Cisco Secure Network Analytics

リリースノート 7.4.1

目次

はじめに

概要

このドキュメントでは、Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.1 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	Data Node
Cisco Stealthwatch データストア	Cisco Secure Network Analytics データストア	Data Store
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	フローセンサー
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、マネージャによって管理される 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。

> ⚠ コンプライアンスのお客様：v7.4.1 へのアップグレードを選択した場合、このバージョンにはコンプライアンス違反が含まれていることに注意してください。特に FIPS および CC モードの場合、Cisco Secure Network Analytics TLS クライアントは、FCS_TLSC_EXT.1.4 に違反して、Client Hello メッセージの Supported Groups Extension で非準拠曲線をアドバタイズします。
>
> 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。

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 v7.4.1 に更新するには、アプライアンスに v7.3.x または v7.4.0 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。
- **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。
- 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

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 2220	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
FC 5200 データベース	FC 5210 データベース

M4 ハードウェア	M5 ハードウェア
FS 1200	FS 1210
FS 2200	—
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210

証明書チェック

v7.4.1 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 で高可用性が設定されており、Secure Network Analytics を v7.4.0 以降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。

ブラウザ

- **互換性のあるブラウザ**：Secure Network Analytics は Chrome、Firefox、および Microsoft Edge の最新バージョン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 v7.4.1 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 v7.4.1 リリースの新機能と改善点は次のとおりです。

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。アプリケーションは、v7.4.1 への更新の一環として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。

既存のアプリケーションをアンインストールする必要はありません。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。レポートビルダー の既存のアプリは削除しないでください。『更新ガイド』の手順に従ってください。Secure Network Analytics を v7.4.1 に更新すると、以前のバージョンと同じ場所にあるレポートビルダーのダッシュボードにアクセスできます。

1. マネージャにログインします。
2. [ダッシュボード(Dashboards)] 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。

データ保持レポート

レポートビルダー からデータ保持レポートが削除され、[Data Store] タブで Data Store のデータを表示できます。詳細については、「**[Data Store] タブ**」を参照してください。

新しいレポート

Flow Collector(**収集トレンドレポート**)、もしくは Data Store または Flow Collector データベース(**データベース取り込みトレンドレポート**)が受信したテレメトリタイプを確認できるよう、レポートビルダーに新しいレポートを追加しました。次のテレメトリタイプのレポートが提供されます。

- NetFlow
- ネットワークの可視性とロギング(NVM)に関する セキュリティ分析とロギング(オンプレミス)
- ファイアウォールログ

マルチテレメトリの Secure Network Analytics の詳細については、「**マルチテレメトリサポート**」を参照してください。

収集トレンドレポート

評価するテレメトリタイプの収集トレンドレポートを実行します。

- すべての Flow Collector がフローを受信していますか。
- 受信したフローの量はどの程度ですか。
- 中断は発生しましたか。

このレポートは、次のようなトラブルシューティングとキャパシティプランに使用します。

- **初期展開**：新しい Flow Collector を展開するときに、想定される量のテレメトリが取り込まれていることを確認します。
- **トラブルシューティング**：Flow Collector がテレメトリを受信していることを確認したり、収集率を確認したり、テレメトリ取り込みの異常を見つけたりします。また、現在の収集レートを過去のレートと比較して、データのトレンドを特定します。
- **キャパシティプラン**：レポートの結果を確認して時系列でのテレメトリの取り込みトレンドを評価します。観測した増大トレンドを使用して今後の拡張を計画し、仕様に基づいて Flow Collector が過負荷にならないようにします。

名前	説明	Data Store ドメインが必要
ファイアウォールログ収集トレンドレポート	Flow Collector が受信した 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の収集トレンドを表示します。	yes
エクスポータ別フロー収集トレンドレポート	選択した Flow Collector およびエクスポータが受信したフローの収集トレンドを表示します。結果はエクスポータ別に表示されます。	
Flow Collector 別フロー収集トレンドレポート	Flow Collector が受信したフローの収集トレンドを表示します。	
NVM 収集トレンドレポート	Flow Collector が受信した Network Visibility Module（NVM）フローの収集トレンドを表示します。	yes

Data Store ドメインの詳細については、「**Data Store ドメインとしてのドメインの設定**」を参照してください。

データベース取り込みトレンドレポート

評価するテレメトリタイプのデータベース取り込みトレンドレポートを実行します。

Data Store（Data Store ドメインが必要）

- Data Store はフローを受信していますか。
- 受信したフローの量はどの程度ですか。
- 中断は発生しましたか。

Flow Collector データベース（非 Data Store ドメインが必要）

- Flow Collector データベースはフローを受信していますか。
- 受信したフローの量はどの程度ですか。
- 中断は発生しましたか。

このレポートは、次のようなトラブルシューティングとキャパシティプランに使用します。

- **初期展開**：新しい Data Store または Flow Collector データベースを展開するときに、このレポートを実行して予想される量のテレメトリが取り込まれていることを確認します。
- **トラブルシューティング**：Data Store または Flow Collector データベースがフローを受信していることを確認したり、テレメトリ取り込みの異常を見つけたりします。また、現在の収集レートを過去のレートと比較して、データのトレンドを特定します。
- **キャパシティプラン**：レポートの結果を確認して時系列でのテレメトリの取り込みトレンドを評価します。観測した増大トレンドを使用して今後の拡張を計画し、仕様に基づいて Data Store または Flow Collector データベースが過負荷にならないようにします。

名前	説明	Data Store ドメインが必要
ファイアウォール ログ データベース取り込みトレンドレポート	Data Store に書き込まれた セキュリティ分析とロギング（オンプレミス）ファイアウォールレコードを表示します。	yes
フローデータベース取り込みトレンドレポート	Flow Collector のデータベースまたは Data Store に書き込まれたフローレコードを表示します。	
NVM データベース取り込みトレンドレポート	Data Store に書き込まれた Network Visibility Module（NVM）レコードを表示します。	yes

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。 （[ユーザ（User）]）アイコン を選択して [監査ログの宛先（Audit Log Destination）]検索します。v7.4.1 では、リモート syslog サーバーのサーバー名か IPv4 アドレスを使用して監査ログの宛先を設定できます。
- **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。 （[ユーザ（User）]）アイコン を選択して「SMTP 構成」を検索します。

サーバー ID 検証：更新の準備（7.3.x ～ 7.4.1 のみ）

7.3.x から 7.4.1 への更新の一環として、次の設定を見直してサーバーの ID 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）（Audit Log Destination（Syslog over TLS））]
- 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。［グローバル設定（Global Settings）］アイコン > ［集中管理（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**
- マネージャの信頼ストアに SMTP サーバー ID 証明書を追加します。

マネージャ信頼ストアにアクセスするには、Manager にログインします。［グローバル設定（Global Settings）］アイコン > ［集中管理（Central Management）］を選択します。マネージャの ••• （［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（Apps）

Secure Network Analytics 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

Analytics

v7.4.1 では、アラートダッシュボードでアラートをクリックして、その詳細とサポートする観察を表示できます。また、フロー分析とデバイスレポートにピボットすることも可能です。

詳細については、『Secure Network Analytics Analytics Beta Guide』を参照してください。

単一の Flow Collector イメージに対する NetFlow および sFlow Support

netFlow と sFlow に単一の Flow Collector イメージを設定できるようになりました。これにより、モードを NetFlow から sFlow に、または sFlow から NetFlow に切り替えることができます。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。

Data Store でのデータ圧縮

新たにインストールする v7.4.1 システムでは、Flow Collector と Data Store 間の帯域幅使用量を削減するためのデータ圧縮がデフォルトで有効になっています。これは、Flow Collector から Data Store へのネットワーク帯域幅が制限されているシナリオで特に便利です。データ圧縮によって帯域幅使用量を最大 90% 削減できます。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。

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）、Virtual Edition（小規模、中規模、または大規模）
マネージャ	Yes	• マネージャ 2200、Virtual Edition（小規模、中規模、および大規模） • マネージャ 2210 またはマネージャ Virtual Edition（v7.4 以降）Virtual Edition には、小規模、中規模、大規模の 3 つのモデルが用意されています。
Flow Collector	Yes	• Flow Collector 4200 番台、5200 番台、Virtual Edition（小規模、中規模、および大規模） • Flow Collector 4210 番台または Flow Collector Virtual Edition（v7.4 以降）* • Flow Collector 5210 番台または Flow Collector Virtual Edition（v7.4 以降）* * Virtual Edition には、小規模、中規模、大規模の 3 つのモデルが用意されています。
フローセンサー	×	• v7.3 以降のすべてのモデル
UDP Director	×	• v7.3 以降のすべてのモデル
エンドポイントコンセントレータ	未サポート	Endpoint Concentrator と Data Store の併用はサポートされていません。

Data Node の混在はサポートされていません。Data Node は、すべて仮想にするか、あるいはすべてハードウェアにする必要があります。

単一ノード Data Store のサポート

v7.4.1 では、特定の条件下で単一ノード Data Store がサポートされます。詳細については、Cisco Secure Network Analytics の設置ガイドとコンフィギュレーション ガイドを参照してください。

一般的な要件

- 最大 4 つの Flow Collector がサポートされます。
- 単一ノード Data Store システムをマルチノードシステムに拡張するオプションが用意されています。

Analytics の要件

- Analytics を実行するには、Manager に少なくとも 6 基の CPU と 40 GB の RAM が必要です。
- システムに必要なリソースを確保してください。
- 中規模の Data Store プロファイルの場合、Data Node で Analytics を正常に実行するには、少なくとも 64 GB の RAM が必要です。

> 単一ノード展開内で Analytics を有効にしている場合、内部 IP スキャナとワーム伝達ジョブは信頼できない可能性があります。

Data Store の機能拡張

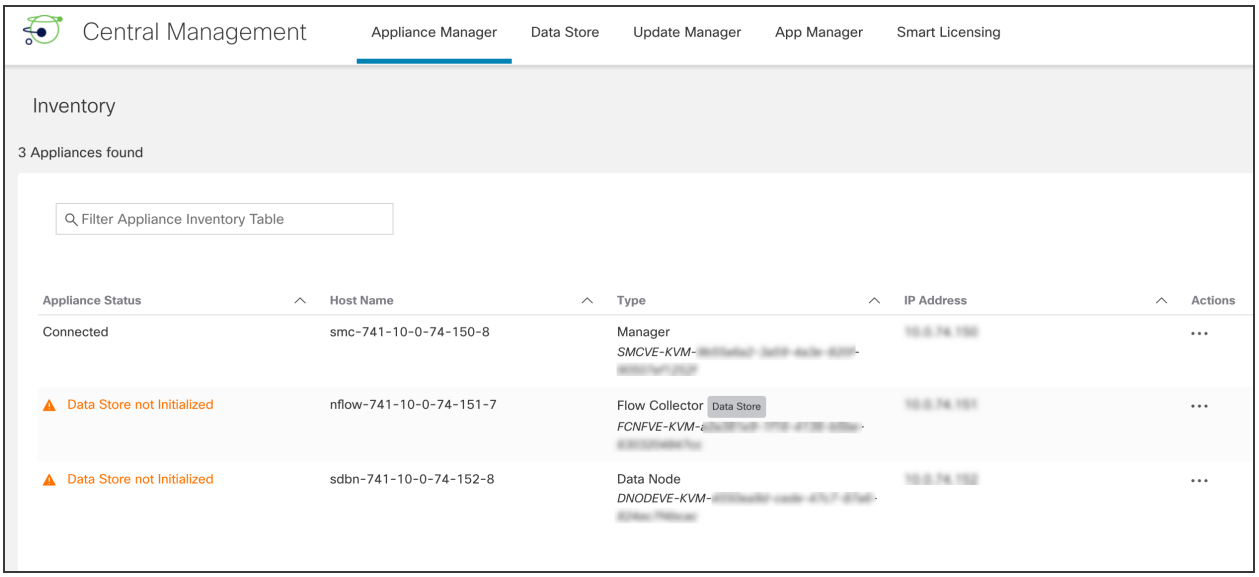
v7.4.1 には、次の Data Store の機能拡張が含まれています。詳細については、Cisco Secure Network Analytics アプライアンスの設置ガイド（ハードウェアまたは Virtual Edition）とシステム コンフィギュレーション ガイドを参照してください。

新しいアプライアンスのエラー状態

次の新しいアプライアンスのエラー状態が追加されました。

Data Storeが初期化されていません（Data Store Not Initialized）

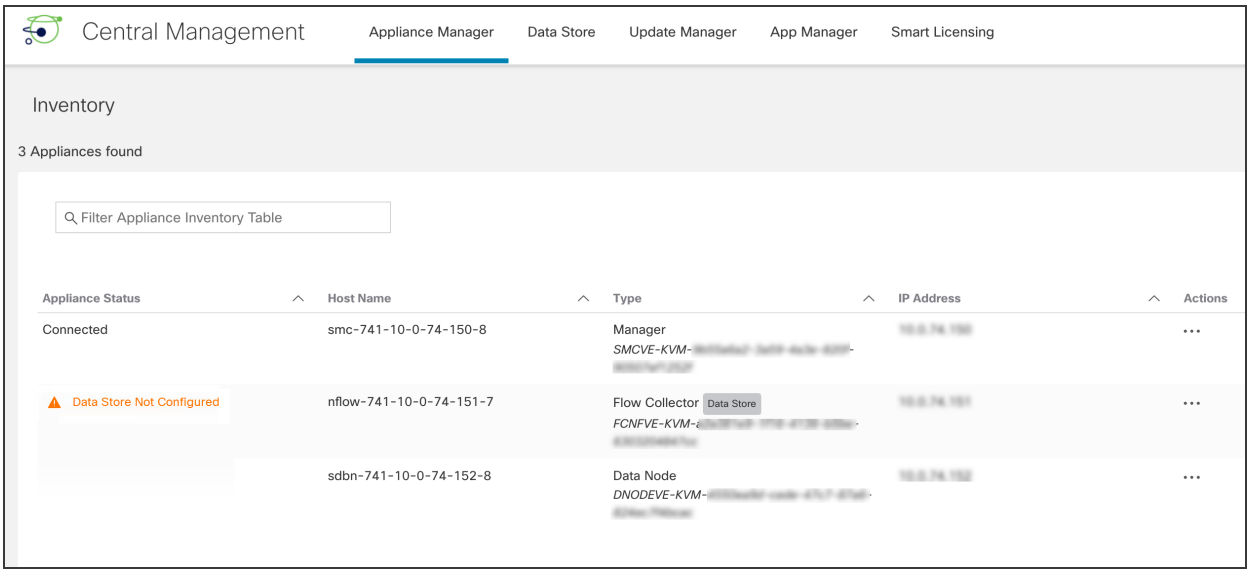
Data Store が初期化されていない場合、[Central Management Appliance Manager] タブの [アプライアンスステータス（Appliance Status）] 列に「Data Storeが初期化されていません（Data Store not Initialized）」というメッセージが表示されます。このエラーが表示された場合は、すべての Manager、Flow Collector、および Data Node を Central Management のインベントリに追加した後に Data Store を初期化する必要があります。順序が重要であることに注意してください。『システム コンフィギュレーション ガイド』の手順に従います。



Data Storeが設定されていません（Data Store Not Configured）

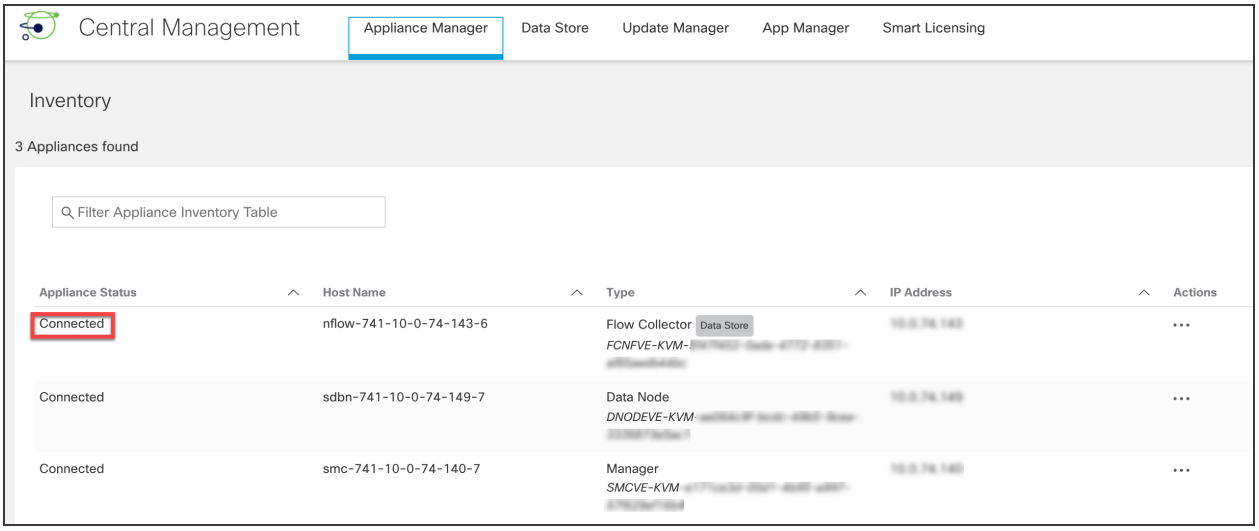
Data Store が設定されていない場合、[Central Management Appliance Manager] タブの [アプライアンスステータス（Appliance Status）] 列に「Data Storeが設定されていません（Data Store not Configured）」というメッセージが表示されます。このエラーが表示された場合は、すべての

Manager、Flow Collector、および Data Node を Central Management のインベントリに追加した後に、Data Store とのセキュア通信が確立されるように新しいアプライアンスを設定する必要があります。順序が重要であることに注意してください。『システム コンフィギュレーション ガイド』の手順に従います。



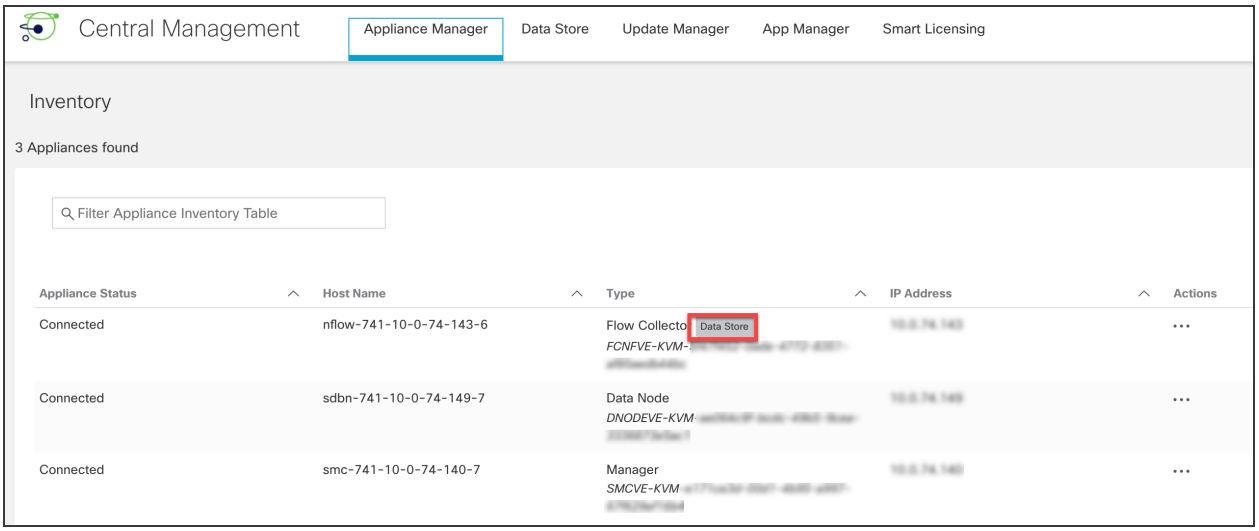
Central Manager アプライアンスの状態：[アップ（Up）] から [接続済み（Connected）]

[Central Management Appliance Manager] タブの [アプライアンスステータス（Appliance Status）] 列には [接続済み（Connected）] というアプライアンスステータスが表示されますが、このステータスは以前 [アップ（Up）] となっていました。



「Data Store」タグで識別される Data Store Flow Collector

Flow Collector に Data Store タグがある場合、フローを Data Store に送信するように設定されています。Data Store ドメインの詳細については、「**Data Store ドメインとしてのドメインの設定**」を参照してください。



[Data Store] タブ

Central Management に [Data Store] タブという新しいタブが追加されました。このタブには、次のサブタブがあります。

- **[データベースコントロール（Database Control）] タブ**
- **[データベースの保持（Database Retention）] タブ**
- **[データベース更新ステータス（Database Update Status）] タブ**

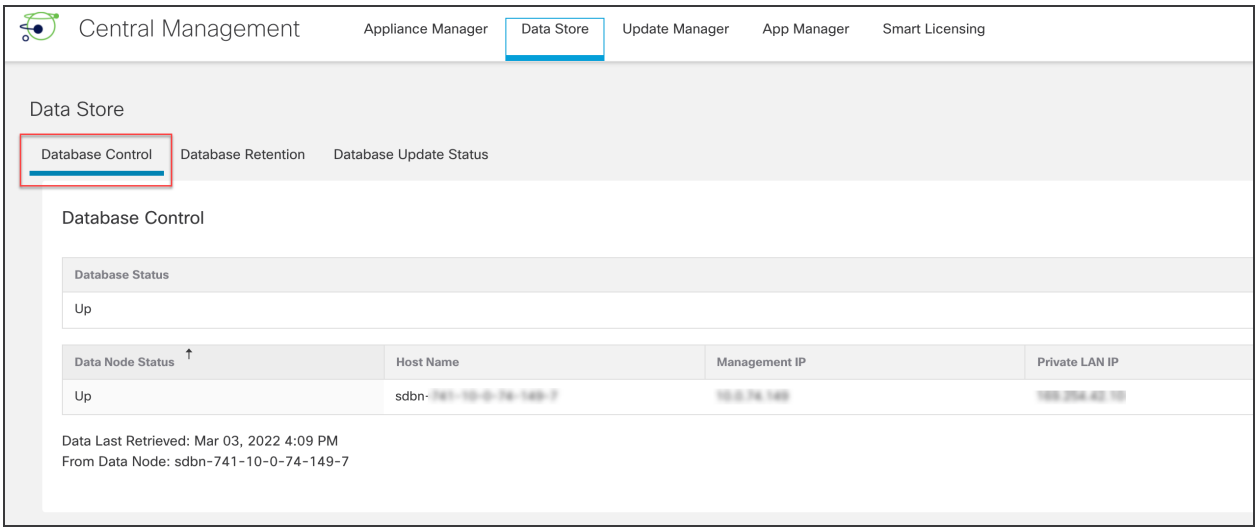
これらの Data Store のサブタブでは、次のようなことが行えます。

- データベースまたは任意の Data Node のステータスを表示する
- データベースの現在のストレージ使用量に関する統計を表示する
- 更新中の Data Node すべてのステータスを表示する
- データベースまたは任意の Data Node の起動または停止
- フロー インターフェイス データの保持ステータスを変更する

[データベースコントロール（Database Control）] タブ

[データベースコントロール（Database Control）] タブを使用して、データベースと各 Data Node のステータスを監視できます。データベースのステータスが [アップ（Up）] でも、各 Data Node のステータスが [ダウン（Down）] か [回復中（Recovering）] になっている場合があります。

> データベース（または Data Node）を起動または停止するときは、必ず [アクション（Actions）] メニューを使用してください。



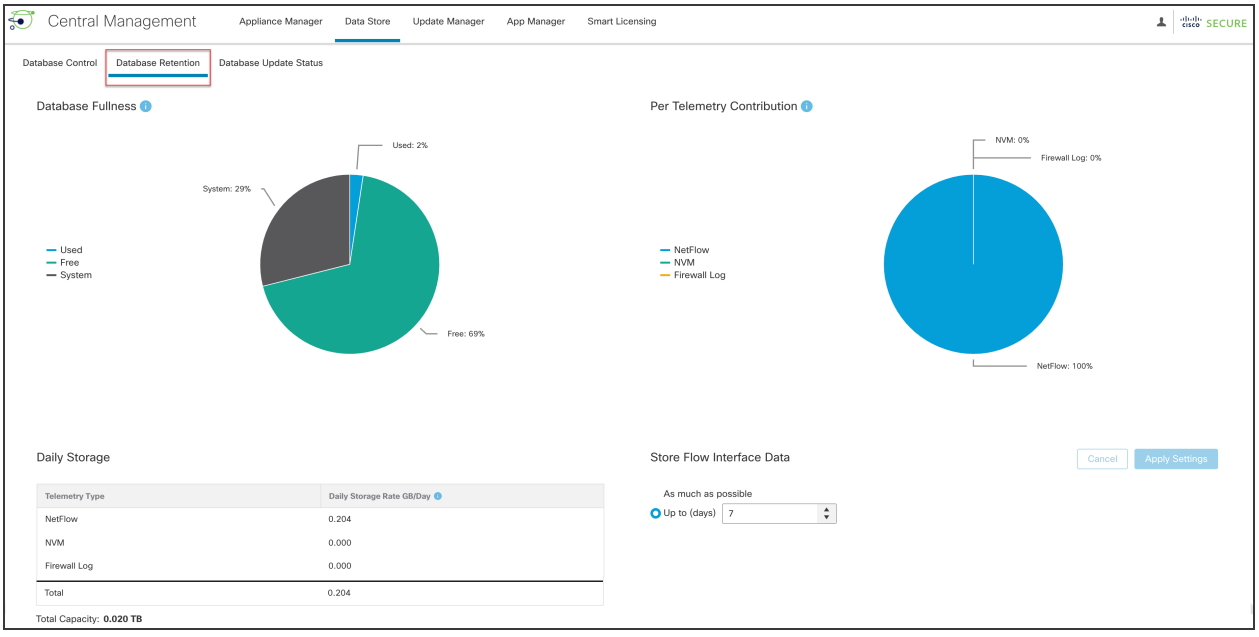
[データベースの保持(Database Retention)]タブ

[データベースの保持(Database Retention)]タブを使用して、以下を確認します。

- データベースの充満度(使用済みの領域と空き領域)
- テレメトリタイプ別の保存量
- 前日にデータベースに追加されたデータの増分量

(毎晩計算される)前日のデータベースのストレージステータスを示します。

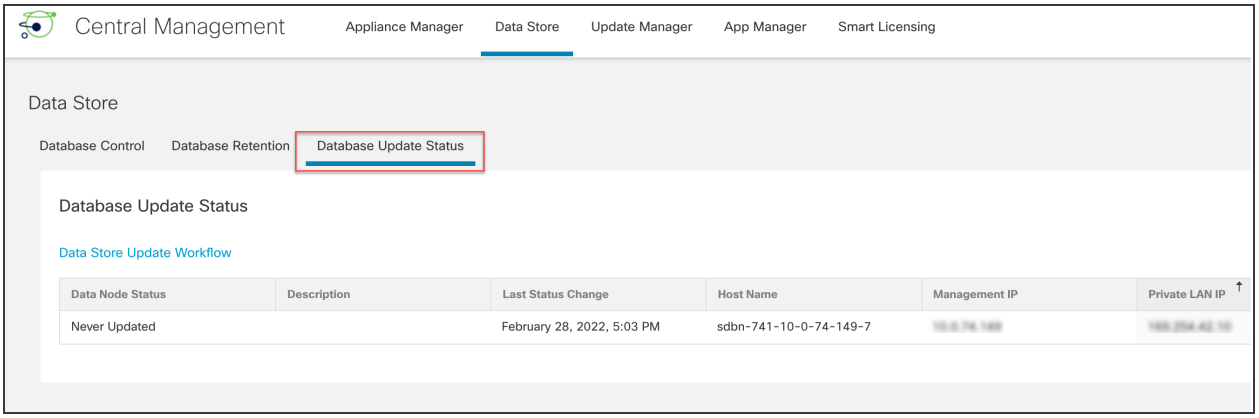
> 前日のデータベースのストレージステータスのみが表示されます。データベースのストレージステータスは毎晩評価されます。1 日を通して更新されるわけではありません。



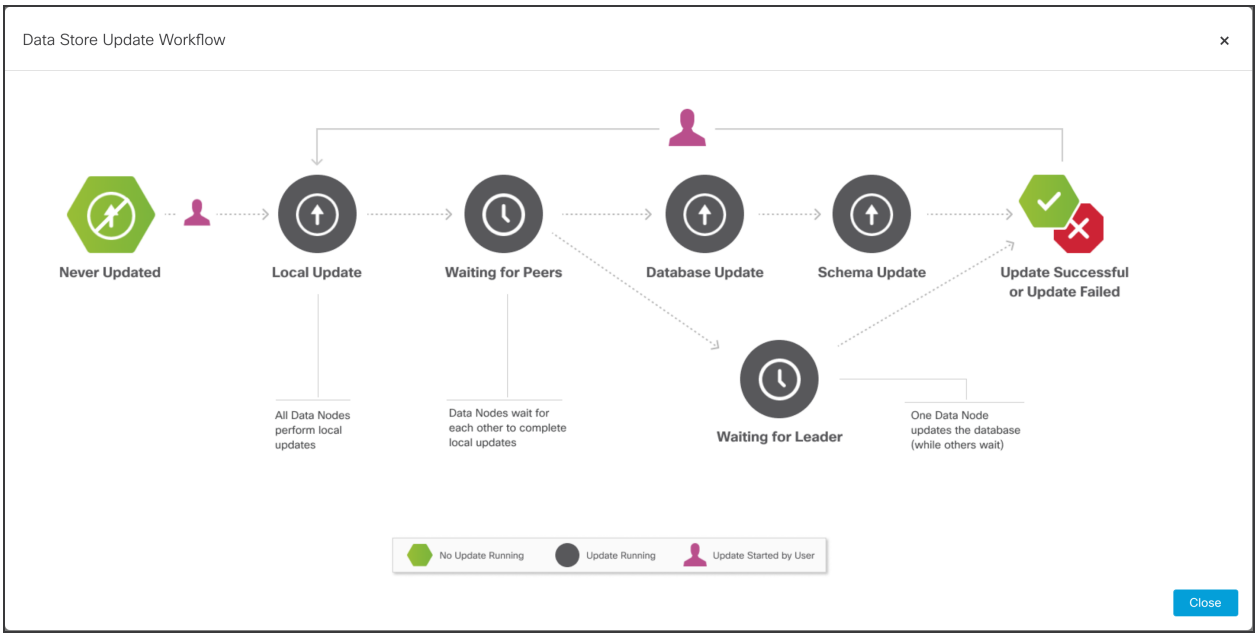
[データベース更新ステータス(Database Update Status)]タブ

[データベース更新ステータス(Database Update Status)]タブには、Data Node の現在の更新ステータスが表示されます。Update Manager でソフトウェア更新(アップグレードまたはパッチ適用)を開始したら、このタブで各 Data Node のステータスを監視して更新が完了したことを確認します。更新のワークフローを視覚的に表示するには、[図の表示(View Diagram)]をクリックします。

更新が完了したら、**[データベースコントロール(Database Control)]タブ**に移動して、データベースのステータスが[接続済み(Connected)]になっていることを確認します。詳細については、『更新ガイド』を参照してください。



次の図に Data Store の更新のワークフローを示します。



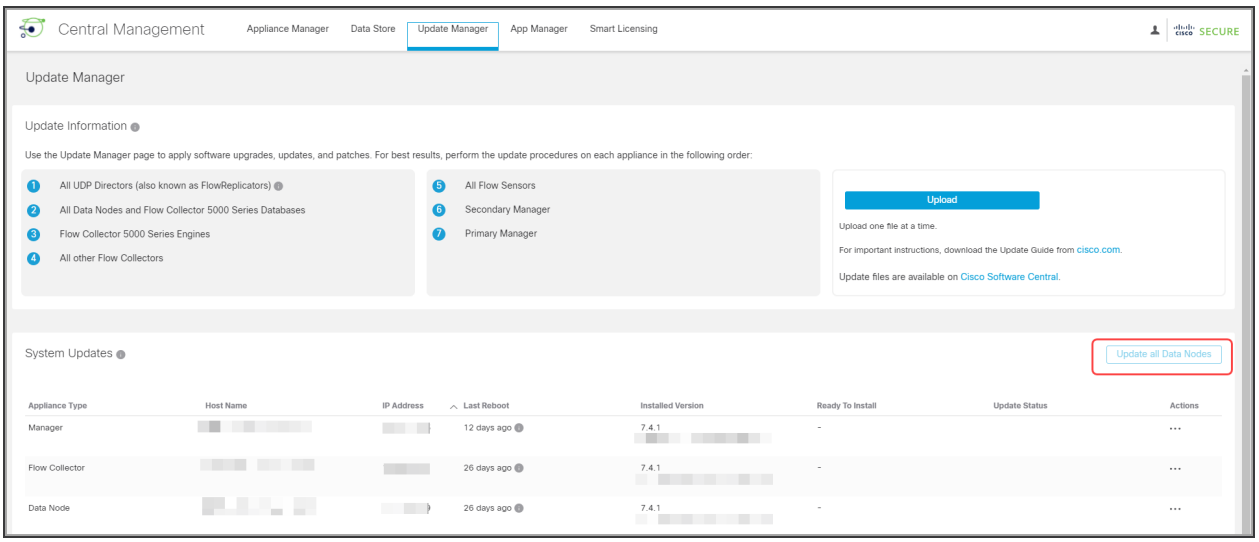
[すべてのData Nodeを更新する(Update All Data Nodes)]ボタン

複数の Data Node を同時に更新できるように、[Central Management] > [Update Manager] に[すべてのData Nodeを更新する(Update all Data Nodes)]ボタンを追加しました。

- **ステータス**:Update Manager には全体的な更新ステータスが表示され、更新が完了すると新しくインストールされたバージョンが表示されます。アプライアンスは更新プロセス中に再起動するため、アプライアンスがオフラインになると、ステータス情報の更新が遅れる場合があ

ります。各 Data Node のデータベースサービス更新の進行状況を監視するには、[Data Store] > **[データベース更新ステータス(Database Update Status)] タブ**に移動します。また、各ページを更新して最新のステータスを確認します。

- **手順**:正常に更新するには、『Cisco Secure Network Analytics システム更新ガイド』または パッチの Readme ファイルに記載された更新順序と手順に従ってください。
- **ベストプラクティス**:各 Data Node を個別に更新できますが、[すべてのData Nodeを更新する(Update all Data Nodes)] ボタンを使用して複数の Data Node を同時に更新することをお勧めします。



ドキュメント

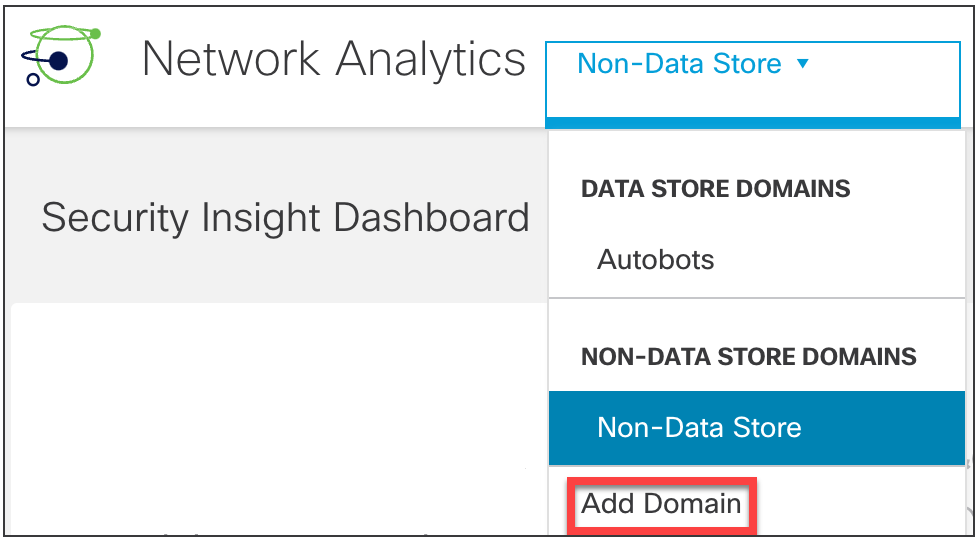
v7.4.1 でドキュメントを再構成しました。新しい v7.4.1 の展開については、https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-installation-guides-list.html にある次のガイドの手順に従ってください。

1. x2xx シリーズ ハードウェア アプライアンス設置ガイド v7.4.1 または Virtual Edition アプライアンス設置ガイド v7.4.1
2. システム コンフィギュレーション ガイド v7.4.1

Data Store ドメインとしてのドメインの設定

Secure Network Analytics のホームページから Data Store ドメインを追加して、Data Store システムに移行できるようになりました。『システム コンフィギュレーション ガイド』の手順に従います。

- **非 Data Store ドメイン**:Data Store が展開されていないドメイン。フローは Flow Collector データベースに保存されます(5000 シリーズのみ)。
- **Data Store ドメイン**:Data Store が展開されているドメイン。フローは Data Node に保存されます。



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。

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。

マルチテレメトリサポート

Data Store を展開している場合は、次のテレメトリタイプを同時に取り込むように Flow Collector を設定できます。

- NetFlow
- Network Visibility Module（NVM）
- Cisco Security Analytics and Logging（オンプレミス）のファイアウォールログ

マルチテレメトリは、次を使用して構成できます。

- 初回セットアップ（First Time Setup）
- Flow Collector 詳細設定（Advanced Settings）。[詳細設定（Advanced Settings）] にアクセスするには、Flow Collector（以前のアプライアンス管理（管理者）インターフェイス）にログインし、[サポート（Support）] > [詳細設定（Advanced Settings）] を選択します。

- マルチテレメトリを設定するときは、テレメトリポートが一意になるようにしてください。テレメトリポートを重複して設定すると、フローデータの消失を回避するためにポートが内部のデフォルト値にリセットされます。
- NetFlow を無効にするように Flow Collector を設定した場合、エクスポータ、ホストグループ、セキュリティイベント、ホストレポートの変更などの設定オプションを更新しても効果はありません。

設定に関するその他のドキュメント

設定の詳細については、以下を参照してください。

- **初回セットアップ時のマルチテレメトリ**：『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。
- **Flow Collector の [詳細設定（Advanced Settings）] を使用したマルチテレメトリ**：ヘルプの手順に従ってください。（[ユーザ（User）]）アイコン を選択して [詳細設定（Advanced Settings）] を検索します。
- **Network Visibility Module（NVM）**：『エンドポイントライセンスおよび Network Visibility Module（NVM）設定ガイド v7.4.1』を参照してください。
- **セキュリティ分析とロギング（オンプレミス）**：『Security Analytics and Logging（オンプレミス）v3.1：ファイアウォールイベント統合ガイド』を参照してください。

Cisco Security Analytics and Logging（オンプレミス）機能拡張

セキュリティ分析とロギング（オンプレミス）の以前のバージョンをアンインストールしないでください。アンインストールすると、既存のデータが削除されます。

システムを v7.4.1 に更新した後、アプリケーションマネージャを使用して セキュリティ分析とロギング（オンプレミス）v3.1.0 にアップグレードしてください。アプリケーションの以前のバージョンは、v7.4.1

と互換性がないため、アップグレードしないと セキュリティ分析とロギング（オンプレミス） にアクセスできません。

セキュリティ分析とロギング（オンプレミス） 機能拡張には次のようなものがあります。

- **ブランディング**：展開オプションは、単一ノードとマルチノードではなく、Manager のみと Data Store になりました。この更新は、Secure Network Analytics の類似した用語による混乱を避けることを目的としています。
- **複数の Flow Collector**：Secure Firewall Management Center（旧 Firepower Management Center）v7.2 は、最大 5 個の Flow Collector をサポートします。
- **Data Store 展開の機能拡張**：
  - Data Store 展開では、1 つの Data Node がサポートされます。要件の詳細については、「単一ノード展開」セクションを参照してください。
  - Data Store 展開では、ファイアウォールログ、NetFlow、および NVM フローを同時に取り込むことができます。詳細については、「マルチテレメトリ」セクションを参照してください。

セキュリティ分析とロギング（オンプレミス） 展開の詳細については、次のドキュメントを参照してください。

- Security Analytics and Logging（オンプレミス）リリースノート v3.1.0
- Cisco Security Analytics and Logging（オンプレミス）スタートアップガイド
- Security Analytics and Logging（オンプレミス）v3.1.0：ファイアウォールイベント統合ガイド

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。
- シスコサポートにご連絡ください。
  - 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：www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

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 7.4.1

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。

障害	説明
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。
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。

障害	説明
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。
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）

障害	説明
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。
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)

障害	説明
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。
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既知の問題（バグ）について概要を示します。可能な場合には、回避策も示しています。参照用に問題番号が示されています。

障害	説明	回避策
LVA-719	Active Directory ルックアップ設定パスワードは、設定ファイルにクリアテキストで保存されます。	**詳細**：パスワードは、ローカルファイルシステム、アプライアンス管理インターフェイスのファイルブラウザ（管理者の資格情報が必要）、および暗号化されていないバックアップ設定ファイルでアクセスできます。 **緩和オプション**：Active Directory ルックアップを設定する場合： • ユーザーアカウントの権限を制限し、アカウントの誤用を監視します。 • バックアップ設定ファイルを暗号化します。ヘルプの「バックアップ設定の暗号化」を参照してください。 Active Directory ルックアップを無効にする場合： • Active Directory ルックアップ設定を削除します。Manager で [展開（Deploy）] > [Active Directory] に移動します。 • 暗号化されていないバックアップ設定ファイルを削除します。ヘルプの「バックアップ設定の暗号化」および「バックアップ設定ファイル」を参照してください。
SWAPP-477	v7.4.0 か v7.4.1 のいずれかに Host Classifier v3.1.0 をインストールしており、システムに複数の Data Store ドメインと非 Data Store ドメインの組み合わせが含まれている場合、5 分ごとに実行されるドメインモニターが 1 分間隔でループし、大量のログが生成されます。その結果、Manager のディスク使用量が増加します。	Host Classifier v3.1.1 がリリースされたらインストールします。

障害	説明	回避策
SWD-12574	ユーザーがログイン試行に失敗せずにコマンドライン インターフェイスにログインすると、エポック日付（1970 年 1 月 1 日）が表示される場合があります。	現在使用可能なものはありません。
SWD-17388	[優先順位の設定（Configure Priorities）] ページの [テレメトリ（Telemetry）] ドロップダウンリストに表示される、現在 Cisco Secure Network Analytics がサポートしているテレメトリソースは **NetFlow** だけです。その他のソースタイプはどれもサポートされていません。	現在使用可能なものはありません。
SWD-17425	既存の Vertica データベースに 1 つ以上の Data Node を追加しても、新しい Data Node を利用するためのデータの再調整は自動的に行われません。	次の手順を実行して手動で再調整を開始します。 1. SSH 経由でルートシェルかコンソール（SSH なし）を使用して、既存の稼働している Data Node に接続します。 2.**su dbadmin** と入力します。 3. makecall ディレクトリで、次のコマンドを実行します。 `/opt/vertica/bin/admintools -t rebalance_data -d sw -p -k 1<dbadmin password>`

障害	説明	回避策
SWD-17452	最初に [観測タイプ (Observation Types)] ページを開いて、データがない (0 の) 観測タイプの横にある (**右矢印**) アイコンをクリックすると、開いている [選択した観測 (Selected Observations)] ページに関連するデータが表示されませんが、これは正しい動作です。 他の観測で 1 つ以上の検索を実行してから、最初に結果が表示されなかった観測を再度検索すると、表の右下隅の結果に [0-0/0 件の結果] と正しく表示されていたとしても、現時点では [時間 (Time)] 列と [デバイス (Device)] 列に不正確にデータが表示されます。	現在使用可能なものはありません。
SWD-17516	Analytics の観測ジョブである InternalIPScanner と WormPropagation が正しく実行されていません。	現在使用可能なものはありません。

障害	説明	回避策
SWD-17612	([アクション(Action)]メニューの ••• ([省略記号(Ellipsis)])アイコン をクリックして)各 Data Node に更新をインストールするときに、データベースのステータスが [アップ(Up)] の場合は失敗バナーが表示されます。 ただし、[すべてのData Nodeを更新する(Update all Data Nodes)] ボタンを使用すると、エラーは発生しますがバナーは表示されません(何も表示されずに失敗します)。	現在使用可能なものはありません。
SWD-17635	より IP が低い 2 つの Data Node 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)] タブのデータが消えます。	現在使用可能なものはありません。
SWD-17644	フェールオーバーによって v7.4.0 から v7.4.1 にアップグレードすると、フェールオーバーがアクティブ化されて、「Data Store が初期化されていません(Data Store Not Initialized)」というエラーが発生します。	必ずセットアップを完了してシステムプロンプトに従います。

障害	説明	回避策
SWD-17668	Network Analytics の[上位アプリケーショントラフィック(Top Application Traffic)]エリアに「表示するデータがありません(No data to display)」というメッセージが表示されます。	現在使用可能なものはありません。
SWD-17676	v7.3.x からのアップグレード時に、(特に Flow Sensor を最後に更新することを選択した場合)Flow Sensor のアプライアンスステータスに[設定の変更を保留中(Config Changes Pending)]と表示されることがあります。	アップグレードプロセスを続行します。プライマリ Manager が更新されると問題は解決します。
SWD-17936 CSCwc25672	Flow Sensor 4240 を v7.4.1 にアップグレードすると、404 エラーが表示され、UNREG または Unregistered がアプライアンスコンソールに表示されます。	**最初にこれを実行**:Flow Sensor の最新の SWU ファイルがあることを確認します。詳細については、『v7.4.1 Update Guide』の「SWU Files」セクションを参照してください。 アプライアンスにアクセスするには、次のように 40 GB の要件を削除します。 1. SSH またはコンソール(SSH なし)経由で root シェルを使用します。 2. makecall ディレクトリで、次のコマンドを実行します。 `sed -i 's/platform="ST-FS4240-K9" nicspeed="eth+,40000"/platform="ST-FS4240-K9"/' /lancope/admin/lib/model.xml` 3. アプライアンスを再起動します。

障害	説明	回避策
[該当なし（N/A）]	単一ノード展開内で Analytics を有効にしている場合、未公開のアラートは不正確に動作します。未公開のアラートとは、Secure Network Analytics がまだ実験段階にあると見なされているために、正式に公開されていないアラートです。デフォルトでは [オフ（Off）] になっています。未公開のアラートは以下のとおりです。 • NetBIOS 接続のスパイク • 新しい IP スキャナ • 新しい SNMP スイープ • アウトバウンド SMB スパイク • SMB 接続のスパイク • 疑わしいリモートアクセスツールのハートビート • Worm Propagation	現在使用可能なものはありません。
NA	Flow Sensor Virtual Edition では、[アプリケーション識別情報のエクスポート（Export Application Identification）] インジケータはデフォルトでオフになっています。	アプリケーション識別を有効にするには、詳細設定を手動で選択する必要があります。

ログの変更

リビジョン	改訂日	説明
1_0	2022 年 4 月 18 日	最初のバージョン
1_1	2022 年 5 月 9 日	一般提供（GA）。
1_2	2022 年 7 月 1 日	「**マルチテレメトリサポート**」セクションを更新し、「**既知の問題**」セクションに SWD-17936 を追加しました。
1_3	2022 年 7 月 15 日	「**既知の問題**」セクションの SWD-17936 の回避策を更新しました。
1_4	2022 年 8 月 5 日	「**更新する前に**」セクションにコンプライアンスのお客様向けの注記を追加しました。

リリースサポート情報

リリース 7.4.1 の公式一般公開（GA）日は 2022 年 5 月 9 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 Stealthwatch リリース サポート ライフサイクルに関するその他の情報については、Cisco Stealthwatch® ソフトウェアリリースモデルおよびリリース サポート タイムライン製品速報を参照してください。

著作権情報