Cisco Stealthwatch

リリースノート 7.2.1

目次

はじめに

概要

このドキュメントでは、Stealthwatch v7.2.1 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。

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（v7.1.x から v7.2.1）』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 7.2 に更新するには、アプライアンスに 7.1.1 以降のバージョン 7.1.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。
- **スマートライセンスの準備状況チェック**：更新プロセスの一環として、SWU ファイルがスマートライセンスの準備状況チェックを実行します。また、アップグレードの前にもスマートライセンスの準備状況チェックを実行できます。詳細については、「**スマートライセンスの準備状況チェック**」を参照してください。手順については、『Stealthwatch 更新ガイド（v7.1.x から v7.2.1）』を参照してください。
- **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。詳細については、「**Cisco Software Central**」を参照してください。
- **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 v6.10.x を使用している場合は、各アプライアンスを v6.10.x から v7.0.x に更新してから、7.0.x を 7.1.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。

VMware

Stealthwatch v7.2.x は VMware v6.5 および v6.7 との互換性があります。Stealthwatch v7.2.x では VMware v6.0 はサポートされていません。詳細については、『vSphere 6.0 End of General Support』の VMware のマニュアルを参照してください。

- **更新前**：Stealthwatch アプライアンスが VMware v6.0 にインストールされている場合は、Stealthwatch を v7.2.x にアップグレードする前に、VMware vCenter と ESXi ホストを v6.5 または v6.7 にアップグレードします。
- **確認**：「**1. VMware バージョンの確認**」と、「**2. VMware ホストの確認**」を参照して VMware 環境を確認します。
- **更新後**：Stealthwatch v7.2.x の更新後に、VMware にオペレーティングシステムのエラーが表示される場合があります。VMware の GUI を確認し、VMware vCenter が v6.5 か v6.7 であることと、オペレーティングシステムが Debian v10 であることを確認します。VMware vCenter またはオペレーティングシステムをアップグレードするには、VMware ガイドを参照してください。
- ホストからホストへの **ライブ マイグレーション**（vMotion などを使用）はサポートされていません。
- **スナップショット**：仮想マシンのスナップショットはサポートされていません。

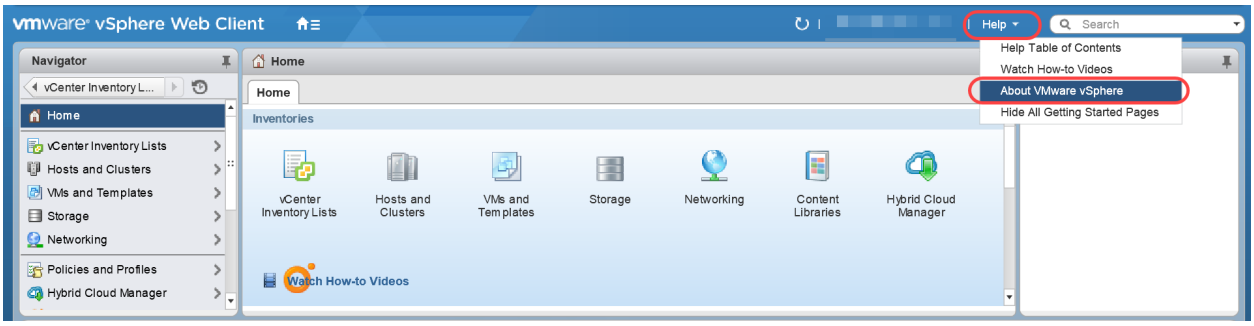
> ⚠ すでにインストールされているカスタム バージョンが上書きされるため、Stealthwatch 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

1. VMware バージョンの確認

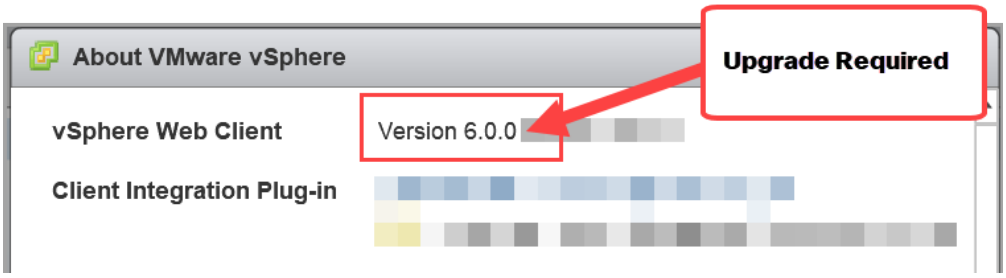
次の手順に従って、VMware vSphere vCenter v6.5 か v6.7 がインストールされていることを確認します。

> ℹ VMware UI のメニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. VMware Web クライアントにログインします。
2. [ホーム（Home）] ページで [vCenter インベントリリスト（vCenter Inventory Lists）] を選択します。
3. [ヘルプ（Help）] > [VMware vSphere バージョン情報（About VMware vSphere）] を選択します。



4. **Web クライアント**のバージョンを確認します。バージョンが 6.0 の場合は、v6.5 か v6.7 にアップグレードする必要があります。手順については、VMware ガイドを参照してください。



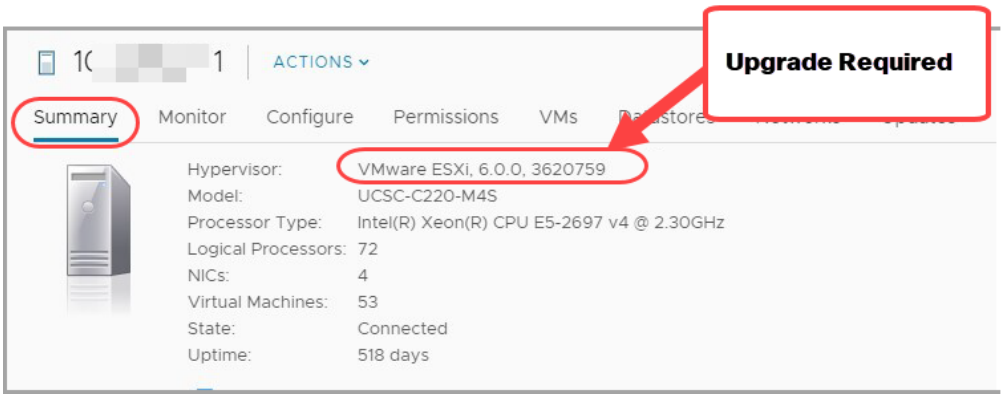
5. 次の項に進みます。

2. VMware ホストの確認

次の手順に従って ESXi ホストを確認し、v6.5 か v6.7 がインストールされていることを確認します。Stealthwatch アプライアンスが複数のホストにインストールされている場合は、それぞれがオンになっていることを確認します。

> VMware UI のメニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. [ナビゲータ(Navigator)] ペインで [vCenter インベントリリスト(vCenter Inventory Lists)] を選択します。
2. [ホスト(Hosts)] を選択します。
3. ホスト名をクリックします。
4. [サマリー(Summary)] タブをクリックします。



5. **ハイパーバイザ** のバージョンを確認します。バージョンが 6.0 の場合は、v6.5 か v6.7 にアップグレードする必要があります。手順については、VMware ガイドを参照してください。
6. Stealthwatch アプライアンスがインストールされている他のホストに対して手順 1 ～ 5 を繰り返します。

スマートライセンスの準備状況チェック

更新プロセスの一環として、SWU ファイルがスマートライセンスの準備状況チェックを実行します。また、アップグレードの前にもスマートライセンスの準備状況チェックを実行できます。手順については、『Stealthwatch 更新ガイド（v7.1.x から v7.2.1）』を参照してください。

準備状況チェックに失敗した場合は、クラスタ内で互換性のないライセンスが検出されています。ライセンスを再設定する必要がある場合もあれば、新しい期間のライセンシングを購入する必要がある場合もあります。Stealthwatch 更新チームに stealthwatch_renewals@cisco.com からお問い合わせください。

スタンドアロン アプライアンス

v7.2.x ではスタンドアロン アプライアンスはサポートされていません。『Stealthwatch 更新ガイド（v7.1.x から v7.2.1）』の手順に従ってアプライアンスを設定し、それらを正常に管理および更新できるようにします。

更新の準備の一環として、ライセンス、証明書、ホスト名などを確認します。『Stealthwatch 更新ガイド（v7.1.x から v7.2.1）』の手順に従っていることを確認します。

Stealthwatch 管理コンソールが必要：クラスタ内に Stealthwatch 管理コンソールがない場合は、この更新を開始する前に Stealthwatch 管理コンソール VE をインストールします。Cisco Software Central（https://software.cisco.com）の Cisco スマートアカウントからイメージをダウンロードできます。『Stealthwatch Installation and Configuation Guide v7.2』の手順に従ってインストールします。

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 7.2 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。

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。

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. [集中管理(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。

新着情報

Stealthwatch システム v7.2.1 リリースの新機能と改善点は次のとおりです。

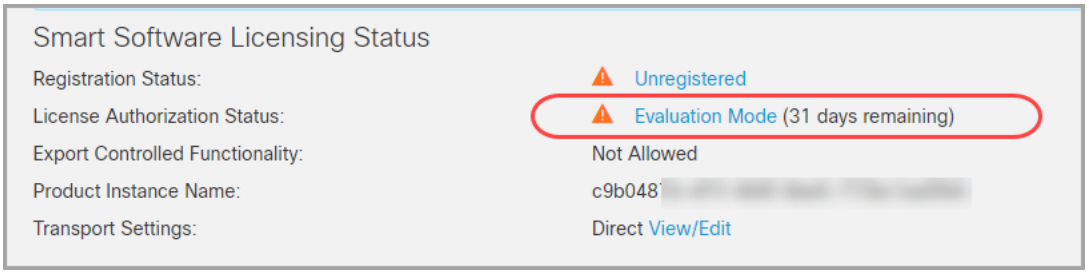
スマート ソフトウェア ライセンシング

v7.2 では、Cisco スマート ソフトウェア ライセンシングを使用して、Stealthwatch のアプライアンスおよび機能をライセンシングします。詳細については、cisco.com のスマートライセンシングを参照してください。

- **オンライン**：スマートライセンシング および Stealthwatch をオンラインで使用するには、『Stealthwatch Smart Software Licensing Guide』を参照してください。この設定にはインターネットアクセスが必要です。
- **オフライン**：クローズド/エアギャップネットワークのライセンスオプションの説明については、Cisco Stealthwatch サポートに連絡してください。
- **Cisco スマートアカウント**：CCOID クレデンシャルを使用して https://software.cisco.com の Cisco スマートアカウントにログインするか、または管理者に連絡します。

評価モード（90 日）

選択した機能を備えた Stealthwatch を評価モードで 90 日間使用できます。



- **残り日数**：評価モードの残り日数を確認するには、管理者ユーザとして Stealthwatch Management Console にログインします。[集中管理（Central Management）] > [スマートライセンシング（Smart Licensing）] の順に移動します。[ライセンス承認ステータス（License Authorization Status）] を確認します。
- **有効期限**：90 日間の評価期間の期限が切れる前に、製品インスタンスを登録し、ライセンスを転送して変換します。評価期間が終了すると、フロー収集が停止します。フロー収集を再開するには、製品インスタンスを登録します。

登録

デフォルトの最大機能で Stealthwatch を使用して、アカウント上の購入済みのライセンスと機能にアクセスするには、Cisco スマートアカウントを設定し、スマート ソフトウェア ライセンスの製品インスタンスを登録します。

登録するには、『Stealthwatch Smart Software Licensing Guide』の指示に従ってください。登録プロセスの一環として、https://software.cisco.com から Cisco Smart Software Manager（Cisco Software Central）にログインし、登録トークンを生成してライセンスを追加します。

自動プロビジョニングされたライセンス

製品インスタンスを登録すると、次のライセンスがアカウントに自動的に追加されます。

- Stealthwatch 管理コンソール VE
- Flow Collector VE

プロビジョニング要求

要求に応じて、次のライセンスタイプがアカウントに転送されます。

ライセンス	詳細
脅威インテリジェンス ライセンス （以前は SLIC と呼ばれていました）	このライセンスを購入しているのにアカウントに表示されない場合は、ライセンスプロビジョニング要求を送信します。
UDP Director VE	このライセンスを 2020 年 3 月 17 日よりも前に購入した場合は、ライセンスプロビジョニング要求を送信してアカウントに転送します。

ライセンスプロビジョニング要求を送信するには、http://cs.co/stealthwatch-license-provisioning でフォームに入力し、送信します。

ライセンスの転送

Stealthwatch を v7.1.x から v7.2.x に更新した場合は、評価モードの期限が切れる前に PAK に転送してスマートライセンシングに変換する必要もあります。

PAK およびライセンシングトークン ID をスマートアカウントに転送するには、次の手順を使用します。次に概要を示します。詳細な手順については、Cisco スマートアカウントにログインし、[ヘルプ（Help）] をクリックします。

1. https://software.cisco.com にある Cisco スマートアカウントにログインします。
2. [ライセンス（License）] セクションで、[スマート ソフトウェア ライセンシング（Smart Software Licensing）] を選択します。
3. [インベントリ（Iventory）] を選択します。
4. [ライセンス（Licenses）] タブを選択します。
5. すべてのライセンスが表示されている場合は、この手順をスキップできます。

   スマートライセンシングのインベントリに表示されていないライセンスがある場合は、次の手順に進み、ライセンスを転送および変換します。

   また、要求を送信する必要があるかどうかを決定するには、「**プロビジョニング要求**」を参照してください。

6. Cisco スマートアカウントの [ホーム（Home）] ページに戻ります。[ライセンス（License）] セクションで、[従来のライセンシング（Traditional Licensing）] を選択します。
7. [スマートアカウント（Smart Account）] ドロップダウンリストから、スマートアカウントを選択します。
8. [PAK/トークンの追加（Add New Pak/Tokens）] をクリックします。

9. **オプション**:[バーチャルアカウントに追加(Add to Virtual Account)]ドロップダウンからバーチャルアカウントを選択します。ライセンスはこのバーチャルアカウントに転送されます。
10. PAK 番号を入力するか、シスコ SO 番号で検索します。
11. [OK]をクリックします。
12. これらの手順を繰り返して、アカウントにさらに PAK とトークンを追加します。

ライセンスの変換

次の手順を使用して、PAK ライセンスを従来のライセンスからスマートライセンシングに変換します。

> ⚠ PAK ライセンスをスマートライセンシングに変換すると、従来のライセンスに戻すことはできません。

1. **チェック**:https://software.cisco.com でアカウントにログインします。
2. [ライセンス(License)]セクションで、[スマート ソフトウェア ライセンシング(Smart Software Licensing)]を選択します。
3. [スマートライセンシングに変換(Convert to Smart Licensing)]または[ライセンス変換(License Conversion)]を選択します。
4. [PAKの変換(Convert PAK)]タブと[ライセンスの変換(Convert Licenses)]タブを確認して、スマートライセンシングへの変換に使用できる PAK を指定します。

    - **手順**:[スマートライセンシングに変換(Convert to Licensing)]ページで[ヘルプ(Help)]をクリックします。
    - **デモ**:デモを視聴するには、「クラシックライセンス(PAK)をスマートライセンスに変換する方法」を参照してください。

サポート

ライセンスの転送と変換のサポートについては、次のいずれかのリソースを通じてお問い合わせください。

- Support Case Manager(https://mycase.cloudapps.cisco.com/case)に移動し、[ソフトウェアライセンス(Software Licensing)]でケースタイプとして[セキュリティ関連ライセンス(Security Related Licensing)]を選択します。
- TAC ワールドワイドサポート番号に連絡し、https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html およびライセンス要求を依頼します。

スマートライセンシングの使用

Stealthwatch でスマートライセンスを使用するには、『Stealthwatch Smart Software Licensing Guide』を参照して詳細を確認してください。この設定にはインターネットアクセスが必要です。

- **承認済み**:製品インスタンスを登録すると、ライセンス承認ステータスが[承認(Authorization)]に変わります。
- **製品インスタンス**:製品インスタンスはお客様の Stealthwatch の製品インスタンスに使用する識別子であり、Stealthwatch管理コンソールと管理アプライアンスが含まれます。

- **メニュー**：登録ステータス、ライセンスステータス、および使用状況を確認するには、Stealthwatch 管理コンソールにログインし、[集中管理（Central Management）] > [スマートライセンシング（Smart Licensing）] の順に選択します。Stealthwatch デスクトップクライアントとアプライアンス管理インターフェイスからは、ライセンシングメニューとデータが削除されています。
- **スマートライセンスの使用状況**：ライセンス数を確認するには、[スマートライセンス使用状況（Smart License Usage）] を確認します。このリストには、ライセンスされている仮想アプライアンスと機能が表示されます。UDP Director を除き、物理アプライアンスはこのリストには表示されません。

サポート

Cisco スマートアカウントとスマートライセンシングのサポートについては、次のいずれかのリソースを通じてお問い合わせください。

- Support Case Manager（https://mycase.cloudapps.cisco.com/case）に移動し、[ソフトウェアライセンス（Software Licensing）] でケースタイプとして [セキュリティ関連ライセンス（Security Related Licensing）] を選択します。
- TAC ワールドワイドサポート番号に連絡し、https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html およびライセンス要求を依頼します。

Cisco Software Central

ダウンロードおよびライセンスセンターは、Cisco Software Central に置き換えられました。ライセンスの管理、パッチのダウンロード、および Stealthwatch v7.2 の更新ファイルのダウンロードについては、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。スマートアカウント管理者がわからない場合は、「**サポート**」を参照してください。

バージョン 7.1.x 以前の Stealthwatch のパッチまたはアップデートファイルにアクセスするには、https://stealthwatch.flexnetoperations.com でダウンロードおよびライセンスセンターを引き続き使用します。

Stealthwatch Training Center

Stealthwatch Training Center のログイン方法がシングルサインオン（SSO）に変更されました。

- **ログイン**：Stealthwatch Training Center にアクセスするには、https://learning.stealthwatch.com で Cisco OneID（CCOID）クレデンシャルを使用してログインします。
- **登録**：Cisco OneID（CCOID）アカウントが必要な場合は、https://identity.cisco.com/index.html で登録します。
- **詳細**：詳細については、https://cisco.bravais.com/s/aHXPCQe0sJHPEX29OVhF を参照してください。

Stealthwatch カスタマーコミュニティ

2020 年 7 月 13 日、カスタマーコミュニティ（https://lancope.force.com/Customer/CustomerCommLogin）は廃止されます。

Cisco Stealthwatch リソースにアクセスするには、次を参照してください。

- **Cisco コミュニティの Stealthwatch 情報ハブ**：https://cisco.bravais.com/s/10pIGhmYWj8hC1uxin6S にアクセスします。
- **トレーニングセンター**：**Stealthwatch Training Center** を参照してください。
- **ドキュメント**：https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html にアクセスします。
- **連絡先**：トレーニングセンターおよび Stealthwatch 情報ハブについては、ラーニングサービスチーム（stealthwatch-training@cisco.com）へ電子メールでお問い合わせください。

パスワードの変更

Stealthwatch のデフォルトの管理者を除くすべてのユーザに、以下が適用されます。

- 新しい Stealthwatch ユーザは、初めてログインするときにパスワードを変更するように求められます。
- 管理者がユーザのパスワードをリセットすると、ユーザは次のログイン時にパスワードを変更するように求められます。
- ユーザが自分のパスワードを変更した場合は、次回のログイン時にパスワードを変更するように求められることはありません。
- リモートユーザは、パスワードを変更するように求められません。
- パスワードが変更されるたびに、監査ログメッセージが作成されます。

Cisco SecureX の統合

Cisco Threat Response の統合が Cisco SecureX に更新されました。SecureX は、可視性を一元化し、自動化を有効にし、ネットワーク、エンドポイント、クラウド、およびアプリケーションにわたってセキュリティを強化する一貫性のある体験を実現するため、シスコの統合セキュリティポートフォリオ全体とセキュリティインフラストラクチャ全体を結びつけます。その結果、すでに存在しているソリューションに組み込まれたセキュリティがシンプルになります。

詳細については、『Cisco SecureX Integration Guide』を参照してください。

現在の CTR 統合の更新

現在の CTR をお使いのお客様が v7.2.1 にアップグレードする場合に SecureX セキュリティリボンを正しく動作させるには、次の手順を実行します。

1. 次の範囲を使用して、CTR サイトで API クライアントを再生成します。

   - casebook
   - inspect:read
   - orbital
   - response
   - users:read
   - enrich:read
   - integration:read
   - profile
   - registry/user/ribbon
   - global-intel:read
   - notification
   - private-intel
   - telemetry:write

2. 新しい API クライアント ID と API クライアントパスワードを使用して、SMC で SecureX 設定を更新します。

セッション設定

[セッション設定(Session Settings)]セクションは、[セキュリティロックアウト(Security Lockout)]セクションに置き換えられて改善され、ユーザの同時セッションおよび失敗したサインオンの試行を制限することができます。セッション設定では、ユーザの最終ログインに関する情報のポップアップ表示を有効または無効にすることもできます。[セッションの設定(Session Settings)]セクションにアクセスするには、[集中管理(Central Management)]>[アプライアンスマネージャ(Appliance Manager)]の順に開きます。

1. アプライアンスの[アクション(Actions)]メニューをクリックして、[アプライアンス設定の編集(Edit Appliance Configuration)]を選択します。
2. [全般(General)]タブを選択して[セッション設定(Session Settings)]セクションを特定します。
3. 必要に応じてフィールドに入力します。

    - **試行失敗回数**:セキュリティロックアウトが発生するまでに許可される、サインオンの試行失敗回数を入力します。フィールドのデフォルトは 0 で、試行回数に制限はありません。
    - **ロックアウトの期間**:セキュリティロックアウトの分単位の期間です。デフォルトは 1 分です。
    - **最終ログイン情報のポップアップ表示の有効化**:最終ログイン情報のポップアップ表示を有効/無効にするには、このチェックボックスをオンにします。
    - **同時セッションの最大数**:ユーザごとに許可される同時セッションの最大数。このフィールドのデフォルトは 0 で、同時セッション数を無制限にすることができます。

パスワードポリシー

[パスワードポリシー(Password Policy)]セクションには新しいフィールドがあり、**パスワードは最長である必要があります**。このフィールドでは、ユーザのパスワードに使用できる最大文字数を指定できます。このフィールドのデフォルトは 256 文字です。

カスタマー サクセス メトリック

テレメトリデータ収集の一部の設定が変更されました。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。

Stealthwatch Web アプリ

Stealthwatch Web アプリには、次の機能が追加されています。

- アラーム重大度の設定
- データ保存の設定
- ドメインプロパティの設定
- DSCP 設定
- エクスポータ SNMP の設定
- フローコレクタの設定
- ホスト ロック セキュリティ イベント(これらはカスタム セキュリティ イベントと同等のものに変換されています)
- サービス設定

> パスワード変更、データロール管理、およびユーザ管理機能に関するドキュメントは、Stealthwatch デスクトップクライアントから削除されています。

ユーザ管理

データロール管理などのほとんどのユーザ管理機能は、Stealthwatch デスクトップクライアントから削除されています。機能の削除後も Stealthwatch デスクトップクライアントでデスクトップ クライアント ロール(以前のユーザ機能ロール)を作成可能ですが、Stealthwatch Web アプリでデスクトップ クライアント ロールを割り当てる必要があります。

この機能の詳細については、Stealthwatch デスクトップ クライアント オンライン ヘルプの「デスクトップ クライアント ロール」のトピックと、Stealthwatch Web アプリケーション オンライン ヘルプの「ユーザの設定」のトピックを参照してください。

デスクトップクライアント、データ、および Web ロール

既存のデスクトップクライアントまたは Web ロールに変更を加えると、ログインしているその Web またはデスクトップ クライアント ロールを持つすべてのユーザがログアウトされます。

さらに、特定のユーザのデスクトップクライアント、Web、またはデータロールの割り当てを変更した場合、変更が適用されるとユーザがログアウトされます。

認証および認可サービス

ユーザ管理には、認証および認可サービスの設定と管理を可能にする、[認証および認可(Authentication and Authorization)]という新しいタブがあります。認証はユーザを確認するプロセスであり、認可はユーザがアクセスできるようにする必要がある内容を確認するプロセスです。認証および認可サービスを SMC から一元管理できます。

認証サービス

Stealthwatch には、自動的に有効になっているローカルの認証サービスがあります。ただし、次のオプションの認証サービスも使用できます。

- Remote Authentication Dial-In User Service（RADIUS）：認証サービスのみ
- Terminal Access Controller-Access Control System（TACACS+）：TACACS+ の設定に関する詳細な手順については、『Stealthwatch TACACS+ コンフィギュレーション ガイド』を参照してください。
- Lightweight Directory Access Protocol（LDAP）

認可サービス

次の認可サービスを使用できます。

- Terminal Access Controller-Access Control System（TACACS+）：TACACS+ の設定に関する詳細な手順については、『Stealthwatch TACACS+ コンフィギュレーション ガイド』を参照してください。
- Lightweight Directory Access Protocol（LDAP）

RADIUS はリモート認可ではサポートされていません。

LDAP

以前は [LDAP設定（LDAP Setup）] は [集中管理（Central Management）] にありましたが、v7.2 では [ユーザ管理（User Management）] に移動しました。LDAP は [認証および認可（Authentication and Authorization）] ページから設定および管理されるようになりました。

ページにアクセスするには、[ユーザ管理（User Management）] > [認証および認可（Authentication and Authorization）] を開きます。LDAP を設定する前に、必ず SMC の信頼ストアに LDAP サーバ証明書をインストールしてください。

Stealthwatch は、Microsoft サーバ上の LDAP のみをサポートします。

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。

- **設定**：『TACACS+ コンフィギュレーション ガイド』に記載の手順に従って、TACACS+ を設定します。Stealthwatch v7.2 では、[SMC Webアプリ（SMC Web App）] > [ユーザ管理（User Management）] で TACACS+ 認証サービスを設定します。
- **ユーザ名**：7.1.2 で TACACS+ ユーザを設定した場合は、引き続き 7.2 で使用できます。v7.2 では、TACACS+ ユーザは Stealthwatch デスクトップクライアントではなく、[SMC Webアプリ（SMC Web App）] > [ユーザ管理（User Management）] で設定されます。
- **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 v7.2 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+ コンフィギュレーション ガイド』を参照してください。

TACACS+ と ISE

Stealthwatch v7.2 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+ コンフィギュレーション ガイド』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。

セッション制限

[SystemConfig を介してのみ（Only through SystemConfig）] で SSO を有効にした場合、[セッション制限（Session Limits）] タブが [ユーザ管理（User Management）] に表示されます。[セッション制限（Session Limits）] にアクセスするには、[ユーザ管理（User Management）] > [セッション制限（Session Limits）] を開きます。

[セッション制限（Session Limits）] では、各デスクトップクライアントまたは Web ロールのセッション制限を、次の方法で同時に指定できます。

- 各ロールのデフォルトをゼロのままにすると、無制限の同時セッションが許可されます。
- 任意のロールに対して、同時セッション数を 1 ～ 99 の間で設定します。

特定のデスクトップクライアントまたは Web ロールを持つユーザがログインすると、そのロールのセッション制限がすでに満たされている場合、そのユーザはアクセスを拒否されます。

> ロールのセッション制限を、そのロールに関連付けられているアクティブセッションの合計数以下に減らすと、すべてのアクティブセッションが自動的に終了します。

ホスト ロック セキュリティ イベントの変換

v7.2 では、Stealthwatch はホスト ロック セキュリティ イベントを使用しなくなりました。v7.2 にアップグレードすると、ホスト ロック セキュリティ イベントに関連するすべての既存のホストロックルールおよび管理ルールが、カスタム セキュリティ イベントと同等のものに変換されます。

v7.2 にアップグレードする前に

ホストロックイベントを確認し、無関係なものを削除します。

アップグレードプロセス中

- Stealthwatch は、ホスト ロック セキュリティ イベントに関連するすべてのホストポリシーとロールポリシーを削除します。
- Stealthwatch は、次のことも行います。

アップグレードプロセス中に、許可された最大数の後 ...	Stealthwatch ...
有効になっているカスタム セキュリティ イベント(182)に到達しました	カスタム セキュリティ イベントに変換される残りのすべてのホストロックルールに、非アクティブステータスを割り当てます。
カスタム セキュリティ イベントに到達しました(2500 ライフタイム)	追加のホストロックルールはいずれも変換されませんが、その代わりに次のファイルにログが記録されます。 /lancope/var/smc/log/smc-configuration.log

v7.2 へのアップグレード後

- Stealthwatch システムでカスタム セキュリティ イベントを有効にできる上限が 182 であるため、Stealthwatch では既存のホスト ロック セキュリティ イベントをすべて変換できない可能性があります。したがって、Stealthwatch システムに含まれるイベントがより少なくなるように、カスタム イベント ルール ロジックを組み合わせることをお勧めします。その結果、より多くのイベントを有効にすることができます。
- 新しいカスタム セキュリティ イベントでは、より頻繁にアラームが発生する可能性があるため、イベントをより正確にするルールロジックを追加して、カスタム セキュリティ イベントの追加機能を活用します。
- ホストロックルールは設定できません。また、ホストロック違反に対して Stealthwatch でアラームを発生させることもできません。
- 保持期間の設定に応じて、既存のホストロック違反アラームにアクセスできます。

エクスポータ SNMP の設定

デフォルトの SNMP ポーリング間隔が 60 分(1 時間)から 720 分(12 時間)に変更されました。この設定を変更するには、ナビゲーションメニューから Stealthwatch Web に移動し、[設定(Configure)]>[エクスポータSNMP(Exporter SNMP)]の順に選択します。エクスポータ SNMP 設定を管理できるのは、管理者または設定マネージャのロールを割り当てられたユーザだけです。

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。ポーリングを頻繁に行っても、使用率のメトリックは最新にはなりません。

SNMPポーリングは、ネットワーク内のインターフェイスの名前と速度を取得するために使用されます。使用率情報は取得されません。使用率情報は、Stealthwatch が収集する NetFlow レコードから取得されます。

可視性アセスメント

Stealthwatch v7.2.1 以降では、可視性アセスメントは Stealthwatch Web アプリケーション内の機能になります。アプリケーションとしてはリリースされません。

新しい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。

フローセンサー 4240

Stealthwatch システムでは新しいアプライアンスが使用できます。フローセンサー 4240は、2 x 40G または 4 x 10G(SFP)インターフェイスを切り替えることができます。このアプライアンスの詳細については、仕様シートを参照してください。

インターフェイス選択のモニタリング

[高度なフローセンサー(Advanced Flow Sensor)]ページの新しい設定が追加されました。この設定で、フローセンサー 4240 が 2 x 40G または 4 x 10G(SFP)インターフェイスを使用するかどうかを指定します。

- このオプションは、フローセンサー 4240 でのみ使用できます。
- デフォルトの設定は 2 x 40G です。

ISE 統合機能の強化

[ISEの設定(ISE configuration)]ページに、新しい統合オプションが追加されました。[セッション設定(Sessions configuration)]オプションでは、ユーザセッションの更新とともに、マシンセッションの更新を受信できます。[マシン認証から導出されたセッションの追跡(Track sessions derived from machine authentications)]をクリックして、このオプションを有効にします。(LSQ-3731)

Docker サービス

Docker サービスは、アプライアンス管理インターフェイスのホームページに表示されます。これらのサービスを開始、再起動、または停止するメニューは、v7.2 で削除されています。サービスが実行されない場合やサポートが必要な場合は、Cisco Stealthwatch サポートまでお問い合わせください。

脅威インテリジェンスフィード

脅威インテリジェンスフィード(旧 Stealthwatch Labs Intelligence Center:SLIC)は、ネットワークに対する脅威に関するグローバル脅威インテリジェンスフィードからのデータを提供します。フィードは頻繁に更新され、悪意のあるアクティビティに使用されたことがわかっている IP アドレス、ポート番号、プロトコル、ホスト名、および URL が含まれています。フィードには、コマンドアンドコントロール サーバ、bogon、および Tor の各ホストグループが含まれています。

- **有効化**:脅威インテリジェンスフィードを有効にするには、StealthwatchWeb アプリにログインします。[集中管理(Central Management)]>[SMC]>[アクション(Actions)]>[アプライアンス設定の編集(Edit Appliance Configuration)]>[全般(General)]タブの順に移動します。詳細については、Stealthwatch オンラインヘルプを参照してください。

- **アラームとセキュリティイベント**: 脅威インテリジェンスフィードが有効になっている場合、Stealthwatch Labs Intelligence Center のアイコンがStealthwatch デスクトップ クライアント企業ツリーにアラームステータスとともに表示され、脅威は各ホストグループのブランチに表示されます。詳細については、『Stealthwatch Desktop Client User Guide』またはStealthwatch デスクトップ クライアント オンラインヘルプを参照してください。

システム設定

新しいメニュー構造でシステム設定が更新されました。アプライアンスに SSH 接続してログインします。メインメニューから次のメニューを選択します。

- **ネットワーク**: アプライアンス管理ポートネットワーク、信頼できるホスト、およびネットワーク インターフェイスを変更するには、[ネットワーク(Network)]を選択します。
- **セキュリティ**: パスワードの変更またはリセット、Syslog コンプライアンスの管理を実行するには、[セキュリティ(Security)]を選択します。
- **リカバリ**: 集中管理からのアプライアンスの削除、工場出荷時の初期状態へのリセットを実行するには、[リカバリ(Recovery)]を選択します。
- **詳細**: アプライアンスモデルの更新、ルートシェルのオープン、管理ユーザアカウントの管理、またはシングルサインオンの設定を実行するには、[詳細(Advanced)]を選択します。

詳細については、『Stealthwatch System Installation and Configuration Guide』を参照してください。

SOAP API の廃止

v7.2 のリリース後、Stealthwatch は SOAP API から REST API への移行を開始します。Stealthwatch API スイートをご利用のお客様は、可能な場合は REST API の同等の機能を使用開始していただく必要があります。移行の一環として、REST API に対応していない SOAP API を特定し、将来のリリースに適切な REST API の同等の機能を含めることができるかどうかを評価します。特定の SOAP API と同等の機能が REST API にあるかどうかを確認するには、Stealthwatch Rest API のドキュメントを参照してください。

今後のリリースに先駆けて、必要に応じて次の情報を提供します。

- 削除された SOAP API。
- 既存の REST API に追加された機能。

デスクトップクライアントのダウンロードアイコン

デスクトップクライアントのダウンロードボタンが、シスコの新しい標準スタイルで更新されました。アイコンをクリックして、デスクトップクライアントをダウンロードします。

パッチインストールのリブート

Stealthwatch の以前のバージョンでは、パッチをインストールする前に Stealthwatch 管理コンソールとフローコレクタが 1 時間以上、かつ 7 日間未満、実行されていることを確認する必要があり、この範囲に入っていなかった場合はアプライアンスをリブートする必要がありました。

Stealthwatch を v7.2.1 に更新した後は、いつでもパッチをインストールできます。リブート範囲は、v7.2.1 での要件ではなくなりました。

コグニティブ統合の機能拡張

Cognitive Analytics は Cognitive Intelligence にリブランドされました。

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 Defect（SWD または LSQ）番号が示されています。

バージョン 7.2.1

障害	説明
SWD-13461	7.1.1 への集中管理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。
SWD-13474	Web アプリで [フローアクション（Flow Actions）] 列が空白だった問題を修正しました。（LSQ-4424）
SWD-13554	地理位置情報がホスト外で動作していなかった問題を修正しました。（LSQ-4429）
SWD-13650	上位のアプリケーショングラフからのフロー検索へのピボットではデータを表示しなかった問題を修正しました。（LSQ-4497）
SWD-13759	パケットクエリが無効なポートまたはプロトコルエラーを返す問題を修正しました。（LSQ-4515）
SWD-14209	企業ツリーにフローセンサーがない問題の修正に役立つデバッグコードを追加しました。（LSQ-4689）
SWD-14210	フローコレクタのフローデータ損失ドキュメントに対する IP アドレスタイプのサポートを追加しました。（LSQ-4628）
SWD-14287	ネットワーク図アプリケーションが表示していたホストグループ図のデータはバイト単位で、値はビット単位だった問題を修正しました。（LSQ-4652）
SWD-14311	複数のカスタムアプリケーションの優先順位のレベルとマッピングを更新しました。（LSQ-4718）
SWD-14415	印刷されたレポートにチャートが表示されなかった問題を修正しました。（LSQ-4735）
SWD-14689	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-14879	アラームのリストにフローコレクタのフローデータの損失を追加しました。（LSQ-4798）

障害	説明
SWD-14889	現在の Ipoque ID を Stealthwatch アプリケーションにマッピングするように、アプリケーション ID の定義ファイルとマッピング XML ファイルを更新しました。(LSQ-4637)
SWD-14892	ユーザ名がドットで終わり、その後に 1 文字が続く一部のユーザに対して Cognitive ウィジェットがロードされなかった問題を修正しました。(LSQ-4813)
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-14935	インターフェイスデータが処理されていない問題を修正しました。(LSQ-4836)
SWD-14997	前日から大きなログファイルを除外するように診断パックを更新しました。(LSQ-4862)
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-15033	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-15062	Stealthwatch インシデントが SecureX に送信されない問題を修正しました。
SWD-15232	複数のカスタムアプリケーションの優先順位のレベルとマッピングを更新しました。(LSQ-4718)
SWD-15423	CiscoJ が MD5 を許可しないために、SLR/PLR が予約コードの生成に失敗する FIPS モードの問題を修正しました。

バージョン 7.2.0

障害	説明
SWD-11703	ISE ユーザセッションでの複数のインターフェイスのサポートが追加されました。(LSQ-3731)
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

障害	説明
	示されない問題を修正しました。（LSQ-3881）
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-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-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-13126	アップグレード後にフローセンサーのネットワークカードが動作を停止する問題を修正しました。（LSQ-4249）
SWD-13169	6.10.3 からアップグレードした後のプロキシ認証に関する問題を修正しました。（LSQ-4220）
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-13325	PKCS12 証明書の処理が更新されました。
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-13538	仮想モデルの更新を実行するために、sysadmin が更新されました。
SWD-13609	enforce-root-login サービスが更新されました。

障害	説明
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）
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-13789	アップグレード後に、SMC デスクトップクライアントのアクションとオプションがグレー表示される問題を修正しました。（LSQ-4547）
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-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-13823	SSO インストールおよびコンフィギュレーション ガイドが更新されました。（LSQ-4518、LSQ-4594）
SWD-13833	Web アプリで [フローアクション（Flow Actions）] 列が空白だった問題を修正しました。（LSQ-4424）
SWD-13883	「ユーザには SSO を使用する権限がありません」というエラーメッセージが追加されました。
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）
SWD-14064	SSO の AssertionConsumerService フィールドの要件が削除されました。
SWD-14114	SMC フロー検索が以前のバージョンよりも低速であった問題を修正しました。（LSQ-4574）
SWD-14209	企業ツリーにフローセンサーがない問題を修正しました。（LSQ-4689）

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-14466	fake_app_exclude_list と呼ばれる新しい詳細設定を作成しました。 この詳細設定により、偽のアプリケーションテスト中に無視される Stealthwatch アプライアンス ID のカンマ区切りリストを追加できます。ID を取得するには、フローコレクタの /lancope/var/sw/today/config フォルダに移動し、application_definitions.xml ファイルを開きます。
SWD-14535	パケットサンプルの処理で検出されたスキップされたパケットを含めずに、FPS の計算がより正確になるように更新されました。(LSQ-4717)
SWD-14593	プロキシドメイン名でハイフン(-)が許可されていない問題を修正しました。(LSQ-4754)
SWD-14607	SMC デスクトップクライアントが 1 時間後にタイムアウトする問題を修正しました。
SWD-14624	OpenDNS 外部ホストグループで IP が欠落している問題を修正しました。
SWD-14860	Vertica Backup Restore (VBR) の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。
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	現在使用可能なものはありません。

問題番号	説明	回避策
	(1970 年 1 月 1 日)が表示される場合があります。	
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。
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	現在使用可能なものはありません。

問題番号	説明	回避策
	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。	
SWD-13461	インストールログには最新のアプライアンスのアップグレードが表示されません。	最新のアップグレード試行を表示するには、`/lancope/var/admin/upgrade/upgradeOutput.log` に移動します。この問題は今後のパッチリリースで修正する予定です。
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。 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

問題番号	説明	回避策
		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-14670	アップグレード後は admin ユーザとしてログインできません。	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**:この問題が発生する可能性があるかどうかを判断するには、すべてのアプライアンスのパスワードポリシーを確認するか、または admin.script ファイルを次のように確認します。 1. [集中管理(Central Management)] を開きます。[アクション(Actions)] > [アプライアンス設定の編集(Edit Appliance Configuration)] > [全般(General)] の順にクリックします。[パ

問題番号	説明	回避策

		フィールドを確認します。
		2. Stealthwatch 管理コンソールが v6.9 からアップグレードされた後、ポリシーがトリガーされたかどうかを確認します。[集中管理(Central Management)]のすべてのアプライアンスでパスワードポリシーを確認します。
		または
		このファイルを確認し、ファイルの下部に MD5 が表示されているかどうかを確認します。
		`/lancope/var/database/dbs/hsqldb/admin/admin.script`
		アップグレード後:v7.2.1 へのアップグレード後にこの問題が発生した場合は、SMC で user.xml ファイルを削除し、tomcat を再起動します(`docker restart smc` を実行します)。これにより、パスワードがデフォルトのパスワードにリセットされます。
		SMC ディレクトリ:
		`/lancope/var/smc/config/users/admin/user.xml`
		この問題が発生したすべてのユーザに対してこの手順を繰り返します。

SWD-14800	v7.2 へのアップグレード後、Stealthwatch クラウドダッシュボードが登録ページに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。
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	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。

問題番号	説明	回避策
	は正確ではありません。	
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。『Stealthwatch 更新ガイド (v7.1.x から v7.2.1)』の手順に従っていることを確認します。 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-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、v7.2.1 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。 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

問題番号	説明	回避策
		グインします。[グローバル設定（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。 **アップグレード後**：v7.2.1 へのアップグレード後にこの問題が発生した場合は、各アプライアンスで次の手順を実行します。 **Stealthwatch 管理コンソール**：SMC 上の user.xml ファイルを削除し、tomcat を再起動します（`docker restart smc` を実行します）。これにより、パスワードがデフォルトのパスワードにリセットされます。 SMC ディレクトリ： `/lancope/var/smc/config/users/admin/user.xml` この問題が発生したすべてのユーザに対してこの手順を繰り返します。 **その他のアプライアンス**： 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、管理者としてアプライアンスにログインし、ユーザパスワードをリセットします。 [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

問題番号	説明	回避策
		す。
SWD-15150	SysAdmin ユーザとしてログインした場合、[システム設定（System Config）] メニューに [集中管理から削除（Remove from Central Management）] オプションがありません。	[集中管理（Central Management）] からアプライアンスを削除する必要がある場合は、ルートユーザとしてログインします。
SWD-15329	証明書エラー（.crt、エラー番号 13）のため、アプライアンスのインストール中にシステム設定を使用する権限が拒否されました。	証明書エラー（.crt）が原因で権限が拒否されたというエラーが表示された場合は、『7.2.1 Installation and Configuration Guide』を参照してください。「トラブルシューティング」の項の **IP アドレスの設定**の手順を参照してください。
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 v7.2.1 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 v7.2.1 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

問題番号	説明	回避策
		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。
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。

ログの変更

リビジョン	改訂日	説明
1_0	2020 年 5 月29 日	最初のバージョン
2_0	2020 年 6 月 9 日	• SecureX 統合セクションを更新しました。 • 「VMware」の項を更新しました。 • 「代替アクセス」の項からアプライアンス管理インターフェイスの手順を削除しました。 • 「ホストロック」の項を更新しました。
2_1	2020 年 6 月 17 日	• 「スタンドアロン アプライアンス」の項を更新しました。 • 既知の問題を更新しました。 • GA リリース日を更新しました。
2_2	2020 年 7 月 1 日	• Stealthwatch カスタマー コミュニティ セクションが追加されました。 • SecureX 統合セクションを更新しました。
2_3	2020 年 7 月 15 日	• 既知の問題を更新しました。
3_0	2020 年 7 月 27 日	• SWD-15423 を「修正点」のセクションに追加しました。
3_1	2020 年 8 月 10 日	• SWD-15550 を「既知の問題」に追加しました。
3_2	2020 年 8 月 19 日	• 「パスワードの変更」セクションを更新しました。
3_3	2020 年 9 月 10 日	• 「既知の問題」の SWD-15002 を更新しました。 • SWD-15570 を「既知の問題」に追加しました。
3_4	2020 年 9 月 11 日	• 「修正点」セクションを修正しました。
3_5	2020 年 9 月 28 日	• 「認証および認可サービス」セクションを更新しました。 • 「パスワードの変更」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

リビジョン	改訂日	説明
		た。 • SWD-15623 を「既知の問題」に追加しました。
3_6	2020 年 11 月 13 日	• スマートライセンスのケースメニューに関する手順を更新しました。

リリースサポート情報

リリース 7.2 の公式一般公開（GA）日は 2020 年 6 月 17 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