Cisco Threat Grid アプライアンス バージョン 2.10 リリースノート

初版：2020 年 1 月 28 日

はじめに

このドキュメントでは、Cisco Threat Grid アプライアンス バージョン 2.10 の新機能、未解決の問題、および終了した問題について説明します。

ユーザ マニュアル

次に、入手可能な Threat Grid アプライアンスのユーザマニュアルを示します。

Threat Grid アプライアンスのユーザマニュアル

Threat Grid アプライアンスのユーザ マニュアルは、シスコ Web サイトの Threat Grid アプライアンスのインストールとアップグレードに関するガイドのページを参照してください。

（注） 新しいドキュメントは、「Threat Grid アプライアンスの製品とサポート」のページから入手できます。

バックアップに関するよくある質問

技術情報と手順については、『Backup Notes and FAQ』を参照してください。

クラスタリングの概要とよくある質問

詳細については、『Clustering Overview and FAQ』を参照してください。

更新のインストール

新しいバージョンで Threat Grid アプライアンスを更新する前に、シスコ Web サイトの Threat Grid アプライアンスのインストールとアップグレードに関するガイドのページから入手できる『AMP Threat Grid Appliance Setup and Configuration Guide』の説明に従って、初期設定および構成手順を完了しておく必要があります。

新しいアプライアンス：新しいアプライアンスが古いバージョンとともに出荷されていて、更新をインストールする場合は、先に初期設定を完了する必要があります。すべてのアプライアンス設定が完了するまで、更新を**適用しないでください**。

ライセンスがインストールされるまでアプライアンスの更新はダウンロードされず、アプライアンスが完全に設定されない限り（データベースを含む）、正しく適用されない可能性があります。

Threat Grid アプライアンスの更新は、OpAdmin Portal 経由で適用されます。

アップデートは一方向です。より新しいバージョンにアップグレードすると、以前のバージョンに戻すことはできません。

更新をテストするには、分析用のサンプルを提出してください。

バージョン 2.10

リリース日：2020 年 1 月 28 日

ビルド番号：2019.12.20200128T085836.srchash.5bec2ec5b74c.rel

このリリースでは、Cloud 3.5.45 リリースに準拠するようにコア Threat Grid ソフトウェアを更新し、アプライアンスの管理とアプリケーションの使用の両方で RADIUS ベースの認証に対するサポートを導入し、パスワードリセットの自動化における重大なバグが修正され、高負荷状態での Elasticsearch 動作が向上します。

修正と更新

バージョン 2.10 には、次の修正および更新が含まれています。

- コア Threat Grid アプリケーションは、リリース 3.5.45 に更新されます。
- RADIUS 認証のサポート（DTLS が有効になっている Cisco Identity Services Engine を使用）が導入されました。
- パスワードのリセットを有効にするために、（リカバリモードの tgsh から）リブートの前に **exit** コマンドを実行する必要がなくなりました。
- リテラル一重引用符文字を含むライセンスが検証に失敗するバグに対処しました。
- 検索操作のクエリが許可された長さを超えた場合の Elasticsearch の動作に対する調整を行いました。
- インストールされているライセンスの期限が切れた場合、期限が切れていない（または有効な）ライセンスが更新メディアに存在している限り、エアギャップ更新の適用が失敗しなくなります。
- アップグレードパスと使用シナリオ間の一貫性を確保するため、ファイルの所有権と権限がアップグレード時に適用されるメカニズムを強化しました。

既知の問題

- 直前のリリースと同様に、このリリースではバルクストレージの障害後にリセットした場合に使用される RAID-1 ストレージアレイに VM イメージのバックアップコピーが作成されます。初期の Cisco Threat Grid アプライアンスモデル（UCS C220-M3 プラットフォームベース）は、後のモデルよりもストレージ量が少なく、このリリースのインストール後に RAID-1 ファイルシステムで使用可能な残りのディスク領域は他のユニットよりも 25% 未満になる可能性が高くなります。これにより、サービス通知がトリガーされます。

  これより後のモデルのハードウェアでは、このリリースのインストール後の RAID-1 アレイの残りのストレージが 25% 未満になることは異常であり、カスタマーサポートへの報告が必要になる場合があります。

- ファームウェアの更新は、更新プロセス中に適用できない場合があります。これが発生した場合、これらの更新は再設定が正常に実行された後のリブートプロセス時に再試行されます。今後のリリースでは、これが発生した場合はサービス通知が提供される可能性があります。