Cisco Stealthwatch

リリースノート 7.3.0

目次

はじめに

概要

このドキュメントでは、Stealthwatch v7.3.1 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。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。サブセットとして、「データストアクラスタ」は、データストアを構成するデータノード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.x から v7.3）』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 に更新するには、アプライアンスに 7.2.1 または後継バージョンの 7.2.x 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、7.1.x を 7.2.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、いずれかのステルスウォッチ 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、別のブラウザからアプライアンスにログインするか、アプライアンス アイデンティティ証明書をカスタム証明書に置き換えるか、または Cisco Stealthwatch サポートに連絡してください。

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、ステルスウォッチ 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ステルスウォッチ 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）**：最新の Cisco を参照してください。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。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

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 を有効にすると、システムの侵害リスクが増加します。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

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-ROLLUP001-7.3.0-01.swu 以降
- patch-fcnf-ROLLUP001-7.3.0-02.swu 以降
- patch-fcsf-ROLLUP001-7.3.0-02.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 リリースの新機能と改善点は次のとおりです。

Stealthwatch Data Store

> ⚠ ご自身で Data Store を導入しないでください。Cisco プロフェッショナルサービスに連絡し、全体的な Stealthwatch 導入内の一部としての配置、導入、および設定の支援を受けてください。

Stealthwatch Data Store は、Stealthwatch フローコレクタによって収集されたネットワークのフローデータを保存する中央リポジトリを提供します。Data Store には次の利点があります。

- Data Store は、フローコレクタと Stealthwatch 導入全体で収集された情報のストレージ容量を大幅に増やします。
- Data Store データベースは、データノードのクラスタで構成されます。各データノードには、フローデータの一部と別のデータノードのデータのバックアップが含まれ、耐障害性と全体的なデータベースアップ稼働時間が改善されます。
- すべてのフローデータが 1 つの集中型データベースに存在し、複数のフローコレクタに分散されていないため、Stealthwatch Management Console はすべてのフローコレクタに個別にクエリする場合よりも Data Store から迅速にクエリ結果を取得できます。Data Store を使用すると、グラフとチャートの作成が大幅に改善されます。

データストア機能の詳細について Data Store のスタートアップガイドを参照し、導入プロセスの概要を理解してください。Stealthwatch 導入の一部としての Data Store の導入の詳細については、Data Store クラスタハードウェアのインストールおよび構成ガイドを参照してください。

Data Store の考慮事項

Data Store を導入する場合は、Stealthwatch の導入に関する次の点に注意してください。

- Data Store を導入する場合は、Stealthwatch Web アプリケーションを使用して Stealthwatch インストールをモニタおよび設定します。Stealthwatch デスクトップクライアントは Data Store と互換性がありません。
- Data Store との互換性を確保するようにフローコレクタを設定すると、アプライアンス管理インターフェイス（アプライアンス管理）によって特定の機能が非表示になります。フローコレクタの設定やその他の関連タスクを実行するには、Central Management を使用します。ストレージ統計情報をモニタする場合は、レポートビルダーアプリを SMC にダウンロードします。
- Data Store との互換性を確保するために SMC を設定した場合は、ETA Cryptographic Audit または Host Classifier アプリケーションを使用できません。
- Endpoint Concentrator と Data Store の併用はサポートされていません。
- Data Store データベース アーキテクチャでは、SMC およびすべてのフローコレクタは Data Store と通信する必要があり、展開時に Data Store と連携するように設定する必要があります。一部のフローコレクタが SMC に直接レポートし、それ以外のフローコレクタが Data Store にレポートする「混合」環境は使用できません。

ネットワークに Data Store を導入する場合で、SMC 2210 および FC 4210 アプライアンスを導入済みの場合は、SMC とフローコレクタで RFD を実行し、シスコ プロフェッショナル サービスと協力してData Store を統合する必要があります。詳細については、シスコサポートまでお問い合わせください。

Data Store アーキテクチャ

各 Data Store データベースクラスタは、3 つ以上のデータノードで構成されます。各データノードは独自のハードウェアシャーシです。Data Store を購入すると、その Data Store モデルで示されたノード数に対応する複数のデータノード ハードウェア シャーシが提供されます。たとえば、DS 6200 Data Store では 3 つのデータノード ハードウェアシャーシが提供されます。Data Store データベースクラスタの一部としてのデータノード間通信を円滑に行うには、10G 速度をサポートする 1 つまたは 2 つのスイッチを導入する必要があります。

複数の Data Store を購入して導入できます。データノードは、Data Store データベースクラスタの一部として、最小 3 台から最大 36 台まで 3 の倍数でクラスタ化できます。

互換性のある SMC およびフローコレクタを使用して Data Store を導入する場合、SMC およびフローコレクタの `eth0` 管理ポートを SFP+ ファイバポートとして設定して、スループットを向上させることができます。Data Store を導入していないユーザは、100Mbps/1Gbps/10Gbps 銅線インターフェイスのみを `eth0` として設定できます。

Data Store ハードウェアおよび Data Store 互換の Stealthwatch アプライアンスの詳細については、Stealthwatch ハードウェアおよびソフトウェアバージョンのサポートマトリックスを参照してください。

ユーザパスワード検証の要件と機能強化

[パスワードの生成(Generate Password)]をクリックすると、ユーザに推奨パスワードが提供されます。ユーザは独自のパスワードを作成することも可能です。パスワードは 8 ～ 256 文字で、Central Management の [パスワードポリシー(Password Policy)] で設定された特定の要件を満たす必要があります。

パスワードの入力中に、ユーザは [パスワードの表示(Show Password)]をクリックして、入力している文字を表示できます。

ユーザのパスワードは次のようには設定できません。

- ユーザのユーザ名とほぼ同じ、または同一である
- 現在のパスワードまたは以前のパスワードと同じ文字を 4 文字以上含む
- 繰り返す文字、またはアルファベットや数字の順の文字を含む
- 辞書にある 4 文字以上の単語を含む
- データ漏洩により漏洩したパスワードのリストに存在する

これらの要件は、Stealthwatch のデフォルトの管理者を除くすべてのユーザに適用されます。

応答の管理

応答の管理の機能は、いくつかの改良を加えて Stealthwatch Web アプリケーションに移行されました。したがって、Stealthwatch v7.3.0 では、応答管理のタスクは Stealthwatch Web アプリケーションでのみ実行できます。v7.3.0 にアップグレードすると、Stealthwatch はすべての応答管理設定を Stealthwatch デスクトップクライアントから Stealthwatch Web アプリケーションに移行します。移行されたルールに v7.3.0 と互換性のない条件が含まれている場合、Stealthwatch は移行プロセス中にこれらのルールを無効にします。そうなった場合、影響を受けたルールは修正してから再度有効にしてください。

Stealthwatch v7.2 から v7.3 にアップグレードすると、Stealthwatch Web アプリケーションは、CEF を使用する Syslog メッセージアクションとして、応答の管理の既存の Common Event Format（CEF）アクションをインポートします。

syslog メッセージを送信するときに形式として CEF を選択すると、メッセージに次の情報が含まれるようになりました。

- Cisco（デバイスベンダー）
- Stealthwatch（デバイス製品）
- 現在の Stealthwatch のバージョン（デバイスのバージョン）

Stealthwatch v7.3.0 では、応答の管理では必要なルールとアクションが作成され、アラームは引き続き SecureX Cisco® Threat Response にエクスポートされます。

応答の管理のルールとアクションに次の改善を加えました。

ルール（Rules）

- アラーム重大度を正確に指定できます（「～以上」だけでなく）。
- ホストグループには、複数選択の機能があります。
- リレーションシップポリシーを選択できます。
- 応答の管理は Cisco® ISE と統合されます。
- 追加の定義済みルールを選択できます。
- 応答管理に、ISE ANC ポリシー、Threat Response インシデント、および Webhook アクションが含まれるようになりました。
- ルール設定時にカスタム セキュリティイベントを選択する場合、アラームとカスタム セキュリティイベントを簡単に区別できます。
- サブ条件とサブ条件セットをより簡単に追加できます。
- ある条件を別の条件セットに移動する場合は、目的の場所に条件をドラッグアンドドロップするだけです。
- [ルール（Rules）] タブ（リストビュー）で、ルールを簡単に有効または無効にできます。

> Stealthwatch Web アプリケーションは、ルール作成時の複数範囲形式を使用した複数の IP 範囲の指定をサポートしていません。

アクション

次の新しいアクションが追加されました。

- **ISE ANC ポリシー** このアクションを使用すると、ホストアラームがトリガーされた送信元ホストまたはターゲットホストに ANC（Adaptive Network Control）ポリシーを適用するように Cisco® ISE（Identity Services Engine）に指示できます。この新しいアクションと連携して、ISE ANC ポリシー割り当てレポートを実行できるようになりました。このレポートでは、応答管理で指定する、またはユーザが手動で指定する ISE ANC ポリシー割り当てをモニタできます。
- **Threat Response インシデント** ルールが提供する条件に基づいて、特定のアラームを SecureX Cisco® Threat Response にエクスポートできます。また、インシデント信頼レベルを設定し、カスタマイズされたターゲットエンティティを作成することもできます。
- **Webhook** このアクションにより、Stealthwatch は Web サービスまたは REST API を介して、外部システムとの応答自動化および統合の機会がより多く提供されます。デフォルトの状態で、Webhook アクションはアラームを Splunk HEC（HTTP イベントコレクタ）に直接エクスポートできます。

次の既存のアクションが強化されました。

- **電子メール** このアクションでは、SMTP サーバでカスタムポート、認証、および暗号化を使用できるようになりました。受信者に任意の電子メールアドレスやメーリングリストを指定でき、電子メールを送信することなく電子メールをプレビューできます。
- **SNMP トラップ** v3 用に新しい暗号化プロトコルが追加されました。
- **Syslogメッセージ** ホスト名を宛先サーバとして指定できます。このアクションには、CEF 形式を使用できます（以前は別のアクションとして提供されていました）。

エクスポータ

エクスポータ ハイブリッド モードは使用できなくなりました。

Stealthwatch Web アプリケーションの [設定（Configure）] > [エクスポータ（Exporters）] オプションを使用して、エクスポータを管理および設定できるようになりました。また、Stealthwatch Web アプリケーションでは、複数のエクスポータを一括編集できます（[名前（Name）] フィールドと [SNMP 設定（SNMP Configuration）] フィールドのみ）（最大10件）。Stealthwatch は、編集が含まれる各行の先頭に青い垂直バーを挿入します。

- フェールオーバー SMC のエクスポータは一括編集できません。
- カスタム設定を一括編集することはできません。
- 次のタイプのエクスポータは、Central Manager を使用して編集する必要があります。
  - フローセンサー
  - 仮想フローセンサー
  - エンドポイントコンセントレータ

インターフェイス

Stealthwatch Web アプリケーションの [設定(Configure)] の [エクスポータ(Exporters)] オプションを使用し、該当するエクスポータの [アクション(Actions)] 列から [インターフェイスの表示(View Interfaces)] を選択して、インターフェイスを管理および設定できます。また、Stealthwatch Web アプリで複数のインターフェイスを一括編集できます(最大10件)。[名前(Name)]、[説明(Description)]、[着信速度(Inbound Speed)]、[発信速度(Outbound Speed)]、[着信しきい値(Inbound Threshold)]、[Outbound Threshold(発信しきい値)]、および [Locked(ロック済み)] フィールドを編集できます。Stealthwatch は、編集が含まれる各行の先頭に青い垂直バーを挿入します。

- フェールオーバー SMC のインターフェイスは一括編集できません。

カスタマー サクセス メトリック

次を含む、テレメトリデータ収集の一部の設定が変更されました。

- ファイアウォールの要件が更新されました
- フローセンサーおよび UDP Director の新しいメトリックが追加されました

詳細については、Stealthwatch Customer Success Metrics のコンフィギュレーションガイドを参照してください。

以前は、シスコはお客様がオプトインした時点で一部のユーザデータを収集していました。このデータはお客様のカスタマーエクスペリエンスの向上とシスコ製品の改善のために役立っています。Stealthwatch システム v7.2.1 現在、このデータが収集されないようにするには、オプトアウトする必要があります。オプトアウトするには、次の操作を実行します。

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、[中央管理(Central Management)] をクリックします。
3. [アクション(Actions)] 列のコンテキストメニューから、[アプライアンス設定の編集(Edit Appliance Configuration)] を選択します。
4. [全般(General)] タブをクリックします。
5. [外部サービス(External Services)] セクションまで下にスクロールし、[カスタマーサクセスのメトリクスを有効にする(Enable Customer Success Metrics)] チェックボックスをオフにします。
6. [設定の適用(Apply settings)] をクリックします。

SMC フェールオーバー

フェールオーバー設定を使用すると、2 つの Stealthwatch 管理コンソール（SMC）間にフェールオーバーペアを確立し、一方の SMC をもう一方のバックアップコンソールとして機能させることができます。

v7.3.0 では、設定メニューをデスクトップクライアントから Stealthwatch Web アプリケーションに移行しました。フェールオーバー設定を保存すると、セカンダリ SMC ドメイン設定が削除されるため、『Stealthwatch フェールオーバー コンフィギュレーション ガイド』に記載されている手順、要件、および指示に従ってください。

> ⚠ プライマリ SMC がオフラインになっても、SMC のロールは自動的に交換されない点に注意してください。『Stealthwatch フェールオーバー コンフィギュレーション ガイド』に記載されている順序で SMC のロールを変更してください。

フェールオーバーの設定

『Stealthwatch フェールオーバー コンフィギュレーション ガイド』には、正常に設定するために重要な、次を含む詳細事項が記載されています。

- **証明書**：アプライアンス間に信頼を設定してアプライアンス同士が通信できるようにするために、必要なアプライアンスの信頼ストアに正しい証明書を保存していることを確認します。
- **バックアップファイル**：フェールオーバー設定を開始する前に、アプライアンスをバックアップします。
- **設定の順序**：セカンダリ SMC を設定してからプライマリ SMC を設定します。フェールオーバー設定を保存すると、セカンダリ SMC ドメイン設定が削除されるため、このガイドに記載されている手順、要件、および指示に従ってください。
- **ロールの変更**：プライマリ SMC がオフラインになった場合は、このガイドに示されている順序で SMC のロールを変更してください。順序は重要で、ロールは自動的に交換されません。
- **トラブルシューティング**：解決策については、『Stealthwatch フェールオーバー コンフィギュレーション ガイド』を参照してください。

> ⚠ 正しく設定して運用するには、『Stealthwatch フェールオーバー 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。

プライマリおよびセカンダリのロール

設定の一部として、プライマリ SMC とセカンダリ SMC を割り当てます。設定を保存すると、次の処理が行われます。

- **プライマリ SMC**：プライマリ SMC はそのドメイン設定、ユーザ設定、およびポリシーをセカンダリ SMC にプッシュします。プライマリ SMC では、アプライアンスの管理、アプライアンス設定の変更、パスワードの変更、アラームの定義、ポリシーの適用などを行います。
- **セカンダリ SMC**：セカンダリ SMC は自身の設定を削除します。したがってプライマリ SMC の構成および設定と同期できます。また、セカンダリ SMC がすべてのユーザに対して読み取り専用に変更されます。したがって、セカンダリ SMC のセクションにアクセスすることもセカンダリ SMC からファイルを取得することもできなくなります。

Cisco Security Services Exchange

Cisco Security Services Exchange（SSE）を［外部サービス（External Services）］セクションに追加しました。このオプションはデフォルトで有効になっており、デバイスを SSE クラウドに登録します。自動的に登録するには、スマートライセンスが必要です。または、SecureX の設定ページで手動で登録できます。

> 次の統合では、SSE を有効にする必要があります。
>
> - カスタマー サクセス メトリック
> - SecureX

SecureX 統合の機能強化

Stealthwatch アラームを Threat Response プライベート インテリジェンス ストアに送信するための設定を応答の管理に移行 しました。インシデントとして Threat Response にアラームを送信するには、次の手順を実行します。

1. StealthWatch Management Console にログインします。
2. ［設定（Configure）］>［応答の管理（Response Management）］をクリックします。
3. ［アクション（Actions）］タブをクリックし、［新しいアクションの追加（Add New Action）］>［Threat Response インシデント（Threat Response Incident）］をクリックします。
4. フォームに入力し、［保存（Save）］をクリックします。

詳細については、「応答管理の設定」ヘルプトピックおよび『SecureX 統合ガイド』を参照してください。

> 以前のバージョンの Stealthwatch で Stealthwatch アラームを CTR に送信するように設定した場合は、Threat Response アクションが自動的に作成されます。

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。

プライマリ Admin

マスター管理者ユーザをプライマリ Admin に変更しました。

Stealthwatch CIMC および BIOS ファームウェアアップデート SWU（M5 ハードウェアのみ）

M5 ハードウェアの場合、Stealthwatch アプライアンス v7.3.1 以降用の SWU ファイルを使用して CIMC および BIOS ファームウェアを更新できるようになりました。SWU ファイルは、次の Stealthwatch アプライアンスの UCS C シリーズ M5（x210）ハードウェアに適用されます。

SMC 2210	FC 4210	FC 5200 エンジン	FC 5210 データベース
FS 1210	FS 3210	FS 4210	UD 2210

新しく作成された SWU ファイル update-common-SW7VM5-FIRMWARE-01.swu 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。

「Downloading」

パッチ更新ファイルをダウンロードするには、次の手順を実行します。

1. シスコ ソフトウェア セントラル（https://software.cisco.com）に移動します。
2. [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。
3. [製品の選択（Select a Product）] フィールドに **Stealthwatch** と入力します。Enter キーを押します。
4. 該当するアプライアンスモデルを選択します。
5. [ソフトウェアタイプの選択（Select a Software Type）] の下にある [Stealthwatch パッチ（Stealthwatch Patches）] を選択します。
6. パッチ更新ファイル（update-common-SW7VM5-FIRMWARE-01.swu）をダウンロードし、任意の場所に保存します。

設置

パッチ更新ファイルをインストールするには、次の手順を実行します。

1. SMC 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、[中央管理（Central Management）] をクリックします。
3. [アップデートマネージャ（Update Manager）] をクリックします。
4. [アップデートマネージャ（Update Manager）] ページで [アップロード（Upload）] をクリックし、保存したパッチ更新ファイル（patch-smc-ROLLUP005-7.2.1-03.swu）を開きます。
5. アプライアンスの [アクション（Actions）] メニュー、[更新をインストール（Install Update）] の順にクリックします。

> インストールプロセスには最長で 90 分かかる場合があります。アプライアンスが自動的に再起動します。

詳細については、『CIMC および BIOS ファームウェア アップデート ガイド』を参照してください。

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 7.3.0

障害	説明
SWD-14260	クライアントとサーバ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（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）

障害	説明
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-7655	大規模なシステムでは、タイムアウトにより診断パックの生成が失敗することがあります。	これに対処するには、アプライアンスの SSH コンソールを開き、doDiagPack コマンドを実行します。この操作により、診断パック生成時のタイムアウトを防ぐことができます。診断パックは、/admin/diagnostics フォルダで［ファイルの参照（Browse File）］を使用してダウンロードできます。SCP を使用してボックスからコピーすることもできます。
SWD-8197	FlowSensor は十分なアプリケーションを検出できませんでした。	より正確なアプリケーション分類を実現するため、アプリケーション識別用のサードパーティ製ライブラリを更新しました。この更新により、一部のトラフィックは以前のバージョンで分類されたようには分類されなくなります。さまざまなアプリケーションのサポートも削除されました。サポートされているアプリケーションの更新は、サードパーティ製ライブラリの今後のリリースによって異なります。
SWD-8673	SecureCRT クライアントを ANSI モードで使用している場合、SystemConfig 特殊文字フォントが正しく表示されません。	この問題を解決するには、別のクライアントに接続して、または別のクライアントを使用して、SystemConfig スクリプトを表示するときに、ANSI カラーを無効にします。
SWD-12141	SMC の［システム管理（System Management）］ページを使用して pre-SWU パッチをインストールしても、更新ステータスに［インストールを待機中（Waiting to install）］と引き続き表示されることがあります。	メッセージがクリアされない場合がありますが、更新がブロックされるわけではありません。ログを確認して、pre-SWU パッチが正常にインストールされたことを確認します。『Stealthwatch Update Guide』の確定の手順に従ってください。

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-13089	アプライアンスの IP アドレス、ホスト名、またはネットワークドメイン名の変更に失敗する可能性があります。	アプライアンス設定ツールまたはシステム設定を使用して、アプライアンスの IP アドレス、ホスト名、またはネットワークドメイン名を変更する前に、Stealthwatch オンラインヘルプの手順を確認してください。 手順の一環として、Central Management からアプライアンスを削除します。 同時に、次のことを確認します。 • Central Management からアプライアンスを削除する前に、アプライアンスのステータスに [アップ（Up）] と表示されていることを確認してください。 • Central Management からアプライアンスを削除すると、アプライアンス証明書が SMC から自動的に削除されます。クラスタ内の他のアプライアンスの信頼ストアを確認します。アプライアンスのアイデンティティ証明書（変更しようとしているアプライアンス）が他のアプライアンスの信頼ストアに保存されている場合には、それを削除します。 • アプライアンスの IP アドレス、ホスト名、またはネットワークドメイン名を変更した後、アプライアンス設定ツールを使用して、アプライアンスを Central Management に追加します。

問題番号	説明	回避策
SWD-13154	このソフトウェアアップデートの一環として、Stealthwatch フローコレクタのプロセスを改善しました。更新には、完了までに最大 2 時間かかる場合があります。 クラスタ内の次のアプライアンスを更新する前に、フローコレクタの更新が完了し、アプライアンスのステータスが [アップ(Up)] と表示されていることを確認してください。 **Flow Collector 5000 シリーズ**:エンジンの更新を開始する前に、データベースの更新が完了し、アプライアンスのステータスが Up と表示されていることを確認してください。次に、クラスタ内の次のアプライアンスを更新する前に、エンジンの更新が完了し、アプライアンスのステータスに [アップ(Up)] と表示されていることを確認してください。	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-14039	Stealthwatch 管理コンソールでアプライアンス設定を復元すると、脅威インテリジェンスフィードが無効になります。	1. [集中管理(Central Management)] を開きます。 2. [SMC] > [アクション(Actions)] メニューをクリックします。 3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。

問題番号	説明	回避策
		4. [全般(General)]タブを選択します。 5. [外部サービス(External Services)]セクションで、[脅威インテリジェンスフィードを有効にする(Enable Threat Intelligence Feed]チェックボックスをオンにします。
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-14187	ブラウザは証明書を拒否し、ユーザによるアプライアンスへのアクセスを防止します。	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日付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、次のオプションを試してください。 • 別のブラウザからアプライアンスにログインする。 • アプライアンス アイデンティティ証明書をカスタム証明書に置き換える。手順については、[集中管理(Central Management)]>[アプライアンス設定の編集(Edit Appliance Configuration)]>[アプライアンス(Appliance tab)]>[SSL/TLS アプライアンスID(SSL/TLS Appliance Identity]を参照し、オンラインヘルプを選択してください。 • Cisco Stealthwatch サポートに連絡してください。
SWD-14800	v7.2.0 にアップグレードすると、Stealthwatch Cloud ダッシュボードは登録ページへリダイレクトされます。	Stealthwatch Cloud ダッシュボードに移動するように求められたら、Stealthwatch Cloud のクレデンシャルを入力します。

問題番号	説明	回避策
SWD-14815	管理 UI から Docker サービスが削除されているため、[ホスト検索（Host Search）] を実行する際の、フロー集約サービスに関する Web UI の警告は正確ではありません。	15 分待ってから、この操作を再試行してください。問題が解決しない場合は、Cisco Stealthwatch サポートまでお問い合わせください。
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、集中管理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-14860	Vertica Backup Restore（VBR）はサポートされていません。	バックアップまたは復元に Vertica を使用しないでください。データが永久に失われる可能性があります。
SWD-14940	DBNode Retention Manager は、長いデータベースバックアップ期間中にパーティションをドロップします。	データベースのトリミングやバックアップ後のスナップショットの削除など、データベースをバックアップする手順が追加されました。必ず Stealthwatch® 更新ガイド v7.1.x ～ v7.2 の手順に従ってください。 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。
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。
SWD-15550	暗号スイートライブラリが更新されたため、Cisco ISE リリース 2.4.0.357 – 累積パッチ 10+ で Stealthwatch v7.3.0 に接続できません。（LSQ-5068）	この問題は今後の ISE パッチで修正する予定です。ISE リリース 2.4.0.357 – 累積パッチ 9 のままにするか、ISE リリース 2.6 にアップグレードするか、または Stealthwatch v7.3.0 にアップグレードしないことを推奨します。
SWD-15570	フローコレクタのスナップショットを削除するコマンドの誤記	データベースのバックアップ指示に含まれているフローコレクタのスナッ

問題番号	説明	回避策
		プショットを削除するコマンドが、ヘルプおよび更新ガイドでは正しくありません。 次のコマンドを使用して、SMC およびフローコレクタのデータベースのスナップショットを削除します。 `/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot ('StealthWatchSnap1');"` また、SMC とフローコレクタのデータベースのスナップショットを削除してください。
SWD-15623	SMC/フローコレクタデータベースのデータの取得エラー	データベースのバックアップ指示に含まれているフローコレクタのスナップショットを削除するコマンドが、ヘルプおよび更新ガイドでは正しくありません。 次のコマンドを使用して、SMC およびフローコレクタのデータベースのスナップショットを削除します。 `/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot ('StealthWatchSnap1');"` また、SMC とフローコレクタのデータベースのスナップショットを削除してください。
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、この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	TBD	最初のバージョン
2_0	2020 年 9 月 8 日	• 必須パッチのための「更新後」セクションを追加しました。 • SWD-15570 を「既知の問題」に追加しました。 • GA の日付を追加しました。
2_1	2020 年 9 月 28 日	• 新着情報に「プライマリ Admin」セクションを追加しました。 • 「ユーザパスワード検証の要件と機能強化」セクションを更新しました。 • 「既知の問題」の SWD-15570 を更新しました。 • SWD-15623 を「既知の問題」に追加しました。
3_0	2021 年 2 月 4 日	• 新着情報に「Stealthwatch CIMC および BIOS ファームウェアアップデート SWU（M5 ハードウェアのみ）」セクションを追加しました。
3_1	2021 年 2 月 19 日	3 番目の小数点位置を含むようにポイントリリース番号を更新しました。
3_2	2021 年 3 月 3 日	GA リリース日を更新しました。

リリースサポート情報

リリース 7.3.0 の公式一般公開（GA）日は 2020 年 9 月 3 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