Cisco Stealthwatch

リリースノート v7.3.1

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。Stealthwatch v7.3 に含まれているすべての機能については、以前のバージョン（v7.3.0）のリリースノートを参照してください。

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.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 7.3.1 に更新するには、アプライアンスにバージョン 7.2.1 または 7.3.0 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）] > [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、「**証明書の失効**」を参照してください。

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。

証明書チェック

v7.3.1 へのアップグレードには、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 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。Central Manager の信頼ストアに証明書の完全なチェーンがあることを確認します。

> ⚠ 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 v7.3.1 への更新は失敗します。

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、必ずレポートビルダーアプリ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(v7.3.1)』を参照してください。

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-ROLLUP001-7.3.1-01.swu 以降
- patch-fcnf-ROLLUP001-7.3.1-01.swu 以降
- patch-fcsf-ROLLUP001-7.3.1-01.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 v7.3.1 リリースの新機能と改善点は次のとおりです。

仮想アプライアンス導入サポートの更新

vSphere vCenter を介した ISO 導入の追加により、仮想アプライアンスのサポートが改善されました。バージョン 7.3.1 以降では、仮想アプライアンス OVF の導入は廃止されています。

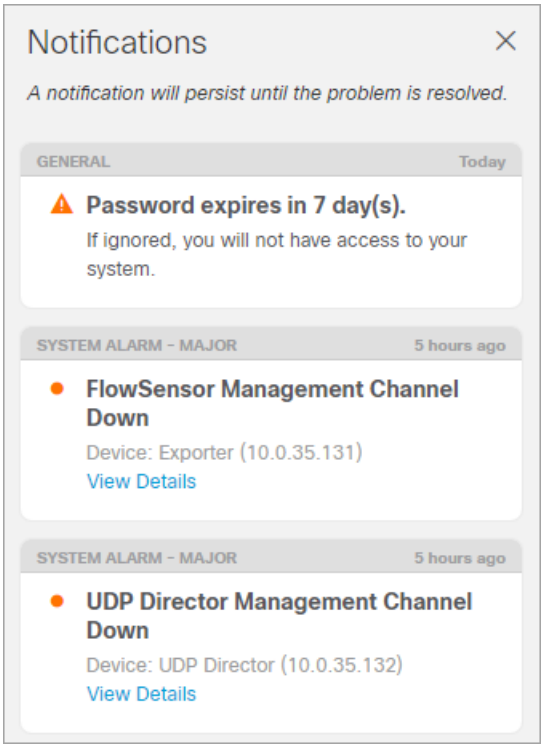
プライマリ Admin

マスター管理者ユーザをプライマリ Admin に変更しました。

システム通知

システム通知の機能によって、全般的なアラームやシステムアラームがある場合は即座にユーザに通知されます。任意のページの、右上隅にあるツールバーの 10 (**アラート**)アイコンの横に表示される数字は、通知があることを表しています。数字はメッセージの件数を示します。アラームが非アクティブの状態になると、[アラート(Alert)]アイコンの数字には反映されなくなります。

[通知(Notifications)]パネルを表示するには、[アラート(Alert)]アイコンをクリックします。ページの右側に[通知(Notifications)]パネルがスライドして表示されます。



[通知(Notification)]パネルに表示される主な通知カテゴリには、[全般的(General)]と[システムアラーム(System Alarms)]の 2 つがあります。

全般

[全般(General)]の通知タイプは、次の 2 つのサブタイプに分類されます。

スマート ライセンス

- **評価期間切れ** 評価期間が切れました。フローの収集は停止し、UDP Director はフローの転送を停止しています。フロー収集を再度開始するには、製品インスタンスを登録します。
- **許可の期限切れ** Stealthwatch が Cisco スマートアカウントとの通信を失うと、許可が期限切れになる場合があります。[許可の期限切れ(Authorization Expired)] は、通信ステータスを示します。ライセンスのステータスを示すものではありません。
- **コンプライアンス違反** アプライアンスまたは機能のライセンスが不足していて、Cisco スマートアカウントに割り当てられているよりも多くのライセンスを使用しています。

システム通知とスマートライセンシングの詳細については、『Stealthwatch Smart Software Licensing Guide』を参照してください。

パスワードの有効期限切れ

[パスワードが期限切れになるまでの期間(Password Expires After)] の値になるまでは、この数字は 10 日のまま変化しません。

システムアラーム

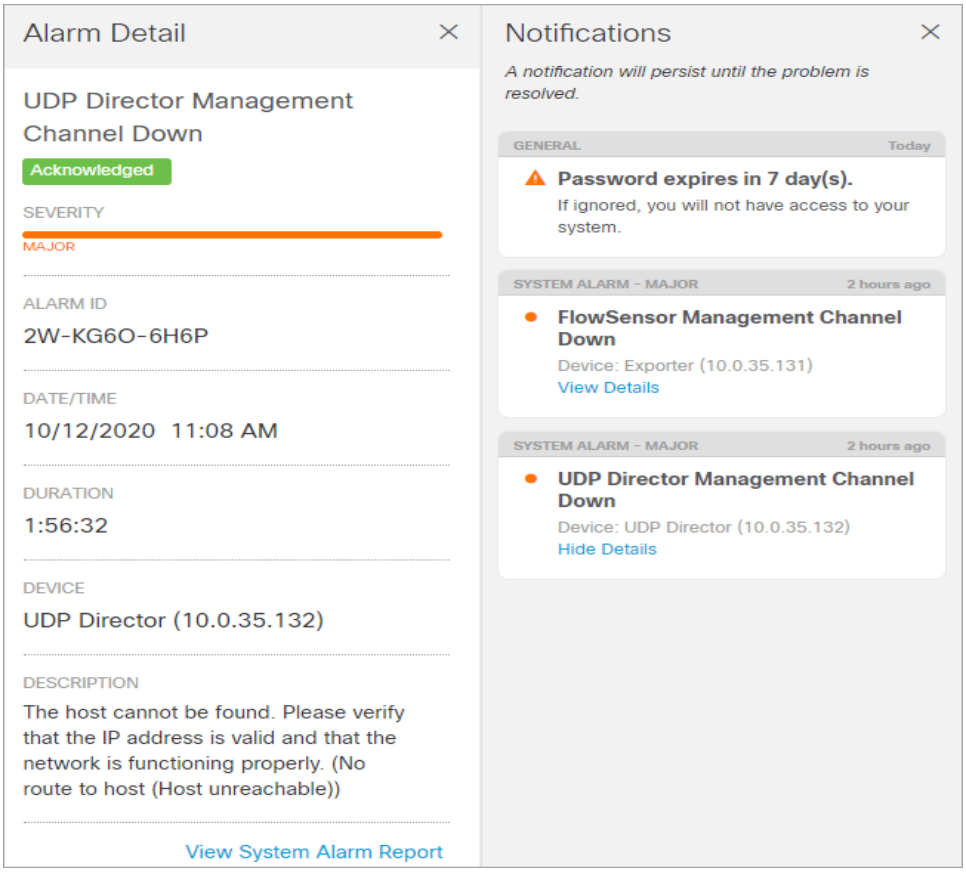
ユーザは、[通知(Notifications)] パネルで次のアラームタイプのサブセットを表示できます。

- データストア
- Flow Collector
- フローセンサー
- SMC
- UDPD

> データストアのアラームは、データストアを展開した場合にのみ機能し、SMC システムアラームのサブセットとして表示されます。

アラームの詳細

あるシステムアラームの詳細を表示するには、該当するシステムアラームの下にある [詳細の表示（View Details）] をクリックします。[アラームの詳細（Alarm Detail）] パネルが [通知（Notifications）] パネルの横に開きます。



データ ストア バーチャル エディション

バージョン 7.3.1 では、2021 年 1 月 4 日から利用可能になったデータ ストア バーチャル エディションが導入されています。SMC VE および 1 つ以上の Flow Collector VE で 3 つのデータ ノード バーチャル エディションを導入できます。機能は、ハードウェアデータストアと同じです。データストアを使用した仮想アプライアンスの導入については、『Stealthwatch Virtual Edition (with a Data Store) Installation Guide』を参照してください。データ ストア バーチャル エディションの導入の初期化および完了については、『Stealthwatch Data Store Virtual Edition Installation and Configuration Guide』を参照してください。

Data Store VE を導入する場合は、仮想 SMC および仮想フローコレクタとともに導入する必要があります。同様に、ハードウェア Data Store 6200 を導入する場合は、ハードウェア SMC 2210 およびハードウェアフローコレクタ 2210 とともに導入する必要があります。ハードウェアアプライアンスではデータ ストア バーチャル エディションを展開できません。また、仮想アプライアンスではハードウェアデータストア 6200 を展開できません。

データストア初期化の簡素化

バージョン 7.3.1 では、データストアの初期化が簡素化されました。アプライアンスからスクリプトを手動で実行するのではなく、SystemConfig ユーティリティを使用してハードウェアと仮想データストアの両方の初期化を実行できます。

さらに、Data Store を最初に導入して初期化した後に追加の SMC、フローコレクタ、またはデータノードを取得した場合は、これらの新しいアプライアンスを追加するスクリプトを手動で実行するのではなく、SystemConfig ユーティリティを使用して追加できます。詳細については、『Stealthwatch Data Store Installation and Configuration Guide』の「メンテナンス」のセクションを参照してください。

ユーザパスワードの機能拡張

パラメータの再利用

[パスワードポリシー(Password Policy)]フィールドの [許可されていない以前のパスワードの数(Number of previous passwords disallowed)]には、最小値 3 と最大値 24 が必要になりました。デフォルト値は 12 です。

パスワードの有効期限のワークフロー

ユーザのパスワードが期限切れになると、ログイン時にパスワードの変更が求められず、アクセスが無効になります。ユーザは、パスワードをリセットするために Stealthwatch 管理者に連絡する必要があります。

> スタンドアロン アプライアンスのユーザのパスワードは、Stealthwatch 管理者が削除して再作成する必要があります。

次のユーザは、パスワードの有効期限が切れてもアクセスが無効になりません。

- デフォルトの Stealthwatch 管理者
- root および sysadmin ユーザ
- リモートユーザ

パスワード強度メーター

次の動作によるパスワード強度メーターが [パスワード(Password)]フィールドに追加されました。

- メーターは、強、可、中、弱を表示します。
- パスワードが弱の場合でも、ユーザはパスワードを保存できます。
- [パスワードの生成(Generate Password)]は、強力なパスワードを作成します。

シスコのバンドル

> ⚠ 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 v7.3.1 への更新は失敗します。詳細については、証明書チェックのセクションを参照してください。

シスコでは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バンドルとして定期的にリリースしています。このバンドルはすべてのアプライアンスおよび Stealthwatch v7.3.1 以降に適用される、共通のアプライアンスパッチ SWU ファイルとしてリリースされます。

各パッチには、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。また、コア証明書用と外部証明書用の各バンドルの内容に関する情報を記載した 2 つのテキストファイルも提供しています。

このバンドルとテキストファイルは、https://software.cisco.com [英語] の Software Central からダウンロードできます。

> ℹ
> - すべてのアプライアンスに最新のシスコバンドルパッチをインストールする必要があります。
> - アプライアンスのイメージを更新すると、シスコのバンドルパッチはリリース配布元の CA に返却されます。パッチの返却後は最新のバンドルに更新する必要があります。

ERSPAN のカプセル化解除

カプセル化リモート スイッチ ポート アナライザ（ERSPAN）のカプセル化解除は、フローセンサーで可能です。このオプションを使用すると、フローセンサーがパケット内の ERSPAN ヘッダーを検出し、ヘッダーのカプセル化を解除して、内部パケットの内容を処理します。

この機能を有効にするには、フローセンサーにログインし、[設定（Configuration）] > [詳細設定（Advanced Settings）] の順に移動します。

> ℹ FS 4210 の ERSPAN のカプセル化解除はサポートされていません。

エンドポイントライセンスの機能強化

エンドポイントライセンスでは、NetFlow を照合する必要なく、ネットワーク内の任意の場所のエンドポイントをモニタできるようになりました。さらに、エンドポイント コンセントレータは最大 60K FPS をサポートするようになりました。

この機能の設定方法の詳細については、エンドポイント コンセントレータ および NVM のコンフィギュレーション ガイドを参照してください。

脅威インテリジェンスフィードと Cisco Talos IP ブロックリスト統合

Talos IP ブロックリストは、脅威インテリジェンスフィードでコマンド アンド コントロール サーバのホストグループとして提供されます。Talos データセットには、Talos の信頼できない脅威レベルの CIDR IP アドレスのリストが含まれます。

フローセンサー VE 10 G NIC サポート

フローセンサー VE に 2 つの NIC 設定サポートが追加されました。

NIC：モニタリングポート	必須の予約済み CPU	必須の最小予約済みメモリ	予測されるスループット	フローキャッシュサイズ（同時フローの最大数）
1 X 10 Gbps *	12	24	8Gbps PCI パススルーとして設定されている 10 G インターフェイス（インテル ixgbe/ixgbe 準拠）	512 K
2 x 10 Gbps *	22	40	16 Gbps PCI パススルーとして設定されている 10 G インターフェイス（インテル ixgbe/ixgbe 準拠）	1M

* 10 Gbps スループットの場合、すべての CPU を 1 つのソケットに設定します。詳細については、『Stealthwatch Virtual Edition (VE) Installation Guide v7.3』を参照してください。

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。

証明書の失効

一部のブラウザでは、SSL/TLS 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、一時的な解決策として別のブラウザからアプライアンスにログインします。

証明書の有効期限を更新するには、次を参照してください。

- **Cisco Stealthwatch 証明書**：Stealthwatch バージョン 7.x アプライアンスはそれぞれ、5 年間有効の固有の自己署名アプライアンス アイデンティティ証明書と一緒にインストールされます。Cisco Stealthwatch アプライアンス アイデンティティ証明書を置き換えるには、管理対象アプライアンスの SSL/TLS 証明書ガイド v 7.3の手順に従います。これらの手順を使用して、アプライアンスホスト情報（IP アドレス、ホスト名、ドメイン名）を変更せずに有効期限を更新できます。
- **カスタムSSL/TLS証明書**：アプライアンスが認証局からのカスタム SSL/TLS 証明書を使用している場合は、『SSL/TLS Certificates for Managed Appliances Guide v7.3』を参照して、アプライアンスのアイデンティティ証明書を置き換えます。

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。そのため、Stealthwatch のコアリリースとリンクさせなくても、必要に応じて Stealthwatch アプリケーションを更新できます。

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

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 7.3.1

障害	説明
SWD-15072	SMCで syslog-ng ファイルのモニタ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）

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)
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。

問題番号	説明	回避策
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	2020 年 12 月 11 日	最初のバージョン
1_1	2021 年 1 月 29 日	データストア情報を更新し、M5 ハードウェア更新 SWU のためのセクションを追加。
1_2	2021 年 2 月 4 日	必要な SMC パッチのため、「更新後」セクションを追加。
1_3	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。
1_4	2021 年 3 月 3 日	SWD-16145（LSQ 4718）を、「修正点」セクションのバージョン 7.3.1 の表に追加しました。
1_5	2021 年 3 月 11 日	「エンドポイントライセンスの機能強化」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 v7.3.1 の公式一般公開（GA）日は 2021 年 2 月 4 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