



Cisco Security Analytics and Logging

- [Security Analytics and Logging \(SaaS\) について \(2 ページ\)](#)
- [FTD デバイスの安全なロギング分析 \(2 ページ\)](#)
- [FTD デバイスに安全なロギング分析 \(SaaS\) を導入する \(11 ページ\)](#)
- [FTD イベントを CDO イベントロギングに送信する \(14 ページ\)](#)
- [Cisco Cloud に FTD イベントを直接送信する \(15 ページ\)](#)
- [FTD イベントタイプ \(16 ページ\)](#)
- [Secure Event Connector \(17 ページ\)](#)
- [Secure Event Connector をインストールする \(18 ページ\)](#)
- [Cisco Security Analytics and Logging \(SaaS\) をプロビジョニング解除する \(38 ページ\)](#)
- [Secure Event Connector の削除 \(38 ページ\)](#)
- [Cisco Secure Cloud Analytics ポータルのプロビジョニング \(39 ページ\)](#)
- [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 \(41 ページ\)](#)
- [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 \(42 ページ\)](#)
- [Cisco Defense Orchestrator での Cisco Secure Cloud Analytics アラートの表示 \(43 ページ\)](#)
- [Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング \(44 ページ\)](#)
- [ファイアウォールイベントに基づくアラートの使用 \(46 ページ\)](#)
- [アラートの優先順位を変更する \(54 ページ\)](#)
- [ライブイベントを表示する \(54 ページ\)](#)
- [イベントロギングページのカラムの表示および非表示 \(58 ページ\)](#)
- [カスタマイズ可能なイベントフィルタ \(61 ページ\)](#)
- [イベントのダウンロード \(63 ページ\)](#)
- [Security Analytics and Logging のイベント属性 \(65 ページ\)](#)
- [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 \(98 ページ\)](#)
- [データストレージプラン \(105 ページ\)](#)
- [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 \(108 ページ\)](#)

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の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。

FTD デバイスの安全なロギング分析

Cisco Security Analytics and Logging (SaaS) を使用すると、すべての Firepower Threat Defense (FTD) デバイスからの接続、侵入、ファイル、マルウェア、セキュリティインテリジェンスの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。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の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 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 FTD イベントの表示方法

接続、侵入、ファイル、マルウェア、およびセキュリティ インテリジェンスのイベントは、個々のルールがイベントをログに記録するように設定され、ネットワークトラフィックがルールの条件に一致する場合に生成されます。イベントが Cisco Cloud に保存されたら、CDO で表示できます。イベントを Cisco Cloud に送信するように FTD を設定するには、次の 2 つの方法があります。

- 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。
- FTD が登録キーを使用して CDO にオンボーディングされている場合、Firepower Device Manager のコントロールを使用して、イベントを Cisco Cloud に直接送信できます。

Secure Event Connector を使用して FTD から Cisco Cloud にイベントが送信される仕組み

基本的な **Logging and Troubleshooting** ライセンスを使用した場合、FTD イベントは次のように Cisco Cloud に到達します。

1. ユーザー名とパスワードを使用するか登録キーを使用して、FTD を CDO にオンボードします。
2. アクセスコントロールルール、セキュリティ インテリジェンス ルール、SSL 復号化ルールなどの個々のルールを設定して、SEC が syslog サーバーであるかのように、いずれかの SEC にイベントを転送します。アクセスコントロールルールでは、ファイルおよびマルウェアポリシーと侵入ポリシーも有効化して、それらのポリシーによって生成されたイベントを SEC に転送することもできます。
3. [システム設定 (System Settings)] > [ロギング (Logging)] で、ファイルイベントのファイルロギングおよびマルウェアロギングを設定します。
4. [システム設定 (System Settings)] > [ロギング (Logging)] で、侵入イベントの侵入ロギングを設定します。
5. 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。
6. 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 [イベントロギング (Events Logging)] ページに表示します。

Logging Analytics and Detection または **Total Network Analytics and Monitoring** ライセンスでは、次の動作も行われます。

1. Cisco Secure Cloud Analytics は、Cisco Cloud に保存されている FTD 接続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。

イベントが FTD から Cisco Cloud に直接送信される仕組み

基本的な **Logging and Troubleshooting** ライセンスを使用した場合、FTD イベントは次のように Cisco Cloud に到達します。

1. 登録トークンを使用して、FTD を CDO にオンボーディングします。
2. アクセスコントロールルール、セキュリティインテリジェンスルール、SSL 復号化ルールなどの個々のルールを設定して、イベントをログに記録します。ただし、イベントの送信先となる syslog サーバーは指定しません。アクセスコントロールルールでは、ファイルおよびマルウェアポリシーと侵入ポリシーも有効化して、それらのポリシーによって生成されたイベントを Cisco Cloud に転送することもできます。
3. ファイルイベントと侵入イベントは、アクセスコントロールルールでファイルおよびマルウェアポリシーおよび侵入ポリシーが接続イベントをログに記録するように設定されている場合、Cisco Cloud に送信されます。
4. FTD の Firepower Device Manager (FDM) でクラウドロギングをアクティブ化して、さまざまなルールで記録されたイベントが Cisco Cloud に送信されます。
5. CDO は、設定したフィルタに基づいて Cisco クラウドからイベントを取得し、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、次の動作も行われます。

1. Cisco Secure Cloud Analytics は、Cisco Cloud に保存されている FTD 接続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。

設定の比較

SEC を介して Cisco Cloud にイベントを送信する場合と、Cisco Cloud にイベントを直接送信する場合の CDO 設定の違いの概要を次に示します。

FTD デバイス設定	Secure Event Connector (SEC) を介してイベントを送信する場合	Cisco Cloud にイベントを直接送信する場合
CDO での FTD のオンボーディング方法	ログイン情報 (ユーザー名とパスワード) 登録トークン	登録トークン シリアル番号
FTD バージョンのサポート	FTD 6.4 以降	登録トークン : FTD 6.5 以降 シリアル番号 : FTD 6.7 以降
Cisco Security Analytics and Logging (SaaS) ライセンス	Logging and Troubleshooting Logging Analytics and Detection (オプション) Total Network Analytics and Monitoring (オプション)	Logging and Troubleshooting Logging Analytics and Detection (オプション) Total Network Analytics and Monitoring (オプション)
FTD ライセンス	基本ライセンス 脅威 : 侵入ルール、ファイル制御ルール、またはセキュリティインテリジェンスフィルタリングから接続イベントを収集する場合。 マルウェア : ファイル制御ルールから接続イベントを収集する場合。	基本ライセンス 脅威 : 侵入ルール、ファイル制御ルール、またはセキュリティインテリジェンスフィルタリングから接続イベントを収集する場合。 マルウェア : ファイル制御ルールから接続イベントを収集する場合。
Secure Event Connector	必須	該当なし
データ圧縮*	イベントは圧縮されます*	イベントは圧縮されません*
データプラン	必須	必須



(注) データサブスクリプションと月次使用量の履歴は、使用する非圧縮データの量に基づいています。

ソリューションのコンポーネント

Cisco Security Analytics and Logging (SaaS) では、次のコンポーネントを使用してイベントを CDO に配信します。

Secure Device Connector (SDC) : SDC は CDO を FTD に接続します。FTD 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、FTD 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 (Event Logging)] ページで確認したり、Secure Cloud Analytics で分析したりできます。テナントに 1 つ以上の SEC が関連付けられている場合があります。環境に応じて、Secure Event Connector を Secure Device Connector または CDO コネクタ VM にインストールします。

Firepower Threat Defense (FTD) : FTD は、シスコの次世代ファイアウォールです。ネットワークトラフィックのステートフルインスペクションとアクセスコントロールに加えて、FTD はマルウェアやアプリケーション層攻撃からの保護、統合された侵入防御、クラウド提供型脅威インテリジェンスなどの機能を提供します。

Logging Analytics and Detection ライセンスや **Total Network Analytics and Monitoring** ライセンスがある場合、Cisco Security Analytics and Logging (SaaS) は Cisco Secure Cloud Analytics を使用して、CDO に提供されたイベントを詳細に分析します。

Cisco Secure Cloud Analytics : Secure Cloud Analytics は、動的エンティティモデリングを FTD 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。

ライセンスング

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)。 **Logging and Troubleshooting** ライセンスを購入する必要があります。このパッケージの目的は、オンボーディングした Firepower Threat Defense デバイスから派生したリアルタイムイベントとイベント履歴をネットワーク運用チームに提供し、ネットワーク内のトラフィックのトラブルシューティングと分析を可能にすることです。

Logging Analytics and Detection または **Total Network Analytics and Monitoring** ライセンスを購入して、Cisco Secure Cloud Analytics を適用することもできます。これらのパッケージの目的は、FTD イベント（および Total Network Analytics and Monitoring ライセンスを購入した場合はネットワークトラフィック）に関するより詳細な洞察をネットワーク運用チームに提供し、異常な動作の可能性をより適切に識別してそれに対応できるようにすることです。

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	CDO 内のライブフィードと履歴ビューの両方で、FTD イベントとイベントの詳細を表示します。	<ul style="list-style-type: none"> • 1 年 • 3 年 • 5 年 	<ul style="list-style-type: none"> • CDO • バージョン 6.4 以降を実行しているオンプレミスの FTD 展開 • FTD イベントをクラウドに渡すための 1 つ以上の SEC の展開。
Logging Analytics and Detection (旧称 Firewall Analytics and Monitoring)	Logging and Troubleshooting の機能に加えて、以下の機能 <ul style="list-style-type: none"> • 動的エンティティモデリングと動作分析を FTD イベントに適用します。 • CDO イベントビューアからクロス起動により、イベントデータに基づいて Cisco Secure Cloud Analytics でアラートを開きます。 	<ul style="list-style-type: none"> • 1 年 • 3 年 • 5 年 	<ul style="list-style-type: none"> • CDO • バージョン 6.4 以降を実行しているオンプレミスの FTD 展開。 • FTD イベントをクラウドに渡すための 1 つ以上の SEC の展開。 • 新たにプロビジョニングされた、または既存の 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	<p>Logging Analytics and Detection の機能に加えて、以下の機能</p> <ul style="list-style-type: none"> 動的エンティティモデリングと動作分析を FTD 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。 FTD 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 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、CDO イベントビューアからのクロス起動によって Cisco Secure Cloud Analytics でアラートを開きます。 	<ul style="list-style-type: none"> 1 年 3 年 5 年 	<ul style="list-style-type: none"> CDO バージョン 6.4 以降を実行しているオンプレミスの FTD 展開 。 FTD イベントをクラウドに渡すための 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 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 Secure Cloud Analytics に渡すためのクラウドベースと統合された Secure Cloud Analytics の展開。 新たにプロビジョニングされた、または既存の Secure Cloud Analytics ポータル。

Firepower Threat Defense。FTD を実行し、セキュリティイベントを生成するルールを作成するには、次のライセンスが必要です。

ライセンス	期間	付与される機能
基本（自動的に含まれる）	永久	<p>オプションのターム ライセンスでカバーされないすべての機能。</p> <p>[このトークンに登録した製品でエクスポート制御機能を許可する (Allow export-controlled functionality on the products registered with this token)]かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。</p>

ライセンス	期間	付与される機能
脅威	ターム ベース	<p>侵入検知および防御：侵入ポリシーが侵入とエクスプロイトを検出するためネットワークトラフィックを分析し、またオプションで違反パケットをドロップします。</p> <p>ファイル制御：ファイルポリシーが特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。マルウェアライセンスが必要な AMP for Firepower を使用すると、マルウェアを含むファイルのインスペクションを実行してブロックできます。任意のタイプのファイルポリシーを使用するには、脅威ライセンスが必要です。</p> <p>セキュリティ インテリジェンス フィルタ：トラフィックがアクセスコントロールルールによって分析を受ける前に、選択されたトラフィックをドロップします。ダイナミックフィードを使用することで、最新のインテリジェンスに基づいて接続をただちにドロップできます。</p>
マルウェア (Malware)	ターム ベース	<p>マルウェアを確認するポリシーであり、Cisco Advanced Malware Protection (AMP) と一緒に AMP for Firepower（ネットワークベースの高度なマルウェア保護）と Cisco Threat Grid を使用します。</p> <p>ファイル ポリシーは、ネットワーク上で伝送されるファイルに存在するマルウェアを検出してブロックできます。</p>

データプラン

Cisco Cloud がオンボーディングされた FTD から 1日に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。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)** のトライアル版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。また、**ロギングボリューム見積ツール** も使用できます。



注意 イベントを Cisco クラウドに直接送信し、同時に **Secure Event Connector** を介して送信するように FTD を設定することができます。これを行うと、同じイベントが 2 回取り込まれ、データプランに対して 2 回カウントされますが、Cisco クラウドには 1 回しか保存されません。必要な料金が発生しないように、いずれか 1 つの方法を使用してイベントを Cisco Cloud に送信するように注意してください。

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) Ordering Guide**』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。ネットワークライフサイクル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。

次の手順

「**FTD デバイスに安全なロギング分析 (SaaS) を導入する (11 ページ)**」に進みます。

FTD 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

- 「**FTD デバイスの安全なロギング分析 (2 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
- マネージドサービス プロバイダーまたは CDO セールス担当者にお問い合わせで CDO テナントを所有している必要があります。
 - テナントは、FTD に接続するために CDO 用の Secure Device Connector (SDC) を使用する場合と使用しない場合があります。テナントには、デバイスログイン情報を使用してオンボーディングする FTD 用に SDC がインストールされている必要があります。これは、ベストプラクティスと見なされます。登録キーまたはシリアル番号を使用して FTD をオンボーディングする場合、SDC は必要ありません。
 - テナントに SDC をインストールしている場合は、SDC のステータスがアクティブであり、最新のハートビートが記録されていることを確認してください。
 - SDC をインストールする場合は、次のいずれかのインストール方法を使用します。
 - 「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 を使用して Secure Device Connector を展開する」を使用します。
 - テナントに CDO イメージを使用して SEC をインストールでき、任意の FTD から、テナントにオンボーディングされた任意の SEC にイベントを送信できます。
 - イベントを FTD から Cisco Cloud に直接送信する場合は、管理インターフェイスのポート 443 で発信アクセスを開いている必要があります。
 - 自身のアカウントのユーザー向けに二要素認証を設定している必要があります。

Secure Logging Analytics (SaaS) を導入し、Secure Event Connector を介して Cisco Cloud にイベントを送信するための新規 CDO カスタマーワークフロー

1. Firepower Threat Defense デバイスをオンボーディングします。管理者のユーザー名とパスワード、または登録トークンを使用して、デバイスをオンボーディングできます。
2. Secure Logging Analytics (SaaS) の Syslog サーバーオブジェクトを作成します。
3. 接続イベントがログに記録されるように FTD ポリシーを設定します。
4. FTD イベントを CDO イベントロギングに送信するように FTD を設定します。
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 (Live)] タブをクリックします。
6. Logging Analytics and Detection ライセンスや Total Network Analytics and Monitoring ライセンスがある場合は、「Cisco Secure Cloud Analytics でのイベントの分析」に進みます。

Secure Logging Analytics (SaaS) を導入し、Cisco Cloud にイベントを直接送信するための新規 CDO カスタマーワークフロー

1. [Firepower Threat Defense](#) デバイスをオンボーディングします。登録キーのみを使用できません。
2. 接続イベントがログに記録されるように [FTD ポリシー](#) を設定します。
3. [Cisco Cloud](#) に [FTD イベント](#) を直接送信するように FTD を設定します。
4. 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 (Live)**] タブをクリックします。
5. [Logging Analytics and Detection](#) ライセンスや [Total Network Analytics and Monitoring](#) ライセンスがある場合は、「[Cisco Secure Cloud Analytics でのイベントの分析](#)」に進みます。

Secure Logging Analytics (SaaS) を導入し、Secure Event Connector を介して Cisco Cloud にイベントを送信するための既存 CDO カスタマーワークフロー

1. [Firepower Threat Defense](#) デバイスをオンボーディングします。管理者のユーザー名とパスワード、または登録トークンを使用して、デバイスをオンボーディングできます。
2. [Secure Logging Analytics \(SaaS\)](#) の Syslog サーバーオブジェクト。
3. 接続イベントがログに記録されるように [FTD ポリシー](#) を設定します。
4. [FTD イベント](#) を [CDO イベントロギング](#) に送信する。
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 (Live)**] タブをクリックします。
6. [Logging Analytics and Detection](#) ライセンスや [Total Network Analytics and Monitoring](#) ライセンスがある場合は、「[Cisco Secure Cloud Analytics でのイベントの分析](#)」に進みます。

Secure Logging Analytics (SaaS) を導入し、Cisco Cloud にイベントを直接送信するための既存 CDO カスタマーワークフロー

1. [Firepower Threat Defense](#) デバイスをオンボーディングします。登録キーのみを使用できません。
2. 接続イベントがログに記録されるように [FTD ポリシー](#) を設定します。
3. [Cisco Cloud](#) に [FTD イベント](#) を直接送信するように FTD を設定します。
4. 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 (Live)**] タブをクリックします。
5. [Logging Analytics and Detection](#) ライセンスや [Total Network Analytics and Monitoring](#) ライセンスがある場合は、「[Cisco Secure Cloud Analytics でのイベントの分析](#)」に進みます。

Cisco Secure Cloud Analytics でのイベントの分析

Logging Analytics and Detection 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 \(39 ページ\)](#)。
2. **Total Network 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 \(42 ページ\)](#) 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 \(43 ページ\)](#) を参照してください。
4. CDO から Secure Cloud Analytics を相互起動し、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 \(43 ページ\)](#) を参照してください。

CDO からの相互起動による Cisco Secure Cloud Analytics アラートの確認

Logging Analytics and Detection 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 を相互起動して、FTD イベントに基づいて Secure Cloud Analytics により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 \(43 ページ\)](#)
- [Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング \(44 ページ\)](#)
- [ファイアウォールイベントに基づくアラートの使用](#)

Secure Analytics and Logging (SaaS) のワークフロー

「[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、Secure Logging Analytics (SaaS) 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い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。

FTD イベントを CDO イベントロギングに送信する

アクセスコントロールルール、セキュリティ インテリジェンス ルール、SSL 復号化ルールからの Firepower Threat Defense (FTD) イベントをイベントロギングビューアで表示するには、最初にそれらのイベントを Cisco Cloud に送信する必要があります。

- **アクセスコントロールルール** ネットワーク接続の開始時または終了時に **FTD イベントタイプ** をログに記録できます。このルールタイプのログの構成についての詳細は、「[Firepower Threat Defense アクセス コントロール ポリシーの設定](#)」と「[Firepower Threat Defense アクセスコントロールルールのログ設定](#)」を参照してください。
- **セキュリティ インテリジェンス ルール** セキュリティ インテリジェンスルールによって生成された **FTD イベントタイプ** をログに記録できます。ログを有効にした場合は、ブロックリストのエントリに一致するものが記録されます。ログを有効にして、除外された接続がアクセス制御ルールに一致した場合、ログメッセージは取得しますが例外エントリに一致するものは記録されません。ログの構成については、『[Firepower セキュリティ インテリジェンス ポリシーの構成](#)』を参照してください。
- **SSL 復号ルール** SSL 復号ルールによって生成された **FTD イベントタイプ** をログに記録できます。

ファイルおよびマルウェアイベントまたは侵入イベントを Cisco Cloud に送信する場合、Secure Event Connector を使用する場合は、[デバイスのログ設定](#)を構成する必要があります。

関連情報：

- [Secure Logging Analytics \(SaaS\) の Syslog サーバーオブジェクトの作成](#)

Cisco Cloud に FTD イベントを直接送信する

Firepower Threat Defense (FTD) 6.5 以降では、接続イベント、侵入イベント、ファイルイベント、およびマルウェアイベントを FTD デバイスから Cisco Cloud に直接送信できます。Cisco Cloud に送信されたイベントは、Cisco Defense Orchestrator (CDO) で監視し、Cisco Secure Cloud Analytics を使用して分析できます。この方法では、Secure Device Connector (SDC) 仮想マシンに Secure Event Connector (SEC) コンテナをインストールする必要はありません。

始める前に

以下のトピックを確認してください。

- [FTD デバイスの安全なログ分析 \(2 ページ\)](#)
- [FTD デバイスに安全なログ分析 \(SaaS\) を導入する](#)

手順

- ステップ 1** イベントを Cisco Cloud に送信する FTD の Firepower Device Manager (FDM) にログオンします。
- ステップ 2** [デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] を選択します。

- ステップ 3 [Cisco Cloudにイベントを送信 (Send Events to the Cisco Cloud)] ペインで、[有効化 (Enable)] をクリックします。

FTD イベントタイプ

イベントタイプ

システムでは、以下のタイプのイベントが生成されます。監視ダッシュボードで関連する統計を表示するには、これらのイベントを生成する必要があります。

データ (診断) イベント

データロギングでは、デバイスとシステムの正常性に関連するイベント、および接続とは関係のないネットワーク設定に関する syslog メッセージが提供されます。個々のアクセス コントロール ルール内に接続ロギングを設定します。

データロギングでは、データプレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバ、NAT などの機能が含まれます。

Connection Events

ユーザーが生成するトラフィックがシステムを通過する場合、この接続に対してイベントを生成できます。これらのイベントを生成するには、アクセスルールで接続ロギングを有効にします。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールでロギングを有効にすると、接続イベントを生成できます。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- 基本的な接続プロパティ：タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど。
- システムによって検出または推測される追加の接続プロパティ：アプリケーション、要求される URL、または接続に関連付けられているユーザーなど。
- 接続がログに記録された理由に関するメタデータ：トラフィックを処理した設定、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など。

Intrusion Events

システムは、ネットワークを通過するパケットを検査し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある、悪意のあるアクティビティについて調べま

す。システムは潜在的な侵入を識別すると、侵入イベントを生成します。これには、エクスプロイトの日時とタイプ、攻撃とそのターゲットについての状況説明が記録されます。侵入イベントは、アクセス制御ルールのロギング設定に関係なく、ブロックまたはアラートするように設定された侵入ルールに対して生成されます。

ファイルイベント

ファイルイベントは、作成したファイルポリシーに基づき、ネットワークトラフィック内でシステムによって検出（オプションとしてブロック）されたファイルを表します。これらのイベントを生成するには、ファイルポリシーを適用するアクセスルールに対してファイルロギングを有効にする必要があります。

システムはファイルイベントを生成する場合、基になったアクセスコントロールルールのロギング設定にかかわらず、関連する接続の終了についても記録します。

マルウェアイベント

システムは、全体的なアクセスコントロール設定の一環として、ネットワークトラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いっどこでどのようにしてマルウェアが検出されたかに関するコンテキストデータを含むマルウェアイベントを生成できます。これらのイベントを生成するには、ファイルポリシーを適用するアクセスルールに対してファイルロギングを有効にする必要があります。

ファイルの判定結果は、正常からマルウェア、マルウェアから正常などに変更できます。AMP for Firepower が AMP クラウドにファイルについて照会し、クエリから 1 週間以内に判定結果が変更されたことがクラウドに特定されると、システムはレトロスペクティブマルウェアイベントを生成します。

Security Intelligence Events

セキュリティインテリジェンスイベントは、ポリシーによってブロックまたはモニターされた各接続のセキュリティインテリジェンスポリシーによって生成された接続イベントの一種です。すべてのセキュリティインテリジェンスイベントには、自動入力された[セキュリティインテリジェンスカテゴリ (Security Intelligence Category)] フィールドがあります。

これらの各イベントには、対応する「通常」の接続イベントがあります。セキュリティインテリジェンスポリシーはアクセスコントロールなどのその他多数のセキュリティポリシーより前に評価されるため、セキュリティインテリジェンスによって接続がブロックされると、その結果のイベントには、以降の評価から収集される情報（ユーザーアイデンティティなど）は含まれません。

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 (Event Logging)] ページに表示されます。管理者は Cisco Stealthwatch 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 (Details)] 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：

- [FTD デバイスの安全なロギング分析](#)
- [SDC 仮想マシンへの Secure Event Connector のインストール \(18 ページ\)](#)
- [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 \(29 ページ\)](#)
- [CDO イメージを使用して SEC をインストールする \(22 ページ\)](#)

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 (Event Logging)] 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 \(22 ページ\)](#) または [VM イメージを使用した SEC のインストール \(29 ページ\)](#) 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 (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。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。

手順

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

Deploy an On-Premises Secure Event Connector



```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0ppq
YkdsbGJuUmZhV1FpT21KaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRIT1teVVEVzh2Qk5FWW44c3V0Z3NTQo0TH15N0xzVGsydEx4N05nbS00STB6SmZ6
aWdQTKRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzcktMREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVENMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VkxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNRTHMxeWduaXdVU1RuWkQxM0c5T2FJWEXCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NFN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fy21zY28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
O18vc3RhZ21uZy5kZXYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fy21zY28tYW1hbGxpby
IKT05MWV9FVkvOVE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM

```
U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQt0GYzZDJKmjQ1ZmU3IqpTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZlMzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEVOQU5UX05BTUU9IKNET1
9jaXNjby1hbWFsbG1vIg==
```

[Copy SEC Bootstrap Data](#)

Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel

OK

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

RtyFUiyIOHKKnkJbKhvhgyRStwterTyufGUIhoJpojP9UOoiUY8VHHGFXREWRTygfVjkhOuihIuyftyXtfcghvjbkhB=

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 ██████████
-----
SEC cloud URL ██████████ 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 loca
=====
```

登録に失敗したことや SEC のオンボーディング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 オンボーディング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 \(34 ページ\)](#) 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

[FTD デバイスに安全なロギング分析 \(SaaS\) を導入する \(11 ページ\)](#) に戻ります。

関連情報：

- [Secure Device Connector のトラブルシューティング](#)
- [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 (Event Logging)] 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 \(22 ページ\)](#) 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 \(35 ページ\)](#)。



- (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 \(22 ページ\)](#) 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。

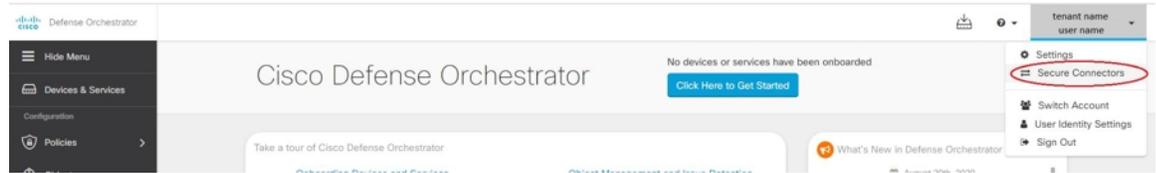
Security Analytics and Logging のトライアル版をリクエストする場合は、CDO にログインし、メインナビゲーションバーで **[モニターリング (Monitoring)]** **[イベントロギング]**

(**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。

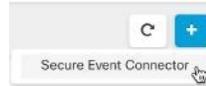
- CDO は、厳密な証明書チェックを必要とし、CDO コネクタとインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、CDO コネクタと CDO の間のトラフィックの検査を無効にします。
- このプロセスでインストールされる CDO コネクタには TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。
- CDO コネクタで適切なネットワークアクセスを確保するには、「[Secure Device Connector を使用した Cisco Defense Orchestrator への接続](#)」を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

手順

-
- 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. オンボードを開始した Secure Event Connector を選択します。ステータスに [導入準備中 (Onboarding)] と表示されます。
  4. [アクション (Actions)] 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。

Deploy an On-Premises Secure Event Connector
✕

i SEC will be deployed on a new VM

**Step 1**

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```

Q0RPX1RPS0V0PSJ1eUp0YkdjaU9pS1NVekKxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
l3SWl3aWMyTnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNKcGRHVWlMQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVFV0T1dNd05DMHlOVGRpTlR0aE1qZzFPR1VpWfN3aVlXMXlJam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJjBepQVEVWZlUxVlFSVkpUUVSTlNVNGlYU3dpYVh0ek1qb2lhWFJrSWl3aVky
eDFjM1JsY2tsa0lqb2lNU0lZSW1sa0lqb2lAbVF3T0dReVpHVXRNMlZpT1MwMfPEYzRMV0kwWldNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWftVmpkRlI1Y0dVaU9pSjFjMlZ5SWl3aWfuUnBJam9pTURB
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZXlMT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXRlQTfsYmE3VkxNOUp4bk9RS1pqaW
lrdDNsYnRRbDnrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZJWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWDpbmZGZGV2LmV2toYXJ0Lm
lvIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ2l1uZy5kZXUubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpbY
IKT05MwV9FVkvOVE1ORz0idHJ1ZSIK

```

[Copy CDO Bootstrap Data](#) ←

Cancel OK

**ステップ 26** 「これらの設定を更新しますか (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 が黄色のオンボーディング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 (27 ページ) に進みます。

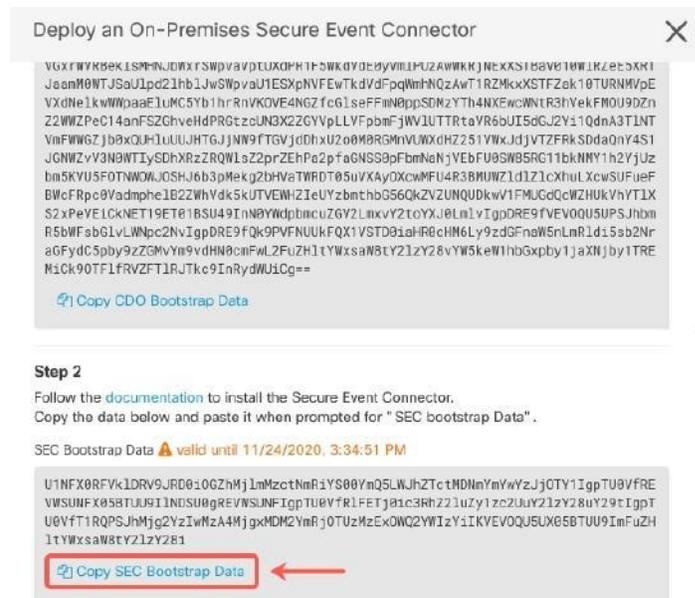
## CDO コネクタ VM への Secure Event Connector のインストール

### 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 (22 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。

### 手順

- 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 上記でオンボーディングした 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、「オンボーディング」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 (Actions) ]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@sdcm-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdcm-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**

**RtyFUiyIOHKnKJbKhvgyRStwterTyufGUihoJpojP9UooiUY8VHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkbB=**

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 のオンボーディング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

[FTD デバイスに安全なログ分析 \(SaaS\) を導入する \(11 ページ\)](#) に戻ります。

## 関連情報：

- [Secure Device Connector のトラブルシューティング](#)
- [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 (Event Logging) ] 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 \(29 ページ\)](#)
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 \(34 ページ\)](#) 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 \(22 ページ\)](#) 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 \(29 ページ\)](#) 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 コネクタは TCP ポート 443 でインターネットへの完全なアウトバウンド接続を確立する必要があります。
- CDO コネクタで適切なネットワーク接続を確立するには、「[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 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。
- CentOS 7 ゲスト オペレーティング システム。
- CDO コネクタと SEC のみをホストすることを目的した 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
- Linux 環境での操作や vi ビジュアルエディタを使用したファイル編集に慣れ親しんでいるユーザーがこの手順を実行してください。
- 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 コネクタ仮想マシンは、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**：この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ます、コマンドが失敗する原因となります。

## 手順

- 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)] ウィンドウのステップ 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](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@sdcc-vm ~]# yum update -y
[root@sdcc-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@sdcc-vm ~]# systemctl start docker
[root@sdcc-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 **sd** 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）。sd 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 sd -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、sd 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 sd
[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、sd 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 sd
[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、展開ウィザードのステップ 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。

## Deploy an On-Premises Secure Event Connector

**i** SEC will be deployed on a new VM

### Step 1

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```
Q0RPX1RPS0V0PSJ1eUpoYkdjaU9pS1NVekxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZXlKM1pYSW1PaU
l3SW13aWMyTnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNkcGRHVWlMQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVFV0T1dNd05DMH1OVGRpT1R0aE1qZzFPR1VpWFN3aV1XMX1Jam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZlUxVlF5VkpUUVVSTlNVNGlYU3dpYVh0ek1qb2lhWFJrSW13aVky
eDFjM1JsY2tsa01qb2lNU01zSW1sa01qb2labVF3T0dReVpHVXRNMlZpT1MwMFpEYzRMV0kwWldNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWFtVmpkR1I1Y0dVaU9pSjFjM1Z5SW13aWFuUnBJam9pTURB
VacmI0YVFLSjFtdnJ5RjVfZ2FqajZfZkNvaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZXlMT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXRlQTFSYmE3VksN0Up4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fY2lZy28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUFF9VUkw9Imh0dHBz
0i8vc3RhZ2l1uZy5kZXYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpby
IKT05MMWV9FVkvOVE1ORz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

Cancel

OK

**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、復号化して **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復号化したデータを表示します。コマンドおよび復号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、復号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 (34 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。 \(35 ページ\)](#)。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 \(35 ページ\)](#) 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 \(35 ページ\)](#) 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 \(29 ページ\)](#)
- [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 \(34 ページ\)](#)

## 手順

- 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 [操作 (Actions) ]ウィンドウで、[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。

## Deploy an On-Premises Secure Event Connector



```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT21KaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYtZQYzVsRjRIT1teVVEVzh2Qk5FWW44c3V0Z3NTQUo0TH15N0xzVGSydEx4N05nbS00STB6SmZ6
aWdQTkRiV1RsRW1tcjI5SkfVZ2NBWEhySkdzcktmREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVfZ2FqaJZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTfsYmE3VkxNOUp4bk9RS1pqaW
1rdDNsYnRRbDnrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmXvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY21zY28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY21zY28tYW1hbGxpby
IKT05MMV9FVkv0VE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

**Step 2**

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.  
Copy the bootstrap data below and paste it when prompted for " SEC bootstrap Data" .

**⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM**

```
U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYy0Y2JkLWEzNWQt0GYzZDJKMjq1ZmU3IqpTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZ1Mzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEV0QU5UX05BTUU9IKNET1
9jaXNjby1hbWFSbG1vIg==
```

[Copy SEC Bootstrap Data](#)

**Step 3**

Verify the connection status of the new SEC by exiting this dialog and checking the " Last Heartbeat" information.

Cancel

OK

- 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、**sdm** 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@sdm-vm ~]$ sudo su sdm
[sudo] password for cdo: <type password for cdo user>
[sdm@sdm-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。

```
[sdm@sdm-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
RtyFUiyIOHKNkJbKhvgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkhB=
```

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 のオンボーディング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 オンボーディング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。これで、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

FTD デバイスに安全なログ分析 (SaaS) を導入する (11 ページ) の手順に戻って、SAL SaaS の実装を続けます。

### 関連情報:

- [Secure Device Connector のトラブルシューティング](#)
- [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 (Event Logging)] 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 \(38 ページ\)](#) を参照してください。

手順

---

**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 (Actions) ] ペインで、[削除 (Remove) ] 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 \(39 ページ\)](#) 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 \(38 ページ\)](#)」を参照してください。

#### 手順

---

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。

## 手順

- 
- 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 \(43 ページ\)](#) 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 \(41 ページ\)](#)」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 \(43 ページ\)](#)」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](#) (42 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。

### 手順

---

**ステップ 1** 1. Cisco Secure Cloud Analytics ポータル UI で、[設定 (Settings)] (⚙️) > [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。
- 分析のために Secure Cloud Analytics にネットワークフローのログデータを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、イベント情報が CDO に送信されるように設定された FTD デバイスから NetFlow データが送信されるように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 Sensor Installation Guide](#)』[英語]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 Public Cloud Monitoring Guides](#)』[英語]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 (43 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 (Event Logging)] 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 ポータルを相互起動し、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 を相互起動します。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。

### 手順

- 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 (Settings)] > [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 を相互起動する

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。

### 手順

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 [監視 (Monitoring)] > [セキュリティ分析 (Security Analytics)] 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 (Monitor)] > [Alerts (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。

### 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ます。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 \(47 ページ\)](#)
2. [後で分析するためにアラートをスヌーズする \(48 ページ\)](#)
3. [詳細な調査のためのアラートの更新 \(48 ページ\)](#)
4. [アラートの確認と調査の開始 \(49 ページ\)](#)
5. [エンティティとユーザーの調査 \(51 ページ\)](#)
6. [Secure Cloud Analytics を使用して問題を解決する \(52 ページ\)](#)
7. [アラートの更新とクローズ \(53 ページ\)](#)

## 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 への相互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。

次の質問に教えてください。

- 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：

### 手順

**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なら、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 (Unsnuzzle 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。

### 手順

**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

**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 (Device)] 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 (Copy)] 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、接続要求に回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ド 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 を使用して問題を解決する

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。
- エンティティが不正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された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不正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する。

### 手順

**ステップ 1** Secure Cloud Analytics ポータルの UI で、[監視 (Monitor)] > [アラート (Alerts)] 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する。

- 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 (Comment)] をクリックします。

アラートをクローズして、有用だったかどうかをマークする。

1. アラートの詳細から、[アラートをクローズ (Close Alert)] をクリックします。
2. アラートが有用だった場合は [はい (Yes)] を、アラートが有用でなかった場合は [いいえ (No)] 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します。
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をオープンする

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オープンする

- 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 (Reopen Alert)] 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 (low)] または [通常 (normal)] 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 (low)]、[通常 (normal)]、または [高 (high)] に設定できます。

- [モニター (Monitor)] > [アラート (Alerts)] 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 (Alert Types and Priorities)] 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 (low)]、[中 (medium)]、または [高 (high)] 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 (Live)] 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 (Live)] 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 (Historical)] 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従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。

### 手順

- 
- 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 (Event Logging)] をクリックします。

ステップ2 [ライブ (Live) ] 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 \(55 ページ\)](#)
- [履歴イベントの表示 \(56 ページ\)](#)
- [イベントビューのカスタマイズ \(57 ページ\)](#)

## 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に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 (Historical) ] 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。準備ができたなら、ライブイベントのストリーミングを再開できます。

### イベントの受信と報告

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。

Events

Search by event fields and values

Historical **Live**

| Date/Time                                        | Event Type |
|--------------------------------------------------|------------|
| ⚙️ Waiting for matching events after 1:38:40 PM. |            |
| May 31, 2019 1:33:35 PM                          | Connection |
| May 31, 2019 1:33:36 PM                          | Connection |
| May 31, 2019 1:33:44 PM                          | Connection |

## 履歴イベントの表示

[ライブ (Live)] 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 (Historical)] 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。

### 手順

- 
- ステップ 1** ナビゲーションウィンドウで、[モニタリング (Monitoring)] > [イベントロギング (Event Logging)] 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 (Historic)] 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

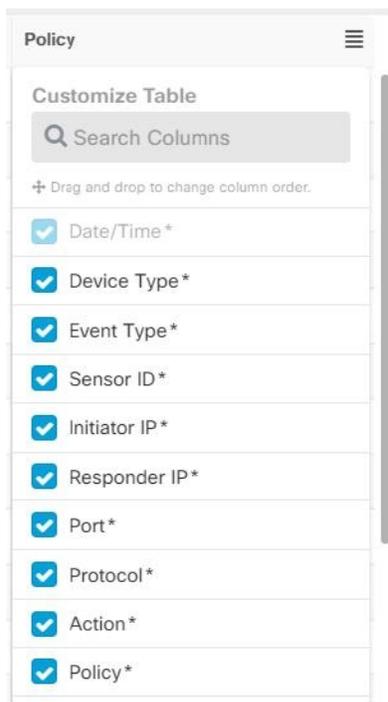
[イベントロギング (Event Logging) ] ページに加えられた変更は、このページから移動して後で戻ったときに備えて自動的に保存されます。



- (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カラムの表示および非表示

[イベントロギング (Event Logging) ] ページには、構成済み 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 (Event Logging) ] ページの列を表示したり非表示にしたりできます。

## 手順

- ステップ 1** CDO の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 2** テーブルの右端までスクロールし、[列の表示/非表示 (Show/Hide Columns) ] 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 (Show/Hide Columns) ] ドロップダウンメニューの列名の上にマウスを置き、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。

以下の表はカラム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   | または<br>FTD (Firepower Threat Defense)     |

| カラム ヘッダ               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| イベント タイプ (Event Type) | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>FTD イベントタイプ</b> <ul style="list-style-type: none"> <li>• 接続：アクセスコントロールルールからの接続イベントを表示します。</li> <li>• ファイル：アクセスコントロール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。</li> <li>• 侵入：アクセスコントロール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。</li> <li>• マルウェア：アクセスコントロール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。</li> </ul> </li> <li>• <b>ASA イベントタイプ</b>：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、『<a href="#">ASA イベントタイプ</a>』を参照してください。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• <b>ASANetFlow イベント ID</b>：ASA からのすべての <a href="#">Netflow (NSEL) イベント</a> がここに表示されます。</li> </ul> </li> </ul> |

| 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нда 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                         | セッションレスポнда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 <b>ResponderPort</b> 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。                                                                                                                                              |

| コラム ヘッダ | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アクション   | <p>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。</p> <ul style="list-style-type: none"> <li>• 接続イベントタイプの場合、フィルタは <code>AC_RuleAction</code> 属性で一致を検索します。それらの値は、<code>Allow</code>、<code>Block</code>、<code>Trust</code> の可能性があります。</li> <li>• ファイルイベントタイプの場合、フィルタは <code>FileAction</code> 属性で一致を検索します。それらの値は、<code>Allow</code>、<code>Block</code>、<code>Trust</code> の可能性があります。</li> <li>• 侵入イベントタイプの場合、フィルタは <code>InLineResult</code> 属性で一致を検索します。それらの値は、<code>Allowed</code>、<code>Blocked</code>、<code>Trusted</code> の可能性があります。</li> <li>• マルウェアイベントタイプの場合、フィルタは <code>FileAction</code> 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。</li> <li>• syslog および NetFlow イベントタイプの場合、フィルタは <code>Action</code> 属性で一致を検索します。</li> </ul> |
| ポリシー    | <p>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。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

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（98 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。

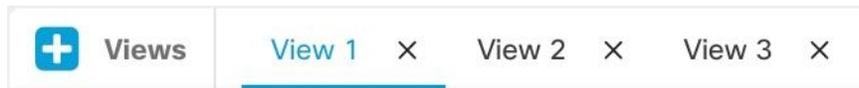
フィルタの要素は、設定時にフィルタのタブに保存されます。[イベントロギング (Event Logging)] ページに戻るたびに、これらの検索機能を使用できます。テナントの他の CDO ユーザーは使用できません。複数のテナントを管理している場合、別のテナントでは使用できません。



(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。

## 手順

- 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 (Event Logging)] 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 \(98 ページ\)](#) 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 (Event Logging)] 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カラムの表示および非表示 \(58 ページ\)](#)」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 (Event Logging)] 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 \(98 ページ\)](#) 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 \(63 ページ\)](#) 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。

## 手順

- 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 \(64 ページ\)](#) について学ぶ

# .CSV.GZ ファイルの生成

## 手順

- 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 (Historical)**] 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 (Cancel) ] をクリックします。

## .CSV.GZ ファイルのダウンロード

### 手順

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 [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。

- Firepower Threat Defense (FTD) 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。

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。

- 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、イベントログインテーブルの[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                          |

| EventGroup  | EventGroupDefinition                          | Syslog メッセージ ID 番号 (最初の 3 桁)        |
|-------------|-----------------------------------------------|-------------------------------------|
| 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<br>コントロール用の EAP または<br>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、<br>210、311、709 |
| 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、<br>グレーリスト                      | 338                                 |
| lic         | ライセンスリング                                      | 444                                 |
| mdm-proxy   | MDM プロキシ                                      | 802                                 |
| nac         | ネットワーク アドミッション<br>コントロール                      | 731、732                             |

| EventGroup     | EventGroupDefinition          | Syslog メッセージ ID 番号 (最初の 3 桁)                                                    |
|----------------|-------------------------------|---------------------------------------------------------------------------------|
| 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                                                                             |
| 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                                         |

| EventGroup     | EventGroupDefinition         | Syslog メッセージ ID 番号 (最初の 3 桁) |
|----------------|------------------------------|------------------------------|
| 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、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。たとえば、[イベントロギング (Event Logging) ]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](#)
- [ボットネット Syslog イベント ID とイベント名](#)
- [フェールオーバー Syslog イベント ID とイベント名](#)
- [ファイアウォール拒否 Syslog イベント ID とイベント名](#)
- [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](#)
- [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](#)
- [IPSec Syslog イベント ID とイベント名](#)
- [NAT Syslog イベント ID とイベント名](#)
- [SSL VPN Syslog イベント ID とイベント名](#)

### AAA Syslog イベント ID とイベント名

| EventID | EventName  |
|---------|------------|
| 109001  | AAA Begin  |
| 109002  | AAA Failed |

| EventID | EventName                           |
|---------|-------------------------------------|
| 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                       |
| 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                       |

| EventID | EventName               |
|---------|-------------------------|
| 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           |
| 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         |

| EventID | EventName                |
|---------|--------------------------|
| 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       |
| 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               |
| 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            |

| EventID | EventName                             |
|---------|---------------------------------------|
| 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   |

| EventID | EventName                               |
|---------|-----------------------------------------|
| 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            |
| 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     |

| EventID | EventName                |
|---------|--------------------------|
| 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           |
| 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        |

| EventID | EventName                                |
|---------|------------------------------------------|
| 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        |
| 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       |

| EventID | EventName                             |
|---------|---------------------------------------|
| 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                |
| 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                 |

| EventID | EventName                            |
|---------|--------------------------------------|
| 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                  |
| 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            |

| EventID | EventName                       |
|---------|---------------------------------|
| 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                   |
| 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        |

| EventID | EventName                |
|---------|--------------------------|
| 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          |
| 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             |

| EventID | EventName              |
|---------|------------------------|
| 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                       |
| 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 |

| EventID | EventName                                      |
|---------|------------------------------------------------|
| 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                                   |
| 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       |

| EventID | EventName                             |
|---------|---------------------------------------|
| 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              |
| 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   |

| EventID | EventName                        |
|---------|----------------------------------|
| 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           |
| 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               |

| EventID | EventName                         |
|---------|-----------------------------------|
| 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     |
| 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  | デバイスマネージャあり : バージョン 6.5.0         |
| 722040  | デバイスマネージャあり : バージョン 6.5.0         |
| 722041  | WebVPN SVC IPv6 not available     |
| 722042  | WebVPN invalid protocol           |
| 722043  | WebVPN DTLS disabled              |

| EventID                   | EventName                            |
|---------------------------|--------------------------------------|
| 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              |
| 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              |
| デバイスマネージャあり : バージョン 7.0.0 | SSL Client session resume            |
| 725004                    | SSL Client request Authentication    |
| 725005                    | SSL Server request authentication    |

| EventID | EventName                     |
|---------|-------------------------------|
| 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 (Event Logging) ] 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。

| Historical               |                                                                  | Live          |                            |                          |      |          |                      |                                                  |                                       |
|--------------------------|------------------------------------------------------------------|---------------|----------------------------|--------------------------|------|----------|----------------------|--------------------------------------------------|---------------------------------------|
| Date/Time                | Event Type                                                       | Sensor ID     | Initiator                  | Responder                | Port | Protocol | Action               | Policy                                           |                                       |
| Aug 20, 2019 10:44:14 AM | Malware                                                          | 192.168.20.53 |                            |                          | 80   | tcp      | Cloud Lookup Timeout | BlockOfficeDocumentsPDFUpload_BlockMalwareOthers |                                       |
| <b>2</b> Application     | HTTP                                                             |               | <b>3</b> FileSize          | 68                       |      |          |                      | <b>5</b> SensorID                                | 192.168.20.53                         |
| ClientApplication        | Web browser                                                      |               | FileType                   | EICAR                    |      |          |                      | SHA_Disposition                                  | Unavailable                           |
| EventSecond              | 1566312254                                                       |               | <b>3</b> FirstPacketSecond | Aug 20, 2019 10:44:08 AM |      |          |                      | SperoDisposition                                 | Spero detection not performed on file |
| EventType                | MalwareEvent                                                     |               | InitiatorIP                |                          |      |          |                      | ThreatName                                       | Unknown                               |
| FileAction               | Cloud Lookup Timeout                                             |               | <b>4</b> InitiatorPort     | 65386                    |      |          |                      | timestamp                                        | Aug 20, 2019 10:44:14 AM              |
| FileDirection            | Download                                                         |               | <b>4</b> LastPacketSecond  | Aug 20, 2019 10:44:14 AM |      |          |                      | URI                                              | /eicar.com                            |
| FileName                 | eicar.com                                                        |               | Protocol                   | tcp                      |      |          |                      | UserName                                         | No Authentication Required            |
| FilePolicy               | BlockOfficeDocumentsPDFUpload_BlockMalwareOthers                 |               | ResponderIP                |                          |      |          |                      |                                                  |                                       |
| FileSHA256               | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f |               | ResponderPort              | 80                       |      |          |                      |                                                  |                                       |

| Date/Time                | Device Type                                                                                                                                               | Event Type | Sensor ID           | Initiator IP | Responder IP | Port | Protocol | Action                   | Policy                        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------|--------------|--------------|------|----------|--------------------------|-------------------------------|
| Jun 12, 2020, 7:27:02 AM | ASA                                                                                                                                                       | 302013     | admin               | 192.168.25.4 | 192.168.0.68 | 443  | TCP      | Built                    |                               |
| <b>6</b> Action          | Built                                                                                                                                                     |            | <b>EventType</b>    | 302013       |              |      |          | <b>Protocol</b>          | TCP                           |
| ConnectionID             | 1169028                                                                                                                                                   |            | IngressInterface    | management   |              |      |          | ResponderIP              | 192.168.0.68                  |
| DeviceType               | ASA                                                                                                                                                       |            | InitiatorIP         | 192.168.25.4 |              |      |          | ResponderPort            | 443                           |
| Direction                | inbound                                                                                                                                                   |            | InitiatorPort       | 36540        |              |      |          | SensorID                 | admin                         |
| EgressInterface          | identity                                                                                                                                                  |            | MappedInitiatorIP   | 192.168.25.4 |              |      |          | Severity                 | Informational                 |
| EventGroup               | session                                                                                                                                                   |            | MappedInitiatorPort | 36540        |              |      |          | <b>6</b> SyslogTimestamp | 2020-06-12 11:15:26 +0000 UTC |
| EventGroupDefinition     | User Session                                                                                                                                              |            | MappedResponderIP   | 192.168.0.68 |              |      |          | timestamp                | Jun 12, 2020, 7:27:02 AM      |
| EventName                | Built TCP                                                                                                                                                 |            | MappedResponderPort | 443          |              |      |          |                          |                               |
| Message                  | ASA-6-302013: Built inbound TCP connection 1169028 for management:192.168.25.4/36540 (192.168.25.4/36540) to identity:192.168.0.68/443 (192.168.0.68/443) |            |                     |              |              |      |          |                          |                               |

| Date/Time                    | Device Type                  | Event Type | Sensor ID                  | Initiator IP                 | Responder IP  | Port                    | Protocol                     | Action | Policy |
|------------------------------|------------------------------|------------|----------------------------|------------------------------|---------------|-------------------------|------------------------------|--------|--------|
| Jun 12, 2020, 7:27:13 AM     | ASA                          | 5          | 192.168.0.169              | 192.168.25.4                 | 192.168.0.169 | 443                     | TCP                          | Update |        |
| <b>Action</b>                | Update                       |            | <b>InitiatorBytes</b>      | 0                            |               | <b>Protocol</b>         | TCP                          |        |        |
| <b>ConnectionID</b>          | 482168                       |            | <b>InitiatorIP</b>         | 192.168.25.4                 |               | <b>ResponderBytes</b>   | 3581                         |        |        |
| <b>DeviceType</b>            | ASA                          |            | <b>InitiatorPackets</b>    | 0                            |               | <b>ResponderIP</b>      | 192.168.0.169                |        |        |
| <b>EgressInterface</b>       | 65535                        |            | <b>InitiatorPort</b>       | 38068                        |               | <b>ResponderPackets</b> | 33                           |        |        |
| <b>EventType</b>             | 5                            |            | <b>LastPacketSecond</b>    | Jun 12, 2020, 7:27:07 A<br>M |               | <b>ResponderPort</b>    | 443                          |        |        |
| <b>FirewallExtendedEvent</b> | 2034                         |            | <b>MappedInitiatorIP</b>   | 192.168.25.4                 |               | <b>SensorID</b>         | 192.168.0.169                |        |        |
| <b>FirstPacketSecond</b>     | Jun 12, 2020, 7:27:07 A<br>M |            | <b>MappedInitiatorPort</b> | 38068                        |               | <b>Severity</b>         | Informational                |        |        |
| <b>ICMPCode</b>              | 0                            |            | <b>MappedResponderIP</b>   | 192.168.0.169                |               | <b>timestamp</b>        | Jun 12, 2020, 7:27:13 A<br>M |        |        |
| <b>ICMPTYPE</b>              | 0                            |            | <b>MappedResponderPort</b> | 443                          |               |                         |                              |        |        |
| <b>IngressInterface</b>      | 9                            |            | <b>NetFlowTimestamp</b>    | 1591961232                   |               |                         |                              |        |        |

| ケース | 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。                                                                                                                                                                                                  |
| 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。<br><br>FirstPacketSecond の値は、LastPacketSecond から ConnectionDuration を差し引いて計算されます。<br><br>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。                                                                                                                                                   |

| ケース | ラベル              | 説明                                                                                                            |
|-----|------------------|---------------------------------------------------------------------------------------------------------------|
| 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。

### 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りますため、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るため、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、こ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 \(47 ページ\)](#)
2. [後で分析するためにアラートをスヌーズする \(48 ページ\)](#)
3. [詳細な調査のためのアラートの更新 \(48 ページ\)](#)
4. [アラートの確認と調査の開始 \(49 ページ\)](#)
5. [エンティティとユーザーの調査 \(51 ページ\)](#)
6. [Secure Cloud Analytics を使用して問題を解決する \(52 ページ\)](#)
7. [アラートの更新とクローズ \(53 ページ\)](#)

## 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 への相互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。

次の質問に教えてください。

- 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：

### 手順

- 
- 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れば、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 (Unsnoodle 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。

### 手順

- 
- 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

---

**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 (Device)] 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 (Copy)] 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ド 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する。

### 手順

**ステップ 1** Secure Cloud Analytics ポータルの UI で、[監視（Monitor）] > [アラート（Alerts）] 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する。

- 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（Comment）] をクリックします。

アラートをクローズして、有用だったかどうかをマークする。

1. アラートの詳細から、[アラートをクローズ（Close Alert）] をクリックします。
2. アラートが有用だった場合は [はい（Yes）] を、アラートが有用でなかった場合は [いいえ（No）] 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します。
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をオープンする

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オープンする

- 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（Reopen Alert）] 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 (low)] または [通常 (normal)] 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 (low)]、[通常 (normal)]、または [高 (high)] に設定できます。

- [モニター (Monitor)] > [アラート (Alerts)] 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 (Alert Types and Priorities)] 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 (low)]、[中 (medium)]、または [高 (high)] 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。

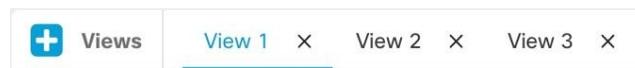
- [ライブまたは履歴イベントのフィルタ処理 \(99 ページ\)](#)
- [NetFlow イベントのみフィルタ処理 \(101 ページ\)](#)
- [ASA または FTD Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない \(101 ページ\)](#)
- [フィルタ要素の結合 \(101 ページ\)](#)

## 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 (Event Logging)] 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。

### 手順

- 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 (Event Logging)] をクリックします。
- ステップ 2** [履歴 (Historical)] タブまたは [ライブ (Live)] 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**：アクセスコントロールルールからの接続イベントを表示します。
- **ファイル**：アクセスコントロール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**：アクセスコントロール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**：アクセスコントロール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。

これらのイベントタイプの詳細については、「[FTD イベントタイプ](#)」を参照してください。

- **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。
- **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нда** : 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ндаの間または両方のスペース）。
  - **レスポнда** : セッションレスポнда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

**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。

### 手順

- 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 (Event Logging)**] 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 (Event Logging)] テーブルには、ASA NetFlow イベントのみが表示されず。

## 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

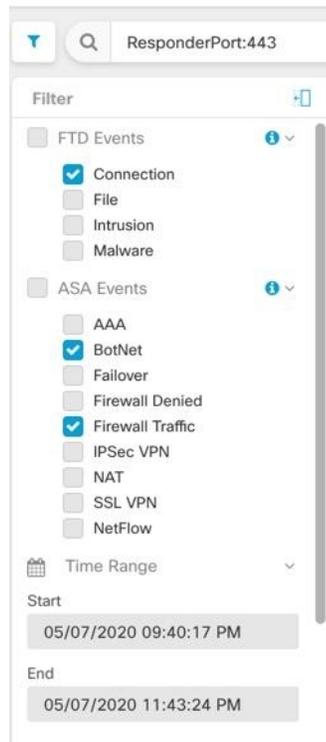
この手順では、syslog イベントのみを検索します。

### 手順

- 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 (Event Logging)**] 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「かつ (AND)」が適用され、カテゴリ内の値は「または (OR)」が適用されます。フィルタ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「または」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「または」ASAのBotNetイベント「または」ファイアウォールトラフィックイベント、「かつ」時間範囲内の2つの時間の間に発生したイベント、「かつ」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リングできます。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、イベントログテーブルで、検索する属性をクリックすることです。それにより、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、マウスの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。

Event Logging

InitiatorIP: \*192.168.20.56\* AND EventType: \*302015\*

Time Range: After 07/30/2020 03:03:27 PM

| Date/Time                | Device Type | Event Type | Sensor ID     | Initiator IP  | Responder IP | Port | Protocol | Action | Policy |
|--------------------------|-------------|------------|---------------|---------------|--------------|------|----------|--------|--------|
| Jul 30, 2020, 3:05:51 PM | ASA         | 302015     | 192.168.20.56 | 192.168.20.56 | 192.168.0.1  | 123  | UDP      | Built  |        |

302015

|                             |                                                                                                                                                              |                            |               |                        |                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------|------------------------|--------------------------------------|
| <b>Action</b>               | Built                                                                                                                                                        | <b>EventType</b>           | 302015        | <b>Protocol</b>        | UDP                                  |
| <b>ConnectionID</b>         | 262235340                                                                                                                                                    | <b>IngressInterface</b>    | identity      | <b>ResponderIP</b>     | 192.168.0.1                          |
| <b>ConnectorID</b>          | 46b319c6-e21d-45b7-a9bd-d7c40fdcae                                                                                                                           | <b>InitiatorIP</b>         | 192.168.20.56 | <b>ResponderPort</b>   | 123                                  |
| <b>DeviceType</b>           | ASA                                                                                                                                                          | <b>InitiatorPort</b>       | 65535         | <b>SensorID</b>        | 192.168.20.56                        |
| <b>Direction</b>            | outbound                                                                                                                                                     | <b>MappedInitiatorIP</b>   | 192.168.20.56 | <b>Severity</b>        | Informational                        |
| <b>EgressInterface</b>      | management                                                                                                                                                   | <b>MappedInitiatorPort</b> | 65535         | <b>SyslogTimestamp</b> | 2020-07-30 19:05:50.654351 +0000 UTC |
| <b>EventGroup</b>           | session                                                                                                                                                      | <b>MappedResponderIP</b>   | 192.168.0.1   | <b>timestamp</b>       | Jul 30, 2020, 3:05:51 PM             |
| <b>EventGroupDefinition</b> | User_Session                                                                                                                                                 | <b>MappedResponderPort</b> | 123           |                        |                                      |
| <b>EventName</b>            | Built_UDP                                                                                                                                                    |                            |               |                        |                                      |
| <b>Message</b>              | ASA-6-302015: Built outbound UDP connection 262235340 for management:192.168.0.1/123 (192.168.0.1/123) to identity:192.168.20.56/65535 (192.168.20.56/65535) |                            |               |                        |                                      |

この例では、イニシエータ IP (InitiatorIP) の値である 192.168.20.56 にマウスの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。「InitiatorIP」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 (EventType) の値である 302015 にマウスのカーソルが合わされてクリックされ、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、「かつ」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のカーソルを合わせ、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、「または」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、「以外 (NOT)」しか使用できないことに注意してください。

Event Logging

InitiatorIP: \*192.168.20.56\* OR EventType: \*302015\*

Time Range: After 08/11/2020 07:22:53 PM

| Date/Time                | Device Type | Event Type | Sensor ID     | Initiator IP  | Responder IP | Port | Protocol | Action | Policy |
|--------------------------|-------------|------------|---------------|---------------|--------------|------|----------|--------|--------|
| Aug 11, 2020, 7:38:30... | ASA         | 302015     | 192.168.20.56 | 192.168.20.56 | 192.168.0.1  | 123  | udp      | Built  |        |

302015

|                             |                                                                                                                                                              |                            |               |                        |                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------|------------------------|--------------------------------------|
| <b>Action</b>               | Built                                                                                                                                                        | <b>EventType</b>           | 302015        | <b>Protocol</b>        | udp                                  |
| <b>ConnectionID</b>         | 262292132                                                                                                                                                    | <b>IngressInterface</b>    | identity      | <b>ResponderIP</b>     | 192.168.0.1                          |
| <b>ConnectorID</b>          | 46b319c6-e21d-45b7-a9bd-d7c40fdcae                                                                                                                           | <b>InitiatorIP</b>         | 192.168.20.56 | <b>ResponderPort</b>   | 123                                  |
| <b>DeviceType</b>           | ASA                                                                                                                                                          | <b>InitiatorPort</b>       | 65535         | <b>SensorID</b>        | 192.168.20.56                        |
| <b>Direction</b>            | outbound                                                                                                                                                     | <b>MappedInitiatorIP</b>   | 192.168.20.56 | <b>Severity</b>        | Informational                        |
| <b>EgressInterface</b>      | management                                                                                                                                                   | <b>MappedInitiatorPort</b> | 65535         | <b>SyslogTimestamp</b> | 2020-08-11 23:38:29.503612 +0000 UTC |
| <b>EventGroup</b>           | session                                                                                                                                                      | <b>MappedResponderIP</b>   | 192.168.0.1   | <b>timestamp</b>       | Aug 11, 2020, 7:38:30 PM             |
| <b>EventGroupDefinition</b> | User_Session                                                                                                                                                 | <b>MappedResponderPort</b> | 123           |                        |                                      |
| <b>EventName</b>            | Built_UDP                                                                                                                                                    |                            |               |                        |                                      |
| <b>Message</b>              | ASA-6-302015: Built outbound UDP connection 262292132 for management:192.168.0.1/123 (192.168.0.1/123) to identity:192.168.20.56/65535 (192.168.20.56/65535) |                            |               |                        |                                      |

マウスの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想されます。

```
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想されます。

```
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нда 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カラム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 がオンボーディングされた 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。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) のトライアル版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 日目は削除されます。

お客様は、発注変更によってイベント保持期間をデフォルトの 90 日間よりも長くアップグレードするか、日単位のボリューム (GB/日) を追加できます。請求は、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、その後削除されます。

#### 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アプローチは次の 2 つです。

- **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、アクセスコントロールルール、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。現在ログに記録しているルールを調べてください。現在記録が必要だと考えているログイベントの数は適切でしょうか。

## 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 [ライセンス](#) 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。

#### 手順

- 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。

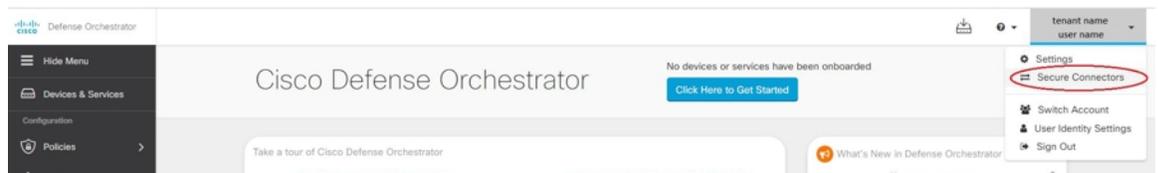
増加したコストは、既存のライセンスの残りの期間に基づいて比例配分されます。詳細な手順については、[Secure Logging Analytics \(SaaS\) 発注ガイド \[英語\]](#) を参照してください。

## 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。

#### 手順

- ステップ 1** アカウントメニューをクリックし、[設定 (Settings)] 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 か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。

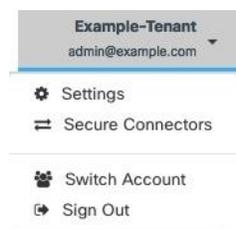
- TCP : 10125
- UDP : 10025
- NSEL : 10425

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。

## 手順

**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 (Details) ] 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。

## Boston-SEC

### Details

|                     |                         |
|---------------------|-------------------------|
| <b>ID</b>           | 54b039f6-8944-46a4-ac07 |
| <b>Tenant ID</b>    | 0a2cddb4-5e63-4491-9fda |
| <b>Version</b>      | 202004270848            |
| <b>IP Address</b>   | 192.168.25.4            |
| <b>TCP Port</b>     | 10125                   |
| <b>UDP Port</b>     | 10025                   |
| <b>NetFlow Port</b> | 10425                   |

