Cisco Tetration リリース ノート

リリース 3.5.1.17

このマニュアルでは、Cisco Tetration ソフトウェア リリース 3.5.1.17 の機能、不具合、および制限について説明します。このリリースは、以前のすべての 3.5.1.x リリースを置き換えます。

Cisco Tetration プラットフォームは、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、オンプレミスおよび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。プラットフォームには、次の機能をサポートする、すぐに使用可能なソリューションが用意されています。

- 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 Tetration プラットフォーム内での解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データが必要です。豊富な Cisco Tetration テレメトリがソフトウェアエージェントやその他の方法を使用して収集され、データセンター インフラストラクチャでの既存および新規のインストールの両方をサポートします。このリリースでは、次のエージェントタイプがサポートされています。

- 仮想マシン、またはベアメタルサーバにインストールされているソフトウェアエージェント
- コンテナホスト 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
- コピーされたパケットから Cisco Tetration テレメトリを生成できる ERSPAN エージェント
- ADC（アプリケーション デリバリ コントローラ）からのテレメトリの取り込み：F5 および Citrix
- Netflow v9 または IPFIX レコードに基づいて Cisco Tetration テレメトリ ベースを生成できる Netflow エージェント

さらに、このリリースでは、以下のもの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得が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 Identity Services Engine（ISE）

また、ソフトウェアエージェントもアプリケーション セグメンテーションのポリシー適用ポイントとして機能します。このアプローチを使用して、Cisco Tetration 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。

これらのリリース 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。

http://www.cisco.com/c/en/us/support/data-center-analytics/tetration-analytics/tsd-products-support-series-home.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
2021 年 4 月 22 日	リリース 3.5.1.17 が使用可能になりました。 このリリースは、以前のすべての 3.5.1.x リリースを置き換えます。

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

- Cisco Firepower Management Center（FMC）との統合：この統合により、多層防御のセキュリティと、アプリケーション ワークロードの一貫したセグメンテーションの利点を環境全体で実現できます。
  - 適切な API 接続情報とクレデンシャルを提供することにより、外部オーケストレータページからセキュリティポリシーの適用ポイントとして Cisco FMC を追加できます。
  - 注：スタンドアロン FTD はこの機能ではサポートされません。
- Amazon Web Services（AWS）Elastic Kubernetes Services（EKS）クラスタに導入されたコンテナワークロードのマイクロセグメンテーションをサポートします。
  - 外部オーケストレータとして Kubernetes を追加するときに、AWS EKS オプションを選択できます。管理者は、AWS IAM クレデンシャルとユーザロールバインディングの詳細を提供する必要があります。
- Red Hat OpenShift 4.x を介して導入されたコンテナワークロードのマイクロセグメンテーション サポートが利用可能になりました。OpenShift 4.x は、Kubernetes のデフォルトのコンテナランタイムとして CRI-O を使用します。CRI-O がサポートされており、このような環境で実行するために既存の適用ワークフローを変更する必要はありません。ワーカーノードのオペレーティングシステムには、OpenShift 4.x で公式にサポートされている RHEL または CentOS のいずれかのバージョンが使用できます。
  - このリリースは、Red Hat OpenShift バージョン 4.6 までをサポートします。
  - このリリースでは、Red Hat CoreOS はワーカーノードのオペレーティングシステムとしてサポートされていません。
- オンプレミス展開の場合のみ：業界標準の STIX / TAXII プロトコルによるサードパーティの脅威インテリジェンス情報のサポート。
  - TAXII ソースタイプ、TAXII ベンダー、TAXII ポーリング URL、コレクション、およびポーリング日数情報を追加します。
  - セキュリティダッシュボードおよび [workload profile file hashes] タブ：STIX ソースからのハッシュ判定の詳細を表示します。
- 既存の表形式の表示オプションに加えて、ポリシーデザイナキャンバスが追加されました。このデザイナキャンバスは ADM ワークスペースの [App view] オプションに代わるものです。
  - [App view] オプションは、このリリースへのアップグレード前に作成され保存されたアプリケーションビューを持つワークスペースで引き続き使用できます。

- Windows サーバワークロードについて Windows Filtering Platform（WFP）を使用する新しい適用オプション。管理者は、エージェント設定ページからこのオプションを有効にできます。
  - [Enforcement] カテゴリで使用できる設定オプションの [Windows Enforcement Mode] では、[WFP]（Windows エージェントでの Windows Filtering Platform の有効化）または [WAF]（Windows エージェントでの Windows Advanced Firewall の有効化）を選択できます。デフォルトでは [WAF] モードが選択されます。
- このリリースでは、ソフトウェアエージェントを使用する場合の新しいフローテレメトリ収集オプションが追加されました。
  - [Flow Visibility] カテゴリの [Flow Analysis Fidelity] 設定オプションでは、[Conversations]（すべてのエージェントの要約フローテレメトリモード）または [Detailed]（すべてのエージェントの完全なフローテレメトリモード）を選択できます。デフォルトでは [Detailed] が選択されます。
- すべてのワークロード保護機能をサポートするために Amazon Linux 2 に追加されたソフトウェア エージェント サポート
- このリリースでは、AIX の詳細な可視性と適用エージェントがすべてのお客様に一般的に利用可能になりました。
  - OS バージョン：7.1、7.2（PPC）
  - 適用を使用するには、ipfilter パッケージバージョン 5.3.0.7 がインストールされ、ワークロードで動作している必要があります。
  - 他のアクティブな AIX またはサードパーティ製ファイアウォールは有効にしないでください。ネイティブの AIX ファイアウォールコマンド（genfilt、chfilt、rmfilt、mkfilt、expfilt、impfilt）を使用しないでください。
- ソフトウェア エージェント インストールをインストールすると、次の新機能を使用できます。
  - デフォルトのインストールディレクトリを変更し、カスタム インストール ディレクトリを指定するオプション
    - Ubuntu および AIX では使用できません。
  - デフォルトのログファイルディレクトリを変更し、カスタム ログファイル ディレクトリの場所を指定するオプション
  - インストールスクリプトで新しいユーザを作成する代わりに、既存の非特権ユーザを使用する
    - Linuxの場合：インストーラスクリプトはこのユーザの Sudo 機能をテストします。
    - Windowsの場合：MSI インストーラは、既存のサービスユーザを指定するオプションを提供します。ここには、AD で管理されているサービスアカウントを指定できます。
- User Session Configuration：[User Idle Session Timeout] は、ユーザのアクティビティがないときにタイムアウトする間隔です。この期間は、オンプレミスアプライアンスごとに、[Company] の [User Session Configuration] で、および Cisco Tetration SaaS では [Organization] の [User Session Configuration] で設定できます。
- Cisco Tetration SaaS は、SAML 2.0 を使用する組織の認証システムを介したユーザ認証のための ID フェデレーションをサポートします。
- Ubuntu の場合、ソフトウェアエージェントはネイティブな .deb パッケージを使用するようになりました。これは、インストールスクリプトでのみサポートされており、/opt/cisco/tetration という新しい固定の場所にインストールされます。
  - 従来のパッケージ化されたインストールは、rpm のサポートを必要とするため推奨されません。
  - これを使用するには、root として（sudo を使用してではなく）インストールした rpm を実行している必要があります。
- ERSPAN アプライアンスで Tetration UI Connector ワークフローが有効になりました。これにより、管理者はアプライアンスの ISO 設定ディスクを生成できます。
- ERSPAN 仮想アプライアンス ISO 設定ファイルの生成は、Tetration UI の取り込みアプライアンス コネクタ ワークフローと統合されています。このファイルを生成するための管理者向けの設定ウィザードとワークフローを提供します。

拡張機能

- Tetration プラットフォームで提供される脆弱性情報の強化：

  - Ubuntu OS および Windows .Net パッケージの CVE 誤検出を削減
  - Windows オペレーティングシステムの脆弱性を報告
  - 既知の CVE のエクスプロイト情報を提供
  - CVE 情報を取得するための Open API のサポート
- 範囲でフィルタされた適用ステータス：適用ステータスページで、ルートまたは子スコープによるステータスデータのフィルタリングがサポートされるようになりました。これにより、テナントオーナーは、テナントルートスコープの一部である任意のサブスコープでステータスデータをフィルタリングできます。
- 適用ステータスのワークスペースレベルの詳細：ワークスペースの現在の範囲の適用ステータスの詳細は、アプリケーション ワークスペース ページのタブとして使用できます。
- 適用の影響分析：4 つの手順から成るポリシー適用ウィザードによって、適用（またはロールバック）するポリシーの変更を表示および選択し、ポリシーの変更の影響を受ける可能性のある適用エージェントでワークロードを検査し、以前のワークスペースから目的のポリシーが適用されていることを確認し、ポリシーの適用を有効化/更新する前に概要を確認できます。
- 適用ポリシーの更新をグローバルに一時停止する：ポリシーの更新を一時停止すると、すべての適用ポイントでファイアウォールルールの更新が行われなくなります。このコントロールは、適用ステータスページにあります。この機能は、サイト管理者およびカスタマーサポート用です。
  - 注：これは、現在のユーザのスコープに関係なく、グローバル設定です。
- OpenAPI API キーの警告：LDAP を使用した認証と許可が有効になっている場合、Tetration UIに、個々のユーザの API キーページとユーザウィザードのユーザ詳細ページに警告が表示されるようになりました。この警告は、LDAP 認証が有効になっている場合に、OpenAPI API エンドポイントへのアクセスが中断されないよう、ユーザを「ローカル認証」に設定するよう推奨することを示しています。
- 物理 Tetration ハードウェアクラスタでは、CIMC 外部化プロセスが簡素化されました。CIMC 外部化を有効にすると、クラスタステータスページで特定のベアメタルノードを展開し、CIMC IP アドレスをクリックすることで、CIMC WebUI にアクセスできます。また、CIMC 外部化機能により、外部化を更新できるようになりました。
- 物理クラスタについて、クラスタ スイッチ インターフェイスがモニタされるようになりました。重要なインターフェイスがアップ状態でないことが判明した場合は、[Service Status] ページに ClusterSwitches サービスに異常があることが表示されます。さらに、サービスが 1 時間の 80 % にわたって正常でない場合、プラットフォームアラートが生成されます。

動作における変更

このリリースの動作には次のような変更があります。

- ソフトウェア エージェント リスト：csv としてダウンロードされるテーブルデータが、ソフトウェア エージェント モデルから返される一連のキーと比較して、より読みやすい列に更新されました。
- Tetration sub-Agent バイナリごとの機能サポートを反映するための Agent Config Page の UI の拡張。[Visibility] を [Flow Visibility] に、[Forensics] を [Process Visibility and Forensics] にそれぞれ名称を変更しました。
- Tetration のすべての機能について、[Tags] と [Annotations] を [Annotations] に名称を変更しました。
- 訪問履歴に関連するすべての機能（タブ/コンポーネント/ルート/機能）を削除しました。
- Tetration-V ESXi クラスタの Ubuntu ベースの仮想マシンでは、ルートディスクのサイズが 8 ギガバイトから 12 ギガバイトに増加しました。
- Workload Active Directory（WAD）コネクタ（アルファ機能）のサポートは、このリリースから削除されました。WAD コネクタが設定されている場合は、このリリースにアップグレードする前に無効化/削除することをお勧めします。

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。

- Open Caveats
- 解決済みの不具合 (p.11)
- 既知の動作

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
CSCvx47947	kubernetes デーモンセットエージェントのアンインストールには jq ユーティリティが必要
CSCvx48421	（静的適用）適用ポリシーの更新の一時停止は、現在のリリースのフェデレーション設定ではサポートされていない。
CSCvx29180	ホストネットワークからクラスタ IP サービスへの Kubernetesトラフィックが Tetration ポリシーをエスケープする。
CSCvy09666	アドレス 10.1.[0-X].0/24 をもっているエージェントが 3.5 へのアップグレード後にコレクタに接続できない
CSCvy10749	クイック分析とポリシー分析で、WFP モードで実行している Windows エージェントの結果が正しくない

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
CSCvw71876	ユーザガイドがスコープおよびテナント関連の UI 動作と一致しない
CSCvw91543	bash をアップグレードして https://access.redhat.com/errata/RHSA-2020:1113 を修正
CSCvp58515	ユーザ ID を小文字にする必要がある旨の注意書きをユーザガイドに追加。
CSCvx00402	ドライブの予測可能な障害エラーが発生すると、ノードとディスクの解放が失敗する
CSCvo19895	/local/tetration/log/tet-ldap-loader ログには AnyConnect VM のタイムスタンプが必要

CSCvx13733	攻撃対象領域テーブルは、スコアが低くなる原因となっているオープンポートと未使用ポートのみを表示すると想定しているユーザに対して混乱を生じさせる。
CSCvu92078	ポリシー分析のフロー出力では、インバウンドポリシーとアウトバウンドポリシーが区別される。ユーザは、キャッチオールポリシーがコンシューマ側またはプロバイダー側のどちらに適用されたかを判別できる。
CSCvw90465	ダッシュボードメトリックのユーザガイドドキュメント
CSCvx74789	Enforcement Agent のアップグレードにより Windows Advanced Firewall が有効になる
CSCvy09069	Tetration 3.5.1.1 クラスタと組み合わせた Linux 3.4.1.1 適用エージェントが適用できない。
CSCvx48433	ユーザガイドに新しいエンドポイント toggle_chassis_locator への参照がない
CSCvx42262	コマンド get_cimc_techsupport が機能しなくなった（またはドキュメントを更新する必要がある）
CSCvw64156	Tetration コネクタアプライアンスの NTP 設定により、ntp を同期できなくなる可能性がある
CSCvx87691	サービスアカウントまたは MSA として実行されている Windows Enforcement Agent が特定の逸脱シナリオを修正できない
CSCvx87674	Windows 10 バージョン 1909 で適用エージェントが特定の逸脱シナリオを修正できない
CSCvw37366	LDAP ユーザを識別するための API コール
CSCvx74451	3.5 へのアップグレード時にライセンス情報が正しく表示されない場合は、既存の（3.5 より前の）ライセンスを適用する
CSCvx76902	クラスタファームウェアのアップグレードが「SSH Error: data could not be sent to the remote host」で失敗することがある

既知の動作

- External Orchestrator TAXII タイプは、STIX 1.x での TAXII フィードをサポートし、IP およびハッシュインジケータのみを取り込みます。Tetration プラットフォームは、TAXII フィードごとに最大 100,000 個の最新の IP インジケータを取り込み、すべての TAXII フィードに対して最大 500,000 個の最新のハッシュインジケータを取り込みます。
- Cisco FMC の統合では、許可アクション「FASTPATH」を使用して FMC プレフィルタポリシーに Tetration ポリシーを導入します。これにより、プレフィルタポリシーが関連付けられているアクセス コントロール ポリシーによるパケットインスペクションが防止されます。このアプローチにより、Tetration ポリシーで定義されている許可されたトラフィックが、トラフィックをブロックするアクセス コントロール ポリシー ルール、またはそのデフォルトアクションによってブロックされることがなくなります。
- Tetration ポリシーの数、および FMC と割り当てられた FTD のリソース設定によっては、External Orchestrator for FMC を介したポリシーの展開が完了するまでに数分かかることがあります。
- カンバセーション機能は、「Universal Visibility Agents」が存在する範囲ではオンにしないでください。現在、「Universal Visibility Agents」とカンバセーション対応エージェントとの間の相互運用性はサポートされていません。

- 設定をカンバセーションモードから詳細可視性モードに変更すると、tet-main ソフトウェア エージェント プロセスが再起動される場合があります。このプロセスの再起動は、Tetration Agent または適用されたポリシーの機能には影響しません。

互換性に関する情報

3.5.1.17 リリースのソフトウェアエージェントは、マイクロセグメンテーション（詳細な可視性と適用）を実現するために、次のオペレーティングシステム（仮想マシンおよびベアメタルサーバ）をサポートしています。

- Linux：
  - Amazon Linux 2
  - CentOS-6.x: 6.1 ～ 6.10
  - CentOS-7.x：7.0 ～ 7.9
  - CentOS-8.x：8.0 ～ 8.3
  - Red Hat Enterprise Linux-6.x：6.1 ～ 6.10
  - Red Hat Enterprise Linux-7.x：7.0 ～ 7.9
  - Red Hat Enterprise Linux-8.x：8.0 ～ 8.3
  - Oracle Linux Server-6.x：6.1 ～ 6.10
  - Oracle Linux Server-7x：7.0 ～ 7.9
  - Oracle Linux Server-8.x：8.0 ～ 8.3
  - SUSE Linux-11.x: 11.2、11.3、および 11.4
  - SUSE Linux-12.x：12.0、12.1、12.2、12.3、12.4
  - SUSE Linux-15. x: 15.0、15.1
  - Ubuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04
  - Ubuntu-20.04
- Windows Server (64 ビット):
  - Windows Server 2008R2 Datacenter
  - Windows Server 2008R2 Enterprise
  - Windows Server 2008R2 Essentials
  - Windows Server 2008R2 Standard
  - Windows Server 2012 Datacenter
  - Windows Server 2012 Enterprise
  - Windows Server 2012 Essentials
  - Windows Server 2012 Standard
  - Windows Server 2012R2 Datacenter
  - Windows Server 2012R2 Enterprise
  - Windows Server 2012R2 Essentials
  - Windows Server 2012R2 Standard
  - Windows Server 2016 Standard
  - Windows Server 2016 Essentials

  - Windows Server 2016 Datacenter
  - Windows Server 2019 Standard
  - Windows Server 2019 Essentials
  - Windows Server 2019 Datacenter

- Windows VDI デスクトップクライアント:
  - Microsoft Windows 8
  - Microsoft Windows 8 Pro
  - Microsoft Windows 8 Enterprise
  - Microsoft Windows 8.1
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Enterprise
  - Microsoft Windows 10
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 Enterprise 2016 LTSB
- IBM AIX オペレーティングシステム：
  - AIX バージョン 7.1
  - AIX バージョン 7.2

- ポリシーを施行するためのコンテナホスト OS バージョン:
  - Red Hat Enterprise Linux リリース 7.1、7.2、7.3、7.4、7.7
  - CentOS リリース 7.1、7.2、7.3、7.4、7.7
  - Ubuntu-16.04

3.5.1.17 リリースでは、可視性ユースケースについてのみ、次のオペレーティングシステムがサポートされています。

- Windows VDI デスクトップクライアント:
  - Microsoft Windows 7
  - Microsoft Windows 7 Pro
  - Microsoft Windows 7 Enterprise

3.3.2.2 リリースでは、ユニバーサル可視性エージェントの次のオペレーティング システムがサポートされています。

- Windows Server 2008 (32 ビットおよび 64 ビット)
- X86 (64 ビット) 上の Solaris 11
- AIX 5.3（PPC）
- Linux
  - Red Hat Enterprise Linux 4.0（32 ビットおよび 64 ビット）
  - CentOS 4.0（32 ビットおよび 64 ビット）
  - Red Hat Enterprise Linux 5.0（32 ビットおよび 64 ビット）
  - CentOS 5.0（32 ビットおよび 64 ビット）

3.5.1.17 リリースでは、次のオペレーティングシステムについて完全可視性エージェントがサポートされなくなりました。

- Red Hat Enterprise Linux リリース 5.x
- CentOS リリース 5.x

3.5.1.17 リリースでは、NX OS および Cisco Application Centric Infrastructure (ACI) モードで、次の Cisco Nexus 9000 シリーズスイッチがサポートされています。

表 4 NX-OS および ACI モードでサポートされている Cisco Nexus 9000 シリーズ スイッチ

製品ライン	プラットフォーム	最小ソフトウェア リリース
Cisco Nexus 9300 プラットフォーム スイッチ (NX-OS モード)	Cisco Nexus 93180YC-EX、93108TC-EX、および 93180LC-EX	Cisco NX-OS リリース 9.2.1 以降
	Cisco Nexus 93180YC-FX、93108TC-FX、および 9348GC-FXP	Cisco NX-OS リリース 9.2.1 以降
	Cisco Nexus 9336C-FX2	Cisco NX-OS リリース 9.2.1 以降
Cisco Nexus 9300 プラットフォーム スイッチ（Cisco ACI モード）	Cisco Nexus 93180YC-EX、93108TC-EX、および 93180LC-EX	Cisco ACI リリース 3.1(1i) 以降
	Cisco Nexus 93180YC-FX、93108TC-FX	Cisco ACI リリース 3.1(1i) 以降

製品ライン	プラットフォーム	最小ソフトウェア リリース
	Cisco Nexus 9348GC-FXP	Cisco ACI リリース 3.1(1i) 以降
	Cisco Nexus 9336C-FX2	Cisco ACI リリース 3.2 以降
	N9K X9736C-FX ラインカードのみを搭載した Cisco Nexux 9500シリーズスイッチ	Cisco ACI リリース 3.1(1i) 以降

使用上のガイドライン

ここでは、Cisco Tetration の使用上のガイドラインを示します。

- Web ベースのユーザ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40.0.0 以降を使用する必要があります。
- sDNS を設定した後、Cisco Tetration クラスタの URL (https://<cluster.domain) を参照します。
- Tetration 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。
  - 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 にお問い合わせください。

検証済みスケーラビリティの制限値

次の表に、Cisco Tetration (39-RU)、Cisco Tetration (8 RU)、および Cisco Tetration クラウドのスケーラビリティ制限を示します。

表 5 Cisco Tetration (39-RU) のスケーラビリティの制限

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)
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

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 6 Cisco Tetration-M (8 RU) のスケーラビリティの制限

設定可能なオプション	規模
ワークロードの数	最大 5000 (VM またはベアメタル)
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

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 7 Cisco Tetration Virtual (VMWare ESXi) のスケーラビリティの制限

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 Tetration Analytics のマニュアルには、次の web サイトからアクセスできます。

Tetration 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

一般的なドキュメント：https://www.cisco.com/c/en/us/support/security/tetration/series.html#~tab-documents

このマニュアルには、インストール情報とリリースノートが含まれています。

表 8 インストール マニュアル

マニュアル	説明
Cisco Tetration Analytics クラスタ展開ガイド	Cisco Tetration 39-RU) プラットフォームと Cisco Tetration (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 Tetration Virtual 導入ガイド	Tetration 仮想アプライアンスの導入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 Tetration クラスター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/tetration-analytics/sw/install/b_Tetration_Analytics_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]

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2021 Cisco Systems, Inc. All rights reserved.