Cisco Threat Grid アプライアンス バージョン 2.9 管理者ガイド

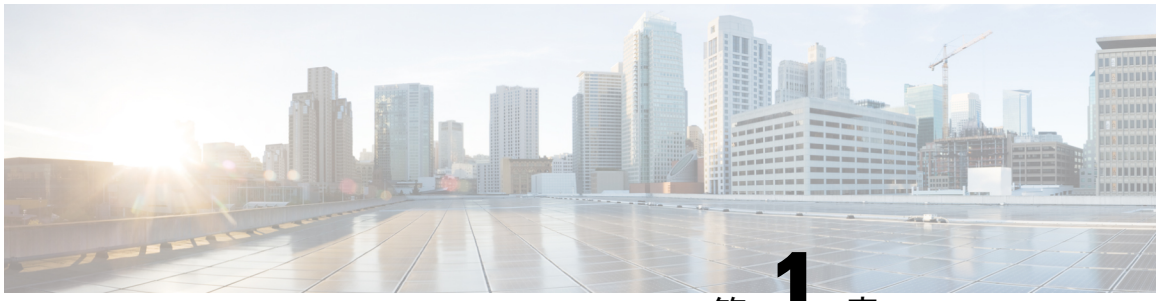
初版：2019 年 12 月 12 日

最終更新：2019 年 12 月 17 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

はじめに

この章では、Cisco Threat Grid アプライアンスの概要、対象読者、および関連する製品マニュアルへのアクセス方法について説明します。ここでは、次の項目について説明します。

Cisco Threat Grid アプライアンスについて

Cisco Threat Grid アプライアンスは、詳細な脅威分析およびコンテンツ分析を使用して、安全性に優れたオンプレミスの高度なマルウェア分析を提供します。Threat Grid アプライアンスは、Cisco Threat Grid M5 アプライアンスサーバ（v2.7.2 以降）にインストールされた完全な Threat Grid マルウェア分析プラットフォームを提供します。さまざまなコンプライアンスおよびポリシーの制限に基づいて運営されている組織が、マルウェアサンプルをアプライアンスに送信できるようにします。

（注） Cisco UCS C220-M3（TG5000）および Cisco UCS C220 M4（TG5400）サーバは、引き続き Threat Grid アプライアンスで使用できますが、サーバのサポートは終了しています。

銀行や医療サービスなどの機密データを扱う組織の多くは、マルウェアアーティファクトといった特定の種類のファイルをマルウェア分析のためにネットワーク外に送信することを許可しない、さまざまな規制ルールおよびガイドラインに従う必要があります。Cisco 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って、組織はネットワークから離れることなく、疑わしいドキュメントやファイルを分析のために送信できます。

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つのアクティビティおよび特性の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事例に照らして、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。

このリリースの最新情報

バージョン 2.9 のこのガイドでは、次の変更が行われました。

表 *1 :* バージョン *2.9mfg* の変更点 - *2019* 年 *12* 月 *17* 日

機能または更新	セクション
変更なし	

表 *2 :* バージョン *2.9* の変更点 - *2019* 年 *12* 月 *12* 日

機能または更新	セクション
Threat Grid Web ポータル UI 管理者のログインパスワードが更新されました。	ログイン名とパスワード（デフォルト）
Threat Grid アプライアンスモデル（UCS C220-M3 サーバをベースとする）に v2.9 をインストールする際のバックアップデータの保持に関する情報が追加されました。	バックアップ データの保持
サポート情報が更新されました。	Threat Grid のサポート

対象読者

このガイドは、アプライアンスのセットアップと設定が完了し、最初のテストマルウェアサンプルが正常に送信および分析された後に、Threat Grid アプライアンス管理者が使用することを目的としています。Threat Grid マルウェア分析ツール、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に関して、組織とユーザを管理する方法について説明します。

さらに、Threat Grid アプライアンスと他のシスコ製品やサービス（Cisco E メールセキュリティアプライアンス、Cisco Web セキュリティアプライアンス、AMP for Endpoints プライベートクラウドデバイスなど）を統合する管理者に向けた情報も提供します。

（注） 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、『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

製品に関する資料

Cisco Threat Grid アプライアンス製品に関する資料の最新バージョンは、Cisco.com から入手できます。

- *Cisco Threat Grid アプライアンス リリース ノート*
- 『*Cisco Threat Grid Version Lookup Table*』
- 『*Cisco Threat Grid M5 Hardware Installation Guide*』

（注） Cisco Threat Grid M5 アプライアンスは、Threat Grid バージョン 3.5.27 以降、およびアプライアンスバージョン 2.7.2 以降でサポートされています。

以前のバージョンの Cisco Threat Grid アプライアンスの製品マニュアルは、Cisco.com の『Threat Grid Install and Upgrade』で入手できます。

Threat Grid Portal UI オンラインヘルプ

Threat Grid ポータルのユーザマニュアル（リリースノート、『Using Threat Grid Online Help』、API に関する資料その他の情報を含む）は、ユーザインターフェイス上部のナビゲーションバーにある **[Help]** メニューから入手できます。

E メール セキュリティ アプライアンスと Web セキュリティアプライアンスに関する資料

E メール セキュリティ アプライアンス（ESA）または Web セキュリティアプライアンス（WSA）の接続に関する詳細については、「ESA/WSA の Threat Grid アプライアンスへの接続」を参照してください。

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。

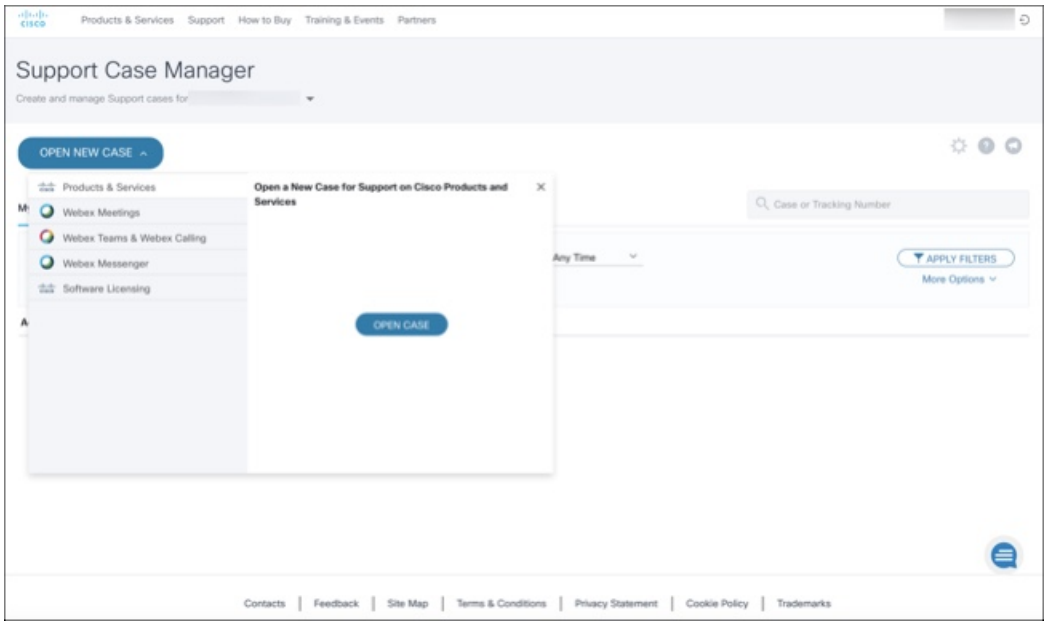
- 『*Cisco Email Security Appliance User Guide*』
- 『*Cisco Web Security Appliance User Guide*』

Threat Grid のサポート

Threat Grid に関するご質問やサポートについては、https://mycase.cloudapps.cisco.com/case でサポートケースをオープンしてください。

ステップ 1 Support Case Manager で、**[Open New Case] > [Open Case]** をクリックします。

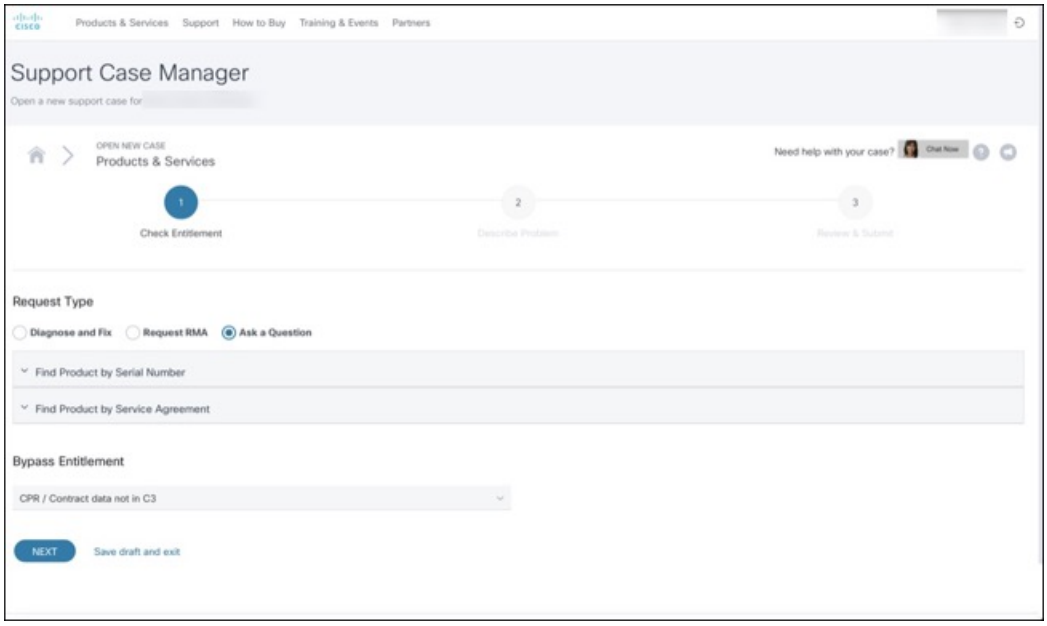
図 *1 :* 新しいケースをオープンする



ステップ 2 [**Ask a Question**] オプションボタンをクリックし、使用中のシスコセキュリティ**製品シリアル番号**または**製品サービス契約**を検索します。検索の対象は、Threat Grid のシリアル番号またはサービス契約である必要があります。

ステップ 3 エンタイトルメントをバイパスする場合は、[**Contract Data not in C3**] を選択し、[**Next**] をクリックします。

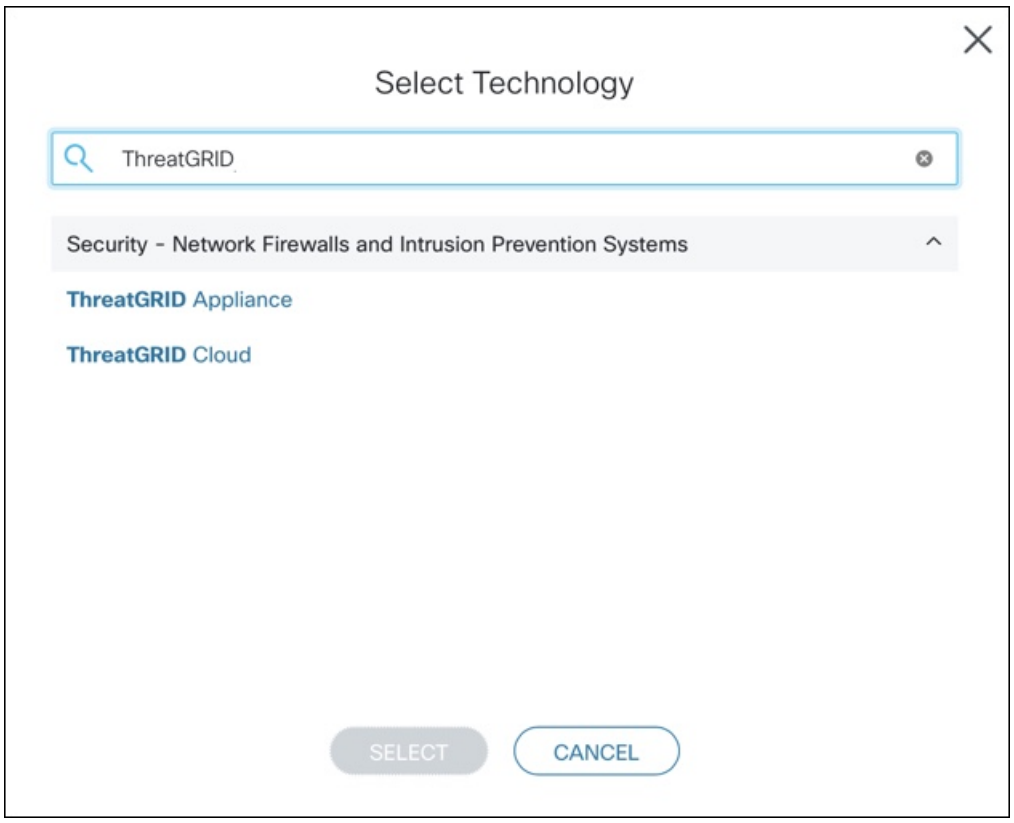
図 *2 :* エンタイトルメントのチェック



ステップ 4 [**Describe Problem**] ページで、問題の [**Title**] と [**Description**] を入力します（タイトルで Threat Grid に言及してください）。

ステップ 5 [**Manually select a Technolog**] をクリックして、**ThreatGRID** を検索します。

図 *3*:テクノロジーの選択



ステップ 6 リストから [**ThreatGRID Appliance**] を選択し、[**Select**] をクリックします。

ステップ 7 フォームの残りの部分をすべて入力し、[**Submit**] をクリックします。

ケースをオンラインで開くことができない場合は、シスコサポートにお問い合わせください。

- **米国およびカナダ**：1-800-553-2447
- **各国の連絡先**：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

サポートを依頼する方法の詳細については、以下を参照してください。

- 次のブログ記事を参照してください。『**Changes to the Cisco Threat Grid Support Experience**』（https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407）
- https://www.cisco.com/c/en/us/support/index.html で**シスコサポート & ダウンロード**のメインページを参照してください。

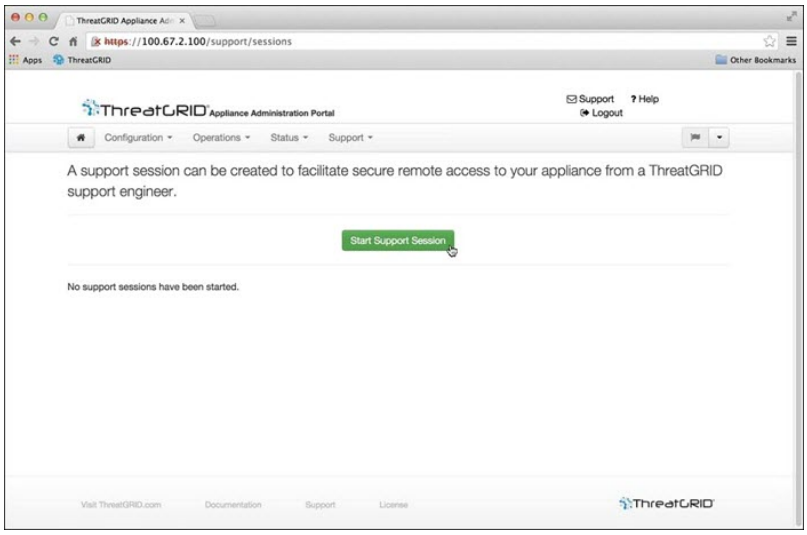
サポート モードの有効化

Threat Grid のエンジニアからのサポートが必要なときに、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、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アクセス権が付与されます。アプライアンスの通常の動作には影響しません。

OpAdmin ポータルの [**Support**] メニューからサポートモードを有効にすることができます。TGSH ダイアログ、レガシーの Face Portal UI から有効にするか、リカバリモードで起動する際に有効にすることもできます。

ステップ 1 OpAdmin ポータルで [**Support**] メニューをクリックして、[**Live Support Session**] を選択します。

図 *4 : OpAdmin* でのライブサポートセッションの開始



ステップ 2 [**Start Support Session**] をクリックします。

（注） OpAdmin 設定ウィザードを終了して、ライセンシングの前にサポートモードを有効にすることができます。

サポート スナップショット

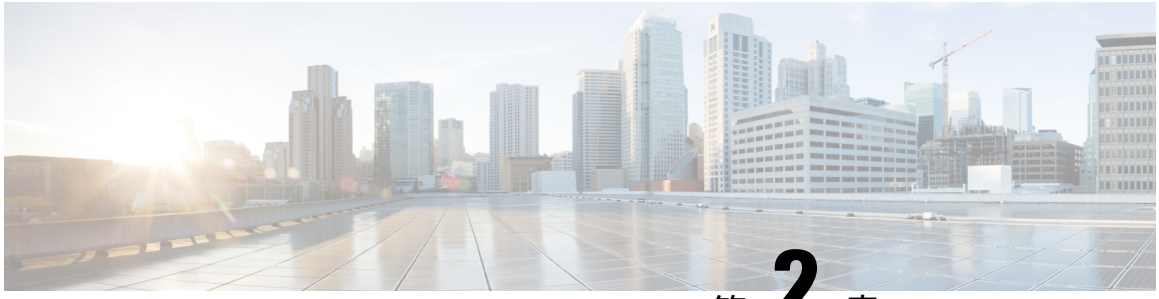
サポートスナップショットは、基本的に実行中のシステムのスナップショットで、ログ、psoutput などが含まれており、サポートスタッフによる問題のトラブルシューティングに役立ちます。

ステップ 1 SSH がサポート スナップショット サービスに指定されていることを確認します。

ステップ 2 [**Support**] メニューから、[**Support Snapshots**] を選択します。

ステップ 3 スナップショットを取得します。

ステップ 4 スナップショットを取得したら、**.tar** ファイルまたは **.gz** ファイルとしてダウンロードするか、[**Submit**] をクリックして、スナップショットを Threat Grid スナップショットサーバに自動的にアップロードします。



第 2 章

管理

この章では、管理者にとって役立つ一般的な情報を提供します。説明する項目は次のとおりです。

ログイン名とパスワード（デフォルト）

デフォルトのログイン名とパスワードを次の表に示します。

ユーザ（User）	ログイン/パスワード
OpAdmin およびシェルユーザ	最初の Threat Grid/TGSH ダイアログでランダムに生成されたパスワードを使用し、次に OpAdmin 設定ワークフローの最初の手順で入力した新しいパスワードを使用します。 パスワードを紛失した場合は、「管理者パスワードのリセット」の手順に従ってください。
Threat Grid Web ポータル UI 管理者	Login: **admin** パスワード：最初の OpAdmin パスワードを使用して初期化します。初期化の後、独立した状態になります。
CIMC	Login: **admin** Password: **password**

管理者パスワードのリセット

デフォルトの管理者パスワードは、アプライアンスの初期設定と設定の際にTGSHダイアログのみで表示されます。初期設定が完了すると、管理者パスワードは、読み取り可能な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に、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。

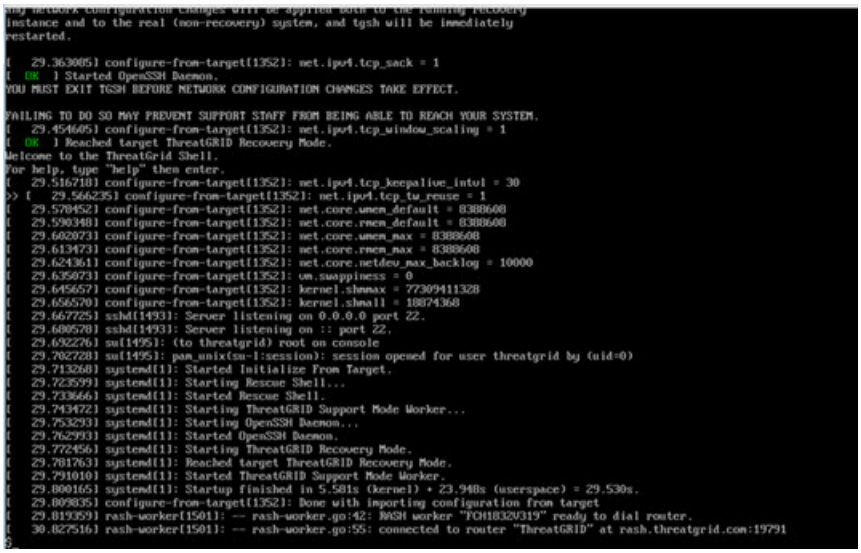
管理者パスワードを紛失してOpAdminにログインできない場合は、次の手順を実行してパスワードをリセットします。

ステップ1 Threat Gridアプライアンスを再起動して、すぐに[Recovery Options]から[**Recovery Mode**]を選択します。

図 *5 :* ブートメニュー：*[Recovery Mode]*

Threat Gridシェルが開きます。

図 *6* : リカバリモードの *Threat Grid* シェル



ステップ 2 `passwd` を実行して、パスワードを変更します。

図 *7 : Enter New Password*

（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、ロギング出力がいずれかの時点で入力と重なるように表示されることがあります。この表示は入力には影響しません。ブラインド入力を続けることができます。2 行のロギング出力は無視します。

ステップ 3 パスワードを（ブラインドで）入力し、**Enter** キーを押します。

ステップ 4 パスワードをもう一度入力して、**Enter** キーを押します。

（注） パスワードは表示されません。

ステップ 5 コマンドラインで **exit** と入力して保存します。

重要 新しいパスワードを保存するには、再起動の前に exit を入力する必要があります。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。

ステップ 6 「**Reboot**」と入力し、**Enter** キーを押して、アプライアンスを通常モードで起動します。

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前に、『*Cisco 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を完了しておく必要があります。

（注） 新しい Threat Grid アプライアンスが古いバージョンのソフトウェアを搭載して出荷された場合、更新をインストールするには、まず初期設定を完了する必要があります。更新は、ライセンスがインストールされていない限りダウンロードされず、Threat Grid アプライアンス（データベースを含む）が完全に設定されていないと、正しく適用されない可能性があります。

更新をインストールする際、次の点を考慮する必要があります。

- Threat Grid アプライアンスの更新プログラムは OpAdmin Portal を使用して適用します。
- 更新サーバが更新を送信すると、クライアントは更新後のバージョンに完全に移行します。暫定リリースをスキップすることが常に可能というわけではありません。スキップできない場合、更新サーバは、次の更新をダウンロードする前に、アプライアンスにリリースをインストールするよう求めます。
- サーバが特定のバージョンのダウンロードを許可する場合、そのバージョンに直接移行することができます。つまり、単一のアップグレードに必要な再起動以外の再起動を途中で求められることはありません。
- 更新は不可逆です。つまり、新しいバージョンにアップグレードした後、前のバージョンに戻すことはできません。

更新のインストール手順については、『*Cisco Threat Grid Appliance Setup And Configuration Guide*』の「Install Threat Grid Appliance Updates」のセクションを参照してください。

バージョン ルックアップ テーブル

正しいビルド番号と対応するリリースバージョンを確認するには、『*Cisco Threat Grid Appliance Version Lookup Table*』を参照してください。

更新に使用されるポート

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。

- リリース更新は、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も適用できます。
- 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。DNS サーバが明示的に指定されていないシステム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

「*database upgrade not successful*（データベースのアップグレードに失敗しました）」のメッセージは、新しいThreat Gridアプライアンスが古いバージョンのPostgreSQLを実行しており、データベースの自動移行プロセスに失敗したことを意味します。v2.0へのアップグレードの前に、この状態を修正することが必要です。

詳細については、『*Cisco Threat Grid Appliance Release Notes v2.0.1*』を参照してください。

データベーススキーマの更新

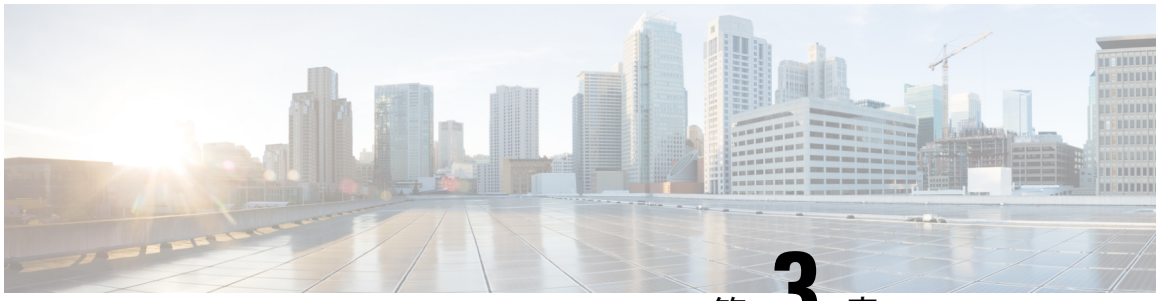
従来、スタンドアロンアプライアンスでは、システムがシングルユーザモードでオフラインになっている間に、更新に関連したデータベース移行が発生しました（最初にアップグレードされたノードがオンラインに戻った後に更新が発生したクラスタは除きます。こうしたクラスタが例外になるのは、バックグラウンドで実行される可能性のある非常に長い更新が発生するためです。このような更新はケースバイケースで処理されました）。

Threat Gridアプライアンス（v2.5.0以降）は、システムの再起動が完了した後にデータベーススキーマを更新します。そのため、起動プロセスの所要時間がやや長くなる場合があります。（非常に長い再起動は、引き続きケースバイケースで処理されます）。

以前のリリースでは、バックアップサポートが有効になっているクラスタ化されていないシステムは、NFSサーバがダウンした場合、正常な動作をベストエフォートで試行していました。この動作は、Elasticsearch機能の変更により、現在は保証できなくなっています。

v2.7.2以降、ES6ネイティブインデックスへのバックグラウンドElasticsearchインデックスの移行が有効になりました。この移行は、Elasticsearch 7.0以降が必要なバージョンのThreat Gridアプライアンスがインストールされる前に、正常に完了している必要があります。

（注） Elasticsearchインデックスの移行により、NFSバックアッププロセスに大幅な遅延が発生し、関連した警告が発生する可能性があります。インデックス移行がアクティブに進行中であることを示す場合、これらの警告は無視する必要があります。インデックス移行プロセスが長時間にわたって先に進まない場合は、サポート付きのチケットのみを生成する必要があります。



第 3 章

構成管理

この章では、初期設定後の Threat Grid アプライアンスの設定に関する追加情報について説明します。説明する項目は次のとおりです。

はじめに

Threat Grid アプライアンスの初期設定は、アプライアンスのセットアップ時に、『*Cisco Threat Grid Appliance Setup And Configuration Guide*』の説明に従って、TGSH ダイアログと OpAdmin ポータルを使用して実行します。

（注） Threat Grid 組織およびユーザアカウントは、Threat Grid Portal UI で管理します（ナビゲーションバーのログイン名の横にあるドロップダウン矢印から選択）。

TGSH ダイアログを使用したネットワーク設定

初期ネットワーク設定は、TGSH ダイアログを使用して実行します（『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照）。このセクションでは、TGSH ダイアログの使用に関する追加情報について説明します。

TGSH ダイアログを使用したネットワークの設定

ネットワークの初期設定を変更する場合は、次の手順を実行します。

（注） DHCP を使用して IP を取得する場合は、「ネットワーク設定と DHCP」を参照してください。

ステップ 1 TGSH ダイアログにログインします。

（注） 認証が [**LDAP Only**] に設定されている場合、TGSH ダイアログにログインするには LDAP を使用する必要があります。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で許可されるのは**システム**ログインのみです。

ステップ 2 TGSH ダイアログのインターフェイスで、[CONFIG_NETWORK] を選択します。

[**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。

ステップ 3 必要な変更を行います（新しいエントリを入力する前に、バックスペースを押して古いエントリを削除する必要があります）。

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

ステップ 5 ネットワーク設定の更新が完了したら、Tab キーで下に移動し、[**Validate**] を選択してエントリを確認します。

エラーが発生した場合は、無効な値を修正し、もう一度 [**Validate**] を選択します。

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

ステップ 6 [Apply] を選択して各種設定を適用します。

行われた設定変更に関する詳細情報が表示されます。

ステップ 7 [OK] を選択します。

[**Network Configuration**] コンソールが再更新され、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上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 を使用することでアクセスできます。

TGSH ダイアログに再接続するには、ユーザ「**threatgrid**」として管理 IP アドレスに SSH 接続します。必要なパスワードは、ランダムに生成される初期パスワードであり、最初に TGSH ダイアログに表示されたパスワードか、OpAdmin 設定の最初の手順で作成した新しい管理者パス

ワードです（『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください）。

リカバリモードでのネットワークの設定

リカバリモードでのネットワークの設定は、システム全体に反映されます（バージョン2.7 以降）。

- すべてのインターフェイスが起動します。
- ファイアウォールルールとポリシールーティングにより、どのプロセスがどのインターフェイスで通信するかが制限されます。

（注） ポート 19791 のサポートモードトラフィックは、3 つのインターフェイスすべての許可リストに含まれています。

リカバリモードでネットワーキングを設定するには、次の手順を実行します。

ステップ 1 Threat Grid アプライアンスを再起動してから、起動メニューで [**Recovery Mode**] を選択します。

ステップ 2 システムが起動したら、**Enter** キーを数回押して clean コマンド プロンプトを表示させます。

ステップ 3 「**netctl clean**」と入力し、次の情報を入力します。

- [**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>
- [**Final Question**]：「**y**」と入力

ステップ 4 **Exit** と入力して設定を適用します。

アプライアンスは、ポート 19791/tcp のクリーンインターフェイスでアウトバウンドサポート接続を開こうとします。

OpAdmin ポータルを使用した設定

初期設定および設定ウィザードについては、『Cisco Threat Grid Appliance Setup and Configuration Guide』を参照してください。新しい Threat Grid アプライアンスでは、管理者が付加的な設定を実行する必要があります。また OpAdmin の設定には、時間の経過とともに更新が必要になる場合があります。

OpAdmin ポータルは、Threat Grid アプライアンス管理者の主要な設定インターフェイスです。Threat Grid アプライアンスの管理インターフェイスで IP アドレスが設定された後に使用できる Web ポータルです。

OpAdmin ポータルは、次のような各種の Threat Grid アプライアンスの設定を決定し管理するために使用されます。

- 管理者のパスワード（OpAdmin および **threatgrid** ユーザの場合）
- 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
- サードパーティ検出およびエンリッチメントサービス（ClamAV、OpenDNS、Titanium Cloud、VirusTotal など）

（注）

- 設定時に IP アドレスが遮断される可能性を減らすために、OpAdmin での設定の更新は 1 回のセッションで完了する必要があります。
- OpAdmin はゲートウェイエントリを検証しません。誤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。ネットワーク設定を管理インターフェイスで実行した場合は、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。
- Threat Grid アプライアンス（v2.7 以降）は、ホスト名としてシリアル番号を使用することにより、一部の NFS v4 サーバとの相互運用性を向上させます。

重要 OpAdmin は HTTPS を使用するため、ブラウザのアドレスバーに HTTPS を入力する必要があります。管理 IP をポイントするだけでは十分ではありません。ブラウザに次のアドレスを入力します。

https://adminIP/

または

https://adminHostname/

SSH キーの設定

SSH キーを設定すると、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。

ルートアクセスやコマンドシェルは提供されません。**[Configuration] > [SSH]**で複数のキーを追加できます。

Threat Grid アプライアンスにアクセスするための SSH 公開キーを設定すると、SSH を使用したパスワードベースの認証が無効になります（v2.7.2 以降）。そのため、2 つの SSH 認証方式は、両方ではなくどちらか一方のみが有効になります。キーベース認証を使用して SSH 接続が成功すると、TGSH ダイアログで、両方のトークンが必要なパスワードの入力を求められます。

通知用のリモート Syslog サーバの設定

電子メールでシステム通知を配信するように設定できる定期的な通知に加えて（OpAdmin の [**Configuration**] > [**Notifications**]）、syslog メッセージと Threat Grid 通知を受信するようにリモート syslog サーバを設定できます。

ステップ 1 OpAdmin ポータルにログインし、**[Configuration] > [Syslog]** をクリックします。

ステップ 2 **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）。

ステップ 3 設定を保存した後に DNS ルックアップを実行するには、[**Verification**] チェックボックスをオンにします。

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**] チェックボックスをオンにしなかった場合、アプライアンスは、DNS で有効な名前かどうかにかかわらず、任意の名前を受け入れます。

ステップ 4 [Save] をクリックします。

Syslog DNS を編集または削除するには、**[Configuration] > [Syslog]** を開き、変更を加えてから、[**Save**] をクリックします。

LDAP 認証の設定

Threat Grid アプライアンスは、OpAdmin ログインと TGSH ダイアログログインのための LDAP による認証と許可をサポートしています。

ドメインコントローラまたは LDAP サーバで管理されるさまざまなログイン情報を使用して、複数のアプライアンス管理者を認証できます。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。

次の点を考慮する必要があります。

- デュアル認証モード（**システムパスワードまたは LDAP**）は、LDAP の設定時に、Threat Grid アプライアンスから誤ってロックアウトされないようにするために必要です。

  最初から [**LDAP Only**] を選択することはできません。まずデュアルモードを実行して、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 からログアウトした後、LDAP ログイン情報を使用して再度ログインして [**LDAP Only**] に切り替える必要があります。

- 認証を [**LDAP Only**] に設定した場合、TGSH ダイアログにログインするには LDAP を使用する必要があります。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で許可されるのはシステムログインのみです。

- Threat Grid アプライアンスが LDAP 認証のみ（[**LDAP Only**]）に設定されている場合は、リカバリモードでパスワードをリセットして、認証モードを再設定し、システムパスワードによるログインを許可することもできます。

- 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 ポータルでは、[**LDAP Only**] モードの場合にのみ LDAP ログイン情報が必要です。[**LDAP Only**] に設定されている場合、TGSH ダイアログでは、システムパスワードではなく、LDAP ユーザ/パスワードの入力のみが求められます。

- 認証が [**System Password or LDAP**] に設定されている場合、TGSH ダイアログでは、これら両方ではなく、システムパスワードのみを入力するように求められます。

- LDAP の問題をトラブルシューティングするには、リカバリモードでパスワードをリセットして LDAP を無効にします。

- SSH を使用して TGSH ダイアログにアクセスするには、[**LDAP Only**] モードの場合、LDAP ログイン情報に加えて、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。

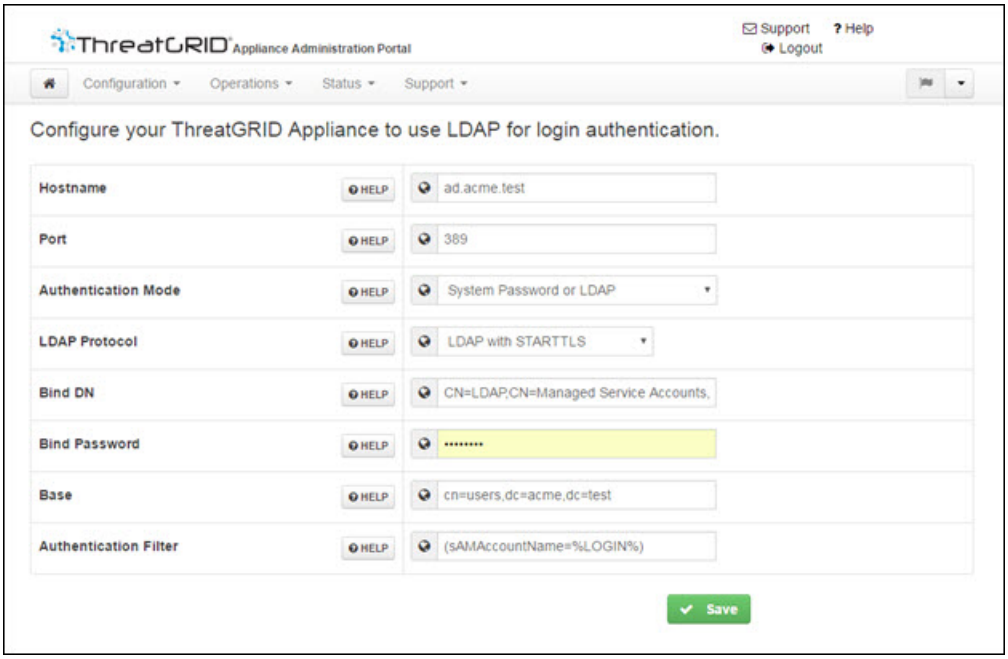
- LDAP はクリーン インターフェイスからの発信です。

OpAdmin での LDAP 認証の設定

OpAdmin ポータルで LDAP 認証を設定するには、次の手順を実行します。

ステップ 1 OpAdmin ポータルにログインし、**[Configuration] > [LDAP]** を選択して [LDAP Configuration] ページを開きます。

図 *8 : LDAP* 認証の設定



ステップ 2 ページのフィールドに入力します。各フィールドの横にある [**Help**] アイコンをクリックすると、詳細な説明と情報を表示できます。

（注） LDAP 認証を最初に設定するときは、[**System Password** or **LDAP**] を選択し、OpAdmin からログアウトしてから、LDAP ログイン情報を使用して再度ログインする必要があります。その後、[**LDAP Only**] を実装するように設定を変更できます。

ステップ 3 [Save] をクリックします。

ユーザが OpAdmin または TGSH ダイアログにログインすると、次のいずれかの画面が表示されます。

図 *9 : [LDAP Only]*

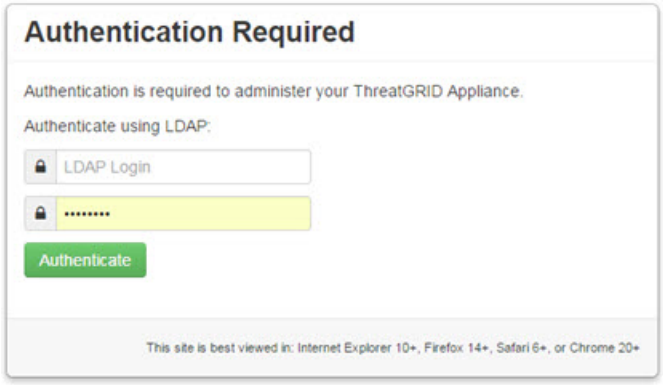
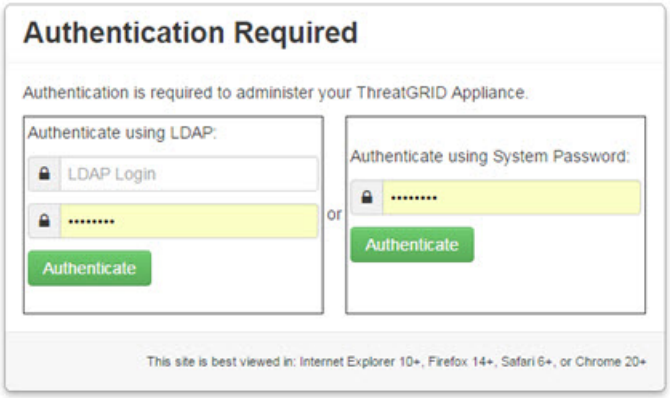


図 *10 : [System Password or LDAP]*



サードパーティ検出およびエンリッチメントサービスの設定

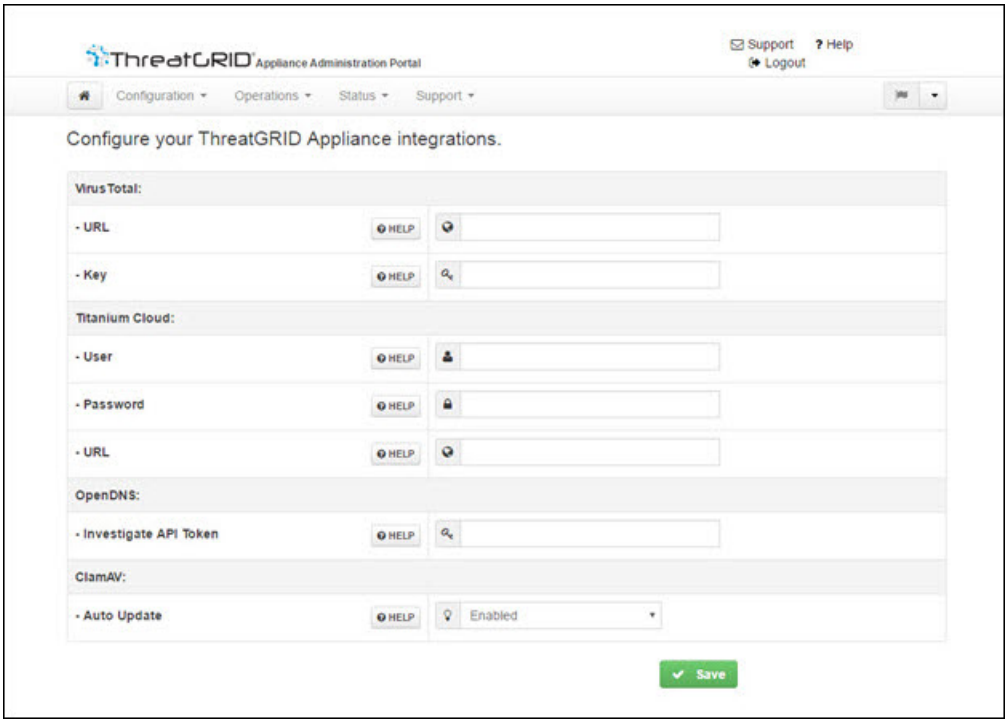
OpenDNS、TitaniumCloud、VirusTotal といった複数のサードパーティ検出およびエンリッチメントサービスとの統合を、[**Integration**] ページを使用してアプライアンスで設定できます（v2.2 以降）。

クラウド検索フェデレーション機能（v2.8 以降で使用可能）により、クラウドエンドポイントが（管理インターフェイスの [**Integrations**] ページで）設定されている場合、Threat Grid クラウドインスタンスに対して検索クエリを再実行する、ポータルアプリケーション UI のオプションが使用可能になります。

（注） OpenDNS が設定されていない場合、分析レポートの [Domains] エンティティページに **whois** 情報（UI のマスクバージョン）は表示されません。

ステップ 1 OpAdmin ポータルにログインし、**[Configuration] > [Integrations]** をクリックして [**Integrations**] ページを開きます。

図 *11* : 統合の設定



ステップ 2 必要な認証情報などの値を入力します。

（注） ClamAV シグネチャは、毎日自動的に更新できます。この署名はデフォルトで有効になっており、[**ClaimAV**] フィールドで無効にすることができます。

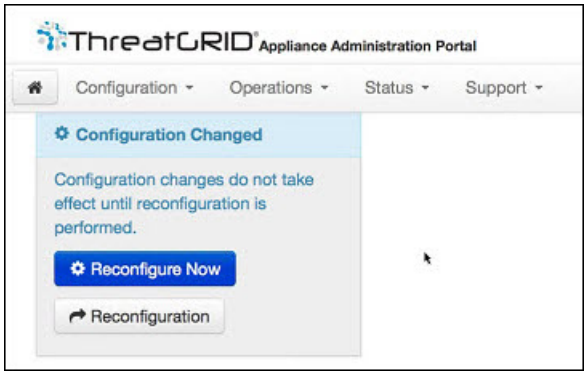
ステップ 3 **[Save]** をクリックします。

設定変更の適用

設定が変更されると、[**Configuration**] メニューの下にライトブルーの [**Configuration Changed**] アラートが表示されます。OpAdmin の設定を更新した場合、新しい設定を別の手順で保存する必要があります。

ステップ 1 [**Configuration Changed**] をクリックして、ダイアログを開きます。

図 *12 :* 設定変更ダイアログ



ステップ 2 [**Reconfigure Now**] をクリックして、変更をアプライアンスに適用します。

DHCP の使用

ほとんどの Threat Grid アプライアンスユーザは、DHCP で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、このセクションを読み、要件を理解することが重要です。

（注） アプライアンスの初期ネットワーク設定で DHCP を使用したものの、静的 IP アドレスに切り替える必要が生じた場合は、「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 ポータルインターフェイスにアクセスして設定するために必要な情報が表示されます。アプライアンスの起動後、DHCP の IP アドレスが表示されるまでに時間がかかる場合があります。

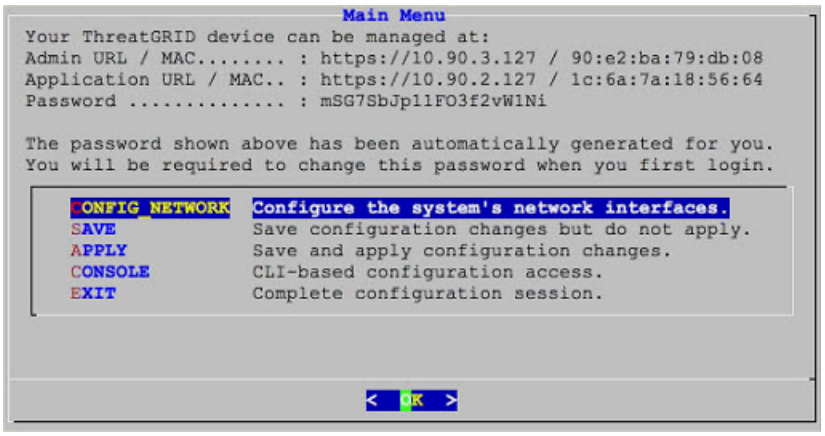
DHCP の明示的 DNS

DHCP を使用する Threat Grid アプライアンスでは、DNS を明示的に指定する必要があります。

警告 DNS サーバが明示的に指定されていないシステムのアップグレードは失敗します。

TGSH ダイアログを開き、次の情報を確認します。

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済み）



- [**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。
- [**Application URL**]：クリーンネットワーク。OpAdmin を使用して設定を完了した後に、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。
- [**Password**]：Threat Grid 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る初期管理パスワード。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。

DHCP を永続的に使用する場合、管理 IP アドレスを静的に変更する必要がない限り、追加のネットワーク設定は必要ありません。

ネットワーク設定と DHCP

初期設定に DHCP を使用した後、3 つのネットワークすべてに関して、IP 割り当てを DHCP から固定的な静的 IP アドレスに調整する必要がある場合は、次の手順を実行します。

（注） OpAdmin はゲートウェイエントリを検証しません。誤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。ネットワーク設定を管理インターフェイスで実行した場合は、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。

ステップ 1 OpAdmin ポータルで、ナビゲーションウィンドウの [**Network**] をクリックします（[License] ウィンドウで **[Configuration] > [Network]** がオンになっていても、DHCP ネットワーク設定は完了していません）。

[**Network**] ページが開きます。

ステップ 2 次のフィールドに入力します。

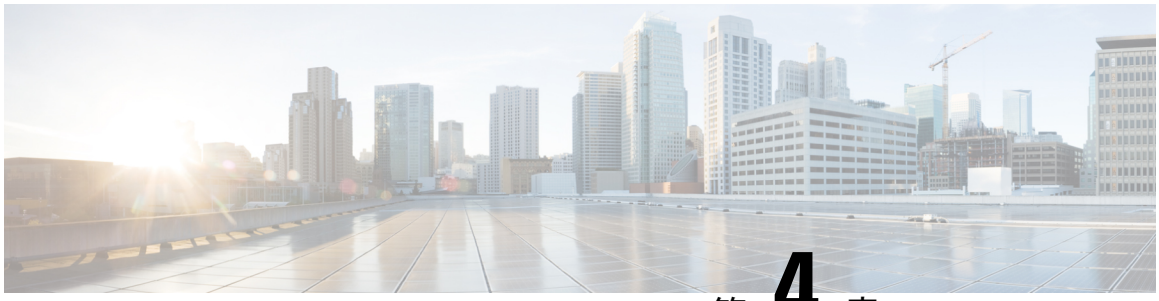
（注） 管理ネットワークの設定は、最初の Threat Grid アプライアンスのセットアップおよび設定時に **TGSH ダイアログ**を使用して設定されています。

- [**IP Assignment**]：クリーンとダーティ両方のネットワーク インターフェイスのドロップダウンリストから [**Static**] を選択します。
- [**IP Address**]：クリーンまたはダーティ ネットワーク インターフェイスの静的 IP アドレスを入力します。
- [**Subnet Mask**]：ネットワーク インターフェイスのタイプに応じて入力されます。
- [**Validate DNA Name**]：クリーン ネットワーク インターフェイスの場合、[**Validate DNA Name**] チェックボックスをオンにして、DNS が IP アドレスに解決されていることを確認します。
- [**Primary and Secondary DNS**]：プライマリおよびセカンダリ DNS サーバの情報を入力します。

ステップ 3 [**Next（Applies Configuration**）] をクリックして、ネットワーク構成の設定を保存します。

（注） 電子メール設定は [**Email**] ページから管理され、NTP サーバは [**Date and Time**] ページで管理されます。

ステップ 4 [**Configuration Changed**] をクリックし [**Reconfigure Now**] を選択して、DHCP 設定を適用します。



第 4 章

SSL 証明書の管理

この章では、Threat Grid アプライアンスの SSL 証明書と、統合されたアプライアンスおよびデバイスの管理について説明します。説明する項目は次のとおりです。

SSL 証明書と Threat Grid アプライアンスの概要

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。次の情報は、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）、AMP for Endpoints プライベートクラウドといった統合先との Threat Grid アプライアンスの接続をサポートするように SSL 証明書を設定する手順の実行に役立ちます。

（注） 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に含まれていません。

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 ポータルの UI と API、および統合先（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）用の**クリーン**インターフェイス。
- OpAdmin ポータル用の**管理**インターフェイス。

サポートされている SSL/TLS バージョン

Threat Grid アプライアンスでは、次のバージョンの SSL/TLS がサポートされています。

- TLS v1.0：管理インターフェイスでは無効（v2.7 以降）
- TLS v3.0：管理インターフェイスでは無効（v2.7 以降）
- TLS v1.2

（注） TLS v1.0 と TLS v3.0 は、管理インターフェイスでは無効になっており（v2.7 以降）、メインアプリケーションでもデフォルトでは無効になっています。これらのプロトコルのいずれかが統合の互換性のために必要な場合は、TGSH から再有効化できます（メインアプリケーションに対してのみ）。

サポートされているお客様提供の CA 証明書

お客様提供の CA 証明書がサポートされており（v2.0.3 以降）、お客様独自の信頼できる証明書または CA 証明書をインポートすることができます。

自己署名デフォルト SSL 証明書

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。管理者はこれらの SSL 証明書を置き換えることができます。

Threat Grid アプライアンスのデフォルト SSL 証明書のホスト名（共通名）は **pandem** で、10 年間有効です。設定時に別のホスト名が Threat Grid アプライアンスに割り当てられた場合、証明書内のホスト名と共通名は一致しなくなります。

証明書内のホスト名は、接続先の ESA アプライアンスや WSA アプライアンス、または他の統合先のシスコデバイスやサービスによって想定されるホスト名とも一致している必要があります。多くのクライアントアプリケーションは、証明書で使用される共通名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

E メールセキュリティアプライアンス、Web セキュリティアプライアンス、AMP for Endpoints プライベートクラウドなどのシスコのセキュリティ製品は、Threat Grid アプライアンスと統合して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。

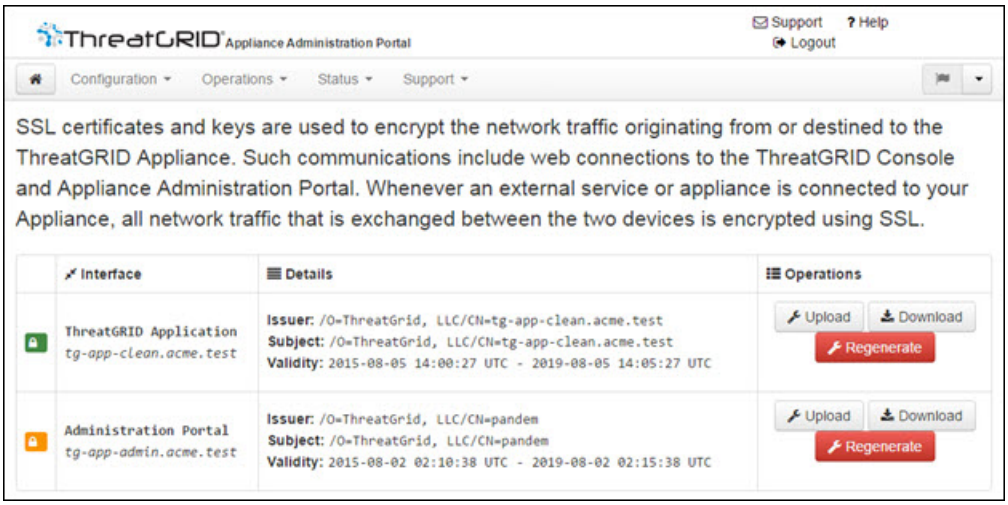
統合するアプライアンスまたは他のデバイスは、Threat Grid アプライアンスの SSL 証明書を信頼できる必要があります。まず、ホスト名が共通名と一致していることを確認する必要があります。一致していない場合は、再生成するか置き換える必要があります。その後、Threat Grid

アプライアンスからSSL証明書をエクスポートし、統合する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アプライアンスの証明書は、[**SSL Certificate**]ページで設定されます。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。

ステップ1 OpAdminポータルで、**[Configuration] > [SSL]** をクリックして、SSL証明書の設定ページを開きます。

図 *14 : SSL* 証明書の設定ページ



この例では、クリーンインターフェイス用の「**ThreatGRID Application**」と管理インターフェイス用の「**Administration Portal**」という2つのSSL証明書を取り上げます。

ステップ2 SSL証明書で使用されている共通名（緑色の南京錠アイコン）とホスト名が一致することを確認します。「SSL 証明書の共通名の検証」を参照してください。

SSL 証明書の共通名の検証

ホスト名は、Threat Gridアプライアンスの SSL証明書で使用される共通名と一致している必要があります。

[SSL Certificate]ページで、インターフェイス名の左側の列にある南京錠アイコンは、SSL証明書のステータスを示しています。

- **緑色**：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共通名と一致していることを示します。
- **黄色**：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共通名と一致していないことを示します。現在のホスト名を使用している証明書に置き換える必要があります（「SSL 証明書の置き換え」を参照）。

SSL 証明書の置き換え

通常、SSL 証明書は、証明書が期限切れになった、ホスト名が変更された、または他のシスコデバイスやサービスとの統合をサポートするためなど、さまざまな理由からいずれかの時点で置き換える必要があります。

Cisco E メールセキュリティアプライアンス、Web セキュリティアプライアンスなどの CSA シスコ統合デバイスでは、記載の共通名が Threat Grid アプライアンスのホスト名と一致する SSL 証明書が必要になる場合があります。デフォルトの SSL 証明書を、同じホスト名を使用して Threat Grid アプライアンスにアクセスする、新たに生成された証明書に置き換える必要があります。

Threat Grid アプライアンスを AMP for Endpoints プライベートクラウドと統合して、その配置更新サービスを使用する場合は、Threat Grid アプライアンスが接続を信頼できるように、AMP for Endpoints プライベートクラウド SSL 証明書をインストールする必要があります。

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。

- 共通名に現在のホスト名を使用するSSL 証明書の再作成します。
- SSL 証明書のダウンロードします。
- SSL 証明書のアップロードします。これは市販の SSL や企業向けの SSL の場合もあれば、OpenSSL を使用して作成したものである場合もあります。
- OpenSSL を使用した SSL 証明書の作成

SSL 証明書の再作成

ホスト名が証明書の共通名と一致しない場合は、[**SSL Certificate**] ページで SSL 証明書を再生成できます。

ステップ 1 OpAdmin ポータルで、 **[Configuration] > [SSL]** をクリックして [**SSL Certificate**] ページを開きます。

ステップ 2 [Operations] 列で、新しい証明書を必要とするインターフェイスのための [**Regenerate**] をクリックします。

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。この証明書の [Common Name] フィールドでは、アプライアンスの現在のホスト名が使用されます。インターフェイス名の横にある [Common Name] 検証用の南京錠アイコンが緑色に変わります。

再生成された証明書（SSL 証明書のダウンロードファイル）を**ダウンロード**して、統合するアプライアンスにインストールできるようになりました。

SSL 証明書のダウンロード

Threat Grid アプライアンスの SSL 証明書を統合先のデバイスにダウンロードしてインストールし、Threat Grid アプライアンスからの接続をデバイスが信頼できるようにすることができます。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [SSL]** をクリックして、SSL 証明書の設定ページを開きます。

ステップ 2 [Operations] 列で、インターフェイス証明書の [**Download**] をクリックします。SSL 証明書の **.cert** ファイルがダウンロードされます。

ステップ 3 ダウンロードした SSL 証明書（**.cert** ファイル）を、E メール セキュリティ アプライアンス、Web セキュリティアプライアンス、AMP For Endpoints プライベートクラウド、または他のシスコ製品に、製品マニュアルに従ってインストールします。

SSL 証明書のアップロード

組織で商用または企業向けの SSL 証明書をすでに運用している場合は、その証明書を使用して Threat Grid アプライアンス用の新しい SSL 証明書を生成し、統合先のデバイスに対して CA 証明書を使用することができます。

ステップ 1 OpAdmin ポータルで、 **[Configuration] > [SSL]** をクリックして [**SSL Certificate**] ページを開きます。

ステップ 2 [Operations] 列で、適切なインターフェイスの [**Upload**] をクリックします。

インターフェイス名の横にある [Common Name] 検証用の南京錠アイコンが緑色に変わります。

OpenSSL を使用した SSL 証明書の作成

オンプレミスの SSL 証明書インフラストラクチャが設置されていない場合、OpenSSL を使用して SSL 証明書を手動で生成し、Threat Grid アプライアンスにアップロードすることができます（「SSL 証明書のアップロード」を参照）。OpenSSL は、OpenSSL 証明書、キー、その他のファイルを作成および管理するための標準的なオープンソース SSL ツールです。

（注） OpenSSL はシスコ製品ではないため、テクニカルサポートは提供されません。OpenSSL の使用方法の詳細については、Web を検索することをお勧めします。シスコは、SSL 証明書を生成するための SSL ライブラリ *Cisco SSL* を提供しています。

ステップ 1 次のコマンドを実行して、新しい自己署名 SSL 証明書を生成します。

```
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）管理の使用を指定します。X.509 は、キーおよび証明書の管理に SSL と TLS が使用する公開キーインフラストラクチャの標準規格です。次の例では、このパラメータを使用して、新しい X.509 証明書を作成します。

-x509：証明書署名要求を生成せずに、自己署名証明書を作成するように req パラメータ X.509 を変更します。

-days 3650：このオプションは、証明書が有効と見なされる期間を設定します。この例では、10 年間に設定されています。

-newkey rsa: 4096：新しい証明書と新しいキーを同時に生成するように指定します。必要なキーが事前に作成されなかったため、証明書を使用して作成する必要があります。パラメータ「**rsa:4096**」は、4096 ビット長の RSA キーを作成することを示します。

-keyout：このパラメータは、作成中の秘密キーファイルが OpenSSl によって保存される場所を示します。

-nodes：このパラメータは、パスフレーズを使用して証明書を保護するためのオプションを OpenSSL がスキップする必要があることを示します。サーバの起動時に、アプライアンスは、ユーザの介入なしでファイルを読み取ることができる必要があります。パスフレーズで保護されている証明書の場合、サーバの再起動のたびにユーザがパスフレーズを入力する必要があります。

-out：このパラメータは、作成中の証明書が OpenSSL によって保存される場所を示します。

-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。この名前には、Threat Grid アプライアンスのホスト名（この例では **tgapp**）と、関連するドメイン名（この例では **acmeco.com**）が含まれます。

  重要　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、少なくとも共通名を変更する必要があります。

ステップ 2　新しい SSL 証明書が生成されたら、**[SSL Certificate]** ページから Threat Grid アプライアンスに証明書をアップロードします（「SSL 証明書のアップロード」を参照）。E メール セキュリティ アプライアンスまたは Web セキュリティアプライアンスに証明書（**.cert** ファイルのみ）をアップロードする必要もあります。

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（v2.0.3 以降）は、配置更新サービス用の Cisco AMP for Endpoints プライベートクラウドとの統合をサポートしています。この統合は、Threat Grid アプライアンスから見ればアウトバウンド接続になります。

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。AMP for Endpoints プライベートクラウドなど、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で解決できない（統合にクリーンインターフェイスが使用されるため）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 で設定できます。

ステップ 1 OpAdmin で、**[Configuration] > [Network]** をクリックします。

ステップ 2 ダーティネットワークとクリーンネットワークの [**DNS**] フィールドに入力します。

ステップ 3 **[Save]** をクリックします。

CA 証明書の管理

OpAdmin ポータルの [**CA Certificate**] ページは、アウトバウンド SSL 接続用の CA 証明書信頼ストアを管理するために使用されます。この機能により、Threat Grid アプライアンスは、Cisco AMP For Endpoints プライベートクラウドを信頼して、悪意があると見なされた分析済みサンプルについて通知することができます。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [CA Certificates]** をクリックします。

ステップ 2 次のインポートオプションのいずれかを選択します。

- サーバから証明書を取得するには、[**Import from Host**] を選択します。AMP for Endpoints プライベートクラウドの [**Host**] と [**Port**] に入力してから、[**Retrieve**] をクリックします。
- [**Import from Clipboard**] を選択し、クリップボードから PEM を貼り付けた後、[**Add Certificate**] をクリックします。

ステップ 3 **[インポート (Import)]** をクリックします。

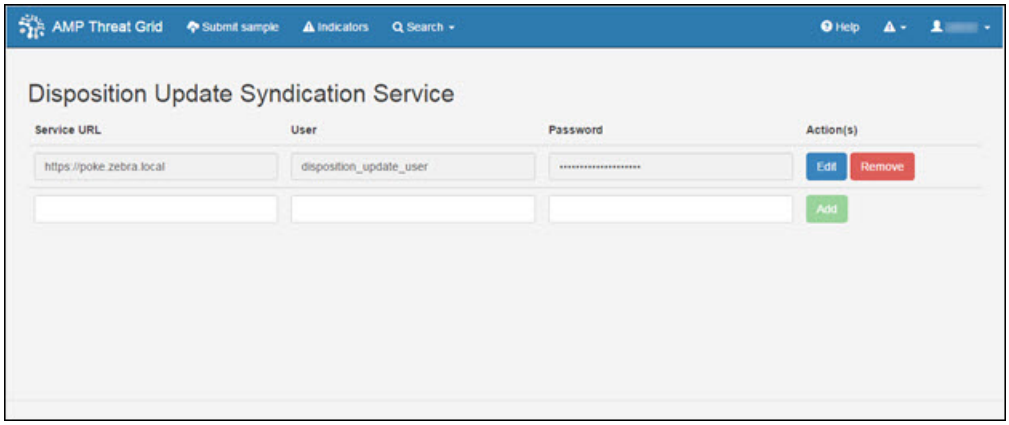
配置更新の配信サービスの管理

Threat Grid portal ユーザインターフェイスで、AMP for Endpoints プライベート クラウド アプライアンスの統合に向けて、配置更新の配信サービスを管理できます。URL は、[**Disposition Update Syndication Service**] ページで追加、編集、削除できます。

（注） AMP for Endpoints プライベート クラウド アプライアンスの統合に関する詳細については、「AMP for Endpoints プライベートクラウドを Threat Grid アプライアンスに接続する」を参照してください。

ステップ 1 Threat Grid ポータルで、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をクリックし、[**Manage FireAMP Integration**] を選択して、[**Disposition Update Syndication Service**] ページを開きます。

図 *15* : 配置更新の配信サービス



ステップ 2 次の情報を入力します。

- [**Service URL**]：AMP For Endpoints プライベートクラウドの URL。
- [**User**]：管理者ユーザ名。
- [**Password**]：AMP for Endpoints 設定ポータルによって提供されるパスワード。

ステップ 3 [**Config**] をクリックします。

ESA/WSA の Threat Grid アプライアンスへの接続

E メールセキュリティアプライアンス（ESA）、Web セキュリティアプライアンス（WSA）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

使用して Threat Grid アプライアンスと統合し、分析用のマルウェアサンプルを送信することができます。

ESA/WSA と Threat Grid アプライアンスの統合は、Cisco Sandbox API（CSA API）によって有効にされます。この統合は、多くの場合 CSA 統合と呼ばれます。

統合先の ESA/WSA 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、まず ESA/WSA の管理者が、使用中のアプライアンスとネットワーク環境に適した SSL 証明書接続をセットアップする必要があります。

このセクションでは、Threat Grid アプライアンスと通信できるように ESA、WSA その他のシスコ製品を設定するために必要な手順について説明します。

ESA および WSA のマニュアル

ESA/WSA の製品マニュアルで、「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

（注） これらのマニュアルで、Threat Grid アプライアンスは、多くの場合「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」と呼ばれています。

- 『*Cisco Email Security Appliance User Guides*』
- 『*Cisco Web Security Appliance User Guides*』

ESA と WSA の統合プロセスの概要

このセクションでは、Threat Grid アプライアンスと E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）、その他の CSA 統合（インバウンド）間の接続を設定する手順の概要を示します。詳細については、「ESA/WSA の統合プロセスの手順」を参照してください。

SSL 証明書の設定

Threat Grid アプライアンスの SSL 証明書の SAN（サブジェクト代替名）または CN（共通名）は、ホスト名および ESA/WSA の想定と一致している必要があります。統合先の ESA/WSA との接続を成功させるには、統合先の ESA/WSA が Threat Grid アプライアンスの識別に使用するものと同じホスト名にする必要があります。

要件に応じて、Threat Grid アプライアンスで自己署名 SSL 証明書を再生成する必要があります。その際、[SAN/CN] フィールドには現在のホスト名が入力されます。この証明書を作業環境にダウンロードし、統合先の ESA/WSA にアップロードしてインストールできます。

あるいは、企業向けの SSL 証明書や市販の SSL 証明書（または手動で生成した証明書）をアップロードして、現在の Threat Grid アプライアンスの SSL 証明書と置き換えなければならない

こともあります。詳細な手順については、「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したら、次の手順として、ESA/WSA が Threat Grid アプライアンスと通信できることを確認します。

ESA/WSA は、ネットワーク経由で 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。製品マニュアルの手順に従って、Threat Grid アプライアンスと ESA/WSA が相互に通信できることを確認します（ESA/WSA の Threat Grid アプライアンスへの接続を参照）。

ESA/WSA ファイル分析設定の実行

ファイル分析セキュリティサービスを有効にし、詳細設定を実行します。

ESA/WSA の Threat Grid アプライアンスへの登録

製品マニュアルに従って設定された ESA/WSA は、自動的に Threat Grid アプライアンスに登録されます。接続先デバイスの登録時に、デバイス ID がログイン ID となる新しい Threat Grid ユーザが自動的に作成され、同じ ID に基づく名前を使用して新しい組織が作成されます。管理者は、新しいデバイスユーザアカウントをアクティブにする必要があります。

Threat Grid アプライアンスでの新しい ESA/WSA アカウントのアクティブ化

ESA/WSA または他の統合が Threat Grid アプライアンスに接続して登録されると、新しい Threat Grid ユーザアカウントが自動的に作成されます。ユーザアカウントの初期ステータスは、非アクティブになっています。Threat Grid アプライアンス管理者は、分析用のマルウェアサンプルの送信に使用する前に、デバイスユーザアカウントを手動でアクティブにする必要があります。

ESA/WSA の統合プロセスの手順

ESA/WSA 間の接続は、Threat Grid アプライアンスから見れば受信になります。この統合では CSA API を使用します。

（注） 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 製品のマニュアルを参照してください。

ステップ 1 Threat Grid アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして設定します。更新を確認し、必要に応じてインストールします。

ステップ 2 ESA/WSA を通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 3 Threat Grid アプライアンスの SSL 証明書 の SAN または CN は、現在のホスト名および ESA/WSA の想定と一致している必要があります。自己署名 SSL 証明書を展開する場合は、（Threat Grid アプリケーションのクリーンインターフェイスで）新しい SSL 証明書を生成し、必要に応じてデフォルトと置き換え、ダウンロードして ESA/WSA にインストールします（「SSL 証明書の置き換え」を参照）。

（注） Threat Grid アプライアンスのホスト名が SAN または CN になってい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。

ステップ 4 ESA/WSA 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ことを確認します。

ステップ 5 Threat Grid アプライアンスの統合に使用する ESA/WSA を設定します。詳細な手順については、ESA/WSA 製品のマニュアルを参照してください。次の手順は ESA に特有のものですが、現在最も一般的なタイプの統合です。

a) **[Security Services] > [File Reputation and Analysis]** をクリックします。
b) [Enable] をクリックします。
c) [Edit Global Settings] をクリックします。
d) [**File Analysis**] セクションでは、ファイル分析がデフォルトで有効になっています。この機能を有効にしない場合は、[**Enable File Analysis**] チェックボックスをオフにします。オフにしないと、次回のコミット後にファイル分析の機能キーがアクティブになります。分析のためにクラウドに送信するファイルタイプを選択します。
e) ESA または WSA の製品マニュアルに従い、必要に応じてファイル分析の [**Advanced Settings**] を設定します。

- [**File Analysis Server URL**]：プライベートクラウドを選択します。
- [**Server**]：オンプレミスの Cisco Threat Grid アプライアンスの URL。この値と証明書には、ホスト名（IP アドレスではない）を使用します。
- [**SSL Certificate**]：オンプレミスの Threat Grid アプライアンスで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。

ステップ 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。この ID で、アクティブ化されるユーザを識別できます。

Threat Grid アプライアンスへの ESA/WSA の登録は、ファイル分析の設定を送信すると自動的に実行されます。

ステップ 7 Threat Grid アプライアンスで新しいデバイスのユーザアカウントをアクティブ化します。

a) 管理者として Threat Grid ポータルにログインします。
b) 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、[**Manage Users**] を選択して Threat Grid [**Users**] ページを開きます。

c) 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）。
d) ユーザの現在のステータスは、非アクティブになっています。[Re-Activate User] をクリックします。
e) 確認ダイアログで、[**Re-Activate**] をクリックしてアクションを確定します。

確定後、ESA/WSA その他の統合されるアプライアンスやデバイスが、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す。

AMP for Endpoints プライベートクラウドを Threat Grid アプライアンスに接続する

Threat Grid アプライアンスは、配置更新サービス用の AMP for Endpoints プライベートクラウドとの統合をアウトバウンド接続としてサポートします。

（注） 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の統合の設定タスクを、指定された順序に従ってデバイス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。

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。

ステップ 1 Threat Grid アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして設定します。更新を確認し、必要に応じてインストールします。

ステップ 2 AMP for Endpoints プライベートクラウドを通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 3 Threat Grid アプライアンスの OpAdmin ポータルで、必要に応じてデフォルトの証明書と置き換えるため、クリーンインターフェイスで SSL 証明書の再作成し、その証明書をダウンロードして AMP For Endpoints プライベート クラウド デバイスにインストールします。

AMP for Endpoints プライベート クラウドデバイスで統合を設定するために必要な次の情報を取得します。

- **ホスト名**：**[Configuration] > [Hostname]** をクリックし、ホスト名をメモします。
- **API キー**：Threat Grid ポータルの [**User Details**] ページから **API キー**をコピーします（ログイン名の横にあるドロップダウンをクリックし、[**Manage Users**] を選択して、統合ユーザアカウントに移動します）。

  （注） この手順を実行するには管理者ユーザでなければならないというわけではありません。Threat Grid アプライアンスで、この目的のために特別にユーザを作成することも可能です。

ステップ 4 Threat Grid アプライアンスとの統合に向けて、AMP for Endpoints プライベート クラウド デバイスを設定します。

a) **[Integrations] > [Threat Grid]** をクリックして、[**Connection to Threat Grid**] セクションに移動します。

b) 次のフィールドに入力します。

- [**Hostname**]：Threat Grid アプライアンスのホスト名を入力します（前の手順で取得）。
- [**API Key**]：統合に使用するアカウントの Threat Grid API キーを入力します（前の手順で取得）。
- [**SSL Certificate**]：Threat Grid アプライアンスの SSL 証明書ファイルを選択します。

c) [Save Configuration] をクリックします。

d) [Test Connection] をクリックします。

接続テストに成功したら、AMP for Endpoints プライベートクラウドで**再設定**を実行して変更を適用する必要があります。適用後、AMP が Threat Grid アプライアンスと通信できるようになり、Threat Grid にサンプルを送信することが可能になります。

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 Threat Grid アプライアンス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。

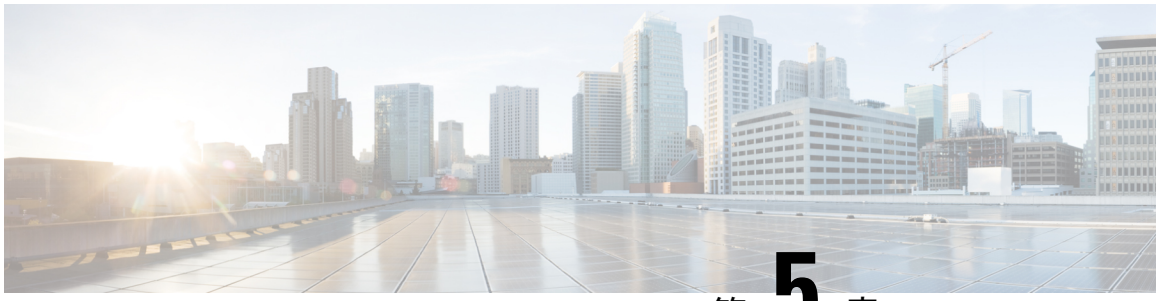
ステップ 5 OpAdmin ポータルで、配置更新の配信サービスをセットアップします。

a) 必要に応じて、DNS を設定します。「DNS の設定」を参照してください。

b) 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するかコピーして貼り付けます。「CA 証明書の管理」を参照してください。

c) 右上のメニューから、[**Manage FireAMP Integration**] を選択し、AMP 配置更新サービスの URL とログイン情報を指定します（「配置更新の配信サービスの管理」を参照してください）。

d) [**Config**] をクリックします。



第 5 章

組織とユーザの管理

この章では、Threat Grid で組織とユーザを管理する方法について説明します。説明する項目は次のとおりです。

はじめに

Threat Grid は、デフォルトの組織と管理者ユーザを使用して Threat Grid アプライアンスにインストールされます。セットアップとネットワーク設定が完了したら、ユーザがログインして分析用のマルウェアサンプルの送信を開始できるように、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。

新しい組織の作成

ユーザは常に特定の組織と関係しています。ユーザを追加する前に、まず組織を作成して、その組織にユーザを追加できるようにする必要があります。

重要 一度作成された組織を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。

ステップ 1 管理者として Threat Grid Portal にログインします。

ステップ 2 [**Administration**] メニューをクリックし、[**Manage Organization**] を選択します。[Organizations] ページが開き、アプライアンスで設定されているすべての組織が表示されます。

ステップ 3 ページの右上隅にある [**New organization**] をクリックして、[New Organization] ダイアログを開きます。

ステップ 4 以下の項目に入力します。

- [**Name**]：組織の名前を入力します（現在、名前にサイズ制限はありません）。
- [**Industry**]：[**Industry**] ドロップダウンリスト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。
- [**ATS ID**]：高度な脅威サービス ID を入力します。

ステップ 5 [**送信 (Submit)**] 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。

ステップ 6 新しく作成した組織を編集し、次の情報を入力します。

- [**Options**]：必要に応じて入力します。
- [**Rate Limit**]：デフォルトのユーザ送信レート制限を設定します。

  API レート制限は、ライセンス契約の条件に基づいて Threat Grid アプライアンス全体に適用されます。この制限は、API送信のみに適用され、手動でのサンプル送信には適用されません。ライセンスのレート制限は、組織に適用されます。

  また、オンラインヘルプの「Using Threat Grid」で説明されているように、個々のユーザにサンプル送信レートを設定することもできます（ナビゲーションバーで **[Help] > [Using Threat Grid Online Help]** をクリックします）。

  レート制限は、暦日ではなく、24 時間単位の時間枠に基づきます。送信レートの上限に達すると、次の API 送信で、429 エラーと、再試行までの待機時間を示すメッセージが返されます。

組織が作成されると、管理者または組織の管理者がその組織を管理できます（オンラインヘルプの「Managing Organizations」を参照してください）。

ユーザの管理

ユーザの追加方法など、ユーザアカウントの作成と管理に関する手順とマニュアルについては、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で、**[Help] > [Using Threat Grid Online help] > [Managing Threat Grid Users]** をクリックします。

（注） ユーザは、API のみで削除でき、サンプルを送信していない場合にのみ削除できます。

E メール セキュリティ アプライアンス、Web セキュリティアプライアンスなど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、「新しいデバイスユーザアカウントの有効化」を参照してください。

新しいデバイスユーザアカウントの有効化

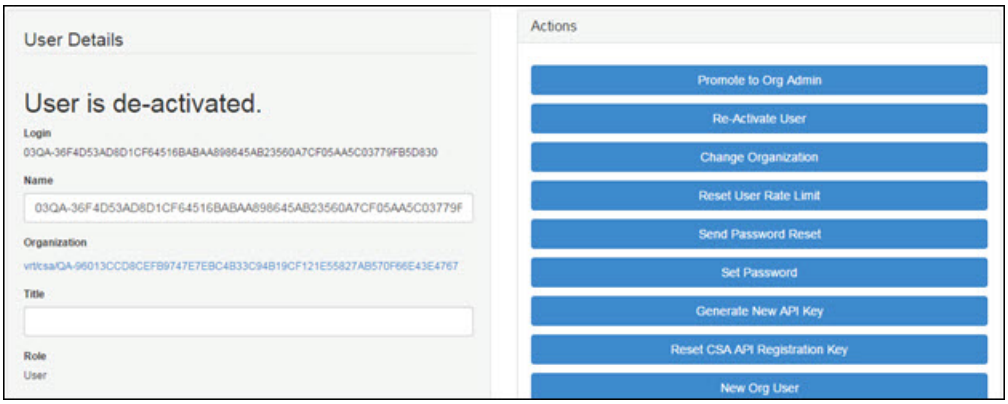
Cisco E メール セキュリティ アプライアンス、Web セキュリティアプライアンス、または他の Cisco Sandbox API 統合が Threat Grid アプライアンスに接続して登録されると、新しい Threat Grid ユーザアカウントが自動的に作成されます。ユーザアカウントの初期ステータスは、非アクティブになっています。デバイスユーザアカウントは、分析用のマルウェアサンプルの送信に使用する前に、Threat Grid アプライアンス管理者が手動でアクティブにする必要があります。

ステップ 1 管理者として Threat Grid ポータルにログインします。

ステップ 2 [**Administration**] メニューをクリックし、[**Manage Users**] を選択します。

ステップ 3 デバイスのユーザアカウントを見つけて、[**User Details**] ページを開きます。ユーザの現在のステータスは、非アクティブになっています。

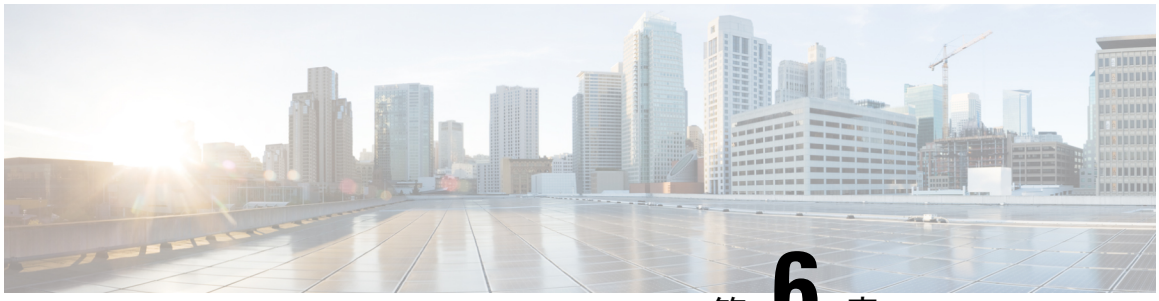
図 *16* : ユーザの詳細



ステップ 4 [Re-Activate User] をクリックします。

ステップ 5 確認ダイアログで、[**Re-Activate User**] をクリックしてアクションを確定します。

確定後、統合するアプライアンスまたはデバイスが Threat Grid アプライアンスと通信できるようになります。



第 6 章

プライバシーとサンプルの可視性

この章では、Threat Grid へのサンプル送信に関するプライバシーとサンプルの可視性モデルについて説明します。説明する項目は次のとおりです。

プライバシーとサンプルの可視性の概要

分析のため Threat Grid アプライアンスにサンプルを送信する際、コンテンツのプライバシーが重要な考慮事項となります。機密文書やアーカイブタイプの資料が分析用に送信される場合、プライバシーは特に重要な考慮事項になります。機密情報を見つけることは、特に検索 API を使用して Threat Grid アプライアンスにアクセスできるユーザにとって、比較的簡単である可能性があるためです。

Threat Grid へのサンプル送信に関するプライバシーとサンプルの可視性モデルは次のとおりです。

- サンプルは、プライベートに指定されていない限り、送信者の組織外のユーザに表示されます。
- プライベートサンプルは、サンプルを送信したユーザと同じ組織内の Threat Grid ユーザのみが閲覧できます。

統合のプライバシーと可視性

プライバシーとサンプルの可視性モデルは、統合によって送信されるサンプルに関連した Threat Grid アプライアンスで変更されます。統合とは、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）および他のデバイスなどのシスコ製品や、サードパーティのサービスのことです（CSA 統合という用語は、Cisco Sandbox API 経由で Threat Grid アプライアンスに統合（または登録）されている、ESA/WSA その他のシスコ製アプライアンス、デバイス、サービスを意味します）。

Threat Grid アプライアンスでのすべてのサンプル送信は、デフォルトでパブリックに設定されるため、所属する組織にかかわりなく、統合を含む他のすべての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、サンプルの送信者と同じ組織に属する他の Threat Grid アプライアンスユーザと統合のユーザのみに表示されます。

次の表で、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について説明します。

図 *17 : Threat Grid* アプライアンスでのプライバシーと可視性

Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✔	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

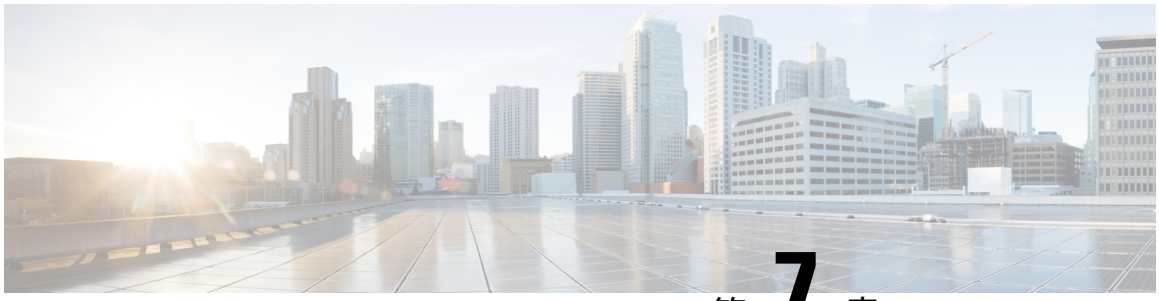
- **フルアクセス**：緑色のチェックマークは、ユーザがサンプルと分析結果にフルアクセスできることを示します。
- **スクラビングレポート**：灰色のチェックマークは、プライベート送信の結果がスクラビングされたことを示します。ユーザはサンプルと分析結果への部分的なアクセス権を持っていますが、サンプルに関する潜在的な機密情報はすべて削除されます。Glovebox には、ファイル名、プロセス名、スクリーンショット、またはアクティビティについての詳細情報は表示されません。

  サンプルの送信者のログイン情報などの詳細情報を [Metadata] セクションから除外します。ビジネスの過程でプライベートサンプルからハッシュが発生した場合、既知の脅威に対する警告が表示されます。さらに詳細な情報が必要な場合は、完全な分析のためにサンプルの独自のコピーを送信します。

  プライベートサンプルはダウンロードされない場合があります。スクラビングレポートには、アーティファクト（ファイル名が削除されたもの）、動作インジケータ、ドメイン、IP が含まれます。

- **アクセスなし**：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できないことを示します。

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は、同じ基本的なプライバシールールが適用されます。



第 7 章

アプライアンスのワイプ

この章では、ワイプアプライアンスの起動オプションを使用する方法について説明します。説明する項目は次のとおりです。

アプライアンスのワイプオプションの概要

アプライアンスのワイプブートオプションを使用すると、Threat Grid アプライアンスのディスクをワイプして、廃棄前にすべてのデータを削除したり、Cisco Demo Loan Program に戻したりすることができます。

重要 アプライアンスのワイプ手順を実行すると、Threat Grid アプライアンスは、シスコに返却してイメージを再作成しない限り稼働しなくなります。

アプライアンスのワイプ手順

アプライアンスをワイプするには、次の手順を実行します。

ステップ 1 アプライアンスを再起動し、ブートアップウィンドウが 4 秒間表示されている間に [**Wipe Appliance**] を選択します。

図 *18* : アプライアンスのワイプオプション

ステップ 2 次の情報を入力します。

- [**Username**]：「wipe」
- [**Password**]：「I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION」

ステップ 3 ワイプオプションを選択します。

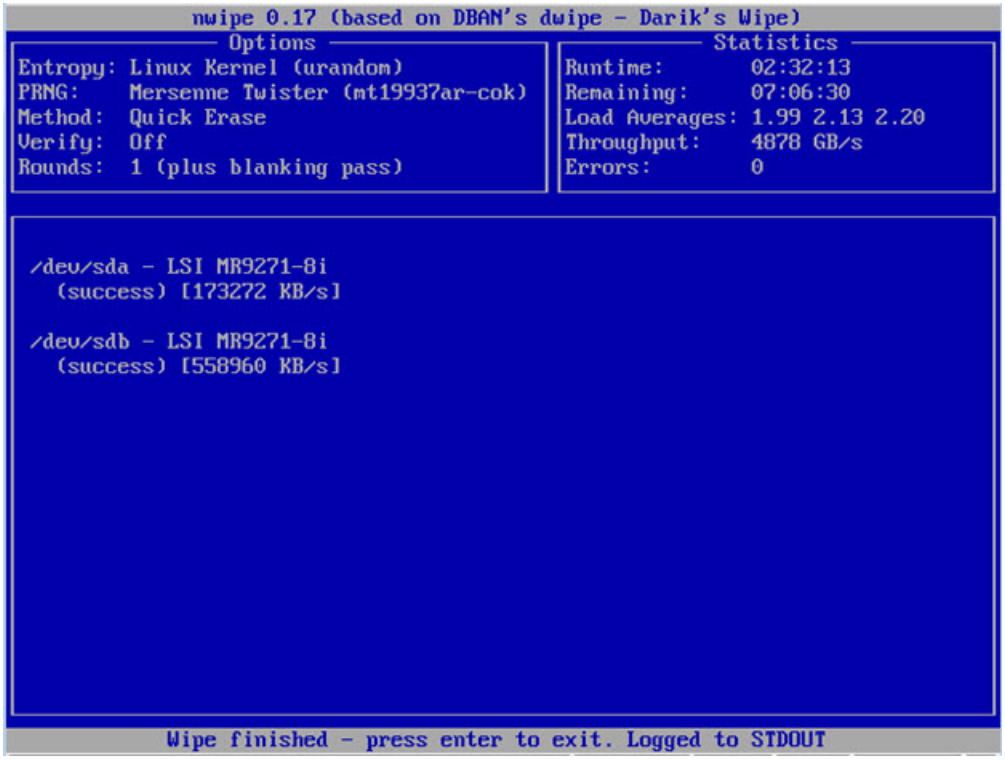
図 *19* : ワイプオプション

- [**Wipe (Fast: Zero Disks)**]：実行に約 2.5 時間かかります。

- [**Wipe (3-pass DOD method)**]：実行に約 16 時間かかります。
- [**Wipe (Random Overwrite)**]：実行に約 12 時間かかります。

ワイプ操作が完了すると、[**Wipe Finished**] ウィンドウが表示されます。

図 *20 : [Wipe Finished]*

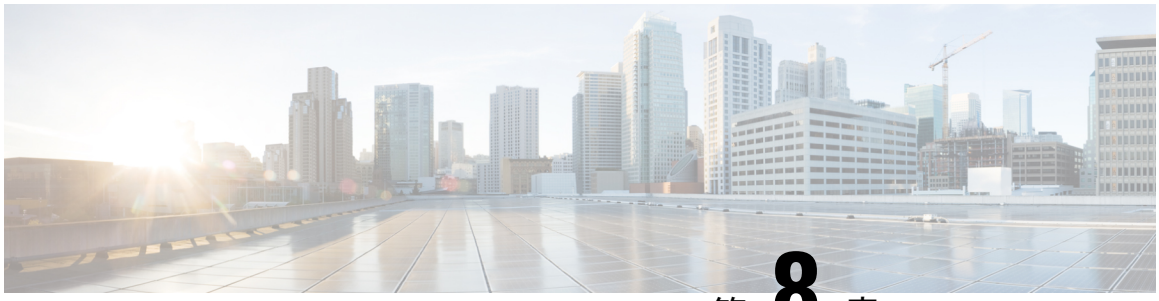


ステップ 4 Enter を押して終了します。

ワイプとクラスタ

ワイプ操作を実行すると、Threat Grid アプライアンスは、シスコに返却してイメージを再作成しない限り稼働しなくなります。クラスタノードのワイプは、完全に削除されるというフラグが OpAdmin でそのノードに付けられた後にのみ実行する必要があります。クラスタからノードを削除しないでください。削除せずに、ワイプしてから再度追加します。そうしないと、再度追加した後にそのノードがマスターになると、望ましくない結果が生じる可能性があります。

OpAdmin の [**Remove**] ボタンをクリックして、そのノードが単に非アクティブということではなく、削除されたことをシステムに通知します。



第 8 章

バックアップ

この章では、Threat Grid アプライアンスの要件、予想される成果、データ保持ポリシー、およびバックアップと復元の手順について説明します。説明する項目は次のとおりです。

Threat Grid アプライアンスのバックアップ

Threat Grid アプライアンス（v2.2.4 以降）は、NFS 対応ストレージへの暗号化されたバックアップ、NFS 対応ストレージからのデータの初期化、さらに、データベースを空の状態にリセットして前述のバックアップのロードを可能にする機能をサポートしています。

（注） リセットは、アプライアンスのワイププロセスとは異なっており、アプライアンスが情報漏えいなしで顧客構内に出荷されるようにするために使用され、バックアップ準備のためにも使用されます。その目的に適したワイププロセスは、リカバリブートローダーにすでに存在していますが、バックアップを復元するためのシステムの準備には適していません。

コンテンツは、サードパーティ製オープンソース製品である gocryptfs を使用して暗号化されます。

（注） パフォーマンス上の理由から、ファイル名の暗号化は無効になっています。Threat Grid 内のサンプルとその他のコンテンツは、どのような状況でも元の名前では保存されないため、顧客の所有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。追加の技術情報と手順については、Cisco.com で『*Threat Grid Appliance Backup Notes and FAQ*』と『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

NFS 要件

NFS バックアップストレージへの暗号化されたバックアップを実現するには、次の NFS 要件を満たす必要があります。

- Threat Grid アプライアンス管理インターフェイスからアクセス可能な TCP 経由の NFSv4 プロトコルを実行している必要があります。
- 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、10 GB 管理インターフェイス経由でアクセス可能である必要があります。
- 十分なストレージが使用可能である必要があります（「バックアップストレージ要件」を参照）。
- 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を手動で入力する必要はありません。これらと競合するパラメータを手動で入力することがサポートされないのは明白で、未定義の動作が発生する可能性があります。

- 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** または **nfsnobody** として実行されている Threat Grid アプライアンスでの唯一のプロセスは、データの暗号化に関するプロセスです。プレーンテキストデータは、最小権限の原則に基づいて、さまざまなサブツリーの個別の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 データやフリーザにアクセスできません。Elasticsearch サービスは、PostgreSQL やフリーザデータにアクセスできません。

- **nfsnobody**アカウントを使用すると、設定が簡素化され、カスタマーサイトごとに**idmap.conf**を構築する必要がなくなり、ローカルとリモートのアカウント名が一緒にマッピングされます。

ファイル システム

Threat Grid アプライアンス（v2.7 以降）では、プライマリファイルシステムとして XFS が使用されます。リセットされていない古いアプライアンスで使用されていたZFSファイルシステムは使用されません。この変更は、特に記載されている場合を除き、既存のアプライアンスには影響しません（「データリセットプロセス」を参照）。

バックアップ ストレージ要件

バックアップストアに合計で 5.6 TB を超えるストレージは必要ありません。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**：通常、使用されるストレージの大部分を占めています。バックアップストアの一括コンポーネントでのデータ保持は、使用中のThreat Gridアプライアンスリリース向けに文書化されたものと同じポリシーと制限に従っており、このコンポーネントの最大ストレージ使用量は 4.1 TB です。『Threat Grid Appliance Data Retention Notes』を参照してください。
- **PostgreSQL データベースストア**：PostgreSQL ストアの 2 つの完全バックアップと、保持されている完全バックアップのうち一番古いものから再生するのに十分な一連の WAL ログが含まれます。合計 500 GB 未満にする必要があります。
- **Elasticsearch スナップショットストア**：合計 1 TB 未満にする必要があります。

バックアップで予想される成果

次のバックアップで予想される成果を考慮する必要があります。

バックアップに含まれるもの

Threat Gridアプライアンスのバックアッププロセスの初回リリースには、お客様所有の次のバルクデータが含まれます。

- Samples
- 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

バックアップに含まれないもの

次のものは、Threat Grid アプライアンスのバックアッププロセスの初回リリースに含まれません。

- [System logs]
- 以前にダウンロードおよびインストールした更新
- SSL キーと CA 証明書を含む、アプライアンス OpAdmin インターフェイスでの設定

その他の予想される成果

バックアッププロセスに関するその他の考慮事項は次のとおりです。

- PostgreSQL ベースバックアップは 24 時間サイクルで実行されます。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。
- Elasticsearch バックアップは 5 分ごとに段階的に行われます。
- 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を処理するために、24 時間ごとに後続のジョブを使用して継続的に実行されます。
- 新しいキーを生成すると、新しい独立したバックアップストアが作成されます。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

バックアップの際、次のようにデータが保持されます。

- **PostgreSQL**：最後の 2 つの正常なバックアップと、それらのバックアップ以降のすべての WAL セグメントが保持されます。
- **Elasticsearch**：最新の 5 分ごとのスナップショット 2 回分が保持されます。
- **バルクストレージ**：単一の Threat Grid アプライアンス向けに使用され文書化されるものと同じ保持ポリシーが、共有ストアに対して使用されます。

長期間にわたって履歴データを保持する場合は、ファイルシステムレイヤまたはブロックレイヤのスナップショットをサポートする NFS サーバを使用することを強くお勧めします。

データベースのベースバックアップは、新しいベースバックアップが正常に作成されるまで保持されます。

（注） バルクストレージでの障害発生後のリセット時に使用するため、仮想マシンイメージのバックアップコピーが RAID-1 ストレージアレイ上に作成されます。初期の Cisco Threat Grid アプライアンスモデル（UCS C220-M3 プラットフォームをベースとする）は、後のモデルよりもストレージが小さく、Threat Grid アプライアンス v2.9 のインストール後に、他のユニットが使用できる空き容量が、RAID-1 ファイルシステムのディスク容量の 25 % 未満になる可能性が高くなります。その場合、サービス通知がトリガーされます。

後のモデルのハードウェアで、v2.9 リリースのインストール後に、RAID-1 アレイの空きストレージが 25 % 未満になる場合、これは正常な状態ではないため、カスタマーサポートに問い合わせる必要があります。

保持期限の厳密な適用

TGSH（v2.6 以降）の **strict_retention** オプションを使用すると、分析済みのアーティファクトを 15 日間を超えて保存しないことにより、保持期間の制限を厳密に適用することができます。このオプションを有効にすると、最初の夜間プルーニングの際に、15 日間を超えて保存されているファイルが削除されます。

（注） 15 日の期間を設定または変更することはできません。

アーティファクトとは、サンプル自体と、サンプルから生成されたその他のものを意味します。アーティファクトには分析レポートの HTML が含まれていません。分析レポートの HTML は、別途記載されているとおり、最初から制限の対象となります。アーティファクトには、データベースエントリや検索インデックスも含まれません。

strict_retention オプションは、デフォルトでは無効（false）になっています。15 日後のアーティファクトのハードプルーニングを有効にするには、**TGSH** でこのオプションを true に設定します。

configure set strict_retention true

バックアップ プロセスの概要

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

ステップ 1 「NFS 要件」に従って、バックアップのターゲットディレクトリを作成します。

ステップ 2 『*Cisco Threat Grid Appliance Setup and Configuration Guide*』の説明に従って、OpAdmin の [**NFS**] ページ（**[Configuration] > [NFS]**）に入力します。

ステップ 3 NFS の設定が完了したら、生成された暗号キーをダウンロードします。バックアップデータを復元するには、このキーが必要です。

重要 お客様には、暗号キーをバックアップして安全に保管する責任があります。Threat Gridにはコピーが保持されません。このキーを使用せずにバックアップを完了することはできません。

ステップ 4 「バックアップ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」の説明に従って、バックアップ復元ターゲットをリセットします。

ステップ 5 バックアップコンテンツの復元 （61 ページ） の説明に従って、バックアップデータを復元します。

バックアップ頻度

データのバックアップ頻度は次のとおりです。

- サンプル、アーティファクト、レポートのバルクストレージの場合、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、ベースバックアップが 24 時間サイクルで作成され、その後は、新たに書き込まれたデータベースコンテンツが 16 MB のしきい値に達するごとに、または 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。

バックアップの頻度を制御または調整することはできません。頻度を変更すると、ストレージ使用率、復元の処理時間、パフォーマンスのオーバーヘッドに関する想定が無効になるためです。

バックアップ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

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。

⚠

注意 このプロセスを実行すると、お客様が所有するデータが破棄されます。タスクを実行する前にすべてのマニュアルを読み、慎重に作業を続行してください。.

（注） リセットは、リカバリモードで使用できるセキュアワイプと同じものではありません。DLP再イメージ化センターに発送する前に、お客様が所有するデータをマシンから完全に削除するのに適しているのは、リカバリモードでのセキュアワイプのみです。ただし、リカバリモードでのセキュアワイプは、リセットに代わるものではありません。セキュアワイプでは、再イメージ化されるまで使用できなくなるアプライアンスが処理され、リセットでは、アプライアンスがバックアップを復元する準備が行われます。

データリセットプロセス

データリセットプロセスが Threat Grid アプライアンス v2.7 以降で更新され、さらに包括的になりました。すべての顧客関連データの確実な破壊を保証するため、（リカバリ ブートローダー メニューの）ワイププロセスは依然として必要ですが、リセットプロセスにより、オペレーティングシステムのログや、そのまま残されていた他の状態がクリアされるようになりました。

Threat Grid アプライアンスが正常にリセットされると、新しいランダム生成のパスワードがコンソールに表示されるようになりました（新規インストール時の動作と同じです）。この改善されたプロセスでは、複数回再起動するようになっています。また、リカバリモードからの起動が可能になりました（以前のプロセスでは、通常の操作で起動した場合にのみ正常に起動することが可能でした）。

Threat Grid アプライアンスのデータがリセットされると、データストアは、ZFS ファイルシステムから XFS ファイルシステムに変更されます。これにより、前方互換性が向上し、サービス単位の I/O 使用率のモニタリングに OS レベルのサポートが提供されるようになります。

また、更新されたデータリセットプロセスでは、システム SDD への新規インストールに必要なすべてのコンテンツを格納するのに十分なストレージが必要です。既存のデータは、このコンテンツの存在と有効性が確認された後にのみ削除されます。長期間にわたって使用されているシステム（特に第 1 世代のハードウェア）の場合、すぐに使用できる十分な空き容量がない可能性があります。その場合は、必要に応じてカスタマーサポートの支援を受けることができます。

ターゲットアプライアンスを事前設定された状態に戻す

メーカーから届いたばかりのシステムで復元するわけではない場合、既存のデータと NFS 関連の設定をシステムから消去することによって、復元のターゲットアプライアンスを事前設定された状態に戻す必要があります。

ステップ 1 Threat Grid アプライアンス TTY または SSH を使用して TGSH ダイアログにアクセスします。

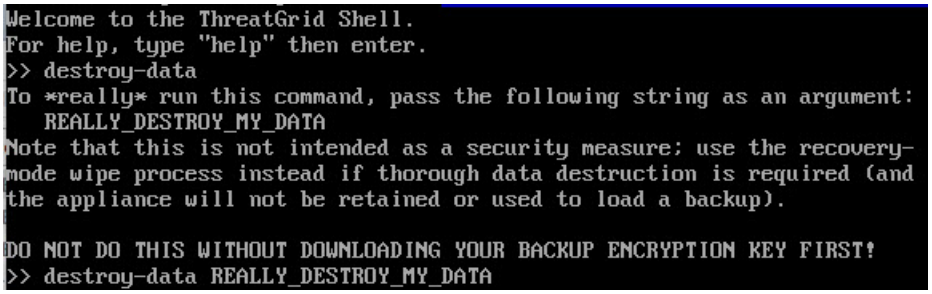
ステップ 2 [**CONSOLE**] オプションを選択して「**tgsh**」と入力します。

（注） リカバリモードによる「**tgsh**」の入力は、この使用例には適していません。

ステップ 3 **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 このコマンドを実行すると、元に戻すことはできません。すべてのデータが破棄されます。

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。

- Samples
- 分析結果、アーティファクト、フラグ付き
- アプリケーションレイヤ（OpAdmin ではない）の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 の設定とログイン情報
- NFS に使用される暗号キーのローカルコピー

復元中のバックアップにアクティブに書き込んでいるアプライアンス

別のシステムまたはThreat Gridアプライアンスが、復元中のバックアップにアクティブに書き込みを行っている場合（実稼働でアクティブに使用されている第2マスターThreat Gridアプライアンスが書き込んでいるコンテンツのテスト復元など）、そのThreat Gridアプライアンスを事前設定された状態に戻します。

ステップ 1 データストアの一貫した書き込み可能なコピーを生成します。

ステップ 2 テスト復元を実行している Threat Grid アプライアンスを、継続的に書き込まれているストアではなく、書き込み可能なコピーにポイントします。

Threat Grid アプライアンスが事前設定された状態の場合は、「バックアップコンテンツの復元」で説明されているとおり、バックアップストアのターゲットとして機能します。

バックアップコンテンツの復元

重要 復元プロセスの間、システムをサンプル送信に使用することはできません。

バックアップコンテンツを復元するには、次の手順を実行します。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [NFS]** をクリックして [**NFS**] ページを開きます。

ステップ 2 [**Upload**] をクリックして、バックアップが作成されたサーバの設定時に生成されたバックアップキーを取得します。

このキーがバックアップの作成に使用されたキーと正確に一致する場合、OpAdmin ポータルに表示される **キー ID** は、設定されたパス内のディレクトリ名と一致している必要があります。インストールウィザードによってバックアップキーと一致するディレクトリが検索され、そのディレクトリが検出されると、検出された場所へのデータの復元が開始されます。

（注） 経過表示バーは表示されません。データの復元に必要な時間は、バックアップのサイズや他の要因によって異なります。テストによると、1.2 GB の復元は迅速ですが、1.2 TB の復元には 16 時間以上かかります。大規模な復元の場合、インストールがハングしているように見えることがありますが、しばらくお待ちください。OpAdmin に復元が成功したと表示され、アプライアンスが起動します。

ステップ 3 復元されたデータが元のデータと同じであることを確認します。

バックアップおよび復元に関する注意事項

- 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 ストアと暗号キーを、最初のプロセスと同じプロセスで設定します。
- 以前の NFS ストアと暗号キーを使用して Threat Grid アプライアンスを設定すると、復元がトリガーされます。
- プライマリ Threat Grid アプライアンスの動作中に別の 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、（アップロードされた暗号化キーを使用して）新しい Threat Grid アプライアンスをポイントします。

重要　特定の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できるのは、1台のサーバのみです。

バックアップに関連するサービスの通知

バックアッププロセス中に、次のサービス通知が表示される場合があります。

- 「**Network storage not mounted（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 で設定を再適用するか、アプライアンスを再起動します。
- 「**Network storage not working（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から 15 分以内に回復しない場合は、アプライアンスを再起動してください。
- 「**Backup file system access failure（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までお問い合わせください。
- **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。
- 「**Newest PostgreSQL base backup more than two days old（最新の PostgreSQL ベース バックアップは 3 日以上前です）**」：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。
- 「**Backup Creation Messages（バックアップ作成メッセージ）**」：バックアップの開始またはトリガーの際に検出されたエラーを反映しています。
- **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。この状態は、アプライアンスを再起動するか、（NFS と暗号化サービスが機能している場合）**TGSH** にログインして `restart elasticsearch.service` コマンドを実行することで改善できます。
- 「**Backup Maintenance Messages（バックアップ 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際に検出されたエラーを反映しています。
- 「**ES Backup (Maintenance) snapshot (...) status FAILED（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [FAILED] になっています）**」：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

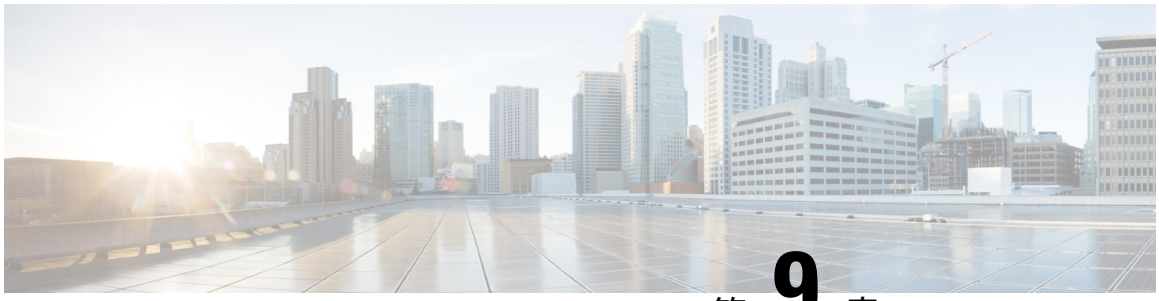
ことを示します。NFSサーバが機能していて空き領域があることを確認します。問題を特定できず、解決しない場合は、カスタマー サポートにお問い合わせください。

- 「**ES Backup (Maintenance) snapshot (...) status INCOMPATIBLE（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [INCOMPATIBLE] になっています）**」：アプライアンスのアップグレードで新しいバージョンのElasticsearchがインストールされた直後にのみ発生します。バックアップストアがアップグレードされて、新しいリリースとの互換性を持つようになるまで表示されます。この状態の間に障害が発生した場合、互換性のないバックアップからの復元には、カスタマーサービスの支援が必要になることがあります。

- 「**ES Backup (Maintenance) snapshot (...) status PARTIAL（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [PARTIAL] になっています）**」：本文に次の2つのメッセージのうちのいずれかが含まれています。「No prior successful backups seen, so retaining（以前に成功したバックアップが見つからないため、そのまま保持します）」（バックアップは存在するものの部分的でしかない場合）。または「Prior successful backups exist, so removing（以前に成功したバックアップが存在するため、削除します）」（後で再試行するために部分的なバックアップを破棄しようとしている場合）。

- 「**ES Backup (Maintenance) - Backup required (...) ms（ES バックアップ（メンテナンス）：バックアップに（...）分間かかります）**」：バックアップに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 Backup (Maintenance) - Unable to query Elasticsearch snapshot status（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でした）**」：Elasticsearch に接続できませんでした。この障害は、バックアップの作成が正常に開始された後に発生します。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。



第 9 章

クラスタ

この章では、Threat Gridアプライアンスのクラスタリングについて説明します。説明する項目は次のとおりです。

Threat Grid アプライアンスのクラスタリングについて

複数の Threat Grid アプライアンスをクラスタ化する機能は、v2.4.2 以降で使用できます。クラスタ内の各 Threat Grid アプライアンスは、共有ファイルシステムにデータを保存し、クラスタ内の他のノードと同じデータを保持します。

クラスタリングの主な目標は、複数の Threat Grid アプライアンスを 1 つのクラスタ（2 ～ 7 ノードで構成）に結合することによって、単一のシステムのキャパシティを増やすことです。さらにクラスタリングは、クラスタのサイズに応じて、クラスタ内の 1 つ以上のマシンが障害から回復するのをサポートする点でも役立ちます。

クラスタのインストールまたは再設定について不明な点がありましたら、データの破壊を避けるため、シスコサポートまでお問い合わせください。

クラスタリングの機能

Threat Grid アプライアンスのクラスタリングには、次の機能があります。

- **共有データ**：クラスタ内のすべてのThreat Gridアプライアンスは、スタンドアロンであるかのように使用できます。それぞれが同じデータにアクセスして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、いずれかのクラスタメンバーで処理され、他のメンバーは分析結果を確認できます。
- **レート制限**：各メンバーの送信レート制限を積算した値がクラスタの制限になります。
- **クラスタサイズ**：推奨されるクラスタのサイズは、3、5、または7 メンバーです。2、4、6 ノードのクラスタはサポートされますが、ノードが 1 つ多いものの機能が低下したクラスタ（1 つ以上のノードが動作していないクラスタ）と同様の可用性になります。
- **タイブレーカー**：クラスタに偶数のノードを含めるように設定すると、タイブレーカーとして指定されたノードは、どのノードがプライマリデータベースを持つかを決定するイベントで二番手に位置付けられます。

  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、他のノードがその役割を引き継ぐ必要があります。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、（タイブレーカーではない）ノードがクラスタからドロップされた場合にのみ、タイブレーカーロールが関係することになります。その場合、クラスタは偶数クラスタになります。

（注） この機能は、2 ノードのクラスタに対してのみ十分にテストされています。

クラスタリングの制限事項

Threat Grid アプライアンスのクラスタリングには、次の制限事項があります。

- 既存のスタンドアロンThreat Gridアプライアンスのクラスタを構築する場合、最初のノード（初期ノード）のみがそのデータを保持できます。クラスタに既存のデータをマージすることは許可されないため、他のノードは手動でリセットする必要があります。

  「バックアップ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」に記載されているとおり、destroy-data コマンドを使用して既存のデータを削除します。

重要 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が稼働しなくなるため、ワイプアプライアンス機能は使用しないでください。

- 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。ご不明な点がありましたら、Threat Grid のサポートまでお問い合わせください。

クラスタリングの要件

Threat Grid アプライアンスをクラスタリングする場合、次の要件を満たす必要があります。

- **バージョン**：サポートされている設定でクラスタをセットアップするには、すべての Threat Grid アプライアンスが同じバージョンを実行している必要があります。常に使用可能な最新のバージョンにしておきます。
- **Clust インターフェイス**：各 Threat grid アプライアンスには、クラスタ内の他の Threat Grid アプライアンスへのダイレクトインターコネクトが必要です。クラスタ内の各 Threat Grid アプライアンスの Clust インターフェイススロットに SFP+ を設置する必要があります（スタンドアロン構成の場合には該当しません）。

  ダイレクトインターコネクトとは、すべての Threat Grid アプライアンスが同じレイヤ 2 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のルーティングが不要で、大幅な遅延や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。
- **エアギャップ展開の場合は非推奨**：デバッグの複雑さが増大するため、エアギャップ展開や、顧客がデバッグへの L3 サポートアクセスを提供できない、または提供を望まないシナリオでは、アプライアンスのクラスタリングは推奨されません。
- **データ**：Threat Grid アプライアンスは、データが含まれていない場合にのみクラスタに結合できます（初期ノードのみがデータを保持できます）。既存の Threat Grid アプライアンスをデータのない状態に移行するには、データベース リセット プロセスを使用する必要があります（v2.2.4 以降で使用可能）。

重要 破壊的なワイプアプライアンスプロセスを使用しないでください。このプロセスにより、すべてのデータが削除され、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が稼働しなくなります。

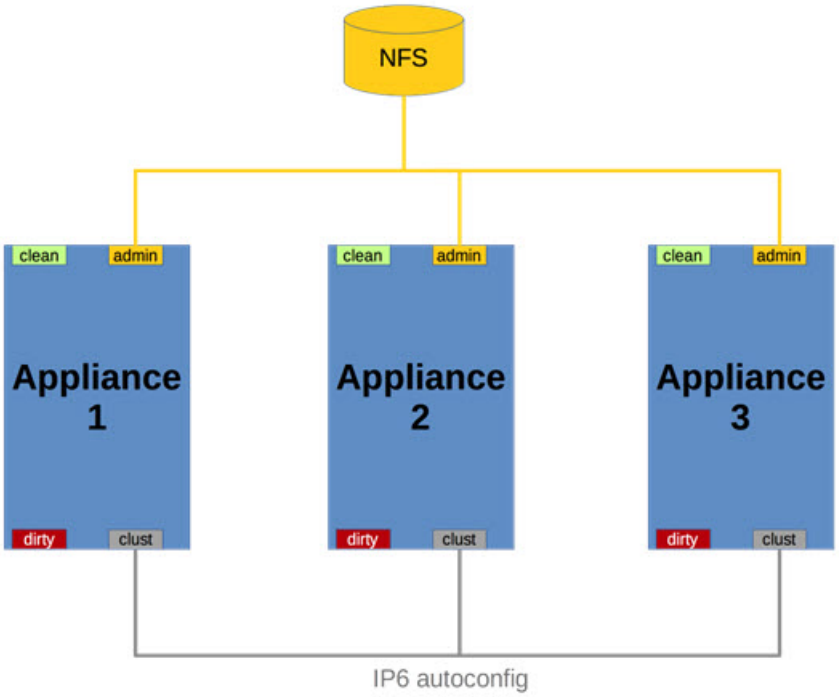
- **SSL 証明書**：1 つのクラスタノードにカスタム CA によって署名された SSL 証明書をインストールする場合、他のノードすべての証明書も同じ CA によって署名されている必要があります。

ネットワーキングと NFS ストレージ

Threat Grid アプライアンスをクラスタリングするには、ネットワーキングおよび NFS ストレージに関して次の点を考慮する必要があります。

- Threat Grid アプライアンスクラスタでは、NFS ストアを有効にして設定する必要があります。NFS ストアが管理インターフェイス経由で使用可能で、すべてのクラスタノードからアクセス可能になっている必要があります。
- 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。既存の Threat Grid アプライアンスのデータを使用して NFS ストアを初期化することはできますが、クラスタの動作中は、クラスタのメンバーではないシステムからアクセスすることはできません。
- NFS ストアはシングルポイント障害であり、そのロールに見合った、冗長性があり信頼性の高い機器を使用することが不可欠です。

図 *22*：クラスタリングネットワーク構成図



クラスタの構築の概要

サポートされてい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である必要があります。バージョンは利用可能な範囲で常に最新のもの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。

クラスタリングの前にThreat Gridアプライアンスがスタンドアロンマシンとして使用されている場合、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。

最初のノードを使用して新しいクラスタを開始し、他のThreat Gridアプライアンスをそのクラスタに結合します。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。

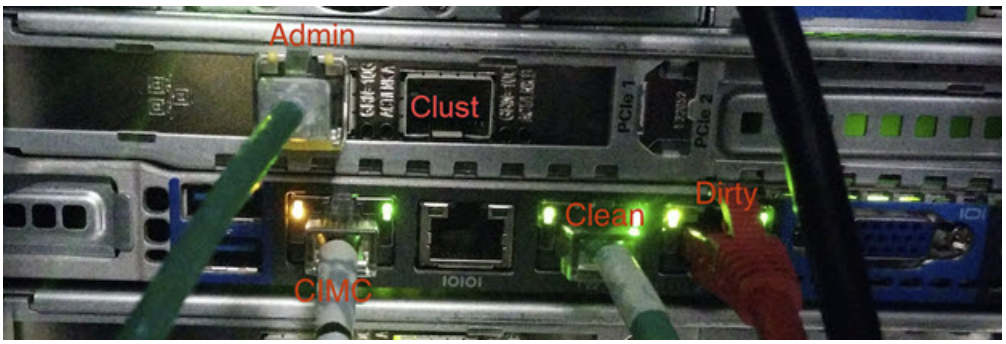
- 既存のスタンドアロンThreat Gridアプライアンスを使用して、新しいクラスタを開始します。
- 新しいThreat Gridアプライアンスを使用して、新しいクラスタを開始します。

Clustインターフェイスの設定

クラスタ内の各アプライアンスには、Clustインターフェイス用のSFP+を追加する必要があります。

4番目の（非管理）SFPポートにSFP+モジュールを取り付けます。

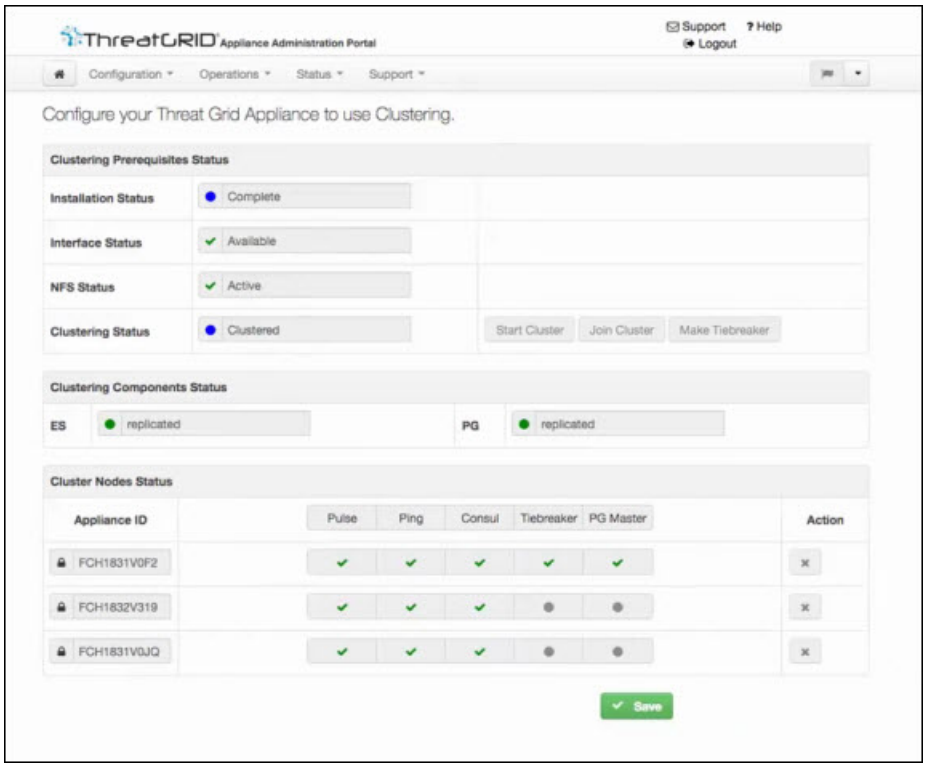
図 *23 : Cisco UCS M4 C220* の *Clust* インターフェイスの設定



クラスタリングの設定

クラスタは、[**Clustering**] ページ（**[Configuration] > [Clustering]**）の OpAdmin ポータルで設定および管理されます。このセクションでは、アクティブで正常なクラスタを理解するための [**Clustering**] ページのフィールドについて説明します（スクリーンショットには 3 つのノードを含むクラスタが示されます）。

図 *24* : アクティブクラスタのクラスタリング設定



前提条件ステータスのクラスタリング

- [**Installation Status**]：Threat Grid アプライアンスのインストールステータス。ステータスが [**Complete**] になっている（完全にセットアップおよび設定されている）必要があります。
- [**Interface Status**]：Clust ネットワーク インターフェイスのステータス。
- [**NFS Status**]：NFS のステータス。ステータスが [**Available**] になっている必要があります。
- [**Clustering Status**]：Threat Grid アプライアンスがクラスタノードとスタンドアロンのどちらになっているかを示します。
  - [**Standalone（unsaved）**]：クラスタの一部として、またはスタンドアロンの Threat Grid アプライアンスとして明確に設定されていません。クラスタリングの前提条件が満たされている場合は、初期セットアップウィザードでこの選択を行います。
  - [**Standalone**]：スタンドアロンノードとして設定されています。リセットしないとクラスタの一部として設定できません。
  - [**Clustered**]：1 つ以上の他の Threat Grid アプライアンスを含むクラスタに結合しています。

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。最新の確定的なデータ（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。

- [**Replicated**]：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。複製済みの状態は、障害発生時のダウンタイムがゼロにな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。
- [**Available**]：すべてが正常に動作しており、参照サービスを使用できます（APIおよびユーザ要求を処理できます）が、複製されません。
- [**Unavailable**]：非機能サービスとして知られています。

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

詳細については、Cisco.com の「*Threat Grid Appliance Clustering FAQ*」を参照してください。

クラスタ ノード ステータス

緑色のチェックマークは、ノードが稼働中で正常であることを示します。

赤色の X は、何かがまだ実行されていないか、正常でないことを示します。

- [**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 ストアを使用しているかどうかを示します。
- [**Ping**]：Clust インターフェイス上でクラスタノードを認識できるかどうかを示します。
- [**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。参加には、Clust で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。

- [**Tiebreaker**]：ノードをタイブレーカーに指定します。タイブレーカーは、クラスタのプライマリノードが選択される際に決定票を投じます。「タイブレーカーノードの指定」を参照してください。
- [**Keep Standalone**]：Threat Grid アプライアンスがクラスタ内の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、クラスタに結合していない Threat Grid アプライアンスの OpAdmin 設定ウィザードプロセスを完了できます。

Thread Grid アプライアンスのクラスタの開始

Threat Grid アプライアンスのクラスタを構築する場合、最初のノードが既存のスタンドアロン Threat Grid アプライアンスまたは新しいアプライアンスのいずれかであるクラスタを開始する必要があります。ご使用の環境に応じたクラスタの開始については、該当するセクションを参照してください。

既存のスタンドアロン アプライアンスを使用したクラスタの開始

既存のスタンドアロン Threat Grid アプライアンスからクラスタの構築を開始できます。この方法では、あるマシンの既存のデータを保存し、そのデータを使用して新しいクラスタを開始できます。クラスタが開始される NFS で、既存のバックアップが使用可能になっている必要があります。

（注） クラスタに結合される他のすべてのノードから、結合前にデータを削除する必要があります。追加されるノード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 よりも前のリリースで、NFS にバックアップされたデータを含むスタンドアロン Threat Grid アプライアンスの場合、新しいクラスタの初期ノードにするために、データベースのリセットとバックアップからの復元を行う必要がなくなりました。以前のバージョンの Threat Grid アプライアンスをお持ちの場合、新しいクラスタを開始する前に、v2.4.3 以降にアップグレードしてからリセット操作を実行することをお勧めします。

最初のノードを対象にクラスタを開始するには、次の手順を実行します。

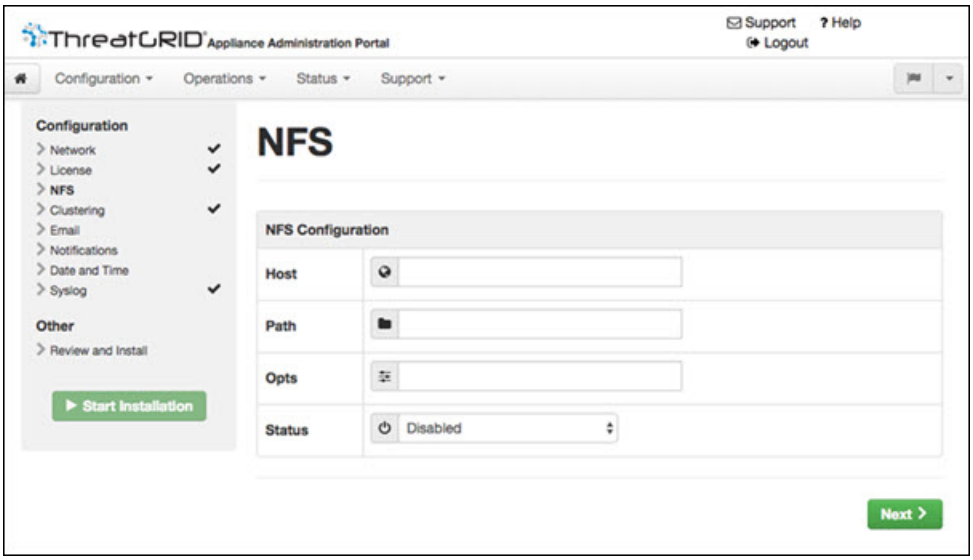
ステップ 1 Threat Grid アプライアンスを最新バージョンに完全に更新します。現在実行されているバージョンによっては、最新バージョンになるまでに複数の更新サイクルが必要になる場合があります。

ステップ 2 まだ実行していない場合は、NFS へのマシンのバックアップを設定します。

（注） この手順では、デフォルト Linux NFS サーバの実装について説明します。サーバの設定によっては手順の調整が必要になる場合があります。

a) OpAdmin ポータルで、**[Configuration] > [NFS]** をクリックして [**NFS**] ページを開きます。

図 *25 : NFS* の設定

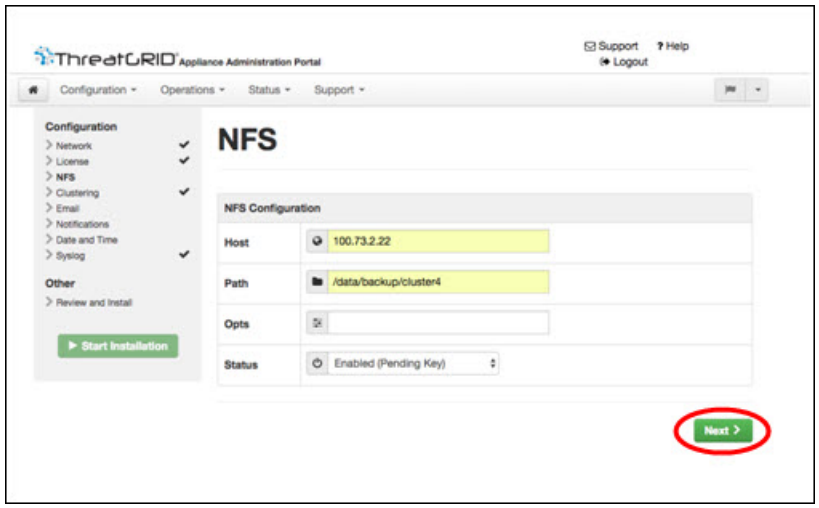


b) 次のフィールドに入力します。

- [**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。
- [**Path**]：ファイルが保存される NFS ホストサーバ上の場所への絶対パス。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。
- [**Opots**]：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。
- [**Status**]：ドロップダウンリストから [**Enabled（Pending Key）**] を選択します。

c) [Next] をクリックします。

図 *26* : 有効化された *NFS* 設定（保留中のキー）



ページが更新され、[**Generate**] ボタンが使用可能になります。

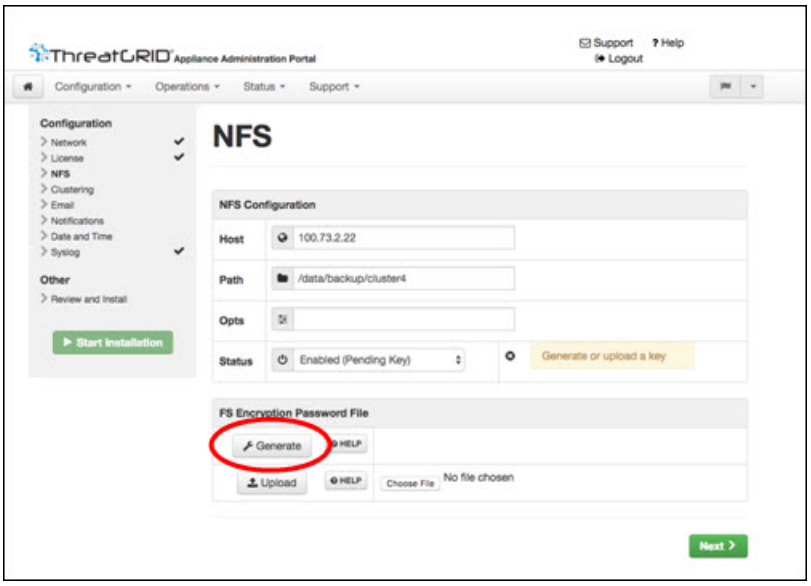
このページを初めて設定するときに、暗号キーの [**Remove**] ボタンと [**Download**] ボタンが表示されます。

[**Upload**] ボタンは、NFS が有効になっているものの、キーが作成されていない場合に使用できます。キーを作成すると、[**Upload**] ボタンが [**Download**] ボタンに変わります。キーを削除すると、[**Download**] ボタンが [**Upload**] ボタンに戻ります。

（注） キーがバックアップの作成に使用されたキーと正確に一致する場合、アップロード後にOpAdmin に表示される [**Key ID**] は、設定されたパス内の特定のディレクトリの名前と一致するはずです。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。

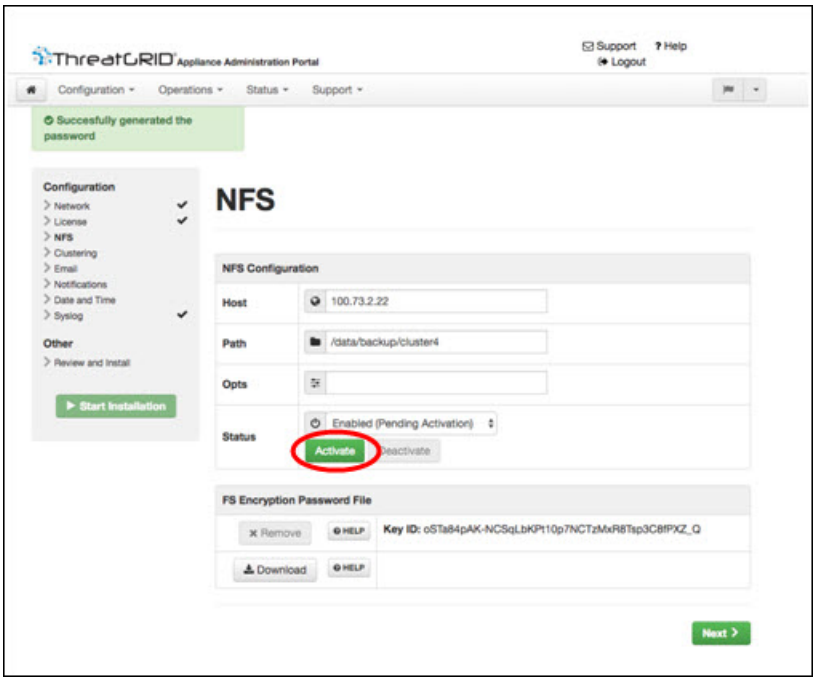
d) [Generate] をクリックして、新しい NFS 暗号キーを作成します。

図 *27* : 新しい *NFS* 暗号キーの生成



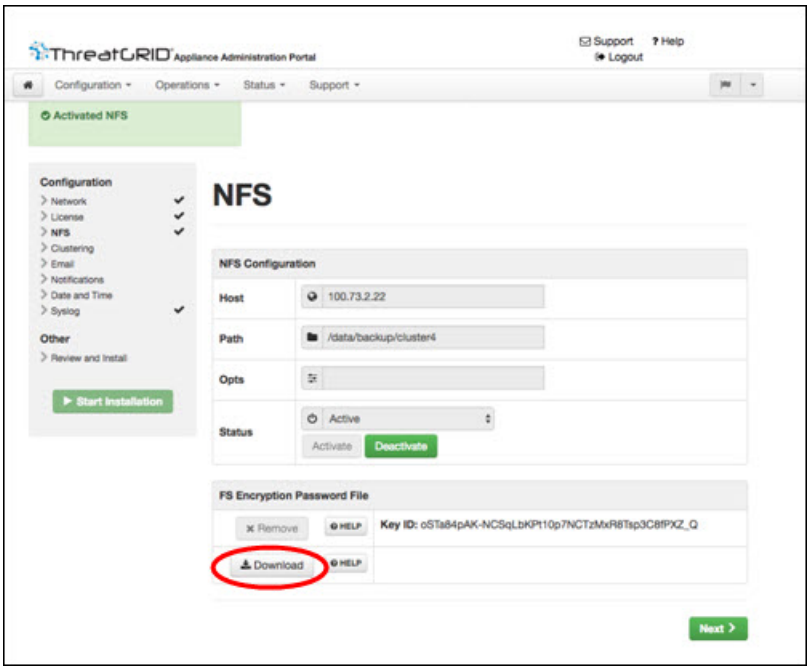
e) [Next] をクリックします。ページが更新されて [**Key ID**] が表示され、[**Activate**] ボタンと [**Download**] ボタンが使用可能になります。

図 *28* : *NFS* 設定のアクティブ化



f) [Activate] をクリックします。アクティブ化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）。[**Status**] が [**Active**] になります。

図 *29 : [Active]* になった *NFS*



g) [**Download**] をクリックして、バックアップの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 この手順を実行しないと、次の手順ですべてのデータが失われます。

ステップ 3 必要に応じて設定を完了し、Threat Grid アプライアンスを再起動して、NFS バックアップ設定を適用します。

ステップ 4 バックアップを実行します。

（注） 推奨どおりに、前もって少なくとも48時間バックアップを実行し、バックアップに問題が発生したことを示すサービス通知がなかった場合、次の手動による手順は不要です。

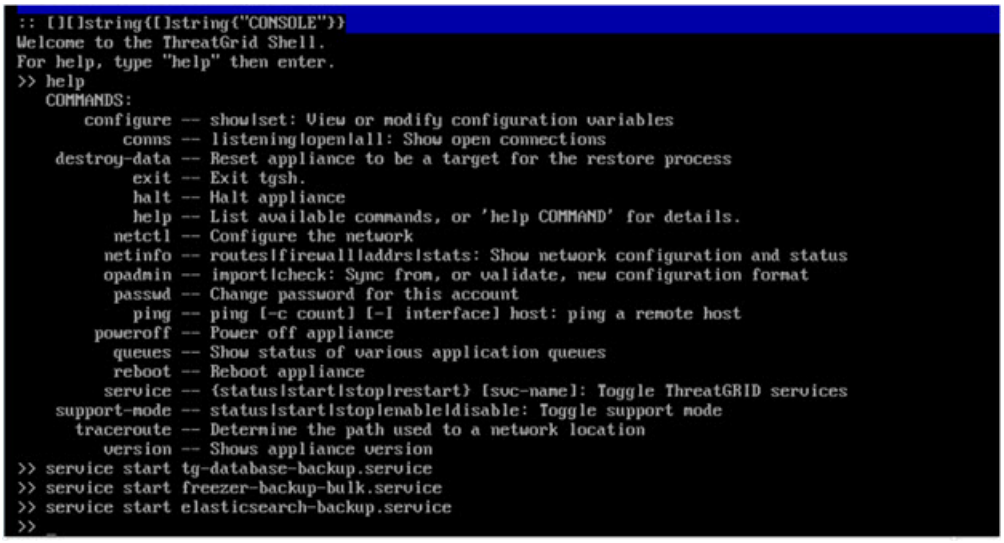
バックアップなどのサービス通知は、Threat Grid Portal UI の右上隅にあるアイコンで表示できます。「**There is no PostgreSQL backup yet（PostgreSQL バックアップがまだありません）**」というサービス通知が表示された場合は、手順を先に進めないでください。

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。

a) **TGSH** を開き、次のコマンドを入力します。

```
service start tg-database-backup.service
service start freezer-backup-bulk.service
service start elasticsearch-backup.service
```

図 *30 : NFS* に対する全データのバックアップの開始



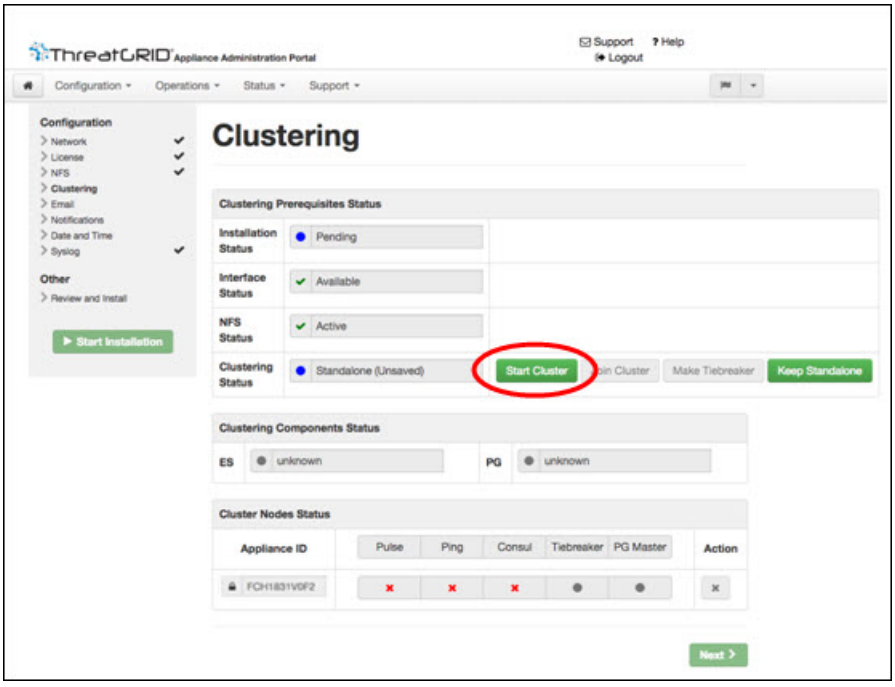
b) 最後のコマンドが返された後、約 5 分間待機します。

ステップ 5 Threat Grid Portal 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。

重要 上述のプロセスが正常に完了しない限り、手順を先に進めないでください。

ステップ 6 **[Configuration] > [Clustering]** に移動します。

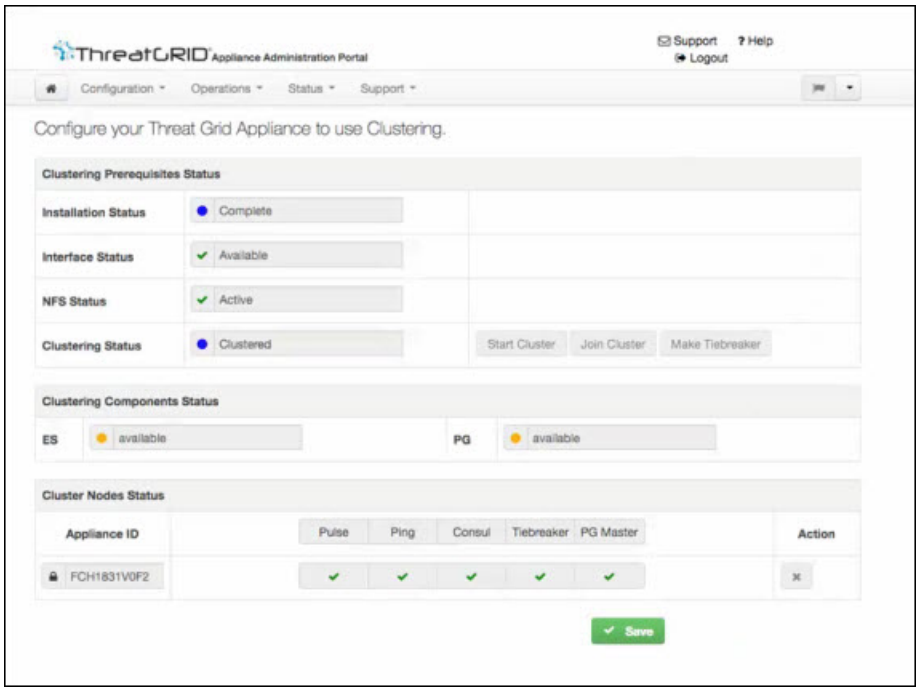
図 *31 :* クラスタの開始



ステップ 7 [**Start Cluster**] をクリックします。

ステップ 8 確認ダイアログで、[OK] をクリックします。[**Clustering Status**] が [**Clustered**] に変わります。

図 32 : [Clustering Status] : [Clustered]



データの復元が完了したら、[**Clustering**] ページに戻って、新しいクラスタの正常性を確認します。

ステップ 9 インストールを終了します。この操作により、クラスタモードでデータの復元が開始されます。

次のタスク

「Threat Grid アプライアンスのクラスタへの結合」で説明されているように、他の Threat Grid アプライアンスの新しいクラスタへ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

このクラスタ開始方法は、クラスタ対応バージョンのソフトウェアを搭載している新しい Threat Grid アプライアンスか、データをリセットした既存の Threat Grid アプライアンスに使用できます。

（注） 「バックアップ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」に記載されているとおり、`destroy-data` コマンドを使用して既存のデータを削除します。アプライアンスのワイプ機能は使用しないでください。

ステップ 1 通常どおり OpAdmin 設定を設定および開始します。

ステップ 2 OpAdmin で、**[Configuration] > [NFS]** をクリックします。

（注） 「既存のスタンドアロンアプライアンスを使用したクラスタの開始」の図を参照してください。

ステップ 3 [**Network**] と [**License**] を設定します。

ステップ 4 NFS の設定ページで、次のフィールドに入力します。

- [**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。
- [**Path**]：ファイルが保存される NFS ホストサーバ上の場所への絶対パス。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。
- [**Opots**]：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。
- [**Status**]：ドロップダウンリストから [**Enabled**（**Pending Key**）] を選択します。

ステップ 5 [Next] をクリックします。

ページが更新されます。[**Generate**] ボタンと [**Activate**] ボタンが使用できるようになります。

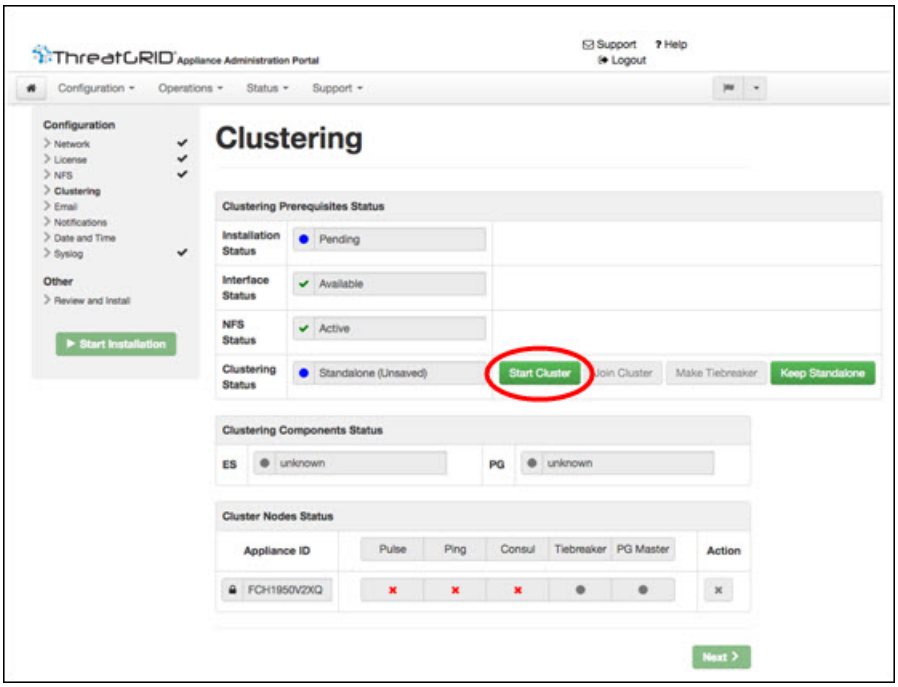
ステップ 6 [Generate] をクリックして、新しい NFS 暗号キーを作成します。

ステップ 7 [Activate] をクリックします。

ステータスが [Active] に変わります。

ステップ 8 [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* : クラスタリング設定ページ



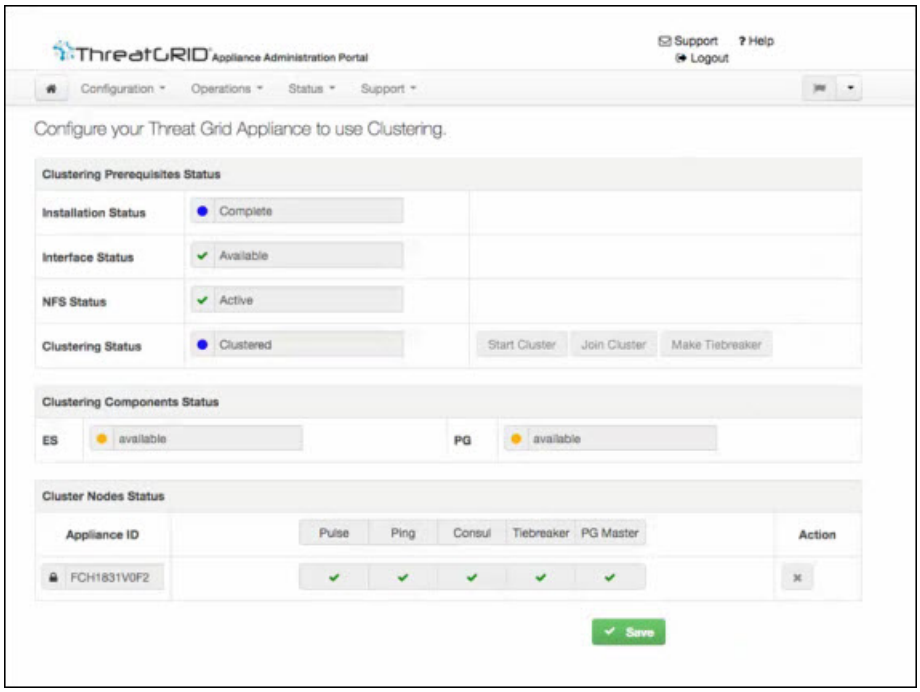
ステップ 9 [**Clustering**] ページで [**Start Cluster**] をクリックしてから、確認ダイアログで [**OK**] をクリックします。

[**Clustering Status**] が [**Clustered**] に変わります。

ステップ 10 ウィザードの残りの手順を完了し、[**Start Installation**] をクリックします。この操作により、クラスタモードでデータの復元が開始されます。

ステップ 11 [**Clustering**] ページを開き、新しいクラスタの正常性を確認します。

図 *34 : [Clustering Status]* : *[Clustered]*



次のタスク

「Threat Grid アプライアンスのクラスタへの結合」に進みます。

Threat Grid アプライアンスのクラスタへの結合

このセクションでは、新規および既存の Threat Grid 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） Threat Grid アプライアンスは、データが含まれていない場合にのみ、既存のクラスタに結合できます。データが含まれている可能性のある最初のアプライアンスの場合とは異なります。

また、クラスタに結合している Threat Grid アプライアンスに最新のソフトウェアバージョンがインストールされていることは非常に重要です（クラスタ内のすべてのノードが同じバージョンを実行している必要があります）。そのためには、Threat Grid アプライアンスの設定と更新が必要になる場合があります。その後、日付をリセットしてクラスタに結合することができます。

一度に 1 つのノードを追加するようにし、次のノードを追加する前に、Elasticsearch（ES）と PostGres（PG）が [**Replicated**] の状態になるまで待機します。[**Replicated**] のステータスは、2 つ以上のノードを含むクラスタで想定されています。

（注） ES および PG の状態が [**Replicated**] に変更されるまでの待機時間は、単一ノードの場合には当てはまりません。バックアップから単一ノードクラスタを初期化する場合は、復元が完了し、アプリケーションが UI に表示されるのを待ってから、2 番目のノードを追加する必要があります。

Threat Grid アプライアンスをクラスタに結合する場合、初期設定時に NFS とクラスタリングを設定する必要があります。

既存のアプライアンスのクラスタへの結合

既存の Threat Grid アプライアンスをクラスタに結合するには、次の手順を実行します。

ステップ 1 Threat Grid アプライアンスを最新バージョンに更新します。この手順では、インストールされている現在のバージョンに応じて、複数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を同じバージョンにする必要があります。

ステップ 2 すべてのデータを削除するには、`TGSH` で **destroy-data** コマンドを実行します。既存の Threat Grid アプライアンスをクラスタに結合する際、クラスタにマージする前に、すべてのデータを削除する必要があります。「バックアップ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。

既存の Threat Grid アプライアンスで `destroy-data` コマンドを実行した後、このアプライアンスは基本的に新しいノードになるため、クラスタに結合するには、新しい Threat Grid アプライアンスを結合する場合と同じ手順に従います。

次のタスク

「新しいアプライアンスのクラスタへの結合」に進みます。

新しいアプライアンスのクラスタへの結合

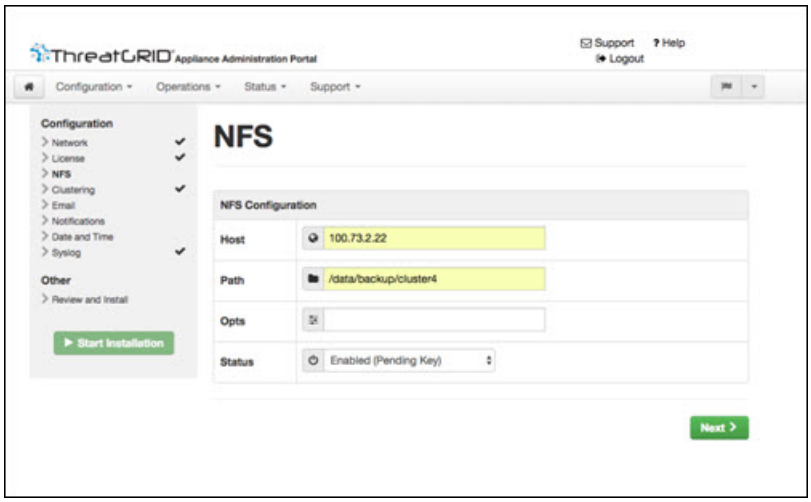
新しい Threat Grid アプライアンスをクラスタに結合するには、次の手順を実行します。

ステップ 1 通常どおり OpAdmin 設定を設定および開始します。

ステップ 2 OpAdmin で、**[Configuration] > [NFS]** をクリックし、クラスタ内の最初のノードで設定された内容と一致する**ホスト**と**パス**を指定します。

ステップ 3 [**Status**] ドロップダウンリストで [**Enabled（Pending Key）**] を選択します。

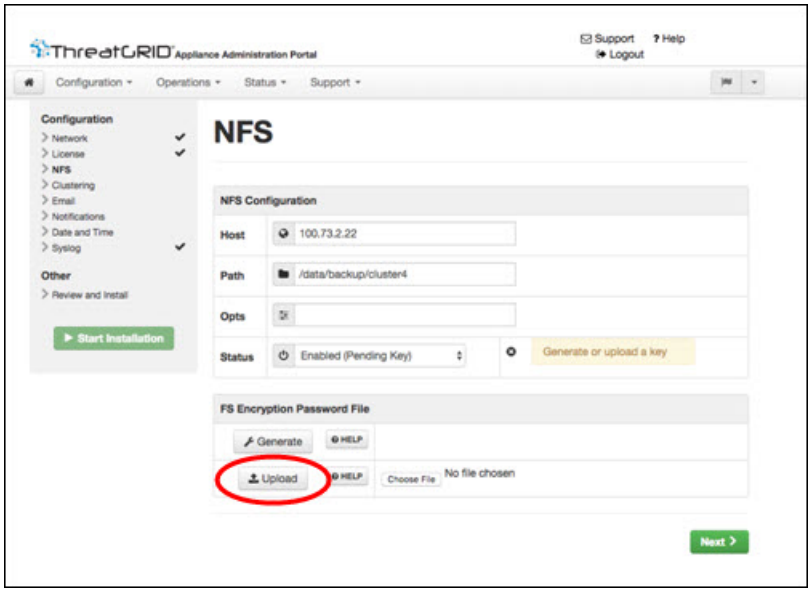
図 *35* : クラスタに結合するための *NFS*



ステップ 4 [Next] をクリックします。ページが更新され、[**Upload**] ボタンが使用可能になります。

（注） キーがバックアップの作成に使用されたキーと正確に一致する場合、アップロード後にOpAdmin に表示される [**Key ID**] は、設定されたパス内の特定のディレクトリの名前と一致するはずです。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

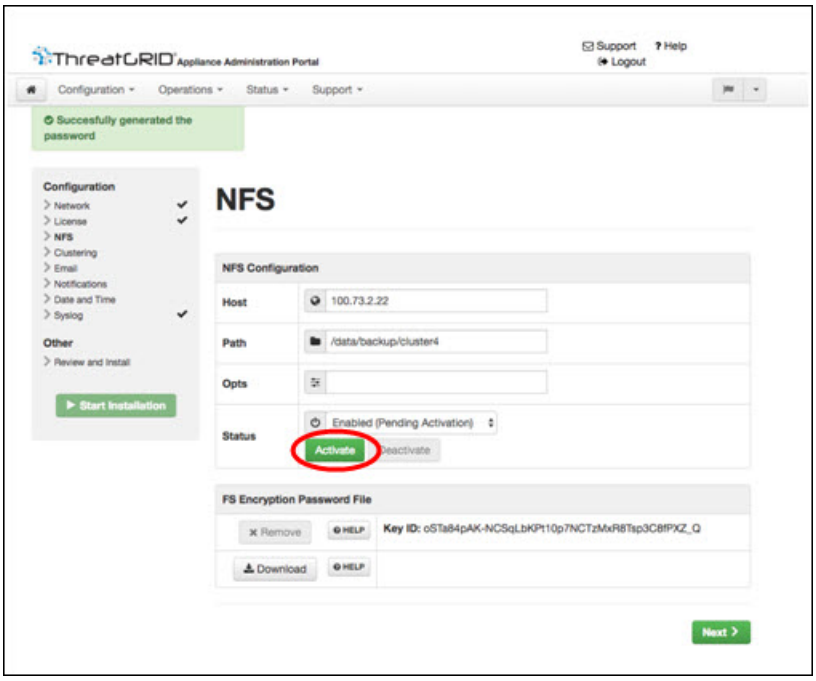


ステップ 5 [**Upload**] をクリックし、新しいクラスタを開始した際の最初のノードからダウンロードした NFS 暗号キーを選択します。

ステップ 6 [Next] をクリックします。

ページが更新されます。[**Key ID**] が表示され、[**Activate**] ボタンが有効になります。

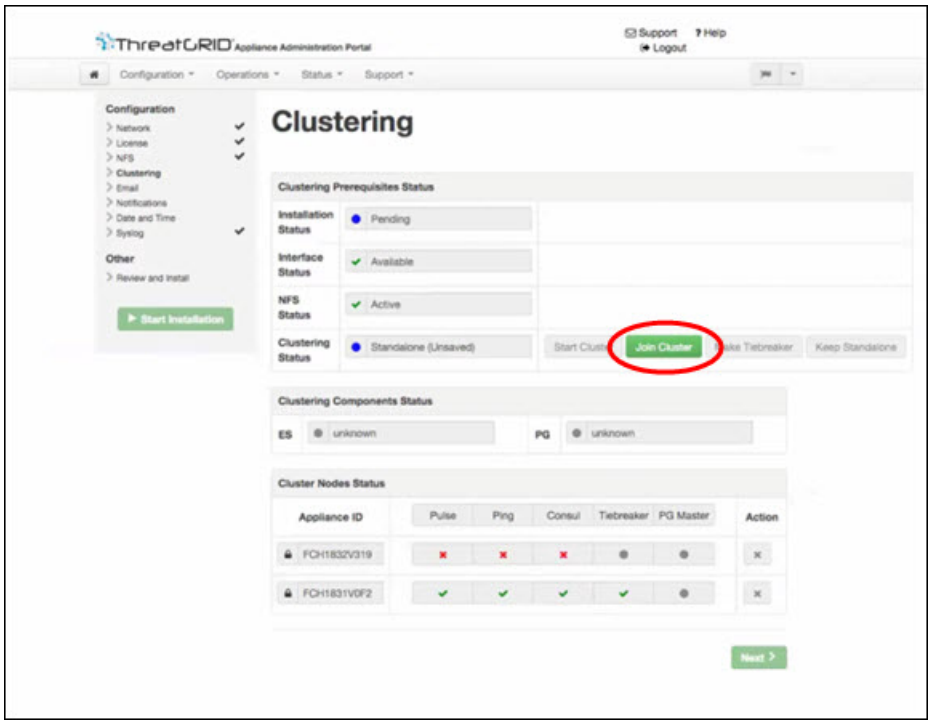
図 *37* : 結合するアプライアンスの *NFS* 暗号キーを有効にします。



ステップ 7 [Activate] をクリックします。数秒後に [**Status**] が [**Active**] に変わります（左下隅）。

ステップ 8 [**Next**] をクリックして、[**Clustering**] ページに進みます。

図 *38* : クラスタの結合

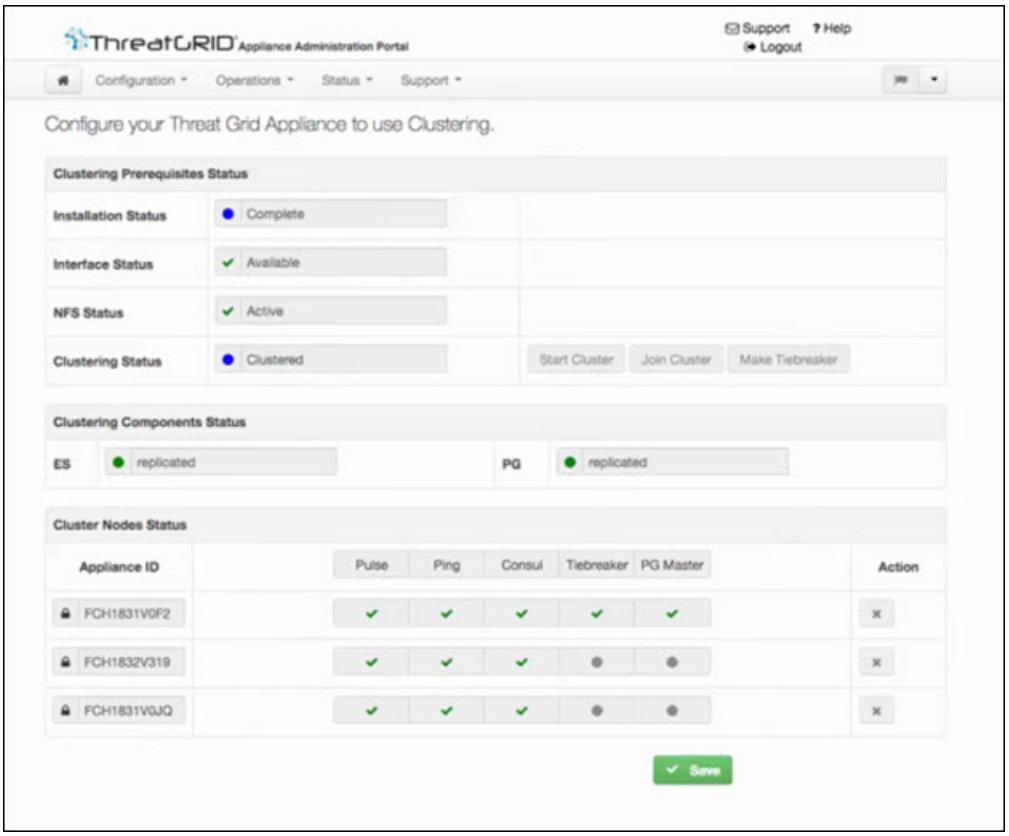


ステップ 9 [**Join Cluster**] をクリックしてから、確認ダイアログで [**OK**] をクリックします。

[**Clustering Status**] が [**Clustered**] に変わります。

ステップ 10 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。

図 *39* : アクティブかつ正常な *3* ノードクラスタ



ステップ 11 クラスタに結合するノードごとに、手順 1 ～ 手順 10 を繰り返します。

タイブレーカーノードの指定

クラスタに偶数のノードを含めるように設定すると、タイブレーカーとして指定されたノードは、どのノードがプライマリデータベースを持つかを決定するイベントで二番手に位置付けられます。

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、他のノードがその役割を引き継ぐ必要があります。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。

クラスタには 3 つ、5 つ、または 7 つのノードを含めることを推奨します。タイブレーカーのサポートは、スタンドアロン Threat Grid 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喪失を軽減するための継続的な取り組みの一環です。

クラスタが完全に正常な状態で、現在のノードがタイブレーカーではない場合、[**Clustering**] ページの [**Make Tiebreaker**] ボタンがアクティブになります。

ノードをタイブレーカーに指定するには、[**MakeTiebreaker**] をクリックします。サービスが一時的に中断されます。その後現在のノードは障害の発生が許容されないノードになり、他のノードはクラスタを解除せずにシャットダウンできます。

前もってタイブレーカーの指定を変更できない状況で、タイブレーカーノードの恒久的な障害が発生した場合は、残るノードをリセットしてバックアップから復元するか、Threat Grid のサポートに連絡して支援を求めてください。

クラスタノードの削除

クラスタからノードを削除するには、[**Clustering**] ページの [**Cluster Nodes Status**] ペインに表示される [**Action**] 列の [**Remove**] アイコン（X）をクリックします。

- クラスタからノードを削除するとは、ノードが一時的にダウンするということではなく、クラスタの一部と見なされなくなることを意味します。Threat Grid アプライアンスは、使用を停止している間に削除する必要があります。削除されたアプライアンスは、別のハードウェアに置き換えられるか、データがリセットされた後にのみクラスタに再度結合されます。
- ノードの削除は、ノードを再度追加しないユーザの意向をシステムに伝えることに相当します。再度追加しようとすると、ノードがリセットされます。
- ノードは、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（合意ストアの一部）でアクティブになっている場合、クラスタから完全に削除されたものとしてマークされません。

（7 ノード未満のクラスタ内の）ライブになっているノードを置き換えるには、新しいノードを追加し、クラスタが緑色になるのを待ってから、[**Remove**] ボタンを使用して古いノードをオフラインにします。この操作は、ノードを戻さない意向をシステムに伝えることに相当します。

ノードをオフラインにすると、クラスタのステータスは黄色に変わります。[**Remove**] をクリックすると、ステータスが緑色に戻ります（削除されたばかりのノードの存在が想定されなくなり、クラスタのサイズが変更されるため）。

クラスタのサイズ変更

[**Remove**] アイコ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。その結果、許容される障害の数に影響が及ぶ場合があります。許容される障害の数（障害許容範囲で定義）が変わるほど大きくクラスタのサイズが変更されると、Elasticsearch が強制的に再起動され、サービスが一時的に中断されます。

例外：上記には、再起動中か、一時的な障害が発生している 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 Threat Grid アプライアンスを追加した場合や、[**Remove**] をクリックした場合は、クラスタサイズが変化して、許容される障害の数が変更されます。その後、クラスタの残りの部分が再設定されるため、短時間の中断が発生します。

障害許容範囲

障害が発生した場合、クラスタ化された Threat Grid アプライアンスは、障害が発生したノードによってアクティブに実行されている分析を除き、データを失うことはありません。また、サービスが中断される期間が最短（1 分未満）のサービスをユーザの関与なしで回復します。

使用可能なノードの数が [**Failure Tolerances**] テーブルの [**Nodes Required**] 列に表示されている数以上である場合、ほとんどの障害は 1 分未満で回復します。または、使用可能なノードの数が増えて前述の数を満たすようになると回復します。この条件は、障害発生前にクラスタが正常な状態だった場合に当てはまります（[**Clustering**] ページで [**Replicated**] と表示されるサービスによって示される）。

特定のサイズのクラスタが許容すると想定される障害の数を次の表に示します。

表 *3 :* 障害許容範囲

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

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。

たとえば、2 つの障害が許容される 5 ノードのクラスタサイズを使用しており、3 つのノードが必要で、5 台のアプライアンスすべてがアクティブにデータを処理しているときに、2 つまでの障害が発生した場合、クラスタは自動的に再設定され、手動による管理アクションなしで動作を続行できます。

別の考慮事項として、5、6、または 7 ノードのクラスタの場合、許容される障害の数が 1 つ増えるごとに、障害が発生し得るノードの比率が高くなることを意味します。この事実は、ノードの数が障害発生率の乗数となるため、特に重要です。（2 つのノードを使用していて、各々にハードウェア障害が 10 年ごとに発生している場合は、ハードウェアの障害発生率を 5 年間に 1 回に変更します）。

障害の回復

多くの場合、障害が発生しても自動的に回復します。回復しない場合は、Threat Grid サポート（support@threatgrid.com）に連絡するか、バックアップからデータを復元する必要があります。詳細については、「バックアップコンテンツの復元」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 つのノードがあるクラスタでは、一方のノードがタイブレーカーで、シングルポイント障害となります。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では、キャパシティとは、ストレージではなくスループットを意味します。3 つのノードを持つクラスタは、単一の Threat Grid 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プルーニングします。その結果、5000 サンプルアプライアンス 3 台を含むクラスタ（合計 15,000 サンプル/日のレート制限）は（フルキャパシティで使用されている場合）、Cisco.com の『*Threat Grid Appliance Data Retention Notes*』に記載されている 10,000 サンプル/日の想定よりも、最短保持期間が 33 % 短くなります。

サンプルの削除

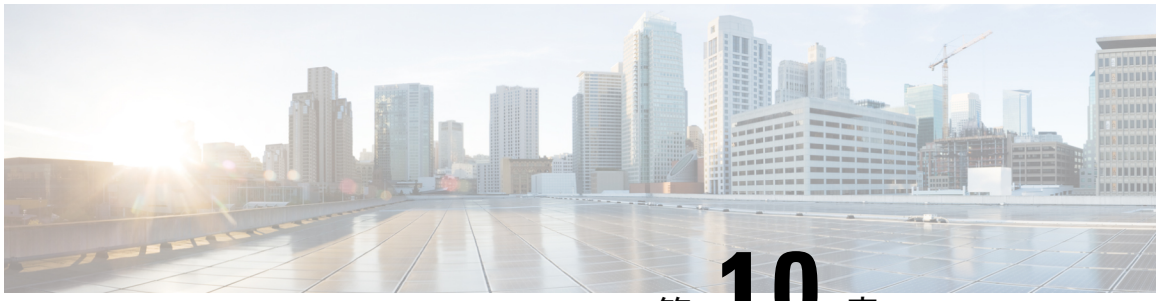
Threat Grid アプライアンス（v2.5.0 以降）では、サンプルの削除がサポートされます。

- [**Delete**] オプションは、サンプルリストの [**Actions**] メニューにあります。
- [**Delete**] ボタンは、サンプル分析レポートの右上隅にあります。

（注） 削除されたサンプルのバックアップコピーがすべてのノードから削除されるまでに、最大 24 時間かかる場合があります。

削除されたサンプルは、ただちに共有 NFS ストアから削除されます。削除要求を処理しているノードからはすぐに削除されますが、他のノードでは、夜間の cron ジョブが実行されるまで保留になります。クラスタモードでは、NFS ストアはサンプルのプライマリソースと見なされます。そのため、サンプルが他のノードから物理的に削除されていない場合でも、いずれのノードからも取得できなくなります。

Threat Grid アプライアンスバージョン2.7 以降では、クラウド製品の動作に合わせて、サンプルの削除にアーティファクトが含まれるように拡張されています。



第 10 章

ネットワーク終了設定

この章では、ネットワーク終了機能とその設定方法について説明します。

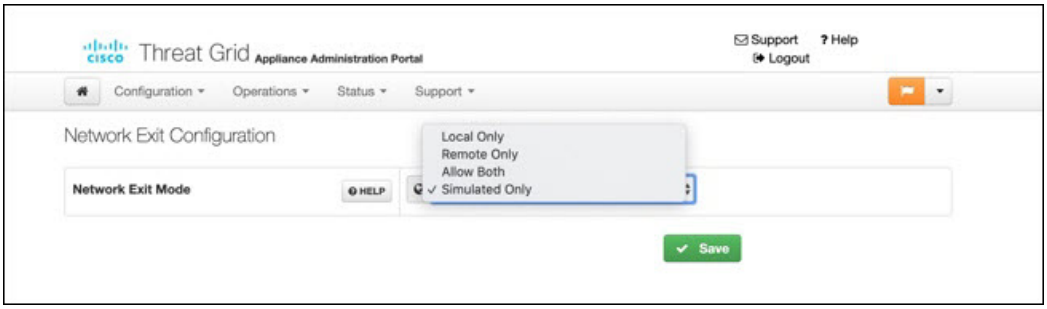
ネットワーク終了の設定

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 の概念と同様に、**ネットワーク終了**設定（v2.4.3 以降）により、サンプル分析中に生成されるすべての発信ネットワークがその場所で終了したように表示されます。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はありません。

（注） 以前に tg-tunnel を使用していた場合は、v2.4.3 をインストールする前に、4.14.36.142:21413 と 63.97.201.68:21413 へのアウトバウンドトラフィックを許可する必要があります。それ以外の場合は、リモート終了の使用を有効にする前に、該当するトラフィックのみを許可する必要があります。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [Network Exit]** をクリックします。

図 *40* : ネットワーク終了設定



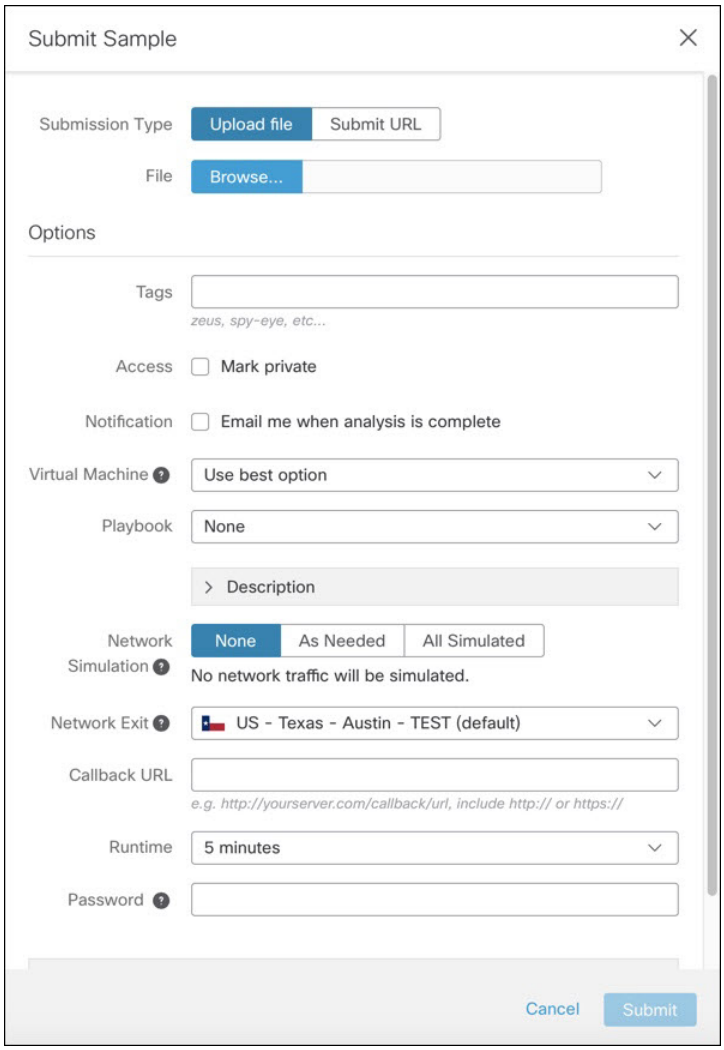
ステップ 2 [**Network Exit Mode**] フィールドで、[**Local Only**]、[**Remote Only**]、[**Allow Both**]、または [**Simulated Only**] を選択します。このフィールドで、UI でサンプルを送信する場合などに、アプリケーションで使用可能にする**ネットワーク終了**オプションを決定します。

[**Local Only**] または [**Remote Only**] を選択した場合、アプリケーションの設定により、ユーザが使用できるのはこれらのオプションのみになります。

[**Simulated Only**] を選択した場合、API ユーザと UI ユーザは、仮想マシンからローカル Threat Grid アプライアンス外の接続先にネットワークトラフィックを送信するオプションを選択できません。

プライベートネットワークへのアクセスは、DNS ルックアップやネットワーク終了が目的であっても許可されません。すべてのマルウェアトラフィックは、設定済みのダーティ DNS サーバを使用して、ダーティインターフェイスから発信されます。

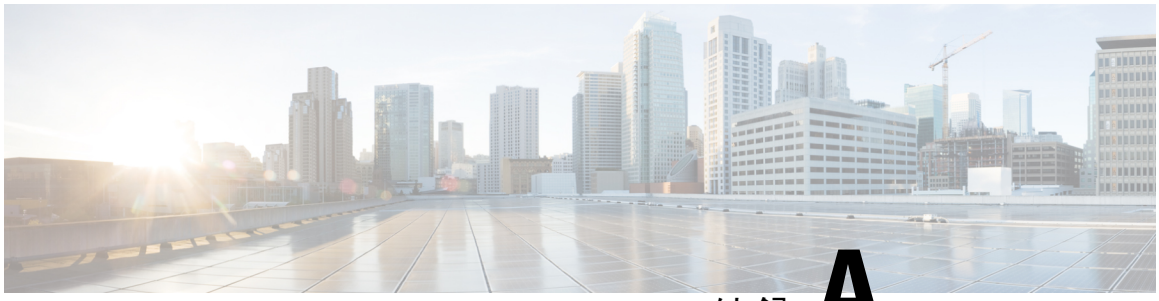
図 *41* : サンプルの送信



（注） 分析中にネットワーク接続をシミュレートする必要が生じることがあります。ネットワーク シミュレーションは、それ以外の方法では（または他の理由で）使用できない可能性があるマルウェアサンプルにネットワークリソースを提示する方法をアナリストに提供します。たとえば、アップストリームサーバにアクセスできない場合、サーバがダウンしている場合、DNS レコードが失われた場合、またはサンプルの実行率と判定率を向上させるためにアウトバウンド接続に対する他の制限が適用されている場合に、ネットワーク接続をシミュレートするネットワーク シミュレーション オプションを選択できます。

さらに、ネットワーク シミュレーションは、エアギャップアプライアンスへの接続方法を少なくともいくつか提供し、それらのアプライアンスに対するサンプルの実行率を改善することができます。

サンプル分析の**ネットワーク シミュレーション**オプションは、Threat Grid Appliance v2.7.1 以降で使用できます。詳細については、Threat Grid Portal UI のオンラインヘルプトピックを参照してください。



付録 A

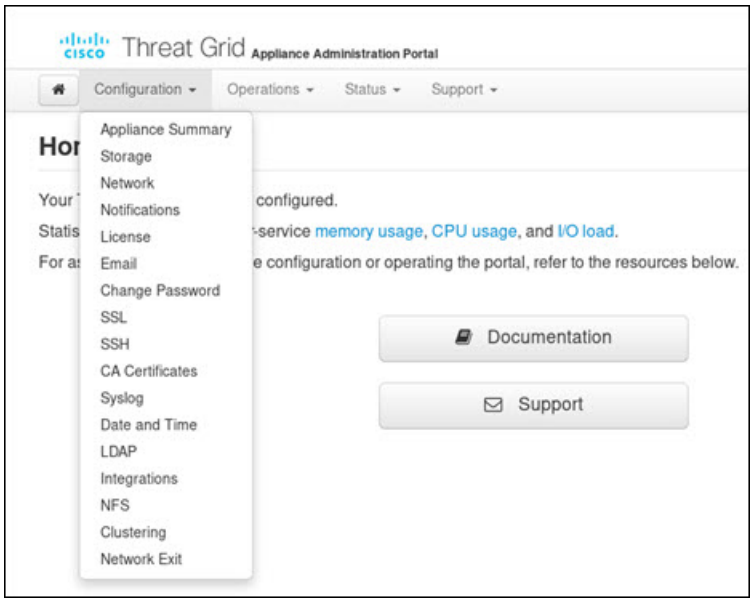
OpAdmin メニュー

この章では、OpAdmin ポータルの各メニューの概要とスクリーンショットを示し、タスクの実行に使用できるさまざまなメニューオプションについて説明します。説明する項目は次のとおりです。

[Configuration] メニュー

OpAdmin ポータルの [**Configuration**] メニューには、Threat Grid アプライアンスを設定するためのオプションが用意されています。設定に変更を加える必要がある場合は、このメニューを使用して編集モードにする必要があります。

図 *42 : OpAdmin* ポータルの *[Configuration]* メニュー

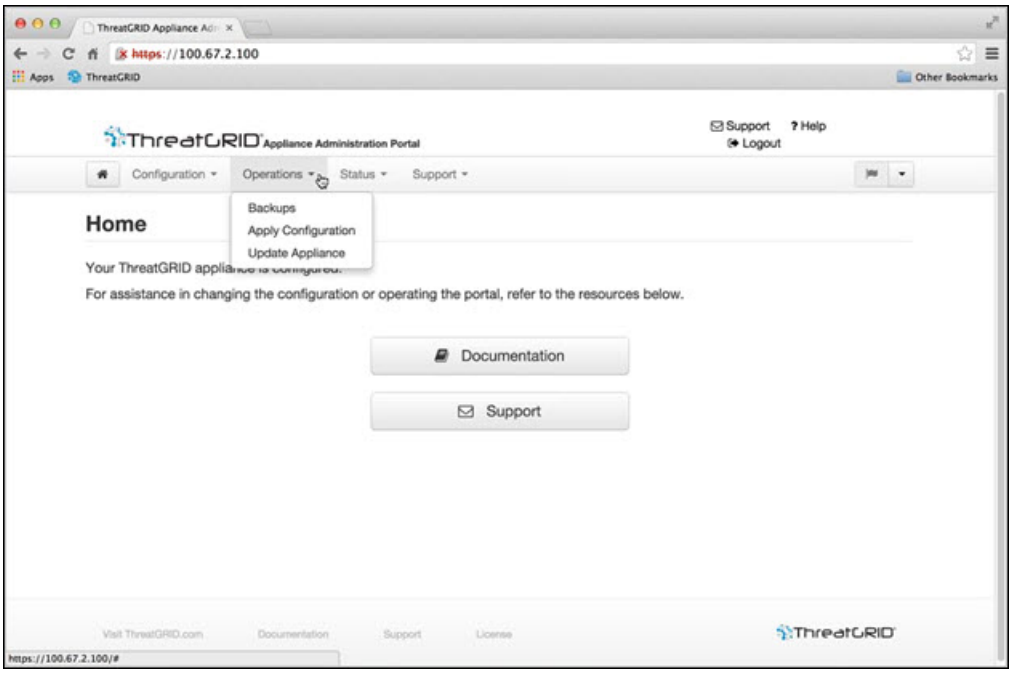


[Operations] メニュー

OpAdmin ポータルの [**Operations**] メニューには、バックアップ、設定の適用、アプライアンスの更新のオプションが用意されています。

（注） [**Operations**] メニューの [**Update Appliance**] を選択して、リリースノートを表示します。

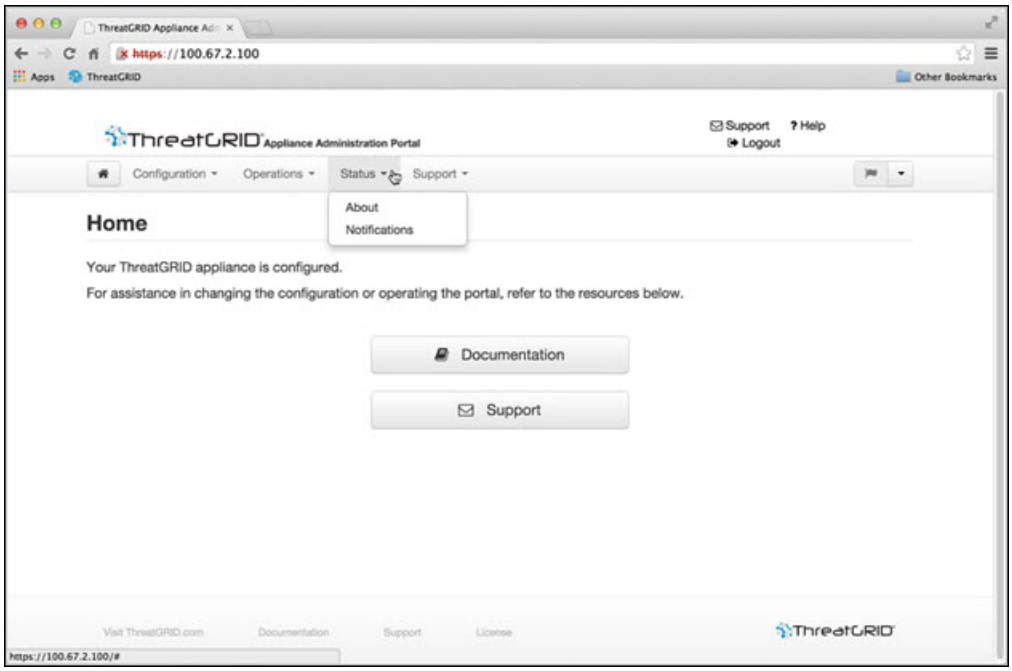
図 *43 : OpAdmin* ポータルの *[Operations]* メニュー



[Status] メニュー

OpAdmin ポータルの [**Status**] メニューは、インストールされているバージョンと通知についての情報を表示するために使用されます。

図 *44 : OpAdmin* ポータルの *[Status]* メニュー

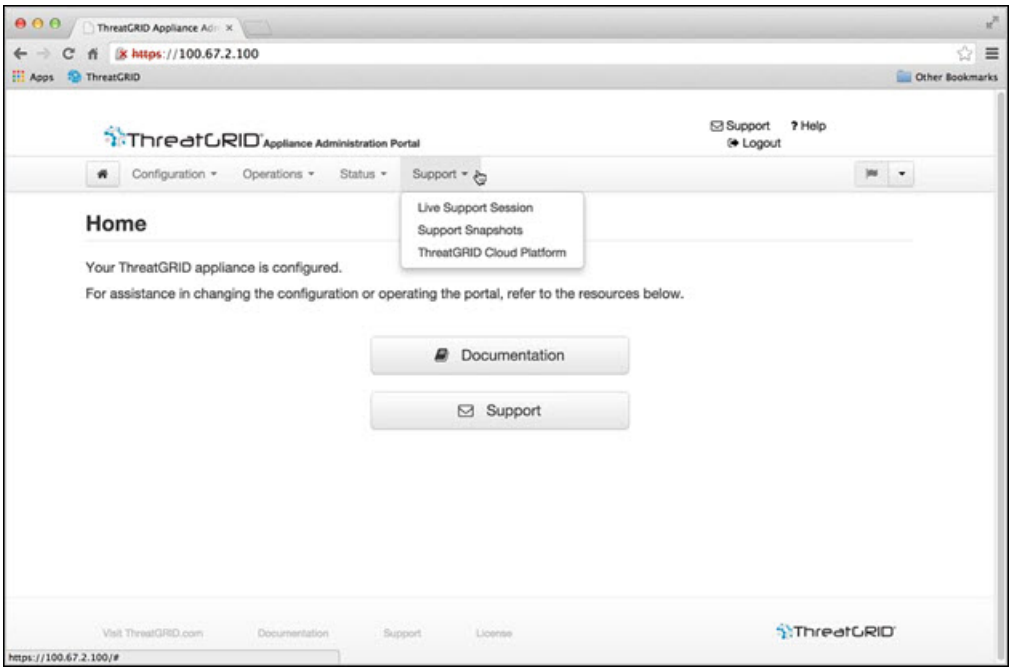


[Support] メニュー

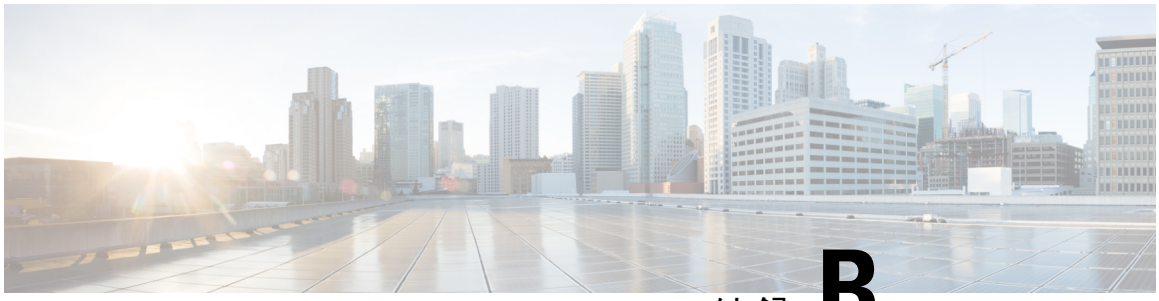
ライブサポートセッションを開始し、システムのスナップショットを取得し、Threat Grid クラウドプラットフォームにアクセスするには、OpAdmin ポータルの [**Support**] メニューを使用します。

OpAdmin メニュー

図 *45 : OpAdmin* ポータルの *[Support]* メニュー



OpAdmin メニュー



付録 B

CIMC の設定

Cisco Integrated Management Controller（CIMC）は、サーバを管理するために使用されるユーザインターフェイスです。この付録には、CIMC ユーティリティを使用したリモートサーバ管理の設定に関する次の情報が含まれます。

CIMC 設定ユーティリティの使用

サーバを起動すると、シスコの画面が表示され、Cisco Integrated Management Controller（CIMC）設定ユーティリティを開始できます。CIMCインターフェイスはリモートサーバ管理に使用できます。

このユーティリティを使用するには、モニタとキーボードをThreat Gridアプライアンスに直接接続する必要があります。

（注） CIMC は、Threat Grid M5 アプライアンスサーバではサポートされていません。

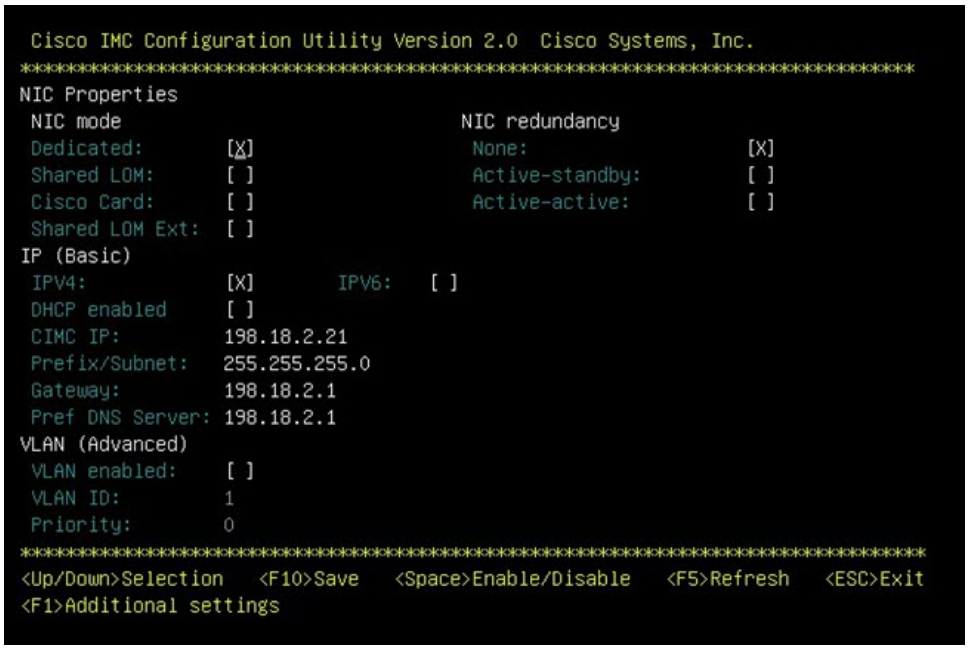
ステップ 1 サーバの電源をオンにします。

CIMC の設定

図 *46 :* シスコの画面

ステップ 2 メモリチェックが完了したら、**F8** を押して CIMC 設定ユーティリティを開始します。

図 *47 : CIMC Configuration Utility*



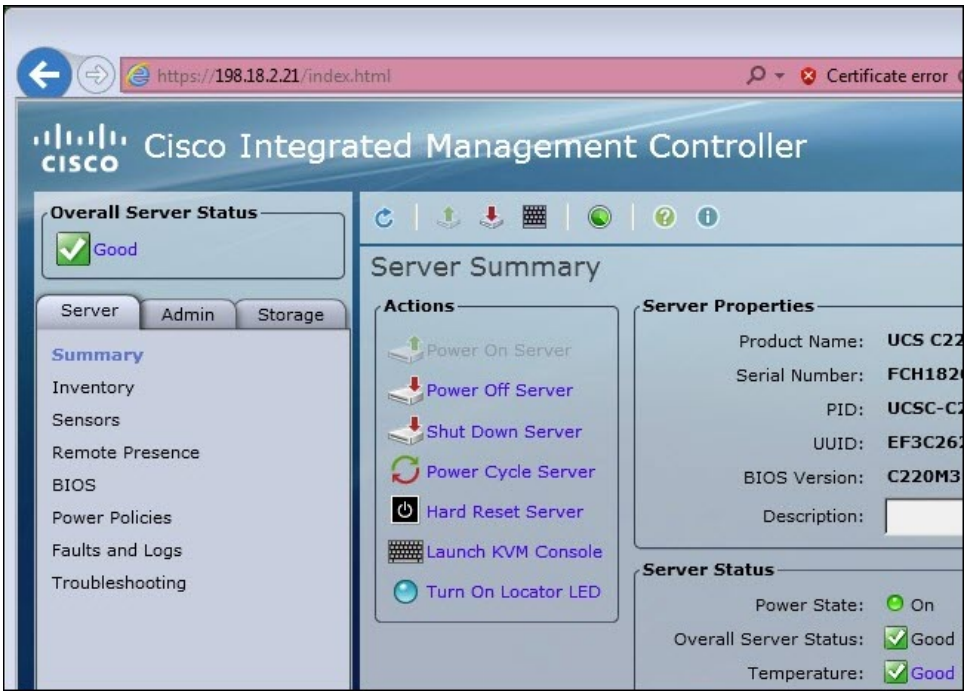
ステップ 3 CIMC 設定ユーティリティで、リモートサーバ管理に使用できる IP アドレスを設定します。

ステップ 4 設定を保存し、ユーティリティを終了します。

ステップ 5 Web ブラウザで「**https://<CIMC-IP address>/**」と入力して、CIMC インターフェイスを開きます。

ステップ 6 初期**ユーザ名**（admin）と**パスワード**（password）を入力します。

図 *48 : Cisco Integrated Management Controller*（*CIMC*）インターフェイス



CIMC インターフェイスを使用して、サーバの正常性を表示したり、KVM を開いて残りのセットアップ手順をリモートで実行したりすることができるようになりました。

CIMC の設定