Cisco Tetration リリース ノート、リリース 3.2.1.20

注: これは、導入のみのリリースです。3.1.1. x リリースを実行している場合は、このリリースにアップグレードしないでください。

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

目次

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 24 日	リリース 3.2.1.20 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。

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

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。

- Cisco UCS C220 M5 ベースのサーバと Cisco Nexus 93180YC FX または 93108TC-FX ベースのスイッチに基づいた新しい Tetration 8 RU および 39 RU クラスタでの Cisco Tetration ソフトウェアの導入をサポートします。

動作における変更

このリリースには、動作の変更は含まれていません。

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

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 には、UAS/Bogon タグは追加されません。

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
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
CSCvm68801	vPC は、8 RU デプロイのパブリックネットワークには設定されません。
CSCvm96270	Python logical volume manager でメモリリークが発生すると、長期間にわたって bmmgr のメモリ不足の問題が発生します。
CSCvn90943	日次サマリーアラートも設定されていない限り、時間単位のサマリーアラートは送信されませんでした。
CSCvn92157	TAN ではデフォルトで HTTPS プロキシが使用されていましたが、SMTP サーバがプロキシの背後にない場合に問題が発生しました。HTTPS プロキシを無視し、可能であれば SMTP に接続する修正を実装しました。
CSCvn97582	データプラットフォームのチャートでは、ユーザが作成したグラフに関連付けられているフィルタは保存されませんでした。
CSCvo08397	Windows センサーのバイナリとリリースバージョンを照合します。
CSCvo10076	Windows センサーで TSO が検出された場合は、エージェントログをフラッディングしないようにしてください。
CSCvo10103	センサーログの詳細を減らします。
CSCvo14338	[Agent upgrade] ページ: すべての結果をダウンロードすると、フィルタリングされたセンサーもダウンロードされます。
CSCvo18079	施行が有効になるまで、NFLOGを開くのを遅延します。
CSCvo19986	[アプリケーション (Applications)] では、ADM の実行について考慮されている時間間隔内のインベントリメンバーが表示されます。Tetration がインベントリに関連付けられている場合、Tetration はワークロードプロファイルに直接リンクします。
CSCvo26557	パケットが iptable の具象ルールによってドロップされると、ドロップの理由が GUI で正しくない場合があります。
CSCvo35282	<exiting> プロセスの終了が検出されると、AIX ユニバーサルセンサーのインストールを続行できません。
CSCvo40172	エージェントインストーラスクリプトを拡張してバージョンをリストし、インストールする特定のバージョンを選択します。

不具合 ID	説明
CSCvo40192	システムの再起動後に、エージェントのエンフォーササービスを開始します。
CSCvo55269	Windows Universal Visibility のセルフテストは、無効な文字が原因で失敗します。
CSCvo59946	SMTP サーバの TAN メール設定で「安全な接続」をオプションに設定します。
CSCvo62460	センサーは、SLES 11 SP2 および SP3 プラットフォームにはインストールできません。
CSCvo62866	ADM はリンクローカルトラフィックをキャプチャしません。
CSCvo73637	断続的に、施行エージェントホストのリブート時に誤ったファイアウォールプロファイルが選択されます。

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
  - 以前のリリース (3.1.1. x) からクラスタをアップグレードするために3.2.1.20 リリースを使用することはできません。代わりに、リリース3.2.1.20 を使用して新しいクラスタを展開する必要があります。
  - 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。
- 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。
- 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、最後に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るたびに、ユーザは施行が停止してから約15分間、そのワークスペースのオブジェクトを削除してはなりません。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 ロードバランサー設定の 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

このリリースは、新規導入のみを対象としています。このリリースの 3.1.1. x リリースからは、このリリースにアップグレードすることはできません。

3.2.1.20 リリースのソフトウェアセンサーは、従来のディープ可視性と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: 5.1 ～ 5.11
  - CentOS-6.x: 6.1 ～ 6.10
  - CentOS-7.x: 7.0、7.1、7.2、7.3、7.4、7.5、および 7.6
  - 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 および 7.6
  - Oracle Linux サーバ-6.x: 6.0 ~ 6.10
  - Oracle Linux サーバ: 7.0、7.1、7.2、7.3、7.4、7.5、および 7.6
  - SUSE Linux-11.x: 11.2、11.3、および 11.4
  - SUSE Linux-12. x: 12.0、12.1、12.2、および 12.3
  - Ubuntu-12.04
  - Unbuntu-14.04 および 14.10
  - Ubuntu-16.04
- 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 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

3.2.1.20 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、および 7.6
  - 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 および 7.6
  - SUSE Linux-11.x: 11.2、11.3、および 11.4
  - SUSE Linux-12. x: 12.0、12.1、12.2、および 12.3
  - Oracle Linux サーバ-6.x: 6.0 ~ 6.10
  - Oracle Linux サーバ: 7.0、7.1、7.2、7.3、7.4、7.5、および 7.6
  - Ubuntu-14.04 および 14.10
  - Ubuntu-16.04
- 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 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

3.2.1.20 リリースでは、ユニバーサル可視性センサー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、6.1、7.1、および 7.2

3.2.1.20 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

* * ハードウェアセンサー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 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。
- 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

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

Cisco 5 tetration (39-RU) の表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 センサー対応 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。

Cisco 6 tetration (8 RU) の表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 センサー対応 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 Yetration 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 センサー対応 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 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 8 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]