Cisco Secure Network Analytics

リリースノート 7.4.2

目次

はじめに

概要

このドキュメントでは、Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.2 リリースの新機能と改善点、バグ修正、および既知の問題について説明します。

Secure Network Analytics の詳細については、Cisco.com をご覧ください。

再ブランディング

Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。注目すべきその他の主な変更点は、Stealthwatch Management Console が Cisco Secure Network Analytics Manager になったことです。

完全なリストについては、次の表を参照してください。

以前のブランディング	新しいブランディング 初出時	新しいブランディング 2 度目以降
Cisco Stealthwatch Cloud	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Stealthwatch Cloud プライベート ネットワーク モニタリング	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Stealthwatch Cloud パブリック クラウド モニタリング	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Cisco Stealthwatch Enterprise または Cisco Stealthwatch	Cisco Secure Network Analytics	Secure Network Analytics
Cisco Stealthwatch データノード	Cisco Secure Network Analytics データノード	データノード
Cisco Stealthwatch データストア	Cisco Secure Network Analytics データストア	データストア
暗号化トラフィック分析（ETA）	暗号化トラフィック分析	暗号化トラフィック分析
Stealthwatch エンドポイントライセンス	Cisco Secure Network Analytics エンドポイントライセンス	エンドポイントライセンス
Stealthwatch Flow Collector	Cisco Secure Network Analytics Flow Collector	Flow Collector

以前のブランディング	新しいブランディング 初出時	新しいブランディング 2 度目以降
Stealthwatch Flow Collector データベース（FCDB）	Cisco Secure Network Analytics Flow Collector データベース	Flow Collector データベース
Stealthwatch Flow Collector NetFlow（FCNF）	Cisco Secure Network Analytics Flow Collector NetFlow	Flow Collector（NetFlow）
Stealthwatch Flow Collector sFlow（FCSF）	Cisco Secure Network Analytics Flow Collector sFlow	Flow Collector（sFlow）
Stealthwatch Flow Sensor（FS）	Cisco Secure Network Analytics Flow Sensor	Flow Sensor
Stealthwatch Management Console（SMC）	Cisco Secure Network Analytics Manager	マネージャ
Stealthwatch Cloud センサー	Cisco Secure Cloud Analytics センサー	センサー
Stealthwatch 脅威インテリジェンスフィードまたは脅威インテリジェンスライセンス	Cisco Secure Network Analytics 脅威フィード	脅威フィード
UDP Director	Cisco Secure Network Analytics UDP Director	UDP Director

用語

このガイドでは、Secure Network Analytics Flow Sensor Virtual Edition（VE）などの仮想製品を含むすべての Secure Network Analytics 製品に対し「**アプライアンス**」という用語を使用しています。

「**クラスタ**」は、Manager が管理する Secure Network Analytics アプライアンスのグループです。

更新する前に

更新プロセスを開始する前に、『Update Guide』を確認してください。

ソフトウェア バージョン

アプライアンスソフトウェアをバージョン 7.4.2 に更新するには、アプライアンスにバージョン 7.3.0、7.3.1、7.3.2、7.4.0、または 7.4.1 がインストールされている必要があります。以下の点にも注意してください。

- **パッチ**：アップグレードする前に、アプライアンスに最新のロールアップパッチをインストールしていることを確認してください。Cisco Software Central（https://software.cisco.com）の Cisco スマートアカウントからファイルをダウンロードできます。

- **ファイルのダウンロード**：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。[ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ソフトウェアのダウンロード（Software Download）] を選択します。[セキュリティ（Security）] > [ネットワークの可視性とセグメンテーション（Network Visibility and Segmentation）] > [Secure Network Analytics] の順に選択します。
- **ファイルのアップロード**：ロールアップパッチまたはソフトウェア アップデート ファイルのインストールを開始する前に、すべての SWU ファイルをアップデートマネージャにアップロードしてください。『更新ガイド』の手順に従ってください。
- **アプライアンス ソフトウェア バージョンの段階的更新**：たとえば、Secure Network Analytics v7.1.x を使用している場合は、各アプライアンスを v7.1.x から v7.2.x に更新した後、v7.2.x を v7.3.2 などに更新します。各更新ガイドは、Cisco.com で入手できます。
- **ベースライン**：v7.4.2 への更新を開始する前に、アプライアンスが同じバージョンの **v7.3.0**、**v7.3.1**、**v7.3.2**、**v7.4.0**、または **v7.4.1** で 1 か月（30 日）以上実行されていることを確認してください。短期間にシステムを複数のバージョンに更新した場合、システムのベースラインが影響を受ける可能性があります。サポートが必要な場合は、シスコサポートまでお問い合わせください。
- **ダウングレード**：更新すると、更新時にインストールされる新機能をサポートするために必要な変更がデータ構造や設定に対して行われるため、バージョンのダウングレードはサポートされていません。
- **TLS**：Secure Network AnalyticsTLS v1.2 が必要です。
- **サードパーティ製アプリケーション**：Secure Network Analytics は、アプライアンスへのサードパーティ製アプリケーションのインストールをサポートしていません。

サポートされているハードウェア プラットフォーム

Secure Network Analytics は、最新世代の UCS ハードウェア（M6）で使用できます。各システムバージョンでサポートされているハードウェア プラットフォームについては、Hardware and Version Support Matrix を参照してください。

CIMC ファームウェアバージョン

共通の更新プロセスまたはハードウェアに固有の共通の更新パッチを使用して、CIMC ファームウェアバージョンを必ず更新してください。

次の表に示すアプライアンスの場合、M4 に共通の更新プロセスは UCS C シリーズ M4 ハードウェアに適用され、共通の更新パッチは M5 ハードウェアに適用されます。

M4 ハードウェア	M5 ハードウェア
Manager 2200	Manager 2210
FC 4200	FC 4210
FC 5020 エンジン	_
FC 5020 データベース	_
FC 5200 エンジン	FC 5210 エンジン

M4 ハードウェア	M5 ハードウェア
FC 5200 データベース	FC 5210 データベース
FS 1200	FS 1210
FS 2200	—
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210

VMware 互換性変更の通知

Secure Network Analytics v7.4.2 は、VMware 7.0 および 8.0 と互換性があります。VMware 6.0、6.5、または 6.7 と Secure Network Analytics v7.4.x はサポートしていません。詳細については、『vSphere 6.0, 6.5, and 6.7 End of General Support』の VMware のマニュアルを参照してください。

証明書チェック

v7.4.2 への更新には、シスコのバンドルに共通の更新によって使用中の環境に問題が発生しないことを確認するため、証明書チェックが含まれています。証明書を使用している場合は、証明書の完全なチェーンが（個別のファイルとして）Central Management の信頼ストアに存在することを確認します。信頼ストアにエンドエンティティ証明書のみがある場合は、アップグレードは失敗します。

シスコのバンドル

最新のシスコのバンドルに共通の更新パッチがインストールされていることを確認してください。詳細については、Cisco Bundles Common Update Patch の readme を参照してください。パッチには、以下の特徴があります：

- 厳選したルート認証局（CA）の事前検証済みのデジタル証明書を提供しています。これには、
- シスコのサービスとの接続に使用するコア証明書バンドルと、シスコ以外のサービスとの接続に使用する外部証明書バンドルが含まれます。

高可用性

UDP Director で高可用性が構成されていて、Secure Network Analytics を v7.4.2 に更新する予定の場合は、更新を開始する前に、UDP Director の高可用性設定を必ず書き留めておいてください。更新が完了したら、高可用性を再構成する必要があります。Secure Network Analytics の更新の詳細については、更新ガイドを参照してください。

サードパーティ製アプリケーション

Secure Network Analytics は、アプライアンスへのサードパーティ製アプリケーションのインストールをサポートしていません。

アプリケーションのバージョンの互換性

以前にアプリをインストールしたことがある場合は、インストールする Secure Network Analytics のバージョンと互換性があることを確認します。

インストールされているアプリケーションのリストを確認する方法と最新の Cisco Secure Network Analytics アプリケーションの互換性情報を確認する方法については、Secure Network Analyticsアプリケーションのバージョン互換性マトリックスを参照してください。

ブラウザ

- **互換性のあるブラウザ**：Secure Network Analytics は Chrome、Firefox、および Edge の最新のラピッドリリースをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft Edge を使用して、ソフトウェア アップデート ファイル（SWU）をアップロードしないことをお勧めします。
- **ショートカット**：ブラウザのショートカットを使用して、いずれかの Secure Network Analytics アプライアンスのアプライアンス管理インターフェイスにアクセスしている場合、更新プロセスの完了後はショートカットが機能しないことがあります。その場合は、ショートカットを一旦削除してから再作成してください。
- **証明書**：一部のブラウザでは、アプライアンス アイデンティティ証明書の有効期限の要件が変更されています。アプライアンスにアクセスできない場合は、『SSL/TLS Certificates for Managed Appliances Guide』を参照して証明書を置き換えるか、Cisco サポートまでお問い合わせください。

代替アクセス

今後のサービスのニーズを想定し、Secure Network Analytics アプライアンスにアクセスする代替方法を有効にしておく必要があります。

次のいずれかのオプションを使用して Secure Network Analytics アプライアンスにアクセスできることを確認してください。

仮想アプライアンス：コンソール（コンソールポートへのシリアル接続）

KVM を介してアプライアンスにアクセスするには、Virtual Manager のドキュメントを参照してください。または、VMware を介してアプライアンスに接続するには、vSphere の vCenter Server Appliance 管理インターフェイスのドキュメントを参照してください。

ハードウェア：コンソール（コンソールポートへのシリアル接続）

ラップトップまたはモニター付きキーボードを使用してアプライアンスに接続するには、「インストールとアップグレードガイド」ページにリストされている最新の『Secure Network Analytics Hardware Installation Guide』を参照してください。

ハードウェア：CIMC（UCS アプライアンス）

CIMC を介してアプライアンスにアクセスするには、『Cisco Integrated Management Controller (CIMC) Configuration Guides』 ページにリストされているプラットフォームの最新のガイドを参照してください。

別の方法

今後サービスが必要になった場合に備えて、次の手順に従い、Secure Network Analytics アプライアンスにアクセスする別の方法を有効にします。

仮想またはハードウェアの方法を使用してアプライアンスにログインできない場合は、アプライアンスのネットワーク インターフェイスで一時的に SSH を有効にできます。

> ⚠ SSH を有効にすると、システムの侵害リスクが増加します。必要な場合にのみ SSH を有効にし、使用が終了したら無効にすることが重要です。

1. Manager にログインします。
2. [グローバル設定(Global Settings)] アイコンをクリックします。
3. [集中管理(Central Management)] を選択します。
4. アプライアンスの [アクション(Actions)] メニューをクリックします。
5. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
6. [アプライアンス(Appliance)] タブを選択します。
7. [SSH] セクションを見つけます。
8. SSH アクセスのみを有効にするか、ルートアクセスも有効にするかを選択します。
   - [SSH の有効化(Enable SSH)]:アプライアンスへの SSH アクセスを許可するには、このチェックボックスをオンにします。
   - [ルート SSH アクセスの有効化(Enable Root SSH Access)]:アプライアンスへのルートアクセスの有効化を許可するには、このチェックボックスをオンにします。
9. [設定の適用(Apply settings)] をクリックします。
10. 画面に表示される指示に従って、変更を保存します。

> ⚠ SSH は、使用が終了したら必ず無効にしてください。

Data Store のプライベート LAN の設定と Data Node の拡張

v7.4.1 以降、Secure Network Analytics は プライベート LAN の IP アドレスに特定の要件を適用します。プライベート LAN の IP アドレスを使用して設定されている Data Node のすべてが次の要件を満たしていることを確認してください。

- 最初の 3 オクテットが **169.254.42** であること。
- サブネットが **/24** であること。

> ℹ 例:169.254.42.x/24(x はサイトによって割り当てられた番号(2 ～ 255))

詳細については、シスコサポートに問い合わせてください。

Data Node パッチ SWU

7.4.0 への更新では、各 Data Node にパッチ SWU をインストールする必要がありました。Secure Network Analytics v7.4.2 への更新では、Data Node パッチ SWU は必要**ありません**。

新着情報

Secure Network Analytics v7.4.2 リリースの新機能と改善点は次のとおりです。

メニュー構造

v7.4.2 でメニュー構造とページ名を変更し、エクスペリエンスを簡素化しました。また、ヘルプメニューの構成も新しい構造に合わせて更新しました。

以前のメニュー構造（v7.4.1、v7.4.0、および v7.3.x）

新しいメニュー構造（v7.4.2）

次の表は、以前のメニューの場所によって編成され、新しいページ名とメニューの場所を示しています。

新しいメニューの一部には、[構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）]（グローバルはカテゴリ）などのカテゴリも含まれており、ここにリストされています。

旧ページ名	新しいページ名	旧メニューの場所	新しいメニューの場所
ネットワーク セキュリティ	Security Insight Dashboard	ダッシュボード	モニタ（Monitor）
Secure Cloud Analytics	Secure Cloud Analytics	ダッシュボード	[モニタリング（Monitor）] > [統合（Integrations）]
可視性アセスメント	可視性アセスメント	ダッシュボード	レポート
レポートビルダー	レポートビルダー	ダッシュボード	レポート
グローバル脅威アラート	グローバル脅威アラート	ダッシュボード	[モニタリング（Monitor）] > [統合（Integrations）]
ETA 暗号化の監査	ETA 暗号化の監査	ダッシュボード	アプリ
Host Classifier	Host Classifier	ダッシュボード	アプリ
Network Diagrams	Network Diagrams	ダッシュボード	アプリ

旧ページ名	新しいページ名	旧メニューの場所	新しいメニューの場所
セキュリティ分析とロギング	セキュリティ分析とロギング（オンプレミス）| ファイアウォールイベント	ダッシュボード	アプリ
ホスト	ホスト	モニタ（Monitor）	[調査（Investigate）] > [アセット（Assets）]
[ホスト グループ（Host Groups）]	[ホスト グループ（Host Groups）]	モニタ（Monitor）	[調査（Investigate）] > [アセット（Assets）]
Users	Users	モニタ（Monitor）	[調査（Investigate）] > [アセット（Assets）]
ISE ANC の割り当て	ISE ANC ポリシーの割り当て	モニタ（Monitor）	[モニタリング（Monitor）] > [統合（Integrations）]
[インターフェイス（Interfaces）]	[インターフェイス（Interfaces）]	モニタ（Monitor）	[調査（Investigate）] > [アセット（Assets）]
アラート（Alerts）	アラート（Alerts）	モニタ	モニタ
オブザベーション（Observations）	オブザベーション（Observations）	モニタ	モニタ
フロー検索	フロー検索	分析（Analyze）	[調査（Investigate）]
保存済み検索（Saved Searches）	保存済み検索（Saved Searches）	分析（Analyze）	[調査（Investigate）] > [検索管理（Search Management）]
保存された結果	保存された結果	分析（Analyze）	[調査（Investigate）] > [検索管理（Search Management）]
ホスト検索	ホスト検索	分析（Analyze）	[調査（Investigate）]
著作権侵害	著作権侵害	分析（Analyze）	[調査（Investigate）]
ジョブ管理	ジョブ管理	ジョブ	[調査（Investigate）] > [検索管理（Search Management）]

旧ページ名	新しいページ名	旧メニューの場所	新しいメニューの場所
ポリシー管理	ポリシー管理	設定（Configure）	[構成（Configure）] > [検出（Detection）]
アラーム	アラームの重大度（Alarm Severity）	設定（Configure）	[構成（Configure）] > [検出（Detection）]
Analytics	Analytics	設定（Configure）	[構成（Configure）] > [検出（Detection）]
アラート（Alerts）	アラート（Alerts）	設定（Configure）	[構成（Configure）] > [検出（Detection）]
ホストグループ管理	ホストグループ管理	設定（Configure）	[構成（Configure）] > [検出（Detection）]
ネットワーク分類	ネットワークスキャナ	設定（Configure）	[構成（Configure）] > [検出（Detection）]
サービス	サービス	設定（Configure）	[構成（Configure）] > [システム（System）]
アプリケーション	アプリケーション	設定（Configure）	[構成（Configure）] > [システム（System）]
応答管理	応答管理	設定（Configure）	[構成（Configure）] > [検出（Detection）]
ドメインのプロパティ	ドメインのプロパティ	設定（Configure）	[構成（Configure）] > [システム（System）]
Flow Collector	Flow Collector	設定（Configure）	[構成（Configure）] > [システム（System）]
エクスポータ	エクスポータ	設定（Configure）	[構成（Configure）] > [システム（System）]
Cisco ISE の設定	Cisco ISE	[展開（Deploy）]	[構成（Configure）] > [統合（Integrations）]
アクティブディレクトリ	アクティブディレクトリ	[展開（Deploy）]	[構成（Configure）] > [統合（Integrations）]
Secure Cloud Analytics の構成	Secure Cloud Analytics	[展開（Deploy）]	[構成（Configure）] > [統合（Integrations）]

旧ページ名	新しいページ名	旧メニューの場所	新しいメニューの場所
ヘルプ	ヘルプ	([ユーザ(User)])アイコン	([ヘルプ(Help)])アイコン
リソース	リソース	([ユーザ(User)])アイコン	([ヘルプ(Help)])アイコン
バージョン情報	バージョン情報	([ユーザ(User)])アイコン	([ヘルプ(Help)])アイコン
Profile	Profile	([ユーザ(User)])アイコン	([ユーザ(User)])アイコン
ログアウト	ログアウト	([ユーザ(User)])アイコン	([ユーザ(User)])アイコン
Central Management	Central Management	([グローバル設定(Global Settings)])アイコン	[構成(Configure)]>[グローバル(Global)] 注:アプライアンスマネージャの名前はインベントリになりました。
Manager の設定	Manager	([グローバル設定(Global Settings)])アイコン	[構成(Configure)]>[グローバル(Global)]
パケットアナライザの設定	パケット アナライザ	([グローバル設定(Global Settings)])アイコン	[構成(Configure)]>[グローバル(Global)]
UDP Director の設定	UDP Director	([グローバル設定(Global Settings)])アイコン	[構成(Configure)]>[グローバル(Global)]
外部ルックアップの設定	外部検索	([グローバル設定(Global Settings)])アイコン	[構成(Configure)]>[グローバル(Global)]
User Management	User Management	([グローバル設定(Global Settings)])アイコン	[構成(Configure)]>[グローバル(Global)]

旧ページ名	新しいページ名	旧メニューの場所	新しいメニューの場所
SecureX の設定	SecureX	⚙([グローバル設定(Global Settings)])アイコン	[構成(Configure)] > [統合(Integrations)]
言語の選択	言語	⚙([グローバル設定(Global Settings)])アイコン	👤([ユーザ(User)])アイコン

証明書有効期限アラームと電子メール通知

アプライアンス アイデンティティ証明書の有効期限が切れている場合、次のシステムアラームがダッシュボードに表示され始めます。

- アプライアンス証明書の有効期限が 90 日未満
- アプライアンス証明書の有効期限が 60 日未満
- アプライアンス証明書の有効期限が 30 日未満
- アプライアンス証明書の有効期限が 14 日未満
- アプライアンス証明書の有効期限が 3 日未満
- アプライアンス証明書の有効期限切れ

これらのシステムアラームはデフォルトで有効になっており、必要に応じてアプライアンス アイデンティティ証明書を置き換えるまで表示され続けます。

以前に Response Management を介して電子メール通知を設定している場合は、アプライアンスのアイデンティティ証明書が期限切れになることを示す電子メールメッセージも受信します。

受信する電子メール通知を変更する場合は、詳細について、管理対象アプライアンスの SSL/TLS 証明書ガイドの「期限切れの証明書の通知の受信」セクションを参照してください。

期限が切れていないシスコの自己署名アプライアンス アイデンティティ証明書の置換(証明書の更新)

既存の証明書の有効期限が切れていない場合に、新しいシスコの自己署名アプライアンス アイデンティティ証明書を生成するためのワークフローが簡素化されました。Manager アプライアンスコンソール([システム設定(System Configuration)])の [証明書の更新(Certificate Refresh)] メニューを使用して、すべての管理対象アプライアンスまたは選択した個々のアプライアンスのアイデンティティ証明書を生成できます。

- **ホスト情報**:アプライアンスのホスト情報(IP アドレス、ホスト名、ドメイン名)は保持されます。
- **必須のパッチ**:『Secure Network Analytics Manager Update Patch v7.4.2』[英語] の手順に従って、Manager にパッチ ROLLUP20230928-01(またはそれ以降)をインストールしてください。
- **手順**:『SSL/TLS Certificates for Managed Appliances Guide』[英語] の手順に従います。
- **カスタム証明書**:アプライアンス アイデンティティ証明書は、この証明書更新手順でシスコの自己署名アプライアンス アイデンティティ証明書に自動的に置き換えられます。カスタム証明

書を使用するには、『SSL/TLS Certificates for Managed Appliances Guide』[英語] の「SSL/TLS アプライアンス アイデンティティ証明書の置換」の手順に従います。

ECDSA 証明書の互換性

アプライアンスのインストール、アプライアンスのアイデンティティ証明書の生成、またはクライアントのアイデンティティ証明書の生成を行う場合、Secure Network Analytics は RSA キーを使用して証明書を生成します。

v7.4.2 では、システム証明書を、NIST P-256、P-384、または P-521 曲線で生成された ECDSA キーを使用するカスタム証明書に置き換えることができます。

また、ECDSA キー(NIST P-256、P-384、または P-521 曲線で生成される)を使用するカスタム証明書を、Central Management のアプライアンス信頼ストアにアップロードすることもできます。

手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

レポートビルダー

v7.4.0 では、レポートビルダーを別のアプリケーションからコア Secure Network Analytics に移動しました。Secure Network Analytics を v7.3.x から v7.4.2 に更新すると、その更新の一環としてアプリケーションは自動的に削除されます。

> ⚠ 既存の レポートビルダー アプリケーションはアンインストールしないでください。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。

『更新ガイド』の手順に従ってください。Secure Network Analytics を v7.4.2 に更新したら、次のようにレポートビルダー ダッシュボードにアクセスします。

1. Manager にログインします。
2. [レポート(Report)] メニューを選択します。
3. [レポートビルダー(Report Builder)] を選択します。
4. 手順については、?([ヘルプ(Help)])アイコン > [ヘルプ(Help)] をクリックしてください。

> ℹ レポートを実行する前に、データを含むデータストアドメインまたは非データ ストアドメインを選択します。

サーバーの ID 検証

v7.4.x では、TLS 接続に対してより厳格なセキュリティチェックが追加されました。これには、追加の証明書要件が含まれる場合があります。すべての新しい構成について、指示に従っていることを確認してください。

- **監査ログの宛先**:ヘルプの手順に従います。?([ヘルプ(Help)])アイコン > [ヘルプ(Help)] を選択して「監査ログの宛先」を検索します。v7.4.1 以降では、リモート syslog サーバーのサーバー名または IPv4 アドレスを使用して監査ログの宛先を構成できます。
- **シスコISEまたは Cisco ISE-Pic**:『ISE and ISE-PIC Configuration Guide』の手順に従います。また、関連情報については、「**厳密なISEサーバー ID 検証**」を参照してください。
- **応答管理に対する SMTP の設定**:ヘルプの指示に従ってください。?([ヘルプ(Help)])アイコン > [ヘルプ(Help)] を選択して「SMTP の設定」を検索します。

サーバーの本人確認：更新の準備（7.3.x ～ 7.4.2 のみ）

7.3.x から 7.4.2 への更新の一環として、次の設定を見直してサーバーのアイデンティティ検証の要件を満たしていることを確認します。

- 監査ログの保存先（TLS経由のSyslog）
- SMTP 構成（応答管理の電子メール通知）

更新を開始する前に、構成を確認してください。構成が要件を満たしていない場合、更新は失敗します。詳細については『更新ガイド』を参照してください。

監査ログの宛先の要件

更新の前に、監査ログの宛先構成が**次の両方の要件**を満たしていることを確認してください。

- Syslog over TLS をサポートする syslog サーバーからのルート認証局（CA）SSL 証明書がアプライアンスの信頼ストアに含まれていることを確認します。監査ログの宛先が構成されている各アプライアンスの信頼ストアを確認します。
- syslog サーバーの ID 証明書の［サブジェクト（Subject）］フィールドまたは［サブジェクトの別名（Subject Alternative Name）］フィールドに syslog サーバーの IP アドレスが含まれていない場合は、アドレスを監査ログの宛先が構成されている各アプライアンスの信頼ストアに追加します。

信頼ストアにアクセスするには、Manager にログインします。［構成（Configure）］＜［グローバル集中管理（GLOBAL Central Management）］を選択します。アプライアンスの ••• （［省略記号（Ellipsis）］）アイコンをクリックします。［アプライアンス構成の編集（Edit Appliance Configuration）］を選択します。［全般（General）］タブを選択し、［信頼ストア（Trust Store）］セクションまでスクロールします。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

SMTP 設定の要件

更新の前に、SMTP 設定が**次の要件のいずれか**を満たしていることを確認してください。

- 認証局（CA）からの SMTP サーバー ID 証明書に、Secure Network Analyticsで設定した IP アドレスまたはホスト名と一致する［サブジェクト（Subject）］または［サブジェクトの別名（Subject Alternative Name）］があることを確認します。**または**
- Manager の信頼ストアに SMTP サーバー ID 証明書を追加します。

Manager の信頼ストアにアクセスするには、Manager にログインします。［構成（Configure）］＜［グローバル集中管理（GLOBAL Central Management）］を選択します。Manager の ••• （［省略記号（Ellipsis）］）アイコンをクリックします。［アプライアンス構成の編集（Edit Appliance Configuration）］を選択します。［全般（General）］タブを選択し、［信頼ストア（Trust Store）］セクションまでスクロールします。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

厳密なISEサーバー ID 検証

Manager が Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE-PIC）クラスタノードと通信するときにサーバー ID 検証を要求するには、厳格な ISE サーバー ID 検証を有効にします。

他のセキュリティチェックに加えて、ISE サーバー ID 証明書が次のいずれかを満たす場合は、通信を許可します。

- これには、共通名またはサブジェクト代替名としてリストされている pxGrid ノード名または ID 情報（FQDN など）が含まれます。または、
- Manager の信頼ストア内の証明書と一致します。

以前のバージョン（7.3.x 以前）から Secure Network Analytics を更新する場合は、この設定を有効にすることを選択できます。Secure Network Analytics の新しいバージョン（v7.4.0 以降）をインストールすると、この設定はデフォルトで有効になります。

この設定を有効または無効にするには、[展開（Deploy）] > [Cisco ISE設定（Cisco ISE Configuration）] を選択します。詳細については、『ISE and ISE-PIC Configuration Guide』を参照してください。

Secure Network Analytics アプリケーション

Secure Network Analytics アプリケーションは、Secure Network Analytics の機能を強化および拡張する、独自にリリース可能なオプションの機能です。

Secure Network Analytics アプリケーションのリリーススケジュールは、通常の Secure Network Analytics のアップグレードプロセスとは無関係です。そのため、Secure Network Analytics のコアリリースとリンクさせなくても、必要に応じて Secure Network Analytics アプリケーションを更新できます。

Secure Network Analytics の新しいリリースに対応するように設計されたアプリが、すぐにインストールできない場合があります。アプリケーションの最新バージョンが提供されるまでに数週間かかる場合もあります。

最新の Secure Network Analytics アプリケーションの情報と可用性については、次を参照してください。

- Secure Network Analytics アプリケーションのバージョン互換性マトリクス
- Secure Network Analytics アプリケーションのリリースノート

アプリケーションへのアクセス

v7.4.2 にアップグレードしたら、次の手順を実行してアプリにアクセスします。

1. 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。
2. Secure Network Analytics[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。

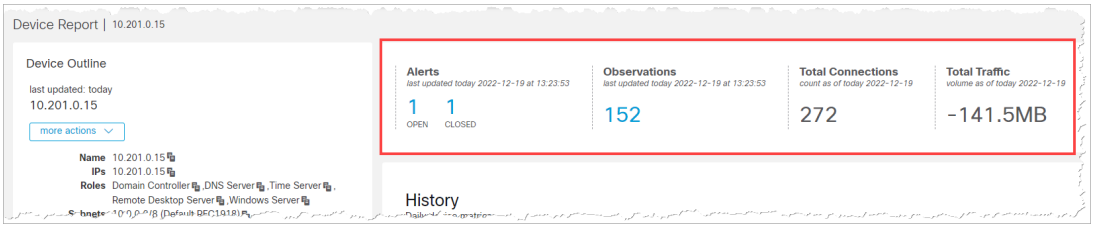
   [アプリケーションマネージャ（App Manager）] ページが開きます。インストールされているアプリケーションのリストが [アプリケーション（Apps）] テーブルに表示されます。

Analytics

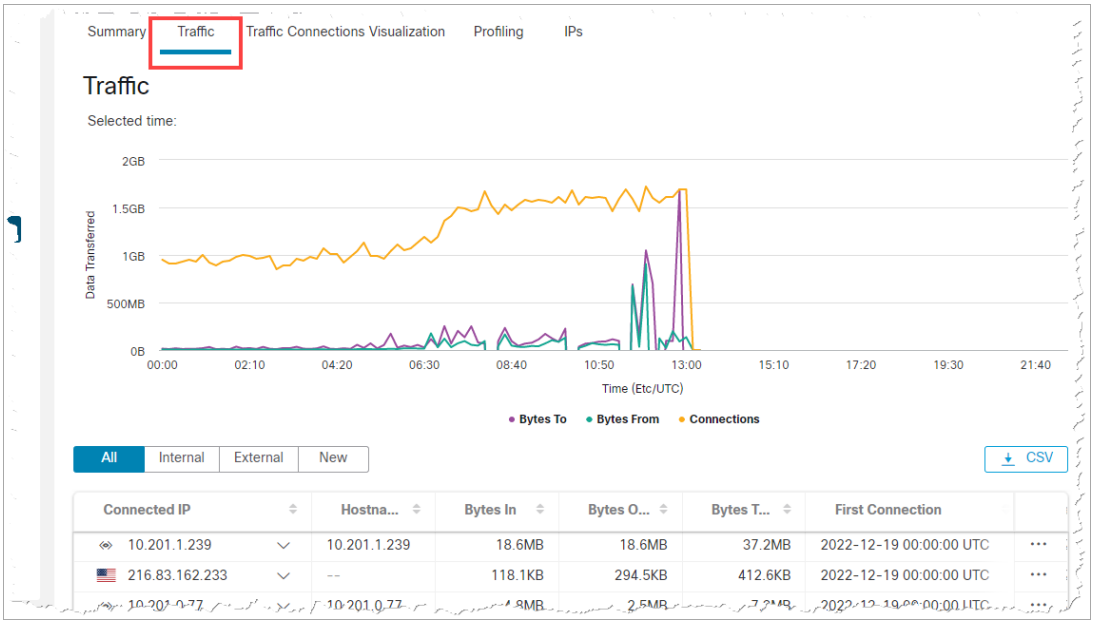
Secure Network Analytics v7.4.2 では、Analytics に対して次の機能強化が行われました。

- Alerts and Observations で SMC フェールオーバーがサポートされるようになりました。アラートおよび観測データは、現在プライマリロールである Manager でのみ処理および保存されます。元のプライマリ Manager を昇格してプライマリロールに戻すと、元のセカンダリ Manager がプライマリロールで機能していたときに処理されたアラートおよび観測データは表示できなくなります。
- v7.4.1 から v7.4.2 にアップグレードすると、顧客のデータは保持されません。

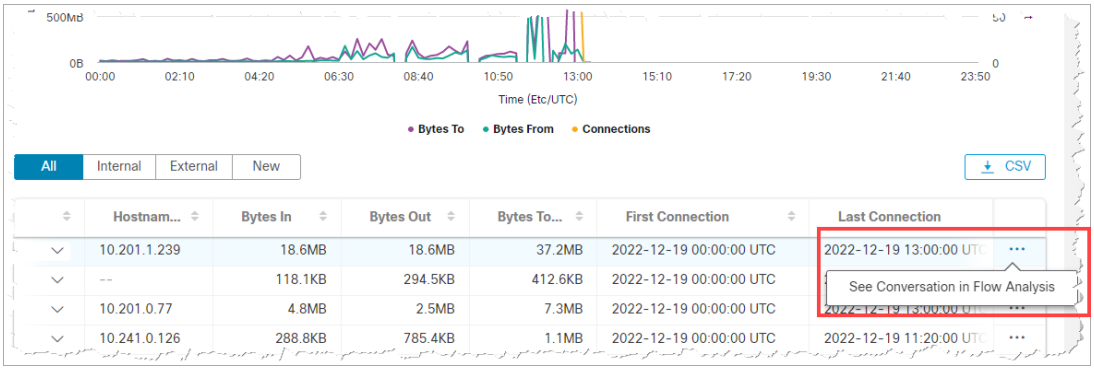
- 次の新しいアラートを追加しました：
  - LDAP 接続の急増
  - アウトバウンド LDAP スパイク
  - プロトコル偽造
  - 反復的な Cisco Umbrella シンクホール通信
- 次の新しい観測結果が追加されました。
  - Cisco Umbrella シンクホールヒットの観測
- アウトバウンド SMB スパイクアラートの名前をアウトバウンド SMB 接続スパイクに変更しました
- 次の新しいシステムアラームが追加されました。
  - Analytics は複数の Data Store ドメインをサポートしていません
  - 分析のパフォーマンスが低下しました
  - 分析結果が不完全です
- デバイスレポート
  - アラートデータを [概要（Summary ）] タブからメインページに移行しました。



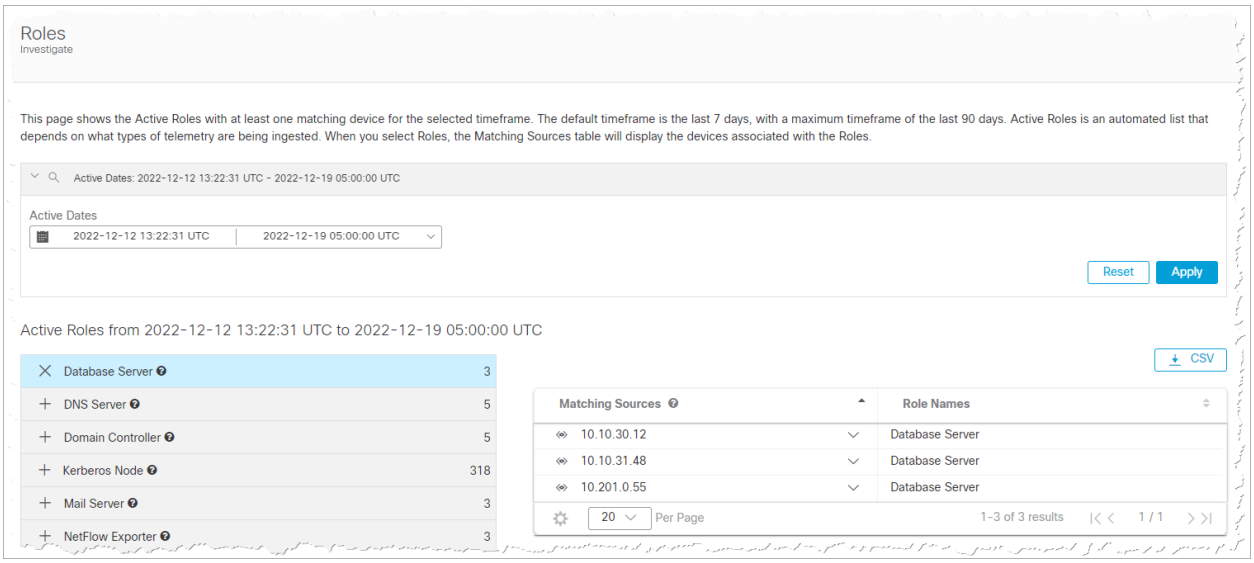
  - [トラフィック接続の視覚化（Traffic Connections Visualization）] タブを追加しました。



- [トラフィック（Traffic ）] タブの表の最後の列に「フロー分析の会話を参照」リンクを追加しました。



- Roles ページ（メニューから [調査（Investigate）] > [アセットロール（ASSETS Roles）] を選択）を追加しました。



Analytics の有効化

Analytics を有効にするには、メインメニューから [構成（Configure）] > [検出分析（DETECTION Analytics）] を選択します。開いたウェルカムページで、ページの右上隅にあるスイッチをクリックして、ラベルに [Analyticsが有効（Analytics On）] が表示されるようにします。

Analytics へのアクセス

Analytics がすでに有効になっている場合は、メインメニューから [監視（Monitor）] > [アラート（Alerts）] を選択します。[アラート概要（Alerts Summary）] が開きます。

Data Store アプライアンスのサポート

Data Store の購入を計画している場合は、Cisco プロフェッショナルサービスに連絡し、全体的な Secure Network Analytics 展開の範囲内および展開の一環として、配置、展開、および設定の支援を受けてください。

次の表で、Data Store アプライアンスのサポートについて説明します。

アプライアンス	必須かどうか	サポートされるモデル
Data Store	Yes	• DS 6200 マルチノード（v7.4 以降）またはシングルノード（v7.4.1 以降）、バーチャルエディション • DN 6300 マルチノードまたはシングルノード（v7.4.2 以降）、バーチャルエディション
Manager	Yes	• Manager 2200、バーチャルエディション • Manager 2210 または Manager バーチャルエディション（v7.4 以降）。バーチャルエディションでは 4 つのモデルが利用可能 • Manager 2300 または Manager バーチャルエディション（v7.4.2 以降）。
Flow Collector	Yes	• Flow Collector 4200 番台、5200 番台、Virtual Edition • Flow Collector4210 番台またはFlow Collector Virtual Edition（v7.4 以降）* • Flow Collector4300 番台またはFlow Collector Virtual Edition（v7.4.2 以降）* • Flow Collector5210 番台またはFlow Collector Virtual Edition（v7.4 以降）* * バーチャルエディションでは 4 つのモデルが利用可能
Flow Sensor	いいえ	• M5SX 以前の世代の場合、v7.4 以降の任意のモデルです。 • M6SX 世代の場合、Flow Sensor は v7.4.2 以降でのみサポートされます。
UDP Director	×	• v7.3 以降のすべてのモデル

Data Node の混在はサポートされていません。データストアはすべて仮想ハードウェアであるか、すべてハードウェアである必要があり、同じ世代のハードウェア（すべて DS 6200 またはすべて DN 6300）である必要があります。

Data Store の機能拡張

v7.4.2 には、次の Data Store の機能拡張が含まれています。詳細については、Cisco 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 Virtual Edition）とシステム コンフィギュレーション ガイドを参照してください。

非 Data Store Flow Collector の Data Store Flow Collector への移行

非 Data Store Flow Collector を Data Store Flow Collector に移行すると、Data Store でのみ使用可能な次のような機能を利用できます。

- **取り込み容量の増加**：Data Store の展開は、1 秒あたり最大 300 万フローまで拡張可能であり、現在の取り込み容量の制限を緩和できます。Data Store モードの Flow Collectors は、パフォーマンスが最大 200% 向上します。
- **マルチテレメトリのサポート**：Data Store の展開では、NetFlow、リモートワーカー/エンドポイント（NVM）、ファイアウォール接続、およびセキュリティ イベント テレメトリを処理できます。
- **長期データ保持**：Data Store の展開はスケーラブルなストレージを提供し、Flow Collectors を追加することなく長期データ保持（最大 2 年間）を可能にします。
- **エンタープライズクラスのデータ回復力**：テレメトリデータはデータノード全体に冗長的に保存されるため、単一ノードの障害時にサービスが中断されることはありません。
- **クエリとレポートの応答時間の大幅な改善**：Data Store は、クエリのパフォーマンスとレポートの応答時間を大幅に改善します。これは、非 Data Store 展開モデルと比較して、場合によっては 10 倍以上高速です。
- **Analytics**：Analytics は、追加の検出機能やモデリング機能に加えて、セキュリティ上の懸念事項を確認して優先順位付けし、対処できる新しいインターフェイス機能を提供します。

  Analytics は以下を提供します。

  - 自動ロール検出
  - 追加アラート機能
  - 実験的なアラートダッシュボード
  - サポートデバイスレポート
- **SAL テレメトリ**：Security Analytics and Logging（SAL）は、ファイアウォール（FTD および ASA）からのログを集約し、ネットワークアクティビティの直感的なビューを提供することにより、意思決定を合理化します。

  SAL は自由に拡張できるため、長期間の保持と分析が可能になり、ファイアウォールで見つかった潜在的な脅威に関するアラートも可能になります。

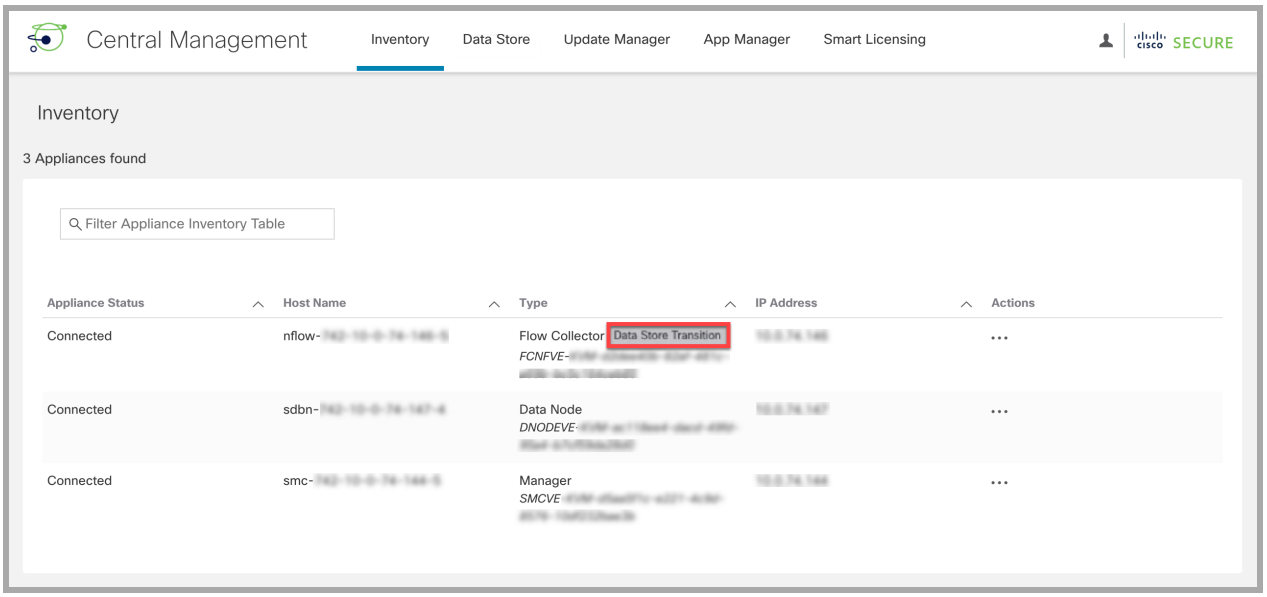
移行前のデータや可視性を失うことなく、既存の Flow Collectors を移行して Data Store データベースを使用できます。最初の移行プロセスが完了すると、必要がなくなるまで既存のデータを保持できます。

移行プロセスを完了すると、Flow Collector は Data Store Flow Collector のみになります。Flow Collector が保存している既存の非 Data Store データはすべて削除され、リソースが回復されるため、Flow Collector のパフォーマンスが向上します。

非 Data Store Flow Collector の Data Store Flow Collector への移行の詳細については、『System Configuration Guide』を参照してください。

「Data Store」移行タグで識別される移行中の Data Store Flow Collector

Flow Collector の [インベントリ(Inventory)] タブまたは [更新マネージャ(Update Manager)] タブに Data Store 移行タグが表示されている場合、Flow Collector は Data Store にフローを送信するように構成されています。詳細については、『System Configuration Guide』を参照してください。



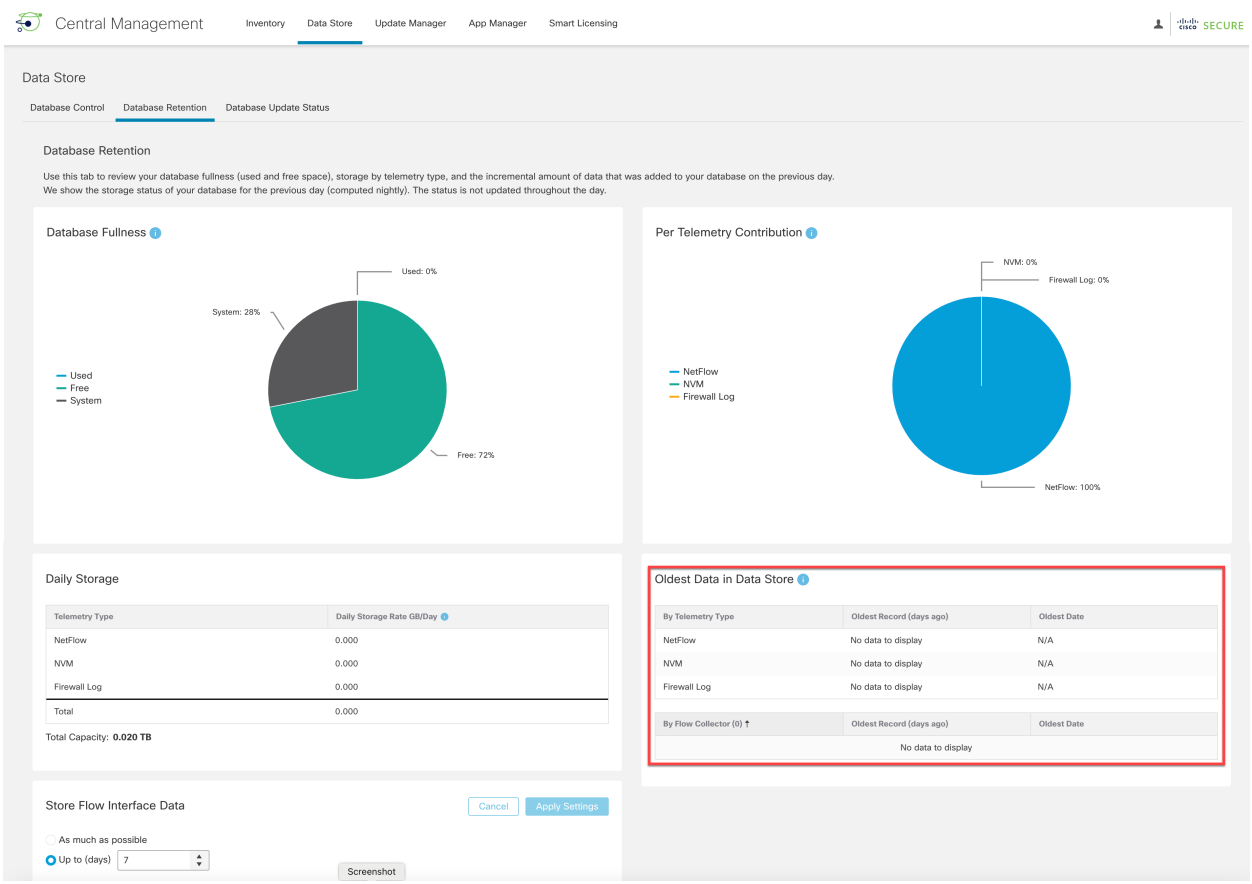
移行中の Flow Collector のデータベースパスワードは変更できません

データベースのパスワードを変更すると、非 Data Store Flow Collector と移行中の Flow Collector のみが新しいパスワードを受け取ります。Data Store のパスワードの変更については、『System Configuration Guide』を参照してください。

Data Store テーブル内の最も古いデータ

この表は、最も古いレコードが Data Store に書き込まれてからの日付と日数を示しています。このデータは 1 日に 1 回更新されます。Flow Collector(または Flow Collector データベース)にローカルに保存されたデータは、このテーブルには含まれません。非 Data Store Flow Collector を Data Store Flow Collector に移行していて、データ保持ポリシーがある場合は、この表を使用すると、Data Store 内に新しいデータがどれだけあるかを理解し、移行を完了するのに最適な時期を知ることができます。

詳細については、『System Configuration Guide』を参照してください。



Data Store ドメインと非 Data Store ドメインの同期

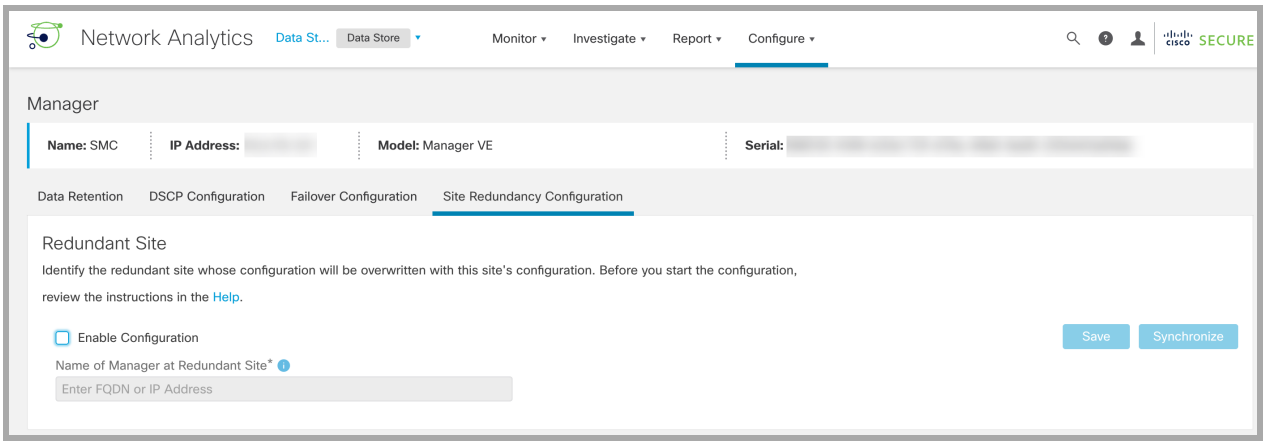
Flow Collector の移行中、移行前の非 Data Store ドメインと Data Store ドメインの間で設定と調整の同期を維持したい場合があります。詳細については、『System Configuration Guide』を参照してください。

冗長サイト設定

サイトの冗長性を使用すると、類似のアプライアンスを使用した個別の展開を含む 2 つの Cisco Secure Network Analytics サイトのクラスタ間でほぼ冗長性を確立できます。

サイトの冗長性により、プライマリサイトでドメインと Analytics 構成を維持し、冗長サイトと手動で同期することができます。また、データセンターが停電した場合に高可用性保護を提供します。サイトの冗長性を使用すると、冗長クラスタのいずれかにログインして、ほぼ同じデータを表示できます。

サイトの冗長性の詳細については、『System Configuration Guide』を参照してください。



Data Store システム設定メニュー

[システム設定（System Configuration）] の [Data Store] メニューを更新しました。これらのメニューは、新しい展開か既存の展開の拡張に使用します。システム設定を正しく行うには、『システム コンフィギュレーション ガイド』の手順に従ってください。

- **SSH**：このメニューを使用して、[Data Store] メニューの他の手順に必要な SSH を一時的に有効にします。システム設定を終了すると、システムで以前の SSH 設定が復元されます。
- **初期化（Initialization）**：すべての Manager、Flow Collector、および Data Node を Central Management のインベントリに追加した後、このメニューを使用して Data Store を初期化します。
- **新しいアプライアンス（New Appliances）**：すべての Manager、Flow Collector、および Data Node を Central Management のインベントリに追加した後、このメニューを使用して Data Store とのセキュア通信が確立されるように新しい Manager と Flow Collector を設定します。
- **新しい Data Node（New Data Nodes）**：すべての Manager、Flow Collector、および Data Node を Central Management のインベントリに追加した後、このメニューを使用して Data Store とのセキュア通信が確立されるように新しい Data Node を設定します。
- **パスワード（Passwords）**：Data Store データベースのパスワード（dbadmin および readonlyuser）を変更します。非 Data Store ドメインで Flow Collector データベース のパスワードを変更するには、[Central Management] > [データベース（Database）] タブに移動します。
- **移行（Transition）**：このメニューを使用して、非 Data Store Flow Collector を Data Store Flow Collector に移行します。

エンドポイントライセンスと Network Visibility Module の機能強化

v7.4.2 では、Cisco Secure Client（AnyConnect を含む）Network Visibility Module（NVM）トラフィックを取り込む Data Store 展開に次の機能が追加されました。

- NVM トラフィックエンドポイント IP を介したホストグループへのエンドポイントの追加
- エンドポイント接続に基づくカスタム セキュリティ イベントの作成
- NVM トラフィックに基づく NetFlow 検出
- Report Builder でのオフネットワークフローの保存と表示

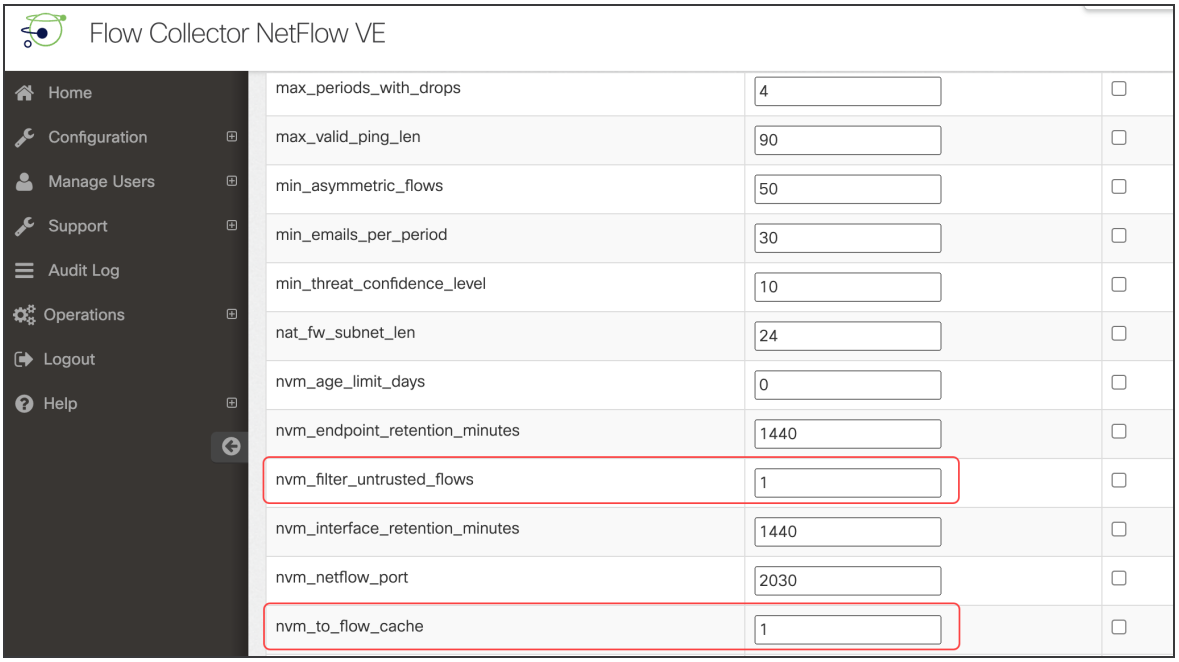
Flow Collector の詳細設定を使用した新たな追加フィールドの設定

nvm_to_flow_cache と **nvm_filter_untrusted_flows** の 2 つの新しいフィールドが追加されました。どちらもデフォルトは **0** であり、NVM の信頼できないトラフィックの処理を改善するには **1** に変更する必要があります。

> この手順を開始する前に、必ず最新の Flow Collector NetFlow ロールアップパッチをインストールしてください。

次の手順を実行します。

1. Manager にログインします。
2. 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。
3. インベントリページで Flow Collector の ••• ([省略記号(Ellipsis)]) アイコンをクリックし、[アプライアンス統計の表示(View Appliance Statistics)] を選択します。Flow Collector の管理インターフェイスが開きます。
4. [サポート(Support)] > [詳細設定(Advanced Settings)] を選択します。
5. NVM 取り込みフローのネットワークベースの検出をキャプチャするには、**nvm_to_flow_cache** フィールドの値を **1** に設定します。このフィールドのデフォルトは **0** です。
6. **nvm_filter_untrusted_flows** フィールドの値を **1** に設定します。このフィールドを有効にすると、ネットワークベースの検出から信頼できないトラフィックが除外され、IP アドレスの競合などの問題が回避されます。このフィールドのデフォルトは **0** です。



7. [適用(Apply)] をクリックします。
8. 確認メッセージが表示されたら、[OK] をクリックします。

Data Store があり、**nvm_filter_untrusted_flows** フィールドの値を 1 に設定すると、信頼できないトラフィックは除外されますが、エンドポイントトラフィック（NVM）レポートの作成に使用される NVM テーブルには保存されたままになります。Data Store がない場合、信頼できないトラフィックは保持されません。

詳細については、Secure Network Analytics『Endpoint License and Network Visibility Module Configuration Guide v7.4.2』を参照してください。

MTU 設定

v7.4.2 では、アプライアンス eth0 ネットワーク インターフェイスの最大伝送単位（MTU）を構成できます。この構成では、eth0 インターフェイスがトランザクションごとに送信できる最大パケットサイズを設定します。1500（デフォルト）、9000、またはネットワーク構成要件を満たす数値を入力します。手順については、『システム コンフィギュレーション ガイド』を参照してください。ファイアウォールログでは 8,192 バイト、NetFlow、sFlow、および NVM フローでは 9,216 バイトの最大 MTU 設定をサポートしています。セキュリティを使用してファイアウォールログを取り込んでいる場合、セキュリティ分析とロギング（オンプレミス）および別のテレメトリタイプでは、8,192 バイトを超える MTU 設定を指定しないでください。

MTU はネットワーク処理に影響します。この番号を変更する場合は、ネットワーク内で一貫して構成されていることを確認してください。

新しい Flow Collector システム アラーム

Secure Network Analytics に Flow Collector データベース更新ドロップアラームが追加されました。このアラームは、次のテレメトリタイプ（有効な場合）のデータベース更新が現在ドロップされていることを示すものです。

- ファイアウォール ログ イベントの更新
- NVM フローの更新
- NetFlow フローの更新

この状態は通常、Flow Collector が Data Store データベースに到達できないか、Data Store データベースが長期間到達できない状態が続いている場合に発生します。

詳細については、「アラームリスト：Flow Collector システムアラーム」というタイトルのヘルプトピックと『Secure Network Analytics 内部アラーム ID ガイド』の両方を参照してください。

修正点

このセクションでは、旧リリースでお客様から報告された問題（バグ/不具合）に関してこのリリースで行われた修正点の概要を示します。参照用に、Secure Network Analytics 問題（SWD または LSQ）番号が示されています。

バージョン 7.4.2

障害	説明
LVA-719	プレーンテキストでパスワードを保存する Active Directory ルックアップ構成の問題を修正しました。
SWD-15689	スマートライセンスページの誤訳に関連する問題を修正しました。（LSQ-5156）
SWD-15941	Rest API の 2k 制限を示すようにドキュメントを更新しました。（LSQ-5262）
SWD-15957	ntpdate の実行が失敗したために発生していた認証済み NTP に関連する問題を修正しました。（LSQ-5285）
SWD-16424	Flow Sensor Virtual Edition を VMware にインストールし、PCI パススルーで構成した後、インターフェイスの順序が正しくない問題を修正しました。**注記**：VMware で PCI パススルーを構成する場合は、仮想インターフェイスが eth0 であり、追加のインターフェイスが eth1、eth2 などであることを確認してください。
SWD-16577	スマートライセンスアカウントの登録時に基本認証が機能しない問題を修正しました。（LSQ-5449）
SWD-16603	Web UI へのログイン時に空白のウィンドウが表示される問題を修正しました。
SWD-16606	Manager でフロー検索が日本語で機能しない問題を修正しました。（LSQ-5106）
SWD-16618	バックスラッシュ（¥）文字を含む SMTP ユーザー名で電子メールのアクションを編集または作成しようとすると、応答管理が警告メッセージを表示する問題を修正しました。
SWD-16724	スマートライセンス予約（SLR）に関連する問題を修正しました。
SWD-16844	LDAP タイムアウトの問題を修正しました。（LSQ-5652）
SWD-17233	SMTP サーバーでの電子メールエラーメッセージの受信に関連する問題を修正しました。
SWD-17309	Flow Collector の再起動後にアクティブなユーザーセッションからフィールド（SGT、SGT ID、およびユーザー名）が欠落する問題を修正しました。

障害	説明
SWD-17379	UDP Director メモリアラームに関連する問題を修正しました。
SWD-17394	SecureX 統合に関連するドキュメントを更新しました。
SWD-17452	[選択された観測(Selected Observations)] ページの観測テーブルに不正確な結果が表示される問題を修正しました。
SWD-17526	データ漏洩アラームの詳細に関連するドキュメントを更新しました。
SWD-17599	macOS Monterey バージョン 12.2.1 および 12.3 でのデスクトップクライアントの機能が改善されました。**注記**:環境にデスクトップクライアントが含まれている場合は、最新バージョンをダウンロードしてください。
SWD-17612	アップデートマネージャの [すべてのデータノードを更新する(Update All Data Nodes)] ボタンを使用してソフトウェアアップデートをインストールするときに、インストールエラーのバナーが表示されない問題を修正しました。
SWD-17617	「*このグループのホストのベースライン化の有効化*」に関連するドキュメントを更新しました。
SWD-17628	ベースラインファイルのグループインデックスがホストグループの数と同じである場合、SIGABRT 問題が発生する問題を修正しました。
SWD-17648	MongoDB の Web UI トップレポートの保持設定を 24 時間から 48 時間に延長し、顧客が長時間実行されているレポートにアクセスするためにより多くの時間を提供します。
SWD-17653	引用符付きで作成されたウェルカムメッセージを編集または保存できない問題を修正しました。
SWD-17656	Flow Sensor パケットキャプチャページの読み込み中に発生していたエラーを修正しました。
SWD-17668	[インターフェイス(Interfaces)] の [上位のアプリケーショントラフィック(Top Application Traffic)] にデータが表示されない問題を修正しました。
SWD-17672	フローの検索結果にフローの負の TCP 再送信値が表示される問題を修正しました。
SWD-17675	Manager による高い CPU 使用率に関連する問題に対処しました。
SWD-17681	エクスポータで特定のアラームが表示されたときに、[モニター(Monitor)] > [インターフェイス(Interfaces)] を選択すると「5020 内部サーバーエラー」が表示される問題を修正しました。

障害	説明
SWD-17743	すべてのインターフェイス（eth0 および eth1）ですべてのテレメトリ（NVM を含む）を確実に処理するように Flow Collector エンジンを強化しました。
SWD-17745	VMware での UEFI モードの有効化が、ユーザーがアプライアンス セットアップ ツール（AST）にアクセスすることを妨げる問題を修正しました。
SWD-17756	IPFIX AVC フィールドのサポートが追加されました。
SWD-17788	AnyConnect バージョン 4.10.0407 以降によってエクスポートされるテンプレート 272 および 273 を確実に受け入れるように Flow Collector エンジンを強化しました。
SWD-17832	v7.4.1 の診断パックに system-stats フォルダがない問題を修正しました。
SWD-17872	SecureX リボンに関連するドキュメントを更新しました。
SWD-17874	Manager に保存されている TrustSec データが、Vertica データベーステーブルで許可されているストレージを超えていた問題を修正しました。
SWD-17888	オペレーティング システム カーネルが許可する任意の有効な MTU 範囲を許可する問題を修正しました。
SWD-17936	v7.4.1 へのアップグレード時に、Flow Sensor 4240 アプライアンスコンソールに [UNREG] または [未登録（Unregistered）] が表示される問題を修正しました。
SWD-17950	既知の問題のリリースドキュメントを更新しました。
SWD-17964	フローを照合するときに ECN ビットを無視するように Flow Sensor エンジンを変更しました。IP ヘッダーの ECN ビットが変更されたため、エンジンは同じフローからのパケットを別のフローに入れていました。
SWD-17966	設定可能なアプリケーションフィルタを導入したため、PACE2 アプリケーション ID が除外され、Flow Sensor から送信されません。
SWD-17972	Manager で構成の復元が失敗する問題を修正しました。
SWD-18019	特定の NBAR ID を Flow Collector に送信するように変更できるネットフロー ツールとスクリプトを追加しました。
SWD-18033	MongoDBRestore に関連する問題に対処しました。
SWD-18036	Flow Collector 4240 の nicspeed 属性が削除される問題を修正しました。

障害	説明
SWD-18136	ホストサマリ REST エンドポイントがアラームに対して不要なデータベースクエリを行う問題を修正しました。
SWD-18170	メールサーバー分類子が不正確な結果を提供していた問題に対処しました。
SWD-18237	Flow Collector エンジンがホスト SGT タグをフローに適用すると、新しいタグが適用されるまでのみ残るように問題を修正しました。
SWD-18264	Data Store のバックアップに関連するドキュメントを更新しました。
SWD-18297	新しい応答管理ルールを作成するときに、「413 ペイロードが大きすぎます」というエラーメッセージが表示される問題を修正しました。
SWD-18329	データノードの更新に関するドキュメントの内容が正確であることを確認しました。
SWD-18330	新しい inactive_purge_days 詳細設定に関連する問題を解決しました。
SWD-18343	SecureX Orbital クエリ統合の問題を修正しました。
SWD-18357	アップデートのインストール後に SMTP 設定がデフォルト設定に再初期化される問題を修正しました。
SWD-18404	大きな XML ファイルを処理する Flow Collector エンジンに関連する問題を修正しました。
SWD-18424	API が、マルチバイト文字コードではなくホストグループ名の誤った文字を表示する問題を修正しました。
SWD-18453	MTU 範囲が 2048 バイトより大きく設定されている場合に、Flow Collector エンジンがデコードエラーを表示する問題を修正しました。
SWD-18501	誤報の問題に関連する UDP Director の問題を修正しました。
SWD-18650	Cisco バンドルに関連する問題に対処しました。
SWD-18674	Manager が SNMP ポーリングの無効化を許可していなかったという翻訳の問題を修正しました。
SWD-18775	特に多数のジョブの処理に関連する問題に対処しました。

バージョン 7.4.1

障害	説明
SWD-16381	監査カテゴリにシステムレベルのタスクが表示されない問題を修正しました。（LSQ-5564）
SWD-16394	『Data Store Virtual Edition 展開概要ガイド v7.3.2』（LSQ-5592）のドキュメントの誤りを修正しました。
SWD-16406	ダッシュボードのアラームに間違った日付が表示される問題を修正しました。（LSQ-5440）
SWD-16487	Flow Collector の CPU 使用率が高くなるホスト分類子ドメインコントローラのクエリに関連する問題を修正しました。（LSQ-5614）
SWD-16501	SSO SAML リクエスト署名がサポートされていないことを示すためにドキュメントを更新しました。
SWD-16599	v7.3.1 へのアップグレード後にログインページが表示されない問題を修正しました。
SWD-16634	SSE コネクタがパブリック証明書を使用して svc-ctr-service と通信しない問題を修正しました。
SWD-16718	v7.1.1 から v7.2.1 へのアップグレード時に Tomcat ログファイルのアクセス許可が変わる問題を修正しました。
SWD-16755	Flow Collector インターフェイス数超過アラームが不必要に開始される問題を修正しました。
SWD-16764	VPN とチェックポイントを通過する ASA のテンプレートが UDPD と干渉する問題を修正しました。
SWD-16828	インターフェイスの上位レポートに誤った結果が表示される問題を修正しました。
SWD-16844	一貫性のないタイムアウトの問題に対処するために、LDAP 認証クエリメソッドのパフォーマンスを改善しました。
SWD-16856	Smart License Manager でエンドポイント（AnyConnect NVM）の使用量が 0 と表示される問題を修正しました。
SWD-16868	Flow Sensor が（eth0 や eth1 などの）同じサブネット上の管理およびデータインターフェイスをサポートしていなかった v7.3.2 の問題を修正しました。

障害	説明
SWD-16891	v7.2.1 にアップグレードした後、Flow Collector のデータベースが起動しなかった問題を修正しました。
SWD-16897	CTR 有効化メトリクスレポートに不正確な結果が示される問題を修正しました。
SWD-16902	ドメインの追加情報を提供するために、コグニティブ インストール ガイドを更新しました。
SWD-16929	pxGrid 2.0 で ISE セッションを受信するためのバッファサイズが不十分だった問題を修正しました。
SWD-17057	エンジンが無効な JSON 変数を含む flex_security_events ファイルを生成する問題を修正しました。
SWD-17097	ユーザーが ISO から v7.4.0 をインストールしてリブートしても、最初の AST 設定画面から先に進めない問題を修正しました。
SWD-17172	大規模な VM の 1G インターフェイスをサポートするように Flow Sensor Virtual Edition を拡張しました。
SWD-17178	GRUB がタイプ 0700 のディスクパーティションを認識しない v7.4.0 の問題を修正しました。
SWD-17252	ドキュメント v7.3.2 以降の ISE 統合ポートの情報を更新しました。
SWD-17265	レポート API（/tenants/{tenantId}/flows/queries）の予期しない http エラーコードに関連する問題を修正しました。
SWD-17311	Network Based Application Recognition（NBAR）機能と Secure Network Analytics をより完全に統合する方法を見直しました。
SWD-17361	Flow Collector 5K アプライアンスでホストおよびフローキャッシュが適切にスケーリングされるようにするために、エンジンのスケーリング上限の問題を修正しました。
SWD-17376	エンジンが原因でホストグループ設定の更新中に SWAAgent がメッセージサーバーをリセットし、ミューテックスロック状態になる問題を修正しました。
SWD-17409	サポートされていないメッセージをエンジンに送信すると、FC エージェント（fc-core）が正しく機能しない問題を修正しました。
SWD-17424	ROS コンテナの最大数を 1,024 から 2,048 に、またはアラームレバーを 700 から 1,700 に増やすことでアラームの問題を修正しました。

障害	説明
SWD-17439	現在のグループ数より大きいグループ ID がベースラインファイルから削除されるたびに発生する SIGABRT の問題を修正しました。
SWD-17450	エンジンのシャットダウンプロセスの非グレースフルシャットダウンで stop_smc_agent() 関数を呼び出す必要がある問題を修正しました。
SWD-17532	Flow Collector エクスポータ数超過インジケータの表示に関する問題を修正しました。
SWD-17551	log_backtrace 関数に関連する SIGABRT の問題を修正しました。
SWD-17574	Security Analytics and Logging（オンプレミス）のドキュメントに記載されている ASA ポート割り当ての内容を更新しました。

バージョン 7.4.0

障害	説明
SWD-15701	カスタム緩和スクリプトを無効にしようとすると発生する NullExceptionPointer の問題を修正しました。（LSQ-5159）
SWD-16053	ドキュメントからエンドポイント コンセントレータへの参照を削除しました。（LSQ-5930）
SWD-16075	スマートライセンスが強化されました。（LSQ-5431）
SWD-16087	フローベースのアイデンティティがユーザーレポートにない問題を修正しました。
SWD-16206	ASA フローのバイトカウントが 0 クライアントバイトを示し、NAT 送信元アドレスを表示することに関連する問題を修正しました。（LSQ-5320）
SWD-16217	ファイル /etc/udev/rules.d/70-persistent-net.rules が空であることに起因する v7.2.1 Flow Sensor コンソールでの segfault エラーの問題を修正しました。
SWD-16296	idgen から生成された ID が失われる問題を修正しました。
SWD-16314	v7.3.0 でエクスポータレベルでの sFlow のフロー検索が結果を返さない問題を修正しました。（LSQ-5508）
SWD-16340	「関連付けられたフロー」検索で IP アドレスまたはプロトコルがフィルタリングされない問題を修正しました。
SWD-16346	非アクティブなエクスポータのエンジンから誤ったステータスが返される問題を修正しました。

障害	説明
SWD-16366	次の内容をドキュメントに追加しました：デフォルトの Data Store の保持期間は 7 日ではありません。
SWD-16369	偵察アラームの再発生に関する syslog メッセージを更新しました。
SWD-16383	SAL CONNECTION_END_EVENT last_packet_second の計算に関する問題を修正しました。
SWD-16396	dpdk の使用時に、エクスポータの eth0 の MTU に関連するフローセンサーの問題を修正しました。
SWD-16401	カスタム緩和スクリプトを無効にしようとすると Manager NullExceptionPointer で発生する問題を修正しました。（LSQ-5159）
SWD-16413	クライアントポート 443 を使用したコグニティブレポートの TLS TCP（HTTPS）トラフィックに関連する問題を修正しました。
SWD-16416	セキュリティイベントの発生率が特に高いことに起因する、アーカイブ時間後に「スレッドが中断されました」というメッセージが表示される v7.3.1 Flow Collector エンジンの問題を修正しました。
SWD-16417	セキュリティイベントの発生率が特に高いことに起因する、host_flow_condition の v7.3.1 Flow Collector エンジン SIGSEGV の問題を修正しました。
SWD-16428	v7.3.0 および v7.3.1 の SNMP ポーリングが保留状態で停止し、何日も、場合によっては何週間も結果が返されない問題を修正しました。（LSQ-5521、LSQ-5496）
SWD-16432	Flow Sensor が誤った FlowSensorInitiator 要素を送信することがある問題を修正しました。
SWD-16441	ベースラインデータファイルがバックアップから除外されるように問題を修正しました。（LSQ-5617）
SWD-16453	すべての内部ホストグループのデフォルトポリシーと、[ホストがターゲットの場合（When Host Is Target）] 設定を無効にするとどうなるかを文書化しました。
SWD-16489	v7.3.1 のライセンスファイルがないと、[プロキシの取得（Proxy Ingest）] オプションがグレー表示される問題を修正しました。（LSQ-5624）
SWD-16503	Flow Collector データベースの Vertica Backup Restore（VBR）がサポートされていないことを明確にするようにドキュメントを更新しました。（LSQ-5636）
SWD-16576	order-by フローで CDS TopConversations のデフォルトのクエリが失敗する問題を修正しました。

障害	説明
SWD-16588	SecureX ユーザーロールが SecureX リボンにアクセスできない問題を修正しました。
SWD-16626	AVC サブアプリケーション値フィールドと 1 バイトの TCP フラグフィールドを処理する際のデコードエラーの問題を修正しました。
SWD-16629	各アラームタイプに関連する syslog 変数に関する詳細を含むようにドキュメントを更新しました。
SWD-16635	解決可能な ISE ノードの ISE 統合の前提条件を含むようにドキュメントを更新しました。
SWD-16647	Web UI のフロー検索の高度なパラメータの使用に関するドキュメントコンテンツを追加しました。
SWD-16669	Web フック URL が 200 文字に制限されることを示す情報を UI に追加しました。
SWD-16844	認証クエリ方法のパフォーマンスに関連する LDAP タイムアウトの問題を修正しました。（LSQ-5652）
SWD-16902	ドメインに関するより詳細なコンテンツを含めるように、Cognitive Analytics 構成ガイドを更新しました。

既知の問題

このセクションでは、このリリースに存在する可能性のあるバグ（欠陥）に関する情報を提供します。各欠陥には、対応する Cisco Defect and Enhancement Tracking System（CDETS）番号があります。CDETS リンクをクリックすると、問題の詳細が表示されます。

障害	CDETS	役職（Title）
SWD-17388	CSCwc17092	クラウド固有のテレメトリタイプは、Secure Network Analytics Alert Configuration ページに表示される
SWD-17425	CSCwc17091	1 つ以上のデータノードが追加された後、Vertica データベースがリバランスしない
SWD-17516	CSCwc17082	基礎となるジョブの不整合により、一部の監視はデフォルトで無効になっている
SWD-17635	CSCwc17079	より低い IP アドレスを持つ 2 つのデータノードがシャットダウンされると、[データベースコントロール（Database Control ）] タブでデータが失われる
SWD-18076	CSCwe51387	Vertica データベースのバックアップでは、バックアップの失敗後にスナップショットが削除されない
SWD-18184	CSCwe25791	SSH ウィンドウを閉じても、Data Store の秘密 SSH キーが削除されない
SWD-18304	CSCwe25801	非アクティブなエクスポータのクリーンアップ機能が機能していない
SWD-18466	CSCwe25789	SecureX が設定されている場合、Analytics ページで SecureX メニューが機能しない
SWD-18592	CSCwe25806	監視では、タイムアウトが原因で 14869 を超える監視を含む CSV をダウンロードできなかった
SWD-18642	CSCwe25792	Manager のバックアップで主要な Data Store ファイルが省略される
SWD-18667	CSCwd86030	脅威フィードを無効にした後に脅威フィードアラートを受信できる
SWD-18684	CSCwe25803	スマートライセンス：フェールオーバーロールを変更すると、CSSM との通信エラーが発生する
SWD-18686	CSCwe25799	スマートライセンス：CSSM との登録エラーと通信エラーがバックグラウンドジョブを引き起こす

障害	CDETS	役職（Title）
SWD-18694	CSCwe25800	分析、観測：デバイスレポートページの「bytes_in」の負の値
SWD-18714	CSCwe25794	SAL が有効になっていると保持管理が正しく機能しない（パーティションの問題）
SWD-18716	CSCwe25793	FIPS/CC モードの場合、データノードが UI からのファイルの閲覧をブロックできない
SWD-18730	CSCwe67091	証明書の期限切れアラームで、証明書の期限が切れていると誤って表示される
SWD-18765	CSCwe25798	アイデンティティ 証明書をアップロードすると、ホスト名の検証が原因でアプライアンス間の通信が切断される可能性がある
SWD-18776	CSCwe25795	Central Managementでは、同じ共通名を持つ証明書を信頼ストアに追加すると、構成チャネルダウンエラーが表示される
SWD-18803	CSCwe67090	7.3.x から 7.4.2 への Flow Sensor のアップグレードが GUI アップグレード方法で失敗する
SWD-18814	CSCwe25802	タイムアウトに達する前に Manager が 7.4.2 SWU の抽出に失敗する
SWD-18822	CSCwe25805	構成変更後に監査ログ「Generating Random EngineID config value」が表示される
SWD-18823	CSCwe25796	Data Store アプライアンスに内部障害がある場合、Central Management バックアップを復元できない
SWD-18826	CSCwe25790	デバイスレポート、監視ページで Analytics リクエストが 504 で失敗する
SWD-18835	CSCwe25788	Central Management の [設定の適用（Apply Settings）] ボタンが、変更されていないインターネットプロキシ構成で使用できるようになる
SWD-18863	CSCwe32908	Manager メニューヘッダーが UI に表示されない
SWD-18869	CSCwe49107	分析パフォーマンス 3 ノードハードウェア：高 FPS で約 10 分ごとに重大なアラームが発生する
SWD-19402	CSCwh17718	サービス、アプリケーションまたはホストグループを削除するか、脅威フィードを無効にすると、カスタム セキュリティ イベントが無効になり、アラームの欠落や誤報が発生する可能性があります。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 1 日	最初のバージョン。
1_1	2023 年 3 月 27 日	*[既知の問題（Known Issues）]* セクションが更新されました。
2_0	2023 年 5 月 26 日	*Analytics* および*エンドポイントライセンス*と *Network Visibility Module* の*機能強化*セクションを更新しました。
3_0	2023 年 10 月 12 日	「*期限が切れていないシスコの自己署名アプライアンス アイデンティティ証明書の置換（証明書の更新*」セクションが追加されました。 *[既知の問題（Known Issues）]* セクションが更新されました。
3_1	2023 年 10 月 20 日	VMware 8.0 のサポートが追加されました。
3_2	2024 年 1 月 22 日	形式が更新されました。

リリースサポート情報

リリース 7.4.2 の公式一般公開（GA）日は 2023 年 3 月 27 日 です。

一般的なソフトウェアのメンテナンスサポート、パッチ、一般的なメンテナンスリリースに関するサポートタイムライン情報、もしくは Cisco Secure Network Analytics ソフトウェア ライフサイクル サポートに関するその他の情報については、『Cisco Secure Network Analytics® Software Lifecycle Support Statement』[英語] を参照してください。

著作権情報