CSM を使用した Cisco ASA と Cisco Security Analytics and Logging（SaaS）の統合

最終更新：2025 年 8 月 12 日

Cisco ASA と Cisco Security Analytics and Logging（SaaS）の統合ガイド

このガイドでは、SAL（SaaS）を使用した ASA の設定方法、SAL（SaaS）でのイベントと syslog メッセージの処理方法、および CDO からのイベントの表示方法について説明します。

概要

syslog および NetFlow セキュアイベントロギング（NSEL）のイベントを外部イベントサービスに送信し、Cisco Cloud にログを保存し、Cisco Defense Orchestrator（CDO）の [Event Logging] ページで表示するように、ASA デバイスを設定できます。[Event Logging] ページでは、イベントのフィルタ処理、ダウンロード、およびセキュリティの問題のトラブルシューティングのための確認を行うことができます。このガイドでは、Cisco Security Manager（CSM）の管理対象 ASA デバイスと Cisco Security Analytics and Logging (SaaS) ソリューションを統合する手順について説明します。

（注） CDO の管理対象 ASA と SAL（SaaS）の統合の詳細については、「Cisco Security Analytics and Logging for ASA Devices」を参照してください。

syslog と NSEL イベント

syslog は、ASA デバイスによって syslog サーバーに送信されるシステムログまたはイベントメッセージで、モニタリングとデバイスの問題のトラブルシューティングに使用されます。syslog メッセージには、イベントのタイプとそのシビラティ（重大度）を示すクラスと ID があります。ASA syslog メッセージの詳細については、『ASA Syslog Guide』を参照してください。

NSEL 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 フロー トラッキング方式です。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。NSEL イベントには同等の syslog メッセージがあります。これらの syslog メッセージは、ファイアウォール拒否およびファイアウォール トラフィックとして CDO イベントフィルタで分類されます。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。詳細については、『Cisco ASA NetFlow Implementation Guide』を参照してください。

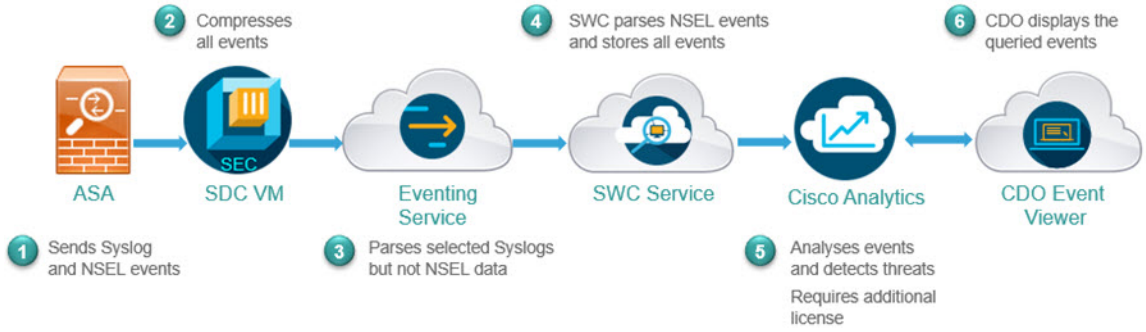
（注） SWC サービスを利用するには、NSEL がデータを SAL（SaaS）に送信できるようにする必要があります。

ASA と SAL（SaaS）の統合のコンポーネント

- Cisco Security Manager（CSM）：ASA デバイスを管理するネットワーク管理ツール。
- オンプレミスの Secure Device Connector（SDC）：SDC は CDO と ASA の間の通信を処理します。オンプレミス SDC は、ネットワークのハイパーバイザにインストールされる仮想アプライアンスです。シスコが提供するイメージを使用してオンプレミス SDC を作成することも、独自の VM を作成して SDC をインストールすることもできます。
- Secure Event Connector（SEC）：ASA デバイスからイベントを受信して Cisco Cloud に転送する、オンプレミスの Secure Device Connector（SDC）にインストールされるアプリケーション。
- Stealthwatch Cloud（SWC）：ネットワークから収集されたイベントの詳細な分析を提供する、クラウドベースの分析ソリューション。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。
- Cisco Defense Orchestrator（CDO）：CDO はクラウドベースのマルチデバイスマネージャで、ローカル ASA デバイスマネージャ（具体的には ASDM）および SSH 接続と共存します。CDO アカウントを使用すると、Cisco Cloud に保存されている ASA イベントログを表示できます。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 Stealthwatch Cloud ポータルを相互起動できます。

次での ASA イベントフロー： SAL（SaaS）

統合が成功した後の SAL での ASA イベントのフローを次に示します。



1. ASA は、CDO で設定された SDC VM の SEC コンポーネントにイベント（syslog および NSEL イベント）を送信します。

2. SEC は ASA から TCP と UDP の両方の syslog を受け入れ、イベントを圧縮します。その後、イベントは Cisco Cloud に安全に転送されます。SEC は、圧縮されたイベントをクラウドベースのイベントサービスに送信します。

（注） イベントは、データの安全な転送を確保するために圧縮されます。データサブスクリプションおよび過去の月次使用量は、この圧縮データでは評価されません。これらは、使用する非圧縮データで評価されます。

3. イベントサービスは syslog イベントを解析します。NSEL データは解析しません。syslog イベントと NSEL データの両方を、Stealthwatch Cloud（SWC）ソリューションに転送します。
4. SWC は NSEL を解析し、結果を syslog イベントとともに保存します。
5. Cisco Analytics サービスは、イベントを分析し、観測結果に基づいて脅威を検出します。このサービスを利用するには、Logging Analytics and Detection ライセンスまたは Total Network Analytics and Detection ライセンスが必要です。
6. CDO イベントビューアには、フィルタ条件に基づいて Cisco Cloud に保存されているイベントが表示されます。

SAL（SaaS） 統合の要件と前提条件

要件または前提条件のタイプ	要件
ASA	Cisco Security Manager（CSM）リリース 4.4 以降。 ソフトウェアリリース 9.0 以降を実行している ASA。 アプライアンスが展開され、イベントを正常に生成している必要があります。
地域のクラウド	• ファイアウォールイベントの送信に使用するシスコ地域クラウドを決定します。 • 複数の地域クラウドのデータをマージまたは集約することはできません。複数の地域からデータを集約するには、すべての地域のデバイスが同じ地域クラウドにデータを送信する必要があります。 イベントは、異なる地域のクラウドから表示したり、異なる地域のクラウド間で移動することはできません。 •

要件または前提条件のタイプ	要件
データプラン	システムに必要なクラウドストレージの容量を決定します。詳細については、ストレージ要件の計算とデータプランの購入 （5 ページ）を参照してください。
ライセンシング	• Cisco Security Analytics and Logging ライセンス：任意 ライセンスのオプションと説明については、SAL（SaaS） ライセンス （4 ページ）を参照してください。 • CDO ライセンス：追加の CDO ライセンスは必要ありません。 • Secure Cloud Analytics ライセンス：追加のライセンスは必要ありません。 • ASA ライセンス：追加のライセンスは必要ありません。 ASA のシスコ スマート ソフトウェア ライセンシングの詳細については、*CLI ブック 1：Cisco ASA シリーズの一般操作 CLI 構成ガイド* のCisco スマート ソフトウェア ライセンシングの項を参照してください。
アカウント（Accounts）	この統合のライセンスを購入すると、この機能をサポートする CDO テナント アカウントが提供されます。
追加の前提条件	各手順のはじめる前にまたは前提条件を参照してください。

SAL（SaaS） ライセンス

ライセンス	詳細
無料トライアル	30 日間の無料トライアルライセンスを取得するには、https://www.defenseorchestrator.com/provision にアクセスしてください。
Logging and Troubleshooting	イベントを Cisco Cloud に保存し、CDO の Web インターフェイスを使用して、保存されたイベントを表示およびフィルタ処理します。

ライセンス	詳細
（オプション）Logging Analytics and Detection	システムは、ASA イベントに Secure Cloud Analytics の動的エンティティモデリングを適用し、行動モデリング分析を使用して Secure Cloud Analytics の観測値とアラートを生成することができます。Cisco Single Sign-On を使用して、プロビジョニングされた Secure Cloud Analytics ポータルを CDO からクロス起動できます。 SAL のライセンスを購入すると、ログを表示するための CDO テナントへのアクセスと、脅威を検出するための Secure Cloud Analytics インスタンスが提供されます。SAL のユーザーは、これらの 2 つのポータルにアクセスして SAL が提供する結果を確認するために個別の CDO ライセンスまたは Secure Cloud Analytics ライセンスを必要としません。
（オプション）Total Network Analytics and Detection	システムは、ASA 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 Secure Cloud Analytics ポータルを CDO からクロス起動できます。 SAL のライセンスを購入すると、ログを表示するための CDO テナントへのアクセスと、脅威を検出するための Secure Cloud Analytics インスタンスが提供されます。SAL のユーザーは、これらの 2 つのポータルにアクセスして SAL が提供する結果を確認するために個別の CDO ライセンスまたは Secure Cloud Analytics ライセンスを必要としません。

SAL（SaaS） ライセンスは、CDO テナントを使用してファイアウォール ログを表示する権利と、分析用の Secure Cloud Analytics インスタンスを提供します。これらの製品のいずれかを使用するために個別のライセンスを保持する必要はありません。

SAL（SaaS） ライセンスを購入するには、シスコの認定セールス担当者に問い合わせるか、発注ガイド（前述のリンク） にアクセスして SAL-SUB で始まる PID を検索してください。

ストレージ要件の計算とデータプランの購入

Cisco Cloud が 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。

データストレージ要件を見積もるには、次の手順を実行します。

- （推奨）購入前に Cisco Security Analytics and Logging (SaaS) の無料トライアルに参加します。SAL（SaaS） ライセンス （4 ページ） を参照してください。
- https://ngfwpe.cisco.com/ftd-logging-estimator でロギングボリューム見積ツールを使用します。

データプランは、さまざまな日単位およびさまざまな年単位で利用できます。データプランの詳細については、『*Cisco Security Analytics and Logging Ordering Guide*』（https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html）を参照してください。

（注） SAL（SaaS）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、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、別の SAL（SaaS） ライセンスを取得する必要はありません。

Syslog を使用した SAL（SaaS） でのイベントデータストレージの設定方法

	操作手順	詳細情報
ステップ	要件と前提条件を確認する	SAL（SaaS） 統合の要件と前提条件 （3 ページ） を参照してください。
ステップ	必要なライセンス、アカウント、およびデータストレージプランを取得する	シスコの認定営業担当者にお問い合わせください。
ステップ	多要素認証を使用して CDO アクセスをセットアップする	CDO へのサインインについては、CDO のオンラインヘルプに記載されている手順を参照してください。 https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/0015_Signing_on_to_CDO

	操作手順	詳細情報
ステップ	VMWare仮想マシンでオンプレミスの Secure Device Connector（SDC）をセットアップする	このコンポーネントは、ASA デバイスがイベントを送信するコンポーネントである SEC のインストールを可能にするためにのみ必要です。 CDO のオンラインヘルプの説明に従って、次のいずれかを使用します。 • （推奨）CDO 提供の VM イメージを使用します。 • CDO 提供のイメージを使用せずに SDC を作成します。 **重要**手順の前提条件を省略しないでください。ただし、この統合には適用されないオンボーディングに関する情報は無視してください。
ステップ	作成した SDC 仮想マシンに Secure Event Connector（SEC）をインストールします。	これは、ASA デバイスがイベントを送信するコンポーネントです。 Secure Event Connector をインストールするには、CDO のオンラインヘルプを参照してください。 **重要**手順の前提条件を省略しないでください。ただし、この統合には適用されないオンボーディングに関する情報は無視してください。
ステップ	ASA に syslog イベントと NSEL イベントを SEC に送信させるように CSM を設定します。	ASA デバイスから syslog イベントを送信するための CSM 設定 （8 ページ）およびASA デバイスから NSEL イベントを送信するための CSM 設定 （11 ページ）
ステップ	イベントが正常に送信されていることを確認する	イベントの表示および操作 （13 ページ）を参照してください。
ステップ	（任意）CDO の一般設定を指定する	たとえば、シスコのサポートスタッフがデータを使用できないようにすることができます。 CDO のオンラインヘルプで、「一般設定」を参照してください。

	操作手順	詳細情報
ステップ	（任意）同僚がイベントを表示および操作するための CDO ユーザーアカウントを作成する	CDO のオンラインヘルプで、「新規 CDO ユーザーの作成」を参照してください。

CDO から SEC の IP およびポート番号を取得する方法

Cisco Cloud に接続するように ASA デバイスを設定するときには、SEC の IP とそのポート番号が必要です。CDO から SEC の詳細を取得するには、次の手順を実行します。

手順

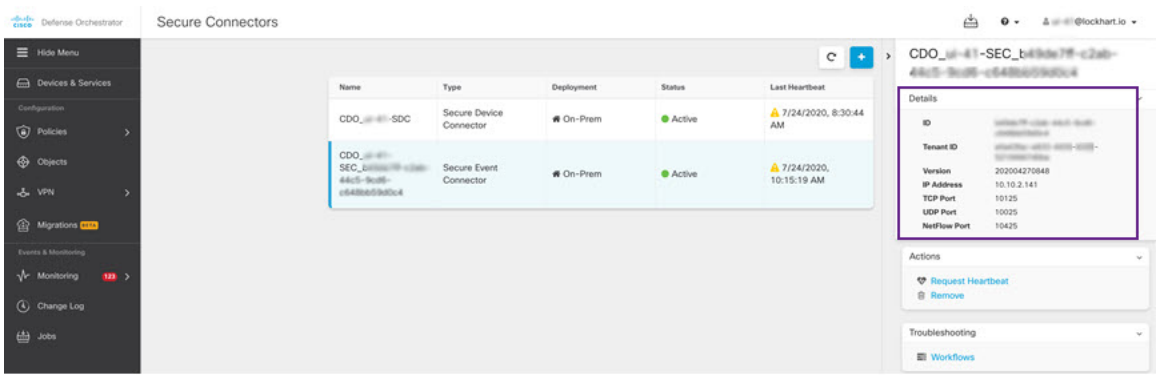
ステップ 1 CDO にサインインします。

ステップ 2 CDO ブラウザウィンドウの右上にある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。

ステップ 3 [Secure Connectors] リストで、目的の SEC をクリックします。

ステップ 4 [Details] セクションで、設定されている IP アドレス、TCP、UDP、および NetFlow のポート番号を探します。

図 *1: SEC の IP* およびポート番号の取得



ASA デバイスから syslog イベントを送信するための CSM 設定

この手順では、セキュリティイベントの ASA syslog メッセージを SAL（SaaS） に送信するための Cisco Security Manager（CSM）の設定について説明します。

始める前に

- 要件と前提条件のセクションを確認します。
- SAL（SaaS） でイベントデータストレージをセットアップします。
- ASA デバイスが SEC に到達できることを確認します。
- カスタム Linux VM に SDC をインストールした場合は、SEC が ASA syslog を受信することを確認します。
- CDO から SEC の IP アドレスとポート番号を取得します。
- EMBLEM ロギング形式とセキュアロギングは、この統合ではサポートされていません。

手順

ステップ 1 Cisco Security Manager の [設定マネージャ（Configuration Manager）] ウィンドウにログインします。

ステップ 2 syslog ロギングを有効にします。

a) 次のいずれかを実行して [syslog ロギングのセットアップ（Syslog Logging Setup）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[ロギングのセットアップ（Logging Setup）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[ロギングのセットアップ（Logging Setup）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

b) [syslog ロギングのセットアップ（Syslog Logging Setup）] ページで、[ロギングの有効化（Enable Logging）] チェックボックスをオンにして syslog ロギングをオンにします。[**保存（Save）**] をクリックします。

（注）
この統合は EMBLEM 形式をサポートしていません。そのため、[EMBLEM で syslog を送信（Send syslogs in EMBLEM）] チェック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 3 syslog サーバー（SEC）のロギングフィルタ設定を指定します。

a) ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[ロギングフィルタ（Logging Filters）]** を選択します。

b) テーブルの [ロギングの宛先（Logging Destination）] 列で [syslog サーバー（Syslog Servers）] を選択し、[編集（Edit）] をクリックします。syslog サーバーオブジェクトが見つからない場合は、[行の追加（Add Row）] をクリックします。

c) [ロギングフィルタの追加/編集（Add/Edit Logging Filters）] ダイアログボックスで、次のいずれかのロギングフィルタ設定を選択します。

- 重大度に基づいて syslog メッセージをフィルタ処理するには、[重大度によるフィルタ（Filter on severity）] をクリックし、重大度を選択します。

（注）
ASA は、指定されたレベルまでの重大度のシステムログメッセージを生成します。

- メッセージ ID に基づいて syslog メッセージをフィルタ処理するには、[イベントリストの使用（Use event list）] をクリックし、ドロップダウンリストから任意のイベントリストを選択します。

（注）
イベントリストが定義されていない場合、ドロップダウンリストは空白になります。少なくとも 1 つのイベントリストを定義する必要があります（**[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[イベントリスト（Event Lists）]**）。

d) 設定を保存します。

ステップ 4 （任意）ロギングパラメータを設定します。

a) （デバイスビュー）**[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[サーバーのセットアップ（Server Setup）]** を選択します。

b) syslog メッセージのタイムスタンプ形式を設定するには、[各 syslog メッセージのタイムスタンプの有効化（Enable Timestamp on Each Syslog Message）] チェックボックスをオンにして、[タイムスタンプ形式の有効化（rfc5424）（Enable Timestamp Format(rfc5424)）] チェックボックスをオンにします。

（注）
RFC5424 は、ASA 9.10(1) 以降でのみサポートされています。

c) （任意）syslog メッセージをデバイス ID とともに表示するように ASA を設定します。

- [インターフェイス（Interface）]：このオプションボタンをクリックして、ASA デバイスのインターフェイスを選択します。
- [ユーザー定義 ID（User Defined ID）]：このオプションボタンをクリックして、ASA デバイスのすべての syslog メッセージに追加する目的の名前を入力します。
- [ホスト名（Host Name）]：syslog メッセージをデバイスのホスト名とともに表示するには、このオプションボタンをクリックします。

（注）
syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。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。

d) **[保存（Save）]** をクリックします。

ステップ 5 syslog メッセージの宛先となる外部ロギングサーバーを設定します。

a) 次のいずれかを実行して [syslog サーバー（Syslog Servers）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[syslog サーバー（Syslog Servers）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]** > **[ロギング（Logging）]** > **[syslog サーバー（Syslog Servers）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

b) [追加（Add）] をクリックして、新しい Syslog サーバーを追加します。

c) [syslog サーバーの追加/編集（Add/Edit Syslog Server）] ダイアログボックスで、次を指定します。

- [インターフェイス（Interface）]：syslog サーバーとの通信に使用するインターフェイス。
- [IP アドレス（IP Address）]：CDO から取得した SEC IP（手順については、「はじめる前に」を参照）。
- [プロトコル（Protocol）]：TCP または UDP を選択します。
- [ポート（Port）]：CDO から取得した、対応する SEC ポート番号（手順については、「はじめる前に」を参照）。

（注）
UDP を選択した場合は、[メッセージを Cisco EMBLEM 形式でロギング（Log messages in Cisco EMBLEM format）] チェックボックスを使用できます。この統合は EMBLEM 形式をサポートしていません。そのため、このチェックボックスがオフになっていることを確認します。

d) [OK] をクリックして設定を保存し、ダイアログボックスを閉じます。定義した syslog サーバーが、テーブルに表示されます。

ステップ 6 設定の変更を送信して展開します。

ASA デバイスから NSEL イベントを送信するための CSM 設定

この手順では、ASA の NetFlow Secure Event Logging（NSEL）イベントを SAL（SaaS） に送信するための CSM 設定について説明します。

始める前に

- 要件と前提条件のセクションを確認します。
- SAL（SaaS） でイベントデータストレージをセットアップします。
- ASA デバイスが SEC に到達できることを確認します。

- カスタム Linux VM に SDC をインストールした場合は、SEC が ASA syslog を受信することを確認します。
- CDO から SEC の IP アドレスとポート番号を取得します。

手順

ステップ 1 Cisco Security Manager の [設定マネージャ（Configuration Manager）] ウィンドウにログインします。

ステップ 2 NetFlow パケットの送信先となる NetFlow コレクタを追加します。ここでは、Secure Event Connector（SEC）が NetFlow コレクタです。

a) [NetFlow] ページにアクセスするには、次のいずれかを実行します。
   - （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[NetFlow]** を選択します。
   - （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]** > **[ロギング（Logging）]** > **[NetFlow]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

b) [コレクタ（Collectors）] セクションで、[追加（Add）] をクリックしてコレクタを追加します。

c) [コレクタの追加と編集（Add and Edit Collector）] ダイアログボックスで、次を指定します。
   - [インターフェイス（Interface）]：NetFlow コレクタとの通信に使用するインターフェイス。
   - [IP アドレスまたはホスト名（IP Address or Hostname）]：CDO から取得した SEC IP アドレス（手順については、「はじめる前に」を参照）。
   - [UDP ポート（UDP Port）]：CDO から取得した SEC ポート番号（手順については、「はじめる前に」を参照）。

d) [OK] をクリックします。

ステップ 3 サービスポリシーを設定します。

a) （デバイスビュー）**[プラットフォーム（Platform）]** > **[サービスポリシー（Service Policy）]** > **[ルール（Rules）]** を選択します。

b) [追加（Add）] をクリックします。

c) [サービスポリシー（MPC）ルールの挿入 1：サービスポリシーの設定（Insert Service Policy (MPC) Rule 1 - Configure a Service Policy）] で、[グローバル：すべてのインターフェイスに適用（Global - applies to all interfaces）] オプションボタンをクリックしてルールをグローバルポリシーに適用し、[次へ（Next）] をクリックします。

d) [サービスポリシー（MPC）ルールの挿入 2：トラフィッククラスの設定（Insert Service Policy (MPC) Rule 2 - Configure the Traffic Class）] で、[トラフィッククラスとして class-default

を使用（Use class-default As the Traffic Class）] オプションボタンをクリックし、[次へ（Next）] をクリックします。

e) [サービスポリシー（MPC）ルールの挿入 3：アクションの設定（Insert Service Policy (MPC) Rule 3 - Configure the Actions）] で、[NetFlow] タブをクリックし、イベントアクションごとに [選択（Select）] をクリックします。

f) [ネットワーク/ホストセレクタ（Networks/Hosts Selector）] で、ステップ 2 で追加したコレクタ（SEC）を [使用可能なネットワーク/ホスト（Available Networks/Hosts）] ボックスから [選択済みのネットワーク/ホスト（Selected Networks/Hosts）] ボックスに移動して、[OK] をクリックします。

g) [終了（Finish）] をクリックします。

ステップ 4 NSEL イベントを介して送信される情報は、syslog 接続イベントの一部と重複しています。冗長な syslog メッセージが SEC に転送されないようにするには、次の手順を実行します。

a) （デバイスビュー）**[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[サーバーのセットアップ（Server Setup）]** を選択します。

b) [NetFlow と同等の syslogs を無効化（Disable NetFlow Equivalent Syslogs）] ボタンをクリックします。

c) [**保存（Save）**] をクリックします。

ステップ 5 設定の変更を送信して展開します。

イベントの表示および操作

クラウドでイベントを表示および検索するには、次の手順を実行します。

手順

ステップ 1 ブラウザを使用して、イベントの送信先の地域 CDO クラウドに移動します。

- 北米：

  http://www.defenseorchestrator.com

- 欧州：

  http://www.defenseorchestrator.eu

ステップ 2 CDO にサインインします。

ステップ 3 ナビゲーションバーから、[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 4 [履歴（Historical）] タブを使用して履歴イベントデータを表示します。デフォルトでは、このタブがビューアに表示されます。

ステップ 5 ライブイベントを表示するには、[ライブ（Live）] タブをクリックします。

（注）
[イベントロギング（Event Logging）] ページは、次のようになっています。

- 詳細に解析された ASA syslog イベントはイタリック体で表示されます。
- NetFlow イベントを表示するには、[フィルタ（Filters）] ペインの [ASA イベント（ASA Events）] で [NetFlow] チェックボックスをオンにします。NetFlow イベントは、イベントタイプ値（1、2、3、および 5）で識別できます。
- [フィルタ（Filters）] ペインの下部にある [NetFlow イベントを含める（Include NetFlow Events）] チェックボックスは、デフォルトでオンになっています。イベントをフィルタ処理して [ファイアウォール拒否（Firewall Denied）] および [ファイアウォールトラフィック（Firewall Traffic）] を表示すると、NetFlow イベントも syslog イベントとともに表示されます。

このページで実行できることの詳細については、CDO のオンラインヘルプでイベント表示の手順を参照してください。

次のタスク

Logging Analytics and Detection ライセンスまたは **Total Network Analytics and Detection** ライセンスがある場合は、CDO のオンラインヘルプで手順を参照して Stealthwatch Cloud ポータルを相互起動してください。

よく寄せられる質問

ASA デバイスを CDO にオンボードする必要はありますか。

いいえ。デバイスを CDO にオンボードしないでください。

SAL（SaaS）でも CDO と Stealthwatch Cloud のライセンスが必要ですか。

いいえ。SAL（SaaS）は、イベントを表示するために Cisco Defense Orchestrator（CDO）を使用し、動作を検出するために Stealthwatch Cloud（SWC）を使用する権利を提供します。これら 2 つの製品のライセンスを個別に保持する必要はありません。ただし、SWC の診断および分析の機能を使用するには、適切なライセンスを取得する必要があります。

ASA をアップグレードする場合は、データプランもアップグレードする必要がありますか。

いいえ。データプランは、Cisco Cloud が ASA から毎日受け取るイベント数に基づいています。デバイスのバージョンに関係なく、データプランを変更できます。「ストレージ要件の計算とデータプランの購入 （5 ページ）」を参照してください。

CDO イベントビューアにイベントが表示されません。何をすればよいですか。

1. SEC で実行されているサービスと、そのサービスと Cisco Cloud との接続の基本的なヘルスチェックを実行します。ヘルスチェックを実行するには、sdc ユーザーとして SDC VM にいる必要があります。詳細については、Cisco Defense Orchestrator のガイドを参照してください。
2. ASA が正しい SEC の IP アドレスと TCP/UDP ポートで設定されていることを確認します。

問題が解決しない場合は、Cisco Defense Orchestrator サポートにお問い合わせください。

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