Cisco Tetration リリース ノート、リリース 3.1.1.65

このマニュアルでは、Cisco Tetration ソフトウェアの機能、不具合、および制限について説明します。

Cisco Tetration は、サーバ、Cisco Nexus®スイッチ、エンドポイントデバイス (ラップトップ、デスクトップ、スマートフォンなど) から収集された豊富なトラフィックテレメトリを使用して、データセンターの運用およびセキュリティの課題の数に対応するように設計されています。プラットフォームは、ホリスティックなワークロード保護プラットフォームを提供するためのアルゴリズムアプローチを使用して高度な分析を実行します。このアルゴリズム的アプローチには、人手を介さない機械学習技術や動作分析が含まれています。プラットフォームには、次の使用事例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。

- ホワイト リスト ポリシーの生成を自動化する動作ベースのアプリケーションの分析情報を提供する
- アプリケーションのセグメンテーションを提供して、ゼロ信頼実績を効率とセキュリティを有効にする
- オンプレミス データセンター、およびプライベート クラウドとパブリック クラウドの環境全体で一貫性のあるポリシー適用を実現する
- プロセスの動作の違い、ソフトウェアの脆弱性、および攻撃対象領域を削減するへの公開を識別する
- アプリケーションの動作の変更やポリシーの遵守違反をほぼリアルタイムに特定する
- 異種環境での包括的なテレメトリ処理をサポートすることにより、実用的な情報を数分で提供する
- スイッチとサーバの両方から収集されたテレメトリデータに基づいた包括的なネットワークのパフォーマンス メトリック
- 詳細なフォレンジック、分析、およびトラブルシューティングのデータを長期間保持する

Cisco Tetration プラットフォーム内でケースの様々な使用事例をサポートするため、プラットフォームではデータセンターインフラストラクチャ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 テレメトリはセンサーと呼ばれるもので収集されます。さまざまなタイプのセンサーがあり、ブラウンフィールドとグリーンフィールドデータセンターインフラストラクチャの両方をサポートするために使用できます。このリリースでは、次のセンサータイプがサポートされています。

- 仮想マシン、ベアメタル、またはコンテナホストにインストールされているソフトウェアセンサー
- Cisco Nexus 9000 cloudscale シリーズスイッチの内蔵ハードウェアセンサー
- 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 センサー
- Cisco Tetration 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 センサー
- 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からテレメトリを収集するための Cisco AnyConnect プロキシ

ソフトウェアセンサーもまた、アプリケーションセグメンテーションのポリシー施行ポイントとしても機能します。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導入全体で一貫性のある適用を実現します。センサー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、でデータパスにセンサーを置く必要がなく、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。

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

表 1 に、このドキュメントのオンライン変更履歴を示します。

表 1 オンライン変更履歴

日付	説明
2019 年 6 月 6 日	リリース 3.1.1.65 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。

新規および変更された機能に関する情報

このセクションには、次のトピックなどの、本リリースでの新規機能および変更された機能をリストしています。

新しいソフトウェア機能

このパッチ リリースには、新しいソフトウェア機能は含まれていません。

動作における変更

このパッチ リリースには、次の動作における変更が含まれています。

- Cisco Tetration クラスタの外部から Kafka にアクセスするポートが、9093 から 443 に変更されました。この変更は、すべての 3.1.1.x リリースに適用されます。この変更により、Datasinks 証明書と Managed Data Tap（MDT）証明書を再度ダウンロードして、kafkaBrokerIps.txt ファイル内のポートの変更を含む最新の tar.gz ファイルを取得する必要があります。

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。

未解決の警告

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。不具合 ID をクリックして、不具合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 開いている注意事項

不具合 ID	説明
CSCvn86706	Lookout 注釈の場合、新しい rootscope が追加されると、UAS サービスが有効でない限り、その rootscope に zeus/bogon タグが追加されない。

解決済みの不具合 (p.11)

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。不具合 ID をクリックして、不具合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 解決済みの不具合

不具合 ID	説明
CSCvn50243	RedHat 5.11 のレガシー詳細可視化センサーが、Tetration にデータを送信できない。
CSCvo77499	作成者が無効になると、ダッシュボードが表示されなくなる。
CSCvo86518	ADM の外部依存関係とポリシー最適化の変更について文書化する必要がある。
CSCvo87526	Netflow センサーがフローの送信を停止する。
CSCvo98967	NameNode がセーフ モードでない場合、SafeModeException が原因で Linux エンフォースメント エージェント インストーラが失敗する。
CSCvp06054	switch_config.yml スクリプトのアップグレード前のチェックでアップグレードと再起動が失敗する。
CSCvp24340	Windows エンフォースメント エージェントの着信ルールで、着信マルチキャストまたはブロードキャスト トラフィックが許可されない。
CSCvp26181	セキュリティ ダッシュボードの脆弱性スコアにデータが表示されない。
CSCvp31371	Citrix NetScaler AppFlow アプライアンスでフロー スティッチングが失敗する。
CSCvp40579	既存ポリシーに「ANY」キーワードが含まれている場合、ADM によってポリシーが再生成される。
CSCvp50694	セキュリティ ダッシュボードとエージェント ワークロード プロファイルに、Windows 2016 エンドポイントの誤った IE バージョンが表示される。
CSCvp71462	フォレンジック イベント データのデフォルト期間を選択できない。
CSCvp77466	Linux カーネルの ip_set コードのバグにより、複数の ipset コマンドの同時実行が原因でシステムがクラッシュする可能性がある。

既知の動作

次のリストには、このリリースでの既知の動作が含まれています。

- 展開とアップグレード
  - Syslog (syslog サーバおよび syslog ポート) の設定フィールドは、アップグレード/展開 GUI で廃止されています。これらのフィールドの変更は、TAN GUI でのみ行うことができます。

- リモート CA の設定フィールド (remote CA、remote CA URL、remote CA username、remote CA password) は、物理および ESX フォームファクタではサポートされていません。
- バグ CSCvn37738 の修正プログラムの副次的影響として、エージェントのアップグレードの途中で MSI のインストールが停止し、エージェントが停止および回復不能状態になることがあります。そのような場合、エージェントを再インストールする必要があります。(logs フォルダにある)「migrate.log」ファイルをチェックして、移行プロセスでエラーが発生しているか確認します。

- TAN
  - ユーザアプリケーションのアラートは、TAN 仮想アプライアンスではサポートされていません。
  - 大きなサイズ（> 64 k）のアラートは、UDP を介して syslog サーバに送信することはできません。
- データタップ/Kafka
  - 8 ラックユニットの展開と ESXi クラスタの設定では、Cisco Tetration は Kafka ブローカのインスタンスを 1 つだけ実行します。このため、インスタンスをホストしているベアメタルまたは VM の使用停止または再コミッションがある場合は、データが失われます。
  - 3.1.x 以前のビルドからアップグレードされたクラスタには、ポートが 443 に変更されている場合でも、アラート MDT（Managed Data Tap）ポートが 9093 として表示されます。ダウンロード可能な証明書には、正しいポート（443）の情報が含まれています。このテキスト情報は、次のリリースで更新されます。
- 施行
  - 施行を有効にしてから無効にすると、エージェントはすべてのルールをフラッシュし、キャッチオールを入力と出力の両方に許可したままにします。
  - エージェントは、最後の既知の正常なポリシーをバックエンドから保存し、サービスの再起動時にポリシーをリロードします。
  - ネットワークポリシーの更新中、Linux のエージェントは、ipset のコンテンツをフラッシュおよび再プログラミングではなく新しいコンテンツとスワップすることにより、ipset リストをよりアトミックな方法で再プログラミングします。これにより、トラフィックがドロップされる可能性が低くなります。
  - ネットワークポリシーの更新中に、Windows のエージェントは、最初に Windows ファイアウォールのインバウンドおよびアウトバウンドのデフォルトポリシーを設定し、現在のルールを削除し、新しいルールをプログラミングし、ネットワークポリシー設定によって指定されたポリシーに従って、インバウンドおよびアウトバウンドのデフォルトをプログラミングします。これにより、拒否キャッチオールポリシーの場合にトラフィックがドロップされる可能性が低くなります。
  - 適用されたワークスペースで適用が停止された場合は常に、適用が停止してから約 15 分間、そのワークスペースのオブジェクトを削除しないでください。これにより、パイプラインがそのワークスペースの状態を更新するのに十分な時間が確保されます。削除されたアプリケーションによって参照されるユーザインベントリフィルタまたは範囲は、アプリケーションの削除後 15 ~ 20 分間は削除されません。

- データリーク
  - データリーク検出には 5 分間の遅延があるため、データリークスコアにはデータリークイベント時間と比べて 5 分の遅延があります。
  - データリークイベントは、現在、フォレンジック分析ページには表示されていません。
- プロセスハッシュの異常
  - 周波数分析 (つまり、出力スコア) は、rootscope レベルでのみ実行されます。
  - 分析は1時間に1回実行されます。
- AnyConnect
  - 複数の AnyConnect プロキシが同じ AnyConnect エンドポイントマシンからデータを取得することは推奨されません。このモードを必要とする使用事例がある場合は、Cisco にご連絡ください。
  - エンドポイントが異なるプロキシ間で反転しない限り、同じエンドポイントが異なる時点で異なるプロキシに接続できます。反転が発生した場合、AnyConnect プロキシは、このような反転が発生したときに少なくとも7日が必要になるようにシナリオを制限します。エンドポイントが2つの異なるプロキシ間で交互に接続されている反転の使用事例がある場合は、Cisco にお問い合わせください。
- Kafka でのポリシー公開
  - この機能を使用するクライアントアプリケーションの場合、この設定には Kafka ブローカーのインスタンスが 1 つしかないため、8 ラックユニットの導入と ESXi クラスタの設定を使用することは推奨されません。アプリケーションをホストしているベアメタルまたは VM の廃止/再コミッションがない場合、作成されたポリシーストリームは正しく回復されず、動作不能になります。代わりに、39ラックユニットのクラスタ設定を使用して、ポリシーストリームの可用性を高めます。
- ADM
  - ADM の実行は、現在のアプリケーションで手動で作成されたポリシーによってすでにカバーされているフローのポリシーを生成しなくなります。
  - クラスタを提供サービスとして使用することはできなくなりました。公開としてマークされ、外部アプリケーションによって参照される既存のクラスタは、インベントリフィルタに変換されます。インベントリフィルタは、範囲またはアプリケーションによって提供されるサービスを示す唯一の方法になります。
  - クラスタがインベントリフィルタに昇格されると、そのクラスタは会話ビューから削除されます。更新された IP アドレスとフィルタのマッピングを生成するには、新しい ADM を実行する必要があります。
  - 除外フィルタは、ADM の実行をまたいで実行されます。クラスタが除外フィルタの一部として使用されている場合、フローはアプリケーションがプライマリの場合にのみ削除されます。
  - Citrix ロード バランサ設定の SLB アップロードでは、ポート範囲として * を使用することはできません。設定では、1 つのポートを設定で指定する必要があります。
- TIM の設定
  - 高可用性モードで F5 が設定されている場合は、次のようになります。
    - TIM F5 プラグインは、設定されたホストのリストから 1 つの F5 のみから設定を取得します。この設定がプライマリおよびスタンバイの REST エンドポイント間で異なる F5 のすべての機能は、TIM が新しいマスターに接続するまで、スイッチオーバー後に遅延が発生する可能性があります。
  - Netscale が HA モードで設定されているときの Citrix 設定。
    - TIM Citrix プラグインは、設定されているホストのリストから 1 つの Netscaler から設定を取得します。この設定がプライマリおよびセカンダリ REST エンドポイント間で異なる Netscaler のすべての機能は、TIM が新しいマスターに接続するまで、スイッチオーバー後に遅延が発生する可能性があります。
  - VMware vCenter HA モードがアクティブな場合は、次のようになります。
    - TIM VMware vCenter プラグインは、一度に 1 つの VMware vCenter エンドポイントからのみ設定を取得します。VMware vCenter HA モードと TIM VMware vCenter プラグインの動作はテストされていません。

互換性に関する情報

このパッチを使用するには、Cisco Tetration のソフトウェア リリース 3.1.1.53、3.1.1.54、3.1.1.55、3.1.1.59、または 3.1.1.61 を実行している必要があります。このパッチ リリースには、以下に記載されているいずれかのリリース バージョンから直接アップグレードできます。

3.1.1.53 リリースの詳細については、次のリリース ノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/sw/release-notes/cta_rn_3_1_1_53.html [英語]

3.1.1.54 リリースの詳細については、次のリリース ノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/sw/release-notes/cta_rn_3_1_1_54.html [英語]

3.1.1.55 リリースの詳細については、次のリリース ノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/sw/release-notes/cta_rn_3_1_1_55.html [英語]

3.1.1.59 リリースの詳細については、次のリリース ノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/sw/release-notes/cta_rn_3_1_1_59.html [英語]

3.1.1.61 リリースの詳細については、次のリリース ノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/sw/release-notes/cta_rn_3_1_1_61.html [英語]

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。
- このリリースでは、Cisco Nexus 9300-EX スイッチのハードウェア センサーからのテレメトリと分析の収集がサポートされています。ただし、収集ルールを定義する必要があります。
- DNS を設定した後、Cisco Tetration クラスタの URL (https://< cluster.domain >) を参照します。

検証済みスケーラビリティの制限値

検証済みスケーラビリティの制限値については、次の URL にある *Cisco Tetration リリース ノート、リリース 3.1.1.53* [英語] を参照してください。

https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/sw/release-notes/cta_rn_3_1_1_53.html [英語]

関連資料

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

Cisco 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

一般的なマニュアル:
http://www.cisco.com/c/en/us/support/data-center-analytics/tetration-analytics/tsd-products-support-series-home.html

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 4 インストールマニュアル

マニュアル	説明
Cisco Tetration クラスター導入ガイド	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： http://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/hw/installation_guide/b_36_server_rack_installation.html [英語]
Cisco Tetration Cloud 導入ガイド	Amazon Web Services での Cisco Tetration Cloud の導入について説明します。 ドキュメント リンク： http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/nexus9000/hw/Tetration/b_tetration_cloud_setup.pdf
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/data-center-analytics/tetration-analytics/sw/upgrade/b_Tetration_Analytics_Upgrade_Guide.html [英語]
最新の脅威データソース	https://updates.tetrationcloud.com/ [英語]