Cisco Secure Workload リリース 3.6.1.36 リリースノート

このドキュメントでは、Cisco Secure Workload ソフトウェアリリース 3.6.1.36 の新機能、不具合、および制限について説明します。

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 3.6.1.36 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 3.6.1.5 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、https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/release-notes/csw_rn_3_6_1_5.html を参照してください。

リリースノートは、制限や警告に関する新しい情報によって更新される場合があります。このドキュメントの最新バージョンについては、次の Web サイトを参照してください。

https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html

次の表は、このマニュアルのオンライン改訂履歴を示したものです。

表 1 オンライン変更履歴

日付	説明
2022 年 5 月 26 日	リリース 3.6.1.36 が利用可能になりました。

目次

このマニュアルの構成は、次のとおりです。

新機能および変更された機能に関する情報

このセクションでは、このリリースで追加された機能と変更された機能を一覧表示しており、次の項目を含みます。

新しいソフトウェア機能

- インベントリのアップロード：[インベントリアップロード（Inventory Upload）] で新しい [マージ（Merge）] オプションを使用できます。
- Infoblox 外部オーケストレータ：さまざまなタイプの DNS レコード（A レコード、AAAA レコード、ネットワークレコード、ホストレコード）を選択できるようになりました。
- 「ADM クラスタリング」と「範囲の提案」で Kubernetes インベントリがサポートされるようになりました。
- VDI 導入：インストールスクリプトと MSI インストーラの新しい *–goldenImage* フラグにより、Windows ゴールデン仮想マシンへのエージェントのインストールが可能になり、ホスト名が変更されると複製された VM でエージェントが実行されるようになりました（エージェントソフトウェアは、メンテナンスまたはアップグレードのために VM が起動する場合でも、ゴールデン VM で実行されることはありません）。

拡張機能

- FMC 外部オーケストレータ：FMC ドメインごとの適用のサポート。外部オーケストレータの設定時にドメイン名を選択することで、FMC ドメインで適用を有効または無効にできるようになりました。
- Windows のセグメンテーションポリシーで、単一のユーザー名に加えて、プロセスレベル制御セクションにユーザーまたはユーザーグループのリストを入力できるようになりました。
- インストーラスクリプトを作成するときに、ユーザーがインベントリラベルを指定できるようになりました。スクリプトでインストールされるすべてのエージェントに、それらのラベルが自動的にタグ付けされます。この機能は、Linux および Windows ワークロードの展開でのみサポートされています。

動作における変更

新しいエージェントのオペレーティングシステムのサポート

- AIX 7.3
- AlmaLinux 8.x
- Rocky Linux 8.x

Ingest アプライアンス

- AnyConnect アプライアンスで IPFIX V5 テンプレートをサポート

[エージェント（Agents）]

- Windows 2008 R2 以降のエージェントで NPCAP バージョン 1.55 を使用

警告

このセクションには、未解決および解決済みの警告と既知の動作のリストが含まれています。

未解決の不具合

次の表は、このリリースで開いている注意事項のリストです。バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

表 2 未解決の問題

不具合 ID	説明
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCvz95023	FMC-CSW オーケストレータ：プロトコルが any に設定されている場合、CSW で IPv6 ホップバイホップがプッシュされる
CSCvz99865	AWS フローログ：AWS フローログを使用したポリシー分析が機能しない。
CSCwb80090	Windows Server 2008 R2 と Cisco Secure Workload エージェントでクロックにずれがある
CSCwb97537	ライセンス数が正確でない

解決済みの不具合

次の表は、このリリースで解決済みの不具合のリストです。バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

表 3 解決済みの問題

不具合 ID	説明
CSCwb21235	namenode スイッチオーバースクリプトが namenode が起動するまで待機しないことがある
CSCwb25637	ゾーン転送で DNS 外部オーケストレータが失敗する
CSCwa17868	LDAP と統合されている場合、ISE コネクタで複数の memberOf 属性を処理できない
CSCwb27430	必要な場合にのみスクリプト API を選択する ServiceNow 設定のオプションを追加し、SNOW 統合に必要な最小ロールを cmdb_read に変更。
CSCwb11295	3.6 でポートなしで HTTP プロキシを有効にすると、AppServer の iptables テンプレートが破損する
CSCwb39558	パッチアップグレード後に AgentContainer および HelmChart のサービスが失敗する。
CSCwa64962	フェデレーション/DBR：ソースクラスタからのセンサー移行のステータスを特定できない
CSCvz95962	会話モード：会話モードの短時間の非 TCP フローでクライアントサーバーが反転することがある
CSCvz57161	EHN：Tet エージェントのインストール時にエージェントタイプの詳細情報の提供が必要
CSCvz32417	ENH：NPCAP バージョンの最新の 1.5 へのアップグレード

CSCwb01213	Cisco Tetration に Rocky Linux 8 との互換性がない
CSCwb25813	Cisco Secure Workload 適用エージェントで IPv6 サブネットが誤って集約されることがある
CSCwb71970	サイトの DNS リゾルバの設定の変更に失敗することがある
CSCwb83818	適用モードが WFP の場合に適用エージェントが Windows ファイアウォールサービスに依存する
CSCwb86649	40Gbps リンクのサーバーで実行されている ERSPAN センサーで 100Kpps しか受信しない
CSCwb92959	AppServer 仮想マシンの noisy.log のログローテーションが機能しない

既知の動作

- Cisco Secure Workload ソフトウェアのメジャーリリース 3.6.1.5 のリリースノート（https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/release-notes/csw_rn_3_6_1_5.html）を参照してください。

互換性に関する情報

互換性の詳細については、Cisco.com のプラットフォーム情報のページを参照してください。

使用上のガイドライン

- Cisco Secure Workload ソフトウェアのメジャーリリース 3.6.1.5 のリリースノート（https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/release-notes/csw_rn_3_6_1_5.html）を参照してください。

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 5 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 25,000（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 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基づいています。

表 6 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）。
1 秒あたりのフロー機能	最大 500,000 台
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基づいています。

表 7 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 1000（VM またはベアメタル）
1 秒あたりのフロー機能	最大 7 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	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常に基づいています。

関連資料

Cisco Secure Workload のドキュメントには、次の Web サイトからアクセスできます。

Cisco Secure Workload **プラットフォーム データシート**：http://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html

Cisco Secure Workload **ドキュメント**：https://www.cisco.com/c/en/us/support/security/tetration/series.html#~tab-documents

表 8 インストール マニュアル

ドキュメント	説明
Cisco Secure Workload クラスタ導入ガイド	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。 ドキュメントリンク： https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html
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。 ドキュメントリンク： https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html
Cisco Secure Workload アップグレードガイド	ドキュメント リンク: https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/upgrade/appliance/cisco-secure-workload-upgrade-guide.html 注：ベストプラクティスとして、メジャー バージョン アップグレードを実行する前に、クラスタにパッチを適用して使用可能な最新のパッチバージョンにすることを常に推奨します。
最新の脅威データソース	https://updates.tetrationcloud.com/ [英語]

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。