Cisco Threat Grid アプライアンス

リリース ノート

バージョン：2.7.2ag

最終更新日：2019 年 8 月 8 日

Cisco Systems, Inc. www.cisco.com

All contents are Copyright © 2015-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムに適応したものです。全著作権所有。著作権©1981、カリフォルニア大学の評判。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。Cisco およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、Cisco およびその供給者は、このマニュアルに適用できるまたは適用できないことによって、発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性が Cisco またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco および Cisco ロゴは、シス コ またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、Cisco と他社との間のパートナーシップ関係を意味するものではありません。

Cisco および Cisco ロゴは、シスコ またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、Cisco と他社との間のパートナーシップ関係を意味するものではありません。

表紙写真 Copyright © 2016 Mary C. Ecsedy. All rights reserved. Used with permission.

All contents are Copyright © 2015-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

コンテンツ

コンテンツ 3
ユーザ マニュアル 10
バックアップに関するよくある質問 10
クラスタリングの概要とよくある質問 10
更新プログラムのインストール 10
ビルド番号/リリース バージョン ルックアップ テーブル 11
バージョン 2.7.2ag 16
バージョン 2.7.2 17
修正と更新 17
セキュリティ更新 17
バージョン 2.7.1 18
修正と更新 18
既知の問題 18
セキュリティ更新 19
バージョン 2.7 20
修正と更新 20
既知の問題 21
その他の注意事項 21
バージョン 2.6 22
修正と更新 22
バージョン 2.5 23
修正と更新 23
バージョン 2.4.3.3 24

修正と更新 24
バージョン 2.4.3.2 25
修正と更新 25
バージョン 2.4.3.1 26
バージョン 2.4.3 26
修正と更新 26
バージョン 2.4.2 28
修正と更新 28
バージョン 2.4.1 30
修正と更新 30
既知の問題 31
セキュリティ更新 31
バージョン 2.4.0.1 32
修正と更新 32
セキュリティ更新 32
バージョン 2.4 33
修正と更新 33
バージョン 2.3.3 34
修正と更新 34
バージョン 2.3.2 35
修正と更新 35
バージョン 2.3.1 36
修正と更新 36
バージョン 2.3 37
修正と更新 37

バージョン 2.2.4 38
修正と更新 38
バージョン 2.2.3 39
重要 39
修正と更新 39
セキュリティ更新 39
バージョン 2.2.2 40
重要 40
バグ修正 40
拡張機能 40
バージョン 2.2.1 41
重要 41
新機能 41
バグ修正 41
セキュリティ修正 41
バージョン 2.2 製造 42
バージョン 2.2 43
要件 43
資料 43
このリリースについて 43
新機能 44
バグ修正 44
セキュリティ修正 44
バージョン 2.1.6 45
新機能 45

既知の問題 45
バージョン 2.1.5 46
新機能 46
バグ修正 46
既知の問題 47
バージョン 2.1.4 48
新機能 48
バグ修正 48
既知の問題 48
バージョン 2.1.3 49
新機能 49
バグ修正 49
既知の問題 49
バージョン 2.1.2 50
バグ修正 50
既知の問題 50
バージョン 2.1.1 51
新機能 51
バグ修正 51
セキュリティ修正 51
既知の問題 51
バージョン 2.1 52
新機能 52
バグ修正 52
セキュリティ修正 53

既知の問題 53
バージョン 2.0.4 54
新機能 54
バグ修正 54
バージョン 2.0.3 55
バージョン 2.0.2 56
セキュリティ更新 56
バージョン 2.0.1 57
バグ修正 57
既知の問題 57
バージョン 2.0 58
新機能 59
バグ修正 59
セキュリティ修正 59
既知の問題 59
バージョン 1.4.6 60
新機能 60
バージョン 1.4.5 61
バージョン 1.4.4 62
バグ修正 62
バージョン 1.4.3 63
新機能 63
セキュリティ更新 63
既知の問題 63
バージョン 1.4.2 64

バグ修正 64
既知の問題 64
バージョン 1.4.1 65
1.4 以前のリリースからのアップグレード 65
バグ修正 65
バージョン 1.4 66
新機能 66
バグ修正 67
バージョン 1.3 68
新機能 68
バグ修正 69
セキュリティ更新 69
その他の注意事項 69
バージョン 1.2.1 70
新機能 70
セキュリティ更新 70
バージョン 1.2 71
新機能 71
バグ修正 71
セキュリティ更新 72
その他の改善点 72
既知の問題 72
バージョン 1.1 ホットフィックス 1 73
バージョン 1.1 74
新機能 74

バグ修正 74
セキュリティ更新 75
1.0+hotfix2 Update - 必須 76

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。

更新プログラムのインストール

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 AMP Threat Grid アプライアンスのインストールおよび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『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。**

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。

ビルド番号/リリース バージョン ルックアップ テーブル

ビルド番号	リリース バージョン	リリース日	注記
2019.02.20190808T000800.srchash.b61789e86a09.rel	2.7.2ag	2019 年 8 月 8 日	エアギャップアプライアンスのみ。
2019.02.20190723T224935.srchash.bb8b40c2e248.rel	2.7.2	2019 年 7 月 23 日	バックアッププルーニングの修正、セキュリティおよび M5 製造の更新。
2019.02.20190703T201951.srchash.0f2b9bc45628.rel	2.7.1	2019 年 7 月 3 日	ネットワーク シミュレーション、ES インデックスをバージョン 6 へ移行。
2019.02.20190601T155353.srchash.b67f91c65917.rel	2.7	2019 年 6 月 1 日	3.5.27 への更新、ES6、XFS、Wal-G、リセット時のデータ ドライブのワイプ。
2018.12.20190204T162246.srchash.cb9269c1357f.rel	2.6	2019 年 2 月 4 日	保持制限の厳格化
2018.08.20180914205342.474e26a8.rel	2.5	2018 年 9 月 14 日	Win10、サンプルの削除。3.5.11 への更新
2017.12.20180601200650.e0c052b0.rel	2.4.3.3	2018 年 6 月 1 日	クラスタの初期化を修正、古い ES/PG 移行のサポートをプルーニング
2017.12.20180519011227.ed8a11e9.rel	2.4.3.2	2018 年 5 月 19 日	CVE-2018-1000085 の ClamAV を更新。バグ修正。

ビルド番号	リリース バージョン	リリース日	注記
2017.12.20180501005218.4e3746f4.rel	2.4.3.1	2018 年 5 月 1 日	PG スキーマで更新確認時の DDL エラー検出を報告
2017.12.20180427231427.e616a2f2.rel	2.4.3	2018 年 4 月 27 日	Remote Virtual Exit Localization、スタンドアロンからクラスタへの直接移行
2017.12.20180302174440.097e2883.rel	2.4.2	2018 年 3 月 2 日	クラスタリング
2017.12.20180219033153.bb5e549b.rel	2.4.1	2018 年 2 月 19 日	OpAdmin のクラスタリング サポート。アプリケーションの 3.4.59 への更新
2017.12.20180130110951.ce6dd56e.rel	2.4.0.1	2018 年 1 月 30 日	セキュリティ更新プログラムを ClamAV にのみ更新
2017.12.20171214191003.4b7fea16.rel	2.4	2017 年 12 月 14 日	クラスタリング EFT。jp/kr contsubs。ポータルを 3.4.57 に更新。
2016.05.201711300223355.1c7bd023.rel	2.3.3	2017 年 11 月 30 日	2.4 アップグレードの開始点
2016.05.20171007215506.0700e1db.rel	2.3.2	2017 年 10 月 7 日	ElasticSearch シャードカウントの減少。
2016.05.20170828200941.e5eab0a6.rel	2.3.1	2017 年 8 月 28 日	バグ修正。

ビルド番号	リリース バージョン	リリース日	注記
2016.05.20170810212922.28c79852.rel	2.3	2017 年 8 月 11 日	ライセンスのダウンロードを自動化。ポータルのソフトウェアを 3.4.47 に更新。
2016.05.20170710175041.77c0b12f.rel	2.2.4	2017 年 7 月 10 日	このリリースでは、バックアップの機能について説明します。
2016.05.20170519231807.db2f167e.rel	2.2.3	2017 年 5 月 20 日	このマイナー リリースには、Windows XP なしで実行する新しい工場出荷時のインストールが使用できます。
2016.05.20170508195308.b8dc88ed.rel	2.2.2	2017 年 5 月 8 日	ネットワーク構成およびオペレーティング システムのコンポーネントに対する変更のマイナー リリースで今後の機能をサポートします。
2016.05.20170323020633.f82e66fe.rel	2.2.1	2017 年 3 月 24 日	SSLv3 の無効化、リソースの問題修正
2016.05.20170308211223.c92516ee.rel	2.2mfg	2017 年 3 月 8 日	製造時のみの変更。お客様への影響はありません。更新サーバ経由での導入は行われません。
2016.05.20170303034712.1b205359.rel	2.2	2017 年 3 月 3 日	システム移行、新しいポータル UI、「Mask」、配置サービス用の複数の URL
2016.05.20170105200233.32f70432.rel	2.1.6	2017 年 1 月 7 日	OpAdmin/tgsh-dialog 用の LDAP 認証サポート

ビルド番号	リリース バージョン	リリース日	注記
2016.05.20161121134140.489f130d.rel	2.1.5.	2016 年 11 月 21 日	ElasticSearch5、CSA パフォーマンス修正
2016.05.20160905202824.f7792890.rel	2.1.4	2016 年 9 月 5 日	主に製造向け
2016.05.20160811044721.6af0fa61.rel	2.1.3	2016 年 8 月 11 日	オフライン更新サポート キー、M4 ワイプ サポート
2016.05.20160715165510.baed88a3.rel	2.1.2	2016 年 7 月 15 日	
2016.05.20160706015125.b1fc50e5.rel-1	2.1(1)	2016 年 7 月 6 日	
2016.05.20160621044600.092b23fc	2.1	2016 年 6 月 21 日	
2015.08.20160501161850.56631ccd	2.0.4	2016 年 5 月 1 日	2.1 更新の開始点。2.1 に更新する前に、2.0.4 である必要があります。
2015.08.20160315165529.599f2056	2.0.3	2016 年 3 月 15 日	AMP 統合、CA 管理、スプリット DNS を導入
2015.08.20160217173404.ec264f73	2.0.2	2016 年 2 月 18 日	
2015.08.20160211192648.7e3d2e3a	2.0.1	2016 年 2 月 12 日	
2015.08.20160131061029.8b6bc1d6	v2.0	2016 年 2 月 11 日	ここから 2.0.1 へ強制的に更新
2014.10.20160115122111.1f09cb5f	v1.4.6	2016 年 1 月 27 日	2.0.4 更新の開始点

ビルド番号	リリース バージョン	リリース日	注記
2014.10.20151123133427.898f70c2	v1.4.5	2015 年 11 月 25 日	
2014.10.20151116154826.9af96403	v1.4.4		
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1 +hotfix1		
2014.10.20150203155142.b06f7b4f	v1.1		
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0 +hotfix2		**注：**1.0+hotfix2 は必須の更新であり、更新システム自体を修正して中断なく大きなファイルを処理できるようにします。
2014.10.20141125162158.8afc5e2f	v1.0		

バージョン 2.7.2ag

このリリースは Threat Grid アプライアンスのリリース 2.7.2 と同じですが、より効率的でコンパクトなオフライン更新メディア生成メカニズムのサポートが追加されている点が異なります。

バージョン 2.7.2

このリリースでは、リリース 2.7.0 および 2.7.1 で NFS バックアップに過剰なストレージが要求される問題が修正されました。また、（コンソールでの明示的な切り替えとして）クリーンインターフェイスを介して opadmin へのアクセスを有効にする機能が追加されています。

修正と更新

- データベースのベースバックアップは、新しいベースバックアップが正常に作成されるまで保持されるようになりました。
- コンソール設定インターフェイスは、（設定を適用して再起動した後）割り当てられたクリーン IP のポート 8443 で管理インターフェイスへのアクセスを有効にする「enable_clean_opadmin」オプションをサポートするようになりました。この機能はデフォルトでは無効になっています。

セキュリティ更新

CVE-2019-10192 および CVE-2019-10193 を含むデータ破損修正のための再配布が更新されました。

バージョン 2.7.1

このリリースでは、アプライアンスのネットワーク シミュレーション サポートの追加、一部のセキュリティ問題に対する緩和策の実装、2.7.0 でデータのリセット後にクラスタ設定が失敗する原因となるバグの修正、新しいバージョンの Elasticsearch に基づく将来のリリースとの互換性に備えたバックグラウンド移行の実装など、さまざまな小規模の改善が行われています。

修正と更新

- アプライアンスでネットワーク シミュレーションを使用できるようになり、2.7.0 における既知の制限が解消されました。
- アプライアンス設定 UI の [exit] セクションには、ローカルにシミュレートされたネットワークのみが VM で使用できる追加のモードがあります。このオプションを管理者として選択した場合、API および UI ユーザは、VM からローカルアプライアンス外の宛先にネットワークトラフィックを送信するオプションを選択できません。
- このリリースから、ES6 ネイティブインデックスへのバックグラウンド Elasticsearch インデックスの移行が有効になりました。この移行は、Elasticsearch 7.0 以降が必要な Threat Grid アプライアンスがインストールされる前に正常に完了している必要があります。
- コマンドライン構成ツールにおけるオプション名のスペルミスは、より意味のあるエラーメッセージで処理されるようになりました。
- 2.7.0 にアップグレードすると、（サポートされている UI プロセスを通じて厳密にインストールおよび設定されるのではなく）サポートによって設定が変更されたクラスタが失敗する可能性のある問題が解決されました。
- ステータスを照会したり、スケジュールされたバックグラウンドジョブの実行を手動でトリガーしたりする機能が改善されました。

既知の問題

Elasticsearch インデックスの移行により、NFS バックアッププロセスに大幅な遅延が発生し、それに関連する警告が発生する場合があります。これらの警告は無視する必要がありますが、サービスの通知はインデックスの移行がアクティブに進行中であることを示し、インデックスの移行プロセスの進行が長時間にわたって失敗した場合に限り、サポートとともに発生します。

セキュリティ更新

- TCP 選択的受信確認サポートを無効にし、最大セグメントサイズを要求するパケットを 300 バイト未満にドロップすることにより、CVE-2019-11477、CVE-2019-11478 および CVE-2019-11479 が軽減されます。
- Kibana Timelion のサポートを無効にすることにより、CVE-2019-7608 が軽減されます。
- bzip2 にパッチを適用して、CVE-2019-12900 の修正を反映します。

バージョン 2.7

このリリースでは、クラウド 3.5.27 リリースに応じたコア Threat Grid ソフトウェアの更新、Elasticsearch 6.5 への移行、およびアプライアンス固有のツールおよびインフラストラクチャのいくつかの拡張機能の提供が行われています。

修正と更新

- サンプル削除機能の範囲は、クラウド製品の動作に合わせ、アーティファクトを含むように拡張されました。
- データ リセットのプロセスがより包括的になりました。すべての顧客関連データが確実に破壊されることを保証するためには今後も（リカバリ ブートローダ メニュー内の）ワイプ プロセスが必要ですが、リセット プロセスにより、以前に残されたオペレーティング システムのログおよびその他の状態がクリアされるようになりました。

  アプライアンスが正常にリセットされると、新しいランダム生成のパスワードがコンソールに表示されます（新規インストール時の動作と同じです）。

  この改善されたプロセスは、複数回再起動するようになっています。また、リカバリ モードからの起動が可能になりました（以前のプロセスでは、通常動作への起動時のみ正常な起動が可能でした）。
- TLSv1.0 および TLSv1.1 は、管理インターフェイスでは無効になっていて、メイン アプリケーションではデフォルトで無効になっています。これらのプロトコルのいずれかが統合の互換性のために必要な場合は、tgsh から再有効化できます（メイン アプリケーションの場合のみ）。
- コア Threat Grid アプリケーションの検索可能なデータストアとして、Elasticsearch 6.5.4 が使用されています。Elasticsearch 7.x のみをサポートする将来のリリースをデータ損失なしでインストールするには、事前にバックグラウンド移行を行い、履歴インデックスを更新しておくことが必要になります。将来のバージョンのリリース ノートに注意してください。
- ホスト名：一部の NFSv4 サーバとの相互運用性を向上させるため、アプライアンスのシリアル番号がホスト名として使用されるようになりました。
- このリリース以降で初めて製造されるアプライアンスは、プライマリ ファイルシステムとして XFS を使用します。この変更は、特に説明がない限り、既存のデバイスには影響しません。
- アプライアンスのデータがリセットされると、それらのデータストアは XFS に変更されます。これにより、前方互換性が向上し、サービス単位の I/O 使用率のモニタリングに OS レベルのサポートが提供されるようになります。
- WAL-E は維持されなくなり、PostgreSQL のバックアップ/復元については WAL-G に置き換えられました。既存の WAL-E アーカイブは今後も使用可能で、大規模なバックアップの復元の際には PostgreSQL の時間が大幅に短縮されます。

- カスタマー サポート接続に使用される IP アドレスのリストが、サポート モードが有効になっているときに DNS 解決が正しく動作しない場合、その時点で実稼働に使用されているサーバを正確に反映するように更新されるようになりました。
- アプライアンスにアクセスするために SSH 公開キーを設定すると SSH によるパスワード ベースの認証が無効になり、SSH 認証方式は両方ではなくどちらか 1 つだけが有効化するようになりました（キー ベースの認証を使用して SSH 接続が成功すると、tgsh のダイアログでパスワードの入力が求められ、両方のトークンが求められます）。
- リカバリ モードでのネットワーク設定がシステム全体をミラーリングするようになりました。すべてのインターフェイスが起動されます。どのプロセスがどのインターフェイスで通信できるかを制限するファイアウォール ルールおよびポリシー ルーティングが有効化されています（ポート 19791 のサポート モード トラフィックは、3 つのインターフェイスすべてに対して許可されます）。
- システム モニタリング グラフを表示するために使用されるツールが、このリリースで更新されました。過去のシステム モニタリング データは、この移行後は保持されません。

既知の問題

アップストリーム 3.5.27 のマニュアルとは異なり、ネットワーク シミュレーションのサポートは、アプライアンスでまだ提供されていません。

その他の注意事項

データ リセット プロセスには、システムの SSD への新規インストールに必要なすべてのコンテンツを保存できる十分なストレージが必要になりました。このコンテンツの存在と有効性が確保された後にのみ、既存のデータが削除されます。システム（特に第 1 世代のハードウェア）は長期にわたって使用されているため、すぐに利用できる十分なスペースがない可能性があります。必要に応じてカスタマー サポートをご利用ください。

バージョン 2.6

リリース日：2019 年 2 月 4 日

このリリースでは、コア Threat Grid ソフトウェアがクラウド 3.5.19 リリースに準拠するように更新されました。また、今後のリリース サイクルを短縮するための内部的な機能拡張も行われています。

修正と更新

- 設定オプションを使用して、保持期間の制限を厳密に適用することができます（分析からのアーティファクトは、利用可能なストレージのため長期の保持が可能であっても 15 日を超えて保持されることがなくなります）。これは、デフォルトでは無効になっています。
- オプションの日本語および韓国語の VM イメージに Microsoft Office が含まれるようになりました。
- スタンドアロン ノードをクラスタの初期ノードとして移行する際に設定の失敗を引き起こす可能性のある問題に対処しました。
- 「tgsh」コマンド（ポケットベル、サービス ステータスの変更、またはローカル タイムゾーンの調整を実行するコマンド）が失敗する原因となっていた問題が解決されました。
- Elasticsearch がループに陥る可能性があるシナリオ（スタートアップ時に一貫性のないインデックスを修復または回復するためのウォッチドッグ タイムアウトが不十分であることが原因）に対処しました。

バージョン 2.5

リリース日：2018 年 9 月 14 日

このリリースでは、コア Threat Grid ソフトウェアがクラウド 3.5 シリーズに準拠するように更新されました。

これは、Windows 10 のサポートを含む最初のアプライアンス リリースです。

この更新をインストールすると、このアプライアンスと統合された ESA/CSA デバイスのアカウント名が変更されます（以前の名前では機密情報が漏洩する可能性があるため）。このプロセスで発生した問題は、「デバイス名の移行（Device Name Migration）」というタイトルで報告されます。ESA または CSA デバイスに対する変更は必要ありません。ご質問については、カスタマー サポートまでお問い合わせください。

修正と更新

- Windows 10 VM サポートが追加されました。
- アプライアンスでサンプル削除のサポートが利用できるようになりました（このリリースのインストール前に元々アップロードされていたサンプルを削除しても、アプライアンスの別の場所に保存されたサンプルのコピーは削除されません。ただし、これらの追加コピーは、『Threat Grid Appliance Data Retention Notes』の「Disk Artifacts」に記載された保持ルールの対象になり、新しいコンテンツが追加されるにつれて最終的にはエージング アウトします）。
- 将来のストレージおよび更新の効率性を向上させるため、VM ストレージ形式が変更されました。
- システム モニタリング グラフを生成するために使用されるツールが更新されました。すべてのダイレクト URL が変更されることを想定しています。
- NFS の無効化が、すでに設定が完了しているアプライアンスでさらにサポートされるようになりました。
- 接続された USB ストレージ デバイスが誤った SMART ハードウェア ステータスの警告を生成することがなくなりました。
- CVE-2018-5391 を使用したサービス妨害攻撃を軽減するために、IP フラグメンテーションの設定が変更されました（これらの攻撃が有効になるには、サンドボックス化されたマルウェアによってではなく、お客様のネットワークから起動される必要があります）。
- システム全体が新しいバージョンの gcc で構築され、カーネルでの完全な retpoline サポートが可能になりました。
- 2.4.0 で導入されたリグレッションが修正され、破損した redis ストアは、クラスタリングが有効になっていない場合でも自動的に修復されるようになりました。

バージョン 2.4.3.3

リリース日：2018 年 6 月 1 日

このポイント リリースでは、新しいクラスタを最初から作成するときのデータベース初期化プロセスの問題に対処しています（スタンドアロン アプライアンスによって作成されたバックアップから初期化される新しいクラスタは影響を受けません）。また、一部の使用されていないソフトウェア ライブラリが削除されました。

修正と更新

- これは予防的な修復です。すでに空のデータベースを使用してクラスタを初期化しているお客様は、「データベースエンコーディングが正しく設定されていません（Database encoding is not set correctly）」という文面のサービス通知を受信します。その場合は、カスタマー サポートに連絡して遡及的な修正をスケジュールする必要があります。
- アプライアンス クラスタを作成するための準備をしないお客様は、この更新プログラムをインストールする必要はありません。
- **2.2 より前のリリースからのデータ移行はサポートされなくなりました。**

  使用されていないコードが削除されたため、ElasticSearch 5 の移行が正常に実行されたことのないアプライアンス（2.1 シリーズの最後）には、カスタマー サポートがこの移行を後から実行できるようにするツールが付属しなくなります。

  同様に、PostgreSQL が 9.6 に更新されていないシステム（2.2.0 より前にも同様に発生）にも、この更新を後から実行できるようにするツールが付属しなくなります。

  これらの移行が完了していないシステムは、2.3 または 2.4 リリースでは正常に動作せず、2.1.6 を実行すると、移行の完了を許可するか、それ以上の更新を実行する前にカスタマー サポートに連絡するようにユーザに指示する通知が表示されます。リリース ノートまたはカスタマー サポートからそうしないように個別の指示がある場合を除き、更新を適用する前には、システムがおおむね正常に動作していることを確認してください。

バージョン 2.4.3.2

リリース日：2018 年 5 月 19 日

このポイント リリースには、1 つのセキュリティ更新と 2 つのバグ修正が含まれています。

修正と更新

- CVE-2018-1000085 に対処するため、ClamAV が更新されました。
- 「win7-x64」仮想マシンが使用できなくなる状態を修復できるようにするため、更新メカニズムが強化されました。

  この状態は、以前に 2.4.1 以降に更新されたシステムにのみ影響します。

  この修正を適用するには、2.4.3.2 のインストール後に更新プログラムのダウンロードを正常に完了させ、その後再起動する必要があります。
- ソフトウェア障害により、2.4.3 以降のインストール後に少なくとも 1 回の更新チェックが実行されるまで、サンプルの実行が妨げられる場合がありました。この問題が修正されました。

2.4.3 より前のリリースから更新する場合は、2.4.3 および 2.4.3.1 のリリース ノートも参照してください。

バージョン 2.4.3.1

リリース日：2018 年 5 月 1 日

さらに、2.4.3.1 では、データベース スキーマの異常の診断レポートが追加されています。この機能の一部として、更新サーバに顧客データが報告されることはありません。レポートはすべてメタデータ（DDL）のみであり、将来のアップグレードの信頼性を確保するためのものです。

バージョン 2.4.3

リリース日：2018 年 4 月 27 日

このリリースでは、コア Threat Grid ソフトウェアが更新されました。リセット プロセスを中断させることなくスタンドアロン アプライアンスをクラスタの最初のノードにプロモーションするサポートが追加されました。また、お客様が利用可能なリモート終了メカニズム（以前の利用制限付きの「tg-tunnel」メカニズムに代わるもの）が追加されました。tg-tunnel を使用しているお客様は、この更新を適用する前に以下の注意事項をよくお読みください。また、ご質問はカスタマー サポートまでお問い合わせください。

修正と更新

- クラウド ポータル リリース 3.4.65 に対応する新しいバージョンのコア Threat Grid ソフトウェアが使用されています。

  利用できる機能は、クラウド ソフトウェアとアプライアンス ソフトウェアの間で異なる場合があります。API の相違点については、API マニュアルの関連セクションを参照してください。UI の相違点については、ポータルのオンライン ヘルプ（[ヘルプ（Help）] > [Threat Grid の概要（Introduction to Threat Grid）] > [Threat Grid クラウドとアプライアンスの比較（Threat Grid Cloud and Appliances Comparison）]）を参照してください。

- NFS にバックアップされたデータがあるスタンドアロン アプライアンスは、データベースをリセットおよびバックアップから復元して新しいクラスタの最初のノードになるようにする必要はなくなりました。

- リモート終了サポートが使用可能になりました。この機能がアクティブになっている場合（tg-tunnel を使用するように以前に設定されているアプライアンスの場合のみ、デフォルトでオンになっています）、マルウェア VM からシスコのデータセンターへ、そこから終了ロケーションへとトラフィックがトンネリングされます。

  このサービスで使用する新しいキーは、ソフトウェア更新プログラムがダウンロードされたときに取得されます（更新がない場合も同様です）。これは、このサービスを使用する前に、少なくとも 1 回更新チェックを実行する必要があることを意味します。ライセンスが期限切れになっているアプライアンスは新しいキーを取得できない可能性があるため、このサービスが使用できなくなる可能性があります。また、オフライン更新メカニズムでのみ更新プログラムをインストールしているアプライアンスでは、このサービスは使用できません。

- 仮想マシンが保存される方法が、VM への小規模な変更を展開する際に必要な最小限のデータ転送量を削減するために変更されました。

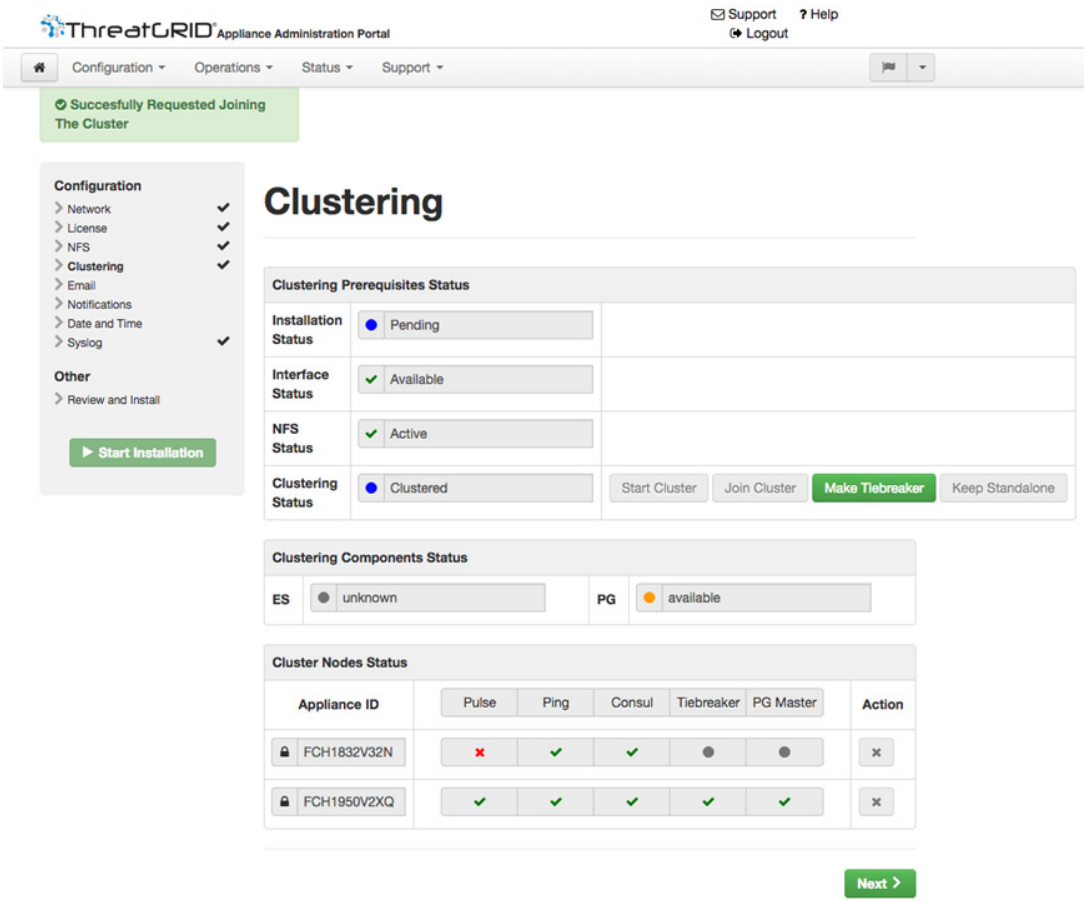
バージョン 2.4.2

リリース日：2018 年 3 月 2 日

これは、アプライアンスのクラスタリングが一般的に機能として使用可能になった最初のリリースです。クラスタリングがまだ初期フィールド トライアル機能と見なされていた最後のリリースであるバージョン 2.4.1 以降、セットアップおよびワークフローのさまざまな改善が行われています。

修正と更新

- 複数の Threat Grid アプライアンスが同じクラスタのメンバーである場合を除き、複数のアプライアンスによる同じキーを使用した読み取り/書き込みアクセスのために単一のデータストアがマウントされることがないようにする安全機能が追加されました。
- クラスタリングに対し、初期フィールド トライアルへの参加を示すライセンスが不要になりました。
- 長時間の稼働後にクラスタのモニタリングで断続的に Elasticsearch クラスタの状態を判断できなくなるシナリオが解決されました。
- NFS 設定は、アクティブにマウントされているときに更新できないようになりました。ノードがクラスタの一部ではない場合は、OpAdmin 管理インターフェイスでマウント解除オプションを使用できます。
- Threat Grid データセンターを介して発信トラフィックをトンネリングしている場合にネゴシエーションに失敗することがある問題が解決されました。
- 新しいクラスタリング設定のページ：



バージョン 2.4.1

リリース日：2018 年 2 月 19 日

このリリースでは、コア Threat Grid ソフトウェアが更新され、アプライアンス クラスタのセットアップおよびメンテナンスのための設定 UI が導入されました。

また、このリリースでは、アプライアンスが再起動するまで新しいサンプル分析操作を実行できない状態を引き起こすバグが修正され、クラスタリングのサポートに多くの安定性向上策が実施されているほか、以前は 2.4.0.1 暫定リリースのみで使用可能であったセキュリティ更新が含まれています。

修正と更新

- クラウド ポータル リリース 3.4.59 に対応する新しいバージョンのコア Threat Grid ソフトウェアが使用されています。注目すべき点として、これには、サンプル レポートの拡張機能が含まれています。詳細については、ポータルのオンライン ヘルプ（[ヘルプ（Help）] > [リリースノート（Release Notes）]）に掲載のリリース ノートを参照してください。

  （利用できる機能は、クラウド ソフトウェアとアプライアンス ソフトウェアの間で異なる場合があります。詳細については、マニュアルを参照してください。相違点については、API マニュアルの関連セクションを参照してください。UI の相違点については、ポータルのオンライン ヘルプ：[ヘルプ（Help）] > [Threat Grid の概要（Introduction to Threat Grid）] > [Threat Grid クラウドとアプライアンスの比較（Threat Grid Cloud and Appliances Comparison）] を参照してください。）

- 多数の仮想マシンが実行されているときに [監督（Supervisor）] コンポーネントが失敗すると、大量の RAM ディスク ストレージが割り当てられたままになり、アプライアンスがリブートされるまでさらなる分析操作を実行できなくなることがありました。この問題が解決されました。

- クラスタリングのサポートに対し、多くの安定性向上策が実施されました。

- クラスタリングのステータスは、OpAdmin UI で表示されます。クラスタリング EFT に参加しているお客様は、スタンドアロンノードからクラスタを構築できます。既存のクラスタに空のデータベースを含む新しいアプライアンスを追加します。クラスタのステータスを確認します。クラスタがフォールトトレラントであるかどうかを確認します。デッド ノードを削除します。どのノードがフェールオーバーまたは移行イベント中にサービスの中断が発生する可能性のあるロールを保持しているか確認し、（可能な場合は）管理します。

既知の問題

- クラスタリング：システムが、UI の [削除（Remove）] オプションを使用して他のノードに削除を通知することなく不適切に削除およびワイプされると、そのシステムが再追加された場合、そのシステムに対するデータベースのミラーリングが失敗する可能性があります。
- NFS/クラスタリングの安全性：
  - 複数のクラスタ化されていないアプライアンス間、クラスタと 1 つ以上のクラスタ化されていないアプライアンスとの間、または複数の個別のクラスタの間で単一の NFS データストアを共有することをユーザが試行できなくするための安全機能は、まだアクティブではありません。
  - マニュアルまたはカスタマー サポートの明示的な指示に従い、既存のバックアップ ストアに関連付けられた暗号キーのみをインストールしてください。
- NFS：管理（OpAdmin）UI では、設定がアクティブ化された後に NFS 設定を変更することは、現在禁止されていません。このような変更を行うことは、特にノードがクラスタのメンバーである場合はサポートされていない操作です。この操作を実行すると、最大でデータ損失までの不規則な影響が発生します。

セキュリティ更新

この通常のリリースには、暫定リリース 2.4.0.1 で導入されたセキュリティ修正が引き続き含まれています。

バージョン 2.4.0.1

リリース日：2018 年 1 月 30 日

この暫定リリースでは、ClamAV が 0.99.3 に更新されています。この更新プログラムは、すぐにインストールすることを強くお勧めします。

修正と更新

- ウイルス定義が更新されなくなる可能性のあるファイル記述子のリークが対処されています。

セキュリティ更新

次の脆弱性が対処されています。

- CVE-2017-12374
- CVE-2017-12375
- CVE-2017-12376
- CVE-2017-12377
- CVE-2017-12378
- CVE-2017-12379
- CVE-2017-12380

バージョン 2.4

リリース日：2017 年 12 月 14 日

このリリースでは、コア Threat Grid ソフトウェアが更新されています。更新としてダウンロード可能なオプションの VM（個別にライセンス供与されたサードパーティ製ソフトウェアを搭載したものを含む）のサポートが追加されています。また、初期フィールド トライアルにご参加のお客様に向けたリリース前機能として、利用が制限されたクラスタリングのサポートが導入されています。

修正と更新

- クラウド ポータル リリース 3.4.57 に対応する新しいバージョンのコア Threat Grid ソフトウェアが使用されています（利用できる機能は、クラウド ソフトウェアとアプライアンス ソフトウェアの間で異なる場合があります。マニュアルを参照してください）。
- VM の配布では、新しい帯域幅効率の高いメカニズムが使用されます。これにより、複数の VM 間で共有されるコンテンツが複数回ダウンロードされることが回避され、さまざまな VM をさまざまな顧客に配布できるようになります。注：このメカニズムは、2.4.0 への更新のサポートに特化して作成された 2.3.x リリースにも存在します。
- 新しい VM である「win7-x64-2」が、すべてのお客様に利用可能になりました。
- 新しい VM である「win7-x64-kr」は、お客様のライセンスに Threat Grid アプライアンス上で Hancom Office を実行するライセンスを購入したことが示されている場合にダウンロードできます。その他のオプションの VM（ロケール固有の目的または用途のためのその他のサードパーティ製ライセンス ソフトウェアを含む）は、近い将来に利用できるようになる可能性があります。
- クラスタリング：複数アプライアンスのクラスタを構築するためのリリース前サポートが導入されました。これには追加のハードウェアが必要であり、現時点では、初期フィールド トライアルの参加資格があり、登録しているお客様のみが使用できます。

バージョン 2.3.3

リリース日：2017 年 11 月 30 日

このリリースでは、より効率的な更新システムが導入されています。新しい更新システムは、後続の仮想マシンのリリース間で変更されたコンポーネントのみをダウンロードし、複数の仮想マシン間で共有ソフトウェア コンポーネントが複数回ダウンロードされることを回避します。

必須項目：

後続の Threat Grid アプライアンス 2.4.0 リリースをダウンロードするには、このリリースのインストールが**必須**です。

修正と更新

- VM の配布では、帯域幅効率の高い新しいメカニズムが使用されます。これにより、複数の VM 間で共有されるコンテンツが複数回ダウンロードされることが回避され、さまざまな VM をさまざまな顧客に配布できるようになります。

バージョン 2.3.2

リリース日：2017 年 10 月 7 日

このリリースでは、バージョン 2.2 以降を実行している場合の、優先度の高い検索の問題に対処しています。検索機能および関連する API は、特定の日数を超えて追加されたデータを検索で評価すると、失敗することがありました（日付は、インデックス データ、つまり少なくとも 1 つのサンプル分析からのデータが含まれている場合にのみ、計算に含まれます）。

修正と更新

- 検索に使用されるインデックスは、効率性が向上し、より多くの日数（5 倍）の検索データがクエリ可能になるように移行されます（この上限は、今後の更新によってさらに引き上げられます）。
- ネットワーク上で取得されたライセンスの末尾に NUL 文字が付かないようになりました（このようなライセンスの有効性や有用性には影響しません）。
- 今後のまだリリースされていない機能をサポートするために、さまざまな更新が導入されました。

バージョン 2.3.1

リリース日：2017 年 8 月 28 日

このリリースでは、2.3.0 リリースにあった、以前のリリースから更新されたアプライアンスに影響を与えるいくつかの問題に対処しています。

修正と更新

- 2.1.4 以前に追加されたデータが一部の検索結果に含まれなくなる問題が解決されています。
- ソフトウェア バージョン 1.2.x で最初にインストールされ、1.4.x に直接アップグレードされたアプライアンスが 2.3.0 の更新を正常に適用できない問題が解決されています。
- [組織管理（Organizational Administration）] ページは、クラウド製品にのみ該当する組織レベルのライセンス設定を表示するのではなく、組織単位のレート制限の設定を正しく表示するように戻りました。

バージョン 2.3

リリース日：2017 年 8 月 11 日

このリリースでは、コア Threat Grid ソフトウェアが更新されています。クラウド製品でアクティブにテストおよびサポートされなくなった VM が削除されています。マルウェア トラフィックをトンネリングしないお客様のため、パフォーマンスの高いネットワーク実装に移行しました。SMTP トラフィックのハニーポットが実装されています。また、マルウェアからの発信 SSH がブロックされるようになりました（この方法で、クラウド サービスの動作と同様になりました）。さらに、ライセンスの自動取得が導入されています。アプライアンスがインターネットに接続している場合は、ライセンスの取得（または期限切れのライセンスの交換）をネットワーク経由で試行できます。自動取得は、現時点（2017 年 8 月 11 日）ではこのソフトウェアのリリース後に販売または更新されたライセンスでのみ使用できます。

IPv4LL（169.254.0.0/16）アドレス範囲の使用は、これまでテストおよびサポートされたことがありませんが、現在は「明示的にサポートされていない」ため、使用しないでください。

修正と更新

- クラウド ポータル リリース 3.4.47 に対応する新しいバージョンのコア Threat Grid ソフトウェアが使用されています（使用可能な機能は、クラウド ソフトウェアとアプライアンス ソフトウェアの間で異なる場合があります。詳細については、UI ヘルプに掲載されているポータルのリリース ノートを参照してください）。
- クラウド製品の一部としてアクティブにテストおよび維持されていない VM が削除されました。Windows XP は、以前にグランドファザリングしていたアプライアンスからも含め、削除されました。Windows 7 は 64 ビットのみとなりました。
- 「winxp」または「win7-x86」VM に送信されるサンプルは引き続き使用できます。「winxp」をハードコーディングしたスクリプトまたはクライアントは、変更する必要があります。
- トンネリングが使用されている場合を除き、マルウェアからの発信ネットワーク トラフィックには、仮想マシンからの出力に対して高パフォーマンスのメカニズムが使用されます。これにより、暗号化されていない発信 SMTP をアプライアンスに対してローカルにサンドボックス化できます。
- サンドボックス化された VM からの発信 SSH はブロックされるようになっています。
- タイム サーバの DNS ルックアップが失敗したために NTP が同期に失敗することがある状況が対処されました。NTP サービスは、ピアが存在しない場合、定期的に再起動されます。

バージョン 2.2.4

リリース日：2017 年 7 月 10 日

このリリースでは、次のバックアップ機能が導入されました。

Threat Grid アプライアンスで、NFS 対応のストレージへの暗号化されたバックアップ、ストレージのデータの初期化、およびバックアップをロードするための空のデータベース状態へのリセットがサポートされるようになりました。

（ここでのリセット機能は、アプライアンスを情報漏えいなく顧客構内へ出荷できるように使用されるワイプ プロセスとは異なります。その目的に適したワイプ プロセスはすでに回復ブートローダに存在しますが、システムのバックアップ復元には適していません。バックアップにはリセット機能が適切です。）

バックアップの機能に関する詳細ドキュメントを入手できます。使用する前によくお読みいただくことを強くお勧めします。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。

修正と更新

- お客様提供の NFSv4 ストアのバックアップおよび復元がサポートされるようになりました。
- システムによるバックアップの復元を準備するために、限られたデータ リセット操作が使用可能になりました（リセット操作はデータベースのコンテンツに適用されますが、リカバリ モードで使用可能なセキュアなワイプ オプションとは異なり、アプライアンスが永続的に使用できなくなることはありません）。
- DHCP が使用中の場合、またはネットワーク インターフェイスがブート後にホットプラグまたは再設定された場合にネットワーク トラフィックがローカル ネットワーク（ゲートウェイ以外）にルーティングされなくなる、2.2.2 で導入されたリグレッションが修正されました。

バージョン 2.2.3

リリース日：2017 年 5 月 19 日

2017 年 7 月 1 日以降に製造された Threat Grid アプライアンスには、Microsoft 要件に準拠した Windows XP のライセンスまたは配布が含まれていません。このマイナー リリースには、Windows XP なしで実行する新しい工場出荷時のインストールが使用できます。

このリリースをインストールしても、Windows XP は、それが以前に使用可能だったアプライアンスから削除されません。

これにより、クリーン インターフェイスに関連付けられた DNS サーバが設定されていない場合に、正常な更新チェックが失敗として OpAdmin で報告される原因となっていたいくつかの問題も修正されています。なお、[更新の実行（Run Update）] ボタンが表示されている場合は、「更新チェックエラー（Update Check Error）」通知が表示されている場合「であっても」、更新を安全に試行できます。

重要

2.2 より前のリリースからアップグレードする場合は、次の場所にあるアプライアンス 2.2 のリリース ノートを参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf

修正と更新

- 作成された実行可能ファイルがホワイトリストに登録されている場合は、[ドキュメントが実行可能ファイルを作成しました（Document Created a Executable File）] インジケータがトリガーされなくなります。
- クリーン ネットワーク DNS サーバが設定されていない場合に、モニタリング サービスおよびロギング サービス（kiries および syslog-ng）が適切に開始されるようになりました。
- 更新チェックの成功が、そのチェックに関する通知を送信できなかった場合でも、OpAdmin で正しく報告されるようになりました。
- Microsoft のライセンス要件に従い、このバージョンの Threat Grid アプライアンスは Windows XP なしでインストールできます。

セキュリティ更新

OpenSSL が 1.0.2k に更新されました。

バージョン 2.2.2

リリース日：2017 年 5 月 8 日

このマイナー リリースでは、今後のリリースで追加される機能をサポートするため、ネットワーク構成およびオペレーティング システムのコンポーネントが変更されています。これにより、TLS ハンドシェイクが成功せずに接続が確立されると、サーバをサポートするすべての接続が（サービスが再起動されるまで）失敗する原因となっていたサポート モードのバグと、新しいウイルス対策シグニチャのダウンロードおよびインストールができなくなる原因となっていたバグが修正されました。

重要

2.2 より前のリリースからアップグレードする場合は、アプライアンス 2.2 のリリース ノート（http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf）を参照してください。

バグ修正

- サポート モードが TLS ハンドシェイクの中断後に動作不能になることがなくなりました。
- 新しいウイルス対策シグニチャがダウンロードされなくなる問題が修正されました。
- 孤立したインテーク キュー要素が自動的にクリーンアップされるようになりました。

拡張機能

DNS サーバが DHCP 経由でクリーン インターフェイスで提供され、OpAdmin 経由で同じインターフェイスに設定されている場合は、両方が使用されるようになりました。

バージョン 2.2.1

リリース日：2017 年 3 月 24 日

重要

バージョン 2.1.5 で導入され、2.1.6 でも使用可能で機能している ElasticSearch の移行が完了していない場合、2.2.x をインストールしないでください。ご質問については、次の電子メール アドレスでカスタマー サポートにお問い合わせください。

support@threatgrid.com

このマイナー リリースでは、時間の経過とともに深刻になる可能性がある 2.2 のパフォーマンスの問題を修正しました。これにより、2.1.5 および 2.1.6 での ElasticSearch の移行を完全に完了させずに 2.2 をインストールした場合の影響が部分的に軽減されます。このリリースでは、長期にわたって非推奨となっていた SSLv3 のサポートも終了します。また、JVM ベースのサービスがメモリ不足状態から正常に回復できるようになりました。

2.2 より前のリリースからアップグレードする場合は、次の場所にある『Appliance 2.2 Release Notes』を参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf

新機能

アプライアンスは、2.1.5 および 2.1.6 での ES5 の移行を完全に完了させずに 2.2 シリーズのリリースがインストールされていた状態から回復できるようになりました。

これは部分的な軽減であることに注意してください。

この移行プロセスは、リリース 2.1.5 および 2.1.6 では整合性および可用性にまったく影響しませんが、2.2.x では、インデックスの移行の際に当該インデックスに追加された新しいコンテンツが、そのインデックスの移行プロセスの完了時に**失われる**可能性があります。したがって、2.1.5 または 2.1.6 での ElasticSearch の移行が**完全に完了**するまで 2.2.x をインストールしないことを**強く**推奨します。

バグ修正

特定の種類のネットワーク イベントを処理する分析プロセスで、時間およびメモリの過剰な消費がなくなり、分析サービスがクラッシュしないようになりました。

セキュリティ修正

SSLv3 は長期にわたって非推奨プロトコルとなっていましたが、不要になったため無効化されました。

バージョン 2.2 製造

リリース日：2017 年 3 月 8 日

製造時のみの変更。お客様への影響はありません。更新サーバ経由での導入は行われません。

バージョン 2.2

リリース日：2017 年 3 月 3 日

要件

2.2 をインストールする前に、2.1.5/2.1.6 での ElasticSearch の移行が**完了している必要があります。**

資料

『AMP Threat Grid Appliance Migration Note』および『Data Retention Note』を確認することが**強く**推奨されます。

- AMP Threat Grid Appliance Migration Note v2.2:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-migration-note-v2-2.pdf

- AMP Threat Grid Appliance Data Retention Note:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-data-retention-v2-2.pdf

このリリースについて

リリース 2.2 ではストレージの効率性が大幅に向上し、1.x リリースで当初インストールされていたシステムでは使用できなかったディスク容量を使用できます。

重要：

将来、この機能には最終的に古いコンテンツのプルーニング（削除）が実装されます。すべてのコンテンツが移行されますが、連続稼働するために、古いコンテンツ、特に非常に大量に生成されてもめったに使用されない分割されたディスクおよびネットワーク アーティファクトが継続的に削除される可能性があります。詳細については、上記のリンクの『*Data Retention Note*』を参照してください。

このリリースでは、Threat Grid アプライアンスは Threat Grid Cloud リリース 3.4.37 とバージョンが同等です（これは「機能」の完全な同等を意味するわけではありません。ハードウェア、サービス、サードパーティのライセンスが必要な機能、またはクラウドでのみ使用可能なその他のコンテンツや設備は、アプライアンスでも使用できない可能性があります）。

つまり、これまではクラウド専用であった一部のサードパーティ検出およびエンリッチメント サービスとの統合は、アプライアンス用に設定できるようになりました。これには VirusTotal、OpenDNS、および TitaniumCloud が含まれます。さらに、アプライアンスは ClamAV シグネチャに更新を日次で自動的にダウンロードできるため、既知のマルウェアの認識が向上します。

新機能

出荷されるアプリケーション バージョンには、次を含む多くの新しい機能があります。

- 配置更新サービス通知用に複数 URL の設定をサポートします。
- 従来のアーカイブ フォーマットで保存されたコンテンツは、より効率的な圧縮解除およびデータタイプごとのストレージ差別化を可能にするフォーマットに移行されます。
- VirusTotal、OpenDNS、および TitaniumCloud の統合は、アプライアンスで設定できるようになりました。
- ClamAV シグネチャは、毎日自動的に更新できます。これはデフォルトで有効ですが、OpAdmin の新たに追加された [統合（Integrations）] ページで無効にできます。
- 失敗したサンプル呼び出しを自動的に再試行できます。これにより、全体的な障害発生率が効果的に減少します。
- アプリケーション フロントエンドは、すべてのタイムスタンプを閲覧ブラウザのローカル タイムゾーンに変換します。結果として、アプライアンス自体の UTC 以外のタイムゾーンは不要になったため、維持されなくなりました。
- *Mask UI* : Threat Grid ポータルのバージョン 3.4.37 では、リリース 2.2 で初めてアプライアンスに導入された UI 強化を搭載します。

注：Mask は、レガシーの *Face* インターフェイスに代わるものですが、ユーザには切り替えオプションが用意されます。Mask では、分析レポートの完全な設計変更を含む、多くの機能強化が含まれています。詳細については、アプリケーションのオンライン ヘルプ ページから入手できる『Portal Release Notes』を参照してください（ポータルのページ上部にある UI ナビゲーション バーから、[ヘルプ（Help）] ボタンをクリックしてヘルプのメイン ページを開きます）。

バグ修正

- MBR パーティション テーブルの使用が原因で、元々 1.x リリースがインストールされていたアプライアンスではアクセスできなかったディスク領域が、割り当てられアクセス可能になりました。
- 1.x リリースからアップグレードされたシステムで、プライマリ ブートローダが破損または使用不可能な場合でも、リカバリ ブートローダを呼び出すことができるようになりました。

セキュリティ修正

- VGA ドライバの潜在的なバッファ オーバーフローに対処するように、基盤となる仮想化技術が更新されました。

バージョン 2.1.6

リリース日：2017 年 1 月 5 日

2.1.6 リリースでは、Threat Grid アプライアンス管理者のインターフェイスに LDAP 認証および認可を追加しました。また、未リリース/リリース予定の機能に関連するさまざまなアーキテクチャの改善が含まれています。

新機能

OpAdmin と TGSH ダイアログ インターフェイスの両方を LDAP 認証用に設定できます。これは、アプリケーション インターフェイスに拡張されるものではありません。

既知の問題

ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.1.5

リリース日：2016 年 11 月 21 日

このリリースでは、CSA API クエリのパフォーマンスが大幅に向上した結果、Cisco ESA および WSA デバイスとの統合の堅牢性とスピードが改善されています。また、堅牢性と将来性を考えてさまざまなバックエンド コンポーネントをアップグレードします。

重要：CSA API のパフォーマンスの向上は、本リリースのインストール後にバックグラウンドで実行される移行プロセスが完了した後でのみ見られることに注意してください。詳細については、このリリースに付属するテクニカル ノート（次のリンクから入手可能）を参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-migration-note-v2-1-5.pdf

新機能

コア アプリケーションは、1.x より新しい ElasticSearch バージョンをサポートするように変更されました。

1.7.x 以前のリリースに加えて、ElasticSearch バージョン 2.x と 5.x の両方がサポートされます（5.0 を使用する前に 2.0 への移行が必須です）。

PostgreSQL はバージョン 9.6.1 へアップグレードされます。

一時的な障害の後の自動回復が内部サービスの多くに拡張されます。

バグ修正

DHCP を介してアドレスを正常に取得する安全なネットワークで遅延が発生したときに、アップグレード時にサービスを正常に起動または再構成することが妨げられなくなりました。

ElasticSearch のタイムアウトを緩和して、ネイティブ 5.0 へのアップグレード前であっても障害の数が減少しました。

失敗およびロールバック済みであると誤ってマークされるというメジャーバージョン データベースのアップグレードにおける脆弱性が低下しました。

ElasticSearch に依存するアプリケーション コンポーネントは、ElasticSearch の初期化完了前に起動できなくなりました。

既知の問題

ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.1.4

リリース日：2016 年 9 月 5 日

このリリースでは、ハードウェア サポートに関連するさまざまな問題に関する問題、特にエアギャップ アプライアンスに対してソフトウェア アップデートのサポートを提供するための前提条件となる問題を解決します。

新機能

ElasticSearch サービスの負荷が過剰になっているシナリオで、モニタリングおよびレポートを利用できるようになりました。

バグ修正

失敗したサービスを自動的に再起動する機能のサポートが、一時的に無効になるのに十分な頻度で失敗するサービスにまで拡張されます（遅延後）。

redis 初期化の遅延が原因で内部サービスを起動できなかったシナリオが対処されました。

ストレージ デバイス名または ID の変更によって、システムが正常にブートしなくなることはなくなりました。

システム ワイプが TG-5004-K9 および TG-5504-K9 ハードウェアで完全にサポートされます。

既知の問題

ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.1.3

リリース日：2016 年 8 月 11 日

このリリースでは、ハードウェア サポートに関連するさまざまな問題に関する問題、特にエアギャップ アプライアンスに対してソフトウェア アップデートのサポートを提供するための前提条件となる問題を解決します。

新機能

ElasticSearch サービスの負荷が過剰になっているシナリオで、モニタリングおよびレポートを利用できるようになりました。

バグ修正

- 失敗したサービスを自動的に再起動する機能のサポートが、一時的に無効になるのに十分な頻度で失敗するサービスにまで拡張されます（遅延後）。
- redis 初期化の遅延が原因で内部サービスを起動できなかったシナリオが対処されました。
- ストレージ デバイス名または ID の変更によって、システムが正常にブートしなくなることはなくなりました。
- システム ワイプが TG-5004-K9 および TG-5504-K9 ハードウェアで完全にサポートされます。

既知の問題

ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.1.2

リリース日：2016 年 7 月 15 日

これは小規模なバグフィックス リリースです。

バグ修正

- クリーンでないシャットダウンにおいて、redis キー/値ストアがサービスの起動をブロックするようなシステム状態のままにすることがなくなりました。
- tg-tunnel への qemu 接続の回帰が解決されました（デフォルトでオフであるこの機能を使用する顧客向け）。
- tg-tunnel を使用しないようにシステムを変更するプロセスが自動化されました。

既知の問題

- 特定の BIOS リリースを搭載する TG-5004-K9 および TG-5504-K9 ハードウェアにおいて、ワイプ サポートが破損することが知られていました。この問題は、このハードウェアのリリース前に解決される予定です。
- ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.1.1

リリース日：2016 年 7 月 6 日

このリリースでは、クリーン ネットワーク DNS の分離機能のサポートにおける問題に対処し、重要なセキュリティ バグを解決し、さまざまなマイナー修正や改善が提供されます。

新機能

- 潜在的なハード ドライブ障害に関する SMART 警告について、ユーザが可視性設定を変更することでサイレント化できます。これにより、エラーの特性やステータスが変更されない限り、同じエラーがそれ以上通知されないようにします。

バグ修正

- クリーンネットワーク DNS の分離が正しく機能するようになりました。
- 再設定後のバックアップにおける偽警告が回避されます。

セキュリティ修正

- CVE-2016-1443 が対処されます。
- SSH はリカバリ モードではデフォルトで有効にならなくなりました。

既知の問題

- 特定の BIOS リリースを搭載する TG-5004-K9 および TG-5504-K9 ハードウェアにおいて、ワイプ サポートが破損することが知られていました。この問題は、このハードウェアのリリース前に解決される予定です。
- ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.1

リリース日：2016 年 6 月 21 日

重要：この更新の開始点は v2.0.4 です。バージョン 2.1 に更新するには、バージョン 2.0.4 になっている必要があります。

このリリースでは、リリース予定のハードウェア リビジョンを完全にサポートし、多数のセキュリティ強化を統合し、Threat Grid ポータル製品のコンテンポラリ リリースに移行します。

新機能

- ファイル タイプ `js`、`dot`、`dotx`、および `dotm` を配置更新サービス経由で FireAMP Private Cloud に悪意ありとして送信できるようになりました。
- すべてのハードウェアで、モジュールのロードと kexec がランタイムで無効になることで、カーネル ベースのルートキットに対する脅威を軽減し、オペレーティング システムのカーネルと initrd の署名が呼び出し前にブートローダによって検証されます。
- ハード ドライブの SMART 警告に関連したサービス通知を、コンテンツを変更している場合にのみ通知を自動的に再オープンできるような方法で非表示にできます。
- 長期間中開いたままになっているデータベース トランザクションが検出され、サービス通知として報告されます。これにより、修正のダウンタイムが長時間必要になるほど深刻になる前に修復できます。

バグ修正

- Glovebox の信頼性が大幅に向上しました。
- ネットワーク インターフェイスが使用可能になるまでに長時間必要となるようなシナリオで、リカバリ モードにおけるネットワークの信頼性が向上しました。
- IPMI からのハードウェア エラーに関連するサービス通知で、アクティブな警告数が 0 であると誤って主張されることがありました。
- システム設定が完了する前に、NTP 障害でサービス通知が発生しなくなりました。
- ブート後少なくとも 10 分が経過するまで、期待されるサービスがアクティブでないために発生する障害はログに記録できません。これにより、サービスが正しく初期化するための時間を得られます。

セキュリティ修正

- VGA ドライバの潜在的なバッファ オーバーフローに対処するように、基盤となる仮想化技術が更新されました。

既知の問題

- 特定の BIOS リリースを搭載する TG-5004-K9 および TG-5504-K9 ハードウェアにおいて、ワイプ サポートが破損することが知られていました。この問題は、このハードウェアのリリース前に解決される予定です。
- ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.0.4

リリース日：2016 年 5 月 1 日

重要：この更新の開始点は v1.4.6 です。2.0.4 更新を完了する前に、バージョン 1.4.6 になっている必要があります。

このリリースには、多数の信頼性の改善やバグフィックスが含まれています。

特に大量のデータを扱うアプライアンスでは、ブート時間が遅くなることがあります。ただし、ブート時間の拡大によって、ブート直後に発生する可能性のあるいくつかの障害が解決されます。

新機能

- 電子メール アラート用に作成される SMTP 接続において、ローカルで設定された認証局を利用できるようになりました。
- 配置更新サービス統合が向上し、FireAMP Private Cloud リリース 2.2.0 に完全に対応します。

バグ修正

- アプライアンスで配置インデックスが更新され、意図した状態に一致するようになりました。これにより、整合性がなかったり古かったりする古いインデックス状態によって発生する可能性のある、顧客に影響を与えるいくつかのバグが修正されました。
- アプライアンスは、従属サービスを開始する前に、ElasticSearch クラスタが完全に使用できるようになるまで待機します。
- ElasticSearch に割り当てられるメモリの量が向上し、その結果、ElasticSearch でエラーなしにインデックス化できるデータの最大有効量が向上しました。
- 一時的なブートローダ設定のオーバーライド（1.x から 2.x へのアップグレード中に発生するオーバーライドなど）がクリアされます。その結果、以前に 1.x リリースからアップグレードしたアプライアンスで、リカバリ モードの使用中にアップグレード モードのメニューを表示するシナリオが解決されました。
- 電子メール アラートが失敗する可能性のあるバグが解決されてました。

バージョン 2.0.3

リリース日：2016 年 3 月 15 日

このポイント リリースでは、FireAMP Private Cloud デバイス統合をサポートするために多くの機能が導入されました。これには、クリーン インターフェイスとダーティ インターフェイス間で DNS を分離する機能、CA 管理、および FireAMP 統合設定が含まれます。

生成された SSL 証明書では CN が subjectAltName として複製されるようになりました。これにより、1 つ以上の subjectAltName が存在する場合に CN フィールドを無視する SSL クライアントとの非互換性が解決されます。そのようなツールを使用している場合は、以前にアプライアンスが生成した証明書の再生成が必要になる可能性があります。

バージョン 2.0.2

リリース日：2016 年 2 月 18 日

このバグフィックス専用リリースでは、緊急のセキュリティ問題に対処します。

セキュリティ更新

GNU C ライブラリのパッチによって、CVE-2015-7547 および CVE-2015-1781 に対処します。

バージョン 2.0.1

リリース日：2016 年 2 月 12 日

このバグフィックス専用リリースでは、2.0 に存在するいくつかの問題を修正します。

バグ修正

デバイスのクォータ チェックの呼び出しがそのクォータに対して数えられなくなりました。

また、ブート時にアプライアンスがハングする可能性がある問題が解決されています。

既知の問題

ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

バージョン 2.0

リリース日：2016 年 2 月 11 日

重要：ここから 2.0.1 へ強制的に更新されます。

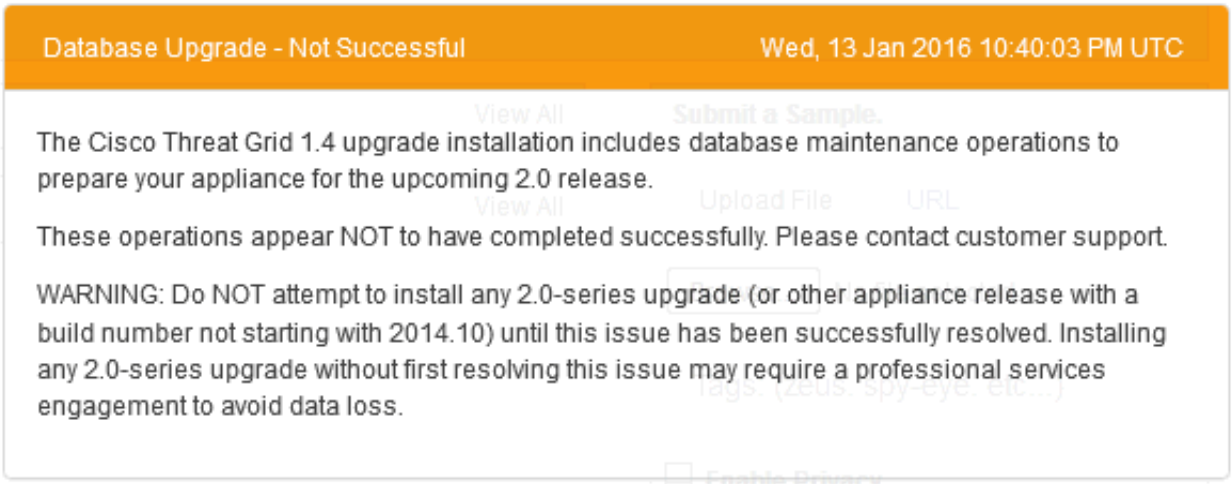
これはメジャー リリースで、更新されたオペレーティング システム上に構築されています。今後のハードウェア リリースをサポートする強化が含まれている他、Threat Grid Cloud Portal 製品と同じソフトウェアを使用できます。

大規模 ElasticSearch データベースがある場合、2.0 アップグレードには時間がかかることがあり、最大で数時間にもなります。

先に 1.4.6 アップグレードを完了し、その直後に 2.0 にアップグレードしてください。

完了前にアップグレードを中断しないでください。中断すると、サポート修復が必要になることがあります。進行中のアップグレードのステータスを確認する最適な方法は、コンソール アクセスを経由することです。

1.4.6 アップグレードが完了したら、2.0 にアップグレードする前に、次のエラーが発生したかどうか Threat Grid ポータルの通知を確認してください。



「データベースの更新に失敗しました（Database Upgrade - Not Successful）」通知

「データベースの更新に失敗しました（Database Upgrade - Not Successful）」メッセージは、新しいアプライアンスで、想定よりも古い PostgreSQL を実行していて、データベースの自動移行プロセスが失敗したことを意味します。

このエラー通知が表示されない場合は、2.0 へのアップグレードを進めることができます。

2.0 アップグレードに必要な時間

大規模 ElasticSearch データベースがある場合、2.0 アップグレードには時間がかかることがあり、最大で数時間にもなります。

完了前にアップグレードを中断しないでください。中断すると、サポート修復が必要になることがあります。進行中のアップグレードのステータスを確認する最適な方法は、コンソール アクセスを経由することです。

次の Threat Grid アプライアンス固有の更新も含まれています。

新機能

- Windows 7 の 64 ビット VM がサポートされるようになりました。
- カスタマー サポートによって開始されたトレースが自動的に周回して削除されるようになりました。そのため、使用可能なスペースを消費する危険なしに、長時間実行できます。
- 内部構成のバックアップは消費量が多くなりますが、両方の SSD で障害が発生した場合でも大規模なデータ損失なしでアプライアンスをリカバリできます。

バグ修正

- 未認証 SMTP は、空の方式リストで認証をアドバタイズするメール サーバ（特に Microsoft Exchange）相手でも正しく動作します。
- 毎晩の更新ダウンロード時に障害に関するサービス通知が正常に配信されるようになりました。

セキュリティ修正

- アカウントの作成または CSA デバイス（ESA、WSA など）の登録に関するアプリケーションレベル通知が通知アラート用に設定された最初の電子メール アドレスに送信されます。アドレスが設定されていない場合、通知は送信されません（以前のリリース バージョンではこのような通知が admin@test.threatgrid.com に送信されていましたが、データ漏えいが発生する可能性がありました）。
- OpenSSL がバージョン 1.0.2f に更新されました。

既知の問題

ディスク I/O スループット グラフには、顧客独自のデータではなく、オペレーティング システムの専用ファイルシステムに対する読み書きのみが含まれます。これは、I/O がまったく示されないことを意味します。起動が完了するとルート ファイルシステムとのやり取りが最小限になるようにシステムが構築されているためです。

今後のリリースではこの問題を解決するために、I/O 使用の決定方法が変更される可能性があります。

バージョン 1.4.6

リリース日：2016 年 1 月 27 日

リリース 1.4.6 は 2.0 へのアップグレード中に使用されるツールをインストールします。

新機能

リリース 1.4.6 のアプライアンスは、2.0 リリースへのアップグレードの対象となっています。

バージョン 1.4.5

2015/11/25

アプライアンス ワイプ機能は、1.4.4 とともに出荷されたデモ アプライアンスで機能するようになりました。詳細については、『Threat Grid Appliance Administrator's Guide』の「Wipe Appliance」セクションを参照してください。

バージョン 1.4.4

このリリースでは、ライセンス検証に影響する重大な問題を修正し、毎晩の更新確認におけるエラーがユーザに表示されなかったバグに対処します。

重要：1.4 以前のリリースからアップグレードする場合は、必ず後述するバージョン 1.4 のリリース ノートをお読みください。

バグ修正

- ライセンス検証で内部の読み取り専用データベースを再構築しようとしなくなりました（ライセンスが無効として誤って拒否されてしまう可能性がありました）。

- 毎晩の更新確認のエラーがユーザに正しく表示されるようになりました。

バージョン 1.4.3

このリリースには、基盤となる仮想化インフラストラクチャのマイナー セキュリティ アップデートが含まれています。また、アプライアンスのディスクをワイプするためのユーザ アクセス可能な機能が追加されました（借用したハードウェアの Cisco Demo Loan Program へのデコミッションまたは返却の場合）。

新機能

- **ワイプ：**Threat Grid アプライアンスのディスクをワイプできる新しいブート メニュー オプションを利用できます。この操作を実行すると、アプライアンスはシスコに返却されない限り稼働しなくなるので注意してください。

セキュリティ更新

- 計画されたイーサネット パケットを使用した潜在的なサービス妨害によって、実行中のサンプルがハングしていましたが、不可能になりました。

既知の問題

- まれな状況で、Windows XP 上の VM 分析が失敗すると認識されていました。これが発生すると、サンプル分析のビデオで黒画面が表示されます。この障害は個々のサンプルとは無関係です。発生した場合は、サンプルを再送信すること（または Windows 7 に切り替えること）が推奨されます。

バージョン 1.4.2

このリリースでは、製品で使用されている基盤となる仮想化技術を更新します。また、いくつかの小規模であるものの重要なバグフィックスがバンドルされています。

重要：1.4 以前のリリースからアップグレードする場合は、必ず後述するバージョン 1.4 のリリース ノートをお読みください。

バグ修正

- Flash（SWF）ドキュメントが正しく有効化されるようになりました。

- 「Glovebox」ツールのライブ サンプル分析実行の操作サポートは、Firefox 40 の新しいセキュリティ デフォルトと互換性を持つようになりました。

- [再生成（Regenerate）] ボタンは、SSL 証明書を生成します。この SSL 証明書は、以前に SSL 証明書を拒否していた一部のソフトウェアやツールで使用できるようになりました。

- Windows 7 仮想マシンは、実行中にハングしにくくなりました。

既知の問題

- まれな状況で、Windows XP 上の VM 分析が失敗すると認識されていました。これが発生すると、サンプル分析のビデオで黒画面が表示されます。この障害は個々のサンプルとは無関係です。発生した場合は、サンプルを再送信すること（または Windows 7 に切り替えること）が推奨されます。

バージョン 1.4.1

このリリースでは、製品に組み込まれている Windows 7 イメージを更新し、Microsoft Office のアクティベーション ダイアログを抑制します。

1.4 以前のリリースからのアップグレード

重要：1.4 以前のリリースからアップグレードする場合は、必ず後述するバージョン 1.4 のリリース ノートをお読みください。

バグ修正

- Windows 7 を使用して Microsoft Office ドキュメントを分析したときに、Microsoft Office のアクティベーション ダイアログが表示されなくなりました。

- 起動プロセスの早期段階でシステム動作の分析用カスタマー サポート ツールを使用しても、これらのツールがアクティブでないときはサービス通知が発生しなくなりました。

バージョン 1.4

このリリースでは、リリース予定の 2.0 リリースへのアップグレードを準備するために必要なストレージ フォーマットの変更に焦点が当てられています。

重要：

初期状態で 1.0 シリーズ ソフトウェアとともに出荷されていたアプライアンスで大量のデータベース コンテンツがあると、このアップグレードを適用するためのメンテナンス ウィンドウが通常よりも長時間必要になることがあります。

初期状態で 1.2 以前のソフトウェア リリース（数か月使用されていました）とともに出荷されていたアプライアンスの場合、アップグレードの適用に 90 分見積もることをお勧めします。

1.0 より前の（シスコ ブランドでない）デバイスから転送されたサンプル データがあるアプライアンスの場合、アップグレード プロセスの時間がさらにかかる可能性があります。ご質問はカスタマー サポートにお問い合わせください。

新機能

- 標準のアップストリーム データベース リリースと互換性がある PostgreSQL 9.4 の構成を使用するすべてのアプライアンスで、データベース ストレージをアップグレードします。

- tgsh-dialog に再度追加された [APPLY] ボタンに新機能：自己設定タスクおよび更新タスクをシステム更新後の場合と同様の方法で完了します。中断された更新試行の後で一貫性のない状態のままになっているシステムを修復するときに使用できます。

- 他のシスコ デバイスによってトリガーされるジョブに使用されるデフォルトの仮想マシンをカスタマー サポートが選択できる機能が追加されました。

バグ修正

- システムの書き込みパフォーマンスを低下している場合に、新しい仮想マシン イメージを含む更新が失敗しにくくなりました。

- コンソールから呼び出される更新ジョブが Opadmin で失敗したと誤って記述されにくくなりました。

- アップグレード プロセス中にサービス通知が作成されなくなりました。

- 一部の Microsoft Office ドキュメント タイプに対して生成されていた誤ったファイル名拡張子が修正されました。

バージョン 1.3

このリリースでは、リモート syslog サポート、システムレベルの問題の電子メール アラート、パフォーマンス グラフの可用性など、アプライアンス固有の機能が数多く追加されます。このリリースによって、Cisco FireSIGHT Management Center 製品との統合のサポートを実装する ThreatGRID サービスがわずかに新しいバージョンへと移行します。また、アプライアンス固有のバグフィックスも組み込まれています。

リモート syslog を設定している場合は、発信トラフィックにクリーン インターフェイスを使用してください。詳細については、1.3 の更新された管理ドキュメントを参照してください。

新機能

- システム モニタリング イベントでトリガーするように電子メール通知を設定できます。

- 管理インターフェイスの SSL 設定ページに追加されたボタンによって、新しい自己署名 SSL 証明書が生成されます。

- 時間経過に伴う CPU、I/O、およびメモリの使用状況に関するグラフを管理インターフェイスで利用できます。

- オペレーティング システム レベルのネットワーク インターフェイス名が、ドキュメントで使用されているように論理名（「clean」、「dirty」、「admin」）と一致するようになりました。

- ホットプラグ ネットワーク インターフェイスがサポートされます。インターフェイスを後で機能できるようにブート時にプラグインしておく必要がありません。ホットプラグ イベントで DHCP 更新を必要とするインターフェイスによって実行されます（SFP を必要とするインターフェイスは、これまでどおりブート時に SFP がインストールされる必要があります）。

- 失敗したサービスは自動的に再起動します。

- 失敗したサービスは、アプリケーションでサービス通知を生成します。

- NTP 同期時の失敗は、アプリケーションでサービス通知を生成します。

- 過剰なデータベース チェックポイント バックログによって、ユーザに認識可能な警告が発生します。

- 空き領域イベントのサービス通知が追加されました。

- アップグレードの可用性に関するサービス通知にリリース ノート コンテンツが追加されました。

バグ修正

- /24 を超える高ビットのネットマスクが途中で切り捨てられなくなりました。

セキュリティ更新

- qemu にパッチが適用され、CD-ROM ドライバ経由のエクスプロイトが無効になりました。CVE-2015-5154 を参照してください。

- アプリケーション デバッグ インターフェイス経由のローカル権限エスカレーションの機会が減少しました。

その他の注意事項

- EULA 条項が更新されました。

バージョン 1.2.1

ThreatGRID アプライアンスを更新し、クラウド サービスの新しいバージョンのソフトウェアに基づくようになります。他のシスコ アプライアンス（ESA および WSA アプライアンスを含む）との統合で、追加された機能間のキーがサポートされます。

このリリースで、アプライアンス固有のコードやインフラストラクチャは変更されていません。

新機能

- Cisco Sandboxing API のサポート

セキュリティ更新

- qemu にパッチが適用され、フロッピー コントローラのエミュレーションを無効にし、CVE-2015-3456 を回避します。

バージョン 1.2

このポイント リリースは、他のシスコ製品との統合を改善し、ソフトウェア アップデート プロセスを合理化し、ハードウェア モニタリング サポートを追加します。

新機能

- ソフトウェア アップデートのチェックは、バックグラウンドで毎晩自動的に実行されるようになりました。

- ソフトウェア アップデートが使用可能になると、通知は Threat Grid アプリケーション内で表示されます。

バグ修正

- 低速接続時にソフトウェア アップデートがタイムアウトしなくなりました。

- シャットダウン時またはリブート時に処理されているサンプルは、喪失、または重複として挿入されなくなりました。1.2 更新が適用されると、プロセスが適切な停止ポイントに達するまで、サンプル処理によりシャットダウンが遅延します。アプライアンスをブートして復帰すると、サンプル処理が再開します（これまでは、サンプル処理によって長時間のシステム シャットダウン遅延やサンプルの喪失が発生する可能性がありました。）。

- アプライアンスの起動中に、「502 Bad Gateway」エラーが発生しなくなりました。

- NTP（Network Time Protocol）同期が正常に実行されるようになりました。

- 生成された SSL 証明書のシリアル番号がすべてのアプライアンス間で一意になりました。注：この修正は、初期状態でバージョン 1.2 以降がインストールされているシステムにのみ影響します。

- 比較的少ない数のサンプルを処理した後でアプライアンスがディスク容量を使い果たしてしまうストレージの不要構成が修正されました。

- 監査ログでクライアントの IP アドレスを正しく示すようになりました。

- SSH キー設定ページのテキストが、root ではなく threatgrid ユーザのキーを設定するというように正しく反映されました。

- 生成された電子メールのパスワード リセット リンクが正しくなりました。

セキュリティ更新

- 管理インターフェイスのセッション Cookie が Threat Grid アプライアンス間で可搬ではなくなりました。

- アップストリーム修正を組み込むように OpenSSL がアップグレードされます。

その他の改善点

- 初期状態でバージョン 1.2 以降がインストールされているアプライアンスで、PostgreSQL データベースはアップストリーム PostgreSQL および関連プロジェクト（EnterpriseDB など）とバイナリ互換性のあるストレージ フォーマットを使用します。

既知の問題

- Windows 7 ジョブを実行する前に、次のユーザ介入が必要です。

1. admin ユーザとしてクリーン インターフェイス上のプライマリ ThreatGRID アプリケーション コンソールにログインします。2. 右上の [管理者としてログイン（Welcome Admin）] をクリックして、ドロップダウン メニューにアクセスします。3. [組織管理（Manage Orgs）] をクリックします。4. [初期組織（Initial Organization）] をクリックします。5. [追加 VMS（Additional VMS）] フィールドに、「win7」と入力します。6. [更新（Update）] をクリックします。

これが完了すると、サンプルを提出するときに [詳細オプション（Advanced Options）] の下で [win7] を選択できます。

- ライセンス解析はテキスト ファイル形式の影響を受けます。ライセンスは、UNIX テキスト ファイルで保存する必要があります。行区切りは CRLF ではなく CR を使用してください。

バージョン 1.1 ホットフィックス 1

ホットフィックス 1 は 1.1 と同一ですが、低速接続時の更新ダウンロードの信頼性に影響するバグも修正されています。

バージョン 1.1

このポイント リリースでは、Threat Grid アプライアンスに複数の新しい機能（Windows 7 サポートを含む）が追加され、複数のバグを修正します。

新機能

- Windows 7 サポートが追加されました。

- 「ダーティ」（つまりマルウェア）インターフェイス経由でアクセス可能なメール サーバのみを使用するのではなく、アプライアンスの「クリーン」ネットワークに接続されたメール サーバ経由で電子メールを送信できます。

- サポート スナップショットをアプライアンスから Threat Grid サポートに直接提出できます。

- サポート スナップショットを Threat Grid サポートに提出する前に確認できます。

- Web ベースの管理インターフェイス（OpAdmin）のみではなく、アップデートをテキストベースの（呪文のような）インターフェイスから適用できます。

- システム パスワードをリカバリ モードから正常に変更できます。

- 有効にするために再起動が要求される管理上の変更が少なくなりました。

- GUI 設定ワークフローで、クライアント側の Javascript 検証がさらに追加されました。

バグ修正

- アウトバウンド電子メール設定のさまざまな問題が解決されました。

- 管理インターフェイス内の通知が正しく表示されます。

- 構成 UI で長時間ジョブのステータスが最小限の遅延でストリーミングされるようになりました。

- 管理インターフェイスを起動できないことがあるケースを修正しました。

- 構成 GUI で、設定の変更を有効にするために再起動が必要かどうかについて、正確に反映していないことがありました。これが修正されました。

- tgsh-dialog（テキストベース）の管理インターフェイスからサポートされないメニュー項目が削除されました。

セキュリティ更新

- 既知の脆弱性（ntpd、bash、openssl）があるアップストリーム パッケージが更新されました。
- 構成バックアップが誰でも判読可能な形式で保存されなくなりました。

1.0+hotfix2 Update – 必須

1.0+hotfix2 は、破損なしに大きなファイルを処理できるように更新システム自体を修正する**必須の更新プログラム**です。