Cisco Secure Malware Analytics アプライアンス（旧 Threat Grid アプライアンス）バージョン 2.20 リリースノート

最終更新：2026 年 8 月 20 日

はじめに

このドキュメントでは、Cisco Secure Malware Analytics（旧 Threat Grid）アプライアンス バージョン 2.20.0 のリリースノート、および既知の問題について説明します。

ユーザーマニュアル

入手可能な Cisco Secure Malware Analytics（旧 Threat Grid）アプライアンスのユーザーマニュアルを次に示します。

Cisco Secure Malware Analytics アプライアンスのユーザーマニュアル

アプライアンスのユーザーマニュアルは、シスコ Web サイトの Cisco Secure Malware Analytics 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、Cisco Secure Malware Analytics 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

Cisco Secure Malware Analytics（旧 Threat Grid）アプライアンスを新しいバージョンに更新する前に、シスコ Web サイトの Cisco Secure Malware Analytics 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『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。

Cisco Secure Malware Analytics アプライアンスの更新は、管理 UI ポータルを介して適用されます。

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。

修正と更新

バージョン 2.20.0

- コアアプリケーションがクラウドバージョン 3.5.149 に更新されました。
- デフォルトの PostgreSQL バージョンが 13.5 にアップグレードされました。マルチノードクラスタ用にアップグレードツールが提供されています。
- ElasticSearch バージョンが 7.17 にアップグレードされました。
- 更新を開始する前に確認のプロンプトが表示されるようになりました。
- OpAdmin インターフェイスの右上隅にアプライアンスのシリアル番号が常に表示されるようになりました。
- スナップショットをサポートするために、Prometheus データ、ログ、および OpAdmin clj 出力が追加されました。
- PostgreSQL データベースのバックアップ保持が 10 件に増え、1 日おきに実行されるようになりました。
- 送信集中時のパフォーマンス低下を回避するため、署名付きコマンドを使用しない transparent_hugepage が無効化されました。
- PostgreSQL のアップグレードをサポートするようにクラスタリングメニューが強化されました。
- OpAdmin の管理者ドキュメントが改善されました。
- 新しい OpenDNS キーをアクティブにする場合は再設定後にリブートが必要であるという注意事項が追加されました。

- クラスタの緊急リカバリのための NFS からの復元が修正されました。
- 更新を適用するためのリブート中に接続失敗ページが表示される問題が修正されました。
- フラグ API 操作が修正されました。
- サービス通知の詳細を表示するときに [終了日（Close On）] フィールドに [範囲外の日付（Date out of range）] が表示される問題が修正されました。
- CVE を緩和するために暗号と HMAC が制限されました。
- CVE-2023-39533 の緩和策として、SHA-1 ハッシュまたは異常に大きい（8192 ビットを超える）RSA キーを含む新しい証明書が OpAdmin で設定されないようにブロックされました。
- RADIUS 認証証明書またはキーに対する変更がリブートしないと適用されない問題が修正されました。
- consul-transient および consul-tiebreaker に対して必要がないときに作成されるサービス通知が修正されました。
- 通知設定に対する変更がリブートしないと適用されない問題が修正されました。
- ストレージステータスページに NFS 統計情報が追加されました。
- OpenDNS 設定の変更がリブートなしで有効になるように修正されました。

既知の問題

- Elasticsearch の移行中のエラー：更新後、Elasticsearch の移行の進行中にアプライアンスが再設定されると、移行が失敗する可能性があります。Elasticsearch Migration サービスの通知がクリアされるまで、再設定しないでください。再設定が原因で移行が失敗した場合は、シェル/コンソールから service restart elasticsearch-migrate-precheck コマンドを使用して再試行してください。移行が完了するまでは再設定を実行しないでください。繰り返し失敗する可能性があります。シェル/コンソールにアクセスできない場合は、サポートにお問い合わせください。詳細については、CDETS の CSCwu05983 を参照してください。

アップグレードに関する注意事項

- このリリースには、アプライアンス上の PostgreSQL データベースのアップグレードが含まれています。ノードが 1 つだけのスタンドアロンのノードおよびクラスタは、アプライアンスをバージョン 2.20.0 に更新すると自動的にアップグレードされます。ただし、マルチノードクラスタでは、クラスタ内のすべてのアプライアンスが 2.20.0 に更新された後、OpAdmin で管理者による手動介入が必要になります。詳細な手順については、2.20.0 管理マニュアルを参照してください。

- アップグレードにはElasticSearchインデックスの移行が必要です。これは、すべてのクラスタノードが 2.20.0 にアップグレードされると、アプライアンスで自動的に実行されます。移行中にAPIによって報告される送信ステータスは、現在の月のインデックスが更新されるときに遅延することがあります。このような遅延は、移行開始後数時間以内に解消されるはずです。インデックスの移行が成功した後、メンテナンス期間中にシステムをリブートする必要があります。
- OpAdmin では、SHA-1 ハッシュまたは異常に大きい（8192 ビットを超える）RSA キーを含む新しい証明書の作成は許可されていませんが、既存の証明書は警告付きで引き続き機能します。
- リリース 2.20.0 では、お客様は、VirusTotal（VT）API キーが /api/v3/intelligence/search エンドポイントをサポートしていることを確認する必要があります。VT API キーの詳細については、VirusTotal の公式ドキュメントを参照してください。

早期警告アドバイザリ

- Cisco Secure Malware Analytics 3.0.0 リリース以降では、NFS は RHEL および Ubuntu ベースのディストリビューションでのみサポートされます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。