Cisco Secure Workload リリースノート、リリース 3.7.1.5

初版：2022 年 8 月 17 日

はじめに

Cisco Secure Workload プラットフォーム（旧称 Cisco Tetration）は、ファイアウォールとセグメンテーション、コンプライアンスと脆弱性の追跡、動作ベースの異常検出、およびワークロードの分離を使用して、オンプレミスやマルチクラウド環境全体のすべてのワークロードにマイクロ境界を確立することにより、包括的なワークロードセキュリティを提供するように設計されています。このプラットフォームでは、高度な分析とアルゴリズムのアプローチを使用して、これらの機能を提供します。

このソリューションは、次の機能をサポートしています。

- アプリケーションの通信パターンと依存関係の包括的な分析から自動的に生成されるマイクロセグメンテーション ポリシー
- ロールベースのアクセス制御による複数のユーザーグループの包括的な制御をもたらす、階層型ポリシーモデルを使用した動的なラベルベースのポリシー定義
- ネイティブ オペレーティング システム ファイアウォール、および ADC（アプリケーション デリバリ コントローラ）や物理ファイアウォールまたは仮想ファイアウォールなどのインフラストラクチャ要素の分散制御による、一貫したポリシーの大規模な適用
- すべての通信のほぼリアルタイムのコンプライアンス モニタリングにより、ポリシー違反または潜在的な侵害を特定して警告
- ワークロード動作のベースライン化とプロアクティブな異常検出
- 動的な緩和と脅威ベースのワークロード分離を行う、一般的な脆弱性の検出

Cisco Secure Workload プラットフォーム内での分析とさまざまな使用事例をサポートするため、環境全体からの一貫したテレメトリ（フローデータ）が必要です。Cisco Secure Workload は、ソフトウェアエージェントやその他の方法を使用して豊富なテレメトリを収集し、データセンターのインフラストラクチャ内にある既存と新規の両方のインストールをサポートします。

このリリースでは、次のテレメトリソースがサポートされています。

- 仮想マシンおよびベアメタルサーバーにインストールされている Cisco Secure Workload エージェント
- コンテナホストのオペレーティングシステムで実行されているデーモンセット

- ミラーリングされたパケットから Cisco Secure Workload テレメトリを生成できる ERSPAN コネクタ
- アプリケーション デリバリ コントローラ（ADC）からのテレメトリの取り込み：F5 と Citrix
- Cisco Secure Workload テレメトリベースの NetFlow v9 または IPFIX レコードを生成できる Netflow コネクタ
- NetFlow セキュアイベントロギング（NSEL）テレメトリを収集するための ASA コネクタ
- VPC フローログ構成を使用して生成されたフローテレメトリデータ用の AWS コネクタ
- NSG フローログ構成を使用して生成されたフローテレメトリデータ用の Azure コネクタ

さらに、このリリースでは、以下との統合によるエンドポイントデバイスのポスチャ、コンテキスト、およびテレメトリの取り込みもサポートされています。

- ラップトップ、デスクトップ、スマートフォンなどのエンドポイントデバイスにインストールされた Cisco AnyConnect
- Cisco ISE（Identity Services Engine）

また、Cisco Secure Workload エージェントは、アプリケーション セグメンテーションのポリシー適用ポイントしても機能します。このアプローチを使用して、Cisco Secure Workload プラットフォームは、パブリック、プライベート、およびオンプレミスの展開全体で一貫性のあるマイクロセグメンテーションを実現します。エージェントはネイティブのオペレーティングシステム機能を使用するポリシーを適用し、データパスにエージェントを置く必要がなく、フェールセーフなオプションが提供されます。その他の製品マニュアルについては、「関連資料」の項を参照してください。

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

新しいルートスコープの作成直後に新しいコネクタを有効にすると、Cisco Secure Workload の UI に誤った AWS コネクタワークフローが表示されます。（CSCvz43857）

[AWS インベントリプロファイル（AWS inventory profile）] ページでは、コネクタでセグメンテーションが有効になっている場合でも、有効になっている適用が無効として表示されます。

ISE コネクタは、SAN のない SSL 証明書を持つ pxGrid エンドポイントへの接続に失敗します。

ISE コネクタが構成されている場合は、それらの TLS 証明書に SAN（subjectAltName）拡張セクションがあることを確認します。アップグレード後、ISE コネクタは、従来の CN 専用 TLS 証明書を提示する ISE エンドポイントに接続しません。

ISE pxGrid TLS 証明書が SAN 拡張で再生成されるまではアップグレードを続行しないでください。

特記事項

この項では、Cisco Secure Workload ソフトウェアに関する重要な注意事項をいくつか示します。

- Web ベースのユーザーインターフェイスにアクセスするには、Google Chrome ブラウザバージョン90.0.0 以降を使用する必要があります。
- DNS を設定した後、Cisco Secure Workload クラスタの URL（https://<cluster.domain>）まで参照します。
- Cisco Secure Workload 仮想アプライアンス環境でコミッション/デコミッション機能を使用する場合は、次の使用上のガイドラインに従ってください。
  - この機能は TAC の支援を受けて使用することを意図しており、誤って使用すると回復不能な障害を引き起こす可能性があります。TACからの明示的な承認がない限り、2つの VM を同時にデコミッションしないでください。次の VM の組み合わせは、同時にデコミッションしないでください。
    - 複数のオーケストレータ
    - 複数のデータノード
    - 複数の namenode（namenode または secondaryNamenode）
    - 複数の resourceManager
    - 複数の happobat
    - 複数の mongodb（mongodb または mongoArbiter）
    - 一度に実行できるデコミッション/コミッションプロセスは1つだけです。異なるVMのデコミッション/コミッションを同時にオーバーラップしないでください。

（注） esx_commission スナップショット エンドポイントを使用する前に、必ず TAC にご連絡ください。

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

機能名	説明
エージェントとエージェントレスのマイクロセグメンテーション	
Azure コネクタ検出のワークフローのサポート	Cisco Secure Workload 3.7 は、Cloud Connector を使用して Azure と Azure Kubernetes Services（AKS）をサポートします。 Azure クラウドコネクタを作成し、メタデータの取り込みを有効にして、Azure ベースのワークロードからラベルとフローデータを取り込み、ネットワーク セキュリティ グループ（NSG）を介してポリシーを適用できるようになりました。各ワークロードにエージェントをインストールする必要はありません。 Azure コネクタを使用して、AKS で実行されている Kubernetes ワークロードからラベルを取得することもできます。 この機能はベータ版です。 詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「*Azure Connector*」を参照してください。
マネージド Kubernetes サービスのサポート：GKE	Cisco Secure Workload 3.7 は、Google Cloud Platform（GCP）コネクタを使用したマネージド Kubernetes サービスをサポートするようになりました。 GCP コネクタは、Google Kubernetes Engine（GKE）を介して展開および管理されるコンテナのフローの可視性をサポートしており、選択したすべての Kubernetes クラスタからノード、サービス、ポッドのメタデータを収集するのに役立ちます。 GCP コネクタの使用方法の詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「*Managed Kubernetes Services Running on GCP（GKE）*」の項を参照してください。
FQDN/DNS ドメイン名ベースのフローの可視性	Cisco Secure Workload 3.7 リリースから、コンシューマとプロバイダーに関連付けられた FQDN/DNS ドメイン名を表示するための新しいオプションが [フロー検索（Flow Search）] ページに導入されました。 [フィルタ検索（Flow Search）] ページにあるテーブルフィルタは、IP アドレスに基づいてフィルタ処理できるドメイン名を表示するように構成できるようになりました。[フロー検索（Flow Search）] テーブルは、IP アドレスに関連付けられたコンシューマとプロバイダーのドメイン名を表示するように構成できるようになりました。 テーブルフィルタの構成方法の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。

機能名	説明
パブリッククラウドの Kubernetes サービスオブジェクトタイプのロードバランサのサポート	このリリースでは、ワークロードからメタデータを収集するために、パブリック クラウド プラットフォーム用の Kubernetes ロードバランササービスが導入されました。 [ワークロードインベントリ（Workloads Inventory）] ページの [サービス（Services）] タブで、ロードバランサのリストと、他の方法では外部オーケストレータを介してのみ検出された他の Kubernetes サービスを表示できるようになりました。 この詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。
新しいメニュー項目	Cisco Secure Workload 3.7 では、セキュア コネクタ クライアントのメトリックが [外部オーケストレータ（External Orchestrators）] ページから移動されました。 この変更により、ステータス行をクリックするだけで、[セキュアコネクタ（Secure Connector）] ページで追加のクライアントメトリックを表示できます。これらのメトリックは、[一般（General）] 列、[インターフェイス（Interface）] 列、および [ルート（Routes）] 列の下に表として表示されるため、エラーのトラブルシューティングに関連する情報を見つけるのに役立ちます。 詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの 「*Secure Connector*」の項を参照してください。
KVM ベースの仮想アプライアンス（Edge と Ingest）	Cisco Secure Workload 3.6 以前のリリースには、ESXi ホスト用の OVA テンプレートをダウンロードするための規定がありました。Cisco Secure Workload 3.7 以降では、QCOW2 イメージをダウンロードして、KVM ベースの環境に Cisco Secure Workload 仮想アプライアンス（Ingest と Edge）を展開できます。 詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドの「*Virtual Appliances for Connectors*」の項を参照してください。
エージェント展開の強化	Cisco Secure Workload 3.7 リリースでは、インストーラスクリプトが拡張され、スクリプトの使用を制限できるようになりました。これにより、スクリプトの使用方法をより詳細に制御できます。 このリリースから、インストーラスクリプトを使用する期間を、利用可能な一連のオプションから実際に選択できるようになりました。 その方法の詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「*Install the Agent*」の項を参照してください。
ユーザーエクスペリエンスの向上	

機能名	説明
ヘルプメニューの向上	Cisco Secure Workload 3.7 リリースでは、UI の [ヘルプ（Help）] メニューが大幅に拡張され、ユーザーが探している情報にアクセスできるようになりました。 ヘルプメニューには、ページ レベル（状況依存）の ヘルプ、ドキュメントセット/ビデオへの簡単なアクセスなど、役立つリンクがいくつかの追加されました。特定のリリースの新機能、[ソフトウェアダウンロード（Software Download）] ページへのクイックアクセス、プラットフォーム情報、サポートされているオペレーティングシステムと要件、およびクリックするだけで他の多くの情報の確認できます。
オーケストレータおよびコネクタ構成のデータのバックアップと復元	このリリースでは、データのバックアップと復元機能が拡張され、外部オーケストレータとコネクタの構成が含まれるようになりました。 この機能強化により、Cisco Secure Workload クラスタのデータと構成を別のオフサイトストレージにコピーできるようになりました。また、これには、外部オーケストレータのこれらの構成も含まれます。障害や事故が発生した場合、これらのストレージにバックアップされたデータを使用して、新しいシステムを簡単に復元できます。 拡張機能については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。
新しいクイックスタートウィザード	現在、スコープが定義されていない場合、このリリースから、スコープツリーの最初のブランチを作成する手順を案内できる新しいウィザードが用意されています。これは、選択したアプリケーションのポリシーを検出して適用するための最初のステップです。 このウィザードは、ラベル、スコープ、および階層型スコープツリーの機能を説明し、これらの概念すべてがどのように関連しているかを示します。 詳細については、『Cisco Secure Workload Quick Start Guide』(英語）を参照してください。
ポリシー管理のワークスペースの向上	各スコープのポリシーを操作するときに表示されるワークスペースが再設計され、セグメンテーションの目標を達成しやすくなりました。 変更の中で「ADM」は、この強力な機能が実際に行うことをより適切に反映するため、名前が「ポリシーの自動検出」に変更されました。 ワークスペースの改善の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。

機能名	説明
ラベルの影響分析	Cisco Secure Workload 3.7 では、ユーザー定義ラベルが拡張され、カスタムラベルの使用方法が表示されるようになりました。 [ユーザーがアップロードしたラベル（User Uploaded Labels）] ページで、これらのカスタムラベルを使用して、インベントリ、スコープ、またはフィルタの使用状況を表示できるようになりました。これらのカスタムラベルのいずれかを編集する必要がある場合は、使用状況を表示することが重要です。これは、変更がこれらのカスタムラベルを使用するスコープ、フィルタ、およびポリシーに直接影響するためです。 これらの使用法の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。
古いエージェントレコードの自動クリーンアップ	多くの実環境展開では、古いエージェントレコードが仮想マシンに蓄積されるいくつかのインスタンスが存在する可能性があり、これにより、最終的にエージェント ステータス アラートのデータベースが増大します。 Cisco Secure Workload リリース 3.7 を起動すると、VM 上の非アクティブなエージェントをクリーンアップするプロセスが自動化されるため、指定した期間が経過した後に非アクティブなエージェントを削除するという手間のかかる手動タスクが不要になります。 指定した期間内にエージェントで自動クリーンアップを有効にする方法の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドの「*Creating an Agent Config Profile*」の項を参照してください。
IPv6 サポート（デュアルスタックモード）	IPv6 サポートの要件と制限については、cisco.com の『Cisco Secure Workload Upgrade Guide』（英語）を参照してください。
Microsoft Edge ブラウザのサポート	このリリースで Microsoft Edge ブラウザのサポートが導入されました。
統合とエコシステム	

機能名	説明
Cisco Secure Firewall Management Center の統合	Cisco Secure Workload 3.7 リリースでは、**Secure Firewall Management Center**（FMC）の統合により、**Cisco Secure Workload**（CSW）のスケールロードをより適切に管理できるようになりました。 CSW は数千の IP アドレスをスケールアップでき、ハイエンドアプライアンスでは150万に達することもあり、動的オブジェクトのマッピング数は最大 300k に達することもあります。ただし、動的オブジェクトごとに数千のマッピングを行う場合、統合がどのように動作するかはまだ明確ではありませんでした。さらに、アグレッシブすぎる統合を避けるためにFMCに設定された「要求制限」があり、この制限では単一の IP から 1 分あたり 120 件を超える要求は許可されませんでした。 このスケールロードの管理方法の詳細については、『Secure Firewall Management Center and Secure Workload Integration Guide』（英語）を参照してください。
Cisco Secure Firewall Management Center のルール順序の管理	Cisco Secure Workload 3.7 では、**Cisco Secure Workload**（CSW）の [外部オーケストレータ（External Orchestrator）] ページから **Cisco Secure Firewall Management Center**（FMC）で Cisco Secure Workload ルールの順序を構成するためのサポートが提供されています。 この機能強化により、Cisco Secure Workload ルールがリストされる順序を、FMC の既存のアクセス制御ルールの上または下に指定できるようになりました。さらに、FMC でのアクセス制御ポリシーのデフォルトアクションの代わりに、Cisco Secure Workload からのキャッチルールを使用するオプションを有効にすることもできます。これらの機能は、Cisco Secure Workload の [外部オーケストレータ（External Orchestrator）] ページで構成されるようになりました。 詳細については、『Cisco Secure Workload and Firewall Management Center Integration Guide』（英語）を参照してください。

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

表 *1 : Cisco Secure Workload* リリース *3.7.1.5* で廃止された機能

機能	機能説明
Neighborhood アプリケーションの廃止	Cisco Secure Workload リリース 3.7.1.5 では、次の機能がサポートされなくなりました。 • パフォーマンス モニターリング • 見張り • ハードウェアエージェント構成とハードウェアエージェントのダウンロード • ダッシュボードフロー、ダッシュボードビュー、ダッシュボードカスタム • ソフトウェアエージェントからのユニバーサル可視性エージェントのタイプ

拡張機能

- ソフトウェアエージェントは、ppc64le アーキテクチャで SUSE Linux Enterprise Server 12 および 15 をサポートするようになりました。
- ソフトウェアエージェントは、ppc64le アーキテクチャで Redhat Enterprise Server 7 および 8 をサポートするようになりました。
- ソフトウェアエージェントは、x86_64 アーキテクチャで Ubuntu 22.04 をサポートするようになりました。
- ソフトウェアエージェントは、x86_64 アーキテクチャと s390x アーキテクチャで Red Hat Enterprise Server 9 をサポートするようになりました。
- 標準の Kubernetes/OpenShift 外部オーケストレータの新しいオプションが導入され、改善された ADM クラスタリングのラベルメタデータが組み込まれました。この機能強化により、ロールベースのアクセス制御（RBAC）権限の要件が変更されました。

  必要な新しい RBAC 権限の詳細を表示するには、『Cisco Secure Workload Upgrade Guide』（英語）を参照してください。
- [セキュアコネクタ（Secure Connector）] ページから最新の Secure Connector クライアントの RPM をダウンロードできるようになりました。
- [セキュアコネクタ（Secure Connector）] ページから 1 回限りの登録トークンを生成することもできます。
- ユーザーは、プロセスとフォレンジックの可視性セクションのエージェント構成プロファイルで、プロセスとパッケージの可視性を選択的に無効にできるようになりました。

- FMC では、動的オブジェクト名が人間可読式になりました。
  - FMC ルール順序の管理での改善
  - ユーザーは、[高/上（High/Top）] または [低/下（Low/Bottom）] の優先順位を選択して、絶対ポリシーを [必須（Mandatory）] セクションにプッシュできます。
  - ユーザーは、[高/上（High/Top）] または [低/下（Low/Bottom）] の優先順位を選択して、デフォルトのポリシーを [デフォルト（Default）] セクションにプッシュできるようになりました。
- ユーザーは、[CSW キャッチオール（CSW catch-all）] オプションまたは [CSW キャッチオールを無視（ignore CSW catch-all）] オプションから選択できるようになりました。
- ユーザーは、ソフトウェア エージェント インストーラ スクリプトの有効期限を設定できるようになりました。
- ユーザーは、エージェント構成プロファイルで期間を設定できるようになりました。この期間を過ぎると、非アクティブなエージェントが自動的に削除されます。
- 入力した IP アドレスと一致するアイテムが複数ある場合、ユーザーはクイック分析で特定のコンシューマ/プロバイダーインベントリを選択できるようになりました。
- ユーザーは、[クラスタ構成（Cluster Configuration）] ページの [設定（Settings）] を使用して、新しいソフトウェアエージェントがクラスタにグローバルに登録されたり、自動アップグレードされないようにすることができるようになりました。
- SPAN エージェントが IPv6 ERSPAN パケットを処理できるようになりました
- セグメンテーション ワークスペースは、ワークスペースやバージョンの選択など、より多くのナビゲーションオプションで強化されており、スコープツリーと状態が組み合わされた絶対ポリシーとデフォルトポリシーのテーブルで構成されています。
- ユーザーは、KVM ベースの（qcow2 形式）アプライアンス（Ingest と Edge）を使用できるようになりました。
- Azure コネクタで複数のサブスクリプションがサポートされるようになりました。
- 3.7 リリースにアップグレードすると、クラスタリーフとスパインスイッチのファームウェアが NX-OS および EPLD バージョン 9.3(8) にアップグレードされます。
- [インベントリアップロード（Inventory Upload）] ページが変更され、ユーザーは上位 5 つの値とすべてのラベルの使用状況を確認できるようになりました。
- 3.7 リリースの Hadoop クラスタは、バージョン 3.2.2 にアップグレードされました。
- Cisco Secure Workload クラスタの内部にあるすべての仮想マシンは、現在 CentOS バージョン 7.9 を使用しています。
- 3.7 リリースにバンドルされている M5 ハードウェア用の Cisco Integrated Management Controller（CIMC）Host Upgrade Utility（HUU）は、バージョン 4.1(3f) に更新されました。

- 3.7 OVA で作成されたすべてのコネクタアプライアンスは、IPv6 アドレス構成をサポートし、デュアルスタックモードで実行されている CSW クラスタに接続します。
- 外部オーケストレータ：Vcenter/Infoblox/DNS は、ホストリストにある IPv6 アドレスに解決される IPv6 アドレスと DNS 名をサポートするようになりました。

動作における変更

- ユニバーサルエージェントは、Cisco Secure Workload でサポートされなくなりました。
- ハードウェアセンサーは、Cisco Secure Workload でサポートされなくなりました。
- Cisco Secure Workload Agent は、SUSE Linux Enterprise Server 11 をサポートしなくなりました。
- Cisco Secure Workload クラスタと外部 S3 サーバー間のデータ交換で、GCM ベースの暗号がサポートされるようになりました。
- Windows エージェント用のエージェント構成プロファイルのデフォルトの適用モードは WFP になりました。
- 外部認証と TaaS の削除時間が 6 時間から 9 時間に延長されました。

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 *2 : 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。

表 *3 : 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。

表 *4 : 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。

（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。

解決済みのバグと未解決のバグ

このリリースで解決済みのバグと未解決のバグには、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。

（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。

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。

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。

表 *5 :* 解決済みの問題

不具合 ID	説明
CSCwc17237	ネットワークの可視性を無効にすると、プロセス/パッケージの可視性も無効になります
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。
CSCwc23159	RHEL 8.x 適用エージェントが [アップグレード（Upgrade）] タブに表示されない
CSCwc53834	namenode サービスを停止すると、誤ったポリシー更新がワークロードにプッシュされる場合がある

不具合 ID	説明
CSCwc32016	Netflow センサーが受信した netflow データをドロップした。
CSCwa44839	Tetration N9K スイッチの脆弱性を評価/修正
CSCwc37463	正規表現クエリを使用すると、スコープメンバーシップにメンバーが 0 と表示される。
CSCvz66166	フェデレーションでは、ワークロードプロファイルのページからエージェントログはダウンロードできない。
CSCwb94169	スタンバイクラスタで kafka FQDN を変更するときにエラーが発生する。
CSCwc59065	特定の IPv6 の範囲でポリシーを処理すると、適用エージェントが再起動することがある。

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
CSCwb80213	vNIC がベアメタルサーバーでハングアップしています。回復するにはサーバーの再起動が必要です。
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。
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。
CSCwc47484	[ソフトウェア エージェント リスト（Software Agents Agent List）] ページにエージェントリストが正しく表示されない。
CSCvz98522	フェデレーションでは、コンプライアンス適用アラートは使用できません。
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。
CSCwc47484	[ソルトウェアエージェントリスト（Software Agents List）] ページにエージェントリストが正しく表示されない
CSCwc63711	Azure セグメンテーションのアクセス許可がありません。

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。