスを購入すると、既存の Secure Cloud Analytics ポータルがある場合は、Secure Cloud Analytics ポータル名を指定して、すぐに CDO ポータルに関連付けることができます。

それ以外の場合は、CDO UI から新しい Secure Cloud Analytics ポータルをリクエストできます。Secure Cloud Analytics アラートに初めてアクセスすると、システムに Secure Cloud Analytics ポータルを要求するページが表示されます。このポータルを要求するユーザーには、ポータルの管理者権限が付与されます。

ステップ 1 CDO で、**[モニタリング（Monitoring）]**>**[セキュリティ分析（Security Analytics）]** を選択し、新しいウィンドウで Secure Cloud Analytics UI を開きます。

ステップ 2 [無料トライアルを開始（Start Free Trial）] をクリックして、Secure Cloud Analytics ポータルをプロビジョニングし、CDO ポータルに関連付けます。

（注） ポータルを要求した後、プロビジョニングに数時間かかる場合があります。

次の手順に進む前に、ポータルがプロビジョニングされていることを確認してください。

1. CDO で、**[モニタリング（Monitoring）]** > **[セキュリティ分析（Security Analytics）]** を選択し、新しいウィンドウで Secure Cloud Analytics UI を開きます。
2. 次の選択肢があります。
   - Secure Cloud Analytics ポータルを要求したものの、まだポータルのプロビジョニング中であることがシステムに表示されている場合は、しばらく待ってから、後でアラートへのアクセスを試行してください。
   - Secure Cloud Analytics ポータルがプロビジョニング済みの場合は、[ユーザー名（Username）] と [パスワード（Password）] を入力し、[サインイン（Sign in）] をクリックします。

（注） 管理者ユーザーは、Secure Cloud Analytis ポータル内でアカウントを作成するように他のユーザーを招待できます。詳細については、Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）を参照してください。

次のタスク

- **Logging Analytics and Detection** ライセンスを購入した場合、設定は完了しています。Secure Cloud Analytics ポータル UI から CDO 統合のステータスやセンサーの正常性のステータスを表示する場合は、「Cisco Secure Cloud Analytics でのセンサーの正常性と CDO 統合ステータスの確認 （81 ページ）」で詳細を参照してください。Secure Cloud Analytics ポータルでアラートを操作する場合は、「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）」および「ファイアウォールイベントに基づくアラートの使用」を参照してください。
- **Total Network Analytics and Monitoring** ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開して、ネットワークフローデータをクラウドに渡します。クラウドベースのネットワークフローデータを監視する場合は、フローデータを Secure Cloud Analytics に渡すようにクラウドベースの展開を設定します。詳細については、総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （82 ページ）を参照してください。

Cisco Secure Cloud Analytics でのセンサーの正常性と CDO 統合ステータスの確認

Sensor Status

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

Cisco Secure Cloud Analytics Web UI では、[センサーリスト（Sensor List）] ページで CDO 統合ステータスと設定済みセンサーを確認できます。CDO 統合は、読み取り専用の接続イベントセンサーです。Stelathwatch Cloud のメインメニューには、センサーの全体的な正常性が示されます。

- 緑色の雲のアイコン（）：すべてのセンサーと CDO（設定されている場合）との接続が確立されています。
- 黄色の雲のアイコン（）：一部のセンサー、または CDO（設定されている場合）との接続が確立されており、1 つ以上のセンサーが正しく設定されていません。
- 赤色の雲のアイコン（）：設定されているすべてのセンサーと CDO（設定されている場合）との接続が失われています。

センサーまたは CDO 統合ごとに、緑色のアイコンは接続が確立されていることを示し、赤色のアイコンは接続が失われていることを示します。

ステップ 1 1. Cisco Secure Cloud Analytics ポータル UI で、[設定]（）> [センサー（Sensors）] を選択します。

ステップ 2 [センサーリスト（Sensor List）] を選択します。

総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開

Secure Cloud Analytics センサーの概要と展開

必要なライセンス：Total Network Analytics and Monitoring

Total Network Analytics and Monitoring ライセンスを取得している場合は、Secure Cloud Analytics ポータルをプロビジョニングした後に、次のことができます。

- オンプレミスネットワーク内に Secure Cloud Analytics センサーを展開し、ネットワークフローデータを分析のためにクラウドに渡すように設定します。
- フローデータを分析のために Secure Cloud Analytics に渡すようにクラウドベースの展開を設定します。

ネットワーク境界のファイアウォールが内部ネットワークと外部ネットワークの間のトラフィックに関する情報を収集する一方で、Secure Cloud Analytics センサーは内部ネットワーク内のトラフィックに関する情報を収集します。

（注） FTD デバイスは、NetFlow データを渡すように設定できます。センサーを展開するときは、イベント情報を CDO に渡すように設定されている FTD デバイスからの NetFlow データを渡すようにセンサーを設定しないでください。

センサーの展開手順と推奨事項については、Secure Cloud Analytics センサーのインストールガイドを参照してください。

クラウドベース展開の設定手順と推奨事項については、Secure Cloud Analytics パブリック クラウド モニタリング ガイドを参照してください。

（注） Secure Cloud Analytics ポータルの UI で手順を確認して、センサーとクラウドベース展開を設定することもできます。

Secure Cloud Analytics の詳細については、Secure Cloud Analytics 無料試用ガイドを参照してください。

次の手順

- 「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 （83 ページ）」に進みます。

Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

[イベントロギング] ページでファイアウォールイベントを確認できますが、CDO ポータル UI から Cisco Secure Cloud Analytics アラートを確認することはできません。[セキュリティ分析（Security Analytics）] メニューオプションを使用して CDO から Secure Cloud Analytics ポータルをクロス起動し、ファイアウォール イベント データ（および [Total Network Analytics and Monitoring] を有効にしている場合はネットワークフローデータ）から生成されたアラートを表示できます。[セキュリティ分析（Security Analytics）] メニューオプションには、1 つ以上のワークフローステータスが開いている場合、開いているワークフローステータスの Secure Cloud Analytics アラートの数を示すバッジが表示されます。

Security Analytics and Logging ライセンスを使用して Secure Cloud Analytics アラートを生成し、新しい Secure Cloud Analytics ポータルをプロビジョニングした場合は、CDO にログインしてから、Cisco Secure Sign-On を使用して Secure Cloud Analytics をクロス起動します。URL を使用して Secure Cloud Analytics ポータルに直接アクセスすることもできます。

詳細については、『Cisco SecureX sign-on』を参照してください。

Cisco Secure Cloud Analytics ポータルへに参加するようユーザーを招待する

Cisco Secure Cloud Analytics ポータルのプロビジョニングをリクエストする最初のユーザーには、Cisco Secure Cloud Analytics ポータルの管理者権限があります。そのユーザーは、他のユーザーを電子メールで招待してポータルに参加させることができます。招待されたユーザーは、Cisco Secure Sign-On のログイン情報を持っていない場合、招待メールのリンクを使用して作成できます。ユーザーは、CDO から Cisco Secure Cloud Analytics へのクロス起動中に、Cisco Secure Sign-On のログイン情報を使用してログインできます。

電子メールで他のユーザーを Cisco Secure Cloud Analytics ポータルに招待するには、次の手順を実行します。

ステップ 1 Cisco Secure Cloud Analytics ポータルに管理者としてログインします。
ステップ 2 **[設定]** > **[アカウント管理（Account Management）]** > **[ユーザー管理（User Management）]** を選択します。
ステップ 3 [電子メール（Email）] アドレスを入力します。
ステップ 4 [招待（Invite）] をクリックします。

CDO から Secure Cloud Analytics をクロス起動する

CDO からのセキュリティアラートを表示するには以下を実行します。

ステップ 1 CDO ポータルにログインします。
ステップ 2 ナビゲーションバーから **[モニタリング]** > **[セキュリティ分析]**を選択します。
ステップ 3 Secure Cloud Analytics インターフェイスで **[監視]** > **[アラート]**を選択します。

Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

Secure Cloud Analytics は、オンプレミスおよびクラウドベースのネットワーク展開をモニターする Software as a Service（SaaS）ソリューションです。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報をソースから収集することによって、トラフィックに関する観測内容が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを

生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

ダイナミック エンティティ モデリング

ダイナミック エンティティ モデリングは、ファイアウォールイベントとネットワークフローデータの動作分析を実行することにより、ネットワークの状態を追跡します。Secure Cloud Analyticsのコンテキストにおいて、エンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。**Logging Analytics and Detection** ライセンスと統合されたSecure Cloud Analytics は、エンティティが通常送信するトラフィックのタイプを判別するために、ファイアウォールイベントやその他のトラフィック情報から引き出すことができます。**Total Network Analytics and Monitoring** ライセンスを購入すると、Secure Cloud Analytics は、エンティティトラフィックのモデル化にNetFlowおよびその他のトラフィック情報を含めることもできます。各エンティティの最新のモデルを維持するため、Secure Cloud Analytics では、エンティティがトラフィックを送信し続け、場合によっては異なるトラフィックを送信する可能性があるため、これらのモデルを徐々に更新します。この情報から、Secure Cloud Analytics は以下を識別します。

- エンティティのロール：これは、エンティティが通常行うことの記述子です。たとえば、エンティティが、一般に電子メールサーバーに関連付けられるトラフィックを送信する場合、Secure Cloud Analytics は、そのエンティティに電子メールサーバーロールを割り当てます。エンティティは複数のロールを実行する場合があるため、ロールとエンティティの関係は多対 1 である可能性があります。
- エンティティの観測内容：これは、ネットワーク上でのエンティティの動作に関する事実（外部 IP アドレスとのハートビート接続、別のエンティティとの間で確立されたリモートアクセスセッションなど）です。CDO と統合すると、ファイアウォールイベントからこれらの事実を取得できます。**Total Network Analytics and Monitoring** ライセンスも購入すると、システムはNetFlowから事実を取得し、ファイアウォールイベントとNetFlowの両方から観測内容を生成することもできます。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

アラートと分析

ロール、観測内容、およびその他の脅威インテリジェンスの組み合わせに基づいてSecure Cloud Analyticsが生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。1 つのアラートが複数の観測内容を表す場合があることに注意してください。ファイアウォールが同じ接続とエンティティに関連する複数の接続イベントをログに記録する場合、アラートが 1 つだけになる可能性があります。

上記の例で言えば、新しい内部デバイスの観測内容だけでは、潜在的な悪意のある動作は構成されません。ただし、時間の経過とともに、エンティティがドメインコントローラと一致する

トラフィックを送信する場合、システムではそのエンティティにドメイン コントローラ ロールが割り当てられます。その後、そのエンティティが、以前に接続を確立していない外部サーバーへの接続を確立し、異常なポートを使用して大量のデータを転送すると、システムは、[新しい大規模接続（外部）（New Large Connection (External)）] 観測内容と [例外ドメインコントローラ（Exceptional Domain Controller）] 観測内容をログに記録します。その外部サーバーが Talos ウォッチリストに登録されているものと識別された場合、これらすべての情報の組み合わせにより Secure Cloud Analytics はこのエンティティの動作に関するアラートを生成し、悪意のある動作を調査して対処するように促します。

Secure Cloud Analytics の Web ポータル UI でアラートを開くと、システムがアラートを生成した原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。また、エンティティが関係性を持っていたその他の観測内容やアラートを確認したり、この動作が他の潜在的に悪意のある動作に結び付いているかどうかを判断することもできます。

Secure Cloud Analytics でアラートを表示して閉じる場合、Secure Cloud Analytics UI からのトラフィックを許可またはブロックできないことに注意してください。デバイスをアクティブモードで展開した場合、ファイアウォール アクセス コントロール ルールを、トラフィックを許可またはブロックするように更新する必要があり、ファイアウォールがパッシブモードで展開されている場合は、ファイアウォールアクセスコントロールルールを更新する必要があります。

ファイアウォールイベントに基づくアラートの使用

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

アラートのワークフロー

アラートのワークフローは、そのステータスに基づいて異なります。システムによってアラートが生成される場合、そのデフォルト ステータスは [オープン（Open）] であり、ユーザーは割り当てられません。アラートのサマリーを表示すると、デフォルトでは、当面注意が必要なすべてのオープン アラートが表示されます。

注：**Total Network Analytics and Monitoring** ライセンスを持っている場合、アラートは、NetFlow から生成された観測結果、ファイアウォールイベントから生成された観測結果、または両方のデータソースからの観測結果に基づいて生成できます。

アラートのサマリーを確認する際は、初期トリアージとして、アラートにステータスを割り当て、タグ付けし、更新することができます。フィルタ機能と検索機能を使用して、特定のアラートを検索したり、さまざまなステータスのアラートを表示したり、さまざまなタグや割り当て対象を関連付けたりすることができます。アラートのステータスは[スヌーズ（Snoozed）] に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。アラートから [スヌーズ（Snoozed）] ステータスを削除して、再びオープンアラートとして表示されるようにすることもできます。アラートを確認する際は、それらのアラートをそのユーザー自身またはシステム内の別のユーザーに割り当てることができ

ます。ユーザーは、自分のユーザー名に割り当てられているすべてのアラートを検索できます。

アラートのサマリーから、アラートの詳細ページを表示できます。このページでは、このアラートを生成させた、裏付けとなる観測内容に関する追加のコンテキストと、このアラートに関連するエンティティに関する追加のコンテキストを確認できます。この情報は、ネットワーク上の問題をさらに調査して悪意のある動作を潜在的に解決するために実際の問題を特定する上で役立ちます。

CDO の Stealthwatch Cloud Web ポータル UI 内やネットワーク上で調査しているときに、発見した内容を説明するコメントをアラートと一緒に残すことができます。これは、将来参照できる調査の記録を作成するために役立ちます。

分析が完了したら、ステータスを[クローズ（Closed）]に更新できます。これにより、デフォルトではオープンアラートとして表示されなくなります。将来、状況が変わった場合は、クローズ アラートのステータスを再度オープンにすることもできます。

ここでは、特定のアラートを調査する方法に関する一般的なガイドラインと推奨事項を示します。Stealthwatch Cloud はアラートをログに記録するときに追加のコンテキストを提供するため、このコンテキストを参照しながら調査を進めることができます。

これらの手順は、総合的または包括的であることを意図したものではありません。これらは単にアラートの調査を開始するための一般的な枠組みを提供するためのものです。

一般に、次の手順でアラートを確認できます。

1. オープンアラートのトリアージ （87 ページ）
2. 後で分析するためにアラートをスヌーズする （88 ページ）
3. 詳細な調査のためのアラートの更新 （89 ページ）
4. アラートの確認と調査の開始 （89 ページ）
5. エンティティとユーザーの調査 （91 ページ）
6. Secure Cloud Analytics を使用して問題を修復する （92 ページ）
7. アラートの更新とクローズ （93 ページ）

オープンアラートのトリアージ

特に複数の調査が必要な場合は、オープンアラートのトリアージを行います。

- CDO から SWC へのクロス起動とアラート表示の詳細については、「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示」を参照してください。

次の質問に答えてください。

- このアラート タイプを優先度の高いものとして設定しましたか。
- 影響を受けるサブネットに高い機密性を設定しましたか。

- この異常な動作はネットワーク上の新しいエンティティによるものですか。
- エンティティの通常のロールは何ですか。また、このアラートの動作はそのロールにどのように適合しますか。
- これは、このエンティティの通常の動作からの例外的な逸脱ですか。
- ユーザーが関与している場合、これはユーザーの予想される動作ですか、それとも例外的な動作ですか。
- 保護されたデータや機密データが侵害を受けるリスクがありますか。
- この動作の継続を許可すると、ネットワークへの影響はどの程度深刻になりますか。
- 外部エンティティとの通信がある場合、それらのエンティティは過去にネットワーク上の他のエンティティとの接続を確立しましたか。

これが優先順位の高いアラートである場合は、調査を進める前に、インターネットからエンティティを隔離するか、隔離しないときは接続を切断することを検討してください。

後で分析するためにアラートをスヌーズする

他のアラートと比較して優先度が低いときに、アラートをスヌーズします。たとえば、組織が電子メールサーバーをFTPサーバーとして再利用する場合、緊急プロファイルアラートが生成されます（エンティティの現在のトラフィックが、以前には一致しなかった動作プロファイルと一致することを示します）。これは想定される動作であるため、このアラートをスヌーズして、後日再検討できます。スヌーズされたアラートは、オープンアラートと一緒に表示されません。これらのスヌーズされたアラートを確認するには、特別にフィルタリングする必要があります。

アラートをスヌーズする：

ステップ1 [アラートを閉じる（Close Alert）] をクリックします。
ステップ2 [このアラートをスヌーズ（Snooze this alert）] ペインで、ドロップダウンからスヌーズ期間を選択します。
ステップ3 [保存（**Save**）] をクリックします。

次のタスク

スヌーズしたアラートを確認する準備ができたら、アラートのスヌーズを解除できます。これにより、ステータスが[オープン（Open）]に設定され、他のオープンアラートとともにアラートが表示されます。

スヌーズしたアラートのスヌーズを解除する：

- スヌーズしたアラートから、[アラートのスヌーズ解除（Unsnooze Alert）] をクリックします。

詳細な調査のためのアラートの更新

アラートの詳細情報を確認します。

ステップ 1 **[モニター（Monitor）]** > **[アラート（Alerts）]** を選択します。

ステップ 2 アラートタイプ名をクリックします。

次のタスク

初期トリアージと優先順位付けに基づいて、アラートを割り当て、タグを付けます。

1. [担当者（Assignee）] ドロップダウンからユーザーを選択してアラートを割り当てます。これにより、ユーザーが調査を開始できるようになります。
2. [タグ（Tags）] ドロップダウンから 1 つ以上のタグを選択して、アラートにタグを追加することにより、将来の識別のためにアラートをより適切に分類したり、アラートの長期的なパターンの確立を試みることができます。
3. 必要に応じて、**このアラートに関するコメント**を入力し、[コメント（Comment）]をクリックすることにより、最初の調査結果を追跡するためのコメントを残し、アラートに割り当てられた担当者を支援することができます。アラートは、システムコメントとユーザーコメントの両方を追跡します。

アラートの確認と調査の開始

割り当てられたアラートを確認する場合は、アラートの詳細を確認して、Stealthwatch Cloud がアラートを生成した理由を把握してください。裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。

アラートがファイアウォールイベントに基づいて生成された場合、ファイアウォールの展開がこのアラートのソースであることはシステムに認識されません。

このソースエンティティの一般的な動作やパターンを理解するために、サポートされている観測内容をすべて表示し、このアクティビティがより長いトレンドの一部である可能性があるかどうかを確認します。

手順の概要

1. アラートの詳細で、観測タイプの横にある矢印アイコン（  ）をクリックして、そのタイプの記録されたすべての観測内容を表示します。
2. [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（  ）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

手順の詳細

ステップ 1 アラートの詳細で、観測タイプの横にある矢印アイコン（）をクリックして、そのタイプの記録されたすべての観測内容を表示します。

ステップ 2 [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

観測内容に対して追加の分析を実行する場合は、サポートされている観測内容をコンマ区切り値ファイルでダウンロードします。

- アラートの詳細の [サポートされている観測内容（Supporting Observations）] ペインで、[CSV] をクリックします。

観測内容から、ソースエンティティの動作が悪意のある動作を示しているか判断します。ソースエンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか（それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど）を確認します。

ソースエンティティの IP アドレスまたはホスト名から、ソースエンティティに関連する追加コンテキスト（関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、送信しているセッショントラフィックのタイプなど）を表示します。

- エンティティに関連するすべてのアラートを表示するには、IPアドレスまたはホスト名のドロップダウンから [アラート（Alerts）] を選択します。
- エンティティに関連するすべての観測内容を表示するには、IPアドレスまたはホスト名のドロップダウンから [観測内容（Observations）] を選択します。
- デバイスに関する情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [デバイス] を選択します。
- このエンティティに関連するセッショントラフィックを表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー] を選択します。

Stealthwatch Cloud のソースエンティティは常にネットワークの内部にあることに注意してください。この点を、接続を開始したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのイニシエータ IP と比較してください。

観測内容から、他の外部エンティティに関する情報を調べます。地理位置情報を調査し、いずれかの地理位置情報データまたは Umbrella データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワー

ク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。

ソースエンティティが接続を確立した外部エンティティの IP アドレスまたはホスト名のコンテキストを確認します。

- このエンティティの最近のトラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [IPトラフィック（IP Traffic）] を選択します。
- このエンティティの最近のセッショントラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- AbuseIPDB の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [AbuseIPDB] を選択します。
- Cisco Umbrella の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Cisco Umbrella] を選択します。
- Google でこの IP アドレスを検索するには、IP アドレスまたはホスト名のドロップダウンから [Google検索（Google Search）] を選択します。
- Talos の Web サイト上でこの情報に関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Talos Intelligence] を選択します。
- このエンティティをウォッチリストに追加するには、IPアドレスまたはホスト名のドロップダウンから [IPをウォッチリストに追加（Add IP to watchlist）] を選択します。
- 前月のこのエンティティのトラフィックを検索するには、IPアドレスまたはホスト名のドロップダウンから [複数日のIPを検索（Find IP on multiple days）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー（Copy）] を選択します。

Stealthwatch Cloud の接続エンティティは、常にネットワークの外部にあることに注意してください。この点を、接続要求に応答したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのレスポンダ IP と比較してください。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

エンティティとユーザーの調査

Stealthwatch Cloud ポータル UI でアラートを確認した後、ソースエンティティ、このアラートに関係している可能性のあるユーザー、およびその他の関連エンティティに対して、追加の調査を直接実行できます。

- ソースエンティティがネットワーク上のどこ（物理的またはクラウド上）にあるかを特定し、直接アクセスします。このエンティティのログファイルを見つけます。それがネット

ワーク上の物理エンティティである場合は、デバイスにアクセスしてログ情報を確認し、この動作の原因となっているものに関する情報があるかどうかを確認します。それが仮想エンティティである場合またはクラウドに保存されている場合は、ログにアクセスして、このエンティティに関連するエントリを検索します。不正なログイン、承認されていない設定変更などに関する詳細について、ログを調査します。

- エンティティを調査します。マルウェアまたはエンティティ自体にある脆弱性を特定できるかどうかを判断してください。デバイスの物理的な変更（組織によって承認されていない USB スティックなど）を含め、何らかの悪意のある変更があったかどうかを確認します。
- ネットワーク上のユーザーまたはネットワーク外のユーザーによる関与があったかどうかを確認します。可能であれば、何をしていたのかをユーザーに尋ねてください。ユーザーに尋ねることができない場合は、そのユーザーがアクセス権を持っていたと考えられるかどうかと、この動作を促す状況（解雇された従業員が退社する前に外部サーバーにファイルをアップロードするなど）が発生したかどうかを確認します。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

Secure Cloud Analytics を使用して問題を修復する

悪意のある動作によってアラートが発生した場合は、悪意のある動作を修正します。次に例を示します。

- 悪意のあるエンティティまたはユーザーがネットワーク外からのログインを試みた場合は、ファイアウォールルールとファイアウォール構成を更新して、それらのエンティティまたはユーザーがネットワークにアクセスできないようにします。
- エンティティが許可されていないドメインまたは悪意のあるドメインにアクセスを試みた場合は、影響を受けるエンティティを調べて、マルウェアが原因かどうかを判断します。悪意のある DNS リダイレクトがある場合は、ネットワーク上の他のエンティティが影響を受けているかどうか、またはボットネットの一部であるかどうかを判断します。これがユーザーによる意図である場合は、ファイアウォール設定のテストなど、正当な理由があるかどうかを判断します。ファイアウォールルールとファイアウォール構成を更新して、ドメインへのそれ以上のアクセスを防止します。
- エンティティが過去のエンティティモデルの動作と異なる動作を示している場合は、動作の変更が意図されたものかどうかを判断します。意図されたものでない場合は、変更の責任がネットワーク上の承認ユーザーにあるかどうかを調べます。ネットワークの外部にあるエンティティが関係している場合は、ファイアウォールルールとファイアウォール構成を更新して意図せぬ動作に対処します。
- 脆弱性またはエクスプロイトを特定した場合は、影響を受けるエンティティを更新したり、それらにパッチを適用して脆弱性を削除するか、ファイアウォール構成を更新して許可されていないアクセスを防止します。ネットワーク上の他のエンティティが同様に影響

を受ける可能性があるかどうかを判断し、それらのエンティティに同じ更新またはパッチを適用します。現時点で脆弱性またはエクスプロイトを修正する手段がない場合は、該当するベンダーに連絡し、それらを通知してください。

- マルウェアを特定した場合は、エンティティを隔離してマルウェアを削除します。ファイアウォールファイルおよびマルウェアイベントを確認してネットワーク上の他のエンティティが危険にさらされているかどうかを判断し、エンティティを検疫および更新して、このマルウェアが広がることを防止します。このマルウェアまたはこのマルウェアの原因となったエンティティに関する情報によってセキュリティ情報を更新してください。ファイアウォールのアクセス制御およびファイルとマルウェアルールを更新して、今後このマルウェアがネットワークに感染するのを防ぎます。必要に応じてベンダーに通知してください。
- 悪意のある動作によってデータが漏洩した場合は、許可されていないソースに送信されたデータの性質を確認します。不正なデータ漏洩に関する組織の規定に従ってください。ファイアウォール構成を更新して、このソースによる今後のデータ漏洩の試みを防ぎます。

アラートの更新とクローズ

調査結果に基づいてタグを追加します。

ステップ 1 Secure Cloud Analytics ポータルの UI で、**[監視]** > **[アラート]**を選択します。

ステップ 2 ドロップダウンから 1 つ以上の**タグ**を選択します。

調査結果と実行された修正手順を説明する最終コメントを追加します。

- アラートの詳細で、[このアラートに関するコメント] を入力し、[コメント] をクリックします。

アラートのステータスをクローズにして、役立つものかどうかが分かるようにマークします。

1. アラートの詳細から、[アラートを閉じる] をクリックします。
2. アラートが役立った場合は [はい] を、アラートが役立たなかった場合は [いいえ] を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味する点に注意してください。
3. [保存（**Save**）] をクリックします。

次のタスク

クローズしたアラートの再オープン

クローズしたアラートに関連する追加情報を検出した場合、またはそのアラートに関連するコメントを追加する場合は、そのアラートを再度開いてステータスを [オープン（Open）] に変更できます。その後、必要に応じてアラートを変更し、追加調査が完了したら再度閉じます。

クローズしたアラートを再オープンします。

- クローズしたアラートの詳細から、[アラートを再オープン] をクリックします。

アラートの優先順位を変更する

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

アラートタイプにはデフォルトの優先順位が設定されています。これは、このタイプのアラートを生成するシステムの機密性に影響します。アラートの優先順位は、シスコのインテリジェンスおよびその他の要因に基づいて、[低] または [通常] にデフォルト設定されます。ネットワーク環境に基づいて、関心のある特定のアラートを強調するために、アラートタイプの優先順位を変更することができます。アラートタイプの優先順位は、[低]、[通常]、または [高] に設定できます。

- **[モニター]** > **[アラート]** を選択します。
- 設定のドロップダウンアイコン（）をクリックし、[アラートのタイプと優先順位] を選択します。
- アラートタイプの横にある編集のアイコン（）をクリックし、[低]、[中]、または [高] を選択して優先順位を変更します。

ライブイベントを表示する

[ライブ]イベントページには、入力したイベントロギングページでのイベントの検索とフィルタリングに一致する、直近 500 件のイベントが表示されます。[ライブ] ページに最大数である 500 のイベントが表示されており、さらに表示されるイベントが追加されると、CDO は最新のライブイベントを表示し、最も古いライブイベントを [履歴] イベントページに転送します。これにより、ライブイベントの総数が 500 に維持されます。この転送には、約 1 分を要します。フィルタリング基準を追加しない場合は、イベントを記録するように設定されたルールによって生成された最新の 500 のライブイベントがすべて表示されます。

イベントのタイムスタンプは、イベントを表示している CDO 管理者の現地時間で表示されます。

ライブイベントが再生中か一時停止中かにかかわらず、フィルタリング基準を変更すると、イベント画面がクリアされ、収集プロセスが再開されます。

CDO イベントビューアでライブイベントを表示するには、次の手順を実行します。

ステップ 1 ナビゲーションウィンドウで、**[モニターリング（Monitoring）]>[イベントロギング]** をクリックします。
ステップ 2 [ライブ] タブをクリックします。

次のタスク

次の関連情報を参照して、イベントを再生および一時停止する方法を確認します。

関連情報：

- ライブイベントの再生/一時停止 （95 ページ）
- 履歴イベントの表示 （96 ページ）
- イベントビューのカスタマイズ （96 ページ）

ライブイベントの再生/一時停止

ライブイベントがストリーミング中に「再生」 または「一時停止」 できます。ライブイベントが「再生中」の場合、CDO は、イベントビューアで指定されたフィルタ処理基準に一致するイベントを受信順に表示します。イベントが一時停止された場合、ライブイベントの再生を再開するまで、CDO はライブイベントページを更新しません。イベントの再生を再開すると、CDO は、イベントの再生を再開した時点からライブページへのイベントの入力を開始します。見逃したイベントが遡って再生されることはありません。

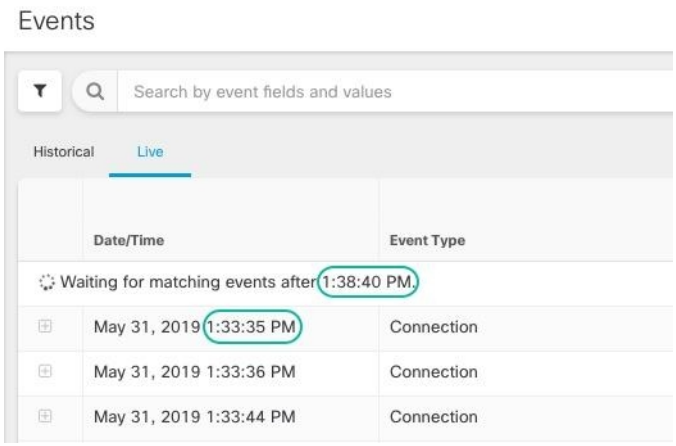
ライブイベントのストリーミングを再生または一時停止したかどうかにかかわらず、CDO が受信したすべてのイベントを表示するには、[履歴] タブをクリックします。

ライブイベントの自動一時停止

イベントを約 5 分間連続して表示した後、CDO は、ライブイベントのストリーミングを一時停止しようとしていることを警告します。その時点で、リンクをクリックしてライブイベントのストリーミングをさらに5分間継続するか、ストリーミングを停止することができます。準備ができたら、ライブイベントのストリーミングを再開できます。

イベントの受信とレポート

Secure Event Connector（SEC）がイベントを受信してから、CDO がライブイベントビューアにイベントを投稿するまでに、わずかに遅れが生じる場合があります。ライブページで遅延を確認できます。イベントのタイムスタンプは、SEC がイベントを受信した時刻です。



履歴イベントの表示

[ライブ]イベントページには、入力したイベントロギングページでのイベントの検索とフィルタリングに一致する、直近 500 件のイベントが表示されます。直近の 500 件より古いイベントは、[履歴] イベントテーブルに転送されます。この転送には、約 1 分を要します。その後、保存したすべてのイベントをフィルタリングして、探しているイベントを見つけることができます。

履歴イベントを表示するには、次の手順を実行します。

ステップ 1 ナビゲーションウィンドウで、[モニターリング（Monitoring）] > [イベントロギング] をクリックします。

ステップ 2 [履歴（Historic）] タブをクリックします。デフォルトでは、[履歴] イベントテーブルを開くと、フィルタは過去 1 時間以内に収集されたイベントを表示するように設定されています。

イベントの属性は、Firepower Device Manager（FDM）または Adaptive Security Device Manager（ASDM）によって報告されるものとほぼ同じです。

- Firepower Threat Defense イベント属性の完全な説明については、『Cisco Firepower Threat Defense Syslog メッセージ』を参照してください。
- ASA イベント属性の詳細については、『Cisco ASA シリーズ Syslog メッセージ』を参照してください。

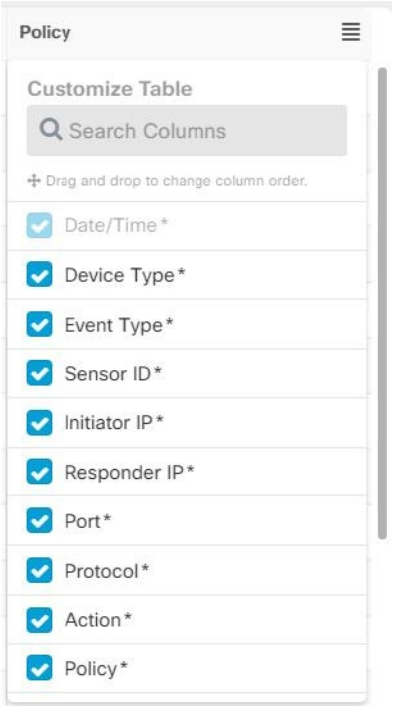
イベントビューのカスタマイズ

[イベントロギング]ページに加えられた変更は、このページから移動して後で戻ったときに備えて自動的に保存されます。

（注） ライブイベントと履歴イベントビューの設定は同じです。イベントビューをカスタマイズすると、変更はライブビューと履歴ビューの両方に適用されます。

列

ライブイベントと履歴イベントの両方のイベントビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン をクリックし、必要な列を選択または選択解除します。



アスタリスクの付いた列は、デフォルトでイベントテーブル内に含まれますが、いつでも削除できます。検索バーを使用して、追加する列のキーワードを手動で検索します。

順序

[イベント（Events）] ビューの列を並べ替えることができます。列の右側にある列フィルタアイコン をクリックして、選択した列のリストを展開し、列を目的の順序に手動でドラッグアンドドロップします。ドロップダウンメニューのリストの上部にある列がイベントビューの左端の列です。

関連情報：

- イベントロギングページでのイベントの検索とフィルタリング
- Security Analytics and Logging のイベント属性

イベントロギングページの列の表示および非表示

[イベントロギング] ページには、設定済み ASA および FTD デバイスから Cisco Cloud に送信された ASA および FTD Syslog イベントと、ASANetFlow セキュアイベントロギング（NSEL）イベントが表示されます。

テーブルで表示/非表示ウィジェットを使用して、[イベントロギング]ページの列を表示したり非表示にしたりできます。

ステップ 1 CDO のナビゲーションバーから、**[モニタリング]** > **[イベントロギング]**を選択します。

ステップ 2 テーブルの右端までスクロールし、[列の表示/非表示] ボタン ≣ をクリックします。

ステップ 3 表示する列のチェックボックスをオンにし、非表示にする列のチェックボックスをオフにします。

ステップ 4 [列の表示/非表示] ドロップダウンメニューの列名にマウスカーソルを合わせ、灰色の **+** をクリックして列の順序を変更します。

列が再び表示されるか非表示にされるまで、表示するように選択した列がテナントにログインしている他のユーザーにも表示されます。

以下の表は列ヘッダーについて説明しています。

カラム ヘッダ	説明
Date/Time	デバイスがイベントを生成した時間。時間はコンピュータのローカル時間で表示されます。
デバイスタイプ（Device Type）	ASA（適応型セキュリティアプライアンス） または FTD（Firepower Threat Defense）

カラム ヘッダ	説明

イベント タイプ（Event Type）	この複合列には、以下のいずれかを含めることができます。
	• **FTD イベントタイプ**
	  • 接続：アクセス制御ルールからの接続イベントを表示します。
	  • ファイル：アクセス制御ルールのファイルポリシーによってレポートされたイベントを表示します。
	  • 侵入：アクセス制御ルールの侵入ポリシーによってレポートされたイベントを表示します。
	  • マルウェア：アクセス制御ルールのマルウェアポリシーによって報告されたイベントを表示します。
	• ASA **イベントタイプ**：これらのイベントタイプは、syslog または NetFlow イベントのグループを表します。syslog ID または NetFlow ID が含まれているグループの詳細については、「ASA イベントタイプ」を参照してください。
	  • 解析されたイベント：解析された syslog イベントには、他の syslog イベントよりも多くのイベント属性が含まれており、CDO はそれらの属性に基づいて検索結果をより迅速に返すことができます。解析されたイベントはフィルタ処理カテゴリではありませんが、解析されたイベント ID は、[イベントタイプ] 列に斜体で表示されます。斜体で表示されていないイベント ID は解析されていません。
	  • ASANetFlow イベント ID：ASA からのすべての Netflow（NSEL）イベントがここに表示されます。

カラム ヘッダ	説明
センサー ID（Sensor ID）	センサー ID は、イベントを Secure Event Connector に送信する IP アドレスです。これは通常、Firepower Threat Defense または ASA の管理インターフェイスです。
[イニシエータ IP（Initiator IP）]	これは、ネットワークトラフィックの送信元の IP アドレスです。イニシエータ アドレス フィールドの値は、イベントの詳細の InitiatorIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
レスポンダ IP（Responder IP）	これは、パケットの宛先 IP アドレスです。宛先アドレスフィールドの値は、イベントの詳細の ResponderIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
ポート（Port）	セッション**レスポンダ**が使用するポートまたは ICMP コードです。宛先ポートの値は、イベントの詳細の **ResponderPort** の値に対応します
プロトコル（Protocol）	これは、イベントのプロトコルを表します。

カラム ヘッダ	説明
操作	ルールによって定義されたセキュリティアクションを指定します。入力する値は、検索対象と完全に一致する必要がありますが、大文字小文字は関係ありません。各イベントタイプ（接続、ファイル、侵入、マルウェア、syslog、および NetFlow）に異なる値を入力します。 • 接続イベントタイプの場合、フィルタは AC_RuleAction 属性で一致を検索します。それらの値は、Allow、Block、Trust のいずれかです。 • ファイルイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、Allow、Block、Trust のいずれかです。 • 侵入イベントタイプの場合、フィルタは InLineResult 属性で一致を検索します。それらの値は、Allowed、Blocked、Trusted のいずれかです。 • マルウェアイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、クラウド ルックアップ タイムアウトである可能性があります。 • syslog および NetFlow イベントタイプの場合、フィルタは Action 属性で一致を検索します。
ポリシー	イベントをトリガーしたポリシーの名前です。ASA と FTD デバイスでは名前が異なります。

関連情報：

イベントロギングページでのイベントの検索とフィルタリング （137 ページ）

カスタマイズ可能なイベントフィルタ

Secure Logging Analytics（SaaS）のお客様は、頻繁に使用するカスタムフィルタを作成して保存できます。

フィルタの要素は、設定時にフィルタのタブに保存されます。[イベントロギング]ページに戻るたびに、これらの検索機能を使用できます。テナントの他の CDO ユーザーは使用できません。複数のテナントを管理している場合、別のテナントでは使用できません。

（注） フィルタのタブで作業しているときにフィルタ条件を変更すると、加えられた変更はカスタムフィルタのタブに自動的に保存されることに注意してください。

ステップ 1 メインメニューから、**[モニタリング（Monitoring）]** > **[イベントロギング]** を選択します。

ステップ 2 値の [検索（Search）] フィールドをクリアします。

ステップ 3 イベントテーブルの上にある青いプラスボタンをクリックして、[表示（View）] タブを追加します。フィルタ表示には、名前を付けるまで、[表示1（View 1）]、[表示2（View 2）]、[表示3（View 3）] のようにラベルが付けられます。

ステップ 4 ビューのタブを選択します。

ステップ 5 フィルタバーを開き、カスタムフィルタに必要なフィルタ属性を選択します。「イベントロギングページでのイベントの検索とフィルタリング （137 ページ）」を参照してください。カスタムフィルタにはフィルタ属性のみが保存されることに注意してください。

ステップ 6 [イベントロギング] テーブルに表示する列をカスタマイズします。列の表示と非表示については、「イベントロギングページの列の表示および非表示 （98 ページ）」を参照してください。

ステップ 7 [表示X（View X）] ラベルの付いたフィルタタブをダブルクリックし、名前を変更します。

ステップ 8 （オプション）カスタムフィルタを作成したので、[検索（Search）] フィールドに検索条件を追加することにより、カスタムフィルタを変更せずに、[イベントロギング]ページに表示される結果を微調整できます。「イベントロギングページでのイベントの検索とフィルタリング （137 ページ）」を参照してください。

ステップ 9 （オプション）カスタムフィルタの結果を .csv.gz ファイルにダウンロードして、さらに並べ替えと分析を行います。[イベントのダウンロード（Downloading Events）]イベントのダウンロード （102 ページ）を参照してください。

イベントのダウンロード

[イベントログ（Event Logging）] ページの [履歴（Historical）] タブに表示されるイベントを、CDO からダウンロードできます。イベントダウンロードのいくつかの機能を次に示します。

- CDOがイベントを .csv ファイルに追加し、.gz 形式で圧縮します。
- 1 つの .csv ファイルに、最大約 50 GB の圧縮情報を収容できます。
- ダウンロード可能なファイルの生成は並行して実行できます。

- 作成された .csv.gz ファイルは Cisco Cloud に保存され、そこから直接ダウンロードされます。これらのファイルは、CDO/Secure Cloud Analytics サーバーリソースを消費しません。
- 作成されたダウンロード可能な .csv.gz ファイルは 7 日間保存され、その後削除されます。
- 進行中のジョブは手動でキャンセルできます。

[イベントログ（Event Logging）] ページに表示されるイベントのダウンロードは、次の 2 段階のプロセスです。

ステップ 1 .CSV.GZ ファイルの生成。（これは、GNU Gzip 形式を使用して圧縮されたカンマ区切り値のファイルです。GNU Gzip の詳細については、https://www.gnu.org/software/gzip/を参照してください）。

ステップ 2 .CSV.GZ ファイルのダウンロード。

次のタスク

.CSV.GZ ファイルの内容 （104 ページ）について学ぶ

.CSV.GZ ファイルの生成

ステップ 1 CDO のメニューバーから、**[モニタリング（Monitoring）]** > **[イベントロギング（Event Logging）]** を選択します。

ステップ 2 そのビューがまだ表示されていない場合は、[履歴] タブをクリックします。

ステップ 3 イベントフィルタと検索フィールドを使用して、ダウンロードするイベントを見つけます。そのフィルタリングと検索の結果に一致し、指定した時間範囲内に発生したイベントが、.csv.gz ファイルに含まれます。

ステップ 4 [.CSVの生成（Generate .CSV）] ボタンをクリックします。

ステップ 5 CDO がイベントを検出する時間範囲を選択します。

ステップ 6 わかりやすいファイル名を入力します。

ステップ 7 [.CSVの生成（Generate .CSV）] をクリックします。[ダウンロードおよび生成したファイル（Downloaded Generated Files）] ボタンをクリックすると、生成したファイルを見つけることができます。

（注） 実行中の .CSV ファイルの生成をキャンセルする場合は、[ダウンロードおよび生成したファイル（Downloaded Generated Files）] ボタンをクリックし、実行中のジョブを見つけて、[キャンセル] をクリックします。

.CSV.GZ ファイルのダウンロード

ステップ 1 CDO のメニューバーから、**[モニターリング（Monitoring）]** > **[イベントロギング]** を選択します。

ステップ 2 [生成されたファイルのダウンロード（Download Generated Files）] ボタンをクリックします。

ステップ 3 生成されたファイルを選択し、[ダウンロード（Download）] をクリックします。ファイルは圧縮形式であることに注意してください。

ステップ 4 ファイルを保存する場所を選択します。

.CSV.GZ ファイルの内容

.csv.gz フィールドの列には、イベントの展開された行に含まれるフィールドが反映されます。タイムスタンプ、FirstPacketSecond、および LastPacketSecond は、**協定世界時（UTC）**の秒単位で .csv ファイルに記録されます。

Security Analytics and Logging のイベント属性

イベント属性の説明

CDO によって使用されるイベント属性の説明は、Firepower Device Manager（FDM）および Adaptive Security Device Manager（ASDM）によって報告されるものとほぼ同じです。

- 適応型セキュリティアプライアンス（ASA）イベント属性の詳細については、「Cisco ASA シリーズ Syslog メッセージ」を参照してください。

一部の ASA syslog イベントは「解析」され、その他には、属性値ペアを使用してイベントログテーブルの内容をフィルタリングするときに使用できる追加の属性があります。syslog イベントのその他の重要な属性については、次の追加トピックを参照してください。

- 解析済みの ASA Syslog イベント
- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性
- Syslog イベントの EventName 属性
- Syslog イベントの時間属性

一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性

一部の syslog イベントには、追加の属性「EventGroup」および「EventGroupDefinition」があります。属性:値のペアでフィルタ処理することにより、これらの追加属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。たとえば、イベントロギングテーブルの [検索（search）] フィールドに「`apfw:415*`」と入力して、アプリケーション ファイアウォール イベントをフィルタできます。

syslog メッセージのクラスおよび関連付けられているメッセージ ID 番号

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
aaa/auth	ユーザ認証	109、113
acl/session	アクセスリスト/ユーザーセッション	106
apfw	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
citrix	Citrix クライアント	723
clst	クラスタリング	747
cmgr	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	セキュアなデスクトップ	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
ipaa/envmon	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
idfw	Identity-Based ファイアウォール	746
ids	侵入検知システム	733
ids/ips	侵入検知システム/侵入防御システム	400
ikev2	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレスの割り当て	735
ips	侵入防御システム	401、420
ipv6	IPv6	325
l4tm	ブロックリスト、許可リスト、グレーリスト	338
lic	ライセンシング	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
vpn/nap	IKE と IPsec /ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
ospf	OSPF ルーティング	318、409、503、613
passwd	パスワードの暗号化	742
pp	Phone Proxy	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
sch	Smart Call Home	120
session	ユーザ セッション	108、201、202、204、302、303、304、314、405、406、407、500、502、607、608、609、616、620、703、710
session/natpat	ユーザーセッション/NAT および PAT	305
snmp	SNMP	212

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
ssafe	ScanSafe	775
ssl/np ssl	SSL スタック/NP SSL	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
tre	トランザクション ルール エンジン	780
ucime	UC-IME	339
tag-switching	サービス タグ スイッチング	779
td	脅威の検出	733
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
vxlan	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN および AnyConnect クライアント	716
session/natpat	ユーザーセッション/NAT および PAT	305

Syslog イベントの EventName 属性

一部の syslog イベントには、付加的な属性「EventName」が含まれます。EventName 属性を使用して、属性と値のペアでフィルタリングすることにより、イベントテーブルをフィルタリングしてイベントを見つけることができます。たとえば、[イベントロギング] テーブルの検索フィールドに「**EventName:"Denied IP Packet"**」と入力することで、「Denied IP packet」のイベントをフィルタリングできます。

Syslog イベント ID とイベント名のテーブル

AAA Syslog イベント ID とイベント名

EventID	EventName
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	認証に失敗
109007	Authorization Success
109008	「許可に失敗しました（Authorization Failed）」
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error

EventID	EventName
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	「許可に失敗しました（Authorization Failed）」
109025	「許可に失敗しました（Authorization Failed）」
109026	AAA error
109027	AAA Server error
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	認証に失敗
109032	AAA ACL error
109033	認証に失敗
109034	認証に失敗
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved

EventID	EventName
113012	認証成功
113013	AAA error
113014	AAA error
113015	認証を却下
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

ボットネット Syslog イベント ID とイベント名

EventID	EventName
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey

EventID	EventName
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

フェールオーバー Syslog イベント ID とイベント名

EventID	EventName
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch

EventID	EventName
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

ファイアウォール拒否 Syslog イベント ID とイベント名

EventID	EventName
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

ファイアウォール トラフィック Syslog イベント ID とイベント名

EventID	EventName
108001	Inspect SMTP

EventID	EventName
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub

EventID	EventName
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	メモリ エラー
324003	GTP Pkt Drop
324004	GTP Version Not Supported
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session

EventID	EventName
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	IPS ICMP Information Request
400020	IPS ICMP Information Reply
400021	IPS ICMP Address Mask Request
400022	IPS ICMP Address Mask Reply
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic

EventID	EventName
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped

EventID	EventName
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied Packet

EventID	EventName
424002	Dropped Packet
431001	Dropped RTP
431002	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

アイデンティティ ベース ファイアウォール **Syslog** イベント **ID** とイベント名

EventID	EventName
746001	Import started

EventID	EventName
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec Syslog イベント ID とイベント名

EventID	EventName
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure（認証失敗）
402121	Packet dropped
426101	cLACP Port Bundle

EventID	EventName
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT Syslog イベント ID とイベント名

EventID	EventName
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	接続制限の超過
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown

EventID	EventName
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN Syslog イベント ID とイベント名

EventID	EventName
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error

EventID	EventName
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed

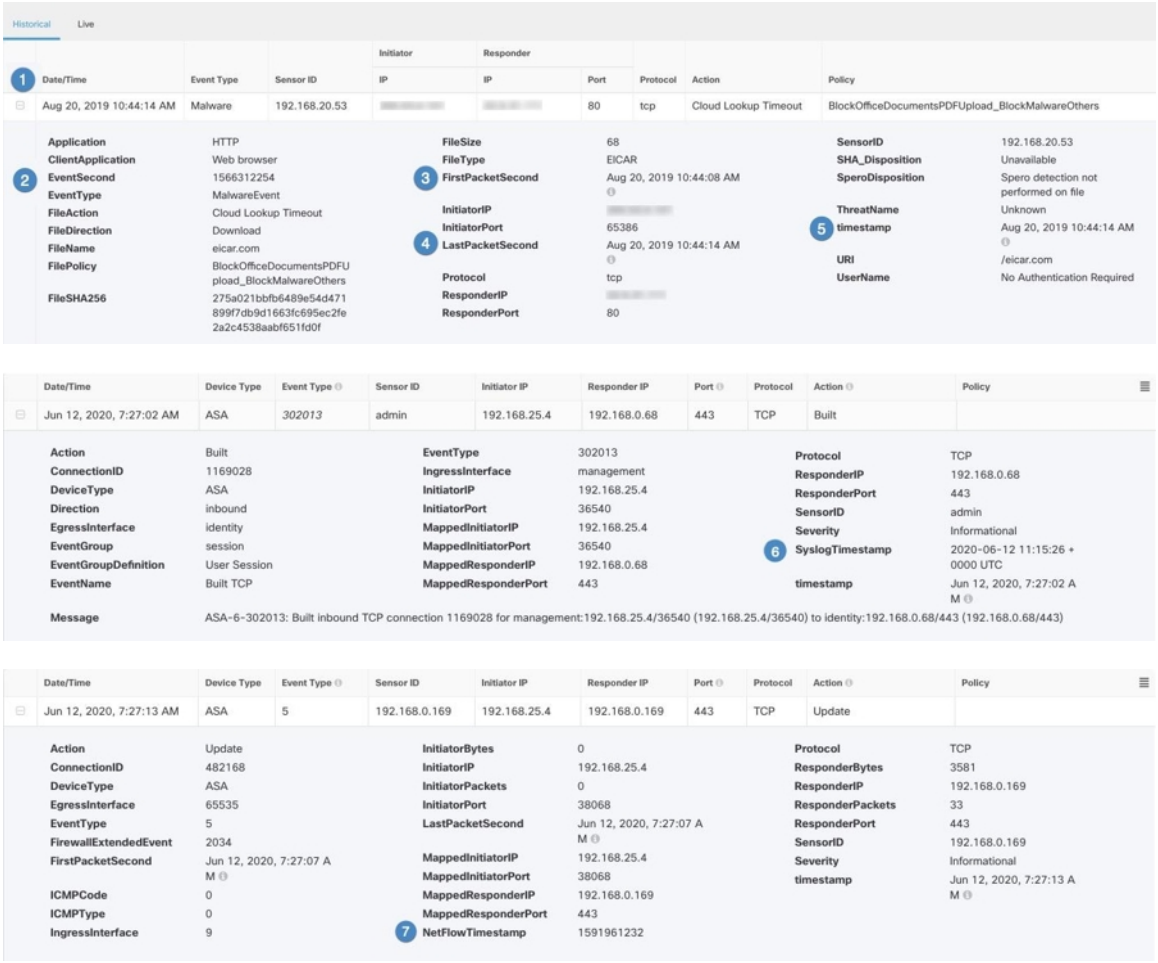
EventID	EventName
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated

EventID	EventName
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS

EventID	EventName
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014	SSL LIB error
725015	SSL client certificate failed

Syslog イベントの時間属性

[イベントロギング]ページのさまざまなタイムスタンプの目的を理解すると、関心のあるイベントをフィルタリングして見つけるのに役立ちます。



番号	ラベル	説明
1	日時	Secure Event Connector（SEC）がイベントを処理した時刻。これは、ファイアウォールでそのトラフィックが検査された時刻と同じではない場合があります。タイムスタンプと同じ値。
2	EventSecond	LastPacketSecond と同じです。

番号	ラベル	説明
3	FirstPacketSecond	接続が開かれた時刻。この時点で、ファイアウォールはパケットを検査します。 FirstPacketSecond の値は、LastPacketSecond から ConnectionDuration を差し引いて計算されます。 接続の開始時にログに記録される接続イベントの場合、FirstPacketSecond、LastPacketSecond、および EventSecond の値はすべて同じになります。
4	LastPacketSecond	接続が閉じた時刻。接続の最後に記録される接続イベントの場合、LastPacketSecond と EventSecond は等しくなります。
5	timestamp	Secure Event Connector（SEC）がイベントを処理した時刻。これは、ファイアウォールでそのトラフィックが検査された時刻と同じではない場合があります。[日時（Date/Time）] と同じ値。
[6]	syslog タイムスタンプ	「ロギングタイムスタンプ」が使用されている場合、syslog の開始時刻を表します。syslog にこの情報がない場合、SEC がイベントを受信した時刻が反映されます。
7	NetflowTimeStamp	ASA で、NetFlow パケットを埋めてフローコレクタに送信するのに十分なフローレコード/イベントの収集が終了した時刻。

Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

Secure Cloud Analytics は、オンプレミスおよびクラウドベースのネットワーク展開をモニターする Software as a Service（SaaS）ソリューションです。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報をソースから収集することによって、トラフィックに関する観測内容が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

ダイナミック エンティティ モデリング

ダイナミック エンティティ モデリングは、ファイアウォールイベントとネットワークフローデータの動作分析を実行することにより、ネットワークの状態を追跡します。Secure Cloud Analytics のコンテキストにおいて、エンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。**Logging Analytics and Detection** ライセンスと統合された Secure Cloud Analytics は、エンティティが通常送信するトラフィックのタイプを判別するために、ファイアウォールイベントやその他のトラフィック情報から引き出すことができます。**Total Network Analytics and Monitoring** ライセンスを購入すると、Secure Cloud Analytics は、エンティティトラフィックのモデル化に NetFlow およびその他のトラフィック情報を含めることもできます。各エンティティの最新のモデルを維持するため、Secure Cloud Analytics では、エンティティがトラフィックを送信し続け、場合によっては異なるトラフィックを送信する可能性があるため、これらのモデルを徐々に更新します。この情報から、Secure Cloud Analytics は以下を識別します。

- エンティティのロール：これは、エンティティが通常行うことの記述子です。たとえば、エンティティが、一般に電子メールサーバーに関連付けられるトラフィックを送信する場合、Secure Cloud Analytics は、そのエンティティに電子メールサーバーロールを割り当てます。エンティティは複数のロールを実行する場合があるため、ロールとエンティティの関係は多対 1 である可能性があります。

- エンティティの観測内容：これは、ネットワーク上でのエンティティの動作に関する事実（外部 IP アドレスとのハートビート接続、別のエンティティとの間で確立されたリモートアクセスセッションなど）です。CDO と統合すると、ファイアウォールイベントからこれらの事実を取得できます。**Total Network Analytics and Monitoring** ライセンスも購入すると、システムは NetFlow から事実を取得し、ファイアウォールイベントと NetFlow の両方から観測内容を生成することもできます。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

アラートと分析

ロール、観測内容、およびその他の脅威インテリジェンスの組み合わせに基づいてSecure Cloud Analyticsが生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。1 つのアラートが複数の観測内容を表す場合があることに注意してください。ファイアウォールが同じ接続とエンティティに関連する複数の接続イベントをログに記録する場合、アラートが 1 つだけになる可能性があります。

上記の例で言えば、新しい内部デバイスの観測内容だけでは、潜在的な悪意のある動作は構成されません。ただし、時間の経過とともに、エンティティがドメイン コントローラと一致するトラフィックを送信する場合、システムではそのエンティティにドメイン コントローラ ロールが割り当てられます。その後、そのエンティティが、以前に接続を確立していない外部サーバーへの接続を確立し、異常なポートを使用して大量のデータを転送すると、システムは、[新しい大規模接続（外部）（New Large Connection (External)）] 観測内容と [例外ドメインコントローラ（Exceptional Domain Controller）] 観測内容をログに記録します。その外部サーバーがTalos ウォッチリストに登録されているものと識別された場合、これらすべての情報の組み合わせによりSecure Cloud Analyticsはこのエンティティの動作に関するアラートを生成し、悪意のある動作を調査して対処するように促します。

Secure Cloud Analytics の Web ポータル UI でアラートを開くと、システムがアラートを生成した原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。また、エンティティが関係性を持っていたその他の観測内容やアラートを確認したり、この動作が他の潜在的に悪意のある動作に結び付いているかどうかを判断することもできます。

Secure Cloud Analytics でアラートを表示して閉じる場合、Secure Cloud Analytics UI からのトラフィックを許可またはブロックできないことに注意してください。デバイスをアクティブモードで展開した場合、ファイアウォール アクセス コントロール ルールを、トラフィックを許可またはブロックするように更新する必要があり、ファイアウォールがパッシブモードで展開されている場合は、ファイアウォールアクセスコントロールルールを更新する必要があります。

ファイアウォールイベントに基づくアラートの使用

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

アラートのワークフロー

アラートのワークフローは、そのステータスに基づいて異なります。システムによってアラートが生成される場合、そのデフォルト ステータスは [オープン（Open）] であり、ユーザーは割り当てられません。アラートのサマリーを表示すると、デフォルトでは、当面注意が必要なすべてのオープン アラートが表示されます。

注：**Total Network Analytics and Monitoring** ライセンスを持っている場合、アラートは、NetFlow から生成された観測結果、ファイアウォールイベントから生成された観測結果、または両方のデータソースからの観測結果に基づいて生成できます。

アラートのサマリーを確認する際は、初期トリアージとして、アラートにステータスを割り当て、タグ付けし、更新することができます。フィルタ機能と検索機能を使用して、特定のアラートを検索したり、さまざまなステータスのアラートを表示したり、さまざまなタグや割り当て対象を関連付けたりすることができます。アラートのステータスは[スヌーズ（Snoozed）]に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。アラートから [スヌーズ（Snoozed）] ステータスを削除して、再びオープンアラートとして表示されるようにすることもできます。アラートを確認する際は、それらのアラートをそのユーザー自身またはシステム内の別のユーザーに割り当てることができます。ユーザーは、自分のユーザー名に割り当てられているすべてのアラートを検索できます。

アラートのサマリーから、アラートの詳細ページを表示できます。このページでは、このアラートを生成させた、裏付けとなる観測内容に関する追加のコンテキストと、このアラートに関連するエンティティに関する追加のコンテキストを確認できます。この情報は、ネットワーク上の問題をさらに調査して悪意のある動作を潜在的に解決するために実際の問題を特定する上で役立ちます。

CDO の Stealthwatch Cloud Web ポータル UI 内やネットワーク上で調査しているときに、発見した内容を説明するコメントをアラートと一緒に残すことができます。これは、将来参照できる調査の記録を作成するために役立ちます。

分析が完了したら、ステータスを[クローズ（Closed）]に更新できます。これにより、デフォルトではオープンアラートとして表示されなくなります。将来、状況が変わった場合は、クローズ アラートのステータスを再度オープンにすることもできます。

ここでは、特定のアラートを調査する方法に関する一般的なガイドラインと推奨事項を示します。Stealthwatch Cloud はアラートをログに記録するときに追加のコンテキストを提供するため、このコンテキストを参照しながら調査を進めることができます。

これらの手順は、総合的または包括的であることを意図したものではありません。これらは単にアラートの調査を開始するための一般的な枠組みを提供するためのものです。

一般に、次の手順でアラートを確認できます。

1. オープンアラートのトリアージ （87 ページ）
2. 後で分析するためにアラートをスヌーズする （88 ページ）
3. 詳細な調査のためのアラートの更新 （89 ページ）
4. アラートの確認と調査の開始 （89 ページ）
5. エンティティとユーザーの調査 （91 ページ）
6. Secure Cloud Analytics を使用して問題を修復する （92 ページ）
7. アラートの更新とクローズ （93 ページ）

オープンアラートのトリアージ

特に複数の調査が必要な場合は、オープンアラートのトリアージを行います。

- CDO から SWC へのクロス起動とアラート表示の詳細については、「Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示」を参照してください。

次の質問に答えてください。

- このアラート タイプを優先度の高いものとして設定しましたか。
- 影響を受けるサブネットに高い機密性を設定しましたか。
- この異常な動作はネットワーク上の新しいエンティティによるものですか。
- エンティティの通常のロールは何ですか。また、このアラートの動作はそのロールにどのように適合しますか。
- これは、このエンティティの通常の動作からの例外的な逸脱ですか。
- ユーザーが関与している場合、これはユーザーの予想される動作ですか、それとも例外的な動作ですか。
- 保護されたデータや機密データが侵害を受けるリスクがありますか。
- この動作の継続を許可すると、ネットワークへの影響はどの程度深刻になりますか。
- 外部エンティティとの通信がある場合、それらのエンティティは過去にネットワーク上の他のエンティティとの接続を確立しましたか。

これが優先順位の高いアラートである場合は、調査を進める前に、インターネットからエンティティを隔離するか、隔離しないときは接続を切断することを検討してください。

後で分析するためにアラートをスヌーズする

他のアラートと比較して優先度が低いときに、アラートをスヌーズします。たとえば、組織が電子メールサーバーをFTPサーバーとして再利用する場合、緊急プロファイルアラートが生成されます（エンティティの現在のトラフィックが、以前には一致しなかった動作プロファイルと一致することを示します）。これは想定される動作であるため、このアラートをスヌーズして、後日再検討できます。スヌーズされたアラートは、オープンアラートと一緒に表示されません。これらのスヌーズされたアラートを確認するには、特別にフィルタリングする必要があります。

アラートをスヌーズする：

ステップ 1 [アラートを閉じる（Close Alert）] をクリックします。
ステップ 2 [このアラートをスヌーズ（Snooze this alert）] ペインで、ドロップダウンからスヌーズ期間を選択します。
ステップ 3 [保存（**Save**）] をクリックします。

次のタスク

スヌーズしたアラートを確認する準備ができたら、アラートのスヌーズを解除できます。これにより、ステータスが[オープン（Open）]に設定され、他のオープンアラートとともにアラートが表示されます。

スヌーズしたアラートのスヌーズを解除する：

- スヌーズしたアラートから、[アラートのスヌーズ解除（Unsnooze Alert）]をクリックします。

詳細な調査のためのアラートの更新

アラートの詳細情報を確認します。

ステップ 1 **[モニター（Monitor）]** > **[アラート（Alerts）]** を選択します。

ステップ 2 アラートタイプ名をクリックします。

次のタスク

初期トリアージと優先順位付けに基づいて、アラートを割り当て、タグを付けます。

1. [担当者（Assignee）] ドロップダウンからユーザーを選択してアラートを割り当てます。これにより、ユーザーが調査を開始できるようになります。
2. [タグ（Tags）] ドロップダウンから 1 つ以上のタグを選択して、アラートにタグを追加することにより、将来の識別のためにアラートをより適切に分類したり、アラートの長期的なパターンの確立を試みることができます。
3. 必要に応じて、**このアラートに関するコメント**を入力し、[コメント（Comment）]をクリックすることにより、最初の調査結果を追跡するためのコメントを残し、アラートに割り当てられた担当者を支援することができます。アラートは、システムコメントとユーザーコメントの両方を追跡します。

アラートの確認と調査の開始

割り当てられたアラートを確認する場合は、アラートの詳細を確認して、Stealthwatch Cloud がアラートを生成した理由を把握してください。裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。

アラートがファイアウォールイベントに基づいて生成された場合、ファイアウォールの展開がこのアラートのソースであることはシステムに認識されません。

このソースエンティティの一般的な動作やパターンを理解するために、サポートされている観測内容をすべて表示し、このアクティビティがより長いトレンドの一部である可能性があるかどうかを確認します。

手順の概要

1. アラートの詳細で、観測タイプの横にある矢印アイコン（）をクリックして、そのタイプの記録されたすべての観測内容を表示します。
2. [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

手順の詳細

ステップ 1 アラートの詳細で、観測タイプの横にある矢印アイコン（）をクリックして、そのタイプの記録されたすべての観測内容を表示します。

ステップ 2 [ネットワークのすべての観測内容（All Observations for Network）] の横にある矢印アイコン（）をクリックして、このアラートのソースエンティティの記録された観測内容をすべて表示します。

観測内容に対して追加の分析を実行する場合は、サポートされている観測内容をコンマ区切り値ファイルでダウンロードします。

- アラートの詳細の [サポートされている観測内容（Supporting Observations）] ペインで、[CSV] をクリックします。

観測内容から、ソースエンティティの動作が悪意のある動作を示しているか判断します。ソースエンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか（それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど）を確認します。

ソースエンティティの IP アドレスまたはホスト名から、ソースエンティティに関連する追加コンテキスト（関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、送信しているセッショントラフィックのタイプなど）を表示します。

- エンティティに関連するすべてのアラートを表示するには、IPアドレスまたはホスト名のドロップダウンから [アラート（Alerts）] を選択します。
- エンティティに関連するすべての観測内容を表示するには、IPアドレスまたはホスト名のドロップダウンから [観測内容（Observations）] を選択します。
- デバイスに関する情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [デバイス] を選択します。
- このエンティティに関連するセッショントラフィックを表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー] を選択します。

Stealthwatch Cloud のソースエンティティは常にネットワークの内部にあることに注意してください。この点を、接続を開始したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのイニシエータ IP と比較してください。

観測内容から、他の外部エンティティに関する情報を調べます。地理位置情報を調査し、いずれかの地理位置情報データまたは Umbrella データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワーク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。

ソースエンティティが接続を確立した外部エンティティの IP アドレスまたはホスト名のコンテキストを確認します。

- このエンティティの最近のトラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [IPトラフィック（IP Traffic）] を選択します。
- このエンティティの最近のセッショントラフィック情報を表示するには、IPアドレスまたはホスト名のドロップダウンから [セッショントラフィック（Session Traffic）] を選択します。
- AbuseIPDB の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [AbuseIPDB] を選択します。
- Cisco Umbrella の Web サイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Cisco Umbrella] を選択します。
- Google でこの IP アドレスを検索するには、IP アドレスまたはホスト名のドロップダウンから [Google検索（Google Search）] を選択します。
- Talos の Web サイト上でこの情報に関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから [Talos Intelligence] を選択します。
- このエンティティをウォッチリストに追加するには、IPアドレスまたはホスト名のドロップダウンから [IPをウォッチリストに追加（Add IP to watchlist）] を選択します。
- 前月のこのエンティティのトラフィックを検索するには、IPアドレスまたはホスト名のドロップダウンから [複数日のIPを検索（Find IP on multiple days）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから [コピー（Copy）] を選択します。

Stealthwatch Cloud の接続エンティティは、常にネットワークの外部にあることに注意してください。この点を、接続要求に応答したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのレスポンダ IP と比較してください。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

エンティティとユーザーの調査

Stealthwatch Cloud ポータル UI でアラートを確認した後、ソースエンティティ、このアラートに関係している可能性のあるユーザー、およびその他の関連エンティティに対して、追加の調査を直接実行できます。

- ソースエンティティがネットワーク上のどこ（物理的またはクラウド上）にあるかを特定し、直接アクセスします。このエンティティのログファイルを見つけます。それがネットワーク上の物理エンティティである場合は、デバイスにアクセスしてログ情報を確認し、この動作の原因となっているものに関する情報があるかどうかを確認します。それが仮想エンティティである場合またはクラウドに保存されている場合は、ログにアクセスして、このエンティティに関連するエントリを検索します。不正なログイン、承認されていない設定変更などに関する詳細について、ログを調査します。
- エンティティを調査します。マルウェアまたはエンティティ自体にある脆弱性を特定できるかどうかを判断してください。デバイスの物理的な変更（組織によって承認されていない USB スティックなど）を含め、何らかの悪意のある変更があったかどうかを確認します。
- ネットワーク上のユーザーまたはネットワーク外のユーザーによる関与があったかどうかを確認します。可能であれば、何をしていたのかをユーザーに尋ねてください。ユーザーに尋ねることができない場合は、そのユーザーがアクセス権を持っていたと考えられるかどうかと、この動作を促す状況（解雇された従業員が退社する前に外部サーバーにファイルをアップロードするなど）が発生したかどうかを確認します。

調査結果に関するコメントを残します。

- [アラートの詳細（ alert detail）] で、[このアラートに関するコメント（Comment on this alert）] を入力し、[コメント（Comment）] をクリックします。

アラートの更新とクローズ

調査結果に基づいてタグを追加します。

ステップ 1 Secure Cloud Analytics ポータルの UI で、**[監視]** > **[アラート]**を選択します。

ステップ 2 ドロップダウンから 1 つ以上の**タグ**を選択します。

調査結果と実行された修正手順を説明する最終コメントを追加します。

- アラートの詳細で、[このアラートに関するコメント] を入力し、[コメント] をクリックします。

アラートのステータスをクローズにして、役立つものかどうかが分かるようにマークします。

1. アラートの詳細から、[アラートを閉じる] をクリックします。

2. アラートが役立った場合は[はい]を、アラートが役立たなかった場合は[いいえ]を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味する点に注意してください。
3. [保存（**Save**）]をクリックします。

次のタスク

クローズしたアラートの再オープン

クローズしたアラートに関連する追加情報を検出した場合、またはそのアラートに関連するコメントを追加する場合は、そのアラートを再度開いてステータスを[オープン（Open）]に変更できます。その後、必要に応じてアラートを変更し、追加調査が完了したら再度閉じます。

クローズしたアラートを再オープンします。

- クローズしたアラートの詳細から、[アラートを再オープン]をクリックします。

アラートの優先順位を変更する

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

アラートタイプにはデフォルトの優先順位が設定されています。これは、このタイプのアラートを生成するシステムの機密性に影響します。アラートの優先順位は、シスコのインテリジェンスおよびその他の要因に基づいて、[低]または[通常]にデフォルト設定されます。ネットワーク環境に基づいて、関心のある特定のアラートを強調するために、アラートタイプの優先順位を変更することができます。アラートタイプの優先順位は、[低]、[通常]、または[高]に設定できます。

- **[モニター]** > **[アラート]** を選択します。
- 設定のドロップダウンアイコン（）をクリックし、[アラートのタイプと優先順位]を選択します。
- アラートタイプの横にある編集のアイコン（）をクリックし、[低]、[中]、または[高]を選択して優先順位を変更します。

イベントロギングページでのイベントの検索とフィルタリング

特定のイベントの履歴イベントテーブルとライブイベントテーブルの検索とフィルタ処理は、CDOで他の情報を検索してフィルタ処理する場合と同様に機能します。フィルタ条件を追加すると、CDOは[イベント（Events）]ページに表示される内容を制限し始めます。検索フィールドに検索条件を入力して、特定の値を持つイベントを検索することもできます。フィルタリ

ングと検索のメカニズムを組み合わせると、検索はイベントのフィルタリング後に表示される結果の中から、入力した値を見つけようとします。

ライブイベントのフィルタリングは、履歴イベントの場合と同じように機能しますが、ライブイベントは時刻でフィルタリングできない点が異なります。

次のフィルタリング方法について説明します。

- ライブまたは履歴イベントのフィルタ処理 （138 ページ）
- NetFlow イベントのみフィルタ処理 （140 ページ）
- ASA または FTD Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない （140 ページ）
- フィルタ要素の結合 （141 ページ）

ライブまたは履歴イベントのフィルタ処理

この手順では、イベントフィルタリングを使用して、[イベントロギング]ページでイベントのサブセットを表示する方法について説明します。特定のフィルタ条件を繰り返し使用する場合は、カスタマイズしたフィルタを作成して保存できます。詳細については、「カスタマイズ可能なイベントフィルタ」を参照してください。

ステップ 1 ナビゲーションバーで、**[モニタリング（Monitoring）] > [イベントロギング]** をクリックします。

ステップ 2 [履歴] タブまたは [ライブ] タブをクリックします。

ステップ 3 フィルタボタン をクリックします。フィルタリング列は、ピンアイコン をクリックして開いた状態でピン留めできます。

ステップ 4 保存されているフィルタ要素がない [表示（View）] タブをクリックします。

ステップ 5 フィルタリングするイベントの詳細を選択します。

- **FTD イベントタイプ**
  - 接続：アクセス制御ルールからの接続イベントを表示します。
  - ファイル：アクセス制御ルールのファイルポリシーによって報告されたイベントを表示します。
  - 侵入：アクセス制御ルールの侵入ポリシーによって報告されたイベントを表示します。
  - マルウェア：アクセス制御ルールのマルウェアポリシーによって報告されたイベントを表示します。
- **ASA イベントタイプ**：これらのイベントタイプは、syslog または NetFlow イベントのグループを表します。syslog ID または NetFlow ID が含まれているグループの詳細については、「ASA イベント タイプ」を参照してください。

- 解析されたイベント：解析された syslog イベントには、他の syslog イベントよりも多くのイベント属性が含まれており、CDO はそれらの属性に基づいて検索結果をより迅速に返すことができます。解析済みの ASA Syslog イベント （36 ページ）解析されたイベントはフィルタリングカテゴリではありませんが、解析されたイベント ID は、[イベントタイプ（Event Types）] 列に斜体で表示されます。斜体で表示されていないイベント ID は解析されていません。

- **時間範囲**：[開始時刻（Start time）] または [終了時刻（End time）] フィールドをクリックして、表示する期間の開始時刻と終了時刻を選択します。タイムスタンプは、コンピュータのローカル時間で表示されます。
- **アクション**：ルールによって定義されたセキュリティアクションを指定します。入力する値は、検索対象と完全に一致する必要がありますが、大文字小文字は関係ありません。各イベントタイプ（接続、ファイル、侵入、マルウェア、syslog、および NetFlow）に異なる値を入力します。
  - 接続イベントタイプの場合、フィルタは AC_RuleAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。
  - ファイルイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。
  - 侵入イベントタイプの場合、フィルタは InLineResult 属性で一致を検索します。それらの値は、Allowed、Blocked、Trusted の可能性があります。
  - マルウェアイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、クラウド ルックアップ タイムアウトである可能性があります。
  - syslog および NetFlow イベントタイプの場合、フィルタは Action 属性で一致を検索します。
- **センサー ID**：センサー ID は、イベントが Secure Event Connector に送信される管理 IP アドレスです。Firepower Threat Defense（FTD）デバイスの場合、センサー ID は通常、デバイスの管理インターフェイスの IP アドレスです。
- **IP アドレス**
  - **イニシエータ**：ネットワークトラフィックの送信元の IP アドレスです。イニシエータ アドレス フィールドの値は、イベントの詳細の InitiatorIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
  - **レスポンダ**：パケットの宛先 IP アドレスです。宛先アドレスフィールドの値は、イベントの詳細の ResponderIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
- **ポート**
  - **イニシエータ**：セッションイニシエータが使用するポートまたは ICMP タイプ。送信元ポートの値は、イベントの詳細の InitiatorPort の値に対応します（範囲の追加：開始ポートと終了ポートと、イニシエータとレスポンダの間または両方のスペース）。

- **レスポンダ**：セッションレスポンダが使用するポートまたは ICMP コード。宛先ポートの値は、イベントの詳細の ResponderPort の値に対応します

- **NetFlow**：ASA デバイス向け NetFlow Secure Event Logging（NSEL） イベントは、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの「NetFlow イベント ID」は、Cisco ASA NetFlow 実装ガイド [英語] で定義されています。

ステップ 6 （任意）[表示（View）] タブの側をクリックして、フィルタをカスタムフィルタとして保存します。

ステップ 7 （任意）さらに分析するために、イベントを .CSV.GZ ファイルにダウンロードできます。「イベントのダウンロード」を参照してください。

NetFlow イベントのみフィルタ処理

この手順では、ASA NetFlow イベントのみを検索します。

ステップ 1 CDO メニューバーから、**[モニターリング（Monitoring）] > [イベントロギング]** を選択します。.

ステップ 2 フィルタアイコン をクリックして、開いた状態でフィルタをピン留めします。

ステップ 3 [Netflow] ASA イベントフィルタをオンにします。

ステップ 4 他のすべての ASA イベントフィルタをオフにします。

[イベントロギング] テーブルには、ASA NetFlow イベントのみが表示されます。

ASA または FTD Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない

この手順では、syslog イベントのみを検索します。

ステップ 1 CDO メニューバーから、**[モニタリング（Monitoring）] > [イベントロギング]** を選択します。

ステップ 2 フィルタアイコン をクリックして、開いた状態でフィルタをピン留めします。

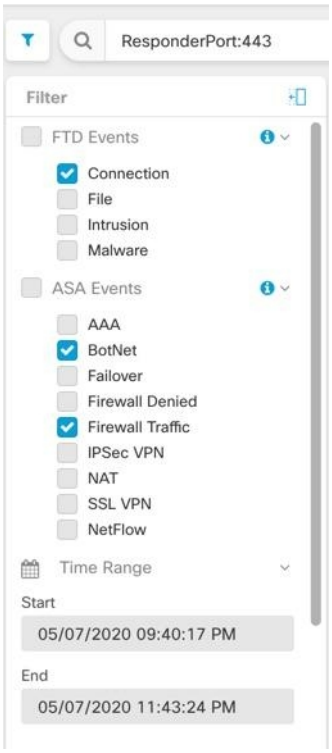
ステップ 3 フィルタバーの一番下までスクロールし、[NetFlowイベントを含める（Include NetFlow Events）] フィルタが**オフ**になっていることを確認します。

ステップ 4 [ASAイベント（ASA Events）] フィルタツリーまでスクロールして戻り、[NetFlow] ボックスが**オフ**になっていることを確認します。

ステップ 5 ASA または FTD フィルタ条件の残りを選択します。

フィルタ要素の結合

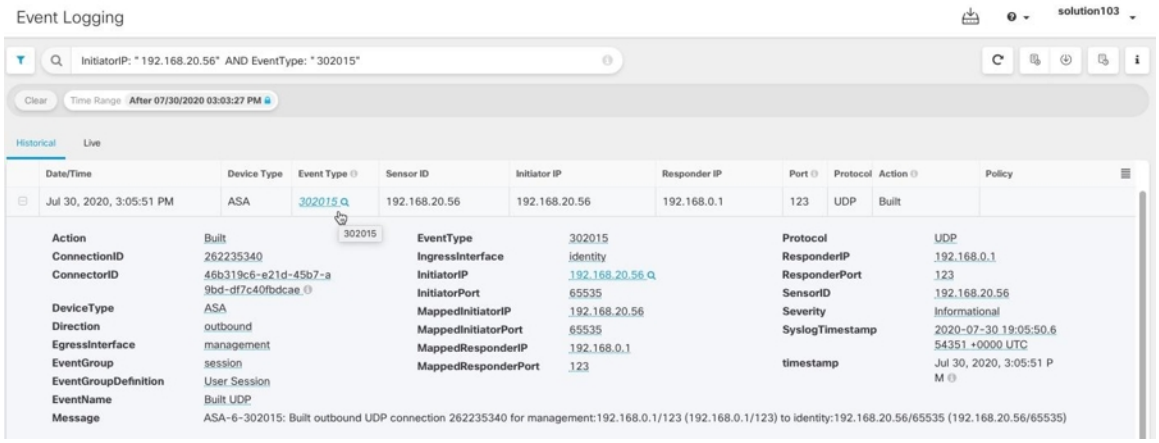
イベントのフィルタリングは、通常、CDO の標準フィルタリングルールに従います。フィルタリングカテゴリには「AND」が適用され、カテゴリ内の値は「OR」が適用されます。フィルタ処理をユーザー独自の検索条件と組み合わせることもできます。ただし、イベントフィルタの場合は、デバイスイベントフィルタにも「OR」が適用されます。たとえば、フィルタで次の値が選択されているとします。



このフィルタを使用すると、CDO では、FTD の接続イベント **OR** ASA ボットネットイベント **OR** ファイアウォール トラフィック イベント、**AND** 時間範囲内の 2 つの時間の間に発生したイベント **AND** ResponderPort 443 も含むイベントが表示されます。時間範囲内の履歴イベントでフィルタ処理できます。ライブイベントページには常に最新のイベントが表示されます。

特定の属性：値ペアの検索

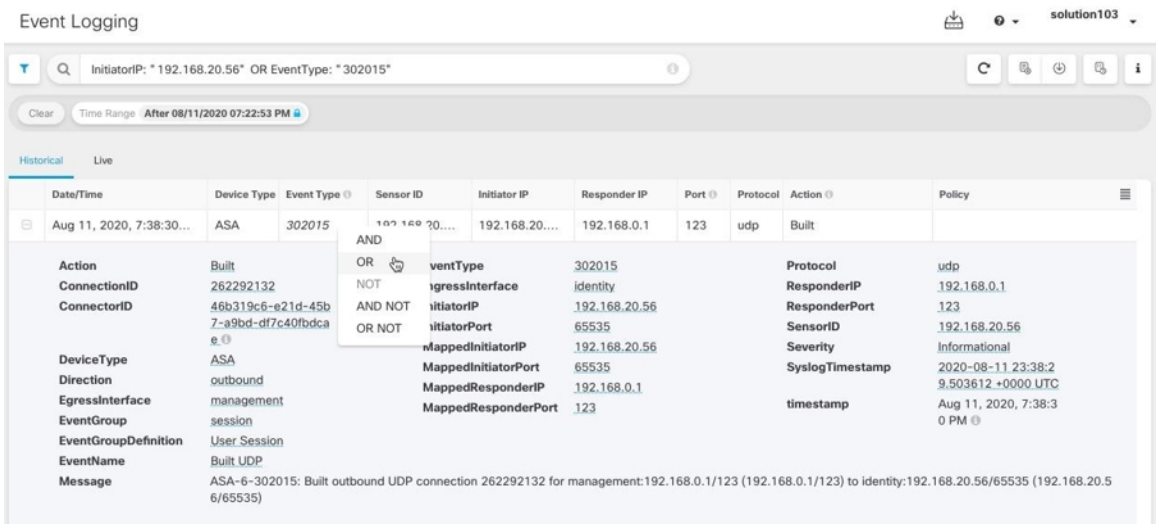
検索フィールドにイベント属性と値を入力することで、ライブイベントや過去のイベントを検索できます。これを行う最も簡単な方法は、イベントロギングテーブルで、検索する属性をクリックすることです。CDO により、その属性が検索フィールドに入力されます。クリックできるイベントは、マウスカーソルを合わせると青色になります。次に例を示します。



この例では、イニシエータ IP の値である 192.168.20.56 にマウスカーソルを合わせてクリックすることにより、検索が開始されています。イニシエータ IP とその値が検索文字列に追加されています。次に、イベントタイプの値である 302015 にマウスカーソルを合わせてクリックし、検索文字列に追加されています。このとき、CDO によって AND が追加されています。そのため、この検索の結果は、192.168.20.56 から開始されたイベント AND イベントタイプが 302015 のイベントのリストになります。

上の例で、値 302015 の横にある虫眼鏡に注目してください。この虫眼鏡にマウスカーソルを合わせ、AND、OR、AND NOT、OR NOT 演算子を選択して、検索に追加する値とともに指定することもできます。次の例では「OR」が選択されています。この検索の結果は、192.168.20.56 から開始されたイベント OR イベントタイプが 302015 のイベントのリストになります。

検索フィールドが空のときにテーブルの値を右クリックした場合は、他の値がないため、「NOT」しか使用できないことに注意してください。



マウスカーソルを合わせると青色で強調表示される値は、検索文字列に追加できます。

AND、OR、NOT、AND NOT、OR NOT フィルタ処理演算子

検索文字列で使用される「AND」、「OR」、「NOT」、「AND NOT」、および「OR NOT」の動作は次のとおりです。

AND

すべての属性を含むイベントを検索するには、フィルタ文字列で AND 演算子を使用します。AND 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、TCP プロトコルを含んだ、「かつ」イニシエータ IP アドレス（InitiatorIP）10.10.10.43 から開始された、「かつ」イニシエータポート（InitiatorPort）59614 から送信されたイベントが検索されます。AND ステートメントを追加するたびに、基準を満たすイベントの数が少なくなることが予期されます。

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

OR

いずれかの属性を含むイベントを検索するには、フィルタ文字列で OR 演算子を使用します。OR 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、TCP プロトコルを含んだ、「または」イニシエータ IP アドレス（InitiatorIP）10.10.10.43 から開始された、「または」イニシエータポート（InitiatorPort）59614 から送信されたイベントがイベントビューアに表示されます。OR ステートメントを追加するたびに、基準を満たすイベントの数が多くなることが予期されます。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT

特定の属性を持つイベントを除外するには、検索文字列の先頭でのみ、これを使用します。たとえば、次の検索文字列では、InitiatorIP が 192.168.25.3 のイベントが結果から除外されます。

```
 NOT InitiatorIP: "192.168.25.3"
```

AND NOT

特定の属性を含むイベントを除外するには、フィルタ文字列で AND NOT 演算子を使用します。AND NOT 演算子は、検索文字列の先頭では使用できません。

たとえば、次のフィルタ文字列では、イニシエータ IP アドレス（InitiatorIP）が 192.168.25.3 のイベントが表示されますが、それらのうち、レスポンダ IP アドレス（ResponderIP）が 10.10.10.1 のものは表示されません。

```
 InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

NOT と AND NOT を組み合わせて、複数の属性を除外することもできます。たとえば、次のフィルタ文字列では、InitiatorIP が 192.168.25.3 のイベントと ResponderIP が 10.10.10.1 のイベントが除外されます。

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

特定の要素を除外する検索結果を含めるには、フィルタ文字列で OR NOT 演算子を使用します。OR NOT 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、プロトコル（Protocol）が TCP のイベント、「または」InitiatorIP が 10.10.10.43 のイベント、「または」InitiatorPort が 59614 ではないイベントが検索されます。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

これは、(Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614") の検索と考えることもできます。

ワイルドカード検索

アスタリスク（*）を「属性：値」ペア検索の「値」フィールドでワイルドカードとして使用して、イベント内の結果を検索することができます。たとえば、次のフィルタ文字列では、

```
URL:*feedback*
```

属性フィールドが「URL」のイベントの文字列が検索され、「feedback」という文字列が含まれているイベントが表示されます。

関連情報：

- イベントのダウンロード
- イベントロギングページの列の表示および非表示
- Security Analytics and Logging のイベント属性

データストレージプラン

Cisco Cloud が導入準備された ASA および FTD から毎日受け取るイベント数を反映したデータストレージプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。データプランは整数量の GB/日で、1 年、3 年、5 年単位でご利用いただけます。取り込み率を判断する最善の方法は、購入する前に Secure Logging Analytics（SaaS）の無料トライアルに参加することです。これにより、イベントボリュームを適切に見積ることができます。

お客様は、自動的に 90 日間のローリングデータストレージを受け取ります。つまり、最新の 90 日間のイベントが Cisco Cloud に保存され、91 日目に削除されます。

お客様は、デフォルトの 90 日間を超える追加のイベント保持にアップグレードしたり、既存のサブスクリプションの発注変更によって日単位のボリューム（GB/日）を追加したりすることができます。課金は、サブスクリプション期間の残りの部分についてのみ日割り計算で行われます。

データ プランの詳細については、『Secure Logging Analytics （SaaS）発注ガイド』を参照してください。

（注） Security Analytics and Logging のライセンスとデータプランをお持ちの場合は、その後は別の Security Analytics and Logging ライセンスを取得するだけで、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで済み、別の Security Analytics and Logging ライセンスを取得する必要はありません。

割り当てに対してどのデータがカウントされますか？

Secure Event Connector に送信されたイベントはすべて、Secure Logging Analytics（SaaS）クラウドに蓄積され、データ割り当てに対してカウントされます。

イベントビューアに表示される内容をフィルタ処理しても、Secure Logging Analytics（SaaS）クラウドに保存されるイベントの数は減りません。イベントビューアに表示されるイベントの数が減るだけです。

イベントは Secure Logging Analytics（SaaS）クラウドに 90 日間保存され、その後消去されます。

ストレージの割り当てをすぐに使い果たしてしまいます。どうすればよいでしょうか？

この問題に対処するには、2 通りのアプローチがあります。

- より多くのストレージをリクエストする。必要なストレージ量の見積りが少なすぎる可能性があります。
- イベントを記録するルールの数を減らす。SSL ポリシールール、セキュリティ インテリジェンス ルール、アクセス制御ルール、侵入ポリシー、ファイルおよびマルウェアポリシーからのイベントをログに記録できます。現在何をログに記録していかを調べてください。考えているほど多くのルールとポリシーからのイベントをログに記録する必要がありますか？

イベントストレージ期間の延長およびイベントストレージ容量の増加

Secure Analytics and Logging のお客様は、これらのライセンシングのいずれかを購入すると、90 日間のイベントストレージを受け取ります。

- **Logging and Troubleshooting**
- **Logging Analytics and Detection**
- **Total Network Analytics and Monitoring**

ライセンスを最初に購入するとき、またはライセンスの有効期間中いつでも、ライセンスをアップグレードして、1 年、2 年、または 3 年分のローリング イベント ストレージを持つことを選択できます。

Security Analytics and Logging のライセンスを初めて購入する際、ストレージ容量をアップグレードするか尋ねられます。「はい」と答えると、購入する PID のリストに追加の製品識別子（PID）が追加されます。

ライセンス期間の途中で、ローリング イベント ストレージを拡張するか、イベントクラウドストレージの量を増やすことを決めた場合、次の手順を実行できます。

ステップ 1 Cisco Commerce のアカウントにログインします。

ステップ 2 自分の Cisco Defense Orchestrator PID を選択します。

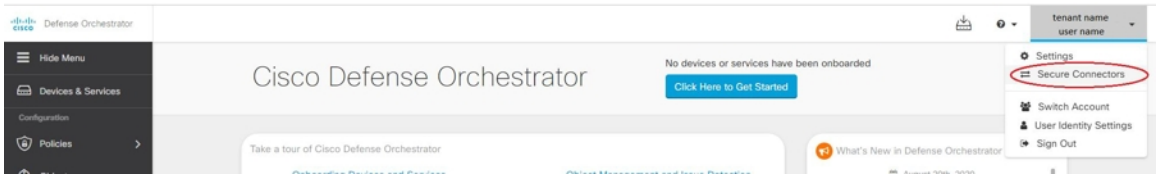
ステップ 3 プロンプトに従って、ストレージ容量の長さまたは容量をアップグレードします。

増加したコストは、既存のライセンスの残りの期間に基づいて比例配分されます。詳細な手順については、Secure Logging Analytics（SaaS）発注ガイド [英語] を参照してください。

セキュリティ分析およびロギングデータプランの使用状況の表示

毎月のロギング制限、使用したストレージ量、いつ使用期間がゼロにリセットされるかを表示するには、次の手順を実行します。

ステップ 1 アカウントメニューをクリックし、[設定] を選択します。



ステップ 2 [ロギングの設定（Logging Settings）] をクリックします。

ステップ 3 [使用履歴の表示（View Historical Usage）] をクリックして、過去 12 ヵ月のストレージ使用状況を表示することもできます。

SecureLoggingAnalytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索

Secure Logging Analytics（SaaS）を使用すると、ご使用の ASA デバイスまたは FTD デバイスから、Secure Event Connector（SEC）上の特定の UDP、TCP、または NSEL ポートにイベントを送信できます。その後、SEC はそれらのイベントを Cisco Cloud に転送します。

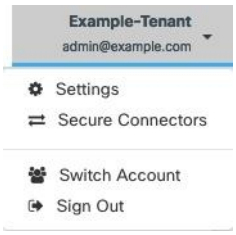
まだ使用されていないポートの場合、SECはそれらのポートを使用してイベントを受信できるようにします。Secure Logging Analytics（SaaS）のマニュアルでは、機能を設定するときにポートを使用することが推奨されています。

- TCP：10125
- UDP：10025
- NSEL：10425

すでに使用されているポートの場合は、Secure Logging Analytics（SaaS）を設定する前に、SECデバイスの詳細を調べて、イベントの受信に実際に使用しているポートを特定します。

SEC が使用するポート番号を見つけるには、次の手順を実行します。

ステップ 1 CDO の任意のページで[アカウント（Account）]メニューを開き、[セキュアコネクタ（Secure Connectors）]を選択します。



ステップ 2 [セキュアコネクタ（Secure Connectors）]ページで、イベントを送信する SEC を選択します。

ステップ 3 [詳細]ペインに、イベントの送信先となる TCP、UDP、および NetFlow（NSEL）ポートが表示されます。