Cisco Stealthwatch

リリースノート 7.1.2

目次

はじめに

概要

本書では、Stealthwatch System v7.1.2 リリースの新機能および改善点、バグ修正、および既知の問題について説明します。Stealthwatch System の詳細については、Cisco.com をご覧ください。Stealthwatch v7.1 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（v7.1.1）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。

ほとんどのアプライアンスは SMC で管理されます。SMC で管理されないエンドポイント コンセントレータなどのアプライアンスは、「スタンドアロン アプライアンス」と呼ばれています。

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 v7.0.x ～ v7.1.2 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 7.1.2 に更新するには、アプライアンスに 7.0.0 以降のバージョン 7.0.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、ソフトウェアバージョンごとに、アプライアンスに最新の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。Stealthwatch 更新ガイド v7.0 ～ v7.1.2 の手順に従ってください。詳細については、Stealthwatch のダウンロードおよびライセンス センター https://stealthwatch.flexnetoperations.com [英語] にログインして確認してください。
- **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 v6.9.x を使用している場合は、各アプライアンスを v6.9.x から v6.10.x に更新してから、6.10.x を 7.0.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 以降が必要です。
- 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。

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。

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 ハードウェア インストレーション ガイドを参照してください。https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html
- **iDRAC Enterprise（Dell アプライアンス）**：ご使用のプラットフォームの最新のマニュアルを参照してください。iDRAC Enterprise にはライセンスが必要です。また、iDRAC Express ではコンソールアクセスを利用することはできません。iDRAC Enterprise をお持ちでない場合は、コンソールまたは SSH での直接接続をお使いください。
- **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。

仮想マシン

- **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。

その他 のオプション

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。

Central Management での SSH の有 効 化

SSH を開く

次の手順に従って、選択したアプライアンスの SSH を開きます。

1. [一元管理(Central Management)] > [アプライアンスマネージャ(Appliance Manager)] を開きます。
2. 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。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [**アプライアンス**(Appliance)] タブを選択します。

SSH の有 効 化

1. [SSH] セクションを見つけます。
2. 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。

3. [設定の適用(Apply settings)] をクリックします。
4. 画面に表示される指示に従って操作します。

> ⚠ 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。

アプライアンス管 理 インターフェイスでの SSH の有 効 化

次の手順に従って、選択したアプライアンスの SSH をアプライアンス管理インターフェイスを使用して開きます。

1. アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)] > [サービス(Services)] の順にクリックします。

3. [SSHの有効化(Enable SSH)]チェックボックスをオンにしてSSHへのアクセスを許可します。
4. ルートへのアクセスも許可するには、[ルートSSHアクセスの有効化(Enable Root SSH Access)]チェックボックスをオンにします。
5. [適用(Apply)]をクリックします。

> ⚠ 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。

SWD-13346のエクスポータの特定と削除

SWD-13346のCPUの負荷を軽減するため、次の手順を実行して、エクスポータを特定し削除します。

> ⚠ 次の手順を確認してください。この問題がお客様の環境に影響しているかどうかが不明な場合や、関連している可能性のあるエクスポータの特定に対する支援については、Stealthwatch カスタマーサポートまでお問い合わせください。

1. この問題に対処するためにtomcatを定期的に再起動する目的で作成された外部cronジョブを削除します(該当する場合)。
2. Stealthwatch 更新ガイド v7.0.x ～ v7.1.2を使用してこのリリースをインストールします。インストールが完了したら、ステップ3に進みます。
3. いずれかのエクスポータにIDエクスポータとしてフラグが設定されているかどうかを確認するには、次のコマンドを使用して、SMCのコマンドライン インターフェイスにログインします。

   ```
   #grep 'identity-source="true"'
   /lancope/var/smc/config/domain_*/exporter*.xml
   ```

   例:#grep 'identity-source="true"' /lancope/var/smc/config/domain_*/exporter.xml*
   /lancope/var/smc/config/domain_102/exporter_1855_192.168.1.1.xml:<exporter
   ip="192.168.1.1" exporter-type="exporter" identity-source="true">

   疑わしいエクスポータは、エクスポータの行の末尾に[ID]フィールドがないことで識別できます(上の例を参照)。

   新しく生成されたXMLがどのように表示されるか、一例を下に示します。

   例:<exporter ip="192.168.1.1" exporter-type="exporter" identity-source="true"
   id="1">

   ファイルが特定された場合には、ステップ4に進みます。ファイルが特定されなかった場合、それ以上のアクションは必要ありません。

4. 次のコマンドを使用してtomcatプロセスを停止し、削除できるようにします。

   ```
   #systemctl stop lc-tomcat.service
   ```

5. ステップ3のファイル出力のリストを参照し、次のコマンドを使用して削除します。

   ```
   #rm -f <path_to_xml_file>
   ```

6. ステップ 3 で見つかったエクスポータからフローを受信するフローコレクタのコマンド ライン インターフェイスにログインします。同じエクスポータを .xml ファイルから手動で削除します。
   a. フローコレクタエンジンを停止して、次のコマンドを使用します。
      `>systemctl stop engine.service`
   b. 次のコマンドを使用して、フローコレクタの設定ディレクトリに移動します。
      `>cd /lancope/var/sw/today/config`
   c. exporters.xml のバックアップコピーを作成します。
      `>cp exporters.xml /lancope/var/exporters.xml.bak`
   d. ステップ 3 で見つかったエクスポータを削除するには、vi または任意のエディタを使用します。特定のエクスポータスタンザの表示例を以下に示します。疑わしい IP を検索し、[エクスポータ(exporter)] タグ間のコンテンツを削除します。完了したら、必ずファイルを保存してください。

      例 : <exporter ip="192.168.1.1">
      <interface if-index="1" active="1" speed-in="1000000000" speed-out="1000000000" threshold-in="90" threshold-out="90"/>
      </exporter>

7. 次のコマンドを使用して、フローコレクタエンジンを再起動します。

   ```
   #systemctl start engine.service
   ```

8. 次のコマンドを使用して、SMC SSH コンソールに戻ります。

   ```
   #systemctl start lc-tomcat.service
   ```

9. 両方のコンソールからログアウトします。これらの変更により、ID タイプアプライアンスに関連したエクスポータ コンフィギュレーション ファイルの再作成が可能になります。

新しい設定ファイルが正しくフォーマットされ、この問題が原因で発生していた CPU の負担が軽減されます。

更新後

アプライアンスを更新した後、必要な次のパッチをインストールしてください。

- patch-smc-ROLLUP002-7.1.2-02.swu 以降

詳細については、Stealthwatch ダウンロードおよびライセンスセンター(Stealthwatch Download and License Center)にあるパッチの readme ファイルで確認してください。

新着情報

Stealthwatch System v7.1.2 リリースの新機能と改善点は次のとおりです。

新しいアラーム

エクスポータアラーム

誤って設定されたエクスポータ（LSQ-3372）の識別に役立てるため、フローコレクタの最長エクスポート超過アラームを追加しました。このアラームは、エクスポータからのフロー期間がしきい値設定を超えた場合にトリガーされます。修正されない場合は、不正確なフローとインターフェイスの統計情報が生成されます。

このアラームは［フローコレクタプロパティ（Flow Collector Properties）］ダイアログで有効/無効にできます。

Cisco Threat Response の統合

Cisco Threat Response（CTR）は、複数の製品やソースから集約されたデータを使用して、脅威を検出、調査、分析し、脅威に対応するために役立つ Cisco Cloud のプラットフォームです。

この統合によって、Cisco Threat Response ピボットメニューの使用、SMC アプライアンス UI の Cisco Threat Response 事例集の使用、Stealthwatch アラームの Cisco Threat Response への送信が可能になり、調査プロセスの際に CTR が Stealthwatch 環境からセキュリティイベントに関する情報を取得できるようになります。

詳細については、Cisco Stealthwatch と Threat Response の統合ガイドを参照してください。

TACACS+

Terminal Access Controller Access Control System（TACACS+）は、認証および認可サービスをサポートし、ユーザが 1 つのクレデンシャルセットを使用して複数のアプリケーションにアクセスできるようにするプロトコルです。Stealthwatch の TACACS+ を設定するには、『TACACS+ Configuration Guide』の手順に従ってください。

- **ユーザ名**：すべてのユーザ名が一意であることを確認してください。
- **ユーザロール**：許可されたユーザのログインの場合、各ユーザに ID グループを割り当て、各 ID グループにシェルプロファイルを設定します。各シェルプロファイルに対して、マスター管理者のロールを割り当てたり、管理者以外のロールの組み合わせを作成したりすることもできます。管理者以外のロールの組み合わせを作成する場合には、要件を満たしていることを確認してください。

以前のバージョン

以前のバージョンの Stealthwatch（v7.1.1 以前）で TACACS+ を設定している場合には、Stealthwatch v7.1.2 で一意の名前を持つ新しいユーザを作成してください。以前のバージョンの Stealthwatch でのユーザ名を使用したり複製したりすることは推奨されません。詳細については、『TACACS+ Configuration Guide』を参照してください。

TACACS+ とISE

Stealthwatch v7.1.2 では、Cisco Identity Services Engine（ISE）を使用して TACACS+ を設定できます。この設定により、ISE 上の TACACS+ ユーザは、自分の TACACS+ クレデンシャルを

使用して Stealthwatch にログインできるようになります。

- ご使用のエンジンに関する ISE マニュアル記載の手順に従って、ISE をインストールして設定します。
- 『TACACS+ Configuration Guide』記載の手順に従って、TACACS+ を設定します。『TACACS+ コンフィギュレーション ガイド』記載の手順に従って、ISE にログインし、TACACS+ ユーザを設定します。

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、コグニティブリリースノート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 の問題（SWD、LSQ、または LVA）番号が示されています。

バージョン 7.1.2

障害	説明
SWD-11995	SWU ファイルアップロードの際のストレージ不足に関する新しいエラーメッセージを追加します。
SWD-12307	セキュリティグループタグ（SGT）が正しく反映されず、SGT を 0 にリセットできず、サブジェクト信頼セキュリティ名（SGN）がフローテーブルに表示されない問題を修正しました。（LSQ-3881）
SWD-12341	フローコレクタエンジンが再起動した後、「today」の前にアーカイブされたすべてのフォルダが削除される原因となったエラーを修正しました。（LSQ-3864）
SWD-12456	従来は、アドレススキャンによりリスクインデックスに 4,000 ポイントが追加され、イベントが発生するたびに「ヒットカウント」と呼ばれる数字が追加されていました。「ヒットカウント」とは、イベントが発生した回数のことです。この仕様は、イベントが発生したときに 4,000 ポイントのみを追加して「ヒットカウント」を追加しないように変更されました。現在はマニュアルの記載と一致しています。（LSQ-3701）
SWD-12460 SWD-12689	事前に定義されたフィルタを使用して、バイトの少数部を切り捨てて丸め処理します。（LSQ-3868）
SWD-12491	メモリと DB 両方の「合計」レコード数が上限に設定された数を超え、セキュリティ イベント トランザクション レポートに「more records available」メッセージが表示された場合に限り、フローコレクタエンジンで [hasMore] を true に設定する必要があります。（LSQ-3995）
SWD-12648	無効なタイムスタンプを持つデータが（毎日）DB に書き込まれる原因となった問題を修正しました。（LSQ-4057）
SWD-12670	MAC 違反アラームが適切に生成されるようになりました。（LSQ-4062）
SWD-12678	マージされた export_delay のデフォルト値が 6.10 から 7.x に変更されます。古いコンフィギュレーション XML ファイルが存在する場合、このデフォルト値が、FS エンジンの起動時に新しいデフォルトとして設定されます。（LSQ-4107）

障害	説明
SWD-12679	SNMP トラップで、「FlowCollector データベースチャネルダウン」に対して正しい MIB が使用されるようになりました。(LSQ-4051)
SWD-12712	FC4K の FPS レートが 400K よりも高いときに tomcat のクラッシュが発生する問題を修正しました。
SWD-12724	フローコレクタエンジンが不正な形式の「username」フィールド値を security_event に書き込み、それにより Vertica 解析エラーが発生するエラーを修正しました。(LSQ-4117)
SWD-12996	エンドポイント コンセントレータ管理 UI でフィルタ処理および表示される新しい Docker サービスが追加されました。(LSQ-4165)
SWD-13000	Stealthwatch デスクトップクライアントが、ライセンスのためにフローコレクタおよびセカンダリ SMC と通信しないエラーを修正しました。(LSQ-4129)
SWD-13096	SMC インベントリからフローコレクタを削除するとサマリーデータが失われることをユーザに通知する警告ダイアログが追加されました。
SWD-13097	FC のアップグレード後に、FCDB でライセンスエラーが発生し、フローがドロップされる問題を修正しました。(LSQ-4224)
SWD-13123	SSO の設定によって「AccessDeniedException」エラーが発生する問題を修正しました。(LSQ-4518、LSQ-4594)
SWD-13235	API コールによるエクスポータ SNMP 設定の更新に関する問題を修正しました。(LSQ-4277)
SWD-13257	検索パラメータに基づくホストグループ名のフィルタリングを変更しました。(LSQ-4185)
SWD-13284	nginx access.log を含めるように診断パックを更新しました。(LSQ-4232、LSQ-4241、LSQ-4308)
SWD-13299	デフォルトの新規/最大フローに対するイベント ID チェックを追加しました。(LSQ-4359)
SWD-13301	上位ポートから上位ホストへのピボット時のフィルタ作成ロジックを追加しました。(LSQ-4360)
SWD-13311	ドメインのすべての設定をエクスポートできない問題を修正しました。(LSQ-4422)
SWD-13315	設定の復元を実行すると Google Analytics が無効になる問題を修正しました。

障害	説明
SWD-13316	504 ゲートウェイのタイムアウトにより再同期が失敗して、セカンダリ SMC で設定チャネルがダウンする問題を修正しました。(LSQ-4333)
SWD-13321	[ホストレポート(Host Report)] ページにパワーアナリストによるホスト分類機能がない問題を修正しました。(LSQ-4493)
SWD-13342	設定の復元を実行すると Customer Success Metrics が無効になる問題を修正しました。
SWD-13346	ID エクスポータの間違った分類が原因で SMC での CPU 平均負荷が上昇することに関連した問題を修正しました。(LSQ-4221) ⚠ この問題が原因で通常の CPU 平均負荷よりも高くなっている場合には、このリリースをインストールしてから、エクスポータの XML ファイルを正しく再生成するための付加的なアクションを完了する必要があります。エクスポータの特定と削除の手順を確認してください。この問題がお客様の環境に影響しているかどうかが不明な場合や、関連している可能性のあるエクスポータの特定に対する支援については、Stealthwatch カスタマーサポートまでお問い合わせください。
SWD-13353	ダッシュボードがプライマリ SMC のみに表示される問題を修正しました。
SWD-13408	GETBULK 関数の使用が SNMPV1 でサポートされない問題を修正しました。(LSQ-4407)
SWD-13454	フェイクアプリケーション アラームが発生しないように、INSTANT_MESSAGING フィルタに ICLOUD と OFFICE365 を追加しました。(LSQ-4293)
SWD-13461	7.1.1 へのアップグレードがインストールログに表示されない問題を修正しました。(LSQ-4447)
SWD-13521	中間証明書の失効チェックを追加しました。
SWD-13637	保存済みの SNMP プロファイル設定にポーリングを繰り返す間隔が適用されない問題を修正しました。(LSQ-4481)
SWD-13721	SNMP ポーリングが CPU 使用率を上昇させている問題を修正しました。(LSQ-4265) 最適なシステムパフォーマンスを実現するには、SNMP ポーリングの間隔を 24 時間に設定します。
SWD-13722	デスクトップクライアントで実行中のフロークエリに関する問題を修正しま

障害	説明
	した。(LSQ-4520)
SWD-13731	FlowAggregator がすべての利用可能な Vertica セッションを使用し、データベースを無効にしていた問題を修正しました。
SWD-13796	プロセス制御ブロックコードが初期化前に参照されていた問題を修正しました。(LSQ-4512)
SWD-13801	フェールオーバーの確立時に tomcat が不安定になる原因だったキャッシュ更新の問題を修正しました。
SWD-13802	enforce-root-login サービスを処理するための新しいスクリプトを追加しました。(LSQ-4476)
SWD-13810	akka-http クライアントではなく apache http クライアントを使用するための「sw-flow-aggregator」サービスを更新しました。(LSQ-4534)
SWD-13881	『the Installation and Configuration Guide』を更新し、統合 Windows 認証 (IWA) で SSO がサポートされないことを内容に含めました。
SWD-13915	デスクトップクライアントのロードに時間がかかりすぎる問題を修正しました。(LSQ-4636)
SWD-13941	過剰なアラームを減らすためにサービス定義 XML を更新しました。(LSQ-4631)

バージョン 7.1.1

障害	説明	詳細情報
LVA-1248	Linux カーネルが更新されました。	CVE-2019-3846 CVE-2019-5489 CVE-2019-10126 CVE-2019-11477 CVE-2019-11478 CVE-2019-11479 CVE-2019-11810 CVE-2019-11833 CVE-2019-11884

障害	説明	詳細情報
SWD-12014	次のメッセージの原因となった問題を修正しました。SMC FailoverSession resync failed: 504 Gateway Time out on sendSnapshot.	LSQ-3853 LSQ-4218
SWD-12031	エンタープライズツリーから FlowSensor VM サーバ名情報を削除しました。	LSQ-3859
SWD-12150	フロー関連アラームのスケール値 1000 が削除されました。	LSQ-3948
SWD-12989	比較的大規模な SMC 設定バックアップファイルのダウンロードに失敗する問題を修正しました。	LSQ-4132

バージョン 7.1.0

障害	説明
LVA-625	ファイルとディレクトリのアクセス権をより限定的になるように更新しました。(LSQ-3719)
LVA-626	サーバ情報を非表示にするため、server.xml に値タグが追加されました。(LSQ-3720)
SWD-8351	[フロー収集のトレンド(Flow Collection Trend)] グラフの x 軸の時間値を修正しました。(LSQ-3748)
SWD-9749	サイバー脅威ドキュメントの生成に失敗しました。(LSQ-3311) ドキュメントを設定またはスケジューリングする場合には、[空のファイルを抑制する(Suppress Empty File)] チェックボックスをオンにします。
SWD-10546	SMC が設定変更を送信する前に、フローコレクタエンジンが起動していることを確認するためのチェック項目が追加されました。(LSQ-3466)
SWD-10971	ペイロードとユーザ名によるフローテーブルのフィルタリングは、500 内部サーバエラーで失敗します。(LSQ-3630) フローテーブル filter xml のシーケンスの問題を修正しました。
SWD-10995	必要に応じて設定ファイルに対する権限を変更するため、フローコレクタを更新しました。(LSQ-3624)
SWD-11013	プライマリ SMC 上のドメインを削除しましたが、フェールオーバーペア

障害	説明
	のセカンダリ SMC からは削除されませんでした。（LSQ-3479） 選択したドメインの設定済みコールリスト全体が、ドメインの削除時にセカンダリ SMC に送信されます。
SWD-11286	ドキュメントでサポートされている VMware バージョンが更新されました。（LSQ-3662）
SWD-11310	特殊文字 | を受け入れるように、ファイル共有パスワードのフィールドが更新されました。（LSQ-3665）
SWD-11311	[フロー検索（Flow Search）] ページの [情報カテゴリとピア（Subject and Peer）] の [ユーザの詳細（User details）] フィールドが更新され、ユーザ名に特殊文字とワイルドカード文字を使用できるようになりました。（LSQ-3667）
SWD-11379	/lancope/admin/lib/system.xsd. の ST_Value パターンにおけるアンダースコアのサポートが追加されました。（LSQ-3678）
SWD-11673	SNMP MIB で複数のオブジェクトタイプを文字列から整数に修正し、新しくインストールされたシステムで変数の処理を追加しました。（LSQ-3694）
SWD-11833	ユーザのリスクインデックスアラームを選択する際にアラームが見つからなかった問題を修正しました。（LSQ-3778）
SWD-11861	[ホストグループトレンド（Host Group Trends）] テーブルで [ICMP 名（ICMP Name）] 列のラベルとツールのヒントが修正され、[送信済みICMPパケットの平均（Average ICMP Packets Sent）] が表示されるようになりました。（LSQ-3786）
SWD-11925	カスタム セキュリティ イベント設定における検証の問題を修正しました。（LSQ-3800）
SWD-11961	偽のアプリケーションアラームが何度も発生しないようにするため、詳細設定を追加して最初の NBAR アプリケーション ID のみをフローに設定できるようにしました。無効にするには、フローコレクタで allow_nbar_app_id_migration を 1 に設定します。（LSQ-3789）
SWD-11991	以前に作成した応答管理ルールを編集できない問題を修正しました。（LSQ-3847）
SWD-12010 SWD-12044	カスタムアプリケーションを含む application_definitions.xml でポート定義を使用するようにエンジンが強化されました。ポート定義を使用してカスタムアプリケーションが定義されている場合、エンジンがフロー内のクライアント/サーバ関係を決定する際に、これらの定義が使用されるようになりまし

障害	説明
	た。（LSQ-3824）
SWD-12071	[アラーム発行ホスト（Alarming Hosts）] ウィジェットがデータのロードに失敗する問題を修正しました。（LSQ-3785）
SWD-12074	UDP Director の転送ルールをユーザが編集できない問題を修正しました。（LSQ-4184）
SWD-12078	フローレコードで「start_time」が変更されていない場合、34 日間以上フロー期間が表示されていた問題を修正しました。（LSQ-3734）
SWD-12234	長時間のクエリを処理するために、nginx のタイムアウト値を増やしました。
SWD-12291	クラッシュが検出されたエリアに対するポインタ検証チェックが追加され、SLIC フィードの更新中にエンジンがクラッシュしたときに処理される SLIC フィードファイルのコピーを保存する機能が追加されました。ファイルは診断パックに含まれており、後日シスコが分析を行って、SLIC フィード自体に含まれるデータがクラッシュを引き起こしているかどうかを判断できます。
SWD-12303	エンジンが再起動されるたびにすべてのホストを再ベースライン化するように、ベースライン化コードを変更しました。（LSQ-3955）
SWD-12337	Active Directory の設定で複数のドメインコントローラが受け入れられない問題を修正しました。（LSQ-4122/4161/4175）
SWD-12419	各ホストのトラフィックがトラフィックトレンド ファイルに適切にアーカイブされない問題を修正しました。（LSQ-3988）
SWD-12463	Central Management のアプライアンスサポート（監査ログ、バックアップ/復元設定ファイル）のデータが表示されない問題を修正しました。
SWD-12575	アップグレードプロセスで、6.8.3 から 6.10.4 へのアップグレード後に Juniper フローが「0% 復号」に移行する問題を修正しました。（LSQ-4084）
SWD-12670	MAC 違反アラームが適切に生成されるようになりました。（LSQ-4062）
SWD-12710	FlowSensor 4k タイムアウト処理の問題を修正しました。（LSQ-4107）
SWD-12996	エンドポイント コンセントレータ管理 UI でフィルタ処理および表示される新しい Docker サービスが追加されました。（LSQ-4165）
SWD-13289	ルートパーティションにスペースが追加されました。このスペースは、次を含むアプライアンスに必要です。 5 GB のルートパーティション。『Stealthwatch® 更新ガイド v7.0.x – v7.1.1』の手順に従ってください。

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-7627	[フロー コレクタ（Flow Collector）]を再起動すると、すべてのアラーム履歴が削除されます。ただし、自分のフロー コレクタに置き換えると、履歴は削除されず、新しいフロー コレクタによって古いフロー コレクタからのアラーム履歴が保持されます。[セキュリティ分析ダッシュボード（Security Insight Dashboard）]と[ホストグループ（Host Group）]ページの（最後のリセット時間以降、特定のカテゴリについてアラームを受信中のホストの数を表示する）アラーム発行ホストウィジェットは、次のリセット時間まで更新されないため、これらの値と[ホストリストビュー（Host List View）]の[ホスト（Hosts）]テーブルのアラームの値の表示が一致しない場合があります。	現在使用可能なものはありません。
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

問題番号	説明	回避策
		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-9052	オフラインライセンスのアクティブ化の失敗または「ストレージバインドの中断」エラー	このエラーは、仮想マシンを移動した場合、ライセンスが複数回アップロードされた場合、またはライセンスが破損している場合に発生することがあります。Stealthwatch のカスタマーコミュニティにアクセスして、サポートを受けてください。
SWD-9563	Internet Explorer v11 を使用して Stealthwatch Web アプリケーションにログインするときに、[ホーム（Home）] ページを更新した時点で、[デスクトップクライアント（Desktop Client）] ドロップダウン矢印と、このリストの左側にある 3 つのナビゲーションアイコン（ページ右上）が消えます。次の 3 つのアイコンがあります。 ・検索（虫メガネアイコン） ・ヘルプ（人型アイコン） ・グローバル設定（歯車アイコン） さらに、フォントの表示は、他のブラウザを使用した場合の表示とは異なります。	ブラウザを閉じて、再度ログインします。
SWD-11822（LVA-664）	Stealthwatch は、v7.0 から有効になるインターフェイス API エンコーディングの変更を行いました。関連するエンドポイントのクエリパラメータを設定するときに、URI 内でエスケープされていない文字を使用することはできなくなりました。	この API との統合を正しく機能させるには、次の手順を実行する必要があります。 以下に関連したすべてのエンドポイントの場合： `/tenants/{tenantId}/devices/{deviceId}/exporters/{exporterIp}/interfaces/{interfaceId}`

問題番号	説明	回避策

		開始時刻や終了時刻などのフィルタは、次のような形式にする必要があります。
		`filter%5bstartTime%5d`
		次の形式は使用しません。
		`filter[startTime]`

SWD-11929	SMC デスクトップクライアントは、Mac の場合、IPv6 経由では起動しません。	現在使用可能なものはありません。
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。
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

問題番号	説明	回避策
		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。
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 [アップ（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。

問題番号	説明	回避策
SWD-13968	ANC クエリが実行されないと、[ネットワーク分類（Network Classification）] ページに潜在的なネットワークスキャナが表示されません。	この問題は patch-smc-ROLLUP002-7.1.2-02.swu で修正されました。
SWD-14671	CIMC/iDRAC Serial-Over-Lan 接続から root ユーザとしてアプライアンス SSH にログインできません。	今後のリリースで修正される予定です。
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。『Stealthwatch Update Guide v7.0.x to v7.1.2』の手順に従っていることを確認してください。 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-15027	ユーザによっては、アップグレード後にアプライアンスのパスワードを変更できない場合があります。	v 6.9.x 以降、パスワードを変更していない場合、システムはこの問題のリスクにさらされます。 **アップグレード前**：この問題を回避するには、v7.1.2 にアップグレードする前に、各アプライアンスの管理者パスワードとすべてのユーザパスワードを変更します。 手順については、『Stealthwatch System Update Guide v7.0.x to 7.1.2』を参照してください。 **アップグレード後**： 1. 『Installation and Configuration Guide』を使用して、各アプライアンスの管理者パスワードをリセットします。 2. ユーザにこの問題が発生した場合は、次のようにユーザパスワードをリセットします。 **SMC**：管理者ユーザとして SMC にログインします。[グローバル設定

問題番号	説明	回避策
		（Global Settings）]アイコン > [ユーザ管理（User Management）]を選択します。 **その他のアプライアンス**：管理者ユーザとしてアプライアンスにログインします。[ユーザの管理（Manage Users）] > [ユーザの追加/編集/削除（Add/Edit/Delete Users）]を選択します。
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、この詳細設定を手動で選択する必要があります。
NA	外部サービス（Cognitive Analyticsなど）は、FIPS 暗号化ライブラリが有効になっている場合には機能しません。	以前のリリースでは、外部サービスと FIPS 暗号化ライブラリの両方を有効にすることはサポートされていませんでしたが、外部サービスの機能が妨げられることはありませんでした。v7.1 以降では、Cognitive Analytics その他の外部サービスを有効にする場合には、FIPS を無効にする必要があります。

リリースサポート情報

リリース 7.1 の公式一般公開（GA）日は 2019 年 8 月 19 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