Cisco Secure Workload リリースノート、リリース 3.7.1.39

初版：2023 年 5 月 10 日

はじめに

このドキュメントでは、Cisco Secure Workload ソフトウェアパッチリリース 3.7.1.39 の機能、バグ修正、および動作の変更について説明します。このパッチは、Cisco Secure Workload ソフトウェアのメジャーリリース 3.7.1.5 に関連付けられています。メジャーリリースの詳細については、こちらを参照してください。

リリースバージョンと日付

バージョン：**3.7.1.39**

日付：**2023 年 5 月 10 日**

新機能および変更された機能に関する情報

この項では、このリリースの新機能と拡張機能、および既知の動作を示します。

互換性に関する情報

- OS のサポート終了に伴い、Windows 8.1 のエージェントパッケージは削除されました。

互換性の詳細については、Cisco.com の「プラットフォーム情報」を参照してください。

既知の動作

Cisco Secure Workload メジャーリリース 3.7.1.5 のリリースノートを参照してください。

新しいソフトウェア機能、新しいハードウェア機能、および廃止された機能

新しいソフトウェア機能

このリリースでは、新しいソフトウェア機能はありません。

新しいハードウェア機能

このリリースでは新しいハードウェア機能はありません。

廃止された機能

このリリースには、廃止された機能はありません。

拡張機能

- ユーザーの氏名は最大 40 文字です。
- フィルタリング時には、Contains 演算子が最初に表示されます。

動作における変更

- ラベル管理の UI で、ラベルの使用数に直接の使用数のみが含まれるようになりました。
- フロー学習されたインベントリは [範囲とインベントリ（Scopes and Inventory）] ページに表示されません。これは、ポリシー検出、ポリシー分析、および適用には影響しません。

検証済みスケーラビリティの制限値

次の表に、Cisco Secure Workload（39-RU）、Cisco Secure Workload M（8-RU）、および Cisco Secure Workload Cloud の拡張性の制限を示します。

表 *1 : Cisco Secure Workload*（*39-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 25000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 50,000（2x）。
1 秒あたりのフロー機能	最大 200 万。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	最大 100（非推奨）。

（注） サポートされているスケールは、最初に制限に達したパラメータに常に基づいています。

表 *2 : Cisco Secure Workload M*（*8-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 5,000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 10,000（2x）。

設定可能なオプション	規模
1 秒あたりのフロー機能	最大 500,000。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	最大 100（非推奨）。

（注） サポートされているスケールは、最初に制限に達したパラメータに常に基づいています。

表 *3 : Cisco Secure Workload Virtual（VMWare ESXi）の拡張性の制限*

設定可能なオプション	規模
ワークロードの数	最大 1,000（VM またはベアメタル）
1 秒あたりのフロー機能	最大 70,000。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	サポート対象外。

（注） サポートされているスケールは、最初に制限に達したパラメータに基づいています。

解決済みおよび未解決の問題

このリリースで解決済みの問題と未解決の問題には、Cisco Bug Search Tool を使用してアクセスできます。この Web ベースのツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品での問題と脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。

解決済みの問題

次の表に、このリリースで解決されたバグを示します。バグ ID をクリックして、シスコのバグ検索ツールにアクセスし、そのバグに関する詳細情報を表示します。

ID	見出し
CSCwe16875	アクセスルールごとに50ポートのFMC制限が適用され、50を超えるポートを含むポリシーは複数のアクセスルールに分割される。
CSCwf78123	[Linux] iptables-legacyが存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwe74218	読み取り専用CSWユーザーがOpenAPIを使用してユーザーラベルを作成および削除できる。
CSCwe21801	コネクタから取得したLDAP属性の比較で大文字と小文字が区別されない。
CSCwe32392	Cisco Secure Workload Anyconnectコネクタからの LDAP クエリの数が多い。
CSCwe20941	LDAP ローダーによる LDAP クエリがポーリング間隔ごとに2回実行される。
CSCwc97458	ワークロードCVE脆弱性検出ロジックで多数の誤検出が報告される。
CSCwd68433	ADMで承認済みポリシーが誤って削除される。
CSCwd64311	[デフォルト構成（Default Config）] ボタンをクリックしたときに、ADMで一部のフラグが設定されずに送信される。
CSCwe47738	[ポリシーの管理（Manage Policies）]をクリックしたときに、ワークスペースの最終更新時刻が現在の時刻に変更される。
CSCwe27066	Anyconnectコネクタ - コントローラのクラッシュ：フローデータをエクスポートできない。
CSCwd85744	ワークロードパッケージの削除がUIに反映されない。
CSCwf03825	AIXエージェントのインストーラがipfilter v5.3.0.7よりも新しいipfilterバージョンを認識しない
CSCwe38118	orchestrator_system/clusterに複数値を使用しようとすると、バッチインデクサのループがクラッシュする。
CSCwe02419	CSWアラートを有効にしても、エッジアプライアンスのコネクタに設定が適用されないことがある。
CSCwf18991	AIX：Catch-allがDENYの場合、DHCPが機能しない。
CSCwe38457	3.7へのアップグレードによってdruidのディスクがいっぱいになることがある。

未解決の問題

次の表にこのリリースで未解決の問題を示します。IDをクリックして、シスコのバグ検索ツールにアクセスし、そのバグに関する詳細情報を表示します。

ID	見出し
CSCwd67224	AIX 7.x で適用が有効になると、フラグメンテーションが原因でエージェントが CSW クラスタに接続できない。
CSCwf78123	[Linux] iptables-legacy が存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwd60340	リリース 3.6 からダウンロードしたエージェントインストーラ スクリプトでリリース 3.7 のセンサーがダウンロードされない。
CSCwb39541	タイムアウトしている Investigate Traffic クエリのエラーメッセージを変更します。
CSCwb91717	保留状態のソフトウェアエージェントの SW ステータスのアップグレードチャートのデータがない。
CSCwb80213	vNIC がベアメタルサーバーでハングアップする（BM の eNIC バージョンをアップグレードする必要がある）。
CSCwc63711	Azure セグメンテーションのアクセス許可がありません。
CSCwd93604	フローの取り込み率が非常に高いクラスタで druid のロードキューが高くなる。
CSCwe83822	3.7.1.22 からの Windows エージェントのアップグレードが MSI 署名チェックに失敗する場合がある。
CSCwb42177	ライブポリシーと適用ポリシーの分析：テーブルにカーソルを合わせると、範囲列とテキストが切り取られる。
CSCwf37266	AIX 適用ルールが、先頭にゼロが含まれるサブネットでは正しく一致しない。

関連資料

ドキュメント	説明
Cisco Secure Workload Cluster Deployment Guide	Cisco Secure Workload（39-RU） プラットフォームと Cisco Secure Workload M（8-RU）のシングルおよびデュアルラックインストールの物理的な構成、設置場所の準備、およびケーブル配線について説明します。 Cisco Tetration（Cisco Secure Workload）M5 クラスタハードウェア導入ガイド
Cisco Secure Workload Virtual Deployment Guide	Cisco Secure Workload 仮想アプライアンス（旧称 Tetration-V）の展開について説明します。 Cisco Secure Workload Virtual (Tetration-V) Deployment Guide
Cisco Secure Workload プラットフォームのデータシート	Cisco Secure Workload プラットフォームのデータシート
Cisco Secure Workload のドキュメント	Cisco Secure Workload のドキュメント
最新の脅威データソース	Cisco Secure Workload

シスコへのお問い合わせ

上記のオンライン リソースでは問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。