Cisco Threat Grid アプライアンス バージョン 2.9 リリースノート

初版：2019 年 12 月 12 日

最終更新：2019 年 12 月 17 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 2.9 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最新ではないバージョンで出荷された場合、更新をインストールするには、最初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**。

アプライアンスの更新は、ライセンスがインストールされていない限りダウンロードされません。また、アプライアンス（データベースを含む）の設定が完全に行われていないと、更新が正しく適用されない場合があります。

Threat Grid アプライアンスの更新を適用するには、OpAdmin Portal を使用します。

更新は不可逆です。つまり、新しいバージョンにアップグレードした後、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 2.9 mfg

リリース日：2019 年 12 月 17 日

ビルド番号：2019.09.20191217T061826.srchash.ee4e1ec4f2c7.rel

このリリースがバージョン2.9と異なるのは、インストール中にホスト名を区別するMFGNFS修正が提供されることのみです。

バージョン 2.9

リリース日：2019 年 12 月 12 日

ビルド番号：2019.09.20191212 T010702. srchash. 6195db15f97a. rel

このリリースでは、クラウド3.5.39リリースに従ってコアThreat Gridソフトウェアが更新されます。管理インターフェイスを無効化できるようになります（無効化されると、クラスタ化されていないアプライアンスはクリーンポートとダーティーポートが接続されている場合のみ正常に動作します）。また、信頼性の低い NFS サーバで使用する際の堅牢性が向上します。他にもさまざまな改善が含まれます。

修正と更新

バージョン 2.9 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 3.5.39 に更新されます。この更新では、悪意があるとみなされるサンプルのスコアリングしきい値が、以前の 95 ではなく 90 で現在のクラウドの動作と同期することに注意してください。
- VMイメージのバックアップメンテナンスはオンライン更新プロセスから切り離され、オンラインのダウンロードではなく、エアギャップ ISO を介して更新されたシステムのリセットの失敗を防ぎます。

- 無効なリモートsyslog設定が、カスタマーサポートの支援なしでシステムを設定できないというシナリオが解決されました。
- NFS ストレージに使用される暗号化レイヤには、サーバからスプリアス ESTALE の結果を受信した際のクラッシュを回避するため、パッチが適用されます。これらのエラーによってデータが破損する可能性が残ることに注意してください。そのため、NFS サーバ側の原因を調査することを強く推奨します。
- プライマリ Threat Grid インターフェイスの管理者ユーザのパスワードは、管理 Web UI への初回ログイン時にユーザが指定したパスワードセットから初期化されるようになりました。
- 物理的な管理ポートを無効化できるようになりました。無効になっている場合、クラスタ化されていないアプライアンスは、クリーンポートとダーティーポートが接続されている場合のみ正しく動作します。管理 UI はクリーンインターフェイスのポート 8443 に表示されます。ポートが無効になっていない場合、管理ポートを切断すると、アプライアンスは機能しなくなります（または、部分的にしか機能しません）。
- デフォルトの自己署名証明書の生成は、MacOS 10.15（Catalina）によって受け入れられる証明書を生成するように変更されました。
- RAID アレイのハードウェアヘルスチェックがハングするまれなシナリオが検出され、アラートが生成されます。
- サービスごとのステータスメトリックを収集するために使用される基本的なメカニズムが大幅に見直されます。
- 長期間にわたって同期されていなかったクラスタが正常に再同期できない問題が解決されました。
- クラスタ化された構成でのみアクティブな失敗したサービスが、失敗時に再起動しない問題が解決されました。

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。