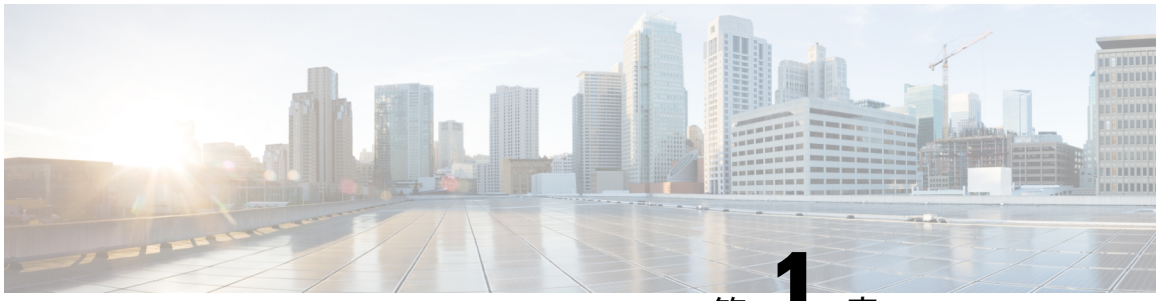
Cisco Security Analytics and Logging（オンプレミス）v3.2.0：ファイアウォールイベント統合ガイド

初版：2023 年 1 月 27 日

最終更新：2023 年 1 月 30 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/



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シスコのセキュリティ分析とロギング（オンプレミス）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

セキュリティ分析とロギング（オンプレミス） 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

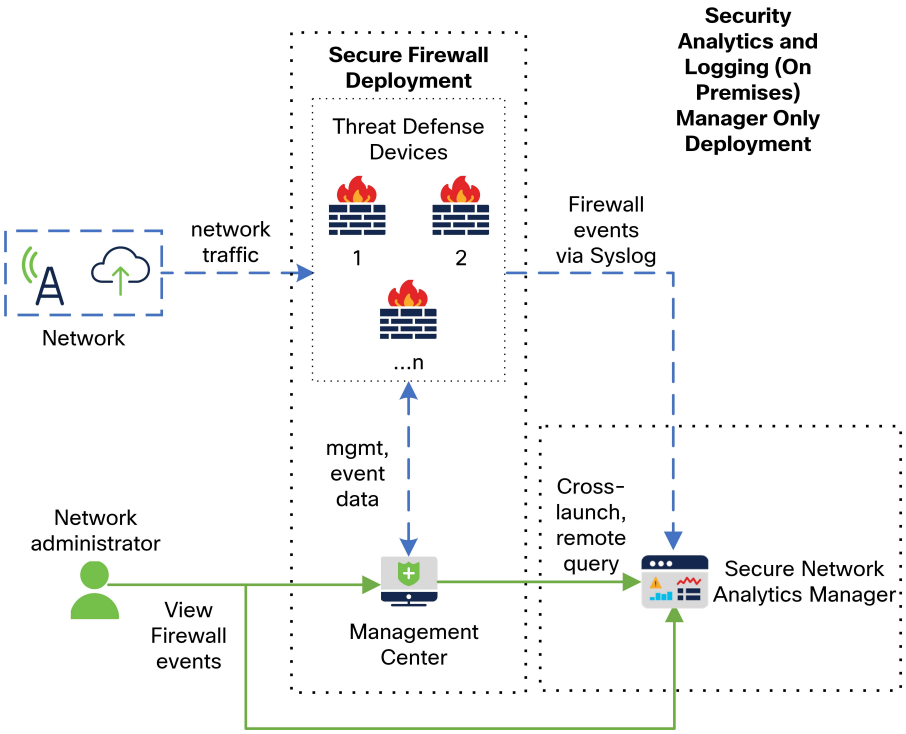
合、セキュリティイベントおよびデータプレーンイベントを Management Center が管理する Secure Firewall Threat Defense デバイスから マネージャ にエクスポートして、その情報を保存します。

Secure Network Analytics の展開には次の 2 つのオプションがあります。

- マネージャのみ：スタンドアロンの Manager を展開してイベントを受信および保存し、そこからイベントを確認および照会します。
- データストア：イベントを受信する Cisco Secure Network Analytics フローコレクタ（最大 5 つ）、イベントを保存する Cisco Secure Network Analytics データストア（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。

マネージャのみ

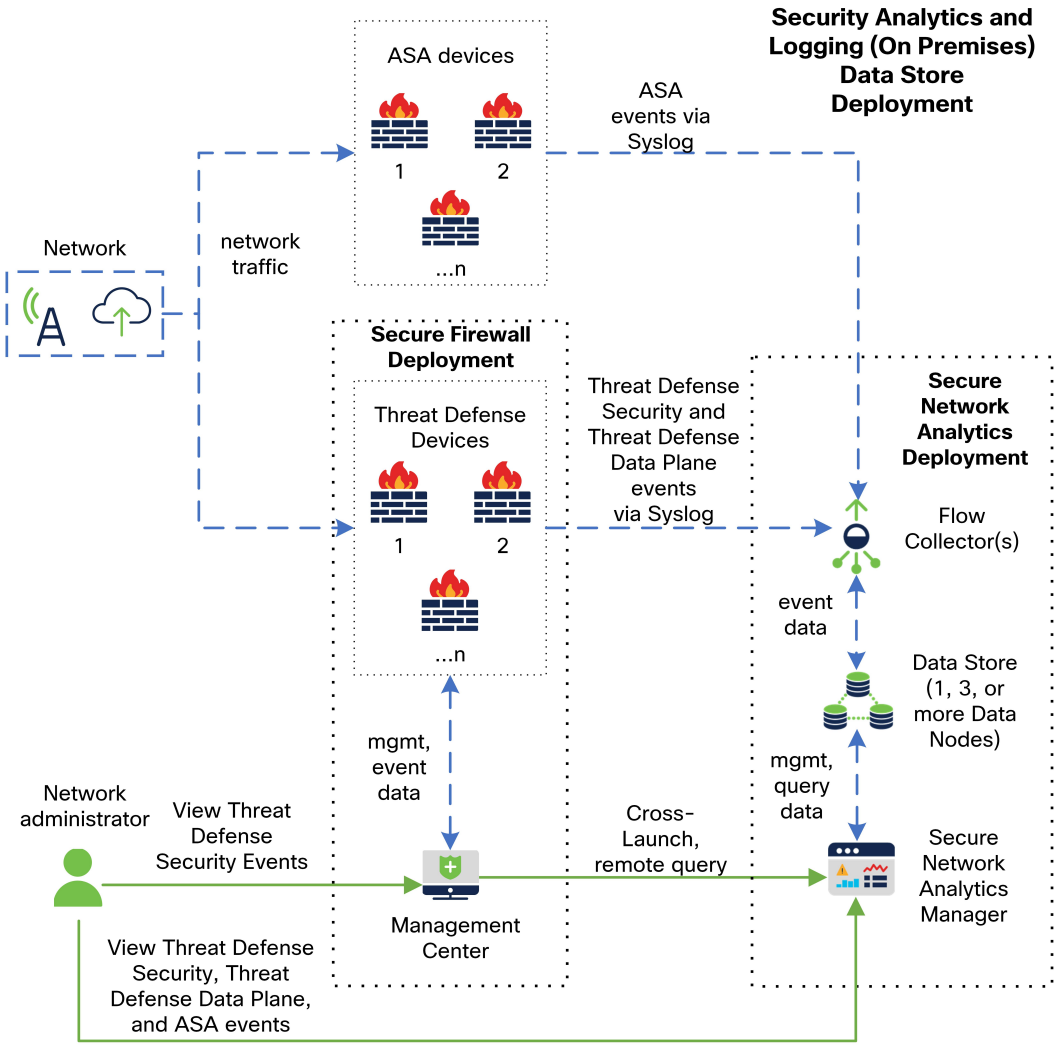
マネージャのみ の展開の例については、次の図を参照してください。



この展開では、脅威に対する防御 デバイスは Secure Firewall のイベントを マネージャ に送信し、Manager がこれらのイベントを保存します。ユーザは Management Center の UI から マネージャ 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。

データストア

マネージャ、データノード、およびフローコレクタを使用した データストア の展開の例については、次の図を参照してください。

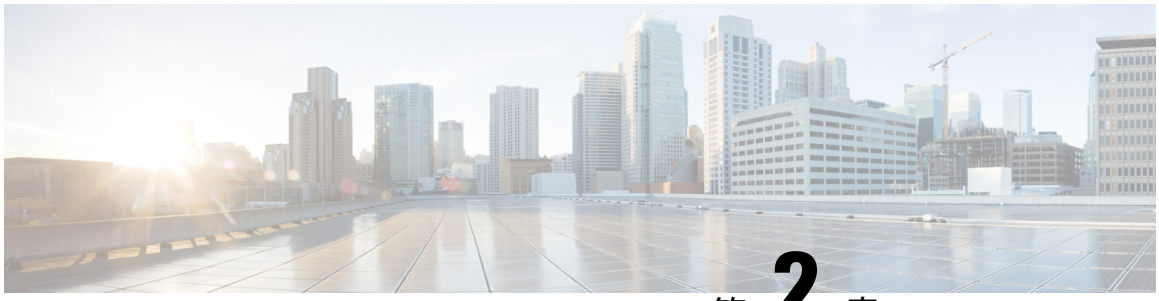


この展開では、脅威に対する防御 および Secure Firewall ASA デバイスはファイアウォールのイベントをフローコレクタに送信します。フローコレクタは、保存のためにデータストアにイベントを送信します。ユーザは Management Center の UI から マネージャ を相互起動して保存されたイベントに関する詳細情報を表示できます。また、Management Center からリモートでイベントを照会することもできます。

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（データストア 展開のみ）
- ASA イベント（データストア 展開のみ）



第 2 章

展開

- 要件 （5 ページ）
- 設定の概要 （15 ページ）
- Secure Network Analytics の展開と設定 （17 ページ）
- Secure Firewall Management Center の設定 （19 ページ）
- ASA デバイスの設定 （27 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セキュリティ分析とロギング（オンプレミス） 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	セキュリティ分析とロギング（オンプレミス） 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 マネージャ、また必要に応じて複数のフローコレクタ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	セキュリティ分析とロギング（オンプレミス） 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 v6.4 以降（syslog を使用） NGIPS v6.4（syslog を使用）	なし	• 脅威に対する防御 v6.4 以降で syslog を使用する方法については、以前のバージョンの Threat Defense デバイスからのイベントの送信を参照してください。
ASA デバイス	v9.12+	なし	

Secure Network Analytics アプライアンス

Secure Network Analytics の展開には次のオプションがあります。

- マネージャのみ：マネージャ のみを展開してイベントを取り込んで保存したり、イベントを確認および照会します。
- データストア：フローコレクタ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、マネージャ を展開してイベントを確認および照会します。

表 *1 :* マネージャのみ

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
マネージャ	Secure Network Analytics v7.4.2	なし	• マネージャ は複数台の 脅威に対する防御 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。 • イベントの取り込みのために セキュリティ分析とロギング（オンプレミス） アプリをインストールし、マネージャでファイアウォールイベントを表示させてください。
セキュリティ分析とロギング（オンプレミス）アプリケーション	セキュリティ分析とロギング（オンプレミス）アプリケーション v3.2.x	GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング	• マネージャ にこのアプリケーションをインストールし、イベントの取り込みを有効にするように設定します。

表 *2:* データストア

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
マネージャ	Secure Network Analytics v7.4.2	なし	• イベントの取り込みのために セキュリティ分析とロギング（オンプレミス） アプリをインストールし、マネージャでファイアウォールイベントを表示させてください。 • Secure Network Analytics v7.4.1+ はシングルノードデータストアとマルチテレメトリで必要です。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
Flow Collector	Secure Network Analytics v7.4.2	なし	• データストア用に設定された最大 5 つのフローコレクタを展開できます。 • 複数台の 脅威に対する防御 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。 • Secure Network Analytics v7.4.1+ はシングル ノード データストアとマルチテレメトリで必要です。
データストア	Secure Network Analytics v7.4.2	なし	• 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。 • フローコレクタで受信したファイアウォールイベントを保存できます。 • Secure Network Analytics v7.4.1+ はシングル ノード データストアとマルチテレメトリで必要です。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
セキュリティ分析とロギング（オンプレミス）アプリケーション	セキュリティ分析とロギング（オンプレミス）アプリケーション v3.2.x	GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング	• マネージャ にこのアプリケーションをインストールし、イベントの取り込みを有効にするように設定します。

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、セキュリティ分析とロギング（オンプレミス） 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 セキュリティ分析とロギング（オンプレミス） 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

セキュリティ分析とロギング（オンプレミス） 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。

- ハードウェアまたはバーチャルエディション（VE）の マネージャのみ の展開では、平均で最大約 20,000 イベント/秒（EPS）でショートバーストでは最大 35,000 EPS を取り込むことができます。
- 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）データストア 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 データストア の展開では、平均で最大約 10 万 EPS、ショートアーストでは最大 350,000 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、セキュリティ分析とロギング（オンプレミス） アプリケーション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、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。

マネージャのみ 推奨事項

マネージャ VE リソース

最適なパフォーマンスを得るために、マネージャ VE を展開する場合は、次のリソースを割り当てます。

リソース	推奨
CPU	12
RAM	64 GB
ハードドライブストレージ	2 TB

マネージャ 2210 仕様

ハードウェアの仕様については、マネージャ 2210 仕様書を参照してください。

推定保持期間

マネージャ VE に割り当てるストレージスペースに基づいて、または マネージャ 2210 を使用している場合は、マネージャのみのみの展開でおおよそ次の時間枠のデータを保存できます。

平均 EPS	平均日次イベント	1TB ストレージの推定保持期間	2TB ストレージの推定保持期間	4 TB ストレージ（ハードウェア）の推定保持期間
1,000	8,650 万	250 日	500 日	1000 日
5,000	4 億 3,000 万	50 日	100 日	200 日
10,000	8 億 6,500 万	25 日	50 日	100 日
20,000	17 億 3,000 万	12.5 日	25 日	50 日

マネージャ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。

（注） この推定取り込みおよび保管の期間について、これらのリソース割り当てでマネージャ VE 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。ストレージ割り当てを 2 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。

データストア 推奨事項

最適なパフォーマンスを得るために、マネージャ VE、フローコレクタ 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 アプライアンスの設置ガイド（ハードウェアまたはバーチャルエディション）とシステム コンフィギュレーション ガイド v7.4.1」を参照してください。

表 *3*: マネージャ *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 *4*: *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 *5*: データノード *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

リソース	推奨
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、データストア 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日間	60 日
75,000	64 億 8,000 万	サポート対象外	40 日間
100,000	86 億 4,000 万	サポート対象外	30日間

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

次の表にマネージャのみの展開の場合にセキュリティ分析とロギング（オンプレミス）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。

表 *6:* マネージャのみ

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、およびマネージャ	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
ユーザーワークステーション	Management Centerおよびマネージャ	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	マネージャ	8514/UDP	脅威に対する防御デバイスからの syslog のエクスポート、マネージャ への取り込み
Management Center	マネージャ	443/TCP	Management Center から マネージャ へのリモートクエリ

次の表にデータストアの展開の場合にセキュリティ分析とロギング（オンプレミス）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 *7:* データストア

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、マネージャ、フローコレクタ、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およびマネージャ	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

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 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、フローコレクタへの取り込み
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、フローコレクタへの取り込み
Management Center	マネージャ	443/TCP	Management Center から マネージャ へのリモートクエリ

設定の概要

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
マネージャのみ の導入	次の選択肢があります。 • マネージャ 2210 をネットワークに展開し、eth0 管理インターフェイスの IP アドレスやその他の情報の割り当てを含む初期設定を実行します。詳細については、『x2xx Series Hardware Appliance Installation Guide』と『Secure Network Analytics System Configuration Guide』を参照してください。 • マネージャ VE ISO をダウンロードし、マネージャ VE をハイパーバイザに展開します。初期設定を実行し、eth0 管理インターフェイスの IP アドレスとその他の情報を割り当てます。詳細については、『Secure Network Analytics Virtual Edition Appliance Guide』を参照してください。
データストア の導入	• マネージャ、フローコレクタ、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。

コンポーネントとタスク	手順
セキュリティ分析とロギング（オンプレミス）アプリケーションをダウンロードして マネージャにインストールし、ファイアウォールのイベントを受信して保存するように Secure Network Analytics の展開を設定	• アプリファイル、app-smc-sal-3.2.0-v2.swu を https://software.cisco.com からダウンロードします。 • マネージャ で、[集中管理（Central Management）] の [アプリケーションマネージャ（App Manager）] に移動し、 アプリケーションをインストールします。アプリケーションの使用方法の詳細については、セキュリティ分析とロギング（オンプレミス） リリースノートとアプリケーションのヘルプを参照してください。
イベントを セキュリティ分析とロギング（オンプレミス）に送信するように Management Center を設定	次の選択肢があります。 • Secure Firewall Management Center の設定 （19 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。 • 「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 を設定する」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。 • 「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 セキュリティ分析とロギング（オンプレミス）に送信するように ASA デバイスを設定	• ASA デバイスの設定 （27 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	次の手順を確認します。 • 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 Management Center での作業」を参照してください。. • Secure Network Analytics の使用方法については、マネージャ Web アプリケーションのオンラインヘルプを参照してください。

Secure Network Analytics の展開と設定

セキュリティ分析とロギング（オンプレミス）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。
   - マネージャのみ の展開と設定 （17 ページ）
   - データストア の展開と設定 （17 ページ）
2. Security Analytics and Logging（オンプレミス）アプリケーションをインストール （18 ページ）。

マネージャのみ の展開と設定

始める前に

- マネージャ をネットワークに展開し、その管理 IP アドレスに Management Center の管理 IP アドレスと 脅威に対する防御 デバイスの管理 IP アドレスの両方から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。詳細については、『Secure Network Analytics Virtual Edition Appliance Guide』を参照してください。
- Secure Network Analytics 製品インスタンスを適切に登録します。マネージャ 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。

マネージャ VE を展開するには、『Secure Network Analytics Virtual Edition Installation Guide』の手順に、マネージャ 2210 を展開する場合は、『x2xx Series Hardware Appliance Installation Guide』と『Secure Network Analytics System Configuration Guide』の手順に従い、マネージャ を設定します。

データストア 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、フローコレクタ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、セキュリティ分析とロギング（オンプレミス）でフローコレクタを使用するように設定します。アプライアンスの構成後、フローコレクタ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

- マネージャ、フローコレクタ、およびデータノードをネットワークに展開したこと、脅威に対する防御 デバイスの管理 IP アドレスがフローコレクタ管理 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 マネージャ 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。マネージャ 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。

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。フローコレクタ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フローコレクタ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。

Security Analytics and Logging（オンプレミス）アプリケーションをインストール

マネージャ に セキュリティ分析とロギング（オンプレミス）アプリケーションをインストールします。詳細については、『セキュリティ分析とロギング（オンプレミス）Release Notes』を参照してください。

ステップ 1 セキュリティ分析とロギング（オンプレミス）アプリケーションをダウンロードするには、https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

ステップ 2 マネージャ にログインします。

ステップ 3 メインメニューから [構成（Configure）]>[グローバル集中管理（GLOBAL Central Management）] を選択します。

ステップ 4 [アプリケーションマネージャ（App Manager）] タブをクリックします。

ステップ 5 [参照（Browse）] をクリックします。

ステップ 6 画面に表示される指示に従って、アプリケーションファイルをアップロードします。

次のタスク

- 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。
- 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。ASA デバイスの設定 （27 ページ） を参照してください。

Secure Firewall Management Center の設定

セキュリティ分析とロギング（オンプレミス） 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 Secure Firewall Management Center でのウィザードの設定。
- 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 セキュリティ分析とロギング（オンプレミス）を展開するためのウィザードについて説明します。

- マネージャのみ：スタンドアロンの マネージャ を展開して、イベントを送信および保存し、そこからイベントを確認および照会できます。 マネージャのみ展開の設定の詳細については、「マネージャのみ 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。
- データストア：フローコレクタを展開してイベントを受信し、データストア を展開してイベントを保存し、マネージャ を展開してイベントを確認および照会できます。データストア 展開の設定の詳細については、「データストア 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 およびセキュリティ分析とロギング（オンプレミス） 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
  - 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。
  - マネージャ のホスト名または IP アドレス。
  - （フローコレクタを使用し、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）フローコレクタの 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、マネージャ 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 マネージャ 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、マネージャ からの SSL 証明書を使用します。

マネージャのみ 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

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

ステップ 1 Secure Firewall 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 [マネージャのみ（Manager only）] のウィジェットで、[開始（Start）] をクリックします。

ステップ 3 Secure Network Analytics Manager のホスト名または IP アドレスとポートを入力し、[次へ（Next）] をクリックします。

ステップ 4 検出された設定を確認します。

1. ロギング用の IP アドレスとポートを確認し、必要に応じて変更します。
2. 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。
3. [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、マネージャ からの SSL 証明書をアップロードします。
4. [次へ（Next）] をクリックします。

ステップ 5 クレデンシャルを入力してマネージャにログインし、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、Secure Network Analytics 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。

次のタスク

- 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。

データストア 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

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

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 マネージャ のホスト名または IP アドレスとポートを入力します。

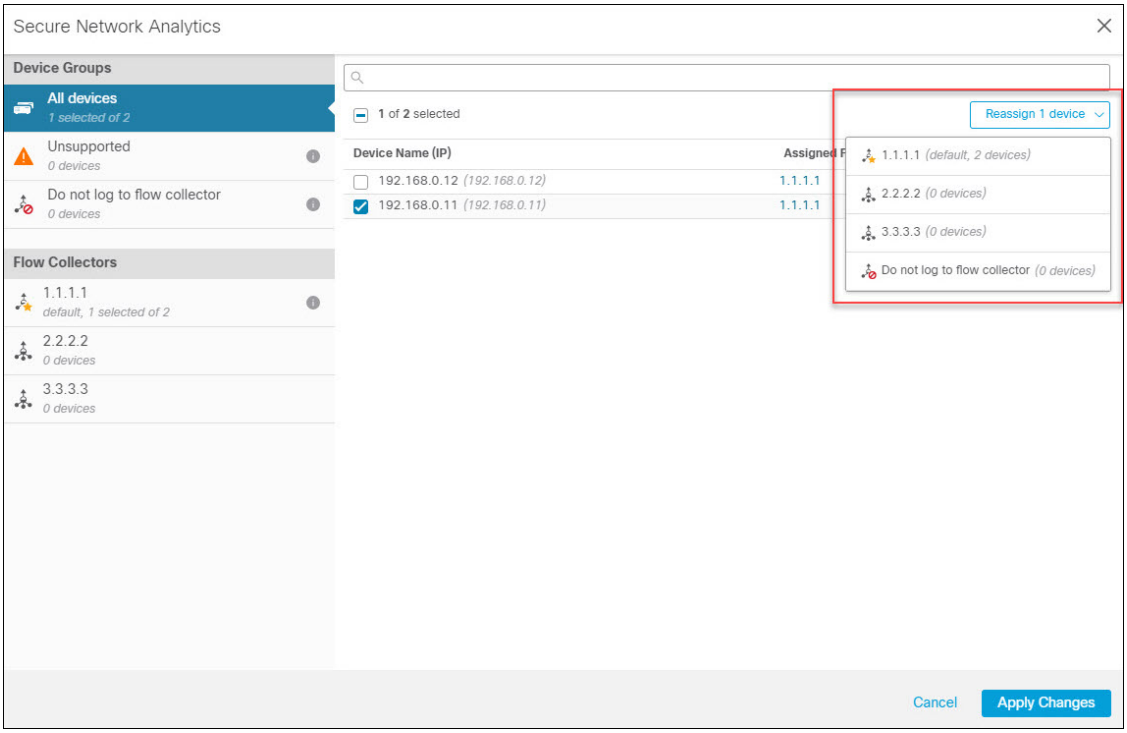
ステップ 4 フローコレクタのホスト名または IP アドレスとポートを入力します。

フローコレクタをさらに追加するには、[+別のフローコレクタを追加（+ Add another flow collector）] をクリックします。

ステップ 5 （オプション）複数のフローコレクタを設定した場合は、管理対象デバイスを異なるフローコレクタに関連付けます。

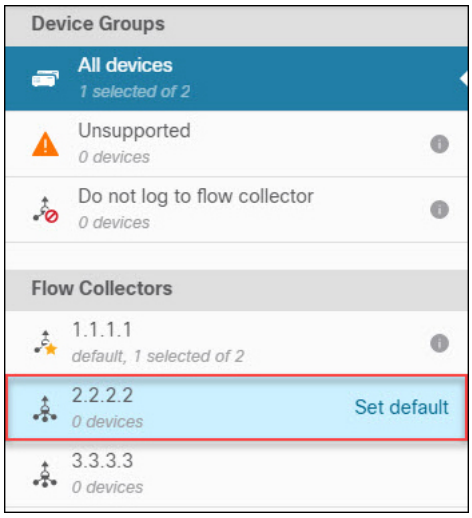
デフォルトでは、すべての管理対象デバイスがデフォルトのフローコレクタに割り当てられます。

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。
3. [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、[フローコレクタ（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フローコレクタ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 [フローコレクタにログを記録しない（Do not log to flow collector）] を選択します。

（注） デフォルトのフローコレクタを変更するには、目的のフローコレクタ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、マネージャ からの SSL 証明書をアップロードします。

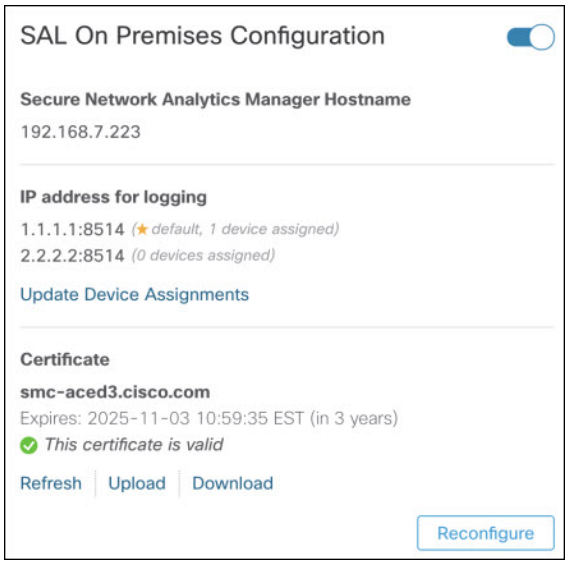
   （注） SSL 証明書を取得してアップロードする方法の詳細については、「Cisco Secure Network Analytics：管理対象アプライアンスの SSL/TLS 証明書」を参照してください。

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マネージャにログインし、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、マネージャ 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。



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 を設定する （24 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 を設定する

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 を設定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、セキュリティ分析とロギング（オンプレミス） データストア 展開でサポートされています。

始める前に

Management Center の Secure Firewall Management Center でのウィザードの設定を使用して、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。

ステップ 1 ロギングをイネーブルにします。

a) [Syslog] > [ロギングの設定（Logging Setup）] > [基本ロギング設定（Basic Logging Settings）] に移動します。

b) [Enable Logging] チェックボックスをオンにします。

ステップ 2 ロギングトラップを設定します。

a) [Syslog] > [ロギング接続先（Logging Destinations）] に移動します。

b) [+ ロギング接続先の追加（+ Add Logging Destination）] をクリックします。

c) [ロギング接続先（Logging Destinations）] で、[Syslogサーバー（Syslog Servers）] を選択します。

d) [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。

e) 重大度を選択します。

ステップ 3 ロギング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。

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 セキュリティ分析とロギング（オンプレミス） 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、セキュリティ分析とロギング（オンプレミス） データストア 展開でサポートされます。

セキュリティ分析とロギング（オンプレミス） 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 フローコレクタへの出力先の設定

（注） セキュアロギングは セキュリティ分析とロギング（オンプレミス） 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 セキュリティ分析とロギング（オンプレミス）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 デバイスがフローコレクタに到達できることを確認します。
- マネージャ の Central Management からフローコレクタの IP アドレスとポート番号を取得します。

ステップ 1 ロギングを有効にします。

logging enable

例：

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

ステップ 2 syslog サーバー（フローコレクタ）に送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

例：

フローコレクタに送信する syslog メッセージの重大度の値（1 ー 7）または名前を指定できます。

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

例：

また、フローコレクタに送信する 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 フローコレクタ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、フローコレクタ 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-THH: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 セキュリティ分析とロギング（オンプレミス）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 デバイスがフローコレクタに到達できることを確認します。
- マネージャ の Central Management からフローコレクタの IP アドレスとポート番号を取得します。

ステップ 1 ASDM にログインします。

ステップ 2 ロギングを有効にします。

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 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。

ステップ 3 syslog サーバー（フローコレクタ）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 フローコレクタ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）]：マネージャ の Central Management から取得したフローコレクタ IP。
- [プロトコル（Protocol）]：UDP を選択します。
- [ポート（Port）]：対応するフローコレクタの 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 セキュリティ分析とロギング（オンプレミス） 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 デバイスがフローコレクタに到達できることを確認します。
- マネージャ の Central Management からフローコレクタの 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。

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

ステップ 2 syslog ロギングを有効にします。

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

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [ロギングのセットアップ（Logging Setup）]** を選択します。

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

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

c) (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。

d) [**保存（Save**）] をクリックします。

ステップ 3 syslog サーバー（フローコレクタ）のロギングフィルタ設定を指定します。

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

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

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

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

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

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

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

d) 設定を保存します。

ステップ 4 （任意）ロギングパラメータを設定します。

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

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

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

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

- [インターフェイス（Interface）]：このオプションボタンをクリックして、ASA デバイスのインターフェイスを選択します。

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

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

d) [**保存（Save**）] をクリックします。

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

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

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

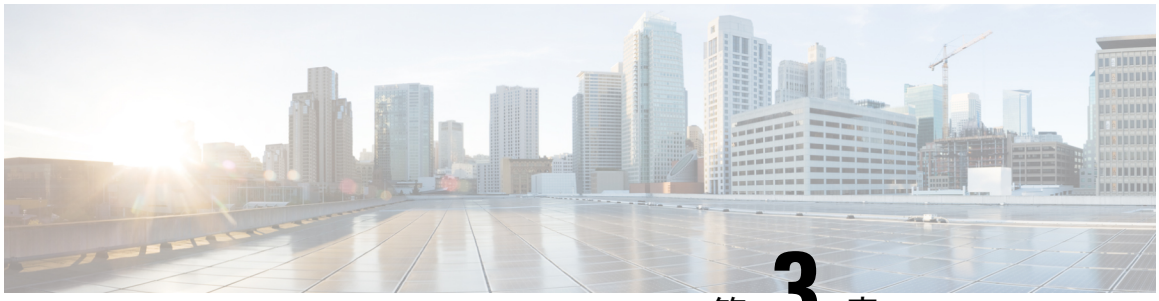
b) [追加（Add）] をクリックして、新しい Syslog サーバーを追加します。

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

- [インターフェイス（Interface）]：syslog サーバーとの通信に使用するインターフェイス。
- [IPアドレス（IP Address）]：マネージャ の Central Management から取得したフローコレクタ IP。
- [プロトコル（Protocol）]：UDP を選択します。
- [ポート（Port）]：対応するフローコレクタの 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。

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 （33 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 （33 ページ）
- 相互起動を使用したイベントの調査 （34 ページ）

次のステップ

セキュリティ分析とロギング（オンプレミス） 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、マネージャ Web アプリケーション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 Management Center での作業

デバイスがセキュリティ分析とロギング（オンプレミス） 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。

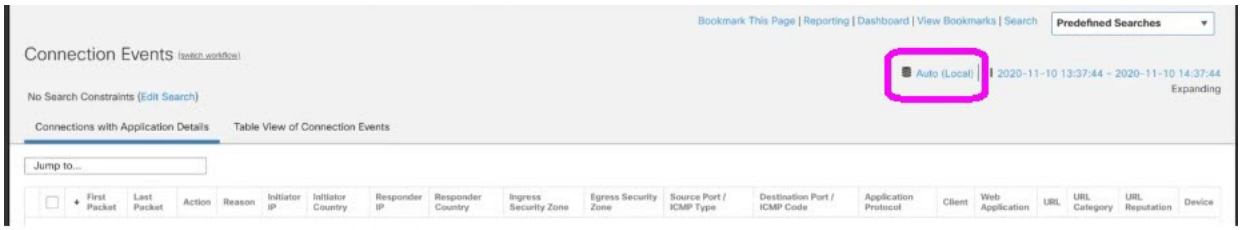
選択したデータソースは、優先順位の低い接続イベントにのみ使用されます。他のすべてのイベントタイプ（侵入、ファイル、マルウェアイベント、それらのイベントに関連付けられた接続イベント、およびセキュリティ インテリジェンス イベント）は、データソースに関係なく表示されます。

始める前に

ウィザードを使用して接続イベントを セキュリティ分析とロギング（オンプレミス） に送信しました。

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、マネージャ で関連するデータを表示できます。

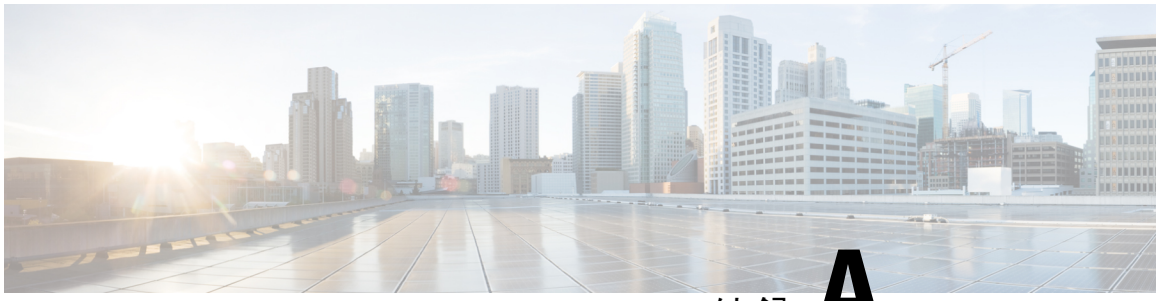
ステップ 1 Management Center でイベントが表示される次のページのいずれかに移動します。

- 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、セキュリティ分析とロギング（オンプレミス）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 マネージャ 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、マネージャ 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 マネージャ にサインインします。



付録 A

トラブルシューティング

- トラブルシューティング （37 ページ）

トラブルシューティング

セキュリティ分析とロギング（オンプレミス） 一般的なトラブルシューティング情報

マネージャ VE では、次のログファイルに セキュリティ分析とロギング（オンプレミス） 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/logs/containers/sal.log`：一般的なアプリケーションのロギング情報（Manager、展開のみ）
- `/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

フローコレクタでは、次のログファイルにセキュリティ分析とロギング（オンプレミス）データストア 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構成(のみ)セキュリティ分析とロギング（オンプレミス）データストア

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フローコレクタを設定した場合は、[フローコレクタの詳細設定（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. フローコレクタ（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。

マネージャのみ 展開時の セキュリティ分析とロギング（オンプレミス） アプリのインストールの失敗

スタンドアロンのアプライアンス（マネージャのみ）としての マネージャ のインストール、またはフローコレクタとデータノード（データストア）を管理する マネージャ のインストールがサポートされています。1 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合、マネージャにアプリケーションをインストールすることはできません。この状況でアプリケーションをインストールしようとすると、インストールは失敗します。これが原因であることを確認するには、`/lancope/var/logs/sal_preinstall.log` でログファイルを確認します。次のメッセージまたは同様のメッセージが表示された場合、インストールで管理対象フローコレクタが検出されたことになります。

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

アプリケーションをインストールするには、すべての管理対象フローコレクタを Central Manager のアプライアンスインベントリから削除したうえで再試行してください。

セキュリティ分析とロギング（オンプレミス）アプリケーションのドロップイベント

アプリケーションは、次のような状況でイベントをドロップすることがあります。

- 接続、ファイル、マルウェア、および侵入イベントだけでなく、すべてのイベントタイプを syslog でエクスポートします。
- 1 秒あたりのイベント (EPS) の平均取り込み速度またはバースト EPS 取り込み速度が、「Secure Network Analytics Resource Allocation」セクションの推奨仕様を超えています。

マネージャのみ の展開の場合、Manager の `/lancope/var/logs/containers/sal.log` ログファイルの情報を確認し、アプリケーションがイベントをドロップしているかどうかを判断します。「`events_dropped`」を含むエントリがないかファイルを検索します。

データストア の展開の場合、フローコクレクタ `lancope/var/sw/today/logs/sw.log` ログファイルの情報を確認し、アプリケーションがイベントをドロップしているかどうかを判断します。「`sal_event`」を含むエントリがないかファイルを検索します。

問題が解消されない場合は、シスコサポートまでお問い合わせください。

セキュリティ分析とロギング（オンプレミス）アプリケーションのクラッシュ

セキュリティ分析とロギング（オンプレミス）アプリケーションがクラッシュした場合（過剰な取り込みレートを起因とする場合など）、マネージャを再起動します。これにより、アプリケーションも再起動されます。

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。