



Cisco Secure Network Analytics 7.5.2 向け Cisco Security Analytics and Logging（オンプレミス）：ファイアウォールイベント統合ガイド

最終更新：2025年7月23日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 1 章

はじめに 1

概要 1

概念とアーキテクチャ 1

サポートされるイベント タイプ 3

第 2 章

展開 5

要件 5

Secure Network Analytics のライセンス 8

Secure Network Analytics Resource Allocation 8

通信ポート 11

構成概要 11

Secure Network Analytics の展開と設定 12

Data Store の展開と設定 13

Secure Firewall Management Center の設定 14

Secure Firewall Management Center でのウィザードの設定 14

Data Store 展開にイベントデータを送信するように Secure Firewall Management Center を設定する 15

Syslog を使用してデータプレーンイベントログを Secure Network Analytics に送信するように Secure Firewall Management Center を構成する 18

Management Center での優先度が低い接続イベントの保存の停止 19

ASA デバイスの設定 20

ASA デバイスから syslog イベントを送信するための CLI コマンド 21

ASA デバイスから syslog イベントを送信するための ASDM 設定 22

ASA デバイスから syslog イベントを送信するための CSM 設定 24

第 3 章

次のステップ 27

次のステップ 27

Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Management Center での作業 27

相互起動を使用したイベントの調査 28

付録 A :

障害対応 31

障害対応 31



第 1 章

はじめに

- [概要 \(1 ページ\)](#)

概要

このガイドでは、ファイアウォールのイベントデータを保存し、より長い保存期間でストレージを増やすように Cisco Security Analytics and Logging (On Premises)を設定する方法について説明します。Cisco Secure Network Analytics (旧 Stealthwatch) アプライアンスを展開し、Firewall 展開に統合することで、イベントデータを Secure Network Analytics アプライアンスにエクスポートできます。

その後、次の操作を実行できます。

- Secure Firewall Management Centerにイベントを保存し、Secure Network Analytics 展開にイベントを保存します。
- このリモートデータソースを指定して、management center でこれらのイベントを表示します。
- イベントビューアを使用して、Cisco Secure Network Analytics Manager (旧 Stealthwatch 管理コンソール) Web アプリケーション UI からイベントデータを確認します。
- management center UI からイベントビューアに相互起動して、相互起動元の情報に関する追加のコンテキストを表示します。



(注) オンプレミスではなく Cisco Cloud にファイアウォールイベントデータを保存する場合、詳細については [Cisco Security Analytics and Logging \(SaaS\) documentation](#) を参照してください。

概念とアーキテクチャ

Security Analytics and Logging (OnPrem) 展開では、Secure Network Analytics アプライアンスを使用して、別のシスコ製品展開からのデータを保存できます。Secure Firewall 展開の場合、セキュ

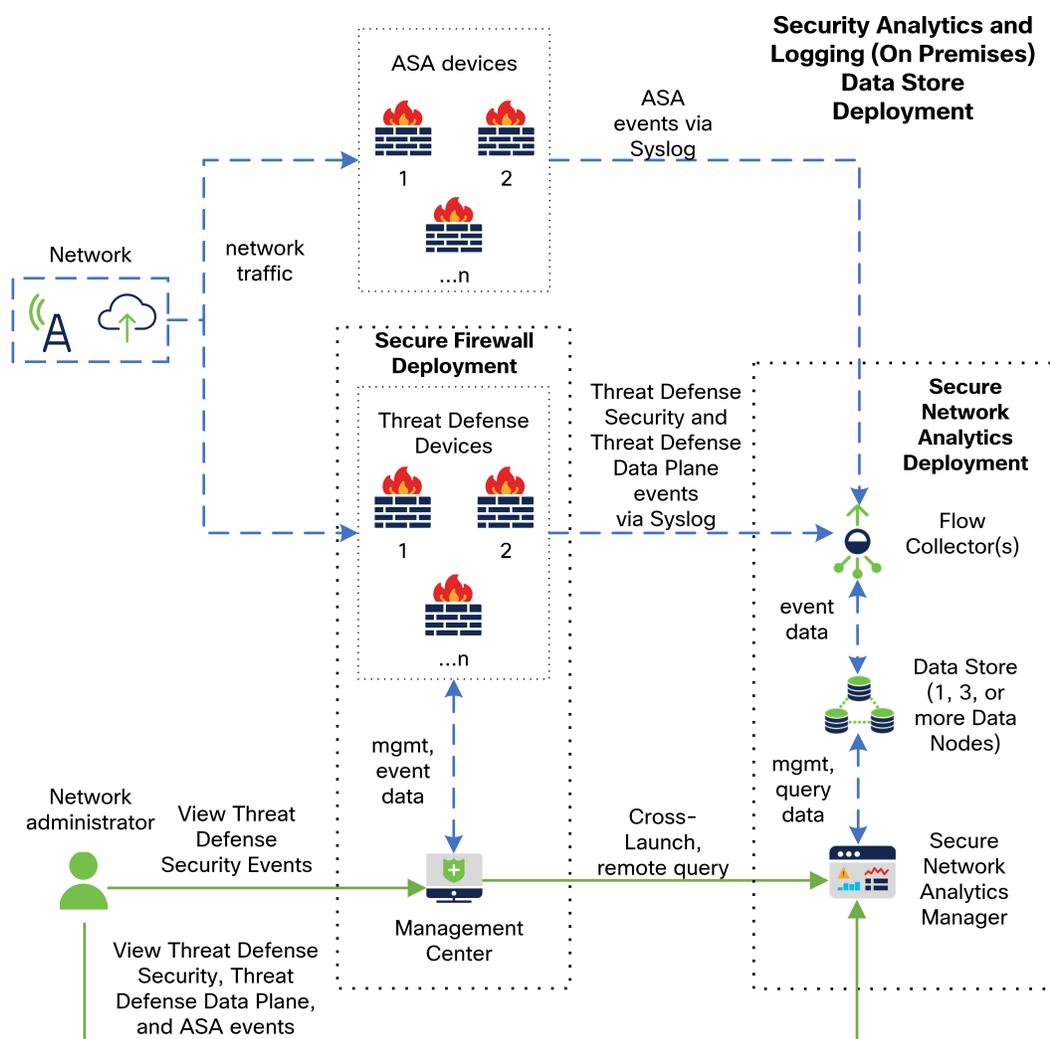
リタイムイベントおよびデータプレーンイベントを management center が管理する Secure Firewall Threat Defense デバイスから Manager にエクスポートして、その情報を保存します。

Secure Network Analytics は次のように展開できます。

- **Data Store** : イベントを受信する Cisco Secure Network Analytics Flow Collector (最大5つ)、イベントを保存する Cisco Secure Network Analytics Data Store (3つの Cisco Secure Network Analytics データノードのセットのうち1つ、3つ、またはそれ以上を装備)、イベントを確認および照会できる Manager を展開します。

Data Store

Manager、データノード、および Flow Collector を使用した Data Store の展開の例については、次の図を参照してください。



この展開では、threat defense および Secure Firewall ASA デバイスはファイアウォールのイベントを Flow Collector に送信します。Flow Collector は、保存のためにデータストアにイベントを送信します。ユーザは management center の UI から Manager を相互起動して保存されたイベン

トに関する詳細情報を表示できます。また、management center からリモートでイベントを照会することもできます。

サポートされるイベントタイプ

- Threat Defense セキュリティイベント
 - 接続
 - 侵入
 - ファイルおよびマルウェア
- Threat Defense データプレーンイベント
- ASA イベント



第 2 章

展開

- 要件 (5 ページ)
- 構成概要 (11 ページ)
- Secure Network Analytics の展開と設定 (12 ページ)
- Secure Firewall Management Center の設定 (14 ページ)
- ASA デバイスの設定 (20 ページ)

要件

次に、ファイアウォールのイベントデータを保存するために Security Analytics and Logging (OnPrem) を展開するためのアプライアンス要件を示します。

ファイアウォール アプライアンス

次のファイアウォール アプライアンスを展開する必要があります。

ソリューションのコンポーネント	必要なバージョン	Security Analytics and Logging (OnPrem) のライセンス	注記
Secure Firewall Management Center (ハードウェアまたは仮想)	v7.2+ 以前のバージョンを実行している management center の場合は、 「 https://cisco.com/go/sal-on-prem-docs 」を参照してください。	なし	• management center ごとに1つの Manager、また必要に応じて複数の Flow Collector と データストアを展開できます。

ソリューションのコンポーネント	必要なバージョン	Security Analytics and Logging (OnPrem) のライセンス	注記
Secure Firewall 管理対象のデバイス	v7.0+ (ウィザードを使用) Threat Defense v6.5 以降 (syslog を使用) NGIPS v6.5 (syslog を使用)	none	<ul style="list-style-type: none"> threat defense v6.5 に対して syslog を使用方法の詳細については、「以前のバージョンの Threat Defense デバイスからイベントを送信する」を参照してください。
ASA デバイス	v9.12+	なし	

Cisco Secure Network Analytics アプライアンス

Secure Network Analytics は次のように展開できます。

- **Data Store** : Flow Collector を展開してイベントを取り込み、データストアを展開してイベントを保存し、Manager を展開してイベントを確認および照会します。

表 1 : Data Store

ソリューションのコンポーネント	必要なバージョン	Security Analytics and Logging (OnPrem) のライセンス	注記
Manager	Secure Network Analytics v7.5.2	なし	<ul style="list-style-type: none"> 単一ノードデータストアと複数テレメトリには、Secure Network Analytics v7.5.2 が必要です。

ソリューションのコンポーネント	必要なバージョン	Security Analytics and Logging (OnPrem) のライセンス	注記
Flow Collector	Secure Network Analytics v7.5.2	なし	<ul style="list-style-type: none"> • データストア用に設定された最大5つの Flow Collector を展開できます。 • 複数台の threat defense デバイスからイベントを受信できます。これらはすべて1つの management center によって管理されます。 • 複数の ASA デバイスから ASA イベントを受信できます。 • 単一ノードデータストアと複数テレメトリには、Secure Network Analytics v7.5.2 が必要です。
データストア	Secure Network Analytics v7.5.2	なし	<ul style="list-style-type: none"> • 3つのデータノードのセットに1つ、3つ、またはそれ以上を展開できます。 • Flow Collector で受信したファイアウォールイベントを保存できます。 • 単一ノードデータストアと複数テレメトリには、Secure Network Analytics v7.5.2 が必要です。

これらのコンポーネントに加えて、すべてのアプライアンスが NTP を使用して時刻を同期できることを確認する必要があります。

Secure Firewall または Secure Network Analytics アプライアンスのコンソールにリモートでアクセスする場合は、SSH 経由のアクセスを有効にできます。

Secure Network Analytics のライセンス

ライセンスなしで、Security Analytics and Logging (OnPrem) を 90 日間評価モードで使用できます。90 日間経過した後も Security Analytics and Logging (OnPrem) の使用を継続するには、ファイアウォール展開から Secure Network Analytics アプライアンスに syslog データで送信する見込みの 1 日あたりの GB に基づいて、スマートライセンスのロギングとトラブルシューティングのスマートライセンスを取得する必要があります。



(注) ライセンスの計算のために、データ量は最も近い GB 数 (切り捨て) で報告されます。たとえば、1 日あたり 4.9 GB を送信する場合は、4 GB と報告されます。

Secure Network Analytics アプライアンスのライセンスに関する詳細については、『[Secure Network Analytics Smart Software Licensing Guide](#)』を参照してください。

Secure Network Analytics Resource Allocation

Security Analytics and Logging (OnPrem) に展開した場合、Secure Network Analytics は次の取り込みレートを提供します。

- 3 つのデータノードを備えたバーチャルエディション (VE) Data Store の展開では、平均で最大約 50k EPS を取り込むことができ、最大 175k EPS の短いバーストが可能です。
- 3 つのデータノードを備えたハードウェア Data Store の展開では、Security Analytics and Logging (OnPrem) および `sal_to_flow_cache` ON で平均で最大約 15 万 EPS を取り込むことができます。

割り当てたハードドライブストレージに基づいて、数週間または数か月にわたってデータを保存できます。これらの推定値は、ネットワーク負荷、トラフィックスパイク、イベントごとに送信される情報など、さまざまな要因の影響を受けます。



(注) EPS の取り込みレートが高いと、Security Analytics and Logging (OnPrem) がデータをドロップする場合があります。さらに、接続、侵入、ファイル、マルウェアのイベントのみではなく、すべてのイベントタイプを送信する場合は、全体的な EPS の増加にしたがい、Security Analytics and Logging (OnPrem) がデータをドロップする場合があります。この場合はログファイルを確認します。

ネットワーク検出のファイアウォール ログ

Cisco Security Analytics and Logging (オンプレミス) データに基づくネットワーク検出を追加しました。この設定を有効にすると、トラフィックパターン、リスク、および攻撃の範囲をより詳細に把握できます。

Flow Collector 管理 UI の詳細設定に、トグル `sal_to_flow_cache` を使用して、ファイアウォール イベント ログの取り込みを有効化または無効化することができます。これは、ファイアウォール ログの取り込みがすでに有効になっている場合に、ネットワーク検出を有効または無効にするために使用されます。

Flow Collector での詳細設定の編集の詳細については、「詳細設定」のヘルプトピックを参照してください。



- (注) `sal_to_flow_cache` オプションは任意であり、セキュリティ分析およびロギング (オンプレミス) データを高度な検出のためにフロー キャッシュの一部にする場合にのみ必要です。

Data Store 推奨事項

最適なパフォーマンスを得るために、Manager VE、Flow Collector VE、およびデータストア VE を展開する場合は、次のリソースを割り当てます。



- (注) シングルノードデータストアを使用している場合、または Secure Network Analytics でマルチテレメトリを有効にしている場合、リソースの割り当てとストレージ容量は次の推奨事項と異なる場合があります。詳細については、[Secure Network Analytics アプライアンス設置ガイド \(ハードウェアまたは仮想エディション\)](#) と [システム構成ガイド v7.5.2](#) を参照してください。

表 2: Manager VE

リソース	推奨
CPU	8
RAM	64 GB
ハードドライブストレージ	480 GB

表 3: Flow Collector VE

リソース	推奨
CPU	8
RAM	70 GB
ハードドライブストレージ	480 GB

表 4: Data Nodes VE (データストアの一部として)

リソース	推奨
CPU	データノードあたり 12
RAM	データノードあたり 32 GB
ハードドライブストレージ	データノード VE あたり 5 TB、または 3 つのデータノードで合計 15 TB

ハードウェア仕様

ハードウェアの仕様については、[アプライアンスの仕様書](#)を参照してください。

推定保持期間 (3 つのデータノード)

データストア VE に割り当てるストレージスペースに基づいて、またはハードウェア展開がある場合は、Data Store 展開でおおよそ次の時間枠でデータを保存できます。

平均 EPS	平均日次イベント	仮想	ハードウェア
1,000	8,650 万	1,500 日	3,000 日
5,000	4 億 3,000 万	300 日	600 日
10,000	8 億 6,500 万	150 日	300 日
20,000	17 億 3,000 万	75 日	150 日
25,000	21 億 6,000 万	60 日	120 日
50,000	43 億 2,000 万	30 日	60 日後
75,000	64 億 8,000 万	サポート対象外	40 日
100,000	86 億 4,000 万	サポート対象外	30 日

データストアが最大ストレージキャパシティに達すると、着信データ用のスペースを確保するために最も古いデータが最初に削除されます。ストレージ容量を増やすには、[Secure Network Analytics システム コンフィギュレーションガイド](#)を使用してデータノードを追加します。



- (注) この推定取り込みおよび保存の期間について、これらのリソース割り当てでこれらの仮想アプライアンスをテストしました。仮想アプライアンスに十分な CPU または RAM を割り当てないと、リソース割り当てが不十分なために予期しないエラーが発生する場合があります。データノードのストレージ割り当てを 5 TB を超えて増やすと、リソース割り当てが不十分なために予期しないエラーが発生する可能性があります。

通信ポート

次の表に Data Store の展開の場合に Security Analytics and Logging (OnPrem) を統合するために開く必要がある通信ポートを示します。さらに、Secure Network Analytics 展開のために開く必要があるポートについては、「[x2xx シリーズ ハードウェアアプライアンス設置ガイド](#)」または「[Virtual Edition アプライアンス インストールガイド](#)」を参照してください。

表 5: Data Store

送信元 (クライアント)	宛先 (サーバ)	ポート	プロトコルまたは目的
Management Center、Threat Defense デバイス、Manager、Flow Collector およびデータストア	外部インターネット (NTP サーバー)	123/UDP	すべて同じ NTP サーバへの NTP 時刻同期
ユーザワークステーション	Management Center および Manager	443/TCP	Web ブラウザを使用した HTTPS 経由でのアプライアンスの Web インターフェイスへのログイン
management center によって管理される Threat Defense デバイス	Flow Collector	8514/UDP	threat defense デバイスからの syslog のエクスポート、Flow Collector への取り込み
ASA デバイス	Flow Collector	8514/UDP	ASA デバイスからの syslog のエクスポート、Flow Collector への取り込み
Management Center	Manager	443/TCP	management center から Manager へのリモートクエリ

構成概要

次に、イベントデータを保存するための展開の大まかな設定手順を説明します。

導入を開始する前に、次のタスクを確認してください。

コンポーネントとタスク	手順
Data Store の導入	<ul style="list-style-type: none"> • Manager、Flow Collector、および1、3、またはそれ以上（3つのセット）のデータノードをネットワークに展開します。各アプライアンスの初期設定を実行し、データストアを初期化します。詳細については、『x2xx Series Hardware Appliance Installation Guide』または『Virtual Edition Appliance Installation Guide』および『Secure Network Analytics System Configuration Guide』を参照してください。
イベントを Security Analytics and Logging (OnPrem) に送信するように management center を設定	<p>次の選択肢があります。</p> <ul style="list-style-type: none"> • Secure Firewall Management Center の設定（14 ページ） セクションを使用して、イベントを Secure Network Analytics アプライアンスに送信するように management center を設定します。 • 「データプレーンイベントログの設定」セクションを使用して、データプレーンイベントロギングを設定します。 • 「Secure Firewall Management Center での優先度が低い接続イベントの保存の停止」セクションを使用して、management center のロギング負荷を軽減します。
イベントを Security Analytics and Logging (OnPrem) に送信するように ASA デバイスを設定	<ul style="list-style-type: none"> • ASA デバイスの設定（20 ページ） セクションを使用して、イベントを Secure Network Analytics アプライアンスに送信するように ASA デバイスを設定します。
次の手順の確認	<p>次の手順を確認します。</p> <ul style="list-style-type: none"> • 詳細については、Secure Firewall のオンラインヘルプを参照してください。「Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Cisco Secure Firewall Management Center での作業」を参照してください。 • Secure Network Analytics の使用方法の詳細については、「Manager オンラインヘルプ」を参照してください。[調査 (Investigate)] > [セキュリティ分析とロギング (オンプレミス) (Security Analytics and Logging (OnPrem))] に移動します。

Secure Network Analytics の展開と設定

Security Analytics and Logging (OnPrem)用の Secure Network Analytics を展開および構成するには、次の手順を実行します。

1. Secure Network Analytics 展開の手順に従います。
 - [Data Store の展開と設定 \(13 ページ\)](#)

Data Store の展開と設定



重要 アプライアンスの初回セットアップ時に、Flow Collector がファイアウォールログを取り込んで保存できるようにしてください。この設定は、Security Analytics and Logging (OnPrem) で Flow Collector を使用するように設定します。アプライアンスの構成後、Flow Collector の詳細設定を使用して、取り込み設定を更新できます。詳細については、「[Security Analytics and Logging \(OnPrem\) Configuration Using Flow Collector Advanced Settings](#)」セクションを参照してください。

始める前に

- Manager、Flow Collector、およびデータノードをネットワークに展開したこと、threat defense デバイスの管理 IP アドレスが Flow Collector 管理 IP アドレスに到達可能であること、および management center の管理 IP アドレスが Manager の管理 IP アドレスに到達可能であることを確認します。さらに設定する場合に備えて、管理 IP アドレスをメモしておきます。
- Secure Network Analytics 製品インスタンスを適切に登録します。Manager VE ライセンスは登録後にアカウントに自動的に追加されます。詳細については、『[Secure Network Analytics Smart Software Licensing Guide](#)』を参照してください。

手順

- ステップ 1 Secure Network Analytics ハードウェアアプライアンスを展開するには、『[x2xx Series Hardware Appliance Installation Guide](#)』の指示に、Secure Network Analytics 仮想アプライアンスを展開するには、『[Virtual Edition Appliance Installation Guide](#)』の指示に従います。
- ステップ 2 『[Secure Network Analytics System Configuration Guide](#)』を使用してアプライアンスを設定します。Flow Collector で初回セットアップを設定するときは、必ず次を選択してください。
 - データストアの一部として Flow Collector を展開するように求められた場合、[はい (Yes)] を選択します。[いいえ (No)] を選択した場合は、新しい仮想アプライアンスまたはアプライアンスの RFD を展開する必要があります。
 - [テレメトリタイプの選択 (Select telemetry types)] 画面で [ファイアウォールログ (Firewall Logs)] を選択します。次に、UDP ポートを入力します。デフォルトでは 8514 が使用されます。[はい (Yes)] をクリックして設定を確認します。

Secure Firewall Management Center の設定

Security Analytics and Logging (OnPrem) に Secure Firewall Management Center を設定すると、次のオプションを使用して Secure Network Analytics にイベントを送信できます。

- イベントを Secure Network Analytics 展開に直接送信するように [Management Center のウィザードを設定する](#)。
- [データプレーンイベントログを設定する](#)。

Secure Firewall Management Center でのウィザードの設定

次に、すべての Secure Firewall Management Center ユーザーがファイアウォールイベントを送信および保存するために Security Analytics and Logging (OnPrem) を展開するためのウィザードについて説明します。

- **Data Store : Flow Collector** を展開してイベントを受信し、**Data Store** を展開してイベントを保存し、**Manager** を展開してイベントを確認および照会できます。**Data Store** 展開の設定の詳細については、「[Data Store 展開にイベントデータを送信するように Secure Firewall Management Center を設定する](#)」を参照してください。

Secure Firewall 統合の前提条件

- Secure Firewall システムが予期したとおりに動作し、送信するイベントを生成する必要があります。
- Secure Network Analytics および Security Analytics and Logging (OnPrem) 製品をセットアップして、ファイアウォールイベントのデータを受信できるようにします。
- 次のいずれかの Secure Firewall ユーザーロールが必要です。
 - 管理者 (Admin)
 - アナリスト (Analyst)
 - セキュリティ アナリスト (Security Analyst)
- 現在、イベントの直接送信をサポートしているデバイスのバージョンから Secure Network Analytics に syslog を使用してイベントを送信している場合、それらのデバイスの syslog を無効にして（または syslog の設定を含めないアクセス コントロール ポリシーをそれらのデバイスに割り当てて）リモートボリュームでイベントが重複しないようにします。
- 次の詳細情報を参照してください。
 - **Manager** のホスト名または IP アドレス。

- (Flow Collectorを使用し、拡張ストレージキャパシティに対して複数の Secure Network Analytics アプライアンスを集約する場合) Flow Collector IP アドレス。(この設定にはホスト名を使用できません。)
- 管理者権限を持つ Secure Network Analytics アプライアンスのアカウントのログイン情報。

これらのログイン情報は management center に保存されません。これらの情報は、Manager の management center の読み取り専用アナリスト API アカウントを確立するために一度使用されます。この統合には専用アカウントは必要ありません。管理者自身のログイン情報を使用できます。

登録プロセス中に Manager からログアウトする場合があります。このウィザードを開始する前に、進行中の作業を完了してください。
- [最初の使用時に信頼する (trust on first use)] オプションを使用しない場合は、Manager からの SSL 証明書を使用します。

Data Store 展開にイベントデータを送信するように Secure Firewall Management Center を設定する

始める前に

- [セキュアファイアウォール統合の前提条件](#)に記載されているすべての要件を満たしていることを確認します。
- 管理対象デバイスのバージョンは 7.0 以降です。

手順

ステップ 1 management center では、[統合 (Integration)] > [セキュリティ分析とロギング (Security Analytics and Logging)] の順に移動します。

ステップ 2 [データストア (Data Store)] ウィジェットで、[開始 (Start)] をクリックします。

ステップ 3 Manager のホスト名または IP アドレスとポートを入力します。

ステップ 4 Flow Collector のホスト名または IP アドレスとポートを入力します。

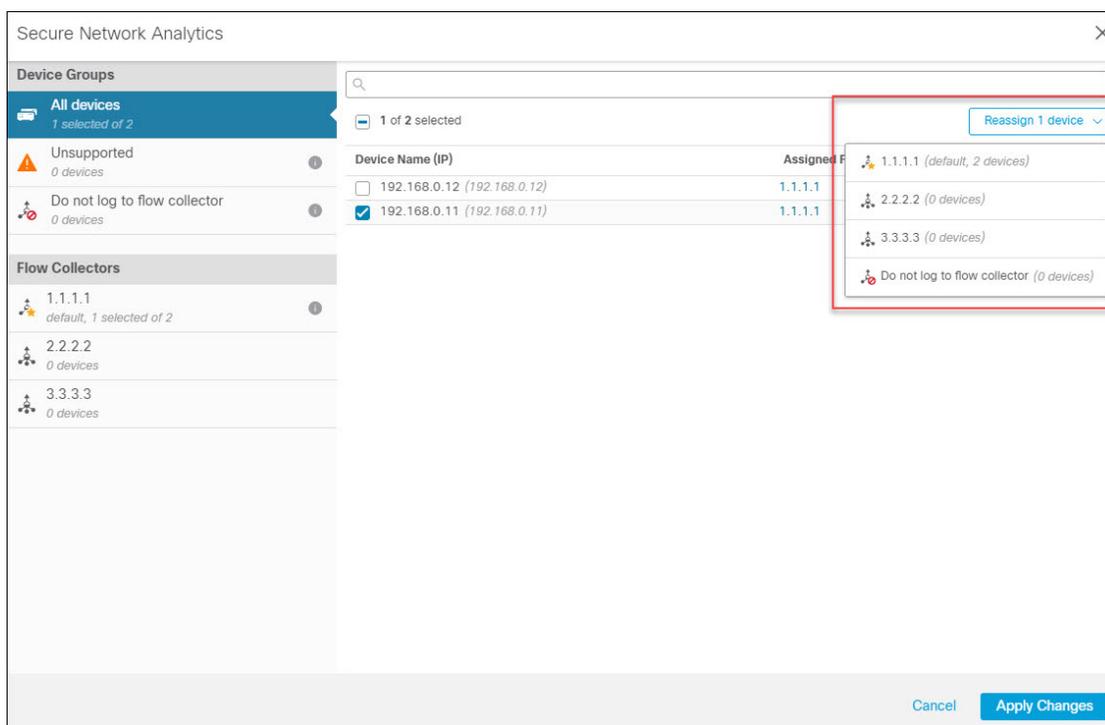
Flow Collector をさらに追加するには、[+別の Flow Collector を追加 (+ Add another flow collector)] をクリックします。

ステップ 5 (オプション) 複数の Flow Collector を設定した場合は、管理対象デバイスを異なる Flow Collector に関連付けます。

デフォルトでは、すべての管理対象デバイスがデフォルトの Flow Collector に割り当てられます。

1. [デバイスを割り当てる (Assign Devices)] をクリックします。
2. 再割り当てる管理対象デバイスを選択します。

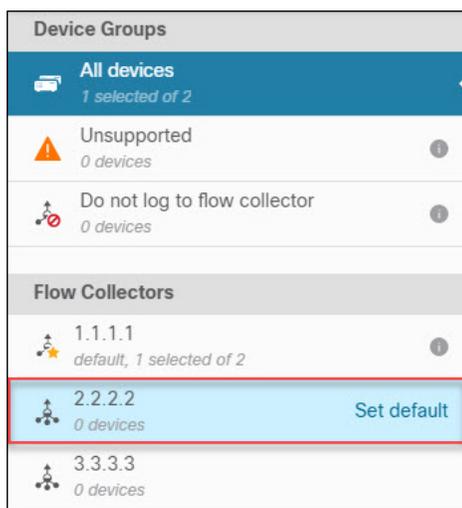
- [デバイスを再割り当てする (Reassign Device)] ドロップダウンリストから、[Flow Collector] を選択します。



管理対象デバイスがイベントデータを Flow Collector のいずれにも送信しないようにする場合は、そのデバイスを選択し、[デバイスを再割り当てする (Reassign Device)] ドロップダウンリストから [Flow Collector にログを記録しない (Do not log to flow collector)] を選択します。

(注)

デフォルトの Flow Collector を変更するには、目的の Flow Collector にカーソルを合わせ、[デフォルトの設定 (Set default)] をクリックします。



4. [変更を適用 (Apply Changes)] をクリックします。

ステップ 6 [次へ (Next)] をクリックします。

ステップ 7 検出された設定を確認します。

1. クロス起動 URL とポートを確認し、必要に応じて変更します。
2. [最初の使用時に信頼する (trust on first use)] オプションを使用しない場合は、Manager からの SSL 証明書をアップロードします。

(注)

SSL 証明書を取得してアップロードする方法の詳細については、「[Cisco Secure Network Analytics : 管理対象アプライアンスの SSL/TLS 証明書](#)」を参照してください。

3. [次へ (Next)] をクリックします。

ステップ 8 クレデンシャルを入力して Manager にログインし、クエリの安全な通信を確立して、[完了 (Complete)] をクリックします。

これらのログイン情報は management center に保存されません。これらの情報は、Manager の management center の読み取り専用アナリスト API アカウントを確立するために一度使用されます。これには専用アカウントは必要ありません。管理者自身のログイン情報を使用できます。

設定を保存した後、[セキュリティ分析とログギング (Security Analytics & Logging)] ページで [デバイス割り当てを更新 (Update Device Assignments)] をクリックして、デバイスの割り当てを更新できます。

SAL On Premises Configuration

Secure Network Analytics Manager Hostname
192.168.7.223

IP address for logging
1.1.1.1:8514 (★ default, 1 device assigned)
2.2.2.2:8514 (0 devices assigned)

[Update Device Assignments](#)

Certificate
smc-aced3.cisco.com
Expires: 2025-11-03 10:59:35 EST (in 3 years)
✔ This certificate is valid

[Refresh](#) | [Upload](#) | [Download](#)

[Reconfigure](#)

次のタスク

- [Syslog](#) を使用してデータプレーンイベントログを [Secure Network Analytics](#) に送信するように [Secure Firewall Management Center](#) を構成する (18 ページ) を使用してデータプレーンのイベントログを送信できるようにします。

- イベントが Secure Network Analytics アプライアンスに正常に保存されていることを確認した後、すべてのイベントがリモートからも使用可能な management center に確実に保存されるまでの時間を確保します。その後、[Management Center](#) での優先度が低い接続イベントの保存の停止を参照してください。



- (注) これらの設定のいずれかを変更する必要がある場合は、ウィザードを再度実行します。設定を無効にするか、またはウィザードを再度実行した場合でも、アカウントのログイン情報を除くすべての設定が保持されます。

Syslog を使用してデータプレーンイベントログを Secure Network Analytics に送信するように Secure Firewall Management Center を構成する

次に、アプライアンスのプラットフォーム設定ポリシーの UI オプションで、Syslog を使用してデータプレーンイベントログを Secure Network Analytics に送信するように management center を構成する方法について説明します。



- (注) データプレーンイベントは、Security Analytics and Logging (OnPrem) Data Store 展開でサポートされています。

始める前に

management center の [ウィザード](#) を使用して、データプレーンイベントログの Secure Network Analytics への送信を有効にしてください。

手順

ステップ 1 ログギングをイネーブルにします。

- [Syslog] > [ログギングの設定 (Logging Setup)] > [基本ログギング設定 (Basic Logging Settings)] に移動します。
- [Enable Logging] チェックボックスをオンにします。

ステップ 2 ログギングトラップを設定します。

- [Syslog] > [ログギング接続先 (Logging Destinations)] に移動します。
- [+ ログギング接続先の追加 (+ Add Logging Destination)] をクリックします。
- [ログギング接続先 (Logging Destinations)] で、[Syslogサーバー (Syslog Servers)] を選択します。
- [イベントクラス (Event Class)] で、[重大度によるフィルタ (Filter on Severity)] を選択します。
- 重大度を選択します。

ステップ3 ログインファシリティを設定します。

- a) [Syslog] > [Syslog設定 (Syslog Settings)] > [ファシリティ (Facility)] に移動します。
- b) [ファシリティ (Facility)] で、[default = LOCAL4(20)] を選択します。

Management Center での優先度が低い接続イベントの保存の停止

接続イベントの大部分は、特定された脅威に関連付けられていません。この大量のイベントを management center に保存しないようにすることができます。

management center に保存されていないイベントは、<https://www.cisco.com/c/en/us/products/collateral/security/%20firesight-management-center/datasheet-c78-736775.html> のデータシートで指定されているように、management center アプライアンスの最大フローレートにカウントされません。

次の接続イベントは優先度が高いと見なされ、接続イベントの保存を無効にした場合でも常に management center に保存されます。

- セキュリティ イベント
- 侵入イベントに関連付けられた接続イベント
- ファイルイベントに関連付けられた接続イベント
- マルウェアイベントに関連付けられた接続イベント

優先度が低い接続イベントを management center に保存しないことで、より多くのストレージスペースを他のイベントタイプに割り当てることができ、脅威を調査するための時間が長くなります。この設定は、統計情報の収集には影響しません。

この設定は、この management center によって管理されているすべてのデバイスからのイベントに適用されます。

始める前に



注意 この手順により、現在 management center に保存されているすべての接続イベントが直ちに完全に削除されます。

この手順を実行する前に、保持する優先度が低いすべての接続が Secure Network Analytics アプライアンスにすでに存在していることを確認します。通常、management center がイベントを Secure Network Analytics に正常に送信していることを確認した後、しばらくしてからこのオプションを有効にすることをお勧めします。

手順

ステップ1 management center での優先度が低い接続イベントの保存を停止する方法は次の2つです。

どちらの方法でも同じ効果があります。

- イベントを Security Analytics and Logging (OnPrem) に送信するためのウィザードを完了したら、[システム (System)] > [ロギング (Logging)] > [セキュリティ分析とロギング (Security Analytics and Logging)] に移動し、[FMC で保存するイベントを少なくする (Store Fewer Events on FMC)] オプションを有効にします。
- [システム (System)] > [設定 (Configuration)] > [データベース (Database)] に移動し、[接続データベース (Connection Database)] セクションを探して、[最大接続イベント数 (Maximum Connection Events)] をゼロ (0) に設定します。

この値を 0 以外に設定すると、優先度が低いすべての接続イベントが最大フローレートにカウントされます。この設定は接続サマリーには影響しません。

ステップ 2 変更を保存します。

次のタスク

[システム (System)] > [設定 (Configuration)] > [データベース (Database)] ページで、他のすべてのイベントタイプのストレージ制限を増やします。

ASA デバイスの設定

ASA のシステムログにより、ASA デバイスのモニタリングおよびトラブルシューティングに必要な情報が得られます。ASA イベントタイプのリストについては、『[Cisco ASA Series Syslog Messages](#)』を参照してください。



(注) ASA イベントストレージは、Security Analytics and Logging (OnPrem) Data Store 展開でサポートされます。

Security Analytics and Logging (OnPrem) に、syslog イベントを送信させるには、ASA デバイスでロギングを設定する必要があります。

- ロギングの有効化
- Secure Network Analytics Flow Collector への出力先の設定



(注) セキュアロギングは Security Analytics and Logging (OnPrem) ではサポートされていません。

ASA デバイスから syslog イベントを送信するための CLI コマンド

セキュリティイベントの syslog メッセージを ASA デバイスから Security Analytics and Logging (OnPrem) に送信するには、次の設定コマンドを使用します。

始める前に

- 要件と前提条件のセクションを確認します。
- ASA デバイスが Flow Collector に到達できることを確認します。
- Manager の Central Management から Flow Collector の IP アドレスとポート番号を取得します。

手順

ステップ 1 ログインを有効にします。

logging enable

例 :

```
ciscoasa(config)# logging enable
```

ステップ 2 syslog サーバー (Flow Collector) に送信する syslog メッセージを指定します。

logging trap {severity_level | message_list}

例 :

Flow Collector に送信する syslog メッセージの重大度の値 (1 - 7) または名前を指定できます。

```
ciscoasa(config)# logging trap errors
```

例 :

また、Flow Collector に送信する syslog メッセージを特定したカスタムメッセージリストを指定することもできます。

```
ciscoasa(config)# logging list specific_event_list message 106100  
ciscoasa(config)# logging list specific_event_list message 302013-302018  
ciscoasa(config)# logging trap specific_event_list
```

ステップ 3 Flow Collector にメッセージを送信するように ASA を設定します。

logging host interface_name syslog_ip [protocol/port]

例 :

```
ciscoasa(config)# logging host management 209.165.201.3 17/8514
```

(注)

1. syslog_ip と port については、Flow Collector IP および対応する syslog ポート番号を指定します（手順については、「はじめる前に」を参照）。
2. UDP プロトコルを示すには 17 を指定します。

ステップ 4 (任意) syslog メッセージのタイムスタンプ形式を設定します。

```
logging timestamp {rfc5424}
```

例 :

```
ciscoasa(config)# logging timestamp  
ciscoasa(config)# logging timestamp rfc5424
```

RFC5424 で指定されているタイムスタンプの形式は yyyy-MM-TTHH:mm:ssZ です（文字 Z は UTC タイムゾーンを示す）。

(注)

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

ステップ 5 (任意) syslog メッセージをデバイス ID とともに表示するように ASA を設定します。

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

例 :

```
ciscoasa(config)# logging device-id context-name
```

syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

ASA デバイスから syslog イベントを送信するための ASDM 設定

セキュリティイベントの ASA syslog メッセージを Security Analytics and Logging (OnPrem) に送信するように ASDM を設定するには、次の手順を使用します。

始める前に

- 要件と前提条件のセクションを確認します。
- ASA デバイスが Flow Collector に到達できることを確認します。
- Manager の Central Management から Flow Collector の IP アドレスとポート番号を取得します。

手順

ステップ 1 ASDM にログインします。

ステップ 2 ログインを有効にします。

- a) [設定 (Configuration)] > [デバイス管理 (Device Management)] > [ロギング (Logging)] > [ロギングのセットアップ (Logging Setup)] をクリックします。
- b) [Enable logging] チェックボックスをオンにして、ロギングをオンにします。
- c) (オプション) [syslogをEMBLEM形式で送信する (Send syslog in EMBLEM)] チェックボックスをオンにして、EMBLEM ログ形式を有効にします。

ステップ 3 syslog サーバー (Flow Collector) のロギングフィルタ設定を指定します。

- a) [設定 (Configuration)] > [デバイス管理 (Device Management)] > [ロギング (Logging)] > [ロギングフィルタ (Logging Filters)] を選択します。
- b) テーブルから [syslog サーバー (Syslog Servers)] を選択し、[編集 (Edit)] をクリックします。
- c) [ロギングフィルタの編集 (Edit Logging Filters)] ダイアログボックスで、次のいずれかのロギングフィルタ設定を選択します。

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

(注)

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

または

メッセージ ID に基づいて syslog メッセージをフィルタ処理するには、[イベントリストの使用 (Use event list)] をクリックします。必要な syslog メッセージ ID で作成されたイベントリストを選択するか、[新規 (New)] をクリックして、syslog メッセージ ID または ID の範囲でリストを作成することができます。

- d) 設定を保存します。

ステップ 4 Flow Collector のアドレスとポートを使用して外部 syslog サーバーを設定します。

- a) [設定 (Configuration)] > [デバイス管理 (Device Management)] > [ロギング (Logging)] > [syslog サーバー (Syslog Server)] を選択します。
- b) [追加 (Add)] をクリックして、新しい Syslog サーバーを追加します。
- c) [syslog サーバーの追加 (Add Syslog Server)] ダイアログボックスで、次を指定します。
 - [インターフェイス (Interface)] : syslog サーバーとの通信に使用するインターフェイス。
 - [IPアドレス (IP Address)] : Manager の Central Management から取得した Flow Collector IP。
 - [プロトコル (Protocol)] : UDP を選択します。
 - [ポート (Port)] : 対応する Flow Collector の syslog ポート (デフォルトでは 8514) 。
 - (オプション) [メッセージをEMBLEM形式で記録する (Log messages in Cisco EMBLEM format)] チェックボックスをオンにして、EMBLEM ロギング形式を有効にします。

ステップ 5 [保存 (Save)] をクリックして設定に変更を適用します。

ASA デバイスから syslog イベントを送信するための CSM 設定

セキュリティイベントの ASA syslog メッセージを Security Analytics and Logging (OnPrem) に送信するように Cisco Security Manager (CSM) を設定するには、次の手順を使用します。

始める前に

- 要件と前提条件のセクションを確認します。
- ASA デバイスが Flow Collector に到達できることを確認します。
- Manager の Central Management から Flow Collector の IP アドレスとポート番号を取得します。
- この統合では、セキュアロギングはサポートされていません。

手順

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

ステップ 2 syslog ロギングを有効にします。

- 次のいずれかを実行して [syslog ロギングのセットアップ (Syslog Logging Setup)] ページにアクセスします。
 - (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ロギング (Logging)] > [Syslog] > [ロギングのセットアップ (Logging Setup)] を選択します。
 - (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)] > [ロギング (Logging)] > [Syslog] > [ロギングのセットアップ (Logging Setup)] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- [syslog ロギングのセットアップ (Syslog Logging Setup)] ページで、[ロギングの有効化 (Enable Logging)] チェックボックスをオンにして syslog ロギングをオンにします。
- (オプション) [syslogをEMBLEM形式で送信する (Send syslogs in EMBLEM)] チェックボックスをオンにして、EMBLEM ログ形式を有効にします。
- [保存 (Save)] をクリックします。

ステップ 3 syslog サーバー (Flow Collector) のロギングフィルタ設定を指定します。

- ポリシーセクタから [プラットフォーム (Platform)] > [ロギング (Logging)] > [Syslog] > [ロギングフィルタ (Logging Filters)] を選択します。
- テーブルの [ロギングの宛先 (Logging Destination)] 列で [syslog サーバー (Syslog Servers)] を選択し、[編集 (Edit)] をクリックします。syslog サーバーオブジェクトが見つからない場合は、[行の追加 (Add Row)] をクリックします。

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

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

(注)

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

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

(注)

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

- d) 設定を保存します。

ステップ 4 (任意) ロギングパラメータを設定します。

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

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

(注)

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

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

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

(注)

syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

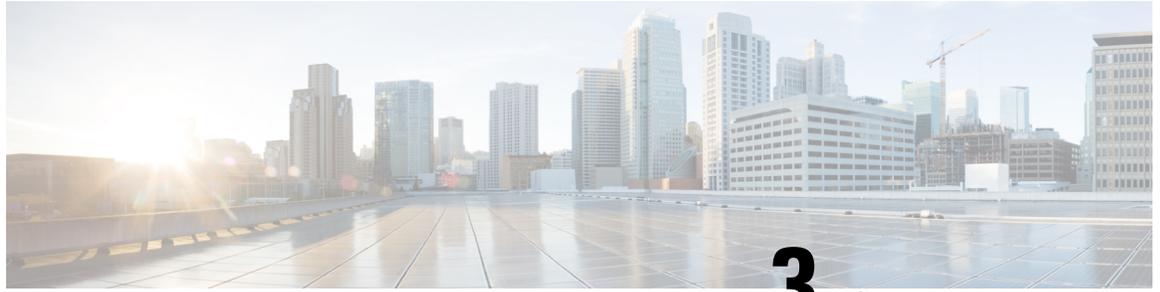
- d) [保存 (Save)] をクリックします。

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

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

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ロギング (Logging)] > [syslog サーバー (Syslog Servers)] を選択します。
 - (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)] > [ロギング (Logging)] > [syslog サーバー (Syslog Servers)] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- b) [追加 (Add)] をクリックして、新しい Syslog サーバーを追加します。
- c) [syslog サーバーの追加/編集 (Add/Edit Syslog Server)] ダイアログボックスで、次を指定します。
- [インターフェイス (Interface)] : syslog サーバーとの通信に使用するインターフェイス。
 - [IPアドレス (IP Address)] : Manager の Central Management から取得した Flow Collector IP。
 - [プロトコル (Protocol)] : UDP を選択します。
 - [ポート (Port)] : 対応する Flow Collector の syslog ポート (デフォルトでは 8514) 。
 - (オプション) [メッセージをEMBLEM形式で記録する (Log messages in Cisco EMBLEM format)] チェックボックスをオンにして、EMBLEM ログ形式を有効にします。
- d) [OK] をクリックして設定を保存し、ダイアログボックスを閉じます。定義した syslog サーバーが、テーブルに表示されます。

ステップ 6 設定の変更を送信して展開します。



第 3 章

次のステップ

- [次のステップ](#) (27 ページ)
- [Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Management Center での作業](#) (27 ページ)
- [相互起動を使用したイベントの調査](#) (28 ページ)

次のステップ

Security Analytics and Logging (OnPrem) の一部として syslog イベントデータを Secure Network Analytics アプライアンスに渡すようにファイアウォール展開を設定したら、次の手順を実行できます。

- management center オンラインヘルプを確認します。
- Secure Network Analytics の詳細については、Managerのオンライン ヘルプを参照してください。[調査 (Investigate)] > [セキュリティ分析とロギング (オンプレミス) (Security Analytics and Logging (OnPrem))] に移動します。

Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Management Center での作業

デバイスが Security Analytics and Logging (OnPrem) を使用して Secure Network Analytics アプライアンスに接続イベントを送信している場合、management center のイベントビューアとコンテキストエクスプローラでリモートに保存されたイベントを表示および操作し、レポートの生成時にそれらのイベントを含めることができます。management center のイベントから相互起動して、Secure Network Analytics アプライアンスの関連データを表示することもできます。

デフォルトでは、指定した時間範囲に基づいて適切なデータソースが自動的に選択されます。データソースをオーバーライドする場合は、次の手順を使用します。



重要 データソースを変更すると、選択した内容は、サインアウト後でも、変更するまでは、イベントデータソース（レポートを含む）に依存するすべての関連する分析機能で維持されます。選択した内容は他の management center ユーザーには適用されません。

選択したデータソースは、優先順位の低い接続イベントにのみ使用されます。他のすべてのイベントタイプ（侵入、ファイル、マルウェアイベント、それらのイベントに関連付けられた接続イベント、およびセキュリティインテリジェンスイベント）は、データソースに関係なく表示されます。

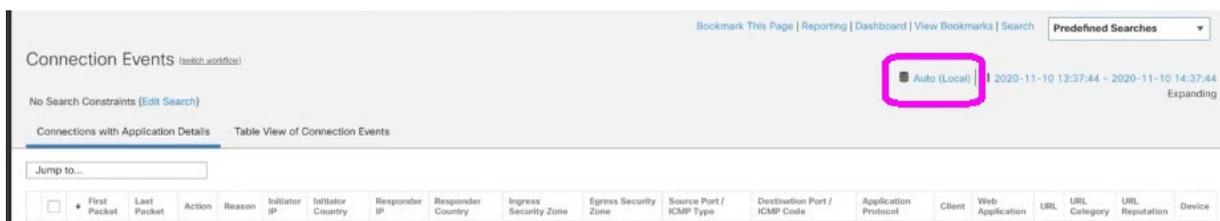
始める前に

ウィザードを使用して接続イベントを Security Analytics and Logging (OnPrem) に送信しました。

手順

ステップ 1 management center Web インターフェイスで、接続イベントデータを表示するページ（[Analysis]>[Connections]>[Events] など）に移動します。

ステップ 2 ページに表示されるデータソースをクリックし、オプションを選択します。



注意

[Local] を選択すると、ローカルデータが選択した時間範囲全体で使用できない場合でも、management center で使用可能なデータのみ表示されます。この状況が発生していることは通知されません。

ステップ 3 （任意） Secure Network Analytics アプライアンスで関連データを直接表示するには、IP アドレスやドメインなどの値を右クリック（統合イベントビューアでクリック）し、相互起動オプションを選択します。

相互起動を使用したイベントの調査

management center でイベントを表示しているときに、特定のイベントデータ（たとえば、IP アドレス）を右クリックして、Manager で関連するデータを表示できます。

手順

ステップ 1 management center でイベントが表示される次のページのいずれかに移動します。

- ダッシュボード ([概要 (Overview)] > [ダッシュボード (Dashboards)])、または
- イベントビューアページ (イベントのテーブルが含まれている [分析 (Analysis)] メニューにあるオプション)

ステップ 2 対象のイベントフィールドを右クリックして、**Security Analytics and Logging (OnPrem)**相互起動リソースを選択します。別のブラウザウィンドウに **Manager** が開きます。まだログインしていない場合は、ユーザー名とパスワードの入力を求められることがあります。クエリを実行するデータの量、**Manager** の速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

ステップ 3 **Manager** にサインインします。



付録 **A**

障害対応

- [障害対応 \(31 ページ\)](#)

障害対応

Security Analytics and Logging (OnPrem) 一般的なトラブルシューティング情報

Manager では、次のログファイルに、Security Analytics and Logging (OnPrem) 関連のトラブルシューティング情報が。

- `/lancope/var/logs/sal_preinstall.log` : アプリケーションのインストールプロセスに固有の情報

Flow Collector では、次のログファイルに Security Analytics and Logging (OnPrem) Data Store 展開に関連するトラブルシューティング情報が記載されています。

- `lancope/var/sw/today/logs/sw.log` : テレメトリロギングに固有の情報
- `/lancope/var/logs/containers/svc-db-ingest.log` : イベントの取り込みとデータベースに固有の情報

Flow Collector の詳細設定を使用した Security Analytics and Logging (OnPrem) 構成 (Data Store のみ)

初回セットアップ時にファイアウォールログを保存しないように Flow Collector を設定した場合は、[Flow Collector の詳細設定 (Flow Collector Advanced Settings)] ページを使用して取り込み設定を更新できます。[詳細設定 (Advanced Settings)] には、次の手順でアクセスします。

1. Flow Collector (旧アプライアンス管理 (Admin) インターフェイス) にログインします。
2. [サポート (Support)] > [詳細設定 (Advanced Settings)] の順にクリックします。
3. `enable_sal` フィールドに 1 を入力して、ファイアウォールイベントログの取り込みを有効にします。
4. ファイアウォールログのポートを変更する場合は、`sal_syslog_port` フィールドに新しい値を入力します (デフォルトのポートは 8514)。

5. [適用 (Apply)] をクリックし、[OK] をクリックします。

翻訳について

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