Cisco Stealthwatch

7.3.2 リリースノート

目次

はじめに

概要

このドキュメントでは、Stealthwatch v7.3.2 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。Stealthwatch の詳細については、Cisco.com をご覧ください。

用語

このガイドでは、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべての Stealthwatch 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、StealthWatch Management Console（SMC）で管理される Stealthwatch 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、『Stealthwatch 更新ガイド（v7.2.1 および 7.3.x から v7.3.2）』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 7.3.2 に更新するには、アプライアンスにバージョン 7.2.1、7.3.0、または 7.3.1 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）] > [Stealthwatch] の順に選択します。
- **アプライアンスのソフトウェア バージョンは段階的に更新してください。**たとえば、Stealthwatch v7.0.x を使用している場合は、各アプライアンスを v7.0.x から v7.1.x に更新してから、v7.1.x を v7.2.x 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**：Stealthwatch には TLS v1.2 が必要です。

> セキュリティを強化するために、**IDentity 1000/1100** アプライアンスを v3.3.0.x に更新して、TLS 1.2 対応の新しい openSSL バージョンを利用することをお勧めします。

サードパーティ製アプリケーション

Stealthwatch 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。

ハードウェア

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。

> ⚠ Dell PowerEdge ハードウェアおよび Flow Collector 5020 は、Stealthwatch v 7.3 ではサポートされていません。ハードウェアの更新については、stealthwatch_renewals@cisco.com で Stealthwatch 更新チームにお問い合わせください。

ブラウザ

- **互換性のあるブラウザ**：Stealthwatch 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 Stealthwatch 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 v7.3』を参照して証明書を置き換えてください。

代替アクセス

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、Stealthwatch 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。

> ⚠ 今後サービスが必要になった場合に備えて、ハードウェアまたは仮想マシンに対して次のいずれかの方法を使用して Stealthwatch アプライアンスにアクセスする別の方法を有効にしておくことは重要です。

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）**：ラップトップや、キーボードとモニタを使用してアプライアンスに接続する方法については、最新の『Stealthwatch Hardware Installation Guide』を参照してください（https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-installation-guides-list.html）。
- **CIMC（UCS アプライアンス）**：https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/b_Cisco_CIMC_CLI_Configuration_Guide/Cisco_CIMC_CLI_Configuration_Guide_chapter1.html で、お使いのプラットフォーム向けの最新の Cisco UCS ガイドを参照してください。

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）：アプライアンスのインストールについては、最新の KVM または VMware のマニュアルを参照してください。
    - たとえば **KVM** については仮想マネージャのマニュアルを参照してください。
    - **VMware** については、VSphere の VCenter サーバアプライアンス管理インターフェイスのマニュアルを参照してください。

別の方法

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. Stealthwatch Management Console 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。

証明書チェック

v7.2.1 または v7.3.0 から更新する場合、v7.3.1 への更新には、シスコのバンドルのアップグレード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。

> ⚠ 追加された証明書の完全なチェーンが Central Manager の信頼ストアにない場合、Stealthwatch v7.2.1 および v7.3.0 から v7.3.2 への更新は失敗します。v7.3.1 からアップグレードする場合、このチェックは適用されません。

更新後のレポートビルダーのインストール

Stealthwatch デスクトップクライアントのレポート機能がレポートビルダーアプリに置き換えられ、Stealthwatch 管理コンソールの Web アプリ/ダッシュボードからレポートを作成およびカスタマイズできるようになりました。

Stealthwatch の更新が完了したら、必ず最新のレポートビルダーアプリ(v1.4.1)をインストールしてください。アプリの以前のバージョンがインストールされている場合は、既存のバージョン上に新しいバージョンをインストールしてください。詳細については、『Stealthwatch 更新ガイド(v7.2.1 および 7.3.x から v7.3.2)』を参照してください。

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。レポートビルダーアプリは削除しないでください。

> ⚠ 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。

更新後

アプライアンスを更新した後、必要なパッチをインストールしてください。

- patch-smc-ROLLUP001-7.3.2-01.swu 以降
- patch-fcnf-ROLLUP001-7.3.2-02.swu 以降

詳細については、Cisco Software Central で、パッチの Readme ファイルを参照してください。

新着情報

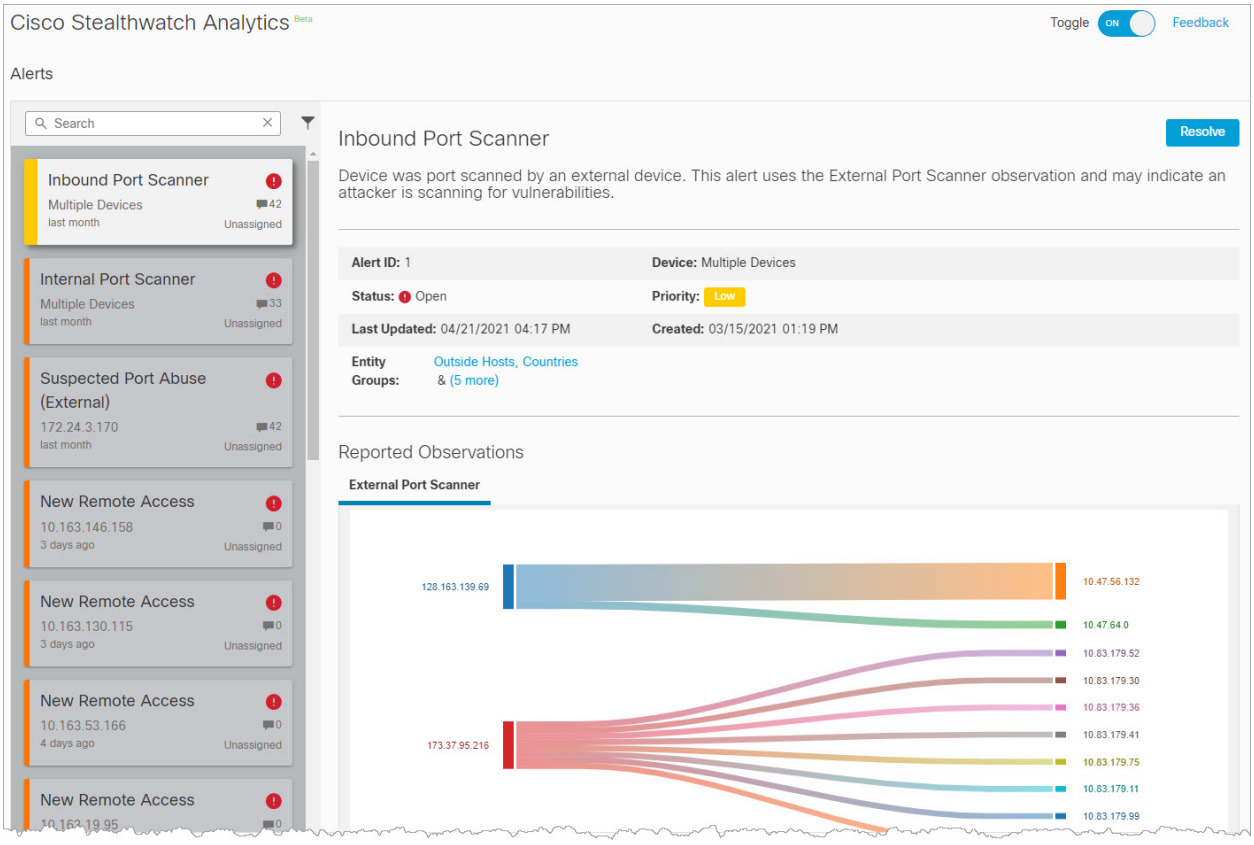
Stealthwatch システム v7.3.2 リリースの新機能と改善点は次のとおりです。

Analytics ベータ版

Stealthwatch では、Analytics ベータ版により、高度なイベント機能と UI ワークフローに早期にアクセスして、手動構成が少なく済む新しく効果的なアラートを利用できます。Analytics ベータ版は、適切なロールをデバイスに割り当て、追加の検出機能を使用して収集されたデータとともにこの情報を利用して、最適化されたアラートを提供します。

Analytics ベータ版を有効にすると、展開内でベータ機能がオンになります。これらの追加機能は、既存の検出機能およびインターフェイスと並行して機能します。シスコの新しい実験的な検出機能とインターフェイス機能を活用しながら、アラーム、セキュリティイベント、Stealthwatch Web アプリケーションを引き続き監視できます。

Stealthwatch Web アプリケーションで Analytics アラートを開くと、システムがアラートを生成した原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。



Analytics ベータ版をご使用の際には、インライン フィードバック フォームを使用してフィードバックをお寄せください。こちらから、Analytics ベータ版 v7.3.2 ドキュメントにアクセスできます。

応答の管理

次のアラームタイプは廃止されたため、応答管理から削除されました。

- ライセンス破損（アラーム ID 60013）
- ライセンス期間 3 日未満（アラーム ID 60022）
- ライセンス期間 14 日未満（アラーム ID 60021）
- ライセンス期間 30 日未満（アラーム ID 60020）
- ライセンス期間 60 日未満（アラーム ID 60019）
- ライセンス期間 90 日未満（アラーム ID 60018）
- Stealthwatch フローレートライセンス超過（アラーム ID 60012）
- Stealthwatch フローレートライセンス利用不可（アラーム ID 60025）
- ライセンスされていない機能（アラーム ID 60014）
- ライセンスされていない FPS 機能（アラーム ID 60024）

エンドポイントライセンス

エンドポイント コンセントレータの削除

v7.3.2 以降、エンドポイント コンセントレータはエンドポイントライセンスの展開に不要となり、Data Store を含むすべての Stealthwatch 展開で Network Visibility Module（NVM）データを処理するようにフローコレクタが拡張されました。この機能拡張により、エンドポイント コンセントレータは v7.3.2 ではサポートされません。

Stealthwatch クラスタを更新する前に、『Stealthwatch 更新ガイド（v7.2.1 および 7.3.x から v7.3.2）』の手順に従って、システムからエンドポイント コンセントレータを削除してください。

エンドポイントライセンスの設定方法の詳細については、『Stealthwatch v7.3.2 エンドポイントライセンスおよび NVM コンフィギュレーション ガイド』を参照してください。

エンドポイントライセンスの機能

Data Store でサポートされるようになったエンドポイントライセンスは、以下を提供します。

- オンネットワークとオフネットワークのデータを含む、エンドポイントに対する完全な可視性
- レポートビルダーアプリのエンドポイントトラフィック（NVM）レポートの NVM フィールドに対する可視性
- NVM データの 30 日間以上の保存
- 処理とクエリのパフォーマンス向上

pxGrid 2.0 への ISE 統合のアップグレード

ISE 統合は pxGrid 2.0 にアップグレードされ、pxGrid ノードのサポートが追加されました。

> ISE バージョンが 2.6 以降であることを確認してください。

Cisco ISE で pxGrid を承認する方法の詳細については、『ISE v7.3.2 構成ガイド』を参照してください。

SecureX リボンのマルチユーザサポート

SecureX との統合で、SecureX セキュリティリボンのマルチユーザサポートが追加されました。これにより、SecureX、コラボレーション ソリューション アナライザ（CSA）、または Thread Grid のアカウントを持つユーザは、Stealthwatch Enterprise のセキュリティリボンを使用して認可を実行できます。

> SMC の更新後、Oauth 範囲を使用して SecureX 上で API クライアントのログイン情報を再生成し、新しいログイン情報で Stealthwatch および SecureX の構成を更新する必要があります。統合を更新する方法の詳細については、『SecureX Integration Guide 7.3』を参照してください。

クロスサイトリクエスト偽造（CSRF）に対する保護

CSRF 攻撃に対する保護を強化するために、Stealthwatch では、HTTPS クライアントは状態変更 HTTPS リクエストの一部として CSRF トークンを送信する必要があります。CSRF トークンはセッション固有であり、認証時に「XSRF-TOKEN」という Cookie で返されます。HTTPS クライアントは、HTTPS リクエストを行うときに、HTTPS ヘッダー「X-XSRF-TOKEN」をこの Cookie の値に設定する必要があります。

追加されたこの保護の一環として、認証 API スクリプトが HTTP 401 エラーで失敗することがあります。

クラスタを v7.3.2 に更新する前に、API スクリプトに次の変更を加える必要があります。

> API スクリプトを更新する手順は、環境によって異なる場合があります。

1. Stealthwatch に対する HTTPS クライアントの認証時に、XSRF-TOKEN Cookie で返された CSRF トークンを保存します。
2. すべての HTTPS リクエスト（「GET」を除く）で、スクリプトは「X-XSRF-TOKEN」という HTTP ヘッダーを介してこの保存された値を返す必要があります。
3. Stealthwatch に対する再認証のたびに、スクリプトは保存されている CSRF トークンの値を更新する必要があります。

> API スクリプトを更新する前にクラスタを更新する必要がある場合は、Cisco Stealthwatch サポートにお問い合わせください。

コグニティブ統合の機能拡張

コグニティブエンジンに関する毎月の機能拡張の完全なリストについては、コグニティブのリリースノートを参照してください。

SNMP エージェントのカスタムユーザ名とパスワード

システムモニタリングのメソッドとして Simple Network Management Protocol（SNMP）を使用する大規模なネットワーク環境がある場合は、SNMP エージェントがシステムステータス情報にアクセスできるようにします。[SNMP エージェント（SNMP Agent）] を有効にすると、クライアントシステムが信頼できるホストの 1 つである場合、ネットワーク経由で SNMP エージェントにアクセスできます。

v7.3.2 では、次のように、カスタムユーザ名とパスワードの暗号化を SNMP V3 構成に追加できます。

- [ユーザ名(User Name)]:SNMP マネージャのユーザ名を入力できます。このフィールドの変更は任意です。デフォルトのユーザ名は読み取り専用です。
- [暗号化パスワード(Encryption Password)]:暗号化に使用するパスワードを入力します(8 文字以上)。
- [認証パスワード(Authentication Password)]:認証に使用するパスワードを入力します(8 文字以上)。

手順については、オンラインヘルプの [システム管理ヘルプ(System Management Help)] > [Central Management] > [アプライアンス構成(Appliance Configuration)] > [SNMPエージェント(SNMP Agent)] を参照してください。

> ⚠ **構成の最大値**:一度に保存できる SNMP 構成は 1 つだけです。構成を V2 から V3 に、またはその逆に変更すると、以前の構成が削除されます。たとえば、カスタムユーザ名を使用して SNMP V3 を設定するとユーザ名が失われ、構成を SNMP V2 に変更すると V3 構成が削除されます。

管理対象アプライアンスの SSL/TLS 証明書ガイド

SSL/TLS 証明書関連の手順は、オンラインヘルプから『SSL/TLS Certificates for Managed Appliances Guide v7.3』に移動されました。このガイドは、次のような内容で構成されています。

- シスコのデフォルトのアプライアンス アイデンティティ証明書の証明書有効期間の変更
- 認証局からの証明書へのアプライアンス アイデンティティ証明書の置き換え
- ホスト名の変更
- ネットワークドメイン名の変更
- IP アドレス(eth0)の変更
- クライアント アイデンティティ証明書の追加
- トラブルシューティング

Security Analytics and Logging(オンプレミス)

Security Analytics and Logging(オンプレミス) がデータストアでサポートされるようになったため、Stealthwatch の展開オプションは次の 2 つになりました。

- シングルノード:イベントを受信および保存するスタンドアロンの Stealthwatch 管理コンソールを展開します。このコンソールから、イベントを確認およびクエリできます。
- マルチノード:イベントを受信するフローコレクタ、イベントを保存する Data Store(3 つの Data Node を含む)、およびイベントを確認およびクエリできる Stealthwatch 管理コンソールを展開します。

SAL オンプレミスの展開の詳細については、『Security Analytics and Logging (On Premises): Firepower Event Integration Guide』を参照してください。

初回セットアップ

データストアを展開する場合は、SMC およびフローコレクタでの初回セットアップ時に SAL オンプレミス を有効にするかどうかを尋ねられます。有効にすることを選択した場合、Data Store を使用して NetFlow を取り込むことができなくなります。

詳細については、Stealthwatch 設置ガイドを参照してください。

Stealthwatch アプリ

Stealthwatch は、Cisco Stealthwatch 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。

Stealthwatch アプリケーションのリリーススケジュールは、通常の Stealthwatch のアップグレードプロセスとは無関係です。したがって、Stealthwatch アプリケーションは、Stealthwatch のコアリリースとは別途に、必要に応じて更新されることがあります。場合によっては、Stealthwatch の新しいリリースに対応するように設計されたアプリケーションをすぐにインストールできないことがあります。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 Stealthwatch アプリの情報と可用性については、次を参照してください。

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

CIMC および BIOS ファームウェアをバージョン 4.1(1)g に更新する場合、該当する ISO ファイルとともに SWU を使用できるようになりました。

M4 ハードウェアの CIMC および BIOS ファームウェアの v4.1(1)g への更新

CIMC および BIOS ファームウェアをバージョン 4.1(1)g に更新する場合、該当する ISO ファイルとともに SWU を使用できるようになりました。

- **ucs-sw1uv7m4-huu.iso** –
  Flow Collector 5020 データベースおよび Flow Collector 5200 データベースを除くすべてのアプライアンスの ISO ファイル
- **ucs-sw2uv7m4-huu.iso** –
  Flow Collector 5020 および Flow Collector 5200 データベースの ISO ファイル
- **update-common-SW7VM4-FIRMWARE-01.swu** –
  バージョン 2.x からの更新時に使用する SWU ファイル

> ファームウェアがバージョン 3.x 以降の場合、SWU は必要ありません。

SWU および ISO ファイルは、Cisco Software Central（https://software.cisco.com）で入手できます。

この更新プロセスは、次の表に示す Stealthwatch アプライアンス用 UCS C シリーズ M4（x200）ハードウェアに適用されます。

M4 ハードウェア（x200 シリーズ）	
Stealthwatch Management Console 2200	Flow Sensor 1200
Flow Collector 4200	Flow Sensor 2200
Flow Collector 5020 エンジン	Flow Sensor 3200
Flow Collector 5020 データベース*	Flow Sensor 4200
Flow Collector 5200 エンジン	UDP Director 2200
Flow Collector 5200 データベース*	__

M5 ハードウェアの場合、**update-common-SW7VM5-FIRMWARE-01.swu** を使用して、CIMC および BIOS ファームウェアを v4.1(1)g に更新できます。このファイルを使用すると、SMC を介して他のパッチ更新 SWU と同様にファームウェアを更新できます。SWU は、Cisco Software Central（https://software.cisco.com）で入手できます。

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。
- Cisco Stealthwatch サポートのお問い合わせ先：
  - 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：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、Stealthwatch Defect（SWD または LSQ）番号が示されています。

バージョン 7.3.2

障害	説明
SWD-15440	ANC クエリに関連するヘルプドキュメントのコンテンツを更新しました。（LSQ-5020）
SWD-15495	顧客のアプリケーションを削除するときの、関係ポリシーの削除に関連する問題を修正しました。
SWD-15529	CTA に関連するヘルプドキュメントのコンテンツを更新しました。（LSQ-4897）
SWD-15831	ユーザーがスマート ライセンス トランスポート ゲートウェイをカスタム トップレベル ドメイン（TLD）に登録できない問題を修正しました。（LSQ-5147）
SWD-15866	FC4210 および FCVE4000 フローのストレージサイズに関連するドキュメントの内容を更新しました。（LSQ-5232）
SWD-15926	M5 ハードウェアの CIMC ファームウェアバージョンに関連する印刷文書の内容を更新しました。（LSQ-5298）
SWD-15942	v2.0.3 および v7.3.0 に対するホスト分類アプリケーションの互換性マトリックスに関連するヘルプドキュメントの内容を更新しました。（LSQ-5253）
SWD-15950	エンジンが不正確な値を検出して拒否するようにデータ検証機能を強化しました。
SWD-15953	root または sysadmin CLI アカウントに適用されない WebUI で構成されたパスワードポリシーに関連するヘルプドキュメントの内容を更新しました。（LSQ-5261）
SWD-15963	[ホストに対してビーコンを実行（Beaconing Host）] セキュリティイベントから [関連フロー（Associated Flows）] テーブルにピボット処理すると結果が返されていた問題を修正しました。（LSQ-5248）
SWD-15965	顧客のレポートに IDP と SPLT のフローが表示されない問題を修正しました。（LSQ-5318）
SWD-15974	『Failover Configuration Guide』の「SMC Databas」および「Network Interfaces」セクションに対応する印刷文書の内容を更新しました。

障害	説明
SWD-15978	診断パックの生成時に eta 分析ツールが自動的に実行されていた問題を修正しました。
SWD-15981	「Config changes failed（設定変更の失敗）」エラーで示される、パススループロキシの設定時にプロキシ設定が保存されない問題を修正しました。（LSQ-5305）
SWD-15982	v7.2.1 から v7.3.1 のインストール/コンフィギュレーション ガイド内の SMC ISE PORT TCP/5222 コンテンツに関連する印刷文書を更新しました。（LSQ-5339）
SWD-16011	セキュリティイベントとアラームの詳細を追加してドキュメントを更新しました。（LSQ-5361）
SWD-16020	ログファイルでの TLS FP の生成に関連する問題を修正しました。
SWD-16024	一部のお客様が誤って DDS システムでデータストアを有効にしていた問題を修正しました。
SWD-16025	古いバージョンの Stealthwatch からアップグレードされた v7.3.x SMC およびフローコレクタのデータベースバックアップが正しく機能しない問題を修正しました。（LSQ-5358）
SWD-16028	v7.3.0 自己署名証明書が SAN フィールドと一致しない問題を修正しました。（LSQ-5375）。
SWD-16043	UDP Director 2210 の仕様書の内容を更新しました。（LSQ-5387）
SWD-16049	フローコレクタの swe-detections-worker サービスが監視結果を登録していなかった問題を修正しました。
SWD-16054	クライアント/サーバーがイニシエータの順序に従っていないことが原因で、ポートスキャンアラームと関連するフローテーブルが空になったままであった問題を修正しました。（LSQ-5366、LSQ-5495、LSQ-545）
SWD-16057	ID が関連付けられていない v7.3.0 SMC ID エクスポータに関連する問題を修正しました。（LSQ-5237、LSQ-5270）
SWD-16083	アップグレードでサポートされていない sfp が許可されるように問題を修正しました。（LSQ-5384）
SWD-16090	セキュリティ イベント スレッドの SIGSEGV に関連する問題を修正しました。

障害	説明
SWD-16111	脅威フィードの更新の SIGSEGV に関連する問題を修正しました。(LSQ-5437)
SWD-16145	問題のあるサイトやアプリケーションが本来あるべき優先度で表示されない問題を修正しました。(LSQ-4718)
SWD-16146	フローコレクタチャネルのダウンアラームが適切に非アクティブにならない問題を修正しました。
SWD-16150	Security_Events_and_Alarm_Categories に関連するヘルプドキュメントのコンテンツを更新しました。
SWD-16160	フローコレクタがスレッドを取り除いていた問題を修正しました。(LSQ-5472)
SWD-16161	SystemInitTimeMilliseconds フィールドが不適切にエクスポートされるたびに、FC エンジンによって計算されるフロー継続時間の値エラーが発生していた問題を修正しました。(LSQ-5477)
SWD-16169	チェックポイント エクスポータからの NetFlow データが FC エンジンによって適切に取り込まれない問題を修正しました。これは、主にチェックポイントで不必要に PEN フィールドを使用していたことが原因です。(LSQ-5470)
SWD-16194	CTA 統合ガイドで提供されるポート情報に関連する印刷文書を更新しました。
SWD-16200	v7.3.0 から v7.3.1 にアップグレードした後の列「tls_fingerprint_hash」に関連する問題を修正しました。(LSQ-5493)
SWD-16238	Flow Sensor によって検出されたアプリケーションのリストから SOCKS を削除し、v7.3 デフォルト アプリケーションの定義ドキュメントで印刷文書の内容を更新しました。
SWD-16290	エンジンではなく一般的なリソースプールを使用するようにベースラインクエリを更新しました。

バージョン 7.3.1

障害	説明
SWD-15072	SMCで syslog-ng ファイルのモニター制限に達した問題を修正しました。
SWD-15494	v7.2.1 フローセンサーのパスワードリセット検証プロセスを修正しました。（LSQ-5035）
SWD-15528	SecureX のタイル属性が更新されました。
SWD-15543	ログインが成功した後でも、TACACS+ 認証サービスのログイン試行が 0 と表示される問題を修正しました。（LSQ-5064）
SWD-15574	ASA Biflow の後半でイニシエータを設定する際の問題を修正しました。（LSQ-5071）
SWD-15684	LDAP および RADIUS 認証のオンラインヘルプを更新しました。
SWD-15685	/smc/rest のnginx タイムアウトが増加しました。
SWD-15702	M5 ハードウェアの更新イメージ アクティブ パーティションの問題を修正しました。
SWD-15734	[プロキシ（Proxy）] ページのレガシー（クラウドベース）ホスト分類子のリストを更新しました。
SWD-15779	フローコレクタのオーバーサブスクライブ アラームの原因と思われる AppID および UserID フィールドの問題を修正しました。（LSQ-4919）
SWD-15779	Palo Alto、AppId/UserId のフィールドがフローコレクタのオーバーサブスクライブ アラームを開始すると考えられる問題を修正しました。（LSQ-4919）
SWD-16145	定義済みアプリケーション優先度レベルに関する問題を修正しました。（LSQ 4718）

障害	説明
SWD-14260	クライアントとサーバー設定機能の最初の作業として、イニシエータを受け入れるようにコードを更新しました。(LSQ-4635)
SWD-14930	ユーザーのタイムゾーンに関係なく、デスクトップクライアントが前回のログイン時間を UTC で表示していた問題を修正しました。(LSQ-4833)
SWD-14932	Cognitive のマニュアルのリンクが期限切れになった問題を修正しました。
SWD-14952	アプライアンスが [中央管理(Central Management)] で管理されている場合、IP アドレスを変更しようとしたときの警告ポップアップを SystemConfig に追加しました。(LSQ-4380)
SWD-15024	API を介したフロークエリが tcpConnections フィールドに負の値を返す問題を修正しました。
SWD-15062	Stealthwatch インシデントが CTR に送信されない問題を修正しました。
SWD-15134	通常の診断を妨げる例外で ISE ログがフラッディングされる問題を修正しました。
SWD-15149	接続フィルタが [ポート/プロトコル(Port/Protocol)] に設定され、サブジェクト方向フィルタが [サーバー(Server)] に設定されている場合に、上位レポートが機能していない問題を修正しました。(LSQ-4882)
SWD-15218	tomcat が ciscoj.log に記録されない問題を修正しました。
SWD-15293 sWD-15294	バインドユーザー名にサポートされていない文字がリストされるように LDAP のマニュアルを更新しました。
SWD-15341	一部の特殊文字がプロキシパスワードで使用できない問題を修正しました。(LSQ-4997)
SWD-15360	アイデンティティ管理デバイスの要件に関する Active Directory のドキュメントを更新しました。(LSQ-4991)
SWD-15441	[トラフィック別の SecureX の上位ホストグループ(SecureX Top Host Groups By Traffic)] タイルにデータが表示されない問題を修正しました。

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。

問題番号	説明	回避策
SWD-12574	ユーザ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、エポックデート（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-13964	データベースの復元に、暗号化された設定のバックアップは含まれません。	この問題を解決するには、doDbRestore コマンドに `-r` を追加し、設定のバックアップを復元せずにデータベースの復元を実行してから、暗号化されたバックアップを手動で復元します。
SWD-14057	SMC アプライアンス管理では、[パケットキャプチャ（Packet Capture）] ページは空白になります。	パケットキャプチャはSMC アプライアンス管理から削除されました。別の方法を使用するには、[ヘルプ（Help）] > [Stealthwatch オンラインヘルプ（Stealthwatch Online Help）] を選択し、SMC パケットキャプチャの手順に従います。
SWD-14855	Firefox を使用している場合、手順 6 でフローセンサー AST が表示されない場合があります。この場合、Central Management にアプライアンスを追加します。	別のブラウザを使用してください。Firefox を使用している場合は、キャッシュをクリアしてページを更新します。
SWD-15002	設定の復元が RFD 後に失敗します。	アプライアンスを工場出荷時のデフォルトにリセットすると、Central Management を使用して設定を復元できません。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

問題番号	説明	回避策
SWD-16183	ルールに DPI 定義がある場合、カスタムアプリケーションがトラフィックにタグを付けません。フロー検索のアプリケーション名は、カスタムアプリケーション名ではなくHTTPS（未分類）として表示されます。	現在使用可能なものはありません。
SWD-16223	スマートライセンスで、複数の予約のうち 1 つしか表示されません。	現在使用可能なものはありません。
SWD-16226	Web UI のエクスポータ SNMP で、認証パスワードとプライバシーパスワードがプレーンテキストで保存されます。	現在使用可能なものはありません。
SWD-16338	ISE 統合フェールオーバーで発生する可能性のある問題があります。	Stealthwatch を Cisco ISE と同時に展開する場合は、それぞれに一意の ISE クライアント証明書とクライアント名を持つプライマリおよびセカンダリ SMC を必ず設定してください。各 SMC の ISE クライアント証明書とクライアント名は違うものである必要があります。 セカンダリ SMC を設定する方法の詳細については、『ISE 構成ガイド』の「ISE 統合フェールオーバーの設定」を参照してください。
SWD-16382	FMC のユーザが IP サブネットフィルタ（10.10.1.0/24）を指定すると、CDS クエリサービスバックエンドでクエリが失敗します。	ipRange 比較演算子を使用すると、FMC で回避策が利用可能になります。ただし、コードの変更が必要であり、アーキテクチャまたはリリースのタイミングによっては実行できない場合があります。
SWD-16383	SAL CONNECTION_END_EVENT last_packet_second の計算に問題があります。	現在使用可能なものはありません。

問題番号	説明	回避策
SWD-16346	非アクティブなエクスポータの誤ったステータスがエンジンから返されます。	現在使用可能なものはありません。
SWD-16408	ISE クライアントが、非 UTC タイムゾーンを含むユーザセッションを解析しません。	回避策は、ISE を UTC 時間に設定することです。
SWD-16378	ダッシュボードおよびレポートの Data Node に関するシステムアラームが、正しい問題を示していない場合があります。タイムフレームの表示（ボックスの右上）に、Data Node がダウンしてからの実際の経過時間よりもはるかに短い時間が表示されることがあります。 [詳細を表示（View Details）] を選択し、[システムレポートの表示（View System Report）] を選択すると、過去 30 日間のアラームが表示されます。	システムレポートでは、[アラーム（Alarm）] 列の上部にある [検索（Search）] ボックスを使用して、特定のアラームの説明を入力できます。次に、[日時（Date/Time）] 列でソートして、特定のアラームの最も古いものや最新のものを確認できます。 また、カレンダーから [日（Day）] を選択し、[次の値より前（Is Before）] で [検索（Search）] アイコンの値を選択して、発生した最初の日を検索することもできます。
NA	FlowSensor VE では、[アプリケーション識別情報のエクスポート（Export Application Identification）] 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	2021 年 6 月 1 日	最初のバージョン
1_1	2021 年 6 月 28 日	「既知の問題」セクションに SWD-16338 を追加。
2_0	2021 年 12 月 21 日	「修正点」セクションを更新しました。

リリースサポート情報

リリース 7.3.2 の公式一般公開（GA）日は TBD 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