Cisco Tetration リリース ノート
リリース 3.3.2.2

このマニュアルでは、Cisco Tetration ソフトウェア リリース 3.3.2.2 の機能、不具合、および制限について説明します。

Cisco Tetration プラットフォームは、サーバ、レイヤ 4 ～ 7 サービス要素、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、数多くのデータ センターの運用およびセキュリティの課題に包括的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 Analytics 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 Analytics テレメトリはエージェントを使用して収集されます。さまざまなタイプのエージェントがあり、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、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 エージェント
- Cisco Nexus 9000 CloudScale シリーズ スイッチの内蔵ハードウェア エージェント
- 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
- 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
- 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 および Cisco ISE 統合

ソフトウェア エージェントもまた、アプリケーション セグメンテーションのポリシー適用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

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 8 月 26 日	リリース 3.3.2.2 が使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
- 注意事項
- 互換性に関する情報
- 使用上のガイドライン
- 検証済みスケーラビリティの制限値
- 関連資料

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
- 動作における変更

新しいソフトウェア機能

このリリースでは、次の新しいソフトウェア機能を使用できます。

- このリリースでは、Cisco UCS C220 M4 シリーズおよび Cisco UCS C220 M5 シリーズサーバを使用して構築された Tetration ハードウェア クラスタをサポートしています。
  - Cisco UCS C220M4 シリーズ クラスタで Tetration ソフトウェアを実行している場合は、3.1.1. x から 3.3.2.2 に直接アップグレードできます。
  - Cisco UCS C220M5 シリーズ クラスタで Tetration ソフトウェアを実行している場合は、3.2.1 から 3.3.2.2 に直接アップグレードできます。
- 完全な可視性とポリシーの適用サポートは、次のオペレーティング システムのバージョンで拡張されています。
  - Red Hat Enterprise Linux リリース 8
  - CentOS リリース 8
  - Ubuntu 18.04 (フォレンジック/CVE/プロセス スナップショットを除く)
  - SUSE Linux 15 (フォレンジック/CVE/プロセス スナップショットを除く)
  - Windows Server 2019
- AIX の詳細な可視性と適用は、次の点に注意して、ALPHA リリースとして次のプラットフォームで使用できます。
  - OSバージョン: 6.1、7.1、7.2 (PPC)

- エージェント展開のサポートは、インストーラ スクリプトでのみ使用できます (クラシック パッケージ ダウンロードは使用できません)。
- このリリースの AIX エージェントは、フローの PID ルックアップ、フローの TCP 関連の統計情報、プロセス フォレンジック、ソフトウェア パッケージ インベントリ、ソフトウェアの脆弱性、およびパケットの性質をサポートしていません。
- 適用を使用するには、ワークロードに ipfilter パッケージが必要です。

■ Cisco ISE 統合によって、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、プリンタ、HVAC システム、その他の IoT デバイスなど) からテレメトリを収集するためのサポートが追加されました。Cisco ISE には次の利点があります。

- エンドポイント デバイス情報を拡張し、デバイスの状況を変化させることで、この情報に基づいて可視性とより強力なマイクロ セグメンテーション ポリシーを提供します。
- LDAP サーバとの統合により、管理者はユーザー、ユーザー グループなどに基づいてマイクロ セグメンテーション ポリシーを拡張できます (最大 6 つの LDAP 属性)。
- Cisco ISE との統合には pxGrid が使用されます。このインターフェイスの詳細については、次のドキュメントを参照してください。 https://www.cisco.com/c/en/us/products/security/pxgrid.html。

■ フロー ステッチとフローの可視化のための NSEL (ネットワーク セキュア イベント ロギング) および AVI ロード バランサーを使用した Cisco ASA との統合。

■ 新しいエージェントのインストールとエージェントのアップグレードの両方について、このリリースの詳細な可視性および適用ソフトウェア エージェント関連の更新:

- エージェント SLA の管理性を向上させるために、このリリースでは、エージェントの設定を 3 つのカテゴリ (適用、可視性、フォレンジック) に整理することができます。また、ユーザーがこれらの機能それぞれに、メモリ クォータ制限、CPU クォータ制限を定義できるようにするための新しい設定オプションも導入されています。
- すべてのエージェントのバイナリは、UI から独立して管理されます。特定のプロセスが設定されている以上の CPU/メモリを使用していることを検出すると、それ自体が再起動します。
- ソフトウェア エージェントは、アップグレードのステータスを報告するようになります。アップグレードが失敗した場合は、UI にエラーが表示されます。
- エージェントは、オープン パケット キャプチャのステータスを報告するようになりました。キャプチャにインターフェイスが使用されている場合は、ステータスが UI に表示されます。
- このリリースでは、「FollowProcess」と呼ばれる新しいフォレンジック イベントを利用できます。
  - ユーザーは、フォレンジック設定のフォレンジック ルールを定義して、特定のフォレンジック信号 (ExecPath、Command String、Username) に基づいてプロセスに従うことができます。
- 「DBR Ready」 (データのバックアップと復元) の新しいインジケータを使用できます。このためには、DBR を有効にする必要があります。
- エージェントでは、次の追加情報を使用できます。
  - 「インターフェイス フローの抽出」ステータスの新しいインジケータ
  - エージェントはテナントに基づいてフィルタリングできるようになりました:「テナントによってフィルタ処理されたエージェント」機能
  - エージェント ステータスの異常情報がエージェントの概要ページで確認できるようになりました (たとえば、非アクティブ、アップグレード失敗、適用ポリシーが同期していないなど)。
  - アップグレード ステータスは [pending (保留中)] で、[Software Agents (ソフトウェアエージェント)] ページではフィルタが可能です。
- このリリースでは、ソフトウェアの脆弱性に関する新しいダッシュボードが用意されています。これにより、最も注意が必要な重要な脆弱性やワークロードに重点を置くことができます。

- 新しいページには、選択した範囲の脆弱性の分布、さまざまな属性ごとの脆弱性の表示がハイライト表示されます。たとえば、エクスプロイトの複雑さは、ネットワークを介してエクスプロイトされたり、攻撃者がローカルアクセスなどを必要としたりする可能性があります。さらに、リモートで悪用可能で、エクスプロイトが最も複雑である脆弱性を迅速に除外するための統計情報があります。
- この新しいページは、最初にフォーカスするワークロードと、最初にパッチを適用するパッケージを特定するためのものです。

- このリリースには、次のワークロード保護機能が含まれています。
  - セキュリティ ダッシュボードの拡張
    - 攻撃対象スコアは、プロセスおよび
      オープン ポートに関連付けられた CVE の脆弱性を考慮に入れます。
    - オープン ポートは、そのポートが攻撃対象の
      スコアの計算に影響を与えないように、範囲のホワイトリストに含めることができます。
    - CVE とポリシー結果の
      数に関する追加の攻撃対象領域は、意思決定をサポートするために UI に表示されます。
  - ハッシュを使用して悪意のあるプロセスを検出するための機能拡張
    - 既知の悪意のあるハッシュの検出
    - また、偽のアラームを減らすために既知の正当なハッシュをホワイトリストに登録します
    - この機能を有効にするには、Tetration クラウド接続を有効にする必要があります。判定を行うために、実行中のプロセス ハッシュに関する情報のみが送信されます。
  - ネットワーク異常検出アルゴリズムの機能拡張
    - より適切な季節性の検出
    - プロトコルごとの (TCP および UDP) ネットワークの異常検出
  - プロセス フォレンジックの機能拡張
    - デフォルトのフォレンジック「MITRE ATT &、プロファイル」が追加されました。このプロファイルには、実行、永続化、権限のエスカレーション、および防衛回避カテゴリ (https://attack.mitre.org) から多数の MITRE ATT & CK 技術を検出できる、24 のデフォルト ルールが含まれています。ユーザーは、必要に応じて追加の MITRE ATT & のテクノロジーをカバーするための追加のルールを作成できます。
  - フォレンジック ルールは、次の新しい使用例をサポートするように設定できます。
    - プロセス属性に基づく親プロセスの子プロセス作成の検出
    - 誤検出を減らすために選択した子プロセス サブツリーをホワイトリストに登録しながら、親プロセスの子プロセスの作成を検出します
    - 親プロセスが特定の基準を満たしている場合にのみ、親プロセスの子プロセスの作成を検出します
    - 親とその親が特定の基準を満たす場合にのみ、子プロセスの作成を検出します
    - ルール内の特定の正規表現。たとえば、Event Type = Follow Process with ancestor Process Info - Exec Path matches (.*)(winword\.exe|excel\.exe|powerpnt\.exe)
    - 既存のプロファイルを新しいフォレンジック プロファイルにコピーし、コピーしたプロファイルを変更することができます
    - デフォルトのフォレンジック ルール「Tetration -Raw ソケット」が更新され、誤検出の可能性を絞り込むことができるようになりました
  - このリリースでは、適用エンジンはアドレス セットの頻繁な計算を必要とせずに「NOT」フィルタをサポートしているため、エージェントの CPU オーバーヘッドを最適化します

- **例**

CMDB のアップロード:
1.0.0.0/8 location=UNKNOWN,...
1.2.3.4/32 location=US

For inventory-filter = {location != UNKNOWN}
以前のリリースでは、このフィルタのアドレスセットには、フローから学習されたすべての IP アドレスが含まれ、常にメンバー数が増加するため、アドレスセットが頻繁に計算されます。
このリリースでは、パイプラインによって自動的に否定が行われ、メンバーシップが決定されます。
この例では、
address_set=
[
(0.0.0.0 - 0.255.255.255)、
(1.2.3.4)、
(2.0.0.0 - 255.255.255.255)
] フロー学習されたインベントリに依存しません。

同様に、for inventory-filter = {subnet != 10.0.0.0/8} は以下に変換されます。
address_set=
[
(0.0.0.0-9.255.255.255)、
(11.0.0.0-255.255.255.255)
] フロー学習されたインベントリに依存しません。

- このリリースでは、ソフトウェアの脆弱性に関する新しいダッシュボードが用意されています。これにより、最も注意が必要な重要な脆弱性やワークロードに重点を置くことができます。
  - 新しいページには、選択した範囲の脆弱性の分布、さまざまな属性ごとの脆弱性の表示がハイライト表示されます。たとえば、エクスプロイトの複雑さは、ネットワークを介してエクスプロイトされたり、攻撃者がローカルアクセスなどを必要としたりする可能性があります。さらに、リモートで悪用可能で、エクスプロイトが最も複雑である脆弱性を迅速に除外するための統計情報があります。
  - この新しいページは、最初にフォーカスするワークロードと、最初にパッチを適用するパッケージを特定するためのものです。
- F5 ロード バランサーのポリシーの適用
  - F5 外部オーケストレーションおよびロードバランサー エージェントに対して、ルート ドメインのサポートが追加されました。このリリースにアップグレードする場合、既存のすべての F5 外部オーケストレーションはデフォルト ルート ドメイン ゼロが割り当てられます。異なるルート ドメインが F5 で設定されている場合は、それに応じて外部オーケストレーションで手動で変更する必要があります。ロードバランサー エージェントの設定についても同様に実行する必要があります。
  - ルート ドメイン F5 のサポートを使用すると、外部オーケストレーションとロード バランサー エージェントは、指定されたルート ドメインに属する仮想サーバのみを考慮します。
  - このリリースでは、F5 ロード バランサー エージェントは、以前のリリースの F5 グローバル ポリシー リストとは対照的に、仮想サーバごとにポリシー ルールをプログラムします。つまり、ロード バランサー エージェントは、仮想サーバ VIP、プロトコル、およびポートに基づいてポリシーをフィルタリングし、個々の仮想サーバ ポリシーにすべてを含むポリシー ルールを配置します。

- データのバックアップと復元
  - データのバックアップと復元によって、クラスタ データが Tetration クラスタから外部ストレージ デバイスにコピーされます。障害が発生した場合は、この外部ストレージから同じフォーム ファクタを持つ任意のクラスタにデータを復元できます。

- このリリースでは、この機能を使用するためにアクティベーション キーが必要です。この機能に関連付けられている別のライセンスはありません。アクティベーション キーを受け取るには、Cisco サポートにお問い合わせください。
- バックアップは、設定に基づいて、スケジュールされた時刻に 1 日 1 回トリガーされます。バックアップが成功すると、チェックポイントと呼ばれます。チェックポイントは、クラスタのプライマリ データストア (Mongo、D8859 Id、HDFS、Consul、および Vault) のポイントインタイム スナップショットです。
- このリリースでは、この機能を有効にするための設定ユーティリティ、データバックアップ設定ウィザード、およびプランナーを提供しています。
- プランナーを使用して、オブジェクト ストアへのアクセスをテストし、ストレージ要件と、各日に必要なバックアップ期間を決定することができます。
- 設定ユーティリティは、クラスタ内のバックアップを設定してスケジュールするために使用されます。最初の完全バックアップの後に、差分 (新しい変更) の変更のみがバックアップされます。これにより、帯域幅の要件を低く抑えることができます。バックアップ スケジュールとともに完全バックアップ スケジュールを設定し、過去にバックアップされたデータをバックアップすることができます。

■ 外部オーケストレーションの拡張機能は、Infoblox との統合をサポートしています。

- この新機能は、1 分ごとに Infoblox サブネットとホストを自動的にインポートし、生成された注釈を使用してインベントリ フィルタ/クエリを作成できます。注釈キー名は、プレフィックス「オーケストレーション」と、アンダースコア文字で区切られた Infoblox 拡張可能属性名で構成されます。たとえば、「orchestrator_Department」というようになります。
- Infoblox 拡張可能属性の名前と値は、Infoblox によって入力され Infoblox SDK API を使用して取得されたものとしてインポートされます。このリリースでは、単一および複数の値がサポートされています。
- ホスト名と参照は、それぞれ「machine_name」および「machine_id」として Tetration にインポートされます。
- Infoblox サブネットはインポートされていますが、Tetration インベントリではまだサブネットがサポートされていないため、インベントリ フィルタ/クエリでそれらを直接使用することはできないことに注意してください。

■ 外部オーケストレーションの拡張機能により、DNS サーバとの統合がサポートされるようになりました。

- この新機能により、ゾーン転送プロトコルを使用した DNS 名から IP へのマッピングの入力が自動化されます。外部オーケストレーションとして DNS サーバを追加する場合は、IP マッピング情報を入力する DNS ゾーンを指定する必要があります。
- 注釈キー名は、プレフィックス *orchestrator_system/dns_name* で構成されます。

■ セキュリティ コネクタ。

- Tetration セキュア コネクタを使用して、外部のオーケストレーション接続するための新しいワークフローが導入されました。
- 外部オーケストレーション (VMWare vCenter、F5 ビッグ IP など) に接続して Tetration ダイヤルアウトを行う代わりに、新しいコンポーネントである Tetration Connector クライアントを使用できるようになりました。コネクタは Tetration クラスタにダイヤルインし、クライアント ネットワーク内で外部オーケストレーションに到達するために、Tetration によって使用できる暗号化された安全なリバース トンネルを作成します。これは、クライアント ネットワーク外部から直接到達可能になるように、既存の接続モデルで外部の通信が必要になる場合、Tetration サービスを顧客に提供するために特に役立ちます。

■ **コネクタと外部アプライアンス**: 完全に新しいワークフローと展開モデルが導入され、Tetration と外部アプライアンスを管理します。この新しいワークフローでは、アプライアンス エージェントと TAN アプライアンスを展開するための多くの手動が削除されます。これらのアプライアンス エージェントおよびコネクタは、Tetration UI を使用して、(構成管理を含む) を直接有効にして管理します。サポートされているアプライアンス (および固有 OVA) の数は、次の 3 つに統合されます。

- Tetration Ingest Appliance: NetFlow や IPFIX などの標準プロトコルを使用して、大規模なエンドポイントとフローデータの取り込みをサポートします。サポートされるコネクタには次が含まれます：
  - F5 BIG-IP

- Citrix NetScaler
- AVI (新規)
- ASA (新規)
- NetFlow
- AWS
- Meraki (新規)
- AnyConnect

- Tetration Edge Appliance: アラート通知またはインベントリ エンリッチメントなどその他の低ボリューム データの取り込みをサポートします。サポートされるコネクタには次が含まれます：
  - Syslog
  - Email
  - Slack
  - PagerDuty
  - Kinesis
  - ISE (新規)

- **コネクタおよび外部アプライアンスの設定管理**: 仮想アプライアンスとコネクタの設定は、直接作成、更新、および削除することができます。設定は、2 つのモードのいずれかで適用できます。
  - **テストと適用**: 設定の有効性をテストし、設定を適用/コミットします。この設定の例には、NTP、AWS、Syslog、Email、Slack、PagerDuty、Kinesis があります。
  - **検出**: 設定の有効性をテストし、設定の追加プロパティを検出し、これらのプロパティを使用して設定を強化し、設定を適用/コミットします。LDAP は、ディスカバリ モードをサポートする設定の一例です。LDAP の基本設定では、最初に有効性 (サーバへの接続など) がテストされます。基本設定が検証されると、共通の単一値属性のリストが検出され、ユーザーに表示されます。その後、ユーザーはユーザー名に対応する属性と、各インベントリ項目に対して取得/注釈付けする必要がある最大 6 個の属性リストを選択します。その後、最後に完全な設定がコネクタに適用されます。

- データ エクスポータは、集約されたフローとホストインベントリ データを Tetration からエクスポートできるように設計された新しい機能です。
  - フローまたはインベントリのデータ エクスポートを設定するには、Explore コマンドを使用します。
  - データは、管理対象データ タップ (MDT) によってエクスポートされます。
  - エクスポートされたデータは、Tetration の外部で使用できます。
  - Tetration Export アプライアンスは、ELG スタック (Elasticsearch、Logstash、Graf ana) を使用するデータを消費するために展開可能で、さらなる分析と仮想化のために使用できます。
  - エクスポートの制限は、すべてのテナントで 1 分あたり 150万 (フロー + インベントリ レコード) です。
  - データ エクスポートを使用するには、「データ エクスポート」機能フラグに対してライセンスを有効にする必要があります。

- コンプライアンス アラートは、ライブ分析ポリシーで設定できます。
  - アラート トリガー条件と生成されたアラート テキストは、アラートが、そのワークスペースに適用されているポリシーまたはライブ ポリシー用かどうかを示します。

- Geo 情報は、[Visit History (訪問履歴)] タブから 2 つの個別のタブ (Geo インバウンドおよび Geo アウトバウンド) に移動され、表形式のビューに加えてマップ ビューが表示されるようになりました。

- このリリースでは、ADM に次の機能拡張が導入されています。
  - アプリケーション ランディング ページには、アプリケーション ワークスペースだけでなく、すべてのポリシー (分析または適用) の概要も表示されます。このページには、ポリシーの追加や新しいフィルタの作成など、さまざまな機能のボタンもあります。以前と同様に、[Applications (アプリケーション)] メニューをクリックすると、最近表示されたワークスペースと概要ページが切り替わります。
  - 公開されたバージョンは、ワークスペースあたり合計 100 に制限されます。この制限に達すると、UI または API を使用して古いバージョンを削除する必要があります。
  - ポリシーのみを生成し、ADM の実行時にクラスタリングをスキップする新しいオプション (詳細設定)。この機能は、アプリケーション コンポーネントのグループ化を理解し、アプリケーション コンポーネントのグループ間でポリシー エッジを生成するユーザーに役立ちます。この機能は、インベントリの粗収集間のポリシー生成にも役立ちます。
  - ポリシーを生成する場合、ADM は外部依存関係リストのフィルタを使用して、IP アドレスをフィルタ (範囲またはユーザー インベントリ フィルタ) にマッピングします。IP アドレスがどのフィルタとも一致しない場合、以前のリリースでは、外部依存関係リストの最後のフィルタ/範囲に割り当てられます。今リリース以降、そのアドレスはルート範囲にマッピングされます。
  - グループ化されていないポリシー表ビュー: このビューは、コンシューマ/プロバイダ/アクションに加えて、ポート (ポート範囲) で区別されます。そのため、ポートに基づいて行を簡単に検索またはフィルタリングできます。特に、ポリシーの信頼性 (またはサーバ ポートの分類に対する信頼度) を表示できます。

- 隣接グラフの機能拡張
  - 隣接アプリケーションの 2 つの追加タブでは、インバウンドおよびアウトバウンドの Geo 情報が表示されます。
  - Geo タブには、集約情報を含むマップビュー、表形式のビュー、および詳細が含まれます。
  - この Geo 情報にはアラートを設定できます。

  注: この機能は、Tetration でシップされる外部 Geo 情報のデータ セットに依存しています。Geo データ セットを最新の状態に保つには、クラスタと Tetration Cisco クラウドからの最新のデータとの間のオープン脅威のテレメトリ更新を有効にします。

- このリリースには、次のようなパフォーマンス関連の拡張機能があります。
  - Yarn HA はこのリリースで導入されました。
  - Hadoop が 2.4.0 (apache バージョン) から 2.7.3 にアップグレードされました
  - このリリース以降では、すべてのオンプレミス Tetration アプライアンスを登録する必要があります。すべてのオンプレミス アプライアンスでこのリリースに Tetration ソフトウェアを展開またはアップグレードする場合は、90 日間の評価期間に入り、この期間内に Cisco にクラスタを登録する必要があります。そうしない場合、アプライアンスは準拠していないと見なされます。ライセンスを取得してアプライアンスで使用する方法の詳細は、サイト管理ユーザーが利用できます。ライセンスがクラスタに適用されると、アプライアンスはコンプライアンス準拠または使用中のいずれかの状態になる可能性があります。コンプライアンス違反または使用超過が原因で、Tetration 機能がブロックされていないか注意してください。
  - 外部認証のデバッグ ログ メッセージを追加して、接続の問題、サインインの問題などのデバッグをサポートする新しいオプション。このオプション
    がオンの場合、追加のログメッセージが `external_auth_debug` に書き込まれます。
  - LDAP に正常に認証されたが、データベースに存在しない場合、LDAP 外部認証モードで新しいオプションを使用して、[Auto Create Users (ユーザーの自動作成)] を実行します。このオプションがオフになっている場合、サイト管理者はユーザーがサインインを試みる前にユーザーを事前プロビジョニングする必要があります。
  - LDAP での認証を有効または無効にするための新しいオプション。このオプションが有効になっている場合、サイト管理者はグループとロールのマッピングを設定する必要があります。つまり、Tetration ロール マッピングに対する Active Directory グループ名です。これらのマッピングは、LDAP で認証するときにユーザーに適用されます。このオプションを無効にすると、ユーザーはプロビジョニングされたときに割り当てられたロールに基づいてロールが割り当てられます。

- アウトバウンド HTTP 接続を有効または無効にするための新しいオプション。
- HTTP プロキシ部分では、80 以外のプロキシ ポート番号を使用できます。
- インポートを承認する前の x.509 証明書のサニタイズ。
- 証明書署名要求を作成することで証明書とキーをインポートするための新しいワークフロー。
- 最初のベアメタル イメージングで、外部スイッチは不要になりました。ベアメタル CIMC は、スパイン (39RU) または leaf1 (8RU) に接続し、最初のベアメタル イメージングが完了した後に残すことができます。

■ データ プラットフォームの機能拡張

- IO.read/IO.write APIs を使用した JSON blob の読み取りおよび書き込みの追加オプション。
- ExternalApi の改善:
  - ExternalApi api コールに関するエラー メッセージがより明確になります。OpenApi のエラー コードがユーザー アプリケーションに返されます。
  - API コール `ExternalApi.delete()` を追加
- 新しい使用例のノートブック: 次に、時間単位のデータを日単位および週単位のプレゼンテーションに集約し、長期的に平均範囲間のトラフィックを取得する方法、およびセグメンテーション ポリシーの有効性スコアを計算する方法を示します。

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。

■ 適用機能は、次の Windows OS バージョンでは使用できません。

- Windows Server 2008
- Windows 7

■ フォレンジック、ソフトウェア パッケージ、CVE およびプロセス スナップショット (またはファイル ハッシュ) は、次の OS バージョンでは使用できません。

- Ubuntu 18.04
- SUSE 15
- AIX 6.1、7.1、7.2 (PPC)

■ 次の OS バージョンは廃止されており、このリリースでは使用できなくなっています。以前のエージェント バージョンを実行していた場合、アップグレードすることはできません。

- Ubuntu 12.04
- Ubuntu 14.10
- RHEL 5.0 ~ 5.6
- CentOS 5.0 ~ 5.6

■ ホスト フォレンジック バイナリはデータ収集とは独立して動作し、独自のバックエンド接続を管理するため、フォレンジック プロセス「tet-worker」は「tet-main」に置き換えられました。ただし、tet-main は、tet-sensor などの使用可能なすべてのコレクタではなく、一度に 1 個のコレクタのみに接続します。

■ Kubernetes ノードで実行されている場合、Tetration 適用エージェントでは、ポリシーが到達するまでポッドの開始が遅延しません。以前のリリースでは、CNI プラグインが Kubernetes に追加されました。これにより、15 秒間、またはポリシーが到達するまで、どちらか早い方でポッドの初期化が一時停止します。このリリースでは、この動作は廃止されています。このリリースでは、Tetration 適用エージェントはポッドの初期化プロセスを妨げることはありません。ポリシーは、受信するとすぐにポッドに適用されます。

- UI ワークフローを優先して、explore powerdown コマンド/オープン API ベースの動作は廃止されています。
- 予想される CIMC と個々のベアメタル コンポーネントのファームウェア バージョンは、UCS ファームウェア RPM から動的にロードされるため、ファームウェア バージョンの比較がより正確になります。
- ネットワーク パフォーマンス モニタリング機能セットが廃止されました。このリリース以降、パフォーマンス モニタリングとファブリック機能はデフォルトで無効になっています。これらは、後続のリリースで削除される予定です。
  - このリリースより前にこの機能を使用していた場合、または NPMD (network performance monitoring & diagnostic) 機能のために Tetration を購入した場合は、Cisco アカウントチームに連絡して、この機能を限定してロック解除する方法をご確認ください。
- 次のアプライアンス エージェントがコネクタとしてサポートされるようになりました。
  - NetFlow、Citrix NetScaler、F5 BIG IP、AWS VPC フロー ログ、および AnyConnect プロキシ。これらのコネクタは、Tetration 入力アプライアンスでコネクタ ワークフローを使用している場合にのみ有効にできます。有効にすると、これらのコネクタはエージェントとして登録されます (以前のリリースと同様)。
- 3.1 のアプライアンス エージェント (NetFlow、Citrix NetScaler、AWS VPC フロー ログ、F5 BIG IP、および AnyConnect プロキシ)は、3.3 ではコネクタとしてのみサポートされています。れらのエージェントは、3.1 から 3.3 への自動アップグレードを実行しません。管理者は、新しいコネクタのワークフローを使用してこれらのエージェントを再展開して、Tetration 統合を管理する必要があります。
  - Cisco Tetration NetFlow 仮想アプライアンス: このリリースでは、このアプライアンスに相当するのは、Tetration 入力アプライアンスに NetFlow コネクタを展開することです。
  - Citrix NetScaler AppFlow アプライアンス: このリリースでは、このアプライアンスに相当するのは、Tetration 入力アプライアンスに Citrix NetScaler コネクタを展開することです。
  - AWS VPC フロー ログ コレクタ アプライアンス: このリリースでは、このアプライアンスに相当するのは、Tetration 入力アプライアンスに AWS VPC フロー ログ コネクタを展開することです。
  - F5 BIG-IP IPFIX コレクタ アプライアンス: このリリースでは、このアプライアンスに相当するのは、Tetration 入力アプライアンスに F5 BIG-IP フロー ログ コネクタを展開することです。
  - Cisco Tetration AnyConnect プロキシ アプライアンス: このリリースでは、このアプライアンスに相当するのは、Tetration 入力アプライアンスに AnyConnect コネクタを展開することです。
- Cisco Tetration Notifier (TAN): アプライアンス エージェントと同様、アラート通知は 3.3 でのみコネクタとしてサポートされています。TAN アプライアンス (これらの通知がインスタンス化されている場合) は、3.1 から 3.3 への自動アップグレードは行われません。管理者は、新しいコネクタのワークフローを使用してこれらの通知を再展開する必要があります。このリリースでは、TAN アプライアンスに相当するのは、Syslog、電子メール、Slack、PagerDuty、および/または Kinesis コネクタを Tetration Edge アプライアンスに展開することです。これは、Tetration Edge アプライアンスが展開された後に、コネクタ ページからのみアラート通知の設定を行うことができることを意味します。
- Spark は 1.6 から 2.3 にアップグレードされます。
  - これには、既存のユーザー アプリケーションに何らかの変更が必要になる場合があります。
  - 既知の潜在的な変更 (SparkSession からの sqlContext の取得など) は、ユーザー ガイドでハイライト表示されています。
- データ レイク マシンとインベントリ データが削除されます (廃止された最後のリリース)。
- データ レイク Shallowflows は廃止されました。このデータには、大幅に削減されたストレージ ウィンドウがあります。
- ルックアウト注釈によってプッシュされた TA_bogon_ipv4 と TA_zeus タグは、ユーザーの注釈にプッシュされず、個別の注釈スペースにプッシュされるため、ユーザーの注釈を変更する際にユーザーが誤って削除することはありません。切り替えは、次のデータパックの更新後に発生します。

- Tetration では、ワークロードのキーが重複しているタグが廃棄されます。このようなタグでワークロードが構成されている場合、タグの 1 つがランダムに承認され、残りは廃棄されます。
- UTF-8 以外の文字はタグでは受け入れられません。このような文字が存在する場合、無効な文字を廃棄することによってタグのキー/値が除去されます。次に例を示します。

  `abc\xc6de\xc8s`は新しいキー/値として`abcdes` を生成します。
  キー/値に有効な文字がないため、\xc6 は破棄されます

  また、タグのキー/値の最大長は、512 文字よりも短くする必要があります。
- ノードで障害が発生した場合、Yarn の手動スイッチオーバーは必要ありません。
- ユーザー定義のポリシーが、承認済みポリシーに移行されました。ポリシーは、ADM の実行によって作成された場合を除き、ユーザー定義としてマークされています。UI または JSON インポートによって作成されたポリシーは、ユーザー定義としてマークされています。許可されたポリシー間でポリシーを切り替えることができます。
- このリリース以降、ポリシー backdated 実験はフロー データではなく会話で実行されます。これは、backdated の実験を高速化するために行われました。
- 静的モードのアプリケーション ワークスペースは廃止されています。すべての新しいワークスペースが動的モードになります。動的モードのワークスペースの主な差別化は、動的クエリを処理するクラスタの機能であり、IP アドレスの静的セットに限定されるものではありません。すべてのワークスペースは、次のリリースで動的モードにアップグレードされます。
- FlowSearch API (POST/openapi/v1/flowsearch) の場合、このリリースよりも前のオプション パラメータは、`scopeName`でした。このリリース以降、 `scopeName` は FLOWSEARCH API に渡されるパラメータの必須パラメータです。
- 範囲選択入力ボックスには、クリック可能であることを示すための拡張機能があり、クリックすると、ボックスに「範囲選択」と表示されます。また、提案リストに表示された最近使用した範囲を使って、自動補完範囲のリストも表示されます。
- ユーザー管理 UI には、ユーザーを作成および編集するためのウィザード ワークフローが含まれるようになりました。これは、以前のリリースで導入されたロール管理のウィザード ワークフローと一致します。
- サイト管理者は、診断用のスナップショットを作成できます。
- アプライアンスがローカル データベース認証モードの場合、新しいユーザーを作成すると、パスワードをリセットするための電子メールが生成されます。
- エージェントは、3 つのグループ (ワークロード、エンドポイント、およびフロー入力) に再編成されています。他のすべてのアプライアンス エージェントは、Tetration コネクタ ページに移動します。

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)
- Known Behaviors

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。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
CSCvq72540	ブロードキャスト アドレスが ADM の誤った範囲に表示される場合がある
CSCvq20740	ADM AppView によるコンシューマおよびプロバイダ ラベルの反転
CSCvq48913	障害が発生したときに PowerShell スクリプトで詳細情報が必要になる
CSCvq91327	追加の不明なノードがクラスタ ステータスに表示される場合がある
CSCvq82858	サイト linter とサイト チェッカーが無効な site_ssh_key としてパスされる
CSCvq26107	UDP ベースの Linux Traceroute を適用するためのルール セットの中断
CSCvo26666	ノード再稼働後、CIMC コマンドを処理するためのキー ファイルがベアメタル ノードから欠落している
CSCvp10656	CIMC 内部ネットワークは、クラスタ展開、アップグレード、または再起動 (編集) 後にテストされない
CSCvp10580	アップグレードまたは再起動の外部で CIMC 内部ネットワークを変更できない
CSCvq96155	ロード バランサー (AVI、F5、Citrix) 適用エージェントに必要な手動アップグレード
CSCvo42565	パスワードを二重引用符で囲まずに、Anyconnect プロキシ VM で # in ldap パスワードを使用することができない
CSCvo19895	/local/tetration/log/tet-ldap-loader ログには、anyconnect VM のタイムスタンプが必要になる
CSCvo17238	可能性のある iRule エラーをより適切に処理し、ロギングを追加するために、iRules を更新する
CSCvq85892	ソフトウェア エージェントのアップグレード ページで netflow/span/f5/netscaler/aws/anyconnect の手動アップグレードを許可する
CSCvr03130	3.3.2.2 でのアップグレード/再起動によって CIMC 内部ネットワーク ゲートウェイを変更できない

解決済みの警告

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
CSCvn78222	オフライン状態で手動で rpm をインストールした後に、ルックアウト注釈のバッチを更新可能
CSCvo89242	デフォルト、不明、および Tetration vrf 名を削除することができない

CSCvp33648	Tetration V の再起動がエラー pyVmomi.VmomiSupport. InvalidPowerState で失敗する
CSCvf78109	Collectd ver にアップグレードします。5.72/ 新しいバージョンでは、拡張機能とより優れたメモリ管理が提供されています。
CSCvm85308	Qualys スキャン結果の検証: HTTP セキュリティ ヘッダーが検出されない
CSCvn86706	ルックアウト注釈: UAS サービスが有効になっていない限り、新しい rootscope zeus タグが追加されない
CSCvo59068	ポート 8080 でのアウトバウンド HTTP 接続が失敗する
CSCvo78365	Linux インストーラ スクリプトのチェックが不足している
CSCvp18606	AttributeError が原因でエラー シャットダウン検証手順が失敗し、UI からのサーバの電源オフが失敗する
CSCvq17715	内部の haproxy 証明書の有効期限が切れている
CSCvq29036	注釈列に / が含まれている場合、フロー検索が「不明」と表示される
CSCvq52863	メジャー アップグレード後 1 年間の有効期限がなくなったヴォールト トークン
CSCvq54100	展開ガイドの M5 8RU の配線イメージが正しくない
CSCvm68801	外部ポート上の LACP が設定されていないため、クラスタへのトラフィックの vPC が失敗します。
CSCvp89096	ケーブルチェックは G2 クラスタで CABLECHECK_UNBOUND_10G_INTF を発生させます
CSCvq77108	非互換モードでの npcap のインストール
CSCvq78946	[3.1.1.67] Anyconnect フローに不正な LDAP ユーザーの注釈が表示される
CSCvq21346	npcap 0.995 が不安定-Tetration の詳細可視性または適用エージェントで使用しない
CSCvp98092	プラットフォームでの電子メールの有効化後に、Tetration プラットフォームでアラートが機能しない
CSCvn50243	redhat 5.11 のレガシー詳細可視化センサーで、Tetration にデータを送信できない
CSCvo87526	Netflow センサーは、30 ~ 60 分後にフローの送信を停止します。
CSCvo98967	NameNode がセーフ モードでない場合、SafeModeException により Linux 適用エージェント インストーラが失敗します。
CSCvp06054	switch_config.yml 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 適用エージェントのインバウンド ルールで、インバウンド 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ません。
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
CSCvp71462	フォレンジック イベント データのデフォルトの時間枠を選択できない
CSCvn90943	時間単位のファブリック アラートの概要が報告されない
CSCvn52935	ソフトウェア センサーが、そのフレンドリ名が英語以外の場合、1 つのインターフェイスでのみパケットをキャプチャする

CSCvn78767	iso から tet-alert-notifier.tar.gz が欠落しているため、Notifier docker コンテナが失敗する
CSCvo02165	エージェント プロファイルのエージェント インテントを変更して自動アップグレードを有効にすると、エージェントがアップグレードされません。
CSCvn49926	コマンド get_cimc_techsupport がテクニカル サポート ファイルを生成できません。
CSCvn49906	2.3.1.52 から 3.1.1.53 へのアップグレード後に GUI から外部オーケストレーションが失われた
CSCvn50142	idle/defunc プロセスが原因で、AIX ユニバーサル センサーのインストール セルフテストが失敗する
CSCvn20704	ポリシー分析を有効にできない
CSCvn28898	MsiInstaller が詳細な可視性エージェントのために windows Agentengine の適用サービスを誤ってインストールする
CSCvn30664	dmidecode からの UUID ケースの変更により、Tetration でセンサーが重複する
CSCvn34366	期間 (".") が CMDB 属性名で受け入れられない
CSCvn37738	Windows ソフトウェアセンサーの msi インストーラを作成して、センサー (自動) アップグレードでシステムを強制的に再起動しないようにします。
CSCvn64220	3.1.1.54 へのアップグレード後に、センサーがエージェントの統計情報を報告しない
CSCvh97957	Cisco Tetration Analytics クロス サイト要求偽造の脆弱性
CSCvm84884	CVE-2014-8730 (Poodle 攻撃-TLS) の影響を受ける可能性があるインターフェイス
CSCvk51665	デフォルトの api ポート (6443) を使用して k8s 外部オーケストレーションを追加しても、k8s からメタデータがインポートされない
CSCvm88166	/app-log のデータの保持の定義/調整
CSCvn12781	Druid サービスが失敗し、UI で「内部サーバ エラー」が返される
CSCvn18783	誤ったデフォルト ゲートウェイを使用して CIMC にアクセスできない
CSCvn20511	サービスが正常でありパイプラインが実行されている間に、フロー検索のフローが更新されない
CSCvi19170	[service status (サービス ステータス)] ページによって報告された ECC メモリ エラーの数が Show Tech と一致しない
CSCvi20538	Bosun アラート: 修正可能な ECC エラーは、ノードのエラー合計ではない個別の DIMM に対して行う必要があります。
CSCvj86257	[Service Status (サービス ステータス)] ページで修正可能な ECC エラーの報告を停止します。
CSCvk34853	再イメージ化中にオーケストレーションに書き込まれたテキストの管理者パスワードを消去します。
CSCvm35195	SLB 設定ファイルの解析後に CitrixParser がクラッシュする可能性があります
CSCvm57680	keepalived は、パブリック ネットワークのインターフェイスがダウンしている場合、appServer の VIP をフェールオーバーしません。
CSCvm63714	Tetr-V//グレースフル クラスタの電源がオフになる
CSCvm85033	Qualys スキャン-フォーム ベース認証のパスワードに対して、AutoComplete 属性が無効になっていません

CSCvn46417	HDFS-6870 の影響を受ける Tetration
CSCvm90092	Tet-sensor によって、RHEL 6 で「/etc/audit/audit.rules」が上書きされる場合がある
CSCvi71219	MSServer2016Standard ソフトウェア エージェントを手動でアップグレードすることができない
CSCvj23172	コマンド get_cimc_techsupport、clear_ecc、clear_sel が Tetration 2.3.1.41 で機能しない
CSCvj46846	テクニカル サポートが Tetration 2.3.1.41 クラスタのスナップショット ファイルに収集/組み込まれない
CSCvk38762	tet-sensor プロセスによって RPM データベースがロックされるため、SUSE エンドポイントで Teteration エージェントの更新が失敗する場合がある
CSCvm49542	システム ログ ファイルが大きいため、エージェント tet-worker プロセスの CPU 使用率が高くなる
CSCvf80588	Cisco Tetration Analytics 認証バイパスの脆弱性
CSCvf80617	Cisco Tetration Analytics リモート コマンド実行の脆弱性
CSCvf80602	Cisco Tetration Analytics 反射型 XSS の脆弱性
CSCvf71955	Cisco Tetration Analytics ハードコードされた SSH 認証キーの脆弱性
CSCvh21899	Cisco Tetration Analytics 証明書検証の脆弱性
CSCvh21844	Cisco Tetration Analytics ACL バイパスの脆弱性
CSCvj45311	フラッシュを要求し、要求の受信を停止する HbaseRegion server periodicFlusher
CSCvc64131	サービスおよびクラスタのステータス ページには、すべてのサービスが表示されるわけではありません。
CSCvc65452	Windows PATH 変数が変更されました
CSCve15116	HDFS および Yarn の Hadoop サービスのスイッチオーバーにはエンジニアリング関連が必要になる
CSCvf22308	一部のクラスタが restartservices を実行できない
CSCvf22828	別の VRF/範囲を使用するように再設定されているときの、デフォルトの範囲に対するハードウェア Swith エージェントのレポート
CSCvf93113	Windows ポリシーによるセンサーのインストールの制限
CSCvg69762	すべての IPv6 トラフィックが収集ルールで除外されている場合、IPV6 アドレスがインベントリに表示される
CSCvg69774	収集ルールのサブネットを使用すると、ip アドレスはフローに表示されるが、インベントリには表示されない
CSCvg72893	アプリケーション ポリシー ビューの動作の変更が TA ユーザー ガイドに記載されていない
CSCvh06306	適用ポリシーがどのワークスペースのエンドポイントにもプッシュされていない
CSCvh08287	適用順序の不一致により適用されない適用ポリシー
CSCvh47800	外部依存関係の粒度が細かい adm を実行しても、ポリシー要求が作成されない
CSCvh48928	Spectre/Meltdown の脆弱性のための、Tetration クラスタ上のパッチ CentOS VM

CSCvh48941	CollectorDatamover VM 上の複数のアプリケーションに使用される Python 2.6.6 には、セキュリティの脆弱性があります。
CSCvh87245	クラスタのアップグレード後、一部のハードウェア センサーが自動的に新しいバージョンにアップグレードされない
CSCvh88191	Tetration が VCenter への複数の TCP 接続を開くと、他の接続をドロップする
CSCvi19883	EX スイッチ ハードウェア エージェントが UDP および TCP トラフィックを反転させることによって、ADM に誤った情報が表示される
CSCvi20041	サービス ステータスおよび Bosun アラートの修正可能な ECC エラー通知では、しきい値が異なります。
CSCvi59083	外部オーケストレーションの設定に正しいプラグイン名が必要になる
CSCvc69960	Linux Tetration Agent が「which」がない状態でインストールに失敗する
CSCvd80405	Google Analytics に GET 要求を行う Tetration クラスタ。
CSCve52628	フロー検索でエラー 504 が返されました。Druid クエリ タイムアウト。
CSCve53091	tetpyclient モジュールとの互換性がない
CSCve53686	TSDB 自体が 2.0 でレポートされない
CSCvg74804	リリース ノートですべての動作の変更を文書化する必要がある
CSCvh89813	ベア メタルの無応答の bmmgr サービスが原因で、単一ノードの再イメージ化が失敗します。
CSCvh89652	Cisco web サイトにある Tetration アップグレード ガイドに、完全なアップグレード パスはありません。
CSCvi21617	読み取り専用ユーザーには、機能を超えて API キーを作成する権限がない
CSCvi23470	SW Windows センサー Universal Visibility 2.2.1.34-lw のみが ARP_REQUEST および UDP データを送信する
CSCvi60993	センサーのインストールは、PAM と「su」を使用するための tet センサーの機能に依存しないようにする必要があります。
CSCvi61862	SLES11 zypper インストールでリポジトリから適切な RPM を選択しない
CSCvi63860	OS が systemd を使用していない場合、Ubuntu で Tet エージェントをインストールすることができない
CSCvd86311	diskIsOff Alert Misreporting
CSCve62618	エラー-{df_instance = run-1000} (sys. diskUsage の場合): エラー コール Eval: 結果が返されませんでした
CSCve95757	Tetration 2.0 誤ドロップ基準が変更された
CSCve98414	データ プラットフォームでコンプライアンス アプリケーションをアクティブ化するときにデータ タップが選択できない
CSCvf67422	証明書が期限切れになると、コレクタはエージェントへのアクセスを拒否するため、フローが停止します。
CSCvf68866	Grafana ではシャロー フローが欠落しおり、ADM フローが期限切れになっている
CSCvg44736	送信元/ターゲット クラスタ番号が、クリックするまで空であることを示している

CSCvg44965	hbase リージョンの一部の「行ロック」がリリースされていないため、UI で不整合が発生している
CSCvn70337	TAN で TAN アプライアンス VM からログをエクスポートする方法が必要になる
CSCvn04971	ASA NSEL netflow フローが Neftlow アプライアンスによってデコードされない
CSCvk62307	iRule でサポートされている f5 の最低限バージョンの確認
CSCvj89293	f5 や Citrix などの仮想アプライアンスからログを収集するオプション
CSCvp89285	Tetration Netflow 仮想アプライアンスでは、IPFIX プロトコルにポート4739を使用する必要があります

既知の動作

- 適用エンジンでは、外部 Kubernetes サービスのバックエンド ポリシーは適用されません
  - 外部 Kubernetes サービスは、エンドポイントが手動で定義されるものです。セレクタを使用してサービスに自動的に関連付けられることはありません。外部サービスの例としては、Kubernetes システムによって作成され、api-server ポッドに接続するデフォルトの「kubernetes」サービスがあります。このサービスのエンドポイントは、初期化時に Kubernetes によって手動で作成されます。このようなサービスが Tetration ポリシーでプロバイダとして使用されている場合、Tetration はバックエンド エンドポイントにルールを書き込みません。
  - CoreDNS ポッドが Kubernetes サービスの ClusterIP にアクセスを許可するように、Tetration ではポリシーのみ書き込みます。Kubernetes サービスを提供するノードまたはポッドでは、ルールは自動的には作成されません。このようなルールは手動で定義する必要があります。
- コンテナの適用は、IPVS モードで実行されている Kubernetes を持つ kubeproxy クラスタをサポートしていません。
  - Kubernetes 1.11 以降では、kubeproxy は IPTABLES ではなく IPVS を使用したサービスの処理をサポートしています。この設定は現在、Tetration ではサポートされておらず、適用を行いません。
- F5 入力コントローラのポリシーの適用
  - Tetration ソフトウェアは、現在のリリースでは F5 入力コントローラのみをサポートしています。
  - ホワイトリスト ポリシー モデル [CATCH ALL rule is DROP] では、F5 入力コントローラ ポッドと Kubernetes API サーバ間のトラフィックを許可するためのポリシーを作成し、F5 入力コントローラ ポッドと F5 ロード バランサー間のトラフィックを許可する別のルールを作成する必要があります。
  - Tetration ソフトウェアは、F5 入力コントローラのポート 80 およびポート 443 のみをサポートします。
- ポリシーを適用するためのロード バランサー エージェント
  - ここで説明する新しい展開メカニズムの変更により、このリリースへの自動アップグレードはサポートされていません。これは、このアプライアンス エージェントを再インストールする必要があることを意味します。
    - サポートされているすべての F5、Avi、および Citrix ロード バランサーに対して 1 つの OVA イメージのみが存在します。エージェントは、作成された VM に直接インストールされて実行され、Tetration クラスタと接続されたロードバランサー アプライアンスへのアクセス権を持つ 1 個の IP アドレスのみが必要です。これは、以前のリリースでは docker コンテナが設定されていないことを意味します。
    - このリリースで提供される OVA は、コンソールを使用したルート ログインを禁止します。作成した VM を起動した直後にコンソールを使用して、組み込みユーザー「tetuser」の新しいパスワードを設定することをお勧めします。新しいパスワードを設定しないと、VM コンソールに入ることができなくなります。
    - VM の初回起動時に設定 iso で「authorized_keys」ファイルが指定されている場合、起動スクリプトは、ルート ログインなしの SSH サービスと公開キー認証のみを有効にします。見つかった「authorized_keys」ファイル

は、内蔵「tetuser」に対して設定されます。これにより、指定された
公開キーを使用して VM にログインできるようになります。

- OVA の展開に加えて、エージェントの RPM (`tet-lbenforcer-f5/avi/citrix-3.3.1-el7_x86_64.rp`) を Tetration UI ページの「ソフトウェア エージェント ダウンロード」からダウンロードして、任意の Linux CentOs-7 互換プラットフォームにインストールすることもできます (docker コンテナ、VM、ベア メタル マシン に関わらず)。
- ホワイトリスト モードでロード バランサーとバックエンド サーバ間のヘルス ステータス チェックを可能にするには、ポリシーを作成する必要があります。

- プロセス ハッシュの異常の特定
  - 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。
  - ワークロード プロファイル ページの [File Hashes (ファイル ハッシュ)] タブには、過去 1 時間に分析されたプロセス ハッシュの詳細のみが表示されます。
- ネットワーク異常の検出
  - 以前検出された「データ リーク」イベントは、引き続き「データ リーク」イベントとして表示されます。
- 先祖系統に基づくフォレンジック イベントのプロセスは、最大 4 レベルです。
- Tetration クラスタは、ネットワーク帯域幅をオブジェクト ストアにスロットルしません。
- パフォーマンスおよびファブリック モニタリング ページがランディング ページとして設定されている場合

  ランディング ページの設定を [performance/fabric] ページにすでに設定している場合、このリリースにアップグレードすると、[performance/fabric] ページに自動的に移動することができますが、認証エラー メッセージが表示されます。これは、このリリース以降、これらのページがデフォルトで無効になっているため予期される動作です。デフォルトのランディング ページを別のページに変更するには、[Preferences (設定)] → [Select (選択)] (ランディング ページ) を使用します。
- 切り替えが発生したとき、このリリースへのアップグレード後、またはその直後に、ルックアウト注釈タグの送信元が無効になることがあります（一部のケース）。TA_ * タグが移動した後に、ソースに対してルックアウト注釈が有効になっていることを確認し、それらが無効になっている場合は、手動で再度有効にします。
- NetFlow コネクタでは、カスタム エンタープライズ情報要素を含む NetFlow v9 または IPFIX レコードが、Tetration にエクスポートされないことがあります。
- 新しいコネクタのワークフローを使用して仮想アプライアンスを導入するとき、オプション フィールドでは、ユーザーがフィールドを入力する場合、アプライアンスの VM セットアップ中に警告が表示されないように、ユーザーがフィールドを明示的に消去する必要があります。回避策は、[Cancel (キャンセル)] ボタンをクリックし、最初から再起動することです。
- Tetration 入力アプライアンス上のコネクタと、Tetration Edge アプライアンス上の ISE コネクタの場合、アップグレードはエージェント アップグレード ワークフローによって管理されます。[True] とマークされた自動アップグレードのエージェント設定の目的は、これらすべてのコネクタに適用する必要があります。これが設定されている場合を除き、これらのコネクタは、Tetration がアップグレードされるとアップグレードされません。他のコネクタ (esp、アラート通知コネクタ) の場合、アップグレードは自動的に行われます。
- 新しいコネクタのワークフローを使用して仮想アプライアンスを導入するとき、オプション フィールドでは、ユーザーがフィールドを入力する場合、アプライアンスの VM セットアップ中に警告が表示されないように、ユーザーがフィールドを明示的に消去する必要があります。回避策は、[Cancel (キャンセル)] ボタンをクリックし、最初から再起動することです。

- アップグレード中に新しい RPM がアップロードされると、adhocKafka がグレースフル シャットダウンされます。これは、Kafka インデックスの破損を回避するために行われます。アップグレード後に kafka が起動します。RPM のアップロード後にアップグレードが中断された場合、adhocKafka は、explore コマンドを使用して再起動する必要があります。

互換性に関する情報

3.3.2.2 リリースのソフトウェア エージェントは、詳細な可視性を実現するために、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 の場合
  - CentOS-5. x: 5.7 ~ 5.11
  - CentOS-6.x: 6.1 ～ 6.10
  - CentOS-7.x: 7.0、7.1、7.2、7.3、7.4、7.5
  - Redhat Enterprise Linux-5.x: 5.1 ～ 5.11
  - Redhat Enterprise Linux-6.x: 6.1 ～ 6.10
  - Redhat Enterprise Linux-7.x: 7.0、7.1、7.2、7.3、7.4、7.5
  - RedHat Enterprise Linux-8.0
  - Oracle Linux サーバ-6.x: 6.0 ~ 6.10
  - Oracle Linux Server-7x:7.0、7.1、7.2、7.3、7.4、7.5
  - 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
  - Unbuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04
- Windows Server (64 ビット):
  - Windows Server 2008 Datacenter
  - Windows Server 2008 Enterprise
  - Windows Server 2008 Essentials
  - Windows Server 2008 Standard
  - 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 7
- Microsoft Windows 7 Pro
- Microsoft Windows 7 Home
- Microsoft Windows 7 Enterprise
- Microsoft Windows 8
- Microsoft Windows 8 Pro
- Microsoft Windows 8 Home
- Microsoft Windows 8 Enterprise
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Pro
- Microsoft Windows 8.1 Home
- Microsoft Windows 8.1 Enterprise
- Microsoft Windows 10
- Microsoft Windows 10 Pro
- Microsoft Windows 10 Home
- Microsoft Windows 10 Enterprise

■ 完全な可視性を確保するためのコンテナ ホスト OS のバージョン:

- Red Hat Enterprise Linux リリース 7.1、7.2、7.3、7.4
- CentOS リリース 7.1、7.2、7.3、7.4
- Ubuntu リリース 16.04

3.3.2.2 リリースでは、ポリシー施行アドオン機能に対して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。

■ Linux の場合

- CentOS-6.x: 6.1 ～ 6.10
- CentOS-7.x: 7.0、7.1、7.2、7.3、7.4、7.5
- Redhat Enterprise Linux-6.x: 6.1 ～ 6.10
- Redhat Enterprise Linux-7.x: 7.0、7.1、7.2、7.3、7.4、7.5
- RedHat Enterprise Linux-8.0
- 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
- Oracle Linux サーバ-6.x: 6.0 ~ 6.10
- Oracle Linux Server-7x:7.0、7.1、7.2、7.3、7.4、7.5
- Ubuntu-14.10

- Ubuntu-16.04
- Ubuntu-18.04

■ Windows Server (64 ビット):

- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Essentials
- Windows Server 2008 Standard
- 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 7
- Microsoft Windows 7 Pro
- Microsoft Windows 7 Home
- Microsoft Windows 7 Enterprise
- Microsoft Windows 8
- Microsoft Windows 8 Pro
- Microsoft Windows 8 Home
- Microsoft Windows 8 Enterprise
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Pro
- Microsoft Windows 8.1 Home
- Microsoft Windows 8.1 Enterprise
- Microsoft Windows 10
- Microsoft Windows 10 Pro
- Microsoft Windows 10 Home
- Microsoft Windows 10 Enterprise

- 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
  - CentOS リリース 7.1、7.2、7.3、7.4
  - Ubuntu リリース 16.04

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。

- 32 ビットおよび 64 ビット (CentOS 4.x、RHEL 4.x、CentOS 5.x、RHEL 5.x など)
- 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）

3.3.2.2 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	ソフトウェア リリースの最小要件
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
	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

* * ハードウェア エージェントを使用するネットワーク パフォーマンス機能は、リリース 3.1 以降を搭載した Cisco ACI モードでのみサポートされます。

使用上のガイドライン

ここでは、Cisco Tetration Analytics 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。

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 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	M4 ベース Cisco Tetration (39-RU) プラットフォームと Cisco Tetration-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：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] M5 ベース Cisco Tetration (39-RU) プラットフォームと Cisco Tetration-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。 https://www.cisco.com/c/en/us/td/docs/data-center-analytics/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html
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]