Threat Grid アプライアンス 管理者ガイド

バージョン：2.4.3、2.4.3.1、2.4.3.2、2.4.3.3

最終更新日：18/6/1

Cisco Systems, Inc. www.cisco.com

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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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とソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコ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、シスコおよびその供給者は、このマニュアルの使用または使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、あらゆる可能性がシスコ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。

シスコおよびシスコのロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標を示します。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という用語の使用はシスコ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。

表紙の写真：アーチーズ国立公園ビジター センターの上方高い尾根に咲いたサボテンの花。万全の防御を行い、持てる資源を最大限に活用し、過酷で厳しい環境でも花開く。Copyright © 2015 Mary C. Ecsedy. All rights reserved. Used with permission.

Cisco Threat Grid アプライアンス管理者ガイド

目次

目次 iii
図一覧 vii
はじめに 8
対象読者 8
はじめに 9
変更点 9
資料 9
2.4.3 ～ 2.4.3.3 の新機能 *9*
Threat Grid Appliance Release Notes *10*
Threat Grid Appliance Setup and Configuration Guide *10*
Threat Grid Portal のリリース ノート *10*
Threat Grid Portal のオンライン ヘルプと API マニュアル *10*
ESA/WSA アプライアンスのマニュアル *10*
ブラウザ 11
ライセンス 11
レート制限 *11*
前提条件 11
管理 12
電源オン 12
ログイン名およびパスワード：デフォルト 14
Threat Grid Portal UI 管理者 *14*
TGA 管理者：OpAdmin および threatgrid ユーザ *14*
CIMC（Cisco Integrated Management Controller） *14*
忘れたパスワードの回復 14
管理者パスワードのリセット *14*
更新プログラムのインストール 17
ビルド番号/バージョン ルックアップ テーブル *18*
ポートの更新 *21*
更新のトラブルシューティング *21*
サポート：Threat Grid へのアクセス 22
サポート対象のモード *22*
サポート サーバ *23*
サポート スナップショット *24*

設定管理 25
ネットワーク インターフェイスの設定管理 – TGSH ダイアログ 25
TGSH ダイアログ インターフェイスの設定方法 *25*
TGSH ダイアログへの再接続 *26*
リカバリ モードでのネットワークの設定 *26*
メイン設定管理 - OpAdmin Portal 27
SSH キー *28*
Syslog *28*
OpAdmin および TGSH ダイアログの LDAP 認証の設定 28
複数のアプライアンス管理者の追加 *29*
LDAP 認証の設定方法 *30*
サードパーティ検出とエンリッチメント サービスの設定 32
デフォルトで自動的に毎日更新される ClamAV シグネチャ *32*
再設定 33
DHCP の使用 33
DHCP の明示的 DNS *33*
ネットワーク構成と DHCP *34*
DHCP 設定の適用 *35*
SSL 証明書と Threat Grid アプライアンス 36
SSL を使用するインターフェイス 36
サポートされる SSL/TLS のバージョン 36
お客様提供の CA 証明書のサポート 36
SSL 証明書 - 自己署名デフォルト 36
インバウンド接続用の SSL 証明書の設定 37
CN 検証 *37*
SSL 証明書の置き換え *38*
SSL 証明書の再生成 *38*
SSL 証明書のダウンロード *39*
SSL 証明書のアップロード *39*
独自の SSL 証明書の生成 - OpenSSL を使用した例 *39*
アウトバウンド接続用の SSL 証明書の設定 40
DNS の設定 *40*
CA 証明書管理 *41*
配置更新サービス管理 *41*
ESA/WSA アプライアンスの Threat Grid アプライアンスへの接続 41
ESA/WSA のマニュアルへのリンク *42*

統合プロセスの概要 *42*
ESA/WSA の統合プロセスの手順 *43*
Cisco AMP for Endpoints プライベート クラウドへの Threat Grid アプライアンスの接続 47
配置更新の配信サービスの管理 53
Threat Grid 組織およびユーザの管理 55
新規組織の作成 55
ユーザの管理 56
Threat Grid アプライアンスの新しいデバイス ユーザ アカウントのアクティブ化 56
プライバシーとサンプルの可視性 58
統合のプライバシーと可視性 58
アプライアンスのワイプ 60
ワイプのオプション *62*
バックアップ 63
NFS 要件 63
バックアップ ストレージ要件 64
期待事項 64
バックアップ データの保持 65
バックアップ プロセスの概要 65
バックアップ頻度 *65*
バックアップの復元ターゲットとしての Threat Grid アプライアンスのリセット 66
バックアップの内容の復元 67
バックアップの復元に関する注記 *68*
バックアップに関連するサービスの通知 68
クラスタリング 71
目標 71
機能 71
制限事項 72
要件 72
ネットワーキングと NFS ストレージ 73
クラスタの構築の概要 74
Clust インターフェイスの設定 74

[クラスタリング（Clustering）] ページ 74
前提条件ステータスのクラスタリング *75*
コンポーネント ステータスのクラスタリング *76*
既存のスタンドアロン アプライアンスによるクラスタの開始 77
新しいアプライアンスを使用したクラスタの開始 86
クラスタへのアプライアンスの結合 88
条件のノードの指定 93
クラスタ ノードの削除 94
クラスタのサイズ変更 94
障害許容範囲 95
障害の回復 96
API/使用の特性 96
運用/管理の特性 96
ネットワーク終了設定 97
付録：OpAdmin メニュー 99
[設定（Configuration）] メニュー 99
[Operations] メニュー 100
[Status] メニュー 101
[Support] メニュー 102
索引 103

図一覧

図 1:起動時のシスコ画面 12
図 2:TGSH ダイアログ 13
図 3:ブート メニュー - リカバリ モード 15
図 4:リカバリ モードでの Threat Grid シェル 16
図 5:新しいパスワードの入力 16
図 6:アプライアンスのバージョン番号 17
図 7:OpAdmin がライブ サポート セッションを開始 23
図 8:LDAP 認証設定 30
図 9:LDAP のみ 31
図 10:システム パスワードまたは LDAP 31
図 11:統合設定 32
図 12:[今すぐ再設定(Reconfigure Now)] 33
図 13:TGSH ダイアログ(DHCP を使用するように設定されたネットワークに接続) 34
図 14:[SSL 証明書設定(SSL Certificate Configuration)] ページ 37
図 15:[配置更新の配信サービス(Disposition Update Syndication Service)] ページ 54
図 16:[ユーザの詳細(User Details)] ページ > [ユーザの再アクティブ化(Re-Activate User)] 56
図 17:Threat Grid アプライアンスでのプライバシーと可視性 59
図 18:アプライアンスのワイプ 60
図 19:ワイプ オプション 61
図 20:ワイプ終了 62
図 21:destroy-data REALLY_DESTROY_MY_DATA コマンドと引数 67
図 22:ネットワーク構成図のクラスタリング 73
図 23:Cisco UCS M4 C220 の Clust インターフェイスの設定 74
図 24:アクティブ クラスタのクラスタリング ページ 75
図 25:NFS の設定ページ: 78
図 26:[NFS 設定(NFS Configuration)] の [有効化(保留中のキー)(Enabled(Pendign Key))] 79
図 27:新しい NFS 暗号キーの生成 80
図 28:[NFS 設定(NFS Configuration)] のアクティブ化 81
図 29:NFS の [アクティブ(Active)] 82
図 30:NFS に対するすべてのデータのバックアップの開始 83
図 31:クラスタの開始 84
図 32:クラスタリング ステータス:[クラスタ化(Clustered)] 85
図 33:クラスタリングの設定ページ 87
図 34:クラスタリング ステータス:[クラスタ化(Clustered)] 88
図 35:クラスタを結合するための NFS 89
図 36:NFS 暗号キーのアップロード 90
図 37:アプライアンスの結合の NFS 暗号キーの有効化 91
図 38:クラスタの結合 92
図 39:アクティブ、正常、3 ノードのクラスタ 93
図 40:障害許容範囲表 95
図 41:[Network Exit 設定(Network Exit Configuration)] 97
図 42:[Network Exit ローカリゼーション(Network Exit Localization)] オプション 98
図 43:OpAdmin の [設定(Configuration)] メニュー 99
図 44:OpAdmin の [運用(Operations)] メニュー 100
図 45:OpAdmin の [ステータス(Status)] メニュー 101
図 46:OpAdmin の [サポート(Support)] メニュー 102

はじめに

Cisco Threat Grid アプライアンス（「TGA」）は、UCS サーバ プラットフォーム（UCS C220-M3 または UCS C220 M4）、またはサーバ クラスタに基づくスタンドアロン デバイスで、事前にインストールされている Threat Grid のマルウェア分析プラットフォームで販売されます。

Threat Grid アプライアンスは、高度なマルウェアの分析によって脅威の詳細な分析およびコンテンツを提供する、安全できわめてセキュアなオンプレミス環境を実現します。

銀行、保険会社、医療サービスなどの、機密データを扱う多くの組織では、さまざまな法規制の遵守ルールやポリシー制限などのガイドラインに従う必要があります。こうした規制により、マルウェア アーティファクトなど特定のタイプのファイルは、マルウェア分析のためにネットワーク外部に送信することが禁止されています。Threat Grid アプライアンスをオンプレミスで維持することにより、これらの組織はネットワークから出ることなく、疑わしいドキュメントとファイルをアプライアンスに送信して分析できるようになります。

Threat Grid アプライアンスを使用することで、セキュリティ チームは非常にセキュアな独自の静的および動的分析テクニックを使用し、すべてのサンプルを分析できるようになります。アプライアンスでは、分析結果を数億もの分析済みマルウェア アーティファクトと関連付け、マルウェア攻撃、キャンペーン、およびその配布状況をグローバルに把握できるようにします。

観測された 1 つの活動/特性サンプルを他の数百万ものサンプルとすみやかに関連付け、比較することで、過去の履歴やグローバルなコンテキストに照らして、その動作を十分に理解できます。この機能は、高度なマルウェアからの脅威と攻撃に対して、セキュリティ チームが効果的に組織を守るために役立ちます。

対象読者

このマニュアルは TGA 管理者ガイドです。本書は、Threat Grid アプライアンスを新たに導入する方法、およびアプライアンスを管理してマルウェア分析を最適化する方法について説明します。また、Threat Grid アプライアンスと、ESA や WSA アプライアンス、AMP for Endpoints プライベート クラウド デバイスなどの他のシスコ製品やサービスとの統合を担当する管理者にも情報を提供します。

Threat Grid アプライアンスのセットアップと設定の詳細については、Threat Grid アプライアンス製品のドキュメント ページで『*Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

はじめに

Cisco Threat Grid アプライアンスは、サンプルを分析するために必要なすべてのコンポーネントが出荷前にあらかじめインストールされた Linux サーバです。新しいアプライアンスを受け取ったら、まずオンプレミス ネットワーク環境に合わせてセットアップおよび設定する必要があります。

サーバが稼働中になってからは、Threat Grid アプライアンス管理者が、Threat Grid マルウェア分析ツールを使用する組織とユーザの管理、アプライアンスの更新、バックアップ、その他のサーバ管理タスクの実行を担当します。

変更点

最新の機能とセキュリティ アップデートを確実にインストールするため、アプライアンスは更新してから使用することを推奨します。

「*更新のインストール*」の項で説明している手順に従って、新しいリリース更新プログラムの有無を確認し、インストールします。

資料

Threat Grid アプライアンスのマニュアル（このドキュメント、『*Threat Grid Appliance Setup and Configuration Guide*』、書式設定されたバージョンのリリース ノート、統合ガイドなどを含む）は、Cisco.com の Web サイトの内部リソース ページ（*Threat Grid アプライアンス製品のドキュメント ページ*）で入手できます。このページには、現在と過去のアプライアンス リリースに関するマニュアルへのリンクが掲載されています。

2.4.3 ～ 2.4.3.3 の新機能

このガイドの主な変更点を、次の表に一覧表示しています。

セクション見出し	ページ	変更点
クラスタリング	71	「条件」ノードの説明が更新されました。
前提条件ステータスのクラスタリング	75	新規セクション
既存のスタンドアロン アプライアンスによるクラスタの開始	77	NFS にバックアップしたデータベースを使用したスタンドアロン アプライアンスに関するメモが追加されました。
ネットワーク終了設定	97	新規セクション。リモート終了サポートが使用可能になり、`tg-tunnel` が置換されました。
OpAdmin の [設定（Configuration）] メニュー	99	**ネットワーク終了**が追加されました。

Threat Grid Appliance Release Notes

[OpAdmin Portal] > [運用（Operations）] > [アプライアンスの更新（Update Appliance）] > [リリースノート（Release Notes）]

注：書式設定された PDF 版の『Threat Grid Appliance Release Notes』も「**Install and Upgrade Guides**」ページから入手できます。

Threat Grid Appliance Setup and Configuration Guide

『*Threat Grid Appliance Setup and Configuration Guide*』は最新のマニュアルに付属しています。これには、ネットワーク インターフェイス、推奨するファイアウォール ルール、ネットワーク構成図、設定手順、その他のタスクを含む設定の詳細情報が記載されています。

Threat Grid Portal のリリース ノート

Portal UI のナビゲーション バー > [ヘルプ（Help）] > [リリースノート（Release Notes）]

Threat Grid Portal のオンライン ヘルプと API マニュアル

Threat Grid Portal の「*Using Threat Grid*」オンライン ヘルプ、API マニュアル、およびその他の情報は、Threat Grid Portal ヘルプのメイン ページから入手できます。

Threat Grid Portal ユーザ インターフェイス > ナビゲーション バー > [Help]

マニュアルへのリンクを含む、「**Help**」ホーム ページが開きます。

ESA/WSA アプライアンスのマニュアル

Threat Grid アプライアンスと ESA または WSA アプライアンスを接続する方法の詳細については、*ESA/WSA アプライアンスの Threat Grid アプライアンスへの接続*を参照してください。

ご使用の ESA/WSA のオンライン ヘルプまたはユーザ ガイドの「*Enabling and Configuring File Reputation and Analysis Services*」の手順を参照してください。

- ESA ユーザ ガイドは次の場所にあります。
  https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
- WSA ユーザ ガイドは次の場所にあります。
  https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

ブラウザ

Threat Grid では、次のブラウザの使用を推奨しています。

- Chrome
- Firefox
- Safari

注：Microsoft Internet Explorer は推奨されておらず、サポート対象外です。

ライセンス

Threat Grid ライセンスは [OpAdmin 設定ライセンス（OpAdmin Configuration License）] ページで管理します。

[Configuration] > [License]

ライセンスについての質問がある場合は、support@threatgrid.com にお問い合わせください。

レート制限

API レート制限は、ライセンス契約条件に基づいてアプライアンス全体に適用されます。これは、API 送信にのみ影響し、手動でのサンプル送信には影響しません。

レート制限はカレンダー日ではなくローリング タイムの時間枠に基づきます。送信制限に達すると、次の API 送信の再試行まで待機する時間を通知するメッセージとともに、429 エラーが返されます。詳細については、「Threat Grid portal UI FAQ entry on rate limits」を参照してください。

前提条件

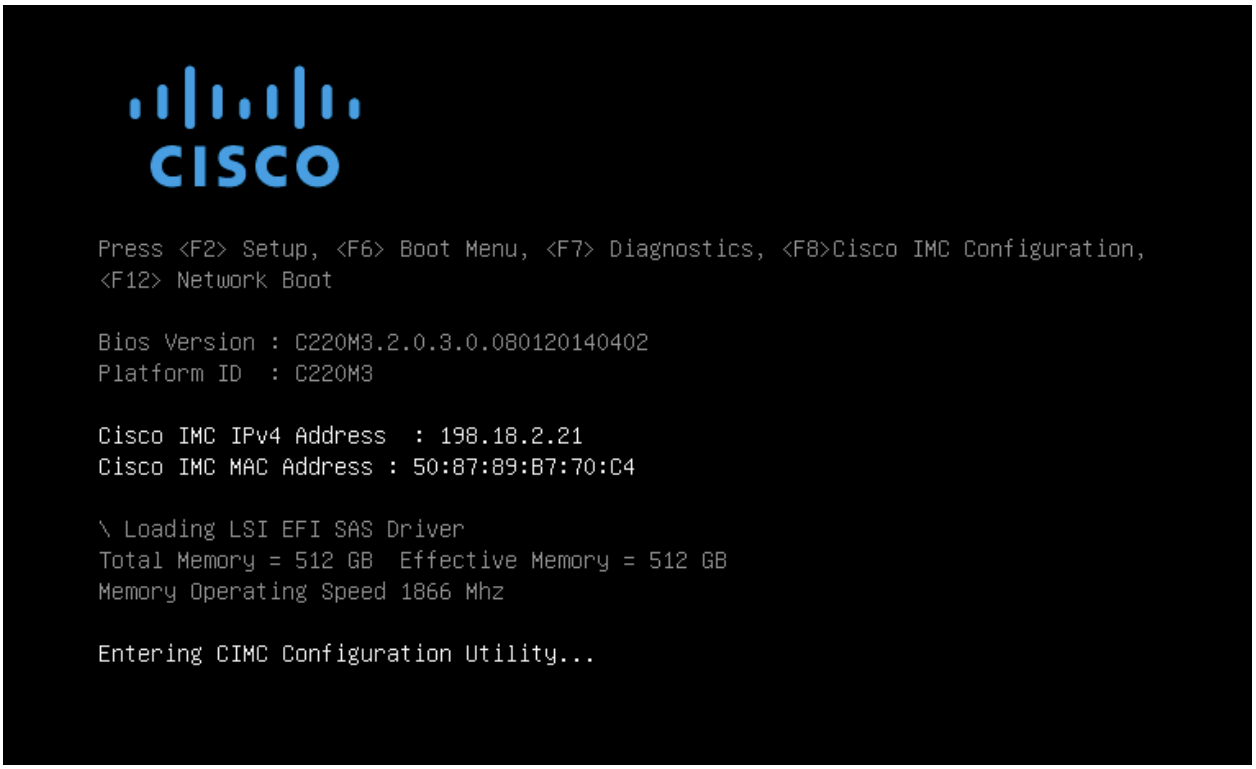
このガイドでは、『*Threat Grid Appliance Setup and Configuration Guide*』で説明されている手順に従って初期セットアップと設定が完了しており、マルウェア サンプルの初期テストが正常に送信され、分析されていることを前提としています。

管理

電源オン

アプライアンスの電源をオンにして、起動するまで待ちます。シスコの画面が一時的に表示されます。

図 1：起動時のシスコ画面

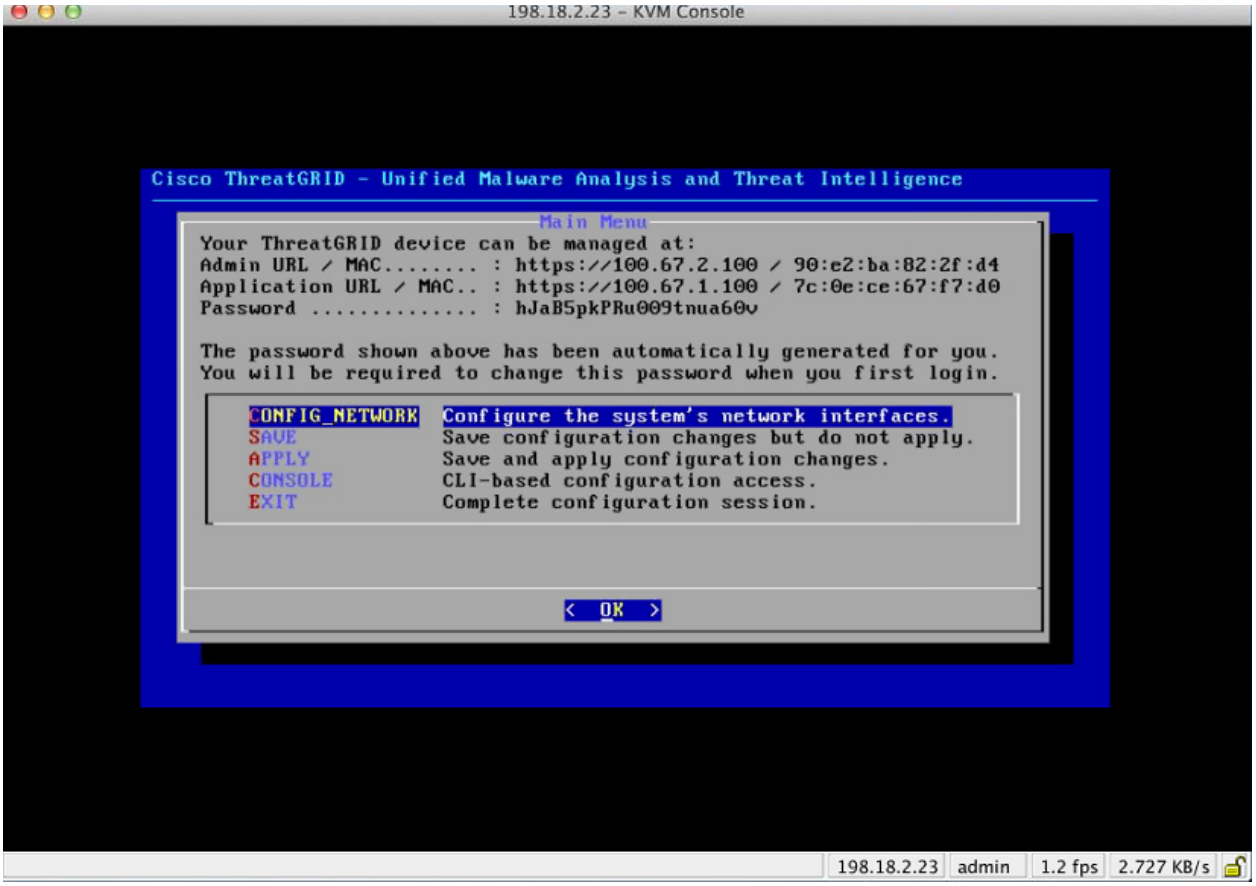


注：CIMC インターフェイスを設定するには、メモリ チェックが完了した後に、F8 を押します。

詳細については、『Threat Grid Appliance Setup and Configuration Guide』の「*Configuring CIMC*」の項を参照してください。

サーバ起動と接続が正常に終了すると、コンソールに **TGSH ダイアログ**が表示されます。

図 2：TGSH ダイアログ



注：TG アプライアンスがセットアップおよび設定された後は、TGSH ダイアログにパスワードが表示されなくなりますが、OpAdmin インターフェイスへのアクセスおよびその設定には、このパスワードが必要です。

パスワードを忘れた場合：このパスワードを忘れた場合の手順については、忘れたパスワードの回復を参照してください。

ログイン名およびパスワード：デフォルト

Threat Grid Portal UI 管理者

ログイン：「admin」

パスワード：　「changeme」

TGA 管理者：OpAdmin および threatgrid ユーザ

OpAdmin 管理者のパスワードは「threatgrid」ユーザのパスワードと同じです。これは OpAdmin インターフェイスで維持されます。デフォルトの管理者パスワードは初期 TGA 設定中に変更されるので、この手順が実行された後は読み取り可能テキストでは表示されなくなります。パスワードを忘れて、OpAdmin にログインできない場合は、下記の「**忘れたパスワードの回復**」の手順に従います。

CIMC（Cisco Integrated Management Controller）

ログイン：「admin」

パスワード：　「password」

忘れたパスワードの回復

デフォルトの管理者のパスワードは、初期のアプライアンス設定および構成時の TGSH ダイアログでのみ表示されます。初期設定が完了すると、パスワードは読み取り可能テキストで表示されなくなります。

注：LDAP 認証は、複数の管理者がいる場合、TGSH ダイアログと OpAdmin ログインに使用できます。アプライアンスに LDAP 認証のみが設定されている場合、リカバリ モードでパスワードをリセットすると、認証モードが再設定され、システム パスワードでもログインできるようになります。

管理者パスワードを忘れて、OpAdmin にログインできない場合は、次の手順を実行します。

管理者パスワードのリセット

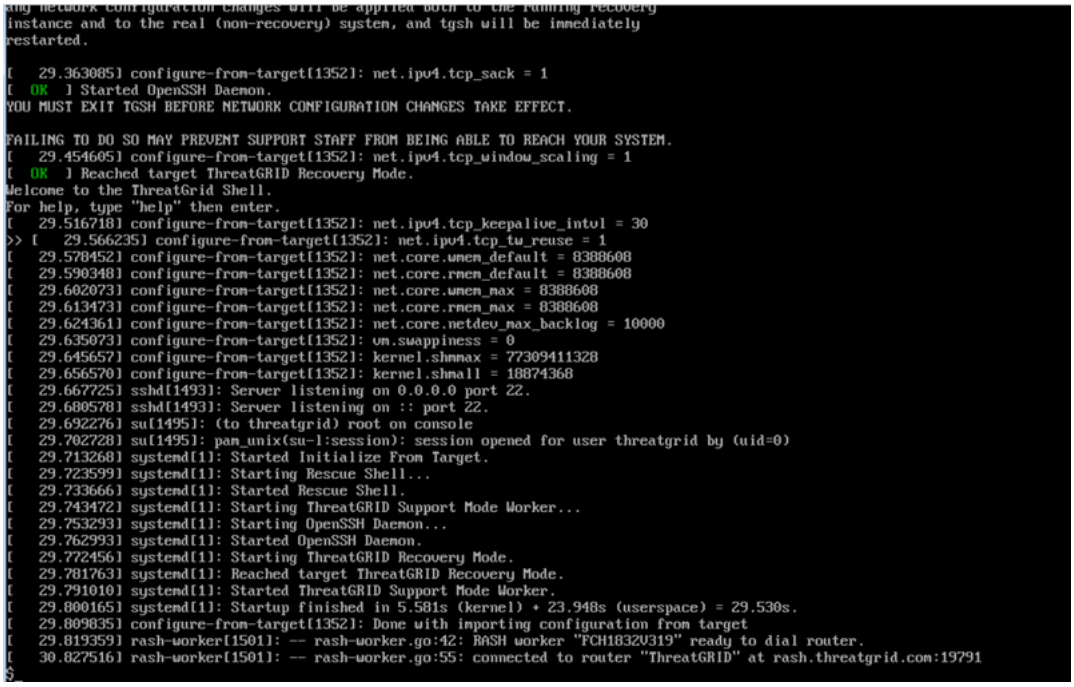
1. アプライアンスを再起動します。

   起動中、以下のように**リカバリ モード**を選択できるわずかな時間枠があります。

図 3：ブート メニュー - リカバリ モード

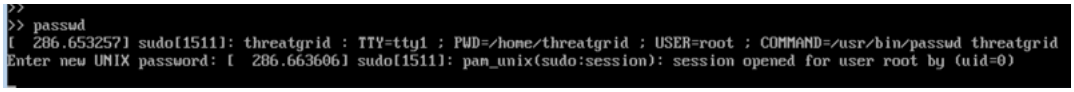
Threat Grid のシェルが開きます。

図 4：リカバリ モードでの Threat Grid シェル



2. `passwd` を実行して、パスワードを変更します。

図 5：新しいパスワードの入力



注：このモードではコマンド プロンプトが常に表示されるとは限りません。また、ロギング出力が任意の時点で入力の上に表示されることがあります。これは入力に影響を与えません。表示に関係なく入力を続けることができます。

3. ロギング出力の 2 行を無視します。パスワードを入力して Enter を押し、次にパスワードを再入力して Enter を再度押します。パスワードは表示されません。

4. 新しいパスワードを保存するために、コマンド ラインから `exit` と入力する**必要があります**。

   再起動では新しいパスワードは保存されません。`exit` を入力しないと、すべてが問題ないように見えても、パスワード変更は認識されずに廃棄されます。

5. 次に、`reboot` コマンドを入力し、Enter を押して、通常モードでアプライアンスを開始します。

更新プログラムのインストール

Threat Grid アプライアンスを新しいバージョンに更新するには、『*Threat Grid Appliance Setup and Configuration Guide*』の説明に従って、初期セットアップと設定の手順を実行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。

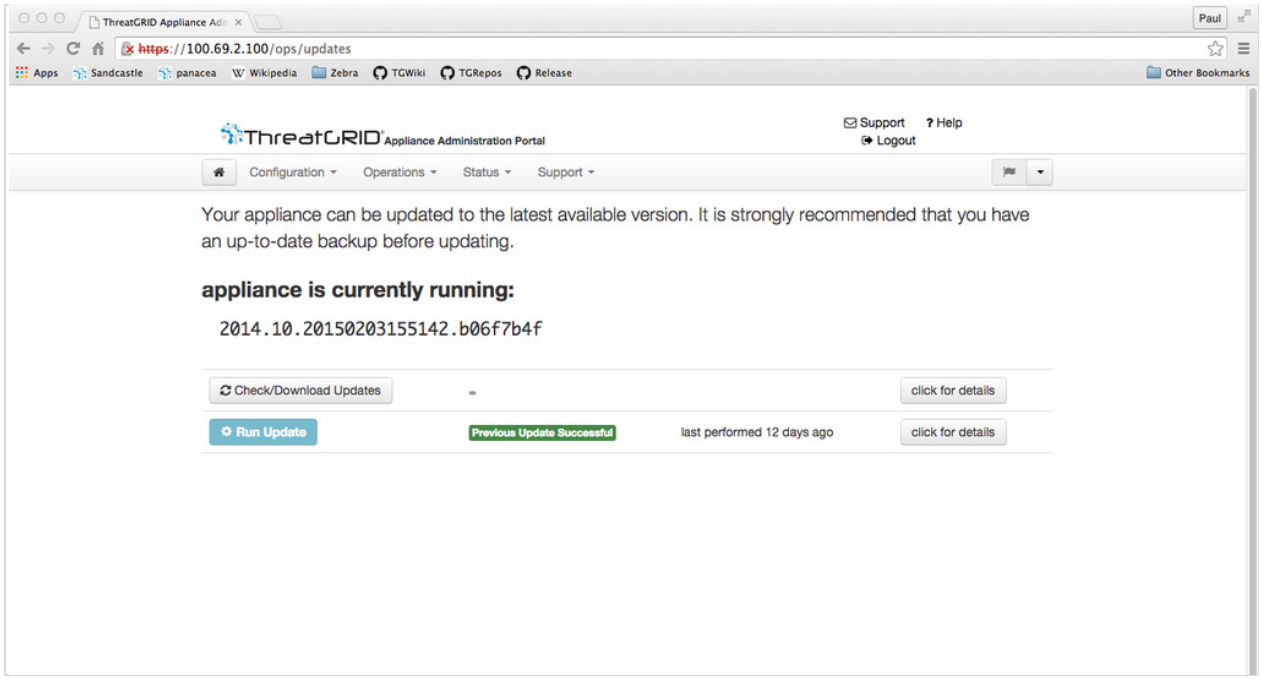
更新は一方向です。より新しいバージョンにアップグレードすると、以前のバージョンに戻すことはできません。

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。

1. [Operations] メニューの [Update Appliance] を選択します。

   *更新*ページが開き、アプライアンスの現在のビルドが表示されます。

図 6：アプライアンスのバージョン番号



2. [Check/Download Updates] をクリックします。アプライアンス ソフトウェアの最新の更新プログラム/バージョンがあるかどうかがソフトウェアによって確認され、存在する場合はダウンロードされます。

注：ダウンロードに時間がかかる場合があります。

- 1.0 から 1.0+hotfix2 への更新には約 15 分かかります。
- 1.0 から 1.3 への完全なアップデートの適用（データ移行なし）には約 30 分かかります。

3. 更新プログラムのダウンロードが完了したら、[Run Update] をクリックしてインストールします。

ビルド番号/バージョン ルックアップ テーブル

アプライアンスのビルド番号は、上記のように、[更新（Updates）] ページ（OpAdmin の [運用（Operations）] > [アプライアンスの更新（Update Appliance）]）で参照できます。

アプライアンスのビルド番号は、次のリリース バージョン番号に対応します。

ビルド番号	リリース バージョン	リリース日	注記
2017.12.20180601200650.e0c052b0.rel	2.4.3.3	2018/6/1	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	2018/5/19	CVE-2018-1000085 の ClamAV を更新バグ修正
2017.12.20180501005218.4e3746f4.rel	2.4.3.1	2018/5/1	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	2018/4/27	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	2018/3/2	クラスタリング
2017.12.20180219033153.bb5e549b.rel	2.4.1	2018/2/19	OpAdmin のクラスタリング サポート。ポータル ソフトウェアを 3.4.59 に更新。
2017.12.20180130110951.rel	2.4.0.1	2018/1/30	セキュリティ更新プログラムを ClamAV にのみ更新

ビルド番号	リリース バージョン	リリース日	注記
2017.12.20171214191003.4b7fea16.rel	2.4	2017/12/14	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	2017/11/30	2.4 アップグレードの開始点
2016.05.20171007215506.0700e1db.rel	2.3.2	2017/10/7	Elasticsearch シャード カウントの減少。
2016.05.20170828200941.e5eab0a6.rel	2.3.1	2017/8/28	バグ修正
2016.05.20170810212922.28c79852.rel	2.3	2017/8/11	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	2017/7/10	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	2017/5/20	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	2017/5/8	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	2017/3/24	SSLv3 の無効化、リソースの問題修正
2016.05.20170308211223.c92516ee.rel	2.2mfg	2017/3/8	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。

ビルド番号	リリース バージョン	リリース日	注記
2016.05.20170303034712.1b205359.rel	2.2	2017/3/3	ストレージ移行、プルーニング、Mask UI、複数処理の更新
2016.05.20170105200233.32f70432.rel	2.1.6	2017/1/5	LDAP 認証の追加
2016.05.20161121134140.489f130d.rel	2.1.5.	2016/11/21	Elasticsearch5、CSA パフォーマンス修正
2016.05.20160905202824.f7792890.rel	2.1.4	2016/9/5	基本的に製造に関係します。
2016.05.20160811044721.6af0fa61.rel	2.1.3	2016/8/11	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	2016/7/15	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	2016/7/6	
2016.05.20160621044600.092b23fc	2.1	2016/6/21	
2015.08.20160501161850.56631ccd	2.0.4	2016/5/1	2.1 更新の開始点。2.1 に更新するには、2.0.4 になっている必要があります。
2015.08.20160315165529.599f2056	2.0.3	2016/3/15	AMP 統合、CA 管理、分割 DNS を導入
2015.08.20160217173404.ec264f73	2.0.2	2016/2/18	
2015.08.20160211192648.7e3d2e3a	2.0(1)	2016/2/12	
2015.08.20160131061029.8b6bc1d6	2.0	2016/2/11	ここから 2.0.1 へ強制的に更新
2014.10.20160115122111.1f09cb5f	1.4.6 **注：**これは 2.0 アップグレードの開始点です。	2016/1/27	2.0.4 更新の開始点
2014.10.20151123133427.898f70c2	v1.4.5	2015/11/25	
2014.10.20151116154826.9af96403	v1.4.4		
2014.10.20151020111307.3f124cd2	v1.4.3		

ビルド番号	リリース バージョン	リリース日	注記
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		

ポートの更新

Threat Grid アプライアンスはポート 22 を使用して SSH でリリース更新プログラムをダウンロードします。

バージョン 1.1 以降のアプライアンスでは、次に説明するように、Web ベースの管理インターフェイス（OpAdmin）からだけではなく、テキスト（curses）インターフェイスからでもリリース更新プログラムを適用できるようになっています。

1.3 現在、DHCP を使用するシステムでは、明示的に DNS を指定する必要があります。それ以前は必要ありませんでした。DNS サーバを明示的に指定していないシステムの 1.3 へのアップグレードは失敗します。

更新のトラブルシューティング

「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が、サポートするバージョンより古いバージョンの PostgreSQL を実行していることを意味します。

これは、自動化されたデータベース移行プロセスが失敗したことを意味する重要な問題であり、2.0 にアップグレードする前に修正する必要があります。

詳細については、v2.0.1 のリリース ノートを参照してください。

サポート：Threat Grid へのアクセス

サポートが必要な場合、Threat Grid エンジニアにサポートを依頼するには、以下の方法があります。

E メール：問い合わせを記載して、support@threatgrid.com に電子メールを送信します。

[サポートへの問い合わせを開く（Open a Support Case）] 。サポート ケースをオープンするには、Cisco.com ID（または、この ID を生成すること）が必要です。また、注文の請求書に記載されているサービス契約番号も必要になります。Cisco Support Case Manager は https://mycase.cloudapps.cisco.com/case から開きます。

コール。シスコの連絡先情報：https://cisco.com/cisco/web/siteassets/contacts/index.html

Threat Grid のサポートを依頼する場合、依頼内容とともに次の情報を送信します。

アプライアンスのバージョン：[OpAdmin] > [Operations] > [Update Appliance]

完全なサービス ステータス（シェルから service status）

ネットワーク図または説明（該当する場合）

サポート モード（シェルまたは Web インターフェイス）

サポート要求の詳細

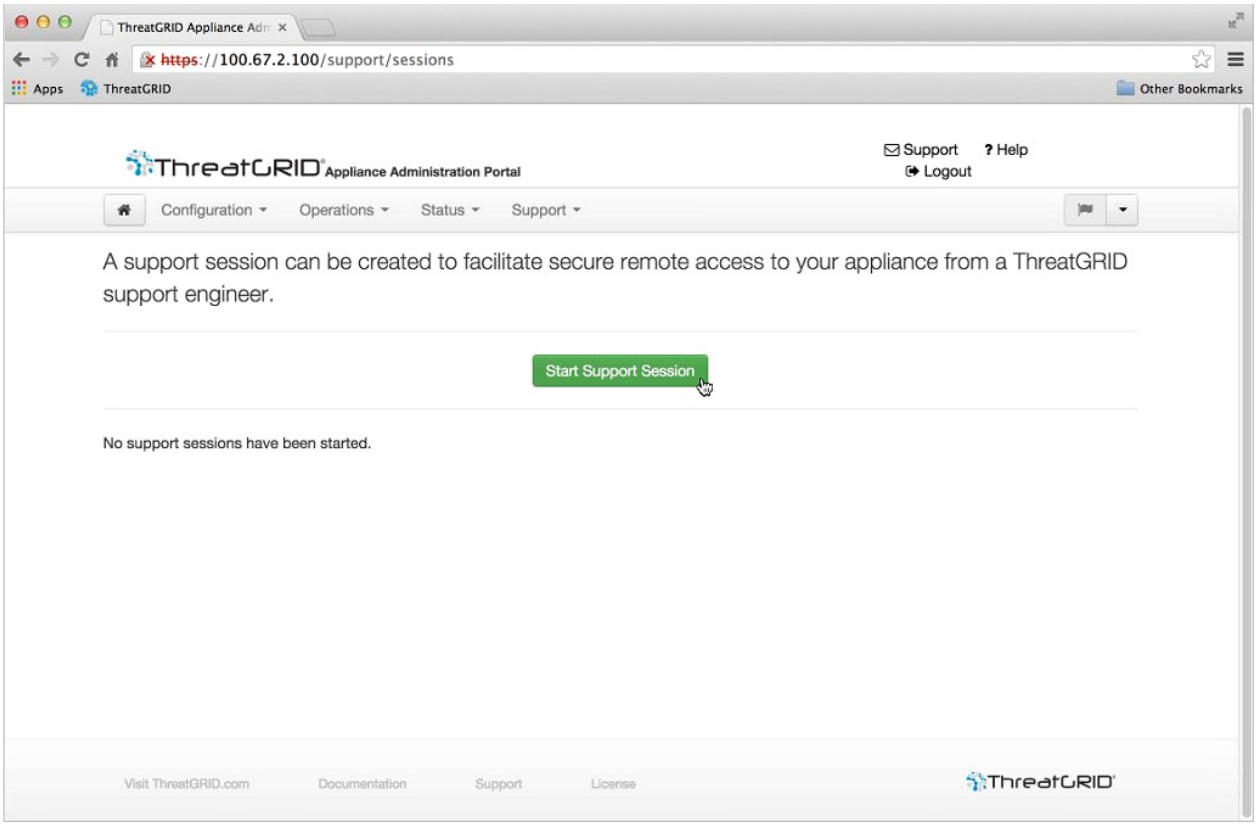
サポート対象のモード

Threat Grid のエンジニアからのサポートを必要とする場合、「サポート モード」を有効にするよう求められる場合があります。このモードは、ライブ サポート セッションであり、Threat Grid サポート エンジニアにアプライアンスへのリモートのアクセス権を付与します。アプライアンスの通常の動作には影響しません。これは、[OpAdmin ポータルサポート（OpAdmin Portal Support）] メニューから実行できます。（また、[サポートモード（SUPPORT MODE）] を、レガシーの Face Portal の UI から、およびリカバリ モードの起動時に、TGSH ダイアログから有効にすることができます。）

Threat Grid テクニカル サポートとのライブ サポート セッションを開始するには、次の手順を実行します。

OpAdmin で [Support] > [Live Support Session] の順に選択し、[Start Support Session] をクリックします。

図 7：OpAdmin がライブ サポート セッションを開始



サポート サーバ

サポート セッションを確立するには、TG アプライアンスが次のサーバに到達する必要があります。

support-snapshots.threatgrid.com

rash.threatgrid.com

アクティブなサポート セッション中のファイアウォールでは、両方のサーバが許可されている必要があります。

サポート スナップショット

サポート スナップショットは、基本的に実行中のシステムのスナップショットです。これには、ログ、PS 出力など、サポート スタッフによる問題のトラブルシューティングに役立つものが含まれます。

1. [Support] メニューから、[Support Snapshots] を選択します。
2. スナップショットを取得します。
3. スナップショットを取得すると、自分で.tar .gz としてダウンロードすることができます。または、[Submit] を押して、Threat Grid スナップショット サーバにスナップショットを自動的にアップロードできます。

設定管理

Threat Grid アプライアンスの初期設定は、『*Threat Grid Appliance Setup and Configuration Guide*』で説明されている手順に従って、アプライアンス設定時に行われています。

Threat Grid アプライアンス設定は **TGSH ダイアログ**と **OpAdmin Portal** インターフェイスで管理します。

Threat Grid 組織およびユーザ アカウントは、Threat Grid Portal UI 経由で（ナビゲーション バーのログイン名の隣にあるドロップダウンの矢印から）管理します。

TGSH ダイアログと OpAdmin 設定タスクについては、以降の項で詳しく説明します。

ネットワーク インターフェイスの設定管理 – TGSH ダイアログ

TGSH ダイアログ インターフェイスは、主に以下の管理に使用します。

- ネットワーク インターフェイスの設定
- OpAdmin 管理者のパスワードの表示
- 更新プログラムのインストール
- サポート モードの有効化
- サポート スナップショットの作成および送信

注：DHCP を使用して IP を取得する場合は、「*ネットワーキング*」のセクションの下にある「*DHCP の使用*」に進んでください。

TGSH ダイアログ インターフェイスの設定方法

1. TGSH ダイアログにログインします。

   注：LDAP のみの認証を設定した場合、LDAP を使用して TGSH ダイアログにログインのみできます。認証モードが [System Password or LDAP] に設定されている場合、TGSH ダイアログのログインはシステム ログインのみ許可されます。

2. **TGSH ダイアログ** インターフェイスで、[CONFIG_NETWORK] を選択します。

   [ネットワーク設定（Network Configuration）] コンソールが開き、現在のネットワーク設定が表示されます。

3. 必要に応じて、設定を変更します。

   注：新しい文字を入力する前に Back Space を押して古い文字を削除する必要があります。

4. ダーティ ネットワークの [DNS Name] を空白のままにします。

5. ネットワーク設定の更新を終了した後で、タブ キーで下に移動し、[Validate] を選択して入力内容を検証します。

無効な値を入力した場合、エラーが表示されることがあります。その場合は、エラーを修正してから、再度検証します。

検証が完了すると、[Network Configuration Confirmation] に入力した値が表示されます。

6. [Apply] を選択して各種設定を適用します。

   コンソールは空白のグレーのボックスになり、その後、実行した設定変更の詳細情報がリストされます。

7. [OK] を選択します。

   [Network Configuration Console] が更新され、入力した IP アドレスが表示されます。これで、ネットワークの設定は完了しました。

TGSH ダイアログへの再接続

TGSH ダイアログはコンソールで開いたままになり、アプライアンスにモニタを接続するか、CIMC が設定されている場合はリモート KVM 経由でアクセスできます。

TGSH ダイアログに再接続する方法の 1 つは、ユーザ「**threatgrid**」で管理 IP アドレスに SSH 接続することです。必要なパスワードは、TGSH ダイアログに最初に表示される、ランダムに生成された初期パスワード、または OpAdmin 設定の最初の手順で作成した新しい管理者パスワードのどちらかです。

リカバリ モードでのネットワークの設定

8. 再起動してブート メニューが表示されるまで待ちます。短い時間しか表示されないので、注意してください（上記の図 3：ブート メニュー - サポート モードを参照してください）。

9. [Recovery Mode] を選択します。システムが起動するのを数分間待ちます。

10. システムが起動したら、Enter を数回押して、clean コマンド プロンプトを表示させます。

11. **netctl clean** を入力し、以下の質問に答えてください。

    Configuration type: static

    IP Address： <クリーン IP アドレス>/<ネットマスク>

    Gateway Address： <クリーン ネットワーク ゲートウェイ>

    Routes： <空白>

    最後の質問に対して y と応答します。

12. **Exit** と入力して設定を適用します。

この時点でアプライアンスはクリーン インターフェイスのポート 19791/tcp でアウトバウンド サポート接続を開こうと試みます。

メイン設定管理 - OpAdmin Portal

初期セットアップおよび設定ウィザードの説明については、『*Threat Grid Appliance Setup and Configuration Guide*』を参照してください。新しいアプライアンスでは、管理者が追加の設定を行う必要があります。また、時間がたつにつれ、OpAdmin の設定を更新しなければならなくなる場合があります。

OpAdmin Portal は、Threat Grid アプライアンス管理者向けの主要な設定インターフェイスです。このインターフェイスは Web ポータルで、TGA の管理インターフェイスで IP アドレスを設定した後に使用できるようになります。

OpAdmin は、アプライアンスを設定するための推奨ツールであり、実際、アプライアンスの設定の多くは OpAdmin を使用しなければ行うことができません。OpAdmin は、以下を含む重要な Threat Grid アプライアンスの設定を構成および管理するために使用します。

- 管理者パスワード（OpAdmin および「threatgrid」ユーザ用）
- Threat Grid ライセンス
- レート制限
- SMTP
- SSH
- SSL 証明書
- DNS サーバ（AMP for Endpoints プライベート クラウド統合用の DNS 設定を含む）
- NTP サーバ
- サーバ通知
- syslog メッセージおよび Threat Grid 通知のリモート サーバの設定
- CA 証明書管理（AMP for Endpoints プライベート クラウド統合用）
- LDAP 認証
- サードパーティの検出と統合サービス（ClamAV、OpenDNS、Titanium Cloud、および VirusTotal を含む）

注：設定中に IP アドレスとの接続が中断される可能性を低くするために、OpAdmin での設定更新は 1 回のセッションで完了する必要があります。

注：OpAdmin はゲートウェイ エントリを検証しません。間違ったゲートウェイを入力して保存すると、OpAdmin インターフェイスにアクセスできなくなります。管理インターフェイスでこうなった場合は、コンソールを使用してネットワーク設定を修正する必要があります。管理インターフェイスがまだ有効であれば、OpAdmin で修正して再起動することによって問題を解決できます。

リマインダ：OpAdmin は、HTTPS を使用します。ブラウザで管理 IP を指定するだけでは不十分です。次をポイントする必要があります。

https://adminIP/

または

https://adminHostname/

SSH キー

SSH キーを設定することによって、Threat Grid アプライアンス管理者は SSH を使用して TGSH ダイアログ（`threatgrid@<host>`）にアクセスできるようになります。

これによりルートへのアクセスやコマンド シェルが提供されることはありません。複数のキーを追加することができます。

[Configuration] > [SSH]

Syslog

定期的な通知を設定して（OpAdmin の [設定（Configuration）] > [通知（Notifications）]）電子メールでシステム通知を配信できるだけでなく、syslog メッセージと Threat Grid 通知を受信するようにリモート syslog サーバを設定することもできます。

1. OpAdmin の [Configuration] > [Syslog] の順に選択します
2. 表示されるフィールドにサーバ DNS を入力した後、ドロップダウン リストからプロトコルを選択します（デフォルトの [TCP] または [UDP] を選択できます）。
3. [検証（Verification）] ボックスをオンにします。これにより、[保存（Save）] をクリックした時点で、DNS ルックアップが実行されます。ホストがその名前を解決できない場合は、エラーが出力され、（有効なホスト名を入力するまで）ホスト名は保存されません。

   [Verification] ボックスをオンにしなければ、アプライアンスは DNS で有効な名前であるかどうかにかかわらず、任意の名前を受入れます。
4. [Save] をクリックします。

編集または削除する場合：Syslog DNS を更新するには、DNS を編集または削除して [保存（Save）] をクリックするだけです。

OpAdmin および TGSH ダイアログの LDAP 認証の設定

2.1.6 リリースには LDAP 認証が含まれ、OpAdmin と TGSH ダイアログのログインの認可は、Threat Grid アプライアンスに追加されました。以前は、OpAdmin と TGSH ダイアログ インターフェイスのパスワードは 1 つだけだったので、複数のアプライアンス管理者がいる場合は、パスワードを共有する必要がありました。これはよくない考えであるだけでなく、そのシナリオを避けることが多くのお客様の要件でもあります。その対処法として LDAP 認証を実装しました。

複数のアプライアンス管理者の追加

ドメイン コントローラまたは LDAP サーバで管理するさまざまなクレデンシャルを持つ複数のアプライアンス管理者を認証できるようになりました。LDAP 設定は単純ではないので、設定する前に詳細を完全に理解して、この手順を注意して行うことを推奨します。

認証モードは、[System Password Only]、[System Password or LDAP]、[LDAP Only] のいずれかです。

3 つの LDAP プロトコル オプション、[LDAP]、[LDAPS]、[LDAP with STARTLS] があります。

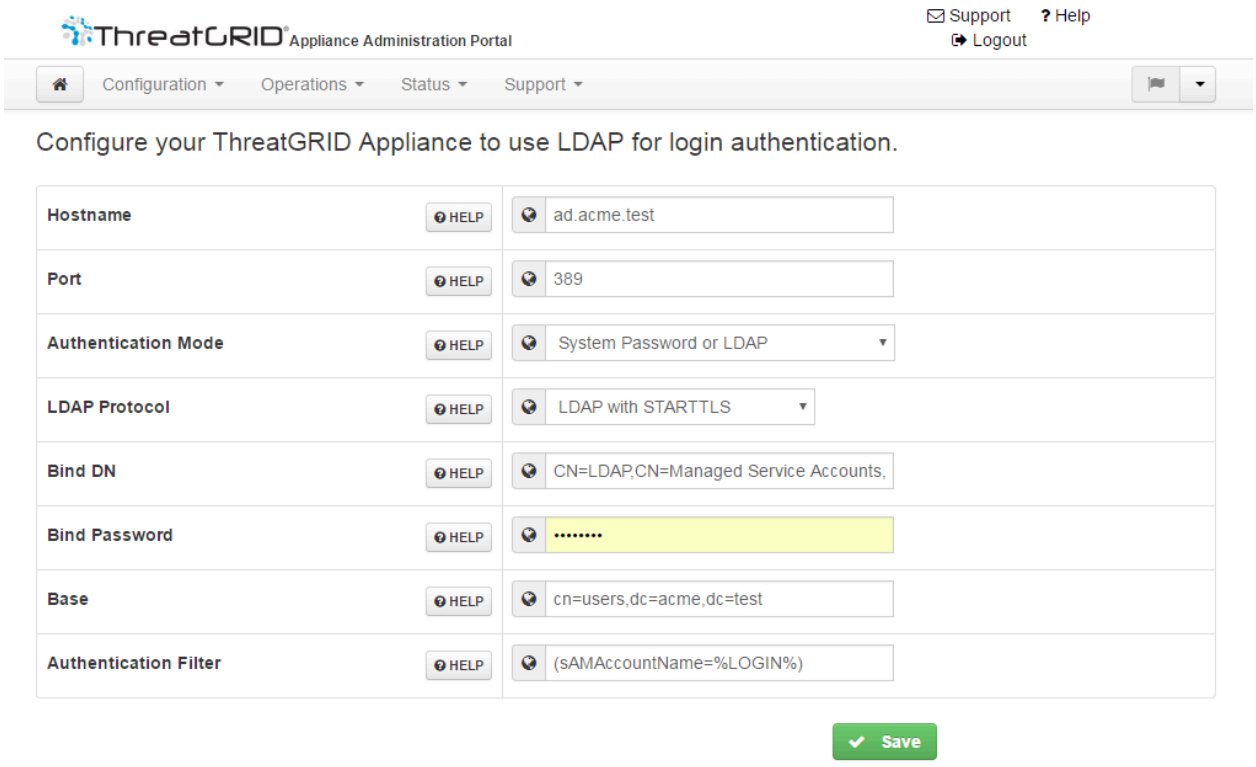
次のことに注意してください。

- 「デュアル」認証モード（[System Password or LDAP]）は、LDAP の設定時に、誤ってアプライアンスからロックされてしまうことを避けるために必要です。[LDAP Only] の選択は最初は許可されていないので、デュアル モードで、まず動作することを確認する必要があります。初期設定後に OpAdmin のログアウトが必要で、その後で、[LDAP Only] に切り替えるために LDAP クレデンシャルを使用して再度ログインします。
- [LDAP Only] 認証を設定した場合、LDAP を使用して TGSH ダイアログにログインのみできます。認証モードが [System Password or LDAP] に設定されている場合、TGSH ダイアログのログインはシステム ログインのみ許可されます。
- アプライアンスに LDAP 認証のみ（[LDAP Only]）が設定されている場合、リカバリ モードでパスワードをリセットすると、認証モードが再設定され、システム パスワードでもログインできるようになります。
- メンバーシップを制限するための認証フィルタが設定されていることを確認します。
- TGSH ダイアログと OpAdmin は [LDAP Only] モードでのみ LDAP クレデンシャルを必要とします。[LDAP Only] に設定すると、TGSH ダイアログはシステム パスワードを要求せず、LDAP ユーザとパスワードを要求します。
- 認証が [System Password or LDAP] に設定されている場合、TGSH ダイアログは、システム パスワードのみ要求し、両方ではありません。
- LDAP のトラブルシューティング：壊れたらリカバリ モードでパスワード リセットを実行することで無効にします。
- SSH 経由での TGSH ダイアログ アクセス：[LDAP Only] モードの時には SSH 経由での TGSH ダイアログ アクセス用の LDAP クレデンシャルに**加えて**、システム パスワードまたは設定済みの SSH キーが必要です。
- LDAP はクリーン インターフェイスからの発信です。

LDAP 認証の設定方法

1. OpAdmin で、[設定（Configuration）] > [LDAP] を選択します。LDAP 設定ページが開きます。

図 8：LDAP 認証設定



2. 各フィールドに値を指定します。

   各フィールドの横にある [?Help] ボタンをクリックして、詳細な説明と情報を表示します。

   LDAP 認証を最初に設定するときは、[System Password or LDAP] を選択し、OpAdmin をログアウトしてから、設定を変更して [LDAP Only] を実装するために、LDAP クレデンシャルを使用して再度ログインするという点に注意してください。

3. [Save] をクリックします。

次に、ユーザが OpAdmin または TGSH ダイアログにログインするときには、次が表示されます。

図 9：LDAP のみ

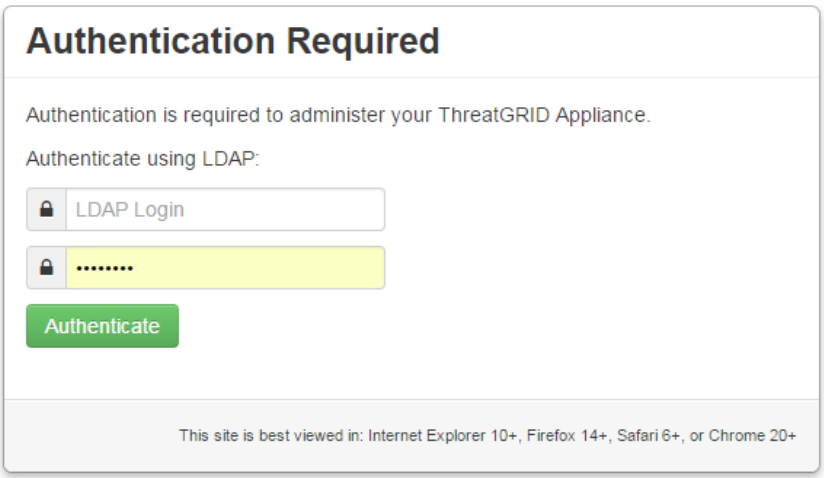
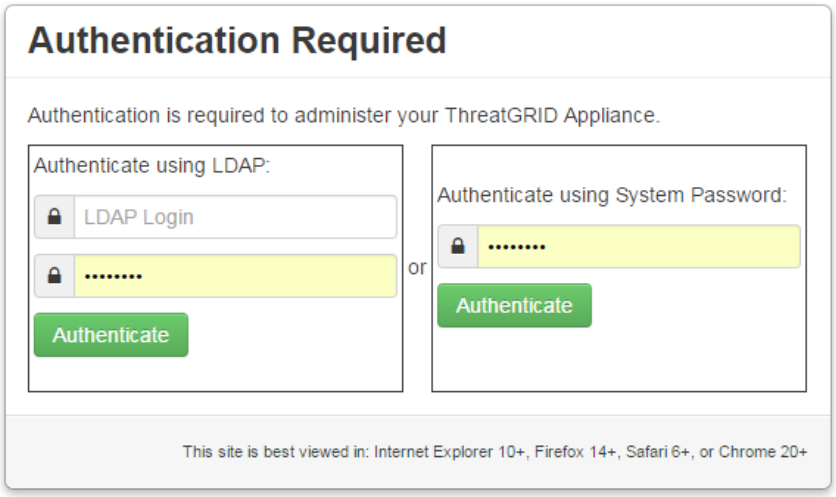


図 10：システム パスワードまたは LDAP



サードパーティ検出とエンリッチメント サービスの設定

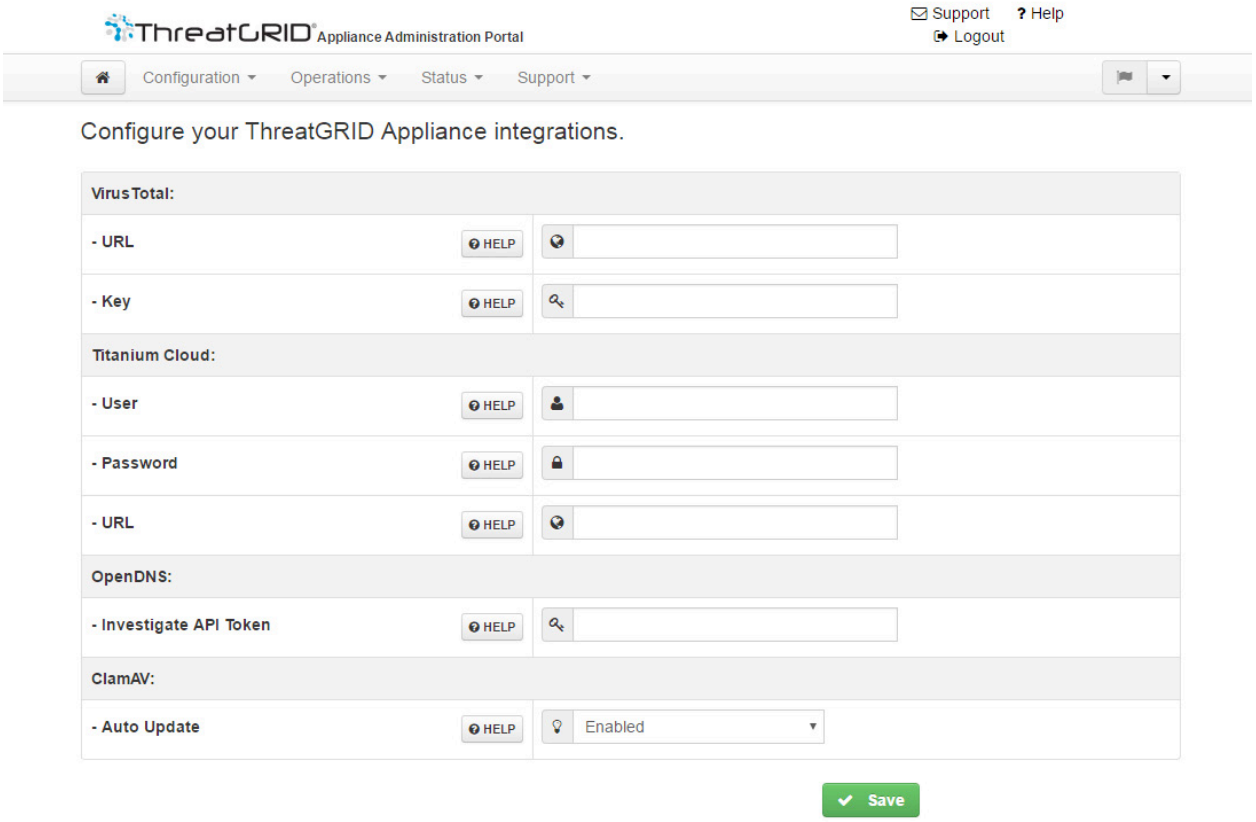
バージョン 2.2 では、OpenDNS、TitaniumCloud、VirusTotal などの複数のサードパーティ検出とエンリッチメント サービスとの統合を、新しい統合設定ページを使用してアプライアンスで設定できます。

OpAdmin で、[設定（Configuration）] > [統合（Integrations）] の順に選択し、統合設定ページを開きます。

必要な認証またはその他の値を入力し、[Save] をクリックします。

OpenDNS：OpenDNS を設定しない限り、ポータルの分析レポートの [ドメイン（Domains）] エンティティ ページの「whois」情報（UI の Mask バージョン）は表示されないことに注意してください。

図 11：統合設定



デフォルトで自動的に毎日更新される ClamAV シグネチャ

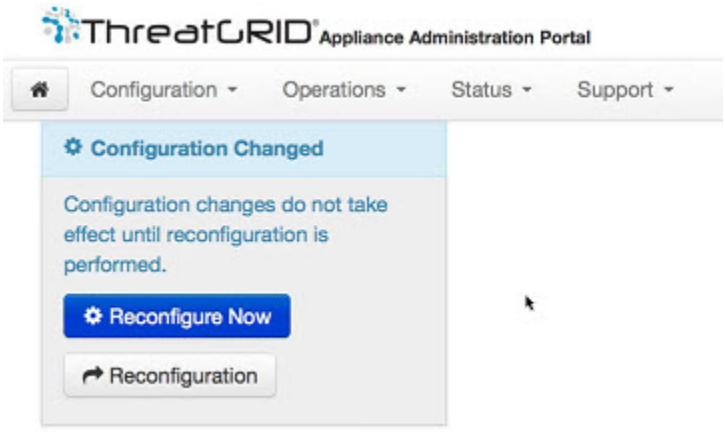
2.2 更新プログラムを使用すると、ClamAV シグネチャは自動的に毎日更新できます。これはデフォルトで有効になり、新しい統合設定ページ（上記）から無効にすることもできます。

再設定

設定の変更が行われると、ライト ブルーのアラートが [設定（Configuration）] メニューの下に表示されます。OpAdmin 設定を更新した場合、別の手順で再設定を保存する必要があります。

1. [Configuration Changed] をクリックします。[Reconfiguration] ダイアログが開きます。

図 12：[今すぐ再設定（Reconfigure Now）]



2. [再設定（Reconfigure）] をクリックし、アプライアンスに変更を適用します。

DHCP の使用

ほとんどのアプライアンス ユーザは DHCP により設定されたネットワークを使用しません。ただし DHCP を使用するように設定されたネットワークに接続している場合は、この項を参照してください。

注：アプライアンス ネットワークの初期設定で DHCP を指定したものの、静的 IP アドレスに切り替える必要が生じた場合は、以下の「*ネットワーク設定と DHCP*」を参照してください。

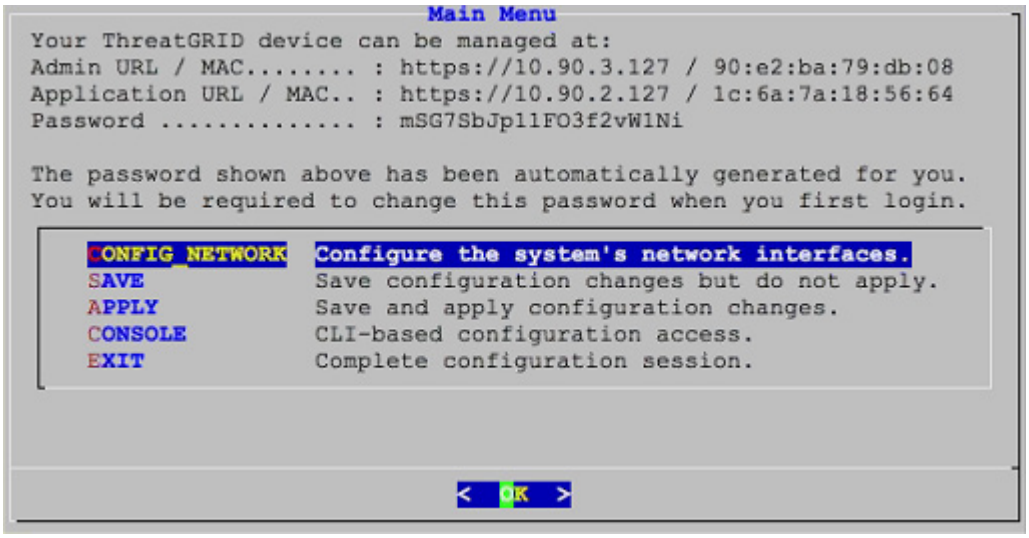
TGSH ダイアログには、OpAdmin Portal インターフェイスにアクセスし、設定するために必要な情報が表示されます。

DHCP の IP アドレスは、アプライアンスの起動直後に表示されないことがあります。しばらくお待ちください。

DHCP の明示的 DNS

v1.3 以降、DHCP を使用するシステムでは明示的に DNS を指定する必要があります。それ以前は必要ありませんでした。DNS サーバを明示的に指定していないシステムの 1.3 へのアップグレードは失敗します。

図 13：TGSH ダイアログ（DHCP を使用するように設定されたネットワークに接続）



管理 URL（Admin URL）：管理ネットワーク。OpAdmin の残りの設定作業を継続するためにこのアドレスが必要です。

アプリケーション URL（Application URL）：クリーン ネットワーク。

注：これは OpAdmin での設定後に、Threat Grid アプリケーションにアクセスするために使用するアドレスです。

ダーティ ネットワークは表示されません。

[パスワード（Password）] は管理者の初期パスワードで、アプライアンスのインストール時にランダムに生成されます。後で、OpAdmin 設定プロセスの最初の手順として、このパスワードを変更する必要があります。

永続的に DHCP を使用する場合、管理 IP アドレスを静的に変更する必要がなければ、追加のネットワーク設定は不要です。

ネットワーク構成と DHCP

初期設定で DHCP を指定し、3 つのネットワークすべてに対して、IP 割り当てを DHCP から永続的な静的 IP アドレスに調整する必要がある場合は、次の手順に従ってください。

注：OpAdmin はゲートウェイ エントリを検証しません。間違ったゲートウェイを入力して保存すると、OpAdmin インターフェイスにアクセスできなくなります。管理インターフェイスでこうなった場合は、コンソールを使用してネットワーク設定を修正する必要があります。管理インターフェイスがまだ有効であれば、OpAdmin で修正して再起動することによって問題を解決できます。

1. 左側の列で [Network] をクリックします。（[License] ウィンドウで [Configuration] > [Network] にチェック マークが付いていますが、DHCP ネットワーク設定はまだ完了していません）。

   [Network Configuration] ページが開きます。

クリーン

2. **IP 割り当て**。ドロップダウンから [静的（Static）] を選択します。
3. **[IP アドレス（IP Address）]**。クリーン ネットワーク インターフェイス用の静的 IP アドレスを入力します。
4. 必要に応じて、[Subnet mask] と [Gateway] を入力します。
5. [Validate DNS Name] の横のチェック ボックスをオンにして、DNS によって、入力した IP アドレスに解決されることを検証します。

ダーティ

6. **IP 割り当て**。ドロップダウンから [Static] を選択します。
7. **[IP アドレス（IP Address）]**。ダーティ ネットワーク インターフェイス用の静的 IP アドレスを入力します。
8. 必要に応じて、[Subnet mask] と [Gateway] を入力します。

管理

管理ネットワークの設定は、アプライアンスの初期セットアップおよび設定中に、**TGSH ダイアログ**を使用して行われています。

DNS

9. [Primary DNS Server] および [Secondary DNS Server] フィールドに入力します。

設定の保存

10. 完了後、[Next (Applies Configuration)] をクリックして、ネットワーク設定を保存します。

SMTP/電子メール

電子メール設定は [Email] ページで管理します。

時間

NTP サーバは、[Date and Time] ページで管理します。

DHCP 設定の適用

DHCP の設定を適用するには、[設定が変更（Configuration Changed）] をクリックし、次に [今すぐ再設定（Reconfigure Now）] をクリックします。

SSL 証明書と Threat Grid アプライアンス

Threat Grid アプライアンスを通過するネットワーク トラフィックは、SSL を使用してすべて暗号化されます。SSL 証明書を管理する方法の詳細は、このガイドの説明範囲外です。ただし、ESA/WSA アプライアンス、AMP for Endpoints プライベート クラウド、およびその他の統合と Threat Grid アプライアンスとの接続をサポートするように SSL 証明書をセットアップするための手順に役立つ情報を以下に示します。

SSL を使用するインターフェイス

SSL を使用する Threat Grid アプライアンスには、次の 2 つのインターフェイスがあります。

- Threat Grid Portal の UI と API、および統合（ESA/WSA アプライアンス、AMP for Endpoints プライベート クラウド配置更新サービスなど）用の**クリーン** インターフェイス
- **OpAdmin Portal** 用の**管理**インターフェイス。

サポートされる SSL/TLS のバージョン

- TLSv1.0
- TLSv1.1
- TLSv1.2

お客様提供の CA 証明書のサポート

2.0.3 リリースでは、お客様提供の CA 証明書がサポートされるようになりました。お客様ご自身で信頼できる証明書または CA 証明書をインポートできます。

SSL 証明書 - 自己署名デフォルト

Threat Grid アプライアンスは、自己署名 SSL 証明書とキーのセットがインストールされて出荷されます。1 つのセットが**クリーン** インターフェイス用で、もう一つのセットが**管理**インターフェイス用です。アプライアンスの SSL 証明書は、管理者が置き換えることができます。

デフォルトの Threat Grid アプライアンスの SSL 証明書のホスト名（共通名）は「*pandem*」で、10 年間有効です。設定時に Threat Grid アプライアンスに別のホスト名を割り当てると、証明書内のホスト名と CN が一致しなくなります。また、証明書内のホスト名は接続先の ESA/WSA アプライアンスまたはその他の統合先のシスコ デバイスまたはサービスによって想定されているホスト名とも一致する必要があります。これは、多くのクライアント アプリケーションにおいて、証明書内の CN がアプライアンスのホスト名と一致する SSL 証明書を必要とするためです。

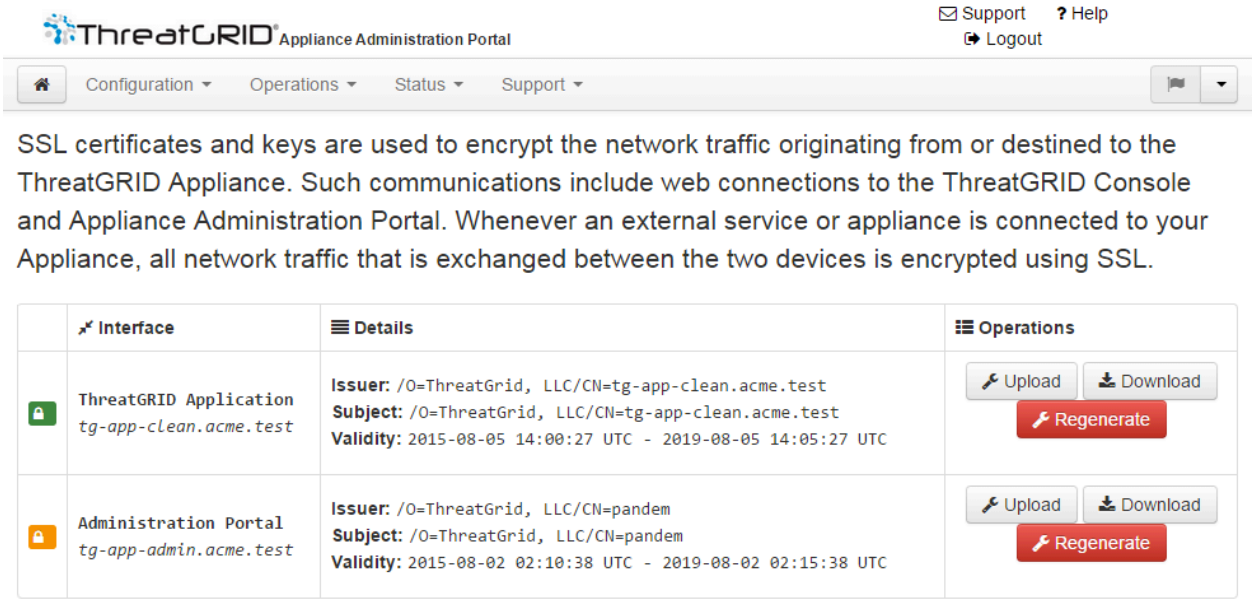
インバウンド接続用の SSL 証明書の設定

ESA/WSA アプライアンスや AMP for Endpoints プライベート クラウドなどのその他のシスコ製品は、Threat Grid アプライアンスと統合して、それにサンプルを送信することができます。このような統合は Threat Grid アプライアンスから見ればインバウンド接続になります。統合先のアプライアンスやその他のデバイスは、Threat Grid アプライアンスの SSL 証明書を信頼できる必要があるため、それを TGA からエクスポート（最初に CN フィールド内で正しいホスト名が使用されていることを確認してから、必要に応じて再生成または交換）して、統合先のアプライアンスまたはサービスにインポートする必要があります。

インバウンド SSL 接続に使用される Threat Grid アプライアンス上の証明書は、[SSL 証明書設定（SSL Certificate Configuration）] ページで設定します。**クリーン** インターフェイスと**管理**インターフェイス用の SSL 証明書は別々に設定することができます。

[OpAdmin] > [Configuration] > [SSL] の順に選択します。[SSL 証明書設定（SSL Certificate Configuration）] ページが開きます。

図 14：[SSL 証明書設定（SSL Certificate Configuration）] ページ



この図には 2 つの SSL 証明書があり、[ThreatGRID Application] がクリーン インターフェイス、[Administration Portal] が**管理**インターフェイスです。

CN 検証

[SSL 証明書設定（SSL Certificate Configuration）] ページで、色付きの鍵マークのアイコンは、TG アプライアンス上の SSL 証明書のステータスを示します。ホスト名は、SSL 証明書内で使用される CN（「共通名」）と一致する必要があります。一致しない場合は、現在のホスト名を使用する証明書と交換する必要があります。後述の「SSL 証明書の置き換え」を参照してください。

緑色の鍵マークのアイコンは、クリーン インターフェイスのホスト名が SSL 証明書で使用されている CN（「共通名」）と一致していることを意味します。

黄色の鍵マークのアイコンは、管理インターフェイスのホスト名がその SSL 証明書の CN と一致していないことを示す警告です。この証明書は、現在のホスト名を使用する証明書と置き換えることが必要になります。

SSL 証明書の置き換え

SSL 証明書は、さまざまな理由から、特定の時点で交換する必要があります。たとえば、期限切れになったり、ホスト名が変更されたりした場合です。また、Threat Grid アプライアンスとその他のシスコ デバイスおよびサービス間の統合をサポートするために SSL 証明書を追加または交換しなければならない場合もあります。

ESA/WSA アプライアンスとその他の CSA シスコ統合デバイスでは、共通名が Threat Grid アプライアンスのホスト名と一致する SSL 証明書が必要な場合があります。この場合、デフォルトの SSL 証明書を置き換えて、同じホスト名を使用する新しい SSL 証明書を生成する必要があり、このホスト名から Threat Grid アプライアンスにアクセスすることになります。

Threat Grid アプライアンスと AMP for Endpoints プライベート クラウドを統合してその配置更新サービスを使用する場合は、AMP for Endpoints プライベート クラウド SSL 証明書をインストールする必要があるため、Threat Grid アプライアンスは接続を信頼することができます。

Threat Grid アプライアンスで SSL 証明書を交換するには、複数の方法があります。

- CN に対して現在のホスト名を使用する新しい SSL 証明書の再生成。
- SSL 証明書のダウンロード
- 新しい SSL 証明書のアップロード。これは、市販の SSL や会社の SSL にすることも、OpenSSL を使用して自分で作成することもできます。
- 独自の SSL 証明書の生成 - OpenSSL を使用した例

これについては、以降のセクションを参照してください。

SSL 証明書の再生成

この方法は、v1.3 よりも前の Threat Grid アプライアンスで、OpenSSL や他の SSL ツールを使用して新しい SSL 証明書を手動で生成する必要があった方法に代わるものです。ただし、この方法は、後述の独自の SSL 証明書の生成 - OpenSSL を使用した例の項で説明されているように未だに有効です。

注: このタスクを実行する前に、Threat Grid アプライアンスを 1.4.2 以降にアップグレードする必要があります。

OpAdmin の [SSL 証明書設定（SSL Certificate Configuration）] ページで、[再作成（Regenerate）] をクリックします。証明書の CN フィールドでアプライアンスの現在のホスト名を使用する新しい自己署名 SSL 証明書が Threat Grid アプライアンス上で生成されます。CN 検証の鍵マークのアイコンが緑色で表示されます。再生成した証明書（.cert ファイル）は、次の項の説明に従ってダウンロードし、統合先のアプライアンスにインストールすることができます。

SSL 証明書のダウンロード

キーではなく、Threat Grid SSL 証明書をダウンロードして統合先のデバイスにインストールできるため、TG アプライアンスからの接続を信頼することができます。この手順に必要なのは .cert ファイルだけです。

1. OpAdmin の [SSL 証明書設定（SSL Certificate Configuration）] ページで、取得する証明書の横にある [ダウンロード（Download）] をクリックします。SSL 証明書がダウンロードされます。
2. 次に、他の SSL 証明書のインストールと同様に、ダウンロードした SSL 証明書を ESA/WSA アプライアンス、AMP for Endpoints プライベート クラウド（以前の FireAMP パブリック クラウド）、またはその他の統合先のシスコ製品にインストールします。

SSL 証明書のアップロード

組織内で市販のまたは会社の SSL 証明書をすでに運用している場合は、それを使用して TGA 用の新しい SSL 証明書を生成したり、ESA/WSA デバイスやその他の統合先のデバイス上の CA 証明書を使用したりできます。

独自の SSL 証明書の生成 - OpenSSL を使用した例

社内で SSL 証明書インフラストラクチャがまだ稼働しておらず、その証明書を他の手段で取得できない場合などは、手動で独自の SSL 証明書を生成する方法もあります。そうすれば、その証明書を前述したようにアップロードすることができます。

次に、「Acme Company」用の新しい自己署名 SSL 証明書を生成するためのコマンドの例を示します。この例では、OpenSSL 証明書、キー、およびその他のファイルを作成および管理するための標準のオープン ソース SSL ツールである OpenSSL を使用します。

注：OpenSSL はシスコ製品ではないため、シスコでは OpenSSL に関するテクニカル サポートは提供していません。OpenSSL の使用に関するその他の情報は、Web で検索してください。シスコでは、SSL 証明書を生成するための SSL ライブラリの *Cisco SSL* を提供しています。

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout
tgapp.key -nodes -out tgapp.cert -subj "/C=US/ST=New
York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

openssl：OpenSSL。

req：X.509 証明書署名要求（CSR）を使用することを指定します。「X.509」とは、SSL および TLS でキーと証明書の管理に使用する公開キー インフラストラクチャの標準です。新しい X.509 証明書を作成するため、このサブコマンドを使用しています。

-x509：このオプションにより、証明書署名要求を生成するのではなく、自己署名証明書を生成するとユーティリティに指示することで、前のサブコマンドが変更されます。

-days 3650：このオプションにより、証明書が有効と見なされる期間が設定されます。ここでは、期間を 10 年間に設定しています。

-newkey rsa:4096：このオプションでは、新しい証明書と新しいキーを同時に生成することを指定します。前の手順で証明書に署名するために必要なキーを作成しなかったため、証明書とともにキーを作成する必要があります。rsa:4096 の部分は、長さが 4096 ビットの RSA キーを生成するように指示します。

-keyout：この行は、作成する、生成される秘密キー ファイルを配置する場所を OpenSSL に指示します。

-nodes：このオプションは、作成する証明書をパスフレーズでセキュリティ保護するためのオプションをスキップするように OpenSSL に指示します。アプライアンスでは、サーバの起動時にユーザの介入なしでファイルを読み込むことができる必要があります。再起動後ごとにパスフレーズを入力する必要があるため、パスフレーズによって、これが実行されなくなります。

-out：このオプションでは、作成する証明書を配置する場所を OpenSSL に指示します。

-subj：例：

C=US：国。

ST= New York：州。

L=Brooklyn：場所。

O=Acme Co：所有者の名前。

CN=tgapp.acmeco.com：Threat Grid アプライアンスの FQDN（「完全修飾ドメイン名」）を入力します。これには、Threat Grid アプライアンスのホスト名（この例では「tgapp」）に、最後に関連付けられたドメイン名（「acmeco.com」）を付加して指定します。

重要:少なくとも Threat Grid アプライアンスのクリーン インターフェイスの FQDN と一致するように共通名を変更することが必要になります。

新しい SSL 証明書が生成されたら、[SSL] ページの [アップロード（Upload）] ボタンを使用して、この SSL 証明書を Threat Grid アプライアンスにアップロードし、また ESA/WSA アプライアンス（.cert のみ）にもアップロードします。

アウトバウンド接続用の SSL 証明書の設定

Threat Grid アプライアンス リリース 2.0.3 には、配置更新サービスのための AMP for Endpoints プライベート クラウドとの統合をサポートする機能が含まれています。

DNS の設定

デフォルトで、DNS はダーティ インターフェイスを使用します。統合ではクリーン インターフェイスが使用されるために、AMP for Endpoints プライベート クラウドなどの統合先のアプライアンスまたはサービスのホスト名がダーティ インターフェイス経由で解決できない場合は、クリーン インターフェイスを使用する別の DNS サーバを OpAdmin で設定することができます。

OpAdmin で、[Configuration] > [Network] の順に選択して、ダーティ ネットワークとクリーン ネットワークの DNS フィールドに値を入力し、[Save] をクリックします。

CA 証明書管理

リリース 2.0.3 で追加された機能の 1 つが、*アウトバウンド*SSL 接続用の CA 証明書管理トラストストアに関する新しいページです。これにより、TGA は、AMP for Endpoints プライベート クラウドを信頼して、分析の結果、悪意があると判断されたサンプルを通知することができます。

OpAdmin で、[Configuration] > [CA Certificates] の順に選択します。次を選択します。

1. [Import from Host]。サーバから証明書を取得します。[Retrieve certificates from server] ダイアログが開きます。
2. AMP for Endpoints プライベート クラウドの**ホスト**と**ポート**を入力して、[取得（Retrieve）] をクリックします。証明書が取得されます。

または

[Import from Clipboard]。クリップボードから PEM を貼り付けて、[証明書の追加（Add Certificate）] をクリックします。

3. [Import] をクリックします。

配置更新サービス管理

このタスクは、Threat Grid Portal UI から実行します。

1. ログイン名の横にあるナビゲーション バーのドロップダウンから、[FireAMP 統合の管理（Manage FireAMP Integration）] を選択します。[配置更新サービス（Disposition Update Service）] ページが開きます（下記の図 15：[配置更新の配信サービス（Disposition Update Syndication Service）] ページを参照）。
2. **AMP for Endpoints プライベート クラウドの URL** と、AMP for endpoints 設定ポータルで指定された**管理者ユーザ名**と**パスワード**を入力して、[設定（Config）] をクリックします。

AMP for Endpoints プライベート クラウド アプライアンス統合の詳細については、下記の「Cisco AMP for Endpoints プライベート クラウドへの Threat Grid アプライアンスの接続」を参照してください。

ESA/WSA アプライアンスの Threat Grid アプライアンスへの接続

ESA/WSA やその他のアプライアンス、デバイス、サービスなどのシスコ製品は、SSL で暗号化された接続を介して Threat Grid アプライアンスと統合される場合があります。これは、マルウェアの可能性があるサンプルを、分析のために Threat Grid アプライアンスに送信するためです。

「CSA 統合」：ESA/WSA アプライアンスと Threat Grid アプライアンスの統合は、Cisco Sandbox API（「CSA API」）によって可能になります。この統合は、「CSA 統合」とも呼ばれています。

統合先の ESA/WSA アプライアンスは、分析用のサンプルを送信する前に、Threat Grid アプライアンスに登録する必要があります。統合先の ESA/WSA を Threat Grid アプライアンスに登録するには、その前に ESA/WSA の管理者が、まずそれらのアプライアンスとネットワーク環境に対して SSL 証明書接続を適切にセットアップする必要があります。

ここでは、Threat Grid アプライアンスを統合先の ESA/WSA アプライアンスやその他のシスコ製品と通信するように設定するために必要な手順について説明します。

ESA/WSA のマニュアルへのリンク

ご使用の ESA/WSA のオンライン ヘルプまたはユーザ ガイドの「*Enabling and Configuring File Reputation and Analysis Services*」の手順を参照してください。（Threat Grid アプライアンスは、これらのガイドでは「分析サービス」または「プライベート クラウド ファイル分析サーバ」と呼ばれます。）

ESA ユーザ ガイドは次の場所にあります。
https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

WSA ユーザ ガイドは次の場所にあります。
https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

統合プロセスの概要

はじめる前に：ここでは、Threat Grid アプライアンスと ESA/WSA アプライアンスやその他の CSA 統合の間の接続（インバウンド）の設定手順の概要を説明します。

各手順の詳細な説明を含む表をこの項の後に示します。

Threat Grid アプライアンス SSL 証明書 SAN または CN は、現在のホスト名と ESA/WSA の想定と一致する必要があります。

Threat Grid アプライアンス SSL 証明書 SAN（「Subject Alternative Name」、定義されている場合）または CN（「Common Name」）はホスト名および ESA/WSA の想定とも一致する必要があります。統合先の ESA/WSA アプライアンスとの接続を成功させるためには、統合先の ESA/WSA アプライアンスが Threat Grid アプライアンスを識別するためのホスト名とも一致する必要があります。

要件によっては、Threat Grid アプライアンス上で自己署名 SSL 証明書を再生成しなければならない場合があります。その場合は、SAN/CN フィールド内の現在のホスト名を使用して、それを作業環境にダウンロードし、統合先の ESA/WSA アプライアンスにアップロードしてインストールする必要があります。

または、会社の SSL 証明書か市販の SSL 証明書（または手動で生成した証明書）をアップロードすることによって、現在の TGA SSL 証明書を置き換える必要があります。

詳細な手順については、前述の「インバウンド接続用の SSL 証明書の設定」を参照してください。

接続の確認：

SSL 証明書の設定が完了すると、次のステップは ESA/WSA アプライアンスが Threat Grid アプライアンスと通信できることを確認することです。

Cisco ESA/WSA アプライアンスが、ネットワークを介して Threat Grid アプライアンスのクリーン インターフェイスに接続できる必要があります。

TGA と ESA/WSA アプライアンスが相互に通信できることを確認するために、ご使用の製品の該当するガイドの手順を実行してください。（上記リンクを参照してください）

ESA/WSA ファイル分析設定を実行します。

ファイル分析セキュリティ サービスを有効にし、詳細を設定します。

Cisco ESA/WSA またはその他のデバイスを Threat Grid アプライアンスに登録します。

それぞれの製品のマニュアルに従って設定された ESA/WSA アプライアンスは、自動的に Threat Grid アプライアンスに登録されます。

接続先のデバイスの登録時に、新しい Threat Grid のユーザがデバイス ID をログイン ID として使用して作成され、新しい組織が同じ ID に基づく名前で作成されます。新しいデバイス ユーザ アカウントは、次の項で説明されているように、管理者によってアクティブにする必要があります。

Threat Grid アプライアンスで新しい ESA/WSA アカウントを有効化します。

ESA/WSA アプライアンスまたはその他の統合が Threat Grid アプライアンスに接続してそれ自体を登録すると、新しい Threat Grid ユーザ アカウントが自動的に作成されます。このユーザ アカウントの初期ステータスは「de-activated」です。他の Threat Grid ユーザと同様に、マルウェア サンプルを分析用に送信するためにデバイス ユーザ アカウントを使用するには、Threat Grid アプライアンス管理者がそのデバイス ユーザ アカウントを手動で有効にする必要があります。

ESA/WSA の統合プロセスの手順

この接続は Threat Grid アプライアンスから*見れば*受信です。

この統合は CSA API を使用します。

接続先で実行する必要のあるタスクの詳細については、ESA および WSA のユーザ ガイドを参照してください。

手順	Threat Grid アプライアンス（「TGA」）	ESA/WSA/その他の CSA API の統合
1	Threat Grid アプライアンスを通常どおりに（つまり、まだ統合が存在しない状態で）セットアップして設定します。 更新プログラムがあるかどうかを確認し、あればインストールします。	

手順	Threat Grid アプライアンス（「TGA」）	ESA/WSA/その他の CSA API の統合
2		ESA/WSA アプライアンスを通常どおりに（つまり、まだ統合が存在しない状態で）セットアップして設定します。
3	**TGA SSL 証明書 SAN または CN は、現在のホスト名と ESA/WSA の想定と一致する必要があります** 自己署名された SSL 証明書を使用するには、次の手順に従います。 必要に応じて、デフォルトを置き換えるための新しい SSL 証明書（Threat Grid アプリケーションの、クリーン インターフェイスで）を生成し、それを ESA/WSA アプライアンスのデバイスにダウンロードしてインストールします。（TGA SSL 証明書については、前述の項 SSL 証明書と Threat Grid アプライアンスで説明されています） SAN または CN として Threat Grid アプライアンスのホスト名がある証明書を生成してください。Threat Grid アプライアンスのデフォルトの証明書は機能しません。 IP アドレスではなくホスト名を使用します。	
4		**接続の確認** Cisco ESA/WSA アプライアンスが、ネットワークを介して Threat Grid アプライアンスの**クリーン** インターフェイスに接続できる必要があります。

手順	Threat Grid アプライアンス（「TGA」）	ESA/WSA/その他の CSA API の統合
5		**TG アプライアンスの統合用の ESA/WSA アプライアンスを設定します。** 手順についての詳細は、ESA/WSA のガイドを参照してください。次の手順は ESA 固有ですが、これが現在最も一般的なタイプの統合です 1. [Security Services] > [File Reputation and Analysis] の順に選択します。 2. [Enable] をクリックします。 3. [グローバル設定を編集（Edit Global Settings）] をクリックします。 ファイル分析は、デフォルトで有効になっています。[Enable File Analysis] のチェックを外さなければ、ファイル分析機能キーは次のコミット後にアクティブ化されます。 4. [File Analysis] セクションで、分析用にクラウドに送信するファイルの種類を選択します。 5. ESA または WSA のガイドに従って、必要に応じて [Advanced Settings for File Analysis] を設定します。 **ファイル分析サーバ URL：** [Private Cloud] を選択します。 **サーバ：** オンプレミスの Cisco Thread Grid アプライアンスの **URL**。 この値と証明書には、IP アドレスではなくホスト名を使用します。

手順	Threat Grid アプライアンス（「TGA」）	ESA/WSA/その他の CSA API の統合
		SSL 証明書： オンプレミスの Cisco Threat Grid アプライアンスから生成した自己署名証明書をアップロードします。 最後にアップロードされた自己署名証明書が使用されます。最新の証明書より前にアップロードされた証明書にアクセスすることはできません。必要ならば、該当する証明書を再びアップロードします。 6. 変更を送信し、保存します。 ページの下部に表示される**ファイル分析クライアント ID** を確認します。これはステップ 7 でアクティブ化する必要がある「ユーザ」を特定します。 **Threat Grid アプライアンスへの登録は自動的** Threat Grid アプライアンスが記載された電子メール セキュリティ アプライアンスや Web セキュリティ アプライアンスの登録は、ファイル分析用に設定を送信すると自動的に発生します。ただし、ステップ 7 に示すように、登録をアクティブ化する必要があります。

手順	Threat Grid アプライアンス（「TGA」）	ESA/WSA/その他の CSA API の統合
7	**Threat Grid アプライアンスの新しいデバイス ユーザ アカウントのアクティブ化** 1. 管理者として Threat Grid Portal UI にログインします。 2. ログイン名の横にあるナビゲーション バーのドロップダウン メニューから、[ユーザの管理（Manage Users）] を選択します。[Threat Grid Users] ページが開きます。 3. デバイス ユーザ アカウントの [User Details] ページを開きます（探すために検索を使用する必要がある場合があります）。 ユーザの現在のステータスは「de-activated」です。 4. [Re-Activate User] をクリックします。ダイアログが表示されて確認を求めます。 5. 確定するには、このダイアログで [再アクティブ化（Re-Activate）] をクリックします。	

これで、ESA/WSA またはその他の統合するアプライアンスやデバイスが、Threat Grid アプライアンスと接続を開始できるようになります。

Cisco AMP for Endpoints プライベート クラウドへの Threat Grid アプライアンスの接続

特に、新しいアプライアンスを設定する場合は、Threat Grid アプライアンス配置更新サービスと AMP for Endpoints プライベート クラウド統合の設定タスクを次の順序でデバイス上で実行する必要があります。すでにセットアップして設定されているアプライアンスを統合する場合は、順序はそれほど重要ではありません。

この接続は、Threat Grid アプライアンスから見れば送信です。この統合では CSA API（Cisco Sandbox API）を使用しません。

接続先で実行するタスクの詳細については、AMP for Endpoints プライベート クラウドのマニュアルを参照してください。

手順	Threat Grid アプライアンス（「TGA」）	AMP for Endpoints プライベート クラウド
1	Threat Grid アプライアンスを通常どおりに（つまり、まだ統合が存在しない状態で）セットアップして設定します。 更新プログラムがあるかどうかを確認し、あればインストールします。	
2		AMP for Endpoints プライベート クラウドを通常どおりに（つまり、まだ統合が存在しない状態で）セットアップして設定します。
3		**TGA 統合用に AMP for Endpoints プライベート クラウドを設定します。** [Integrations] > [Threat Grid] の順に選択して、[Connection to Threat Grid] セクションに移動します。 Threat Grid アプライアンスとの接続を完了するには、それを信頼する必要があります。DNS ホスト名、SSL 証明書、および API キーが必要です。 この情報を探す場合は、TGA 列のステップ 3.1 に進みます。

手順	Threat Grid アプライアンス（「TGA」）	AMP for Endpoints プライベート クラウド
3.1	**SSL 証明書：-** Threat Grid アプライアンスの OpAdmin インターフェイスで、[設定（Configuration）] > [SSL] の順に選択します。 必要に応じて、デフォルトを置き換えるための新しい SSL 証明書を（「Threat Grid Application」のクリーン インターフェイスから）再生成し、それを AMP for Endpoints プライベート クラウド デバイスにダウンロードしてインストールします。（TGA SSL 証明書については、SSL 証明書と Threat Grid アプライアンスで説明されています。） **ホスト名** [Configuration] > [Hostname] の順に選択します。 **API キー：** API キーは、統合に使用するアカウントの [User Details] ページの Threat Grid Face Portal UI で見つかる場合があります。 1. **Threat Grid Portal UI** に移動します。 2. ログイン名の横にあるナビゲーション バーのドロップダウン メニューから、[ユーザの管理（Manage Users）] を選択します。 3. 統合のユーザ アカウントの [User Details] ページ（必要に応じて検索を使用）に移動して、**API キー**をコピーします。これは、「管理者」ユーザである必要はなく、Threat Grid アプライアンス上でこの目的のために特別に作成された別のユーザも可能なことに注意してください。	

手順	Threat Grid アプライアンス（「TGA」）	AMP for Endpoints プライベート クラウド
3.2		[Connection to Threat Grid] フィールドに値を入力します。 1. TGA ホスト名を入力します 2. 統合に使用するアカウント用の Threat Grid API キーを入力します。 3. TGA SSL 証明書ファイルを選択します。 4. [Save Configuration] をクリックします。 5. [Test Connection] をクリックします。 6. 接続テストに通過したら、AMP for Endpoints プライベート クラウド上で再設定を実行して変更を適用する必要があります。 技術的には、これによって、AMP が Threat Grid アプライアンスと対話できるようになり、この時点でサンプルを TG に送信できます。ただし、配置更新サービスをセットアップするための残りの手順を実行して、配置結果を TGA に伝達する必要があります。 （詳細については、AMP for Endpoints プライベート クラウドのユーザ マニュアルを参照してください。）
4	**配置更新サービスの設定** 次の手順では、配置更新サービスの設定方法について説明します	

手順	Threat Grid アプライアンス（「TGA」）	AMP for Endpoints プライベート クラウド
4.1	**必要に応じて DNS を設定します。** FireAMP 統合には、クリーン インターフェイスが使用されます。ただし、デフォルトで、DNS はダーティ インターフェイスを使用します。AMP for Endpoints プライベート クラウドのホスト名がダーティ インターフェイスに解決できない場合、クリーン インターフェイスを使用する別の DNS サーバを OpAdmin に構成できます。 OpAdmin で、[Configuration] > [Network] の順に選択して、**ダーティ** ネットワークと**クリーン** ネットワーク上の DNS に関するフィールドに値を入力し、[Save] をクリックします。	

手順	Threat Grid アプライアンス（「TGA」）	AMP for Endpoints プライベート クラウド
4.2	**CA 証明書管理：** 次のステップは、統合先のデバイスを信頼できるように、AMP for Endpoints プライベート クラウド SSL 証明書を Threat Grid アプライアンスにダウンロードまたはコピーして貼り付けることです。 1. OpAdmin で、[Configuration] > [CA Certificates] の順に選択します。AMP for Endpoints プライベート クラウド ホストまたはクリップボードからインポートする SSL 証明書を選択できます。 2. インポートする証明書を選択して、[Import from Host] をクリックします。[Retrieve certificates from server] ダイアログが開きます。FireAMP アプライアンス配置サービス用の**ホスト**と**ポート**を入力して、[Retrieve] をクリックします。 3. 証明書が取得されます。 4. [インポート（Import）] をクリックします。 （または [Import from Clipboard] をクリックします。クリップボードから PEM を貼り付けて、[Add Certificate] をクリックします）。	

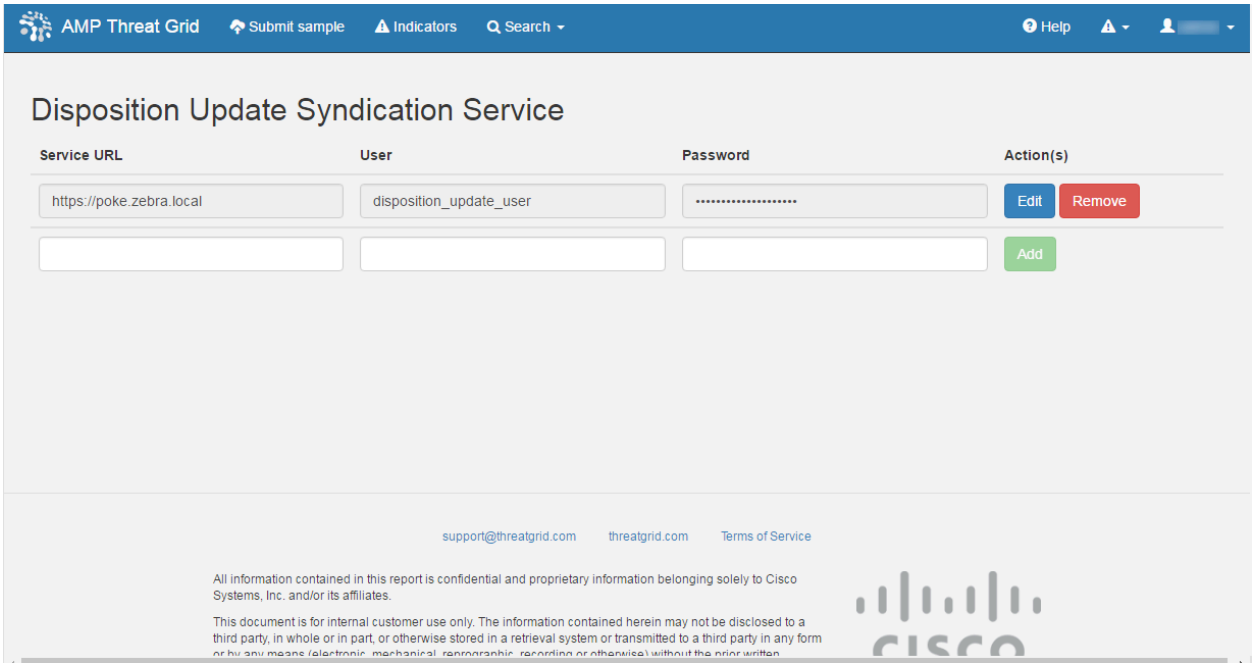
手順	Threat Grid アプライアンス（「TGA」）	AMP for Endpoints プライベート クラウド
4.3	**FireAMP 統合管理：** Threat Grid Face Portal UI で、右上のメニューから、[Manage FireAMP Integration] を選択します。[Disposition Update Syndication Service] ウィンドウが開きます（下記を参照）。 AMP 配置更新サービス URL を入力します（この URL は FireAMP アプライアンス上で検索できます。[統合（Integrations）] > [Threat Grid] > [AMP for Endpoints プライベートクラウドの詳細（AMP for Endpoints Private Cloud Details）] の順に選択します）。 **管理者ユーザ名とパスワード**を入力して、[Config] をクリックします。	

配置更新の配信サービスの管理

2.2 リリースでは、配置更新通知用に複数の URL を設定するためのサポートが追加されました（「マルチ POKE」とも呼ばれます）。

URL は新しい [Disposition Update Syndication Service] ページから追加、編集、および削除できます。

図 15：[配置更新の配信サービス（Disposition Update Syndication Service）] ページ



Threat Grid 組織およびユーザの管理

Threat Grid は、デフォルトの組織および管理ユーザが設定された状態でアプライアンスにインストールされます。アプライアンスのセットアップとネットワークの設定が完了した後、他のユーザがアプライアンスにログインして分析対象のマルウェア サンプルを送信できるよう、追加の組織とユーザ アカウントを作成できます。

組織の構成によっては、組織、ユーザ、管理者を追加する際に複数のユーザやチーム間での計画と調整が必要になる場合があります。

新規組織の作成

ユーザは常に組織に所属します。したがって、ユーザを追加するには、まず組織を作成し、そこにユーザを追加する必要があります。

重要：いったん作成された組織をこのインターフェイスから削除することはできないため、このタスクは慎重に計画する必要があります。

1. 管理者として Threat Grid Portal にログインします。
2. 管理者のメニューをクリックし、[組織の管理（Manage Organization）] を選択します。

   [Organizations] ページが開き、アプライアンスに設定されているすべての組織がリストされます。
3. 画面の右上隅にある [Add Organization] ボタンをクリックします。[Properties] ダイアログ ボックスが開きます。
4. すべてのフィールドは必須です。

   [Name]：組織名を追加します（現在、名前の文字数制限はありません）。

   [Industry] 。[Industry] ドロップダウンから、ビジネスのタイプを選択します該当する業界がリストにない場合は、[Unknown] に設定したままにし、Threat Grid サポート（support@threatgrid.com）に連絡してオプションの追加を依頼してください。

   その他のオプションを入力します。

   [Rate Limit]：

   API レート制限は、ライセンス契約条件に基づいてアプライアンス全体に適用されます。これは、API 送信にのみ影響し、手動でのサンプル送信には影響しません。ライセンス内のレート制限は組織に適用されます。

   デフォルトのユーザ送信レート制限を設定します。また、Threat Grid Portal オンライン ヘルプ（ナビゲーション バーで [Help] > [Using Threat Grid Online Help] の順に選択）の「Using Threat Grid」で説明されている手順に従って、ユーザごとにサンプル送信レートを設定することもできます。

   レート制限はカレンダー日ではなくローリング タイムの 24 時間の時間枠に基づきます。送信制限に達すると、次の API 送信の再試行まで待機する時間を通知するメッセージとともに、429 エラーが返されます。

   [Priority] フィールドはなくなる予定ですが、ここでは「50」を入力しておきます。
5. [Create] をクリックします。新しい組織が作成され、[Organizations] リストに表示されます。

ユーザの管理

ユーザ アカウントの作成と管理の注意事項とマニュアル（ユーザを追加する方法を含む）については、Threat Grid Portal UI のオンライン ヘルプを参照してください。ナビゲーション バーから [ヘルプ（Help）] > [Threat Grid オンラインヘルプ（Threat Grid Online Help）] > [Threat Grid ユーザの管理（Managing Threat Grid Users）] *を選択します。*

注：サンプルの送信がない場合、ユーザは API の b）から a）のみ削除できます。

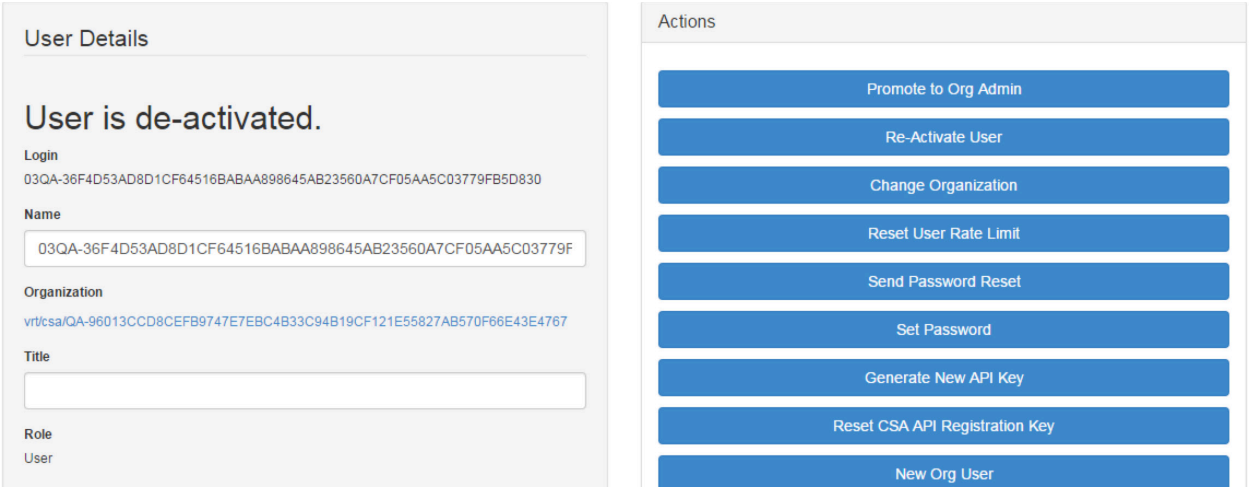
Cisco ESA/WSA アプライアンスおよびその他のデバイスを統合するためのデバイス ユーザ アカウントの管理については、次のセクションで説明します。

Threat Grid アプライアンスの新しいデバイス ユーザ アカウントのアクティブ化

ESA/WSA アプライアンスまたはその他の CSA（Cisco Sandbox API）統合が Threat Grid アプライアンスに接続してそれ自体を登録すると、新しい Threat Grid ユーザ アカウントが自動的に作成されます。このユーザ アカウントの初期ステータスは「de-activated」です。他の Threat Grid ユーザと同様に、マルウェア サンプルを分析用に送信するためにデバイス ユーザ アカウントを使用するには、Threat Grid アプライアンス管理者がそのデバイス ユーザ アカウントを手動で有効にする必要があります。

1. 管理者として Threat Grid Portal UI にログインします。
2. ログイン名の横にあるナビゲーション バーのドロップダウン メニューから、[ユーザの管理（Manage Users）] を選択します。[Threat Grid ユーザの詳細（Threat Grid User Detailss）] ページが開きます。
3. デバイス ユーザ アカウントの [ユーザの詳細（User Details）] ページを開きます（探すために検索の使用が必要な場合があります）。ユーザの現在のステータスは「de-activated」です。

図 16：[ユーザの詳細（User Details）] ページ > [ユーザの再アクティブ化（Re-Activate User）]



4. [ユーザの再アクティブ化（Re-Activate User）] をクリックします。ダイアログが表示されて確認を求めます。
5. 確定するには、このダイアログで [ユーザの再アクティブ化（Re-Activate）] をクリックします。

ESA/WSA またはその他の統合先アプライアンスやデバイスは、Threat Grid アプライアンスとの接続を開始できるようになりました。

プライバシーとサンプルの可視性

サンプルを分析するために Threat Grid アプライアンスに送信する場合は、その内容のプライバシーが重要な留意事項になります。機密文書やアーカイブ タイプを分析のために送信する場合は、プライバシーが特に重要な留意事項になります。検索 API と組み合わせると、機密資料を見つけることは、Threat Grid アプライアンスへのアクセス権がある機密資料の場合比較的容易だからです。

Threat Grid にサンプルを送信する際のプライバシーおよびサンプルの可視性モデルは、比較的単純なものになっています。プライベートとしてサンプルを指定しない限り、送信者の組織外部のユーザにサンプルが可視になります。*プライベート* サンプルは、そのサンプルを送信したユーザと同じ組織内にいる Threat Grid ユーザにしか表示されません。

統合のプライバシーと可視性

「 統合」から送信されたサンプルの場合、Threat Grid アプライアンスでのプライバシーおよびサンプルの可視性モデルは変更されます。統合とは、ESA/WSA アプライアンスおよびその他のデバイスなどのシスコ製品またはサードパーティのサービスです（「CSA 統合」という用語は、ESA/WSA およびその他のシスコ アプライアンス、デバイス、および統合されている他のサービスを意味します。つまり、Cisco Sandbox API を介した Threat Grid アプライアンスを使用して登録されています）。

Threat Grid アプライアンスに対するすべてのサンプル送信は、デフォルトでパブリックとして設定されるため、どの組織に所属しているかに関わらず、統合を含む他のあらゆるアプライアンス ユーザが表示できます。

アプライアンスのすべてのユーザが、他のすべてのユーザが送信したサンプルのあらゆる詳細を確認できるということです。

Threat Grid ユーザは、プライベート サンプルを Threat Grid アプライアンスに送信することもできます。この場合、サンプルが可視になるのは、サンプル送信者と同じ組織からの他の Threat Grid アプライアンス（統合を含む）のユーザだけです。

以下の表で、Threat Grid アプライアンスでのプライバシーおよびサンプルの可視性モデルを説明します。

図 17：Threat Grid アプライアンスでのプライバシーと可視性

	Public Submissions (Default)	Private Submissions	Integration Submissions (Public by Default)
Users from Same Org	✔	✔	✔
Users from Different Org	✔	✖	✔
Integrations from Same Org	✔	✔	✔
Integrations from Different Org	✔	✖	✔

緑色のチェックマークは、ユーザがサンプルと分析結果にフル アクセスしたことを意味します。

赤色の「X」は、ユーザがサンプルまたは分析結果にアクセスしていないことを意味します。

同じ基本的なプライバシー ルールが AMP for Endpoints プライベート クラウドと Threat Grid アプライアンスの統合に適用されます。

アプライアンスのワイプ

V1.4.4 には、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 オプションが導入されています。

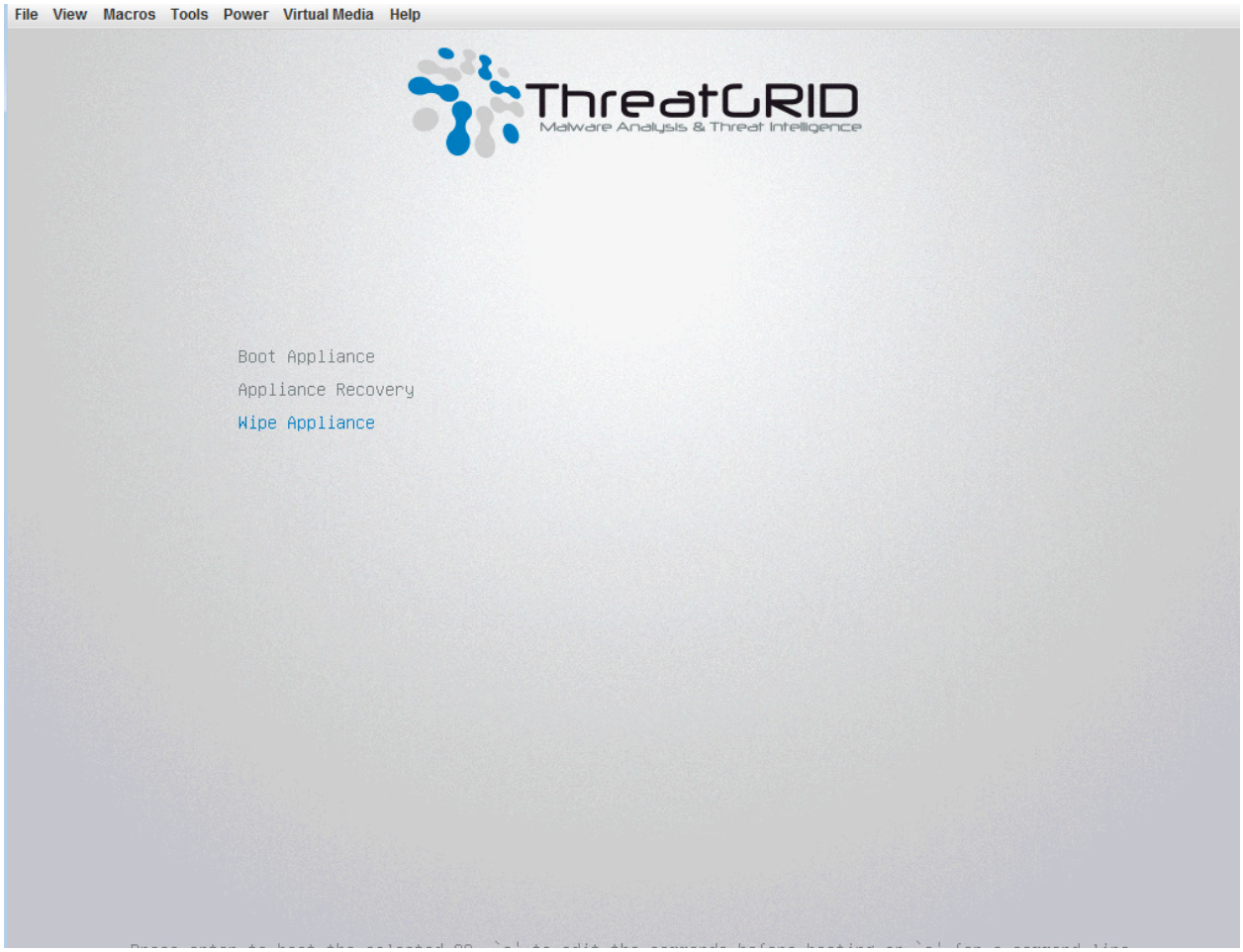
アプライアンスのワイプ オプションを使用すると、アプライアンスの廃止前、または Cisco Demo Loan Program に返却する前に、アプライアンスからすべてのデータを削除できます。このプロセスにはいくつかのバリエーションがあります。中には、高度なテクニックを使用してデータを取得しようという試行に対してセキュリティを強化するために、追加パスを提供しているものもあります。（高度なテクニックを使用しても最近のハード ドライブ エンコーディングには対抗できないと見られているため、最速の単一パスのワイプ オプションであっても安全かつ十分です）

重要：この操作を実行すると、シスコに返却してイメージを再作成しない限り、アプライアンスを運用できなくなることに注意してください。

1. アプライアンスを再起動します。

   起動中、[アプライアンスのワイプ（Wipe Appliance）] を選択できる 4 秒間の時間枠があります。

図 18：アプライアンスのワイプ



2. このオプションには、次のユーザ名とパスワードが必要です。

   ユーザ名：　「wipe」

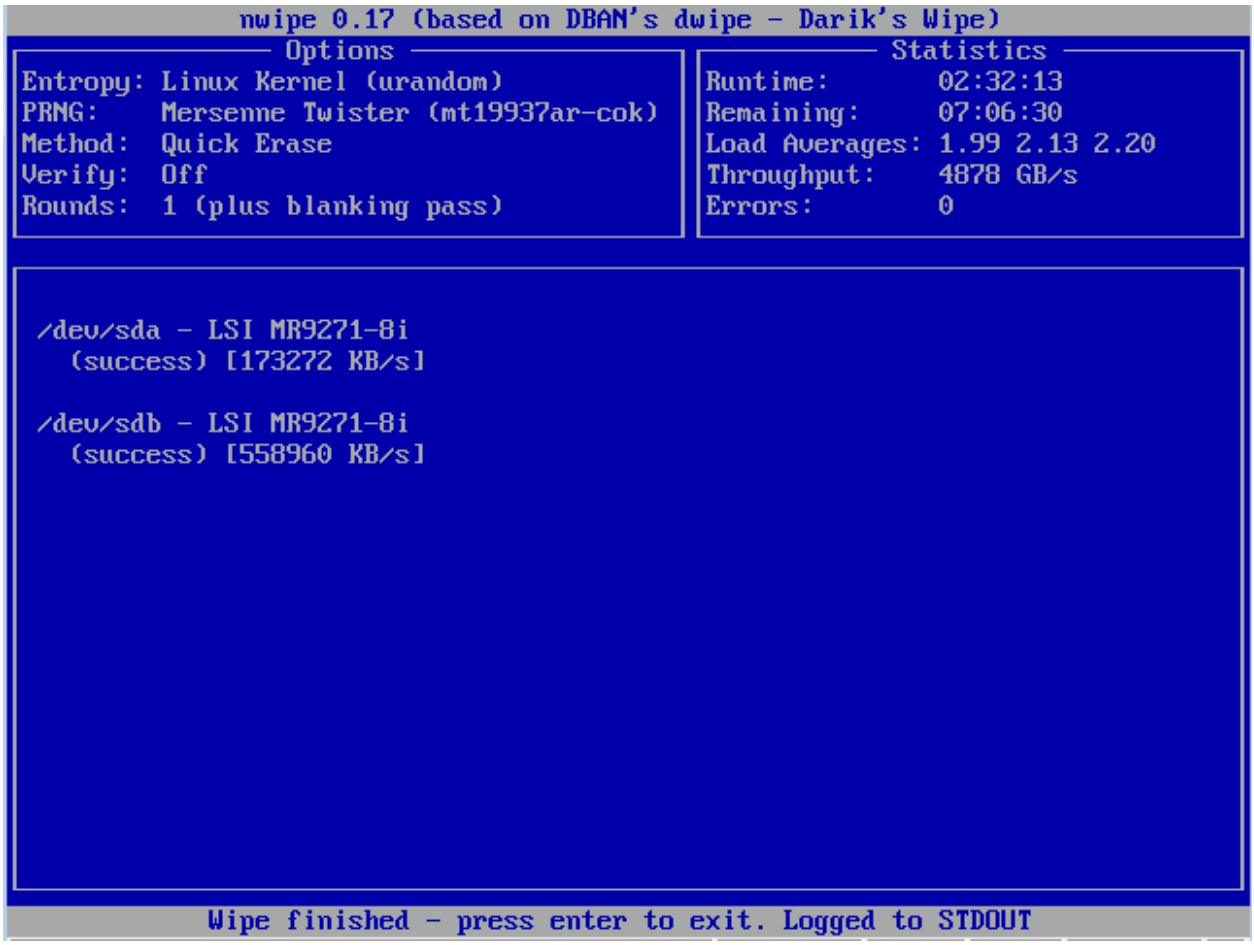
   パスワード：　「I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION」

3. 次に、ワイプのオプションを選択します。次に、ワイプのオプションを選択します。各オプションのおおよその実行時間については、ワイプのオプションを参照してください。

図 19：ワイプ オプション

4. ワイプ操作が完了すると、[Wipe Finished] 画面が表示されます。

図 20：ワイプ終了



5. **Enter** を押して終了します。

ワイプのオプション

ワイプのオプション	おおよその実行時間
Wipe（Fast: Zero Disks)	2.5 時間
Wipe（3-pass DOD method)	16 時間
Wipe（Random Overwrite)	12 時間

バックアップ

2.2.4 リリースには、バックアップの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洩なく顧客構内へ出荷できるように使用されるアプライアンスの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。

コンテンツは gocryptfs、サードパーティのオープン ソース製品を使用して暗号化されます。

パフォーマンス上の理由からそのファイル名の暗号化は無効になります。サンプルと Threat Grid の他のコンテンツはどのような状況下でも元の名前で保存されないため、これによって顧客独自のデータが漏洩することはありません。

ご使用の前に、ドキュメントをよくお読みいただくことを強くお勧めします。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。追加の技術情報と注意事項については、「*Backup Notes and FAQ*」、『*Threat Grid Appliance Setup and Configuration Guide*』を参照してください。いずれも Cisco.com の 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のページ**で利用できます。

NFS 要件

- アプライアンスの管理インターフェイスからアクセス可能な、TCP を介した NFSv4 プロトコルを実行する必要があります。
- 設定されているディレクトリは、nfsnobody（UID 65534）で書き込み可能である必要があります。
- NFSv4 サーバは、Admin 10 Gb インターフェイスを介してアクセスできる必要があります。
- 十分なストレージ。詳細については、以下の「バックアップ ストレージ要件」を参照してください。
- 次のマウント パラメータが無条件で使用されます。`rw`、`sync`、`nfsvers=4`、`nofail`
  注：これらのパラメータは、手動で入力する必要はありません。それらと競合するパラメータを手動で入力すると明示的にサポート対象外になり、定義されていない動作を引き起こす可能性があります。
- 無効な NFS 設定（または、誤って設定されている NFS サーバでのサービスを示している設定）をすると、通常、設定を適用するプロセスが失敗します。OpAdmin でのこの設定を修正して再適用すると成功します。
- `nfsnobody` による書き込みへのファイルの公開は安全です。`nfsnobody` として実行する Threat Grid アプライアンスまたは `nfsnobody` への書き込みでのプロセスのみ、データの暗号化を使用します。プレーンテキスト データは、最小限の権限の原則に基づいて異なるサブツリーの明確なユーザ アカウントで公開されます。アプライアンス上の PostgreSQL サービスは Elasticsearch データまたはフリーザにアクセスできません。Elasticsearch サービスは PostgreSQL またはフリーザのデータにアクセスできません。
- `nfsnobody` アカウントを使用して設定を簡素化し、各顧客のサイト マッピングのローカルおよびリモートのアカウント名に対して、`idmap.conf` を構築する必要がなくなるようにします。

バックアップ ストレージ要件

バックアップ ストアは、次のコンポーネントで構成されています。

オブジェクト ストア。実際には、一般的にこれが使用するストレージの大部分になります。バックアップ ストアの一括コンポーネントに対するデータ保存は、使用するアプライアンス リリースのドキュメント化したものと同じポリシーと制限に従っています。2.2.x シリーズのアプライアンスの場合、http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-data-retention-v2-2.pdf のドキュメントが適用可能で、このコンポーネントの最大ストレージ使用量は 4.1 TB と見なされます。

PostgreSQL データベース ストア。これには、PostgreSQL ストアの 2 つの完全バックアップと、保持された完全バックアップの一番古いものから再生するために十分な一連の WAL ログが含まれます。これは、合計で 500 GB 未満である必要があります。

Elasticsearch スナップショット ストア。これは、合計で 1 TB 未満である必要があります。

合計ストレージ。したがって、上記に示すように、バックアップ ストアには **5.6 TB を超える必要はありません**。

期待事項

バックアップに含まれる：Threat Grid アプライアンスのバックアップ プロセスの最初のリリースには、次の顧客独自の一括データが含まれます。

- サンプル
- 分析結果、アーティファクト、フラグ付き
- アプリケーション層の（OpAdmin ではない）組織およびユーザ アカウントのデータ。
- データベース（ユーザおよび組織を含む）
- Face または Mask ポータルの UI 内で行われた設定

含まれない：

- システムログ
- 以前にダウンロードおよびインストールした更新
- このリリースには、SSL キーと CA 証明書を含むアプライアンス OpAdmin インターフェイス内部で行われた設定は含まれません

PostgreSQL：PostgreSQL ベース バックアップは 24 時間サイクルで処理を行います。データベースのバックアップの復元はできません。少なくとも 1 回正常に完了するまで警告が表示されます。

Elastisearch：Elasticsearch バックアップは、5 分ごとに 1 回、段階的に行われます。

Freezer：Freezer バックアップは、進行中のバックアップから失われたオブジェクトに対処するために、24 時間ごとに、背後で行われるジョブとともに継続的に処理を行います。

新しいキーの生成：新しいキーの生成によって、独立したバックアップ ストアを新しく作成します。オリジナルのように、この新しいストアは、24 時間サイクルのベース バックアップが行われるまで有効になりません。

バックアップ データの保持

PostgreSQL：PostgreSQL の場合、最後の 2 つの正常なバックアップおよびこれらのバックアップ以後のすべての WAL セグメントは保持されます。

Elasticsearch：Elasticsearch の場合、最後の 2 つの 5 分間のスナップショットが保持されます。

一括ストレージ:一括ストレージの場合、単一のアプライアンスに従ってドキュメント化された同じ保持ポリシーは共有のストアに使用されます。

履歴データを長期間保持するお客様には、ファイルシステム層またはブロック層のスナップショット サポートによる NFS サーバをご使用いただくことを強く推奨します。

バックアップ プロセスの概要

Threat Grid アプライアンスでのバックアップ プロセスは、次の手順で構成されます。

手順 1 上記の NFS 要件に従ってバックアップ ターゲット ディレクトリを作成します。

手順 2 『Threat Grid Appliance Setup and Configuration Guide』の説明に従って、OpAdmin のセットアップ ウィザード（[設定（Configuration）] > [NFS]）の NFS 設定ページを完了します。

手順 3 NFS 設定を完了したら、生成される暗号キーをダウンロードします。

特記事項：お客様の責任において、暗号キーのバックアップを取り、安全に保存してください。

Threat Grid のコピーは保持されません。

バックアップはこのキーがないと使用できません。

手順 4 バックアップの復元ターゲットをリセットします。（手順については、「*バックアップの復元ターゲットとしての Threat Grid アプライアンスのリセット*」を参照してください。）

手順 5 バックアップ データを復元します。(手順 3 から暗号キーが必要になります。手順については、「*バックアップの内容の復元*」を参照してください。）

手順の詳細については、次のセクションを参照してください。

バックアップ頻度

サンプル、アーティファクトとレポートの一括ストレージの場合、コンテンツは継続的にバックアップされます。さらに、パスが実行されると、24 時間サイクルで不足しているコンテンツが検索されて転送されます。

PostgreSQL データベースの場合、24 時間サイクルでベース バックアップが作成され、その後、新たに書き込まれたデータベースのコンテンツのしきい値が 16 MB に達するとすぐに、または少なくとも 5 分ごとに増分コンテンツが継続的に追加されます。

Elasticsearch データベースの場合、コンテンツはバックアップ ストアに 5 分間サイクルで段階的に追加されます。

バックアップ頻度を制御したり調整することはできません。これらの値を調整してストレージ使用率、復元処理時間、および無効なパフォーマンスのオーバーヘッドに関して予測するときは、調整できなくなります。

バックアップの復元ターゲットとしての Threat Grid アプライアンスのリセット

注意! このプロセスを利用すると、顧客独自のデータが中断されます。十分注意してください。すべてのタスクを実行する前にドキュメントのすべてに目を通してください。

アプライアンスを復元ターゲットとして使用する前に、事前設定された状態にする必要があります。アプライアンスは、この状態で出荷されます。ただし、設定した後に事前設定された状態に戻すには、明示的な管理操作が必要になります。（詳細については、*バックアップの復元ターゲットとしての Threat Grid アプライアンスのリセット* を参照してください）。

注：リセットは回復モードで利用可能なセキュリティで保護されたワイプと同じではありません。回復モードのセキュリティで保護されたワイプのみが、DLP reimaging center に出荷する前にマシンから顧客独自のデータを完全に削除するのに適しています。ただし、回復モードでセキュリティで保護されたワイプはこのリセットに置き換えられません。セキュリティで保護されたワイプは再度イメージ化されるまで使用不可なアプライアンスをレンダリングします。その間、このリセットはバックアップを復元するためのアプライアンスを準備します。

システムに対して復元しない場合は、製造元から更新してください。

復元ターゲットのアプライアンスは、既存のデータと、システムからの NFS 関連の設定をオフにして事前設定された状態に戻す必要があります。

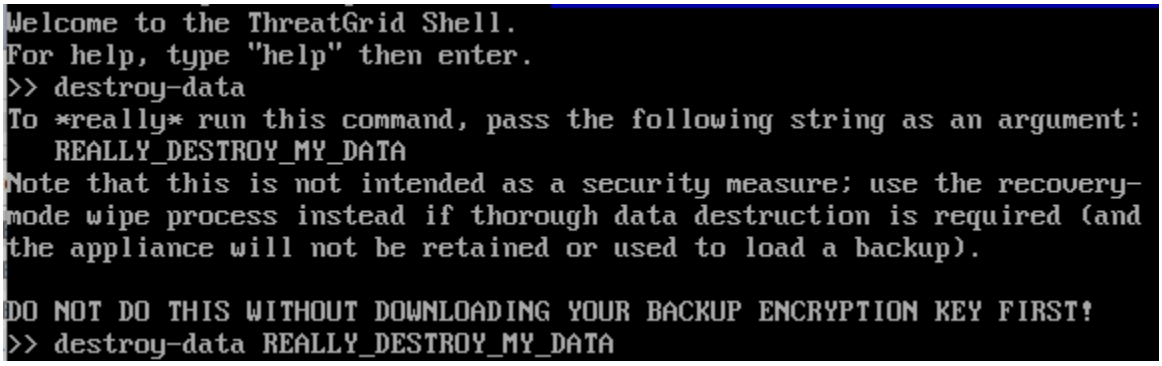
a) アプライアンスの TTY または SSH のいずれかを介して `tgsh-dialog` 設定インターフェイスにアクセスします。

b) [コンソール（CONSOLE）] オプションを選択して、tgsh を入力します。（回復モードを介した tgsh の入力は、この使用例には適していません。）

c) `tgsh` プロンプトで、コマンド `destroy-data` を入力します。プロンプトをよく読んで、指示に従ってください。

注意! このコマンドで元に戻す操作はありません。

図 21：destroy-data REALLY_DESTROY_MY_DATA コマンドと引数



次のデータが破棄されます。

- サンプル
- 分析結果、アーティファクト、フラグ付き
- アプリケーション層の（OpAdmin ではない）組織およびユーザ アカウントのデータ。
- データベース（ユーザおよび組織を含む）
- Face または Mask ポータルの UI 内で行われた設定
- NFS 設定と資格情報。
- NFS に使用される暗号キーのローカル コピー。

別のシステムが復元されるバックアップにアクティブに作成している場合：

（たとえば、これが、1 秒ごとに書き込まれるコンテンツのテスト復元の場合、マスター アプライアンスは実稼働でアクティブに使用されます。）

データストアの一貫性のある、書き込み可能なコピーを生成し、継続的に書き込まれているストアではなくこの書き込み可能なコピーにテスト復元を実行しているアプライアンスをポイントします。

アプライアンスが事前設定された状態の場合、次のセクションで説明されているように、バックアップ ストアのターゲットとして機能します。

バックアップの内容の復元

特記事項：システムは、復元プロセス中にサンプル送信に使用することはできません。

必須：暗号キー。

バックアップの暗号キーのアップロード：

OpAdmin のセットアップ ウィザードの [NFS 設定（NFS Configuration）] ページ（[設定（Configuration）] > [NFS]）で、[アップロード（Upload）] をクリックして、バックアップが作成されたサーバを設定するときに以前生成されたバックアップ キーを取得します。

- キーがバックアップを作成するために使用されたキーと正確に一致する場合、アップロードが設定されたパスのディレクトリ名と一致した後、キー ID が OpAdmin に表示されます。
- インストール ウィザードでは、バックアップ キーと一致するディレクトリをチェックし、検出されると、その場所にデータの復元を開始します。
- **必要な時間：**データの復元に必要な時間の量は、バックアップの *サイズとその*他の要因によって異なります。テストでは、1.2 GB の復元は簡単であっという間ですが、1.2 TB の復元には 16 時間以上必要です。
- 注：経過表示バーが存在しないため、時間のかかる復元では、インストールがハングして表示される可能性があります。しばらくお待ちください。OpAdmin で復元に成功したことが報告されると、アプライアンスが起動します。
- 復元されたデータは、元データと非常に似ています。

バックアップの復元に関する注記

復元プロセス中にサンプル送信を使用することはできません。

バックアップは、セットアップ ウィザードからのみ復元できます。

以前に使用したものと同じ NFS ストアと、以前に使用したものと同じ暗号キーを、元と同じプロセスで設定します。

以前の NFS ストアおよび暗号キーを使用してアプライアンスを設定する操作で、復元キーがトリガーされます。

特記事項:指定したアクティブなバックアップ ストアのデータを使用して一度に実行することができるのは 1 つのサーバのみです。

プライマリ アプライアンスが動作している間にさまざまな Threat Grid アプライアンスで復元プロセスをテストするには、バックアップ ストアの一貫したスナップショットのコピーを作成し、そのコピー上で（アップロードされた暗号キーを使用して）新しいアプライアンスをポイントします。

バックアップに関連するサービスの通知

ネットワーク ストレージがマウントされていません。バックエンドとして使用されているネットワーク ファイルシステムが完全に動作していることを確認して、OpAdmin を介して設定を再適用するか、アプライアンスを再起動します。

ネットワーク ストレージが動作していません。バックエンドとして使用されているネットワーク ファイルシステムが完全に動作していることを確認します。システムが NFS サーバの問題の修正に 15 分以内で回復しない場合は、アプライアンスを再起動してください。

バックアップ ファイルシステムのアクセスに失敗しました。カスタマー サポートに連絡してください。

PostgreSQL のバックアップが見つかりません：これは、バックアップ ストアが設定された時間内のポイントと（自動的に 24 時間サイクルで実行される）最初のベース バックアップが行われる時間内のポイント間で正常な状態です。これが完了するまで、バックアップ完了とは見なされず、復元することはできません。このメッセージが 48 時間を超えて続く場合または続く場合に限り、カスタマー サポートに連絡してください。

最新の PostgreSQL ベース バックアップは 3 日以上前です：これはシステムが PostgreSQL の新しいベース バックアップの生成に成功していないことを示します。修正されない場合、（古くなりつつあるバックアップ ポイントから復元するために必要な書き込みの完全なチェーンを保持するための）バックアップ ストアでの使用が制限されなくなり、行われる復元に必要な処理時間が許容できる長さを超えます。カスタマー サポートに連絡してください。

バックアップの作成メッセージ：バックアップを開始またはトリガーしたときにこれらのリフレクト エラーが検出されました。

非アクティブの ES バックアップ（作成）：Elasticsearch が開始して、バックアップ ストアが使用不可能であることを示します。これは、アプライアンスを再起動することで、または（NFS および暗号化サービスが機能している場合）tgsh にログインし、コマンド `service restart elasticsearch.service` を実行することで改善できます。

バックアップのメンテナンス メッセージ：以前に作成されたバックアップのステータスを確認するときにこれらのリフレクト エラーが検出されました。

ES バックアップ（メンテナンス）スナップショット（...）ステータスの失敗：これは、Elasticsearch データベースのバックアップの最近の更新で、インデックスが正常に書き込まれなかったことを示します。NFS サーバが機能していて空き領域があることを確認します。問題を特定できず、解決しない場合は、カスタマー サポートにお問い合わせください。

ES バックアップ（メンテナンス）スナップショット（...）ステータスの互換性なし：アプライアンス更新で新しいバージョンの Elasticsearch をインストールしたすぐ後にのみ発生します。バックアップ ストアがこの新しいリリースと互換性があるようにアップグレードされるまで表示されます。カスタマー サービス サポートが必要になる可能性がある互換性のないバックアップからの復元は、この状態の間にエラーが発生する必要があります。

ES バックアップ（メンテナンス）スナップショット（...）ステータスの一部：本文に 2 つのメッセージのいずれかを含みます。以前の成功したバックアップが見つからないため、保持します。（まったくないよりはよい部分的なバックアップを保持している場合）または以前の成功したバックアップが存在するため、削除します。（しばらくしてから再試行するためにその部分バックアップを破棄している場合）

ES バックアップ（メンテナンス）：バックアップに（...）秒必要：バックアップには 60 秒を超える時間が必要な場合に発生します。これは必ずしもエラーとは限りません。Elasticsearch では定期的なメンテナンスを実行し、これがアイドル状態のシステムにも重要な書き込み負荷を発生させることがあります。ただし、これが負荷が少ない期間で一貫して発生する場合は、ストレージ パフォーマンスを調査するか、サポートが必要な場合はカスタマー サービスに連絡してください。

ES バックアップ（メンテナンス）：Elasticsearch スナップショット ステータスのクエリを実行できません： Elasticsearch に接続できませんでした。バックアップの作成が正常に開始した後にこの障害が発生します。一般に、他のアプライアンスの障害と同時に発生するため、それらの問題の修復に重点を置く必要があります。アプライアンスが他の点では完全に機能しているときにこのエラーが発生し、自分では解決できない場合は、カスタマー サポートに問い合わせてください。

クラスタリング

複数の Threat Grid アプライアンスをクラスタ化する機能は、早期のフィールド トライアルの v2.4.0 で導入され、v2.4.2 で一般的に使用可能な機能となりました。

クラスタ内の各アプライアンスが共有ファイル システムにデータを保存することで、クラスタ内の他のノードで同じデータを共有することができます。

目標

クラスタリングの主な目標は、2 ～ 7 のノードで構成されるクラスタに一緒にいくつかのアプライアンスを結合することで、単一のシステムの容量を増やすことです。

その他の目標は、クラスタのサイズに応じて、クラスタの 1 つまたは複数のマシンの障害を回復するサポートをすることです。

> **ご質問がある場合カスタマー サポートへの連絡：**データを破損する可能性がある誤りを回避するために、クラスタのインストールまたは再設定をする際のアクティブな操作について、ご質問が***ある場合はカスタマー サポートにご連絡ください***。

機能

- **共有データ：**スタンドアロンの場合はクラスタ内のすべてのアプライアンスを使用できます。すべてが同じデータにアクセスしてそのデータを表示することができます。
- **サンプル送信処理：**送信されたサンプルは、クラスタ メンバーのいずれかで他のメンバーとともに処理され、分析結果を表示することができます。
- **レート制限：**各メンバーの送信レート制限がクラスタの制限になるまで追加されます。
- **クラスタ サイズ：**推奨されるクラスタ サイズは、3、5、または 7 のメンバーです。2、4、6 のノード クラスタがサポートされていますが、可用性の特徴により、次のサイズの低下したクラスタ（つまり、1 つまたは複数のノードが動作しないクラスタ）に似ています。
- **条件：**クラスタに偶数のノードを含めるように設定すると、条件として指定された 1 つによって、どのノードがプライマリ データベースを決定するかを選ぶときに「第 2 投票」を取得します。

  クラスタ内の各ノードにはデータベースが含まれていますが、プライマリ ノードのデータベースのみが実際に使用されます。プライマリ ノードがダウンした場合は他のノードがその役目を引き継ぎます。条件を設定していると、ノードがちょうど半分失敗したとき、ただし、条件が失敗したノード上ではない場合のみ、クラスタがダウンするのを防止できます。

  奇数クラスタには、関連付けられた投票はありません。奇数クラスタでは、条件ロールのみ、ノード（条件ではない）がクラスタからドロップされる場合に関連をもちます。その後、クラスタは偶数になります。

  注：この機能は 2 ノードのクラスタのみに完全にテストされます。

制限事項

- 既存のスタンドアロン アプライアンスのクラスタを作成するとき、第 1 ノード（最初のノード）のみがそのデータを保持できます。他のノードは、クラスタに既存のデータをマージすることが許可されていないために手動でリセットする必要があります。以前にドキュメント化された `destroy-data` コマンドを使用して既存のデータを削除します。（ワイプ アプライアンスを使用しないでください。イメージの再作成のためにシスコに返されるまでアプライアンスは操作不能になります。）
- ノードを追加または削除すると、クラスタのサイズとメンバー ノードのロールによって、短時間停止することがあります。
- M3 サーバのクラスタリングはサポートされていません。ご質問がある場合は、support@threatgrid.com までお問い合わせください。

要件

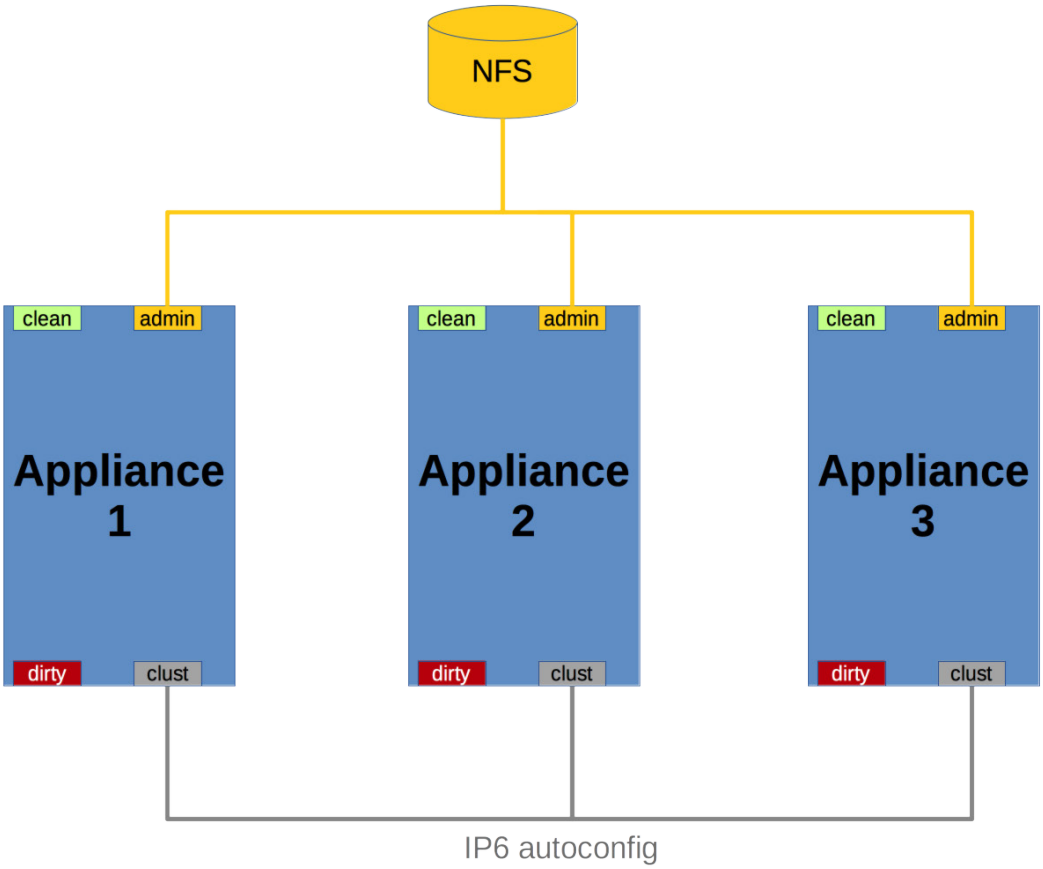
- **バージョン：**すべてのアプライアンスで同じバージョンを実行し、サポートされている設定でクラスタを設定して、常に最新のバージョンを使用可能にする必要があります。
- **Clust インターフェイス：**各 Threat Grid アプライアンスには、それぞれの Clust インターフェイス スロットにインストールされている（スタンドアロン アプライアンスに含まれていない）SFP+ を使用した、そのクラスタの他のアプライアンスに対する直接相互接続が必要です。このコンテキストの「直接」は、すべてのアプライアンスが、同じレイヤ 2 のネットワーク セグメント上にあり、他のノードに到達するために必要なルーティングがなく、さらに大きな遅延またはジッターがないことを意味します。ノードが単一の物理ネットワーク セグメント上にないネットワーク トポロジはサポートされていません。
- **非推奨のエアギャップされた導入：**デバッグの複雑さが増大したために、アプライアンス クラスタリングは、エアギャップされた導入または顧客がデバッグにアクセスする L3 サポートを提供できないまたは希望しない他のシナリオでは推奨されません。
- **データ：**データが含まれていない場合、アプライアンスのみがクラスタに結合される可能性があります。（最初のノードのみにデータを含めることができます。）既存のアプライアンスをデータのない状態に移動するには、アプライアンス 2.2.4 に追加されたデータベースのリセット プロセスを使用する必要があります。

  1.4.3 に追加されたワイプ アプライアンスの破壊プロセスを使用しないでください。（ワイプ アプライアンスではすべてのデータのみを削除するだけでなく、イメージの再作成のためにシスコに返されるまでアプライアンスは操作不能になります。）
- **SSL 証明書：**顧客が 1 つのクラスタ メンバーにカスタム CA によって署名された SSL 証明書をインストールしている場合、その他のすべてのノードの証明書は、同じ CA によって署名される必要があります。

ネットワーキングと NFS ストレージ

- Threat Grid アプライアンス クラスタには、有効になっていて設定済みの NFS ストアが必要です。管理インターフェイス経由で使用可能である必要があり、すべてのクラスタ ノードからアクセス可能である必要があります。
- 各クラスタは、キーが 1 つある 1 つの NFS ストアによってバックアップする必要があります。その NFS ストアを既存のアプライアンスからのデータで初期化する間、クラスタが動作している間クラスタのメンバーではないシステムによってアクセスされないようにする必要があります。
- NFS ストアはシングル ポイントの障害であり、そのロールに対して使用されていない、信頼性の高い機器を使用することが絶対に必要です。

図 22：ネットワーク構成図のクラスタリング



クラスタの構築の概要

サポートされる方法でクラスタを構築するには、すべてのメンバーが同じバージョンにあることが必要です。常に最新バージョンにする必要があります。これは、すべてのメンバーが完全に更新されるように最初にスタンドアロンを構築する必要があることを意味します。アプライアンスが前にスタンドアロン マシンとして使用している場合、最初のメンバーのデータのみを保持できます。その他は構築の一部としてリセットする必要があります。

最初のノードで新しいクラスタを開始し、他のアプライアンスを結合します。

新しいクラスタを開始するために使用できる 2 つの異なるパスがあります。

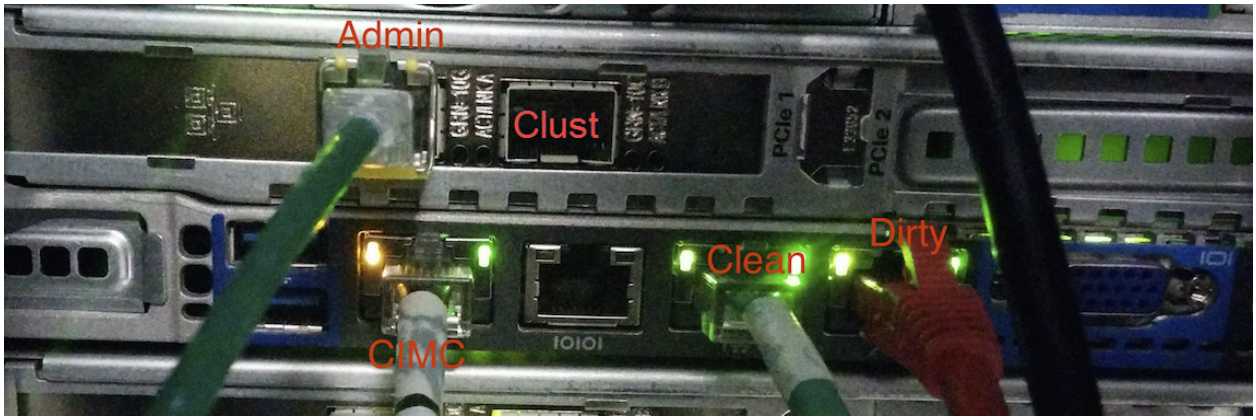
- 既存のスタンドアロン アプライアンスを使用した新しいクラスタの開始
- 新しいアプライアンスを使用した新しいクラスタの開始

Clust インターフェイスの設定

必須：クラスタの各アプライアンスには、Clust インターフェイスの追加の SFP+ が必要です。

以前にラベル化された**予約済み**の 4 つ目（非管理者）の SFP ポートの SFP+ モジュールをインストールします。次の 2 つの図に示すように、**Clust** インターフェイスに使用されます。

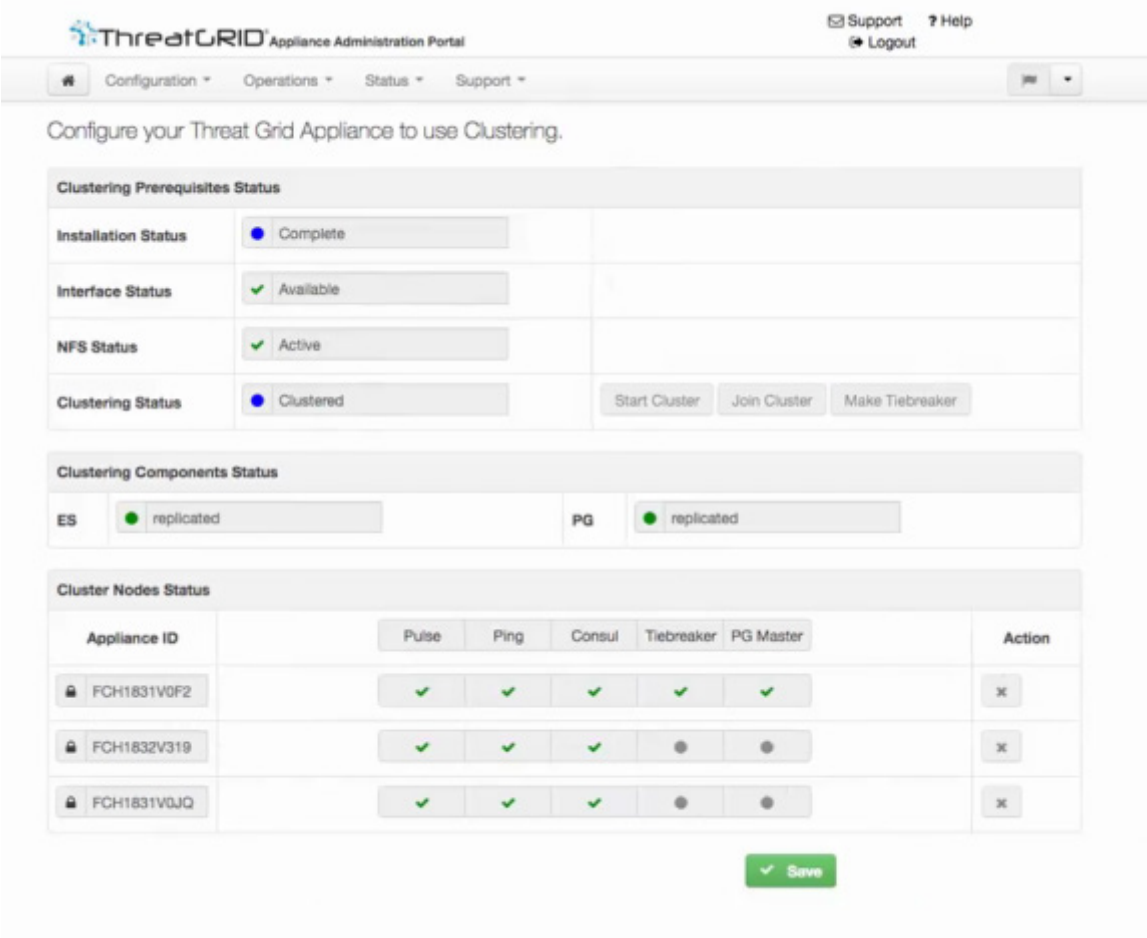
図 23：Cisco UCS M4 C220 の Clust インターフェイスの設定



[クラスタリング（Clustering）] ページ

クラスタは、OpAdmin の [Clustering（クラスタリング）] 設定ページ（[設定（Configuration）] > [クラスタリング（Clustering）]）で設定および管理されます。次の図は、3 ノード、アクティブ、正常なクラスタを示しています。

図 24：アクティブ クラスタのクラスタリング ページ



前提条件ステータスのクラスタリング

インストール ステータス アプライアンスのインストール ステータス。**完了にする必要があります**。アプライアンスは、完全に設定して構成する必要があります。

インターフェイス ステータス：クラスタリングのネットワーク インターフェイスのステータス「Clust」。

NFS ステータス：NFS は使用可能である必要があります。

クラスタリング ステータス：アプライアンスがクラスタ ノードまたはスタンドアロンかどうかを示します

- **スタンドアロン（保存されていない）**：アプライアンスは、明示的にクラスタの一部またはスタンドアロン ユニットのいずれかとして設定されていません。初期設定ウィザードとクラスタリングの前提条件が一致する場合、このシステムがクラスタ化されているかどうかの選択をすることが可能です。
- **スタンドアロン**：スタンドアロン ノードとして設定されています。リセットなしでクラスタの一部として設定することはできません。
- **クラスタ化**：アプライアンスが他の 1 つまたは複数のアプライアンスでクラスタ化されます。

コンポーネント ステータスのクラスタリング

ES：Elasticsearch。検索機能を必要とするクエリに使用されるサービス。

PG：PostgreSQL。最新の最終データ（アカウント ルックアップなど）が必要なクエリに使用されるサービス。

両方のサービスは、次のステータス値のいずれかで説明されます。

- **複製済み**：すべてが正常に動作しています。また、障害時に引き継ぎに必要なすべてのものも所定の位置にあります。アプライアンスは障害を許容して操作を続行できます。「複製済み」状態は、障害のダウンタイムがゼロであるという意味ではありません。むしろ、障害には、ゼロのデータ損失と制約ダウンタイムが伴います（通常の状況で 1 分未満、失敗した特定のクラスタ ノードでのアクティブな分析を除く）。

  ノードがダウンするメンテナンス操作は、クラスタが複製された状態のときにのみ実行する必要があります。

  完全に複製されたクラスタの場合、リカバリは自動的に行われ、通常のシナリオで完了するのに必要な時間は 1 分未満です。

- **利用可能**：すべてが正常に動作して、参照サービスを使用できます（つまり、API およびユーザ要求を処理できます）が、複製されません。

- **利用不可**：サービスは機能していません。

（詳細については、*Threat Grid アプライアンス製品のドキュメントのページ*で公開せれている「*Clustering FAQ*」を参照してください。）

ステータスの色：

- **緑色**：複製済み
- **黄色**：利用可能
- **赤色**：利用不可
- **灰色**：不明

クラスタ ノード ステータス

Pulse：（初期設定中ではなく、サービスを実行している間に）ノードがアクティブに接続されていて、NFS ストアを使用したかどうかを示します。

Ping：クラスタ ノードが「Clust」インターフェイス上で確認できるかどうかを説明します。

Consul：ノードがコンセンサス ストアに参加しているかどうかを示します。これには、「Clust」上のネットワーク接続と互換性のある暗号キーの両方が必要です。

緑色のチェックマークは、実行中と正常な状態を示します。

赤色の「X」は、一般に、何かがまだ実行されていないか、または正常な状態ではないことを意味します。

条件：「条件」としてノードを指定します。クラスタのプライマリ ノードを決定するための選択で決定する投票をキャストします。

スタンドアロンの保持：アプライアンスがクラスタにノードとして設定されていないことを示します。このオプションを選択すると、ユーザは非クラスタ化のアプライアンスに OpAdmin 設定ウィザード プロセスの残りの部分を完了できます。

既存のスタンドアロン アプライアンスによるクラスタの開始

クラスタを開始するこの方法を使用すると、ユーザは 1 つのマシンからの既存のデータを保持し、それを使用して新しいクラスタを開始できます。これには、クラスタを開始する NFS に存在するように既存のバックアップが必要です。

注：クラスタに結合されているその他のノードはすべて、結合する前にそのデータを削除する必要があります。つまり、追加したノードからのデータをクラスタにマージすることはできません。

注：v2.4.3.3 より前のリリースでは、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。顧客が v2.4.3.3 以降にアップグレードしてから、（以前のリリースでアプライアンスを受信する）新しいクラスタを初期化する前にリセット操作を実行することをお勧めします。

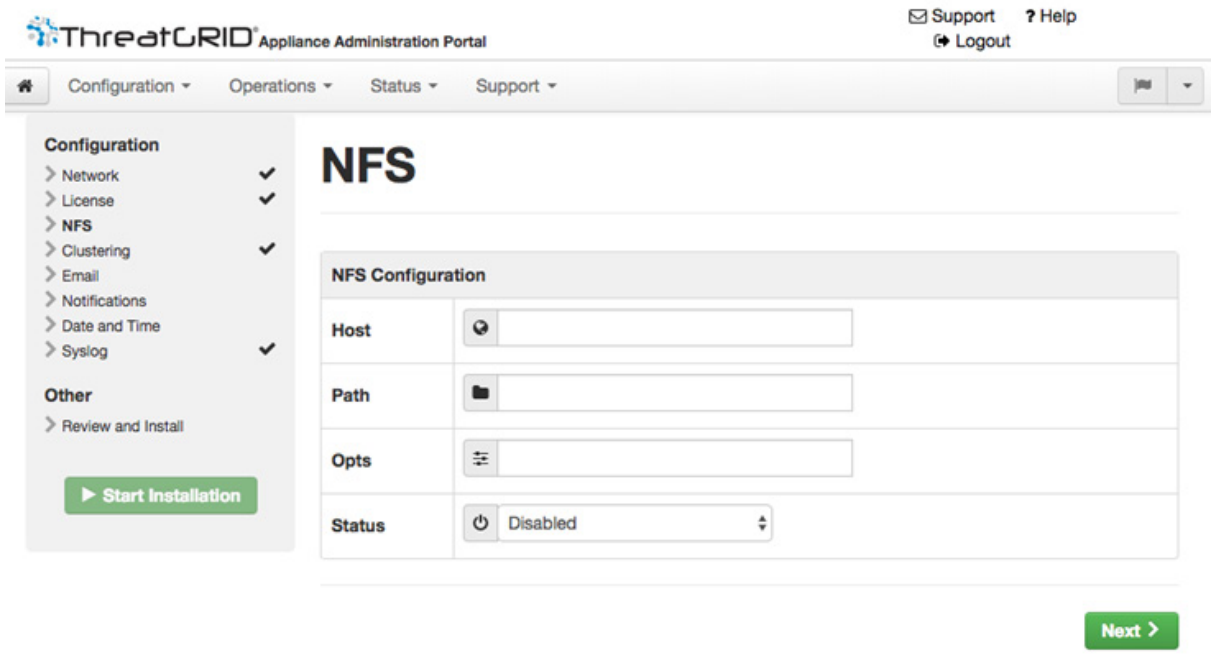
第 1 ノードの詳細な手順：

1. 最新バージョンにアプライアンスを完全に更新します。現在実行しているバージョンによって、最新のものにするために複数の更新サイクルが必要になる場合があります。
2. 完了していない場合は、この手順で説明しているように NFS にマシンのバックアップを設定します。

   注：このセクションでは、デフォルトの Linux NFS サーバの実装を説明しています。サーバの設定によっては調整が必要になる場合があります。

   OpAdmin（[設定（Configuration）] > [NFS]）でセットアップ ウィザードの *NFS* の設定ページを完了します。

図 25：NFS の設定ページ：



2.1 NFS の [ホスト（Host）] および [パス（Path）] を設定し、[ステータス（Status）] ドロップダウンから [有効化（保留中のキー）（Enabled（Pendign Key））] を選択します。

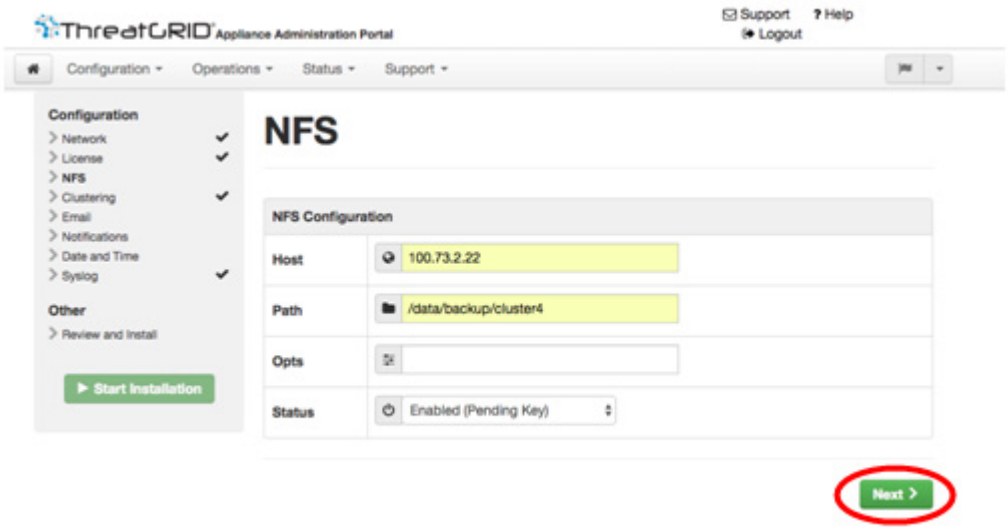
ホスト（Host）：NFSv4 ホスト サーバ。IP アドレスを使用することをお勧めします。

パス（Path）：ファイルを保存する NFS ホスト サーバ上にある絶対パス。これにはキー ID サフィックスは含まれません。自動的に追加されます。

オプション（Opts）：このサーバで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウント オプション。

ステータス（Status）：ドロップダウンから [有効化（保留中のキー）（Enabled（Pendign Key））] を選択します。

図 26：[NFS 設定（NFS Configuration）] の [有効化（保留中のキー）（Enabled（Pendign Key））]



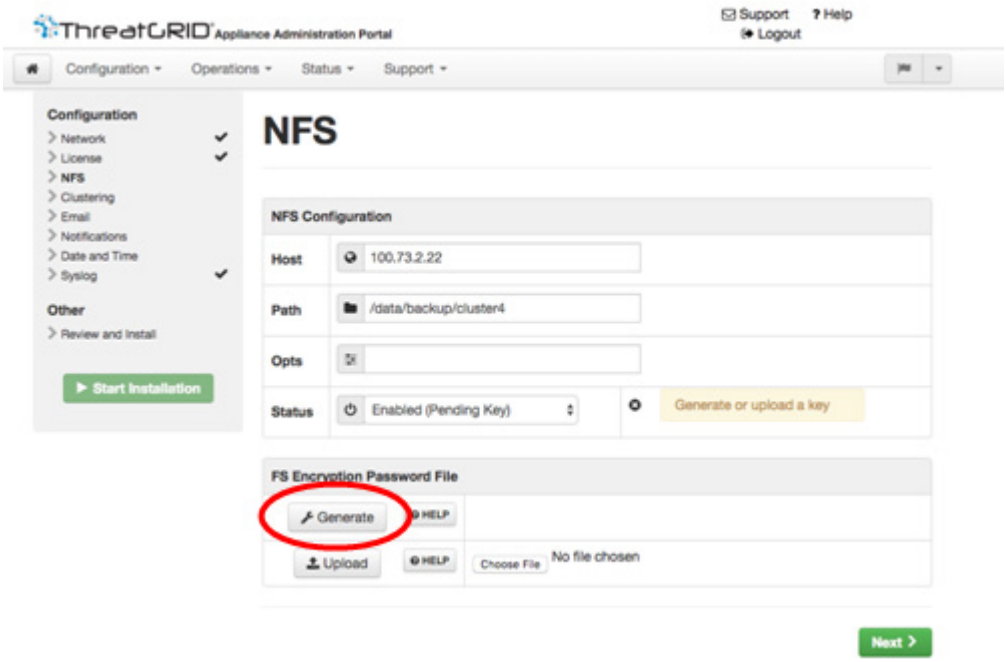
2.2 [次へ（Next）] をクリックします。ページがリフレッシュされます。[作成（Generate）] ボタンが使用できるようになります。

このページを最初に設定するときに、暗号キーを削除または**ダウンロード**するオプションが表示されます。NFS が有効になっているがキーが作成されない場合は、[アップロード（Upload）] を使用できます。

キーを作成すると、[アップロード（Upload）] が [ダウンロード（Download）] ボタンに変わります。（キーを削除すると、[ダウンロード（Download）] ボタンが再び [アップロード（Upload）] になります。）

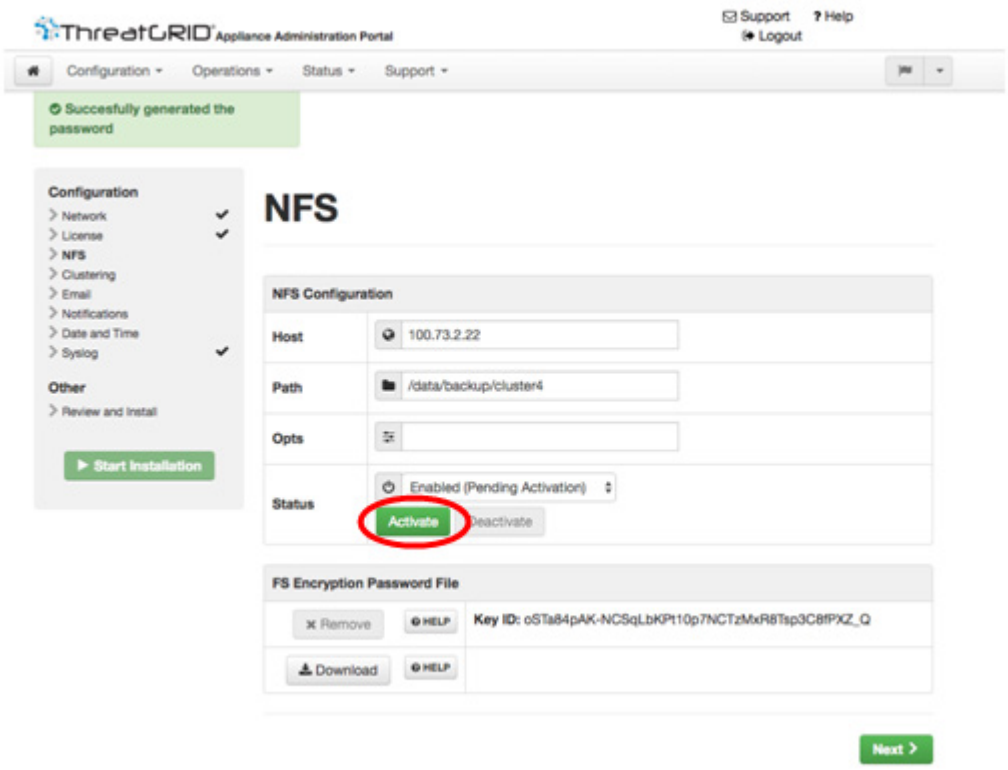
注：キーがバックアップを作成するために使用されたキーと正確に一致する場合、アップロードが設定されたパスのディレクトリ名と一致した後、キー ID が OpAdmin に表示されます。暗号キーを使用せずにバックアップを復元することはできません。設定プロセスには、NFS ストアおよび暗号化データをマウントするプロセスと、NFS ストアのコンテンツからアプライアンスのローカル データストアを初期化するプロセスが含まれます。

図 27：新しい NFS 暗号キーの生成



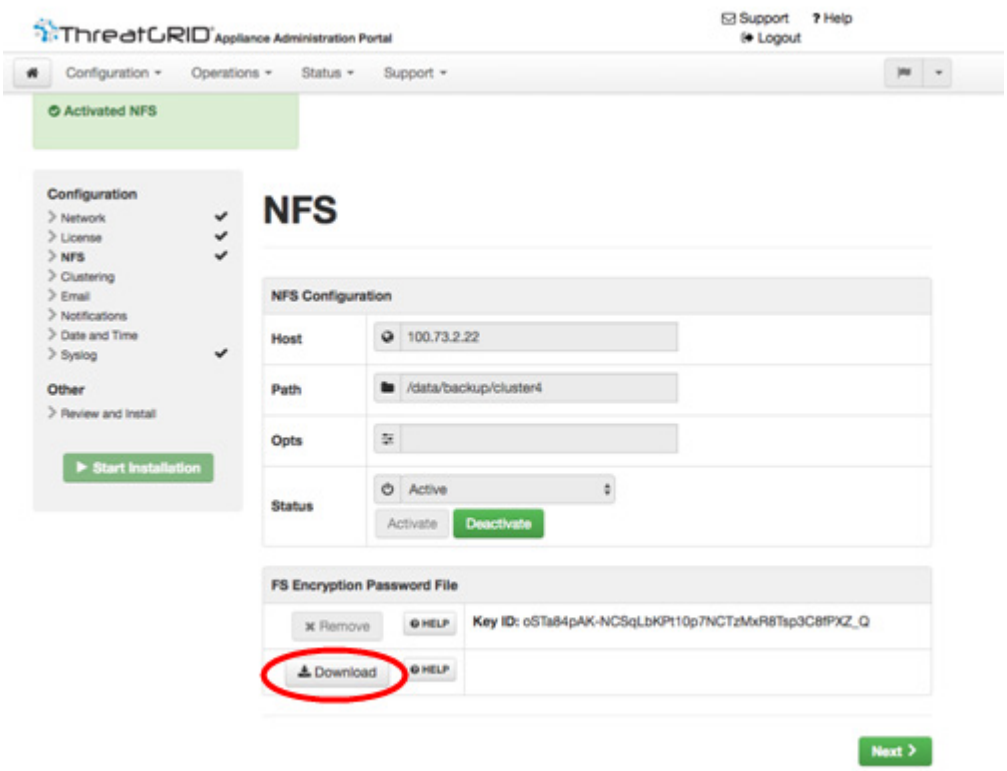
2.3 [生成（Generate）] をクリックして、新しい NFS 暗号キーを生成します。[次へ（Next）] をクリックします。ページがリフレッシュされます。キー ID が表示されて、[アクティブ化（Activate）] と [ダウンロード（Download）] が利用可能になります。

図 28：[NFS 設定（NFS Configuration）] のアクティブ化



2.4 [アクティブ化（Activate）] をクリックします。これには数秒かかります（ステータス インジケータは左下隅にあります）。ステータスが [アクティブ（Active）] になります。

図 29：NFS の [アクティブ（Active）]



2.5 [ダウンロード（Download）] をクリックして、バックアップ暗号キーをダウンロードします。安全な場所に生成したファイルを保存します。クラスタに追加のノードを結合するためのキーが必要です。

重要：この手順を行わないと、次の手順ですべてのデータが失われます。**

3. 必要に応じて設定を終了し、NFS バックアップ設定を適用するためにアプライアンスを再起動します。
4. バックアップします。

上記で推奨しているように、少なくも 48 時間バックアップして、バックアップの問題を示すサービス通知がない場合は、次の手動による手順は必要ありません。

バックアップとその他のサービス通知は、Threat Grid portal UI の、右上隅にあるアイコンから使用できます。「PostgreSQL バックアップがまだありません」というサービス通知が表示された場合は、続行しないでください。

再起動後に即座にバックアップを実行する場合は、完了していることを確認するために NFS に対するすべてのデータのバックアップを手動で開始する必要があります。手動バックアップ コマンドの実行は、スタンドアロン ボックスをクラスタに再構築する直前にバックアップを設定する場合にのみ必要です。

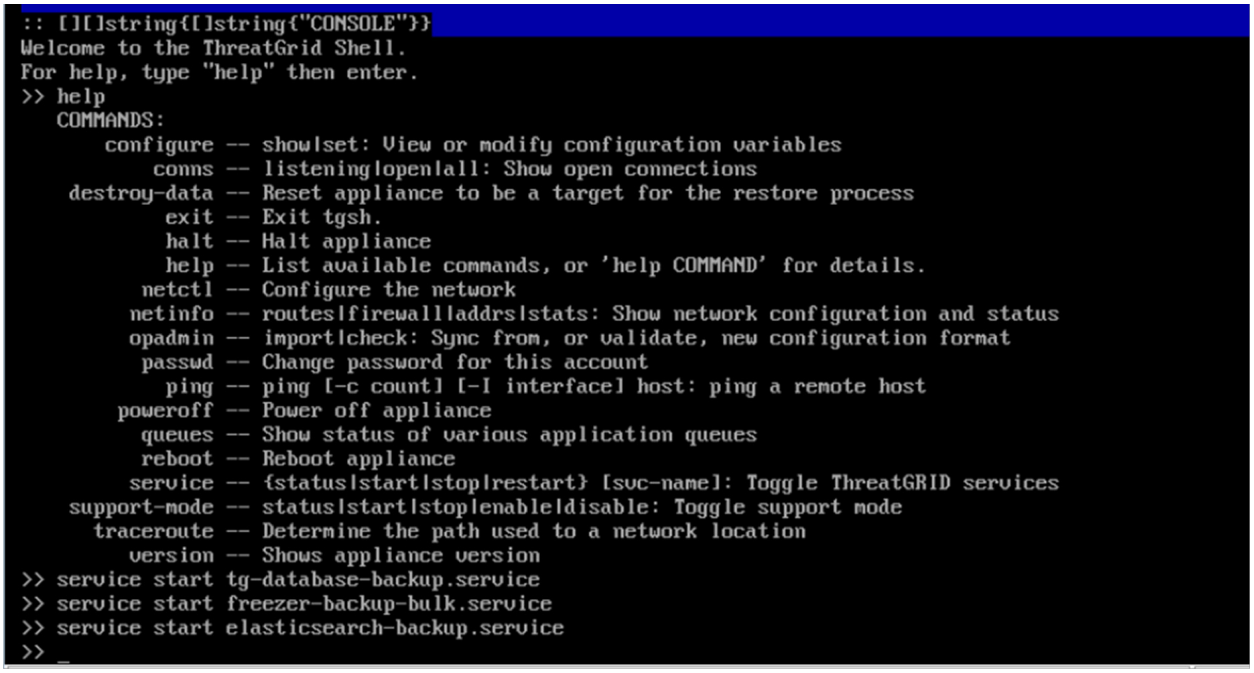
これについては、次のコマンドを入力して tgsh で行います。

```
service start tg-database-backup.service

service start freezer-backup-bulk.service

service start elasticsearch-backup.service
```

図 30：NFS に対するすべてのデータのバックアップの開始



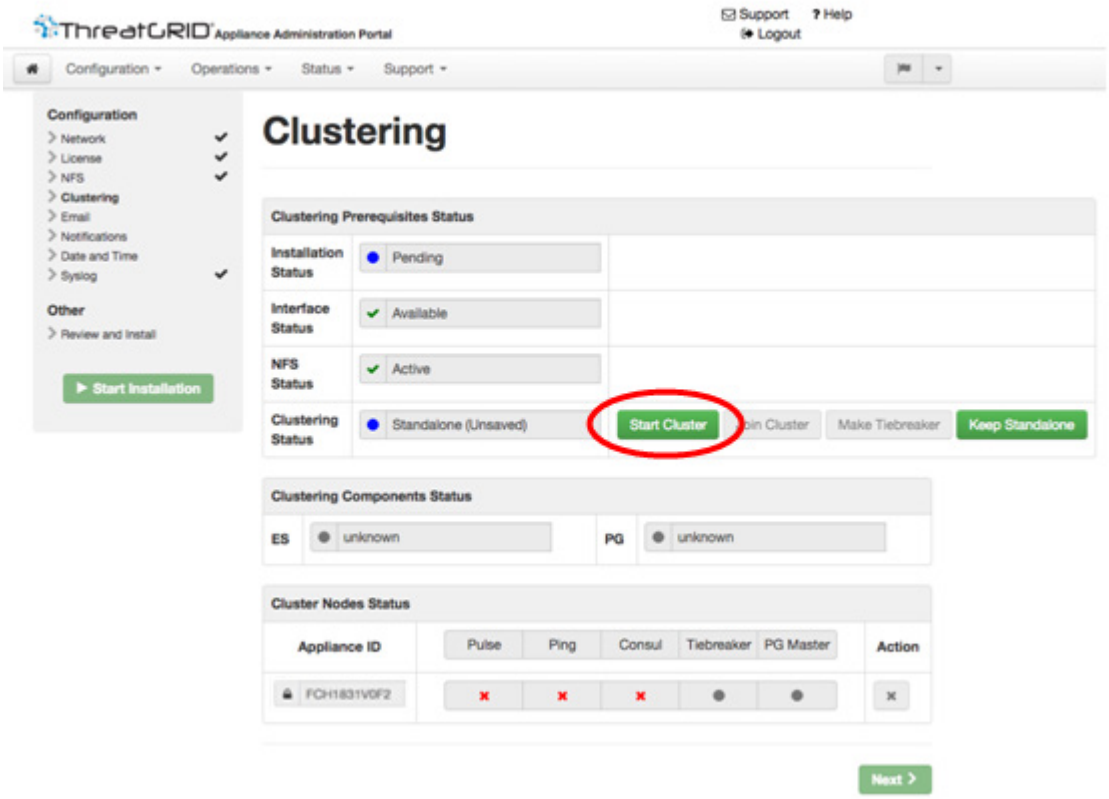
最後のコマンドが返された後、約 5 分待ちます。

5. 次に、アプライアンス UI でサービス通知を確認します。任意の通知に、PostgreSQL バックアップがまだありませんという警告などのバックアップ プロセスの障害が示されている場合は、続行しないでください。

****これらのプロセスが正常に完了するまで続行しないでください。****

6. [クラスタリング（Clustering）] ページ（[設定（Configuration）] > [クラスタリング（Clustering）]）に移動します。

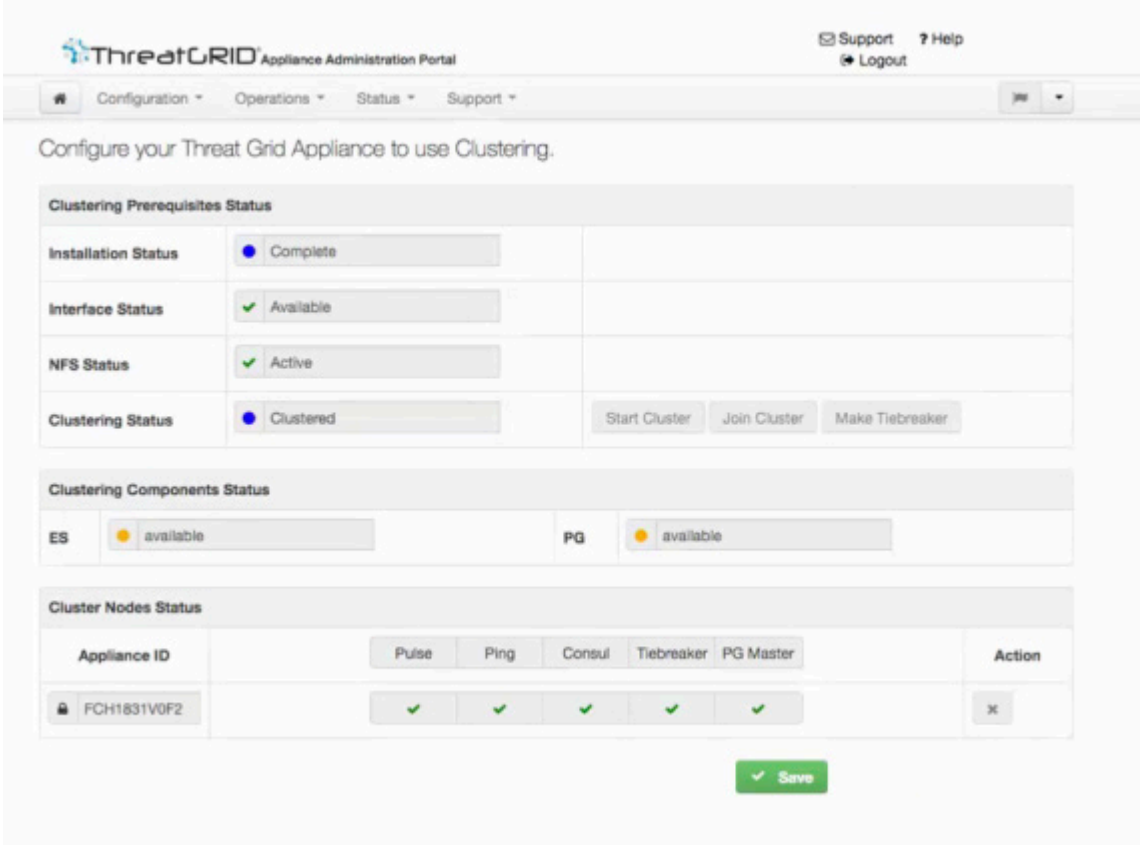
図 31：クラスタの開始



7. [クラスタの開始（Start Cluster）] をクリックし、クラスタリング ステータスを [クラスタ化（Clustered）] に変更する確認ポップアップで [OK] をクリックします。

データの復元が完了すると、新しいクラスタの状態を確認するためのクラスタリング設定ページに戻ります。

図 32：クラスタリング ステータス：[クラスタ化（Clustered）]



8. インストールを終了します。これにより、クラスタ モードでデータの復元が開始されます。

セクション「クラスタへのアプライアンスの結合」（p. 88）で説明するように、新しいクラスタへの他のアプライアンスの結合を開始できます。

新しいアプライアンスを使用したクラスタの開始

このクラスタを起動する方法は、アプライアンス ソフトウェアのクラスタ対応バージョンに同梱されている新しいアプライアンス、またはデータをリセットした既存のアプライアンスに使用できます。

特記事項:新しいクラスタを最初から作成するときにデータベースの作成を処理する方法で問題を判明しました。これによって影響を受ける顧客の数を最小限に抑えるために、スタンドアロン アプライアンスを最初に作成して、以下の手順ではなく、前のセクションで説明したように、クラスタに拡張することをお勧めします。ご質問がある場合は、support@threatgrid.com までお問い合わせください。
-- Threat Grid アプライアンス チーム、2018 年 5 月 29 日

注：以前にドキュメント化された `destroy-data` コマンドを使用して既存のデータを削除します。（ワイプ アプライアンスを使用しないでください。）

1. 通常どおり OpAdmin 設定を設定および開始します。
2. OpAdmin 設定ウィザードの *NFS* ページ（[設定（Configuration）] > [NFS]）を参照してください。

   注：上記のセクション「既存のスタンドアロン アプライアンスによるクラスタの開始」の図を参照してください。
3. ネットワークおよびライセンスを設定します。
4. [NFS] ページで、NFS の [ホスト（Host）] および [パス（Path）] を設定して、**ステータス**を [有効化（Enabled）] に設定します。

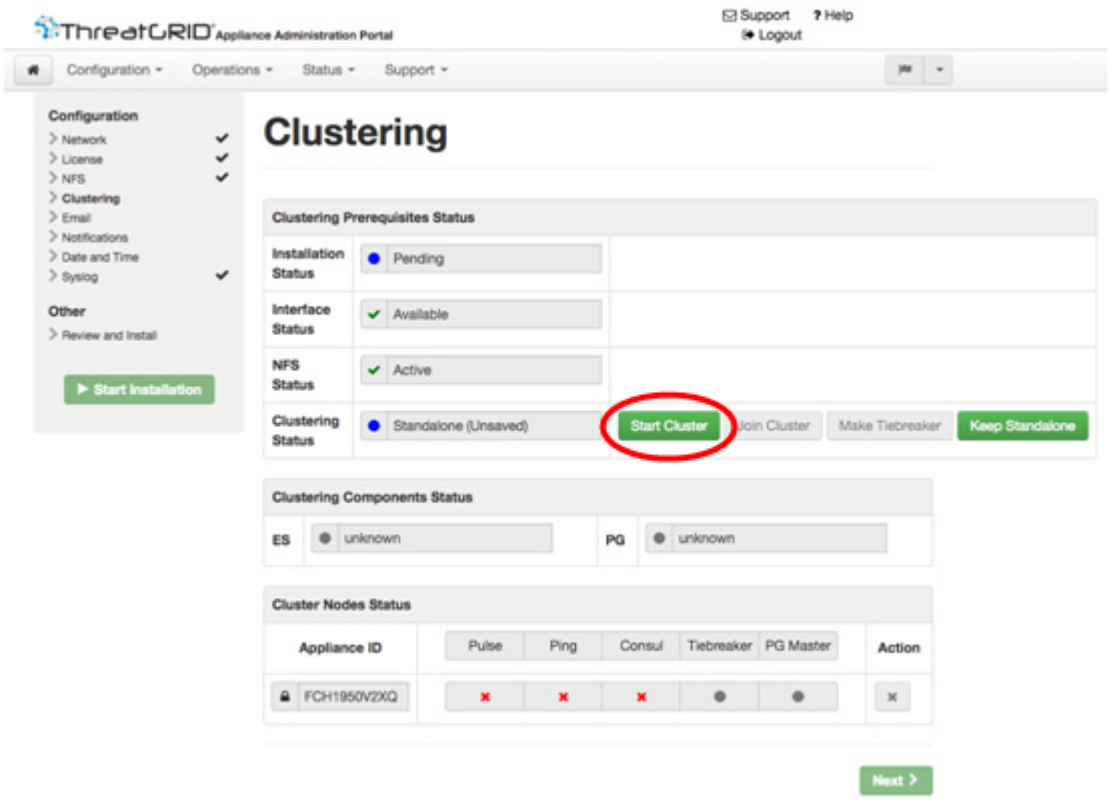
   ホスト（Host）：NFSv4 ホスト サーバ。IP アドレスを使用することをお勧めします。

   パス（Path）：ファイルを保存する NFS ホスト サーバ上にある絶対パス。これにはキー ID サフィックスは含まれません。自動的に追加されます。

   オプション（Opts）：このサーバで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウント オプション。

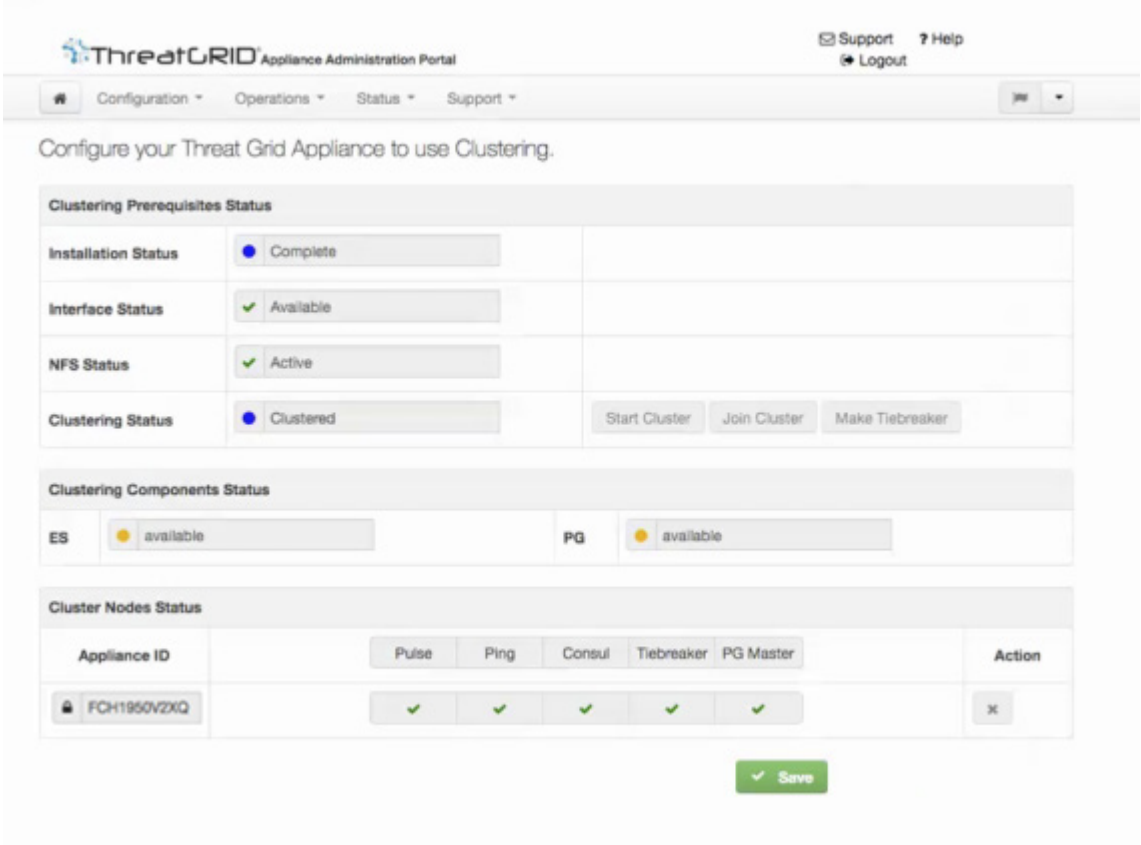
   ステータス（Status）：ドロップダウンから [有効化（保留中のキー）（Enabled（Pendign Key））] を選択します。
5. [次へ（Next）] をクリックします。ページがリフレッシュされます。[生成（Generate）] および [アクティブ化（Activate）] ボタンが使用できるようになります。
6. [生成（Generate）] をクリックして、新しい NFS 暗号キーを作成します。
7. [Activate] をクリックします。**ステータス**が [アクティブ（Active）] に変わります。
8. [ダウンロード（Download）] をクリックして、保管のために暗号キーのコピーをダウンロードします。クラスタに追加のノードを結合するためのキーが必要です。

図 33：クラスタリングの設定ページ



9. クラスタリングの設定ページ（[設定（Configuration）] > [クラスタリング（Clustering）]）を参照します。
10. [クラスタの開始（Start Cluster）] をクリックして、確認ポップアップで [OK] をクリックします。クラスタリング ステータスが、[クラスタ化（Clustered）] に変わります。
11. ウィザードの残りの部分を完了し、[インストールの開始（Start Installation）] をクリックします。これにより、クラスタ モードでデータの復元が開始されます。
12. 新しいクラスタの状態を確認するために *クラスタ*の設定ページを開きます。

図 34：クラスタリング ステータス：[クラスタ化（Clustered）]



次のセクション「**Error! Reference source not found.**」で説明されているように、新規または既存のアプライアンス ノードをクラスタに結合する場合があります。

クラスタへのアプライアンスの結合

このセクションでは、新規または既存のアプライアンスをクラスタに結合する方法について説明します。

注：データが含まれていない場合にのみ、アプライアンスが既存のクラスタに結合される可能性があります。（初期、第 1 のアプライアンスとは異なります。データが含まれる可能性があります。）

また、結合は最新バージョンのマシンでのみ試行されることが非常に重要です。クラスタ内のすべてのアプライアンスは、同じバージョンを実行する必要があります。これは、最初にアプライアンスを設定することが必要です。その後そのアプライアンスを更新し、データをリセットして、クラスタに結合します。

一度に 1 つのノードを追加し、Elasticsearch（「ES」）と PostGres（「PG」）が次のノードに進む前に「複製済み」の状態に到達するまで待ちます。「複製済み」は、2 つ以上のノードのクラスタで予定されています。「複製済み」に到達するまでの状態が ES と PG に変更されるまでの待ち時間は、単一ノード ケースには適用されません。（つまり、バックアップから単一ノード クラスタを初期化している場合、復元が完了して、アプリケーションが 2 番目のノードに進む前に UI で作業/表示可能になるまで待つ必要があります。）

既存のアプライアンスのクラスタへの結合

既存のアプライアンスをクラスタに結合するときに、クラスタにマージする前にデータのすべてを削除する必要があります。

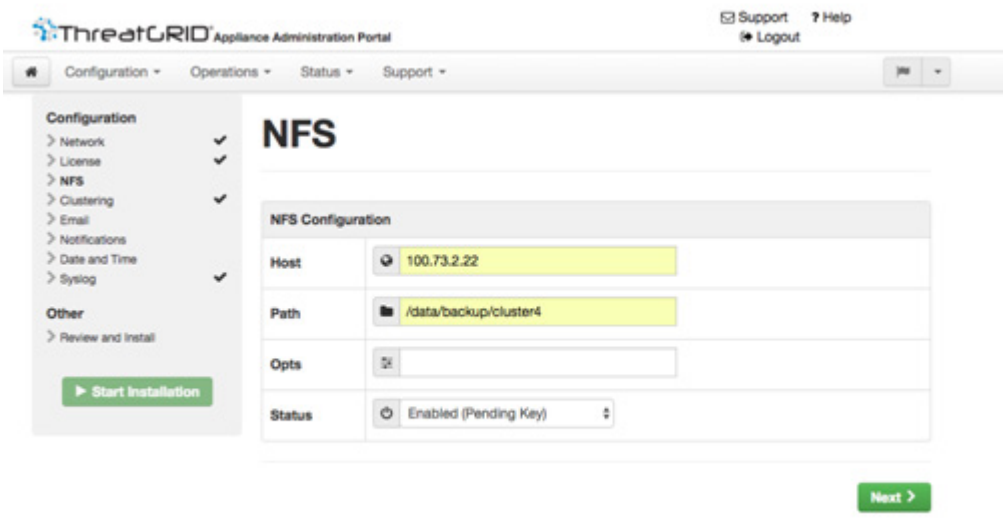
- 最新バージョンにアプライアンスを更新します。これにより、現在実行されているバージョンによっていくつかの更新サイクルが必要になる場合があります。クラスタ内のすべてのノードは、同じバージョンにあることが必要です。
- `tgsh` の `destroy-data` コマンドを実行してすべてのデータを削除します。

既存のアプライアンス上で `destroy-data` を実行した後、基本的に新しいノードになり、クラスタへの結合は、次のセクションで説明されているように、新しいアプライアンスへの結合と同じ手順に従います。

新しいアプライアンスのクラスタへの結合

1. 通常どおり OpAdmin 設定を設定および開始します。
2. OpAdmin ウィザードの NFS 設定ページ（[設定（Configuration）] > [NFS]）を参照して、クラスタ内の第 1（初期）ノードと同じ [ホスト（Host）] および [パス（Path）] で NFS を設定します。ステータス [有効化（保留中のキー）（Enabled（Pending Key））] を選択します。

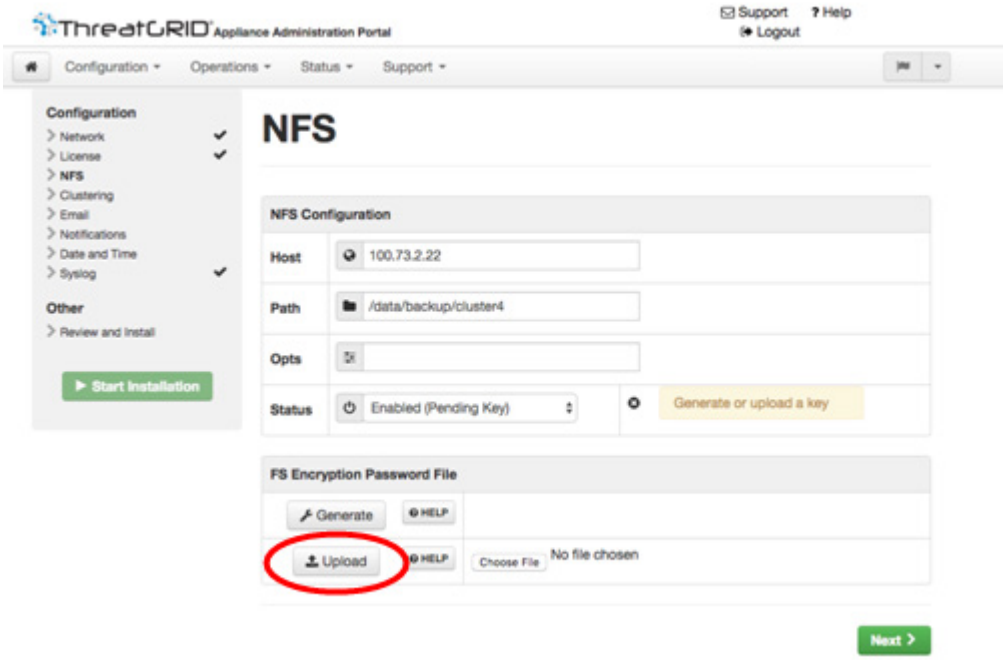
図 35：クラスタを結合するための NFS



3. [次へ（Next）] をクリックします。ページが更新され、[アップロード（Upload）] が使用可能になります。

   注：キーがバックアップを作成するために使用されたキーと正確に一致する場合、アップロードが設定されたパスのディレクトリ名と一致した後、キー ID が OpAdmin に表示されます。暗号キーを使用せずにバックアップを復元することはできません。設定プロセスには、NFS ストアおよび暗号化データをマウントするプロセスと、NFS ストアのコンテンツからアプライアンスのローカル データストアを初期化するプロセスが含まれます。

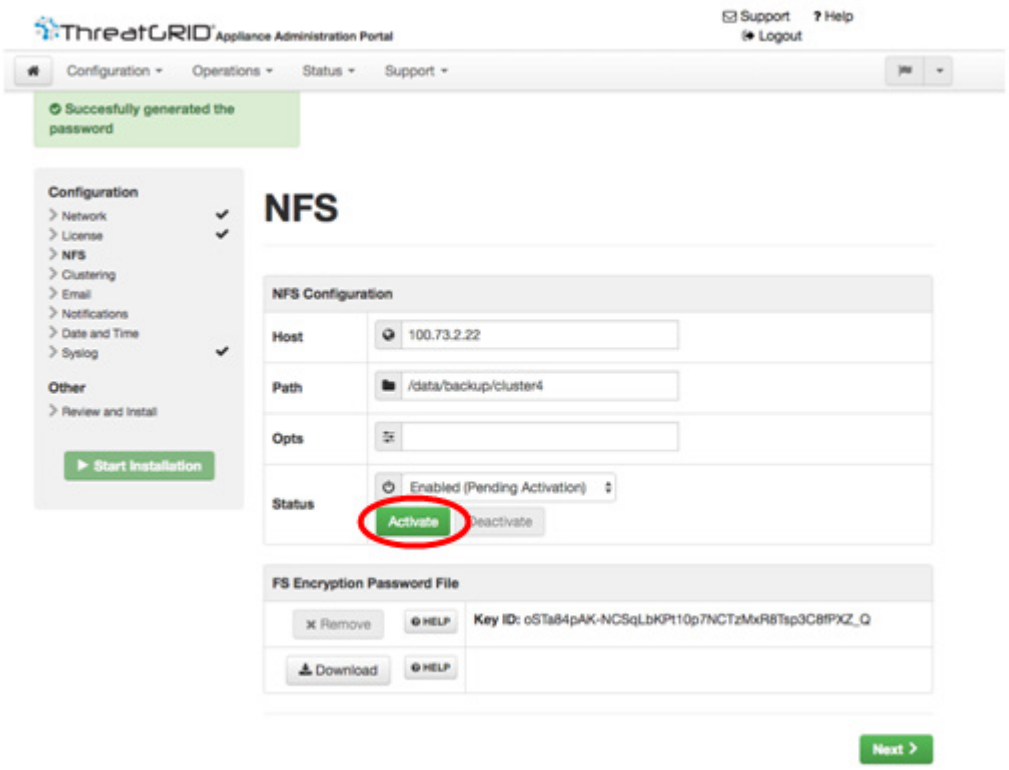
図 36：NFS 暗号キーのアップロード



4. [アップロード（Upload）] をクリックして、新しいクラスタを開始するときに最初のノードからダウンロードした NFS 暗号キーを選択します。

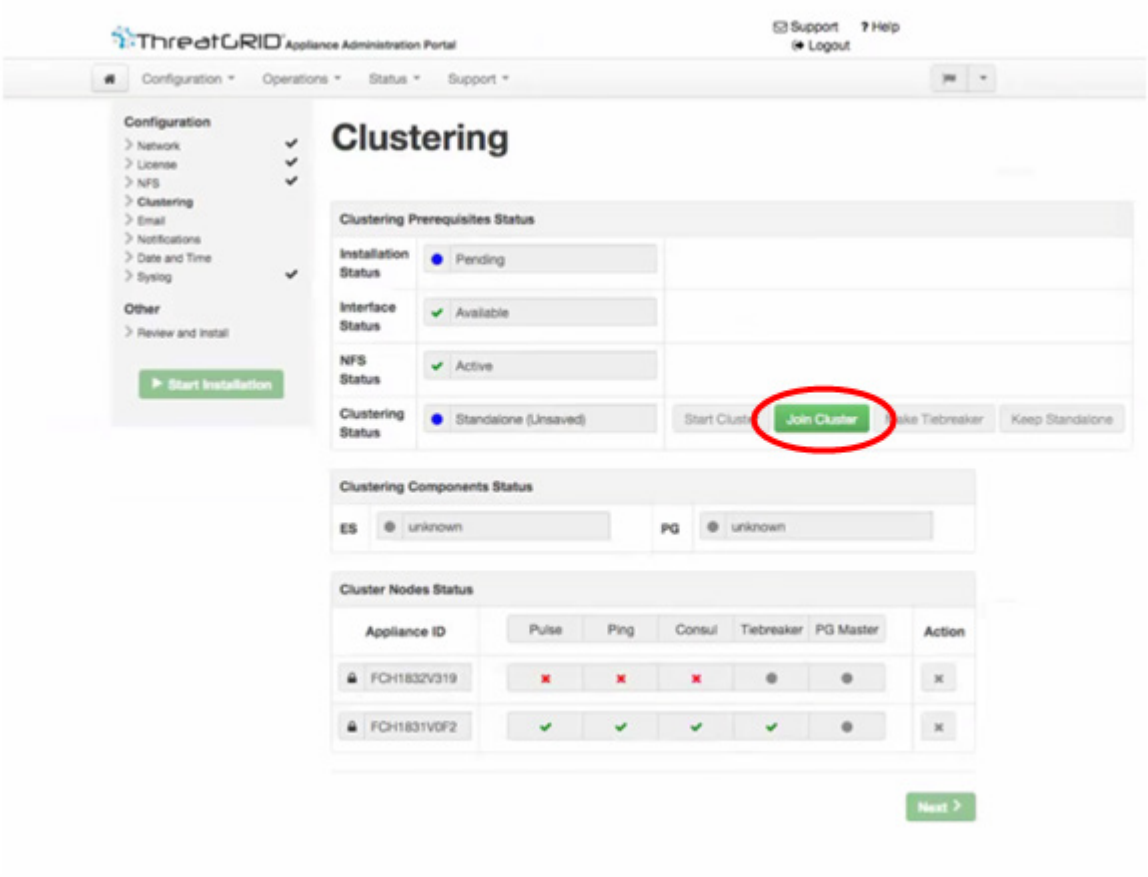
5. [次へ（Next）] をクリックします。ページがリフレッシュされます。キー ID が表示されて、[アクティブ化（Activate）] が使用できるようになります。

図 37：アプライアンスの結合の NFS 暗号キーの有効化



6. [Activate] をクリックします。これには数秒かかります（ステータス インジケータは左下隅にあります）。ステータスが [アクティブ（Active）] になります。
7. [次へ（Next）] をクリックして、ウィザードの [クラスタリング（Clustering）] 設定ページを続行します。

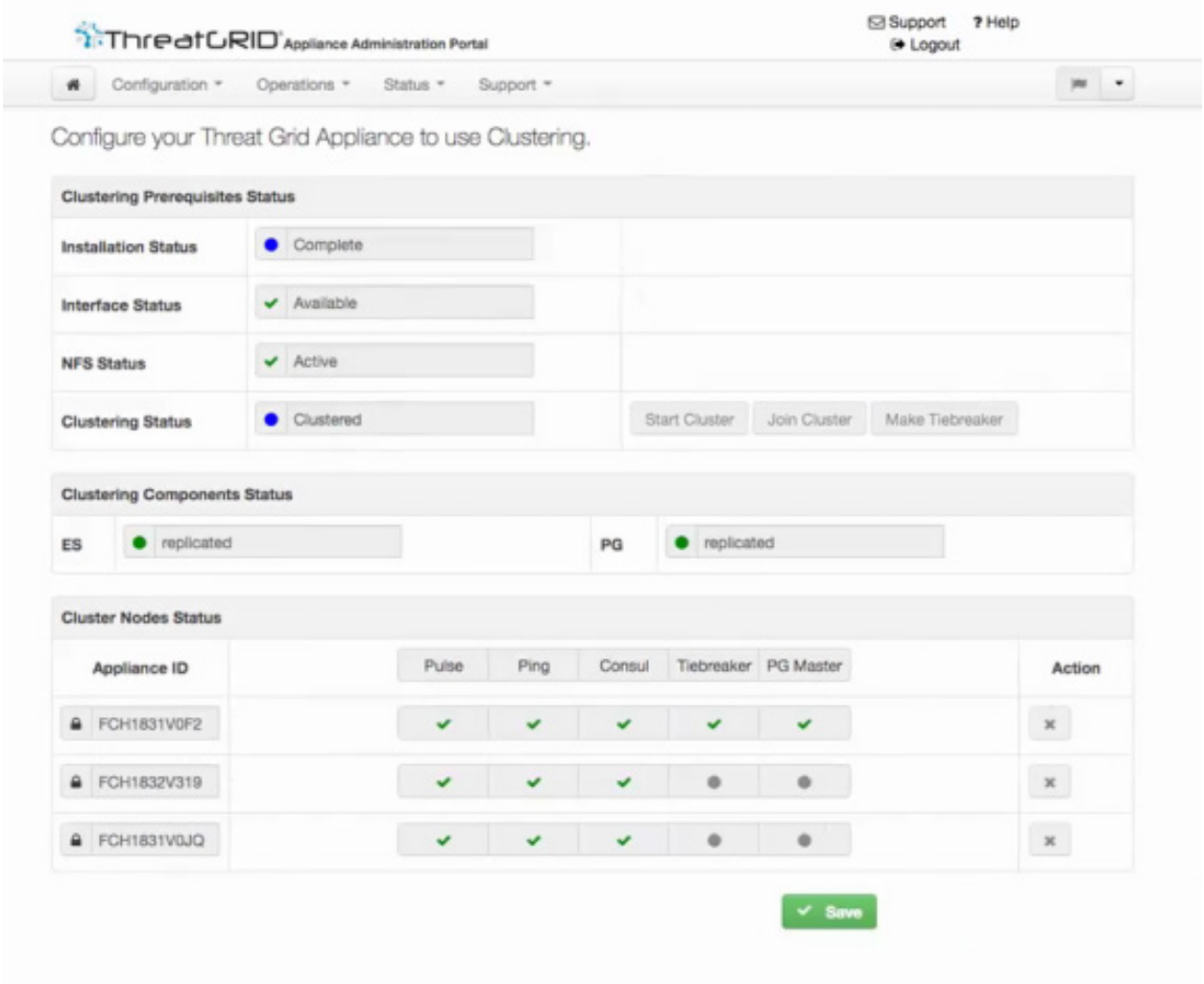
図 38：クラスタの結合



8. [クラスタの結合（Join Cluster）] をクリックして、確認ポップアップで [OK] をクリックします。クラスタリング ステータスが、[クラスタ化（Clustered）] に変わります。
9. インストールを終了します。これにより、クラスタ モードでデータの復元が開始されます。

クラスタに結合する各ノードのこれらの手順を繰り返します。

図 39：アクティブ、正常、3 ノードのクラスタ



条件のノードの指定

クラスタに偶数のノードを含めるように設定すると、条件として指定されたものが、プライマリ データベースを持つノードを決定する選択をするときに「第 2 投票」を取得します。

クラスタ内の各ノードにはデータベースが含まれていますが、プライマリ ノードのデータベースのみが実際に使用されます。プライマリ ノードがダウンした場合は他のノードがその役目を引き継ぎます。条件を設定していると、ノードがちょうど半分失敗したとき、ただし、条件が失敗したノード上ではない場合のみ、クラスタがダウンするのを防止できます。

3、5、または 7 ノード クラスタをお勧めします。条件のサポートは、スタンドアロン アプライアンスから 2 ノード クラスタに移行する際の信頼性の損失を軽減するための継続的な努力の一環です。

クラスタが完全に正常な状態で、現在のノードが条件でない場合、[条件の作成（Make tiebreaker）] ボタンがアクティブになっています。[条件の作成（Make tiebreaker）] をクリックすると一時的なサービスの中断が起こります。その後、現在のノードは失敗しないようになり、その他のノードはクラスタを破損せずにシャットダウンすることができます。予定の時刻より早い指定を変更できずに条件ノードの永続的失敗が発生した場合は、残存しているノードをリセットするかバックアップから復元してください。または support@threatgrid.com に問い合わせてください。

[クラスタリング（Clustering）] 設定ページで、条件としてクラスタを指定するには、[条件の作成（Make Tiebreaker）] をクリックします。

クラスタ ノードの削除

クラスタからアプライアンス ノードを削除するには、[クラスタリング（Clustering）] 設定ページで、[削除（Remove）] ボタンを使用します。

クラスタの削除は、一時的にダウンしているノードではなく、クラスタの一部と見なされなくなったことを示します。停止しているときにアプライアンスを削除します。つまり、アプライアンスが別のハードウェアに置き換えられているとき、またはそのデータをリセットした後にのみ、クラスタに再度結合されるときです。アプライアンスの削除は、ノードを再度追加しないことをシステムに示します。再度追加する場合はリセットされます。

アプライアンスは、パルスがある（NFS にアクティブに書き込まれている）場合、または consul で（コンセンサス ストアの一部）アクティブになっている場合は、クラスタから完全に削除されません。

[クラスタリング（Clustering）] 設定ページで、[削除（Remove）] をクリックします。

ライブ中のノード（7 ノードより少ないクラスタ内）を置換するには、新しいノードを追加して、クラスタが緑色になるまで待ちます。応答がないシステムに警告するために [削除（Remove）] ボタンを使用してオフラインの古いものを削除します。

最初にノードをオフラインにするときに、クラスタ ステータスは黄色に変わります。[削除（Remove）] をクリックすると、ステータスは緑色に戻ります（クラスタが今削除されたノードが表示されることを今後想定しないサイズに変更するためです）。

クラスタのサイズ変更

[削除（Remove）] ボタンを使用してクラスタからノードが削除されると、クラスタのサイズが変更されます。これは、許容が予想される障害の数に影響する可能性があります。クラスタが（次のセクションの障害許容範囲表で定義されているように）予想される障害の許容範囲の数を変更する方法でサイズを変更する場合、Elasticsearch を強制的に再起動します。これは、一時的なサービス中断の原因になります。

例外：上記には、再起動しているまたは一時的な障害がある PostgreSQL マスター以外のシステムは含まれません。中断は、そのノードをアクティブに使用したクライアントを除くケースで、またはサンプルを実行している場合は、最小限にする必要があります。すでにクラスタの一部ではないアプライアンスを追加する場合、または [削除（Remove）] をクリックする場合、許容される障害の数が変更されるなどクラスタのサイズが変更され、クラスタの残りが再設定するときに一時的に中断されます。

障害許容範囲

障害が発生した場合、クラスタ化されたアプライアンスは、失敗したノードによってアクティブに実行されている分析の例外でデータを失うことはありません。最小限（1 分未満）のサービス中断期間でユーザの関与なくサービスを回復します。

ほとんどの失敗は、使用可能なノードの数が**必要なノード**列の数より少なくなければ、1 分未満で回復します。または、（[クラスタリング（Clustering）] ページで「複製済み」としてリストされているサービスによって示されるように）*クラスタ*はそれらの障害が発生する前に正常な状態であれば、使用可能なノードの数が増えてその数を満たした後に回復します。

特定のサイズのクラスタで許容が予想される障害数。

図 40：障害許容範囲表

クラスタ サイズ	許容される障害	必要なノード
1	0	1
2	1*	1*
3	1	2
4	1	3
5	2	3
6	2	4
7	3	4

*非条件のみ

次の図は、最良のシナリオを表します。すべてのノードがアップするときにクラスタがボード上で緑色に表示されない場合、示された完全な障害の数を許容できない場合があります。

例：2 つの許容される障害と 3 つの必要なノードがある 5 ノード クラスタ サイズがあり、5 つすべてのアプライアンスでデータをアクティブに処理している場合、クラスタは、独自に再設定し、最大 2 つの障害が発生した場合には人による管理アクションなしで操作を続行できます。

その他の考慮事項：5、6、または 7 ノード クラスタで、許容される障害の数の +1 は、失敗するノードの割合が高いことを意味します。これは、ノードの数が障害レートに分散乗数として機能するときに特に重要です。（ノードが 2 つあり、それぞれにハードウェア障害が 10 年に 1 回発生する場合、ハードウェア障害レートは 5 年に 1 回となります。）

障害の回復

ほとんどの障害は自動的に回復します。回復しない場合、Threat Grid サポート（support@threatgrid.ccom）に連絡する必要があります。または、データをバックアップから復元してください。詳細については、バックアップの内容の復元を参照してください。

API/使用の特性

クラスタ内の任意のノードに送信されたサンプルのステータスは、クラスタ内の他のノードからクエリされることがあります。送信が行われる個々 のノードを追跡する必要はありません。

1 つのノードに行われたサンプル送信の処理は、クラスタ内のすべてのノード間で分割されます。クライアント側からアクティブに負荷分散する必要はありません。

運用/管理の特性

2 ノード クラスタで、ノードの 1 つは「条件」で、シングル ポイント障害として機能します。ただし、他のノードは、（カットオーバー中に一時的な障害を超える）悪影響なく、クラスタから削除される可能性があります。2 ノード クラスタが正常な（両方のノードが完全に動作している）場合、条件の指定はユーザによって変更され、シングル ポイント障害であるノードを置換する可能性があります。

フェールオーバーが発生している間にサービスが一時的に中断される可能性があります。フェールオーバー中にアクティブに実行されているサンプルは自動的に再実行されません。

クラスタリングのコンテキスト内で呼ばれる「容量」は、ストレージではなくスループットを指します。3 ノード クラスタは、1 つのアプライアンスと同じ最大ストレージ レベルまでデータを取り除きます。したがって、3 つの 5000 サンプル アプライアンスのクラスタ（レート制限が合計 15,000 サンプル/日）は、最大限のキャパシティで使用すると、保持は「**Threat Grid Appliance Data Retention Note**」（cisco.com の他のアプライアンスのドキュメントにあります）で提供される 10,000 サンプル/日の概算見積もりよりも最低 33 % 短くなります。

ネットワーク終了設定

地理的な場所は、マルウェア分析において重要な問題になることがよくあります。マルウェアのいくつかの種類は、地理的な場所によって異なる方法で動作しますが、その他の種類は特定の領域をターゲットにする可能性があります。VPN に対する概念と同様に、Network Exit の設定により、サンプル分析中に生成される発信ネットワークがその場所で終了するように表示されます。

「tg-tunnel」ソリューションは分析中に場所の開示を防止する必要がある Threat Grid アプライアンスのユーザに提供されました。tg-tunnel は Network Exit ローカリゼーション機能によって 2.4.3 のバージョンに置き換えられました。機能は同じですが、顧客制御トグルや自動設定への移行/インストールに置き換えられました。

設定ファイルが自動的に配布されるため、サポート スタッフが手動でインストールまたは更新する必要がなくなります。

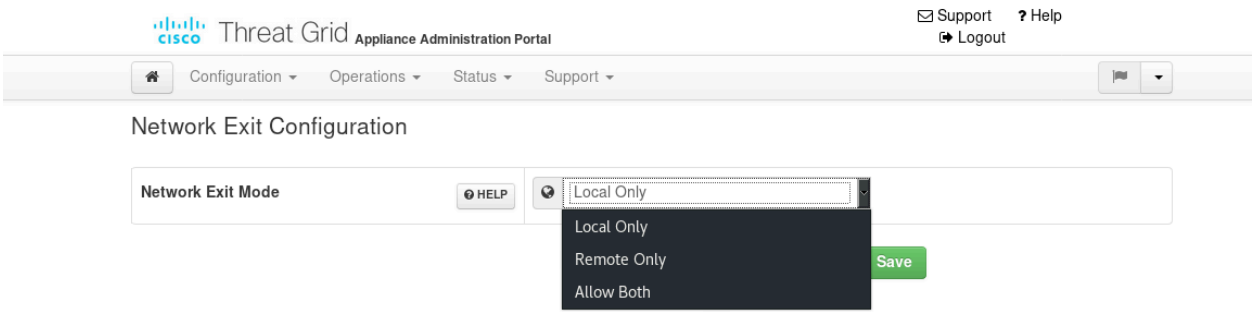
注：これまで tg-tunnel を使用していたお客様は、2.4.3 リリースをインストールする前に 4.14.36.142:21413 および 63.97.201.68:21413 発信トラフィックを許可する必要があります。または、リモート終了の使用を有効化する前にそのトラフィックのみ許可する必要があります。

ユーザは、終了を選択することはできません。Network Exit の機能は、現在 tg-tunnel で取得している機能と同じですが、顧客制御トグルや自動設定の実行/インストールの機能とは異なります。

トグルは tg-tunnel 構成を以前に手動でインストールしたお客様にデフォルトで搭載されており、不要なネットワーク上での不正なトラフィック漏洩リスクを回避します。

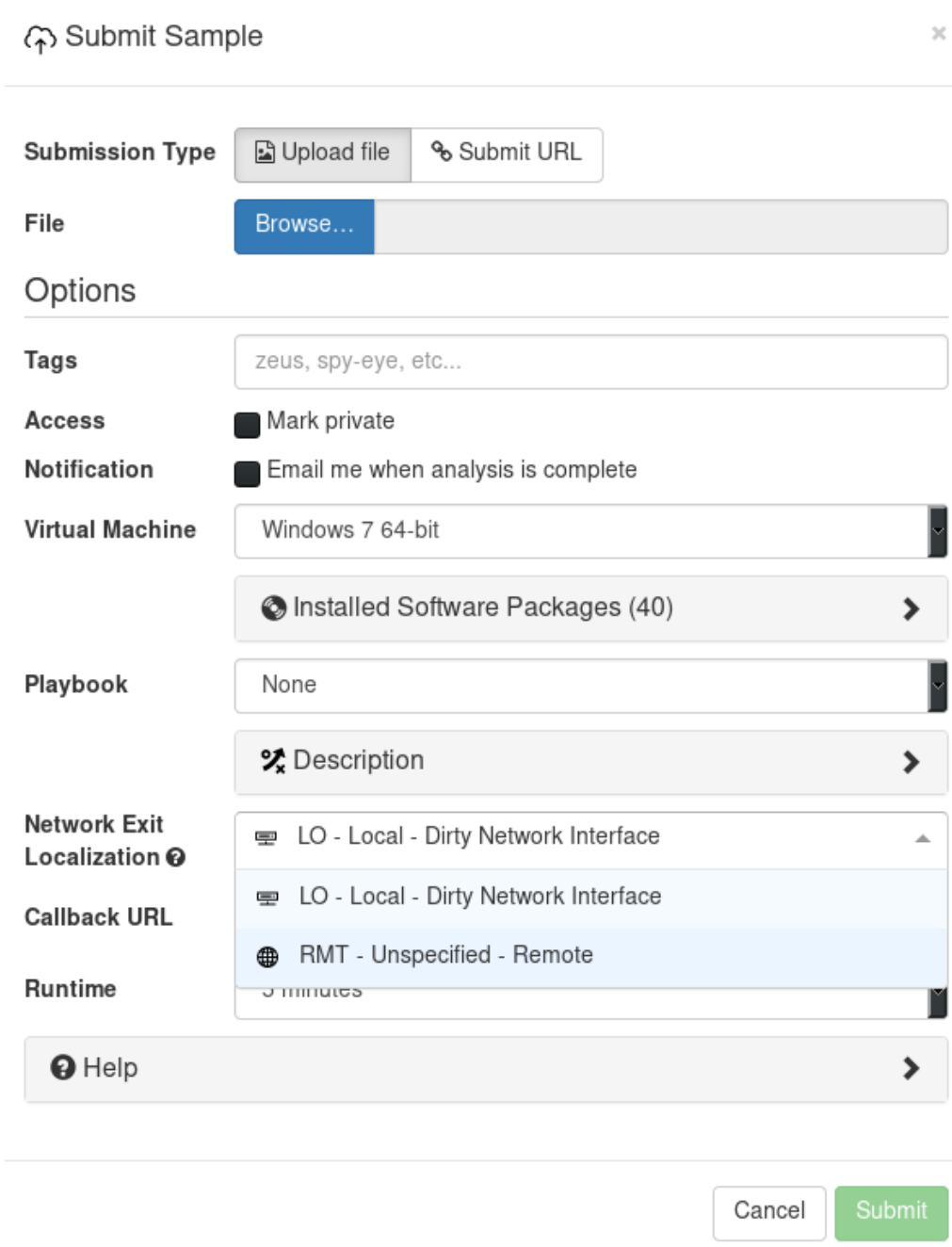
[OpAdmin] > [設定（Configuration）] > [Network Exit] の順に選択します。[Network Exit 設定（Network Exit Configuration）] ページが開きます。

図 41：[Network Exit 設定（Network Exit Configuration）]



ここで選択および保存したオプションによって、UI のサンプルを送信するときに、[Network Exit ローカリゼーション（Network Exit Localization）] オプションのユーザが決定されます。[ローカルのみ（Local Only）] または [リモートのみ（Remote Only）] に設定する場合、アプリケーションによって、これらのオプションのみユーザが使用できるようになります。

図 42：[Network Exit ローカリゼーション（Network Exit Localization）] オプション

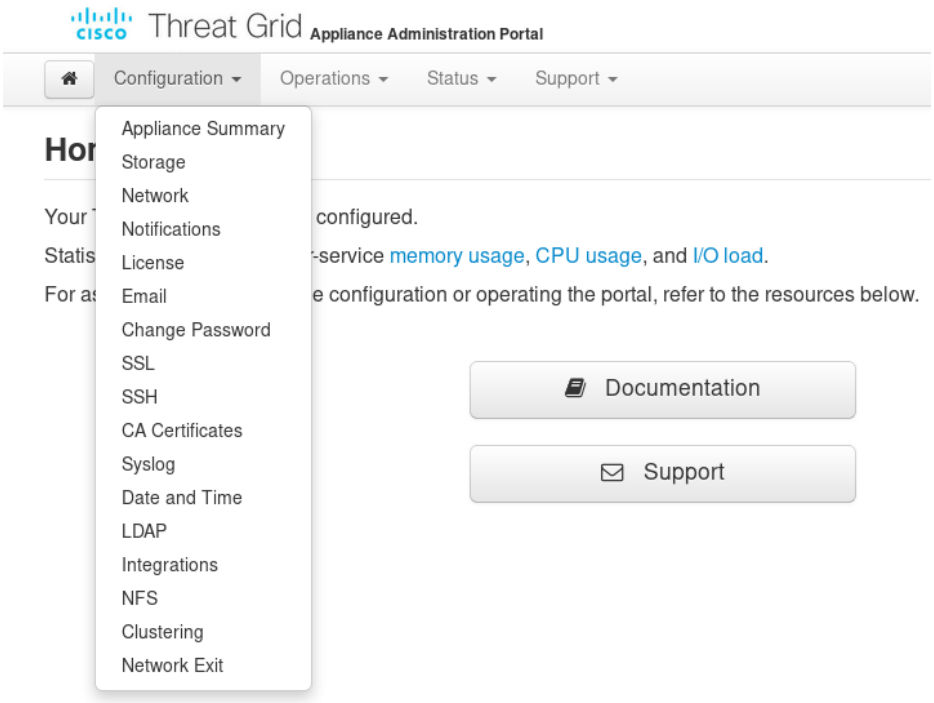


付録：OpAdmin メニュー

次のスクリーンショットに OpAdmin 内の多くのタスクを実行するために使用可能なさまざまなメニュー オプションを示します。

[設定（Configuration）] メニュー

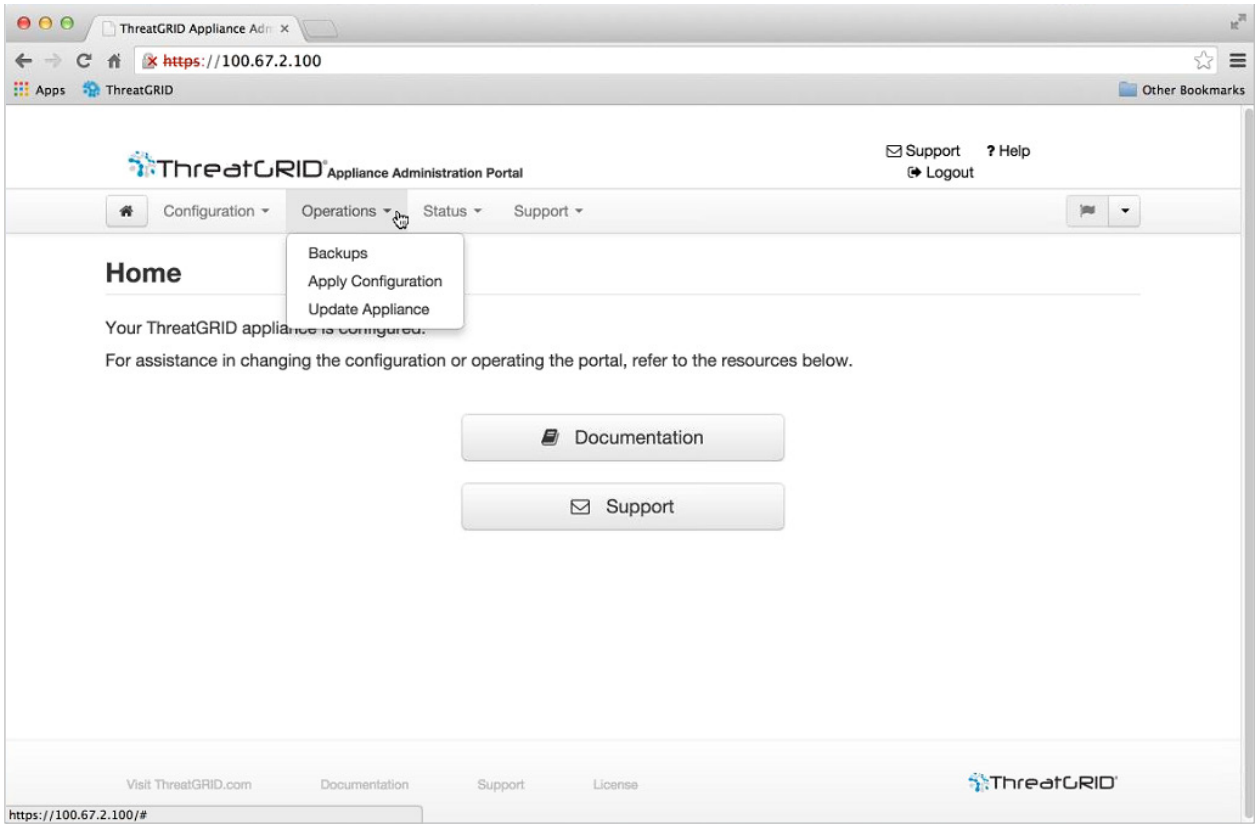
図 43：OpAdmin の [設定（Configuration）] メニュー



注：将来 OpAdmin の各種設定を変更する必要が生じた場合、編集モードにするために [設定（Configuration）] メニューからアクセスする必要があります。

[Operations] メニュー

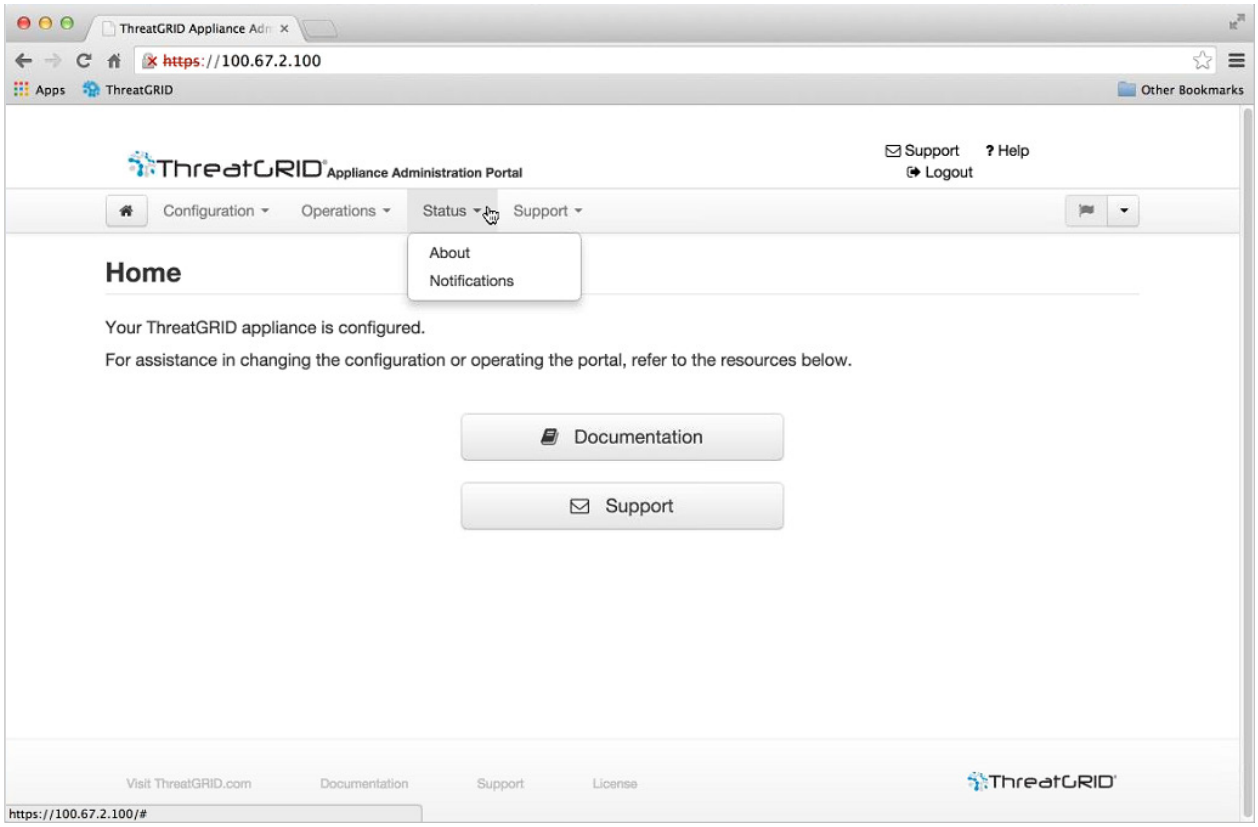
図 44：OpAdmin の [運用（Operations）] メニュー



注：リリース ノートを表示するには、[Update Appliance] を選択します。

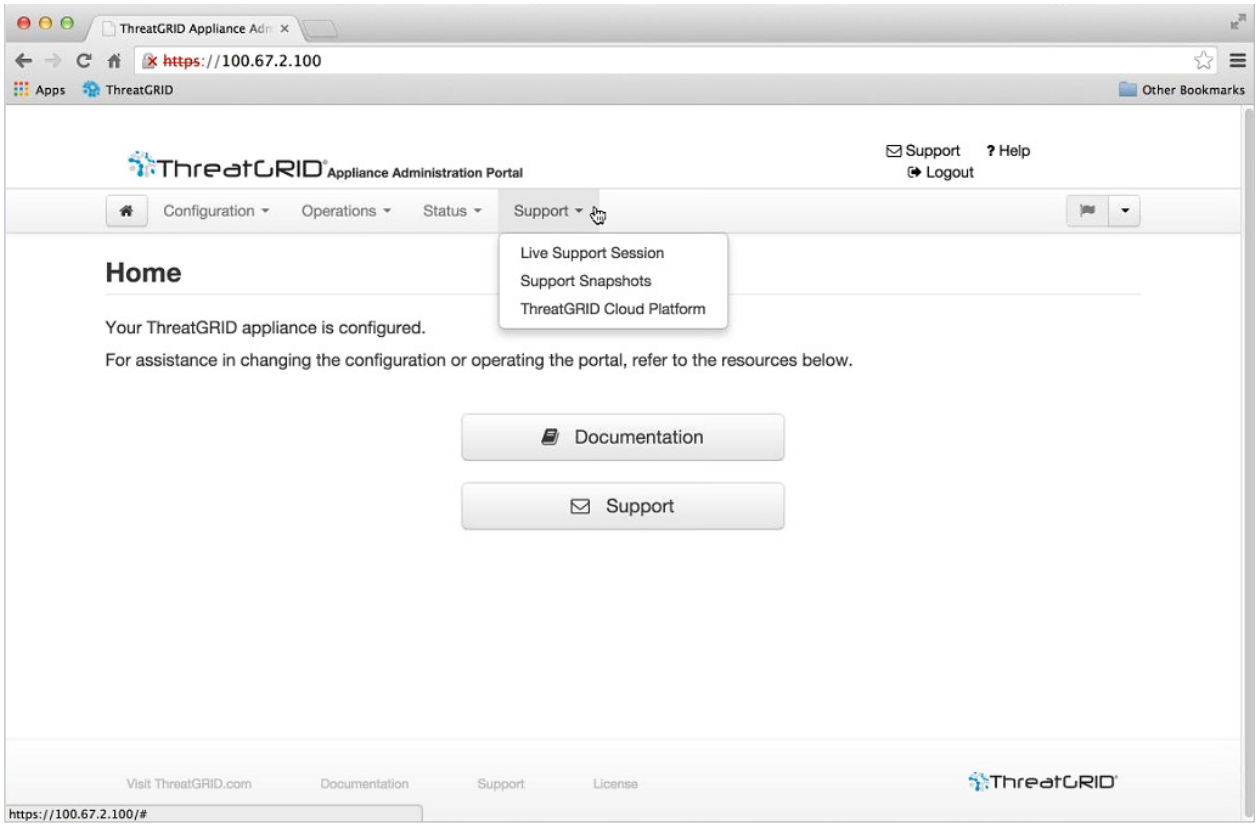
[Status] メニュー

図 45：OpAdmin の [ステータス（Status）] メニュー



[Support] メニュー

図 46：OpAdmin の [サポート（Support）] メニュー



このメニューからライブ サポート セッション（サポート モード）にアクセスできます。詳細については、「サポート対象のモード」のセクションを参照してください。

索引

[Threat Grid ユーザの詳細(Threat Grid User Detailss)] ページ 56
[クラスタリング(Clustering)] ページ 83
[サポート(Support)] メニュー 102
[ステータス(Status)] メニュー....101
[ユーザの詳細(User Details)] ページ....56
[更新(Updates)] ページ 17
[統合設定(Integration Configuration)] ページ....32
[設定(Configuration)] メニュー 99
[運用(Operations)] メニュー 100
[配置更新サービス(Disposition Update Service)] ページ
  Threat Grid Portal で見つかりました....41
[配置更新の配信サービス(Disposition Update Syndication Service)] ページ....54
AMP for Endpoints プライベート クラウド
  CA 証明書の管理 41
  fka FireAMP プライベート クラウド....39
  SSL 証明書の設定 40
  クリーン インターフェイス上の DNS サーバ 40
  統合の手順....47
API
  マニュアル 10
  レート制限....11
CA 証明書
  サポートされる自身の証明書のインポート 36
CA 証明書管理
  AMP for Endpoints プライベート クラウド 41
Chrome 11
CIMC インターフェイス
  構成 12
Cisco SSL 39
ClamAV シグネチャ....32
Clust インターフェイスの設定 74
CONFIG_NETWORK....25
Consul 76
CSA 統合 41, 58
  SSL 証明書 38
destroy-data 66
DHCP
  使用 33
  初期ネットワーク設定の使用....34
DHCP の使用 33
DHCP 構成時の設定
  適用 35
DNS 名
  ダーティ ネットワーク....25
DNS 設定:統合のクリーン インターフェイス....40
Elasticsearch バックアップ
  データの保持....65
ElasticsearchElasticsearch バックアップ 64
ES
  Elasticsearch....76
ESA、WSA 統合
  SSL 証明書設定 37
ESA/WSA アプライアンスの Threat Grid アプライアンスへの接続 41
ESA/WSA の統合の手順....43
FireAMP パブリック クラウド
  名前を変更した AMP for Endpoints プライベート クラウド 39
Firefox....11
Freezer バックアップ 64
geocryptfs
  バックアップ 63
HTTPS
  OpAdmin 28
LDAP
  TGSH ダイアログ ログインの使用 25
LDAP サーバ....29
LDAP 設定ページ....30
LDAP 認証
  複数の管理者に使用可能....14
  設定 28
Microsoft Internet Explorer
  使用しないでください....11
Network Exit
  設定 97
NFS ステータス 75
NFS ホスト....78, 86
NFS 要件
  クラスタリング 73
nfsnobody....63
NFSv4 サーバ 63
OpAdmin
  HTTPS の使用 28
OpAdmin Portal 27

OpAdmin メニュー参照 99
OpAdmin 管理者パスワード 14
OpenDNS
サンプル分析レポートの whois に必要 32
OpenDNS 統合 32
OpenSSL
例 39
passwd コマンド 16
Ping 76
PostgreSQL
バックアップ データの保持 65
PostgreSQL ベース バックアップ 64
PS
PostgreSQL 76
REALLY_DESTROY_MY_DATA 66
Safari 11
SSH
リリースの更新のダウンロード 21
SSH キー 28
SSL
Admin およびクリーン インターフェイスによる使用 36
サポートされるバージョン 36
SSL の共通名
自己署名デフォルトは pandem 36
SSL 証明書 36
AMP for Endpoints プライベート クラウド 40
ESA、WSA、AMP for Endpoints プライベートクラウド 37
アウトバウンド接続の設定 40
インバウンド接続の設定 37
クラスタリング 72
ダウンロード 39
再作成 38
現在のステータスの表示 37
置き換え 38
自己署名デフォルト 36
自己署名デフォルト ホスト名 36
自身の証明書のアップロード 39
自身の証明書の作成：OpenSSL を使用した例 ...39
SSL 証明書の置き換え 38
SSL 証明書設定ページ 37
syslog サーバ
リモート 28
syslog メッセージ
受信 28
TGSH ダイアログ 12
再接続 26
TGSH ダイアログ インターフェイス
設定 25
TGSH ダイアログへの再接続 26
tg-tunnel
Network Exit による置き換え 97
発信トラフィックを許可 97
Threat Grid
サポート 22
ライセンス 11
Threat Grid Portal UI のヘルプ 10
Threat Grid アプライアンス リリース ノート 10
Threat Grid シェル 15
Threat Grid パスワード 14
Threat Grid 組織およびユーザの管理 55
TitaniumCloud 統合 32
updates 9
VirusTotal 統合 32
アップロード（Upload） 40
アプライアンスからのデータの削除 60
アプライアンスで SSL 証明書のステータス 37
アプライアンスのワイプ 60
アプライアンスの更新 17
アプライアンスへのリモート アクセス
ライブ サポート セッション 22
インストール ステータス 75
インターフェイス ステータス 75
クラスタ ノード ステータス 76
Consul 76
Ping 76
スタンドアロンの保持 77
条件 77
クラスタ ノード状態管理
パルス 76
クラスタ モード 85
クラスタからのアプライアンスの削除 94
クラスタのサイズ変更 94
クラスタの結合 92
クラスタへのアプライアンスの結合 88
クラスタへのノードの追加 88
クラスタリング 71
Clust インターフェイスの設定 74
NFS 要件 73
SSL 証明書 72
アプライアンスの削除 94
クラスタ サイズ 71
クラスタ ノード ステータス 76
クラスタ モードでのデータの復元 85
クラスタのサイズ変更 94

クラスタへのアプライアンスの結合 88
コンポーネント ステータスのクラスタリング 76
サンプル送信クエリ....96
サンプル送信処理のオーダー....71
ネットワーク構成図....73
バージョン 72
レート制限....71
前提条件ステータスのクラスタリング 75
同じデータ....71
新しいアプライアンスの開始....86
既存のアプライアンスの開始 77
最初のノードにデータを含めることができます ..72
条件機能 71
要件 72
設定および構成 74
障害の回復....96
障害許容範囲....95
非推奨のエアギャップされた導入 72
クラスタリング : Elasticsearch および PostgreSQL のステータスの色....76
クラスタ内で許可されるノードの数 71
クリーン インターフェイスの FQDN
CN は一致する必要があります....40
ゲートウェイ エントリ
検証 27
ゲートウェイ エントリの検証 27
コンポーネント ステータスのクラスタリング....76
サードパーティ統合
OpenDNS....32
TitaniumCloud....32
ウイルスの合計 32
設定 32
サーバ
LDAP....29
NFSv4 63
サポート 23
ラッシュ 23
サービス通知
バックアップ関連 68
サポート....22
サーバ....23
サポート スナップショット....24
サポート セッションの開始 23
サポート モード....22
ライブ サポート セッションの開始 102
有効にするためのオプション 22
サポートへのお問い合わせ 22
サンプルの可視性とプライバシー....58
サンプル分析レポートの whois
OpenDNS 設定が必要 32
シェル
リカバリ モード 16
開く....15
スタンドアロン（Standalone）....75
スタンドアロン（保存されていない） 75
スタンドアロンの保持....77
ステータスのクラスタリング 75
スナップショット
サポート 24
ダーティ ネットワーク
DNS 名....25
ダウンロード
SSL 証明書 39
データの復元に必要な時間 68
トラブルシューティング
更新 21
ネットワーク インターフェイスの設定管理....25
ネットワーク終了設定 97
ネットワーク設定
現在の表示....25
バージョン ルックアップ
ビルド番号 18
パスワード
OpAdmin....14
管理者 14
紛失した管理者パスワードのリセット....14
パスワードの紛失 13
バックアップ....63
ElasticsearchElasticsearch....64
Freezer 64
NFS 要件 63
PostgreSQL....64
ストレージ要件 64
データの保持....65
内容からの復元 67
合計ストレージ要件....64
含まれない内容....64
含まれる内容....64
復元ターゲットとしてのアプライアンスの
リセット 66
復元上のノート 68
新しいキーの生成で新しいストアを作成....65
概要 65
バックアップ ストレージ要件
Elasticsearch スナップショット ストア....64

PostgreSQL データベース ストア.....64
オブジェクトのストア.....64
バックアップに関連するサービスの通知.....68
バックアップの NFS 要件.....63
バックアップのストレージ要件.....64
バックアップの内容の復元.....67
バックアップの新しいキーの生成.....65
バックアップ復元ターゲットとしてのアプライアンスのリセット.....66
バックアップ頻度
Elasticsearch データベース.....66
PostgreSQL データベース.....65
一括ストレージ.....65
制御したり調整することはできません.....66
パルス.....76
ビルド番号
リリース バージョン ルックアップ.....18
ブート メニュー.....15
プライバシーとサンプルの可視性.....58
ブラウザ
Microsoft Internet Explorer は使用しないでください.....11
推奨.....11
ポート 22.....21
マニュアル.....9
API.....10
ESA/WSA ユーザ ガイド.....10
マルチ POKE.....53
ユーザ
削除.....56
管理.....55, 56
ユーザのステータス
再アクティブ化.....57
非アクティブ化.....56
ユーザの再アクティブ化.....57
ユーザの管理.....56
ユーザの追加.....56
ライセンス
管理.....11
ライブ サポート セッション.....23
ライブ サポート セッションの開始.....23
ラッシュ サーバ.....23
リカバリ モード.....14
ネットワークの設定.....26
リカバリ モードでのネットワークの設定.....26
リブート
リカバリ モード.....14
リリース ノート
Threat Grid Portal の UI.....10
Threat Grid アプライアンス.....10
リリース バージョン
ビルド ルックアップ テーブル.....18
レート制限.....11
API にのみ適用.....55
クラスタ制限はすべてのメンバの合計.....71
ログイン名およびパスワード
デフォルト.....14
ワイプ アプライアンス
オプション.....62
ワイプとリセット.....66
一括ストレージ
バックアップ データの保持.....65
事前設定された状態
復元ターゲットに必要.....66
低下したクラスタ.....71
使用停止または返却前のデータの削除.....60
内容
バックアップの復元.....67
再設定.....33
初期設定.....25
初期設定および構成
設定および構成ガイドを参照.....27
利用不可
コンポーネント ステータスのクラスタリング.....76
利用可能
コンポーネント ステータスのクラスタリング.....76
前提条件.....11
前提条件ステータスのクラスタリング.....75
定期通知.....28
復元ターゲット
バックアップのアプライアンスのリセット.....66
事前設定された状態に戻す.....66
破棄されるデータ.....67
必要な時間
更新.....18
新しいアプライアンス
更新.....17
新しいアプライアンスの更新.....17
新しいアプライアンスを使用したクラスタの開始...86
新しい統合デバイス アカウントの有効化.....56
新規組織の作成.....55
既存のアプライアンスによるクラスタの開始.....77
暗号キー
バックアップの内容の復元に必要.....67
バックアップを復元するためのアップロード.....68

暗号化されたバックアップ 63
更新
SSH ポート 22 経由でダウンロード 21
インストール 17
テスト 17
トラブルシューティング 21
元に戻せない 17
更新のインストール 17
更新のテスト 17
更新のポート 21
更新の実行 18
更新の確認/ダウンロード 17
条件 77
条件サポート
2 ノードのクラスタ 71
検証（Validate） 25
構成
ウィザード 27
構成の変更
詳細なリスト 26
構成時の設定
適用 26
無効化された SSLv3 19
現在のネットワーク設定 25
現在のビルドの表示 17
現在のビルド番号 17
管理者
複数の追加 29
管理者パスワード 13
紛失 13
紛失した管理者パスワードのリセット 14
組織
新規作成 55
管理 55
組織の管理 55
組織の追加 55
統合 32
AMP for Endpoints の手順 47
ClamAV シグネチャ 32
ESA/WSA アプライアンスの Threat Grid アプライアンスへの接続 41
ESA/WSA アプライアンスの手順 43
プライバシーと可視性のルール 58
新しいデバイス ユーザ アカウントの有効化 56
複数のアプライアンス管理者 29
複製済み
コンポーネント ステータスのクラスタリング 76
設定
LDAP 30
LDAP 認証 28
Network Exit 97
TGSH ダイアログ インターフェイス 25
アウトバウンド接続の SSL 証明書 40
サードパーティ統合 32
更新 27
管理 25
統合の DNS 40
設定の変更 33
設定および構成ガイド 10
設定管理
ネットワーク インターフェイス 25
認証
OpAdmin および TGSH ダイアログの LDAP の設定 28
複数の管理者の LDAP 29
起動 12
送信レート制限 55
通知 28
バックアップ関連 68
適用
DHCP 構成時の設定 35
構成時の設定 26
設定変更 33
配置更新サービス 40
タスクの設定 47
配置更新サービス管理 41
配置更新の配信サービス 53
開始する前に 9
障害の回復
クラスタリング 96
障害許容範囲
クラスタリング 95
クラスタ化されたアプライアンス 95
集合 75
電源の投入 12