Threat Grid アプライアンス
設定および構成ガイド

バージョン：2.4.3、2.4.3.1、2.4.2、2.4.3

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

目次

図一覧

はじめに

Cisco Threat Grid アプライアンスは、安全かつ高度にセキュリティ保護された、オンプレミスの高度なマルウェア分析を提供し、詳細な脅威分析およびコンテンツを使用します。Threat Grid アプライアンスは、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。これは、単一の UCS サーバ（Cisco UCS C220-M3 または Cisco C220 M4）にインストールされます。さまざまなコンプライアンスおよびポリシーの制約の下で運営されている組織は、アプライアンスにマルウェア サンプルを送信できます。

銀行、健康サービスなど、機密データを扱う多くの組織は、さまざまな規制やガイドラインに従う必要があり、マルウェア分析のために特定の種類のファイル（マルウェア アーティファクトなど）をネットワーク外部へと送信することは許可されません。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。

このガイドの対象読者

新しいアプライアンスをマルウェアの分析に使用するには、組織のネットワークに対して設定および構成する必要があります。このガイドは、新しい Threat Grid アプライアンスの設定および構成タスクを行うセキュリティ チームの IT スタッフを対象としています。

このドキュメントでは、マルウェアのサンプルを分析に送信するまでを対象とした、新しい Threat Grid アプライアンスの初期設定および構成を完了する方法について説明します。

詳細については、Cisco.com の **Install and Upgrade ページ**にある『Cisco Threat Grid *Appliance Administrator's Guide*』を参照してください。

リリース ノート

詳細な更新情報については、『Release Notes』を参照してください。これは、次の OpAdmin Portal にあります。

[運用 (Operations)] メニュー > [アプライアンスの更新 (Update Appliance)]

リリース ノートは累積的であり、最新バージョンにはそれまでのすべてのノートが含まれています。Threat Grid アプライアンスのその他のドキュメントとともに、フォーマットされた PDF バージョンをオンラインで参照することもできます。

http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html

バージョン ルックアップ テーブル

Threat Grid アプライアンスのリリース情報リストについては、「ビルド番号/バージョン ルックアップ テーブル」を参照してください。

注：Threat Grid Portal の UI でリリース ノートを参照するには、UI のナビゲーション バーで [ヘルプ (Help)] をクリックします。

最新情報

新機能の完全な説明については、必ず『*Release Notes*』、および『Migration Notes』や『Data Retention Notes』など、その他のリリース ドキュメントを参照してください。主な内容はこれらのドキュメントに含まれています。

Network Exit のサポート

VPN に対する概念と同様に、Network Exit の設定により、分析中に生成される発信ネットワーク トラフィックがその場所で終了するように表示されます。Network Exit Localization は、3.4.61 リリースで Threat Grid クラウド ポータルに追加され、v2.4.3 のアプライアンスで使用できるようになりました。

これは tg-tunnel に代わる機能です。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えいリスクを回避します。

詳細については、『*Threat Grid Appliance Guide*』の「*Network Exit Configuration*」セクションを参照してください。

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、早期フィールド トライアルの v2.4.0 で導入され、v2.4.2 で正式に利用可能となりました。

クラスタリングの主な目的は、1 つのクラスタに複数のアプライアンス（現在は 2 ～ 5）を関連付けて単一システムの機能を強化することです。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、クラスタ内の他のアプライアンスで同じデータを使用することができます。

現在使用可能なクラスタリング機能の詳細については、Cisco.com Web サイトの **Threat Grid Appliance Install and Upgrade ページ**より入手可能な『*Threat Grid Appliance Administrator's Guide*』の「*Clustering*」セクションおよび「Clustering FAQ」を参照してください。

ダーティ インターフェイスでの IPv4LL アドレス空間の使用がサポート対象外に

ダーティ インターフェイスでの IPv4LL アドレス空間 (168.254.0.16) の使用はサポート対象として文書化されていませんでしたが、バージョン 2.3.0 以降これがエラーとして認識されるようになり、明示的にサポート対象外となりました。

自動ライセンスの取得

アプライアンスがインターネットに接続している場合は、ライセンスの取得や期限切れのライセンスの交換をネットワーク経由で試行できます。自動取得は現在 (17/08/11)、ソフトウェアのバージョン 2.3 をリリース後に販売または更新されたライセンスでのみ使用できます。

Windows のその他の変更点

2.3 リリースには、Windows に関する次の変更点が含まれています。

- Windows XP が削除されます（すでにアプライアンスで適用対象外となっている場合も含みます）。
- Windows 7 は 64 ビットのみのサポートとなります。
- 「winxp」または「win7 x86」VM に送信されるサンプルは引き続き使用できます。「winxp」をハードコーディングしたスクリプトまたはクライアントは、変更する必要があります。

バックアップ

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

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

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。バックアップ機能に関する詳細ドキュメントを入手できます。『Threat Grid Appliance Administrator's Guide』の「*Backup Notes and FAQ*」、および「Backup」セクションを参照してください。どちらのドキュメントも、Cisco.com Web サイトの **Threat Grid Appliance Install and Upgrade ページ**から入手できます。

Windows XP の変更点

2017 年 7 月 1 日以降に製造された Threat Grid アプライアンスには、Microsoft 要件に準拠した Windows XP のライセンスまたは配布が含まれていません。2.2.3 マイナー リリースでは、Windows XP を使用しないで実行できるように新しく工場出荷時のインストールが行われています。

サード パーティ検出との統合およびエンリッチメント サービス

バージョン 2.2 では、OpenDNS、TitaniumCloud、および VirusTotal との統合がアプライアンスの新しい構成ページで設定できるようになりました。OpAdmin で、[構成 (Configuration)] > [統合 (Integrations)] の順に選択してこのページを開きます。詳細については、『*Threat Grid Administrator's Guide*』を参照してください。

配置更新サービス マネージャ用の複数の URL

バージョン 2.2 は、配置更新サービス マネージャ用に複数の URL を構成する機能も備えています。

ClamAV シグネチャの自動的な日次更新

バージョン 2.2 を使用すると、ClamAV シグネチャに対する更新のダウンロードを日単位で自動的にアプライアンスにダウンロードできるようになりました。この機能はデフォルトで有効になっており、OpAdmin の新たに追加された統合ページから無効にすることもできます。

LDAP 認証

LDAP 認証は、2017 年 1 月 5 日にリリースされたバージョン 2.1.6 で OpAdmin および TGSH ダイアログの管理者インターフェイスに追加されました。これは、複数のアプライアンスの管理者で同じログインおよびパスワードを共有しないお客様のためのサポートです。詳細については、『*Threat Grid Administrator's Guide*』を参照してください。

Cisco UCS C220 M4 サーバ

2016 年 11 月 17 日にリリースされた C220 M4 サーバには、ハードウェアの更新に加え、セキュア ブート機能が含まれています。アップグレードについてご質問がある場合は、support@threatgrid.com までお問い合わせください。

注：Threat Grid では、契約済みの期限が切れるまで、M3 に対するサポートの提供を継続します。既存の M3 向けの Over-the-Wire アップデートとして、以下に記載された事項を除きまったく同様の M4 機能が利用可能です。

M5 サーバ アップグレードは、現在開発中です。既存の M3 および M4 をご利用中のお客様で、サーバのアップグレード、データの移行、バックアップ、ロールアウト戦略などがお客様のニーズに適しているかなどご不明な点がある場合は、support@threatgrid.com にお問い合わせください。お客様の個別の要件に合わせた M5 へのアップグレード方法を計画し、最適なアプローチを検討していきます。

AMP for Endpoints プライベート クラウドの統合

2.0.3 リリースには、Fire AMP プライベート クラウド（AMP for Endpoints プライベート クラウドに名前変更）と Threat Grid アプライアンスの統合を容易にする機能が含まれています。これには、DNS をクリーン ネットワーク インターフェイスとダーティ ネットワーク インターフェイス、CA 管理、および AMP for Endpoints プライベート クラウド統合構成で分割するための機能が含まれます。

生成される SSL 証明書は、subjectAltName として複製された CN を持つようになりました。これは、1 つ以上の subjectAltName が存在すると CN フィールドを無視する SSL クライアントとの非互換性に対処するものです。このようなツールを使用している場合、アプライアンスによって以前に生成された証明書は、再度生成する必要が生じる場合があります。

バージョン 2.0

バージョン 2.0 は、更新されたオペレーティング システムに構築されたメジャー リリースです。これには、将来のハードウェア リリースの強化機能が含まれます。また、Threat Grid Portal の UI をクラウド バージョンにさらに近付けます。この機能強化には、数多くの新しいまたは更新された動作指標などの変更が含まれます。

詳細については、リリース 3.3.45 以降の『*Threat Grid Portal Release Notes*』を参照してください。（Portal UI のナビゲーション バーで [ヘルプ (Help)] を選択し、リリース ノートへのリンクをクリックします。）

サポート：Threat Grid へのアクセス

Threat Grid エンジニアのサポートを要求するには、以下の複数の方法があります。

- **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** を使用して、サポート ケースを入力します。
- **コール。**Cisco の電話番号と連絡先情報については、**Cisco Contact ページ**を参照してください。

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、[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 サポートを利用してライブ サポート セッションを開始するには：

[OpAdmin] で、[サポート (Support)] > [ライブサポートセッション (Live Support Session)] の順に選択し、[サポートセッションの開始 (Start Support Session)] をクリックします。

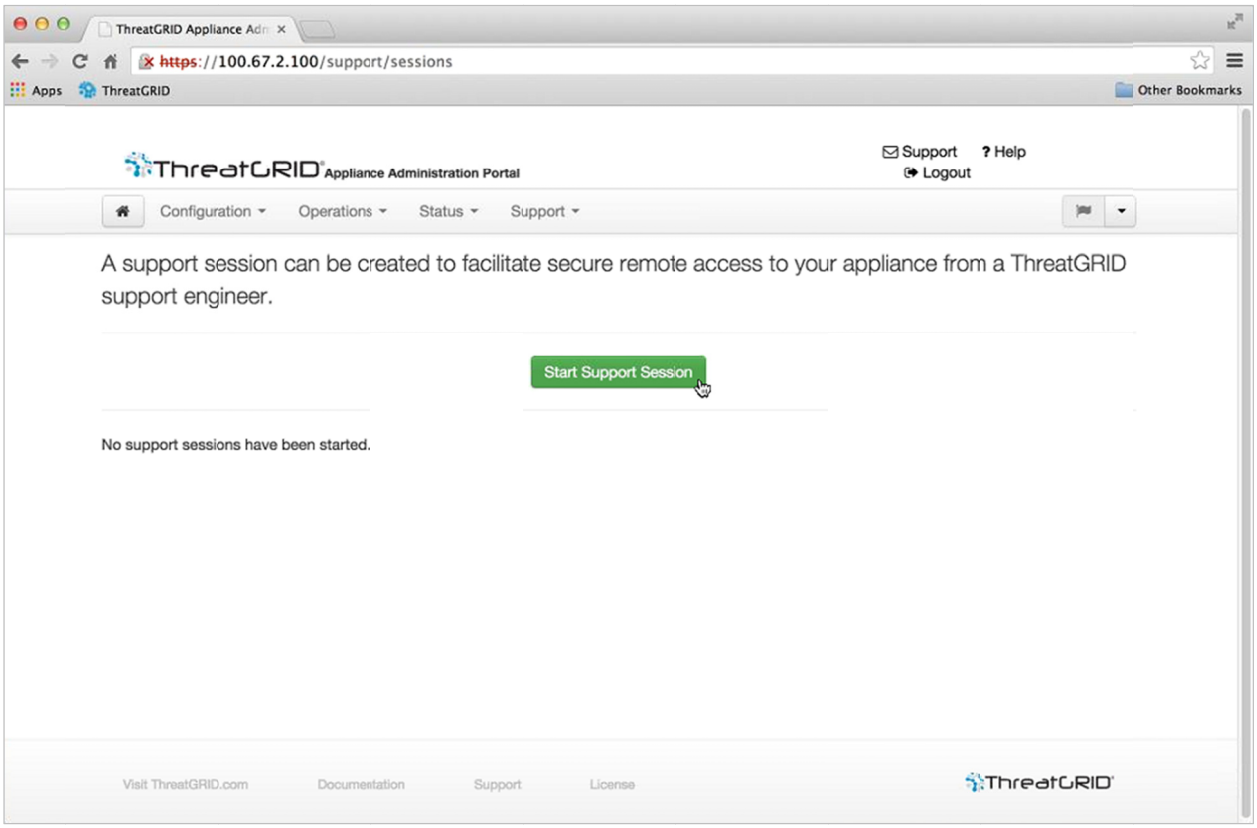
注：ライセンシングの前に、OpAdmin ウィザードのタスクフローを中止して サポート モードを有効にすることができます。

サポート モードの開始：バージョン 1.4.4 より前のライセンスの回避策

Threat Grid アプライアンス v1.4.4 で解決されたライセンスに関する問題があります。ソフトウェア バージョンが 1.4.4 よりも前の場合、ライセンスが受け入れられるには、*サポート モード*のサーバに少なくとも 1 回は正常に接続する必要があります（2015 年 11 月 14 日以降）。接続は、ライセンスの検証時に進行中またはアクティブである必要はありません。

必須：この手順を有効にするには、ダーティ ネットワークが稼働している必要があります。

図 1：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. SSH がサポート スナップショット サービスに対して指定されていることを確認します。
2. [Support] メニューから、[Support Snapshots] を選択します。

3. スナップショットを取得します。
4. 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、[実行 (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。

計画

Cisco Threat Grid アプライアンスは、出荷前にシスコの製造部門によってインストールされた Threat Grid ソフトウェアを備える Linux サーバです。新しいアプライアンスを受け入れた場合、オンプレミスのネットワーク環境用に設定および構成する必要があります。開始前に、考慮し、計画するいくつかの問題があります。環境要件、ハードウェア要件、およびネットワーク要件は、次のとおりです。

ユーザ マニュアルとオンライン ヘルプ

Threat Grid アプライアンス：Threat Grid アプライアンスのユーザ マニュアル（本ドキュメント、『*Threat Grid Appliance Administrator's Guide*』、リリース ノート、統合ガイドなど）は、Cisco.com の **Install and Upgrade ページ**にあります。

Threat Grid Portal UI のオンライン ヘルプ：Threat Grid Portal のユーザ マニュアル（リリース ノート、「Using Threat Grid」オンライン ヘルプ、API ドキュメンテーション、およびその他の情報）は、ユーザ インターフェイスの最上部にあるナビゲーション バーの [ヘルプ (Help)] メニューから利用できます。

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
Network Exit のサポート	3	新機能についての説明
ダーティ インターフェイスでの IPv4LL アドレス空間の使用がサポート対象外に	4	新規セクション
tgsh	15	新規セクション

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
- Microsoft Internet Explorer：**サポート対象外。使用しないでください。**Microsoft Internet Explorer は推奨されておらず、サポートされていません。

環境要件

Threat Grid アプライアンスは UCS C220-M3 または C220-M4 サーバに導入されます。アプライアンスのセットアップおよび設定を行う前に、サーバの仕様に従って、電源、ラック スペース、冷却、その他の課題に対する環境要件が満たされていることを確認します。

ハードウェア要件

管理インターフェイス用のフォーム ファクタは SFP+ です。アプライアンスをクラスタリングしている場合は、それぞれの顧客インターフェイスで追加の SFP+ モジュールが必要になります。

注：SFP+ モジュールは、設定ウィザードを実行するセッションでアプライアンスの電源を入れる前に接続する必要があります。

スイッチで使用できる SFP+ ポートがないか、または SFP+ が好ましくなければ、1000Base-T のトランシーバを使用できます（シスコ機器互換のギガビット RJ 45 銅線 SFP トランシーバ モジュール Mini -GBIC - 10/100/1000 Base-T 銅線 SFP モジュール）。

図 2：Cisco 1000BASE-T 銅線 SFP (GLC-T)

モニタ：サーバにモニタを接続できます。また、CIMC (Cisco Integrated Management Controller) が設定されている場合、リモート KVM を使用できます。

ハードウェアに関するドキュメント

Cisco UCS C220 M4 サーバのインストールおよびサービス ガイド：

- Cisco UCS C220 M4 サーバのインストールおよびサービス ガイド

Cisco UCS C220 M3 サーバのインストールおよびサービス ガイド：

- https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220.html

Cisco UCS C220 M3 高密度ラック サーバ（スモール フォーム ファクタ ディスク ドライブ モデル）の仕様書：

- https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/C220M3_SFF_SpecSheet.pdf

シスコには、電源/冷却のカルキュレータがあり、これが役立つ場合もあります。

- https://mainstayadvisor.com/Go/Cisco/Cisco-UCS-Power-Calculator.aspx

ネットワーク要件

Threat Grid アプライアンスには 3 つのネットワークが必要です。

管理 (ADMIN)：「管理」ネットワーク。 アプライアンスのセットアップを実行するために設定する必要があります。

- OpAdmin 管理トラフィック (HTTPS)
- SSH
- NFSv4（発信。IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。

クリーン (CLEAN)：「クリーン」ネットワークはアプライアンスへの信頼できる着信トラフィック（要求）に使用されます。これには、統合されたアプライアンスが含まれています。たとえば、Cisco E メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンス (ESA/WSA) は、クリーンなインターフェイスの IP アドレスに接続します。

注：クリーン ネットワーク インターフェイスの URL は OpAdmin Portal の設定が完了するまで*機能しません*。

次の特定の制限を受けるネットワーク トラフィックの種類は、クリーン インターフェイスからの発信にすることができます。

- リモートの Syslog 接続
- Threat Grid アプライアンス自体によって送信される電子メール メッセージ
- AMP for Endpoints プライベート クラウド デバイスへの配置更新サービス接続
- 上記のいずれかに関連する DNS 要求
- LDAP

ダーティ (DIRTY)：「ダーティ」ネットワークはアプライアンスからの発信トラフィック（マルウェア トラフィックを含む）に使用されます。

注：内部ネットワーク アセットを保護するために、企業 IP とは異なる専用の外部 IP アドレス（つまり、「ダーティ」インターフェイス）の使用を推奨します。

ネットワーク インターフェイスの設定情報および説明については、以下の「ネットワーク インターフェイス」セクションおよび「ネットワーク インターフェイスの設定」セクションを参照してください。

DNS サーバ アクセス

配置更新サービスのルックアップ、リモートの Syslog 接続の解決、および Threat Grid ソフトウェア自体からの通知に使用されるメール サーバの解決以外の目的に使用される DNS サーバは、ダーティ ネットワークを介したアクセスが可能になっている必要があります。

デフォルトでは、DNS はダーティ インターフェイスを使用します。クリーン インターフェイスは AMP for Endpoints プライベート クラウドの統合に使用されます。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 インターフェイスに構成できます。

詳細については、『*Threat Grid Appliance Administrator's Guide*』を参照してください。

NTP サーバ アクセス

NTP サーバは、ダーティ ネットワークを介してアクセスできる必要があります。

統合：ESA/WSA/AMP for Endpoints など。

Threat Grid アプライアンスを他のシスコ製品（ESA/WSA アプライアンス、AMP for Endpoint プライベート クラウドなど）とともに使用する場合、追加の計画が必要になることがあります。

DHCP

DHCP を使用するように構成されているネットワークに接続する場合、『*Threat Grid Appliance Administrator's Guide*』の「**Using DHCP**」セクションに記載されている指示に従ってください。

ライセンス

Cisco Threat Grid からライセンスとパスワードを受信します。

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。

組織およびユーザ

アプライアンスの設定とネットワーク構成を完了したら、ユーザがログインおよび分析用にマルウェア サンプルを送信できるように、最初の Threat Grid 組織を作成し、ユーザ アカウントを追加する必要があります。このタスクでは、要件に応じて、複数の組織およびユーザ間のプランニングや調整が必要になることがあります。

Threat Grid 組織の管理は、『*Threat Grid Appliance Administrator's Guide*』で説明されています。Threat Grid ポータルのヘルプでは、ユーザの管理について説明されています。

変更点

初期のアプライアンス設定および構成手順は、Threat Grid アプライアンスの更新をインストールする前**に完了する必要**があります。

このガイドに記載されている初期構成の完了後、すぐに更新を確認することをお勧めします。

更新は、順に実行する必要があります。Threat Grid アプライアンスの更新は、ライセンスがインストールされるまでダウンロードできません。また、更新プロセスでは、初期アプライアンス構成が完了している必要があります。アプライアンス更新の手順は、『*Threat Grid Appliance Administrator's Guide*』に記載されています。

注：SSH の更新に指定されたことを確認します。

ユーザ インターフェイス

サーバをネットワークに接続し、正常に起動した後で Threat Grid アプライアンスを構成するために、複数のユーザ インターフェイスを利用できます。LDAP 認証は、TGSH ダイアログとバージョン 2.1.6 の OpAdmin で利用できます。

TGSH ダイアログ

最初のインターフェイスは、ネットワーク インターフェイスを構成するために使用される **TGSH ダイアログ**です。TGSH ダイアログは、アプライアンスが正常に起動すると表示されます。

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には、ユーザ「**threatgrid**」として管理 IP アドレスに SSH 接続を行います。

必要なパスワードは、イニシャル、ランダムに生成されたパスワード（TGSH ダイアログで最初に表示されているもの）または、OpAdmin Portal の構成の最初の手順で作成する新しい管理パスワード（次のセクションで説明）のいずれかです。

tgsh

Threat Grid のシェル。これは、複数のコマンドの実行（destroy-data や forced backup など）や専門家によるローレベルのデバッグに使用される、管理者のインターフェイスです。tgsh にアクセスするには、TGSH ダイアログで [CONSOLE] を選択します。

注：OpAdmin は Threat Grid ユーザと同じクレデンシャルを使用します。したがって、tgsh によって行われたパスワードの変更/更新は OpAdmin にも影響を及ぼします。

注意：tgsh によるネットワーク設定の変更は、Threat Grid のサポートから特に指示がない場合はサポートされません。OpAdmin または TGSH ダイアログを代わりに使用する必要があります。

OpAdmin Portal

これは、主要な Threat Grid GUI 構成ツールです。ライセンス、電子メール ホスト、SSL 証明書などを含むアプライアンス構成の多くは、OpAdmin を使用しないとできません。

Threat Grid Portal

Threat Grid ユーザ インターフェイス アプリケーションはクラウド サービスとして利用可能です。また、Threat Grid のアプライアンスにインストールされています。Threat Grid Cloud サービスと、Threat Grid アプライアンスに含まれる Threat Grid Portal との間で通信は行われません。

CIMC

別のユーザ インターフェイスには Cisco Integrated Management Controller（「CIMC」）があり、これはサーバを管理するために使用されます。

ネットワーク インターフェイス

管理インターフェイス

- 管理ネットワークに接続します。管理ネットワークからの**着信のみ**です。
- OpAdmin UI トラフィック
- TGSH ダイアログへの SSH（着信）
- バックアップとクラスタリングを行う NFSv4（発信。IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。すべてのクラスタ ノードからアクセスできる必要があります。

注：管理インターフェイス用のフォーム ファクタは SFP+ です。図 2：Cisco 1000BASE-T 銅線 SFP (GLC-T を参照してください。

クラスタ インターフェイス

以前に予約された管理者以外の SFP+ ポートが、クラスタリングで使用されるようになりました。

- クラスタリングに必要なクラスタ インターフェイス（任意）
- ダイレクト インターコネクトには追加の SFP+ モジュールが必要です。このインターフェイスでは、設定の必要はありません。アドレスが自動的に割り当てられます。

クリーン インターフェイス

- クリーン ネットワークに接続します。クリーンには、社内ネットワークからアクセスできる必要がありますが、インターネットへの発信アクセスができないようにする必要があります。
- UI と API トラフィック（着信）
- サンプルの送信
- SMTP（構成済みメール サーバへの発信接続）
- SSH（TGSH ダイアログへの着信）
- Syslog（構成済み Syslog サーバへの発信）
- ESA/WSA：CSA の統合
- AMP for Endpoints プライベート クラウドの統合
- DNS：オプション。
- LDAP（発信）

ダーティ インターフェイス

ダーティ ネットワークに接続します。インターネット アクセスを必要とします。**発信のみ**です。

- DNS
  注：AMP for Endpoints プライベート クラウドとの統合を設定し、AMP for Endpoints アプライアン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。
- NTP
- アップデート

- 通常動作モードのサポート セッション
- サポート スナップショット
- マルウェア サンプルから開始されたトラフィック
- リカバリ モード サポート セッション（発信）
- OpenDNS、TitaniumCloud、Virus Total、ClamAV
- SMTP の発信接続が組み込みのハニーポットにリダイレクトされます。

注：ダーティ インターフェイスでの IPv4LL アドレス空間 (168.254.0.16) の使用はサポート対象として文書化されていませんでしたが、バージョン 2.3.0 以降これがエラーとして認識されるようになり、明示的にサポート対象外となりました。

CIMC インターフェイス

推奨Cisco Integrated Management Controller（「CIMC」）インターフェイスが構成済みの場合、サーバの管理およびメンテナンスに使用できます。詳細については、付録 A - CIMC 設定（推奨）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

Web UI 管理者

- **ログイン：** admin
- **パスワード：** 「changeme」

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 の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、『*Threat Grid Appliance Administrator's Guide*』の「**Support**」セクションに記載されている「**Lost Password**」の手順に従います。

CIMC (Cisco Integrated Management Controller)

- **ログイン：** admin
- **パスワード：** 「password」

設定と構成手順の概要

このドキュメントでは、次の設定および初期構成の手順を説明します。

- サーバの設定。
- 次のネットワーク インターフェイスの設定：
  - 管理者
  - クラスタ
  - クリーン
  - ダーティ
- 初期ネットワーク構成：TGSH ダイアログ。
- 主要な構成：OpAdmin Portal。
- 更新のインストール。
- アプライアンスの設定をテストします。分析用のサンプルを送信します。
- 管理構成：『*Threat Grid Appliance Administrator's Guide*』に記載されているとおり、OpAdmin Portal で、残りの管理構成タスク（ライセンスのインストール、電子メール サーバ、SSL 証明書など）を完了します。

設定と構成に必要な時間

サーバの設定および初期構成の手順を完了するには、約 1 時間必要です。

注：初期のアプライアンス構成インストール手順では、TGSH ダイアログの [適用 (Apply)] セクションの実行にしばらく時間がかかるため、お待ちください。これらの手順は、場合によって完了まで 10 分かかる場合があります。

サーバの設定

開始するには、アプライアンスの背面にある両方の電源を接続し、付属の KVM アダプタを外部モニタおよびキーボードに接続して、サーバの前面にある KVM ポートに、下の図のように差し込みます。

CIMC が構成に含まれる場合、リモート KVM を使用できます。CIMC の構成については、「*付録*」の「**CIMC の構成（オプション）**」を参照してください。

ハードウェアおよび環境の詳細なセットアップ情報については、サーバ製品のマニュアルを参照してください。製品ドキュメンテーションへのリンクは、上の「ハードウェアに関するドキュメント」セクションに記載されています。

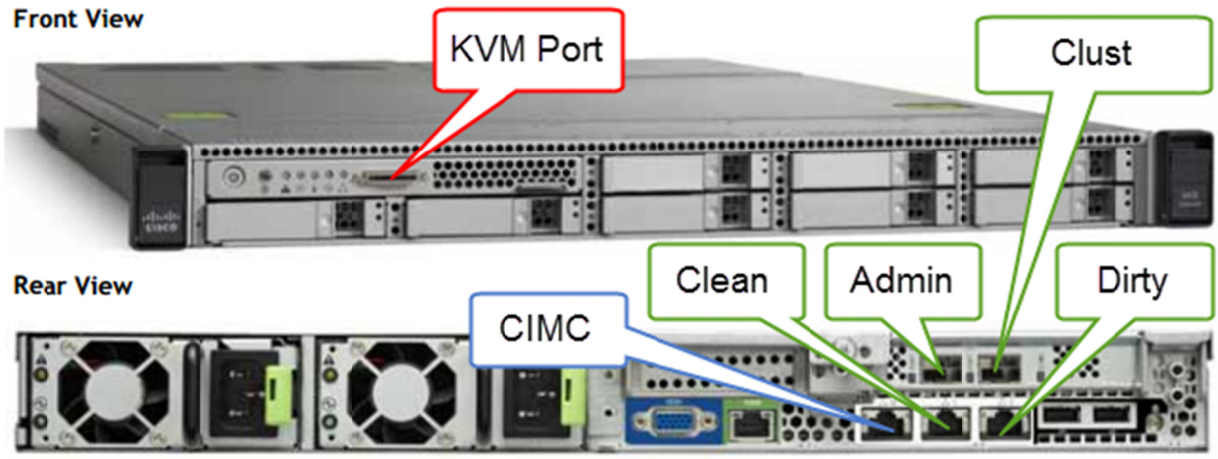
ネットワーク インターフェイスの設定

SFP+ モジュールは、設定ウィザードを実行するセッションでアプライアンスの電源を入れる前に接続する必要があります。ただし、ネットワークまでの SFP の配線は、電源投入後設定までの間に実行できます。

アプライアンスの背面にある SFP+ ポート（2 個）と 3 個のイーサネット ポートを見つけ、下図のようにネットワーク ケーブルを接続します。

C220 M3 ラック サーバ設定

図 3：Cisco UCS C220 M3 SFF ラック サーバ



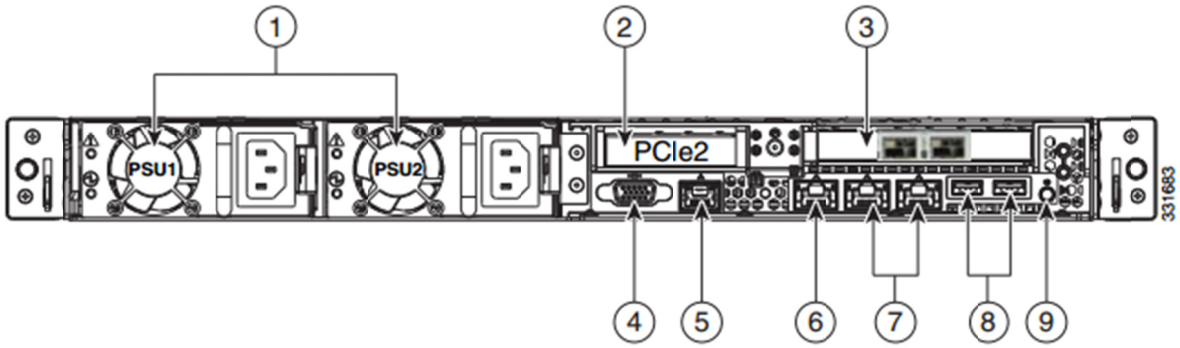
アプライアンスが動作するために、インターフェイスが適切に接続され、構成されている必要があります。

注：アプライアンスの詳細は、上図と異なる場合があります。ご質問がある場合は、**support@threatgrid.com** までお問い合わせください。

注：「クラスタ」はオプションの管理者以外の SFP+ ポート（クラスタリングで予約済み）です。

C220 M3 サーバの詳細については、下の図を参照してください。

図 4：Cisco UCS C220 M3 背面の詳細図

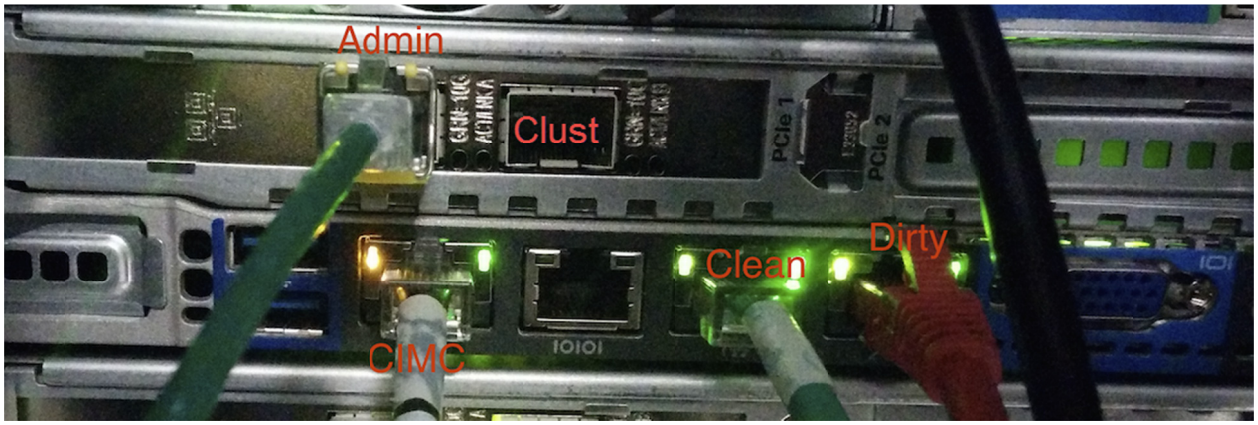


1	Power supplies (up to two)	6	One 10/100/1000 Ethernet dedicated management port
2	Slot 2: Low-profile PCIe slot on riser: (half-height, half-length, x16 connector, x8 lane width)	7	Dual 1-GbE ports (LAN1 and LAN2)
3	Two SFP+ Ports. Slot 1: Admin Slot 2: Clust	8	USB ports
4	VGA video connector	9	Rear Identification button/LED
5	Serial port (RJ-45 connector)[1]	—	—

注：リリース 1.0 ～ 1.2 については、ブート時にインターフェイスが挿入されていない場合、再ブートが必要になることがあります。これは、1.3 より前の問題です（SFP を必要とするインターフェイスは、1.3 以降でもブート時に挿入されている必要があるため、これを除く）。SFP に挿入されたネットワーク ケーブルは、安全にホットプラグ可能です。

C220 M4 ラック サーバ設定

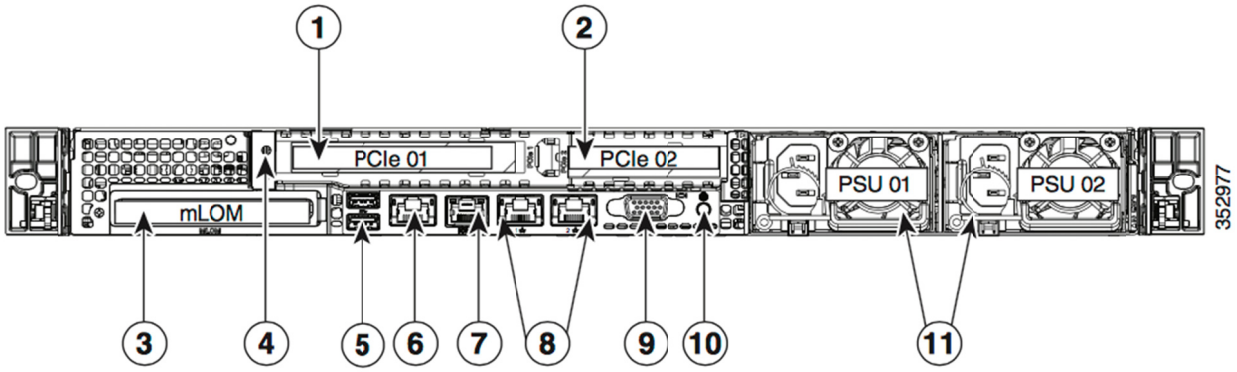
図 5：Cisco UCS C220 M4 SFF ラック サーバ



注：オプションのクラスタ インターフェイスにはポート 3 スロット 2 を使用します。

注：アプライアンスの詳細は、上図と異なる場合があります。ご質問がある場合は、**support@threatgrid.com** までお問い合わせください。

図 6：Cisco UCS C220 M4 背面の詳細図



1	PCIe riser 1/slot 1	**7**	Serial port (RJ-45 connector)
2	PCIe riser 2/slot 2	**8**	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
3	Modular LAN-on-motherboard (mLOM) card slot	**9**	VGA video port (DB-15)
4	Grounding-lug hole (for DC power supplies)	**10**	Rear unit identification button/LED
5	USB 3.0 ports (two)	**11**	Power supplies (up to two, redundant as 1+1)
6	1-Gb Ethernet dedicated management port		

コネクション:

1　　管理、クラスタ

8　　（左）クリーン

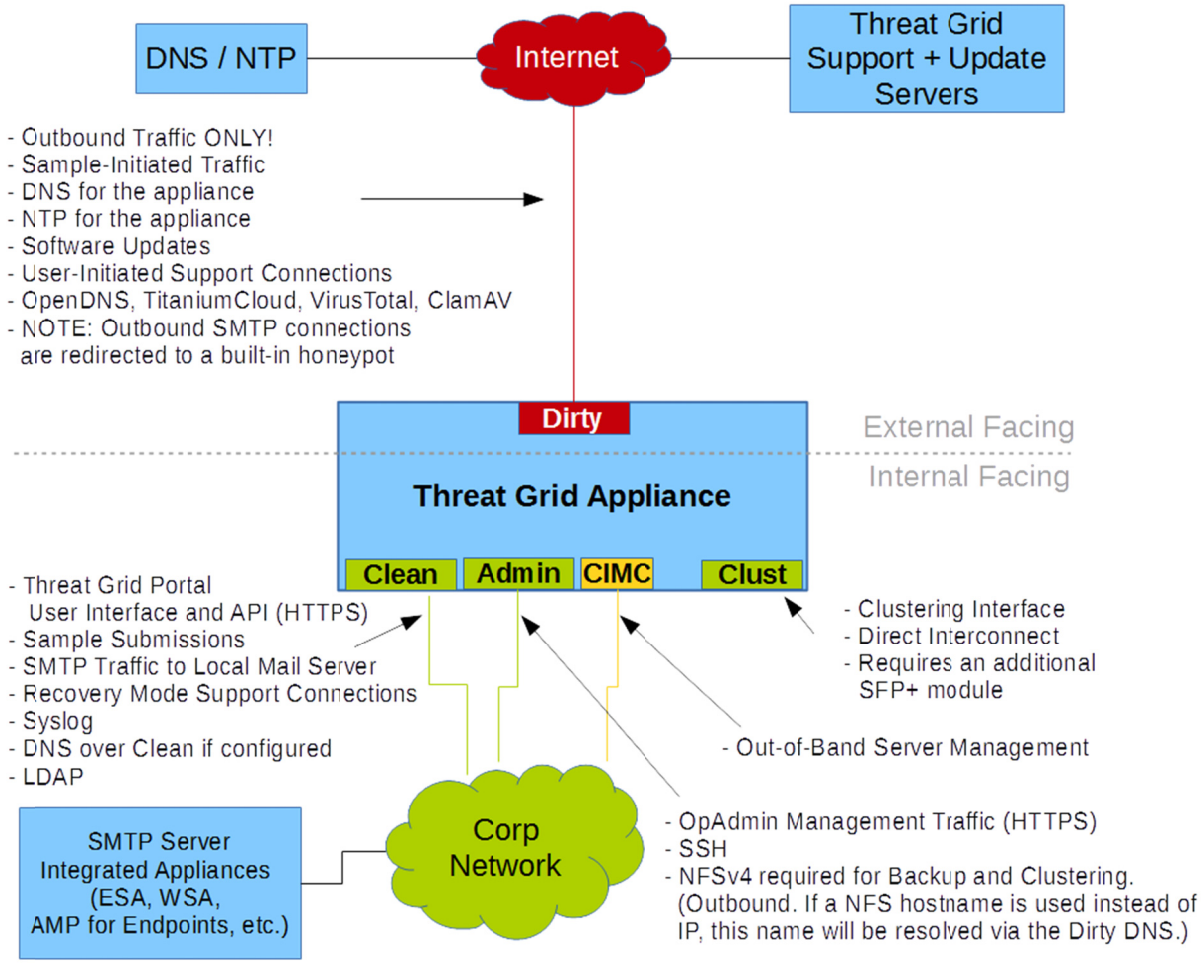
8　　（右）ダーティ

6　　CIMC

ネットワーク インターフェイスの設定図

このセクションでは、Threat Grid アプライアンスの最も論理的/推奨される設定について説明します。ただし、お客様のインターフェイス設定はそれぞれ異なります。ネットワーク要件によっては、たとえば、ダーティ インターフェイスを内部に接続したり、クリーン インターフェイスを外部の適切なネットワーク対策を施したインターフェイスに接続しようと決定することがあります。

図 7：ネットワーク インターフェイスの設定図



ファイアウォール ルールの提案

注：ポート 22 および 19791 のダーティ インターフェイス上で制限付きの発信ポリシーを実装すると、経時的な更新の追跡が必要となり、ファイアウォールの維持等により多くの時間がかかる可能性があります。以下の設定に関するセクションで、必要な送信先を参照してください。

注：ダーティ インターフェイスでの IPv4LL アドレス空間 (168.254.0.16) の使用はサポート対象として文書化されていませんでしたが、バージョン 2.3.0 以降これがエラーとして認識されるようになり、明示的にサポート対象外となりました。

ダーティ インターフェイスによる発信

送信元	送信先	プロトコル	ポート	操作	コメント
ダーティ インターフェイス	インターネット	ANY	ANY	許可 (Allow)	サンプルからの発信トラフィックを許可します。（正確な結果を取得するには、指定されたポートやプロトコルにかかわらず、マルウェアからコマンド アンド コントロール サーバへのアクセスが許可されている必要があります。）

ダーティ インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
ANY	ダーティ インターフェイス	ANY	ANY	拒否 (Deny)	すべての着信接続を拒否します。

クリーン インターフェイスによる発信

送信元	送信先	プロトコル	ポート	操作	コメント
クリーン インターフェイス	SMTP サーバ	TCP	25	許可 (Allow)	アプライアンスはクリーン インターフェイスを使用して、設定済みメール サーバへの SMTP 接続を開始します。

クリーン インターフェイスによる発信（任意）

以下は、設定されるサービスの内容に依存します。

送信元	送信先	プロトコル	ポート	操作	コメント
クリーン インターフェイス	企業の DNS サーバ	TCP/UDP	53	許可 (Allow)	任意。クリーン DNS が構成されている場合のみ必須
クリーン インターフェイス	AMP プライベート クラウド	TCP	443	許可 (Allow)	任意。AMP for Endpoints プライベート クラウド統合が使用されている場合のみ必須。
クリーン インターフェイス	Syslog サーバ	UDP	514	許可 (Allow)	Syslog メッセージおよび Threat Grid 通知を受信するように指定されたサーバへの接続を許可
クリーン インターフェイス	LDAP サーバ	TCP/UDP	389	許可 (Allow)	任意。LDAP が構成されている場合のみ必須
クリーン インターフェイス	LDAP サーバ	TCP	636	許可 (Allow)	任意。LDAP が構成されている場合のみ必須

クリーン インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
ユーザ サブネット	クリーン インターフェイス	TCP	22		tgsh-dialog への SSH 接続を許可します。
ユーザ サブネット	クリーン インターフェイス	TCP	80		アプライアンスの API と Threat Grid ユーザ インターフェイス。これは HTTPS TCP/443 にリダイレクトします。
ユーザ サブネット	クリーン インターフェイス	TCP	443		アプライアンスの API と Threat Grid ユーザ インターフェイス
ユーザ サブネット	クリーン インターフェイス	TCP	9443		Threat Grid UI Glovebox への接続を許可

管理インターフェイスによる発信（任意）

以下は、設定されるサービスの内容に依存します。

送信元	送信先	プロトコル	ポート	操作	コメント
管理インターフェイス	NFSv4 サーバ	TCP	2049	許可 (Allow)	任意。Threat Grid アプライアンスが NFSv4 共有にバックアップを送信するように設定されている場合のみ必須。

管理インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
管理サブネット	管理インターフェイス	TCP	22	許可 (Allow)	TGSH ダイアログへの SSH 接続を許可します。
管理サブネット	管理インターフェイス	TCP	80	許可 (Allow)	OpAdmin Portal インターフェイスへのアクセスを許可します。これは HTTPS TCP/443 にリダイレクトします。
管理サブネット	管理インターフェイス	TCP	443	許可 (Allow)	OpAdmin Portal インターフェイスにアクセスを許可します。

シスコ未検証/導入が推奨されるダーティ インターフェイス

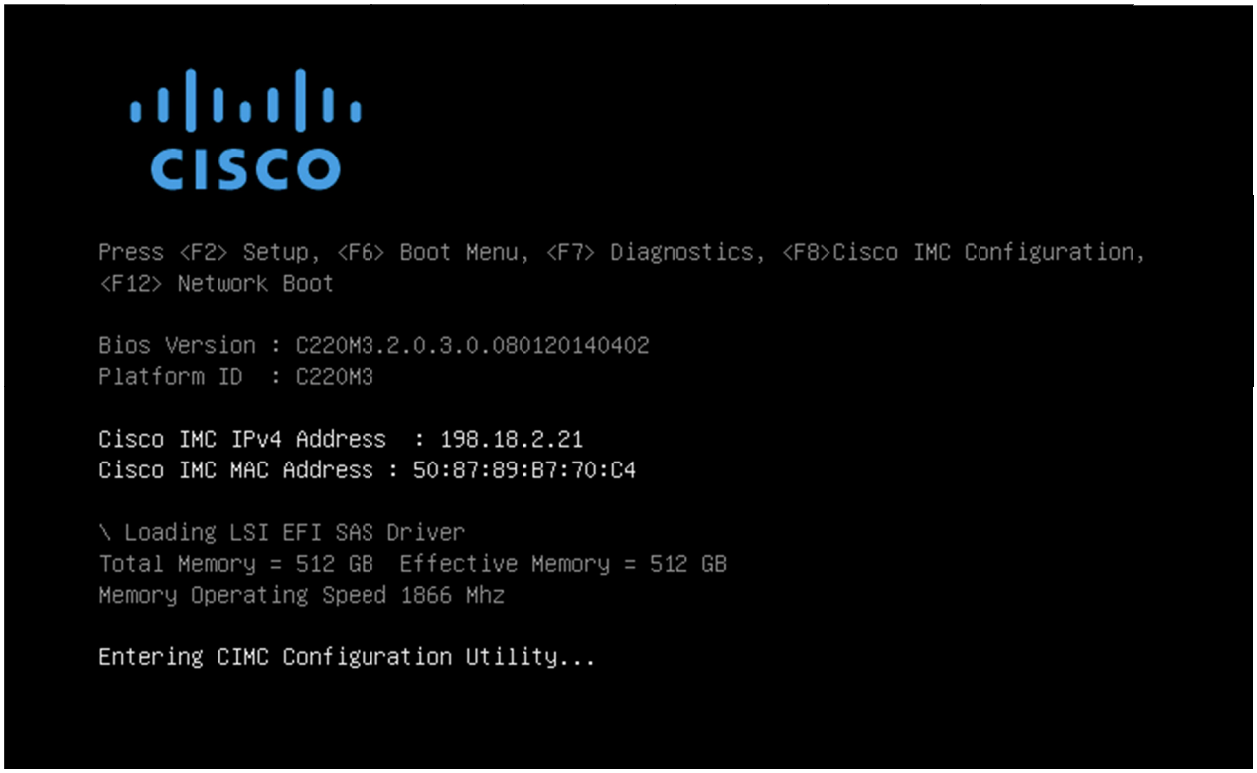
送信元	送信先	プロトコル	ポート	操作	コメント
ダーティ インターフェイス	インターネット	TCP	22	許可 (Allow)	スナップショット サービスとライセンス サービスを更新およびサポート
ダーティ インターフェイス	インターネット	TCP/UDP	53	許可 (Allow)	発信 DNS を許可
ダーティ インターフェイス	インターネット	UDP	123	許可 (Allow)	発信 NTP を許可

送信元	送信先	プロトコル	ポート	操作	コメント
ダーティ インターフェイス	インターネット	TCP	19791	許可 (Allow)	Threat Grid サポートへの接続を許可
ダーティ インターフェイス	Cisco Umbrella	TCP	443	許可 (Allow)	サードパーティの検出およびエンリッチメント サービスに接続
ダーティ インターフェイス	VirusTotal	TCP	443	許可 (Allow)	サードパーティの検出およびエンリッチメント サービスに接続
ダーティ インターフェイス	TitaniumCloud	TCP	443	許可 (Allow)	サードパーティの検出およびエンリッチメント サービスに接続

電源投入および起動

サーバ周辺機器とネットワーク インターフェイスを接続したら（電源ケーブルを接続してプラグインすることを忘れないでください）、アプライアンスの電源を入れ、起動するまで待機します。シスコの画面が一時的に表示されます。

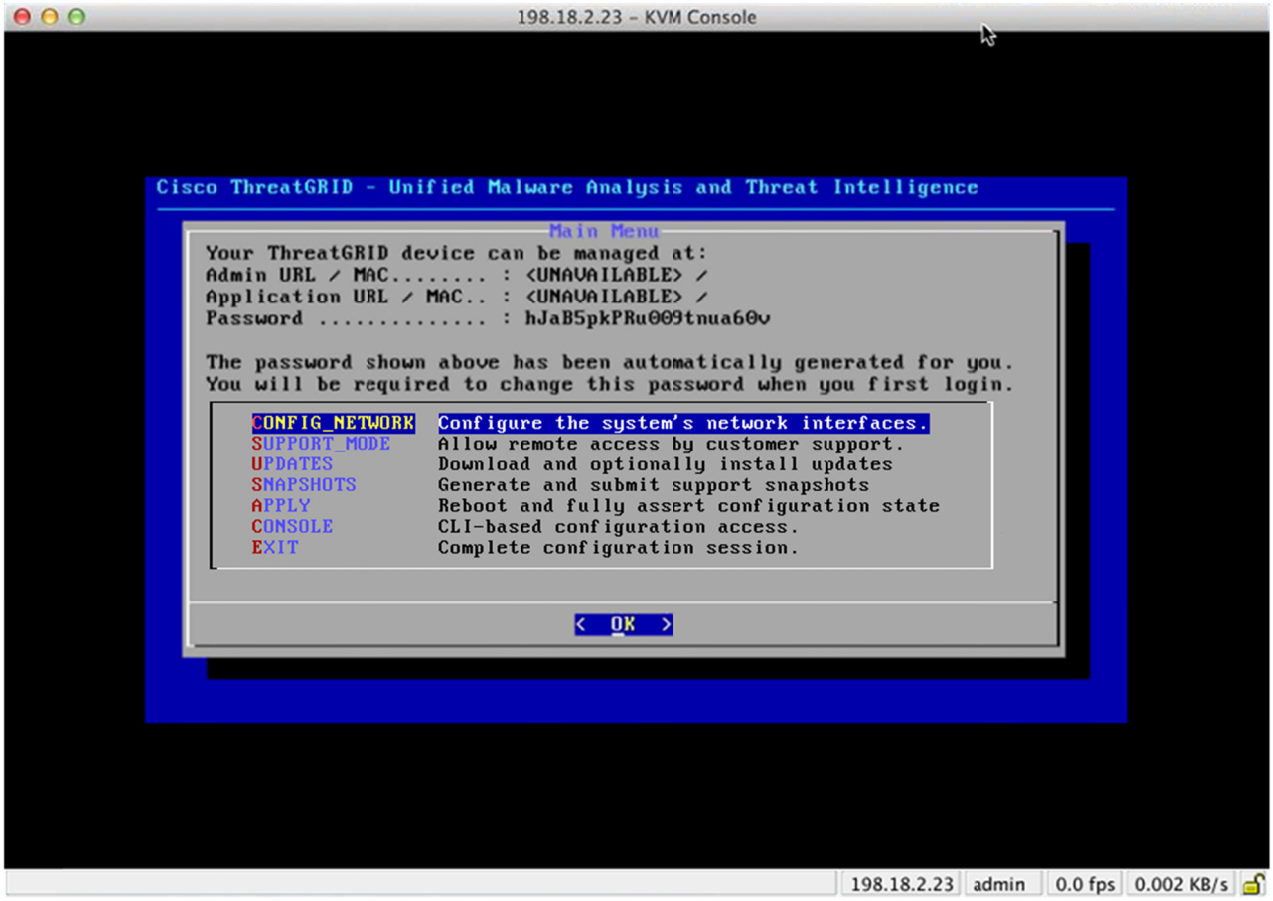
図 8：起動時のシスコ画面



注：このインターフェイスを構成する場合、メモリ チェックの完了後、**F8** を押し、付録 A 「CIMC の構成」の手順に従います。

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 9：TGSH ダイアログ



Admin URL に利用不可として示されている：ネットワーク インターフェイスの接続がまだ構成されておらず、このタスクを実行するために OpAdmin Portal はまだ到達できません。

注：OpAdmin Portal 構成手順で、便利なように管理者パスワードを別のテキスト ファイルにメモ（コピーして貼り付け）しておきます。

重要：TGSH ダイアログは、初期管理者パスワードを表示します。このパスワードは、構成ワークフロー手順で後から OpAdmin Portal インターフェイスにアクセスし、インターフェイスを構成するために必要です。

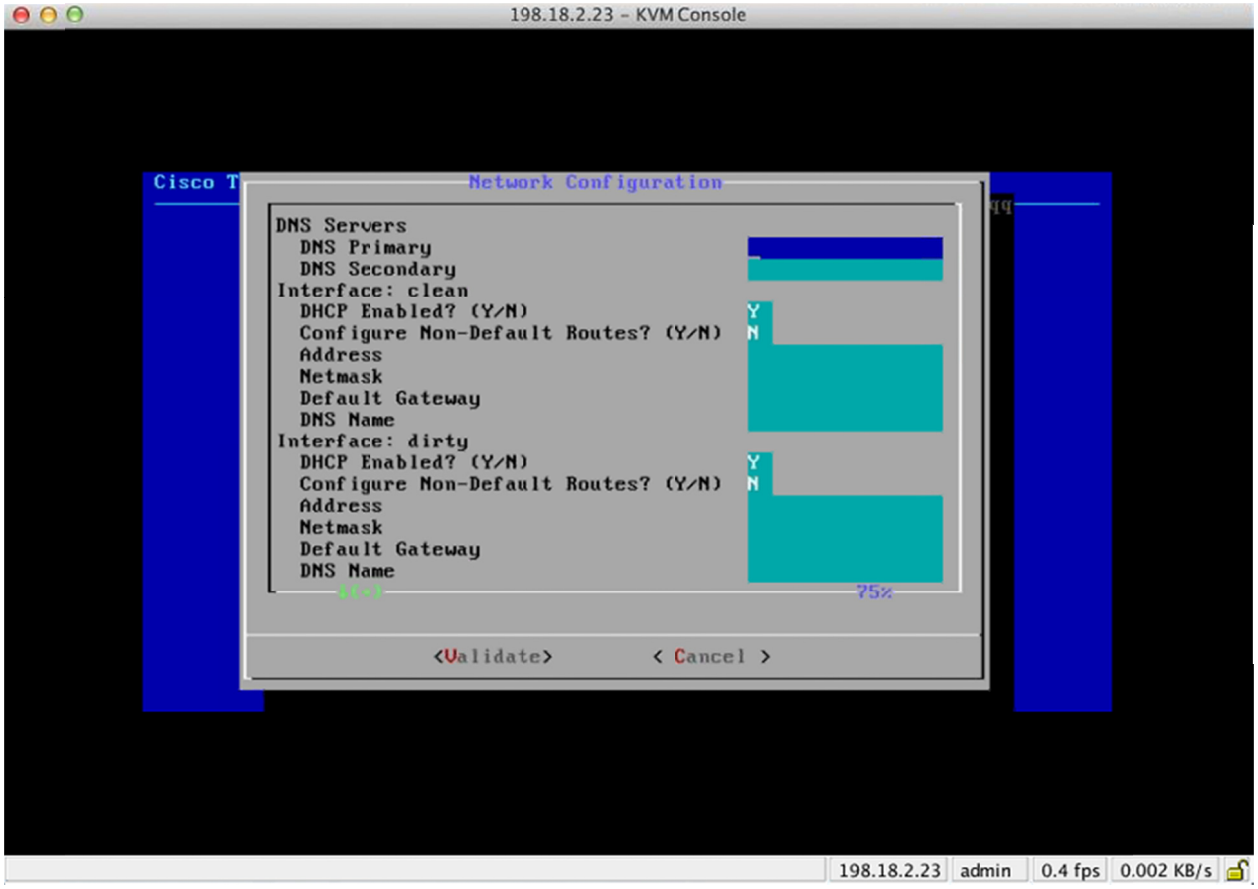
初期ネットワーク構成 – TGSH ダイアログ

初期ネットワーク構成は、TGSH ダイアログで完了します。目的は、OpAdmin インターフェイス ツールへのアクセスを許可する基本的構成を完了し、残りの構成（ライセンス、電子メール ホスト、SSL 証明書）を完了できるようにすることです。

DHCP ユーザ：次の手順は、静的 IP アドレスを使用していることを想定しています。DHCP を使用して IP を取得している場合、詳細については、『*Threat Grid Appliance Administrator's Guide*』を参照してください。

1. TGSH ダイアログのインターフェイスで、[CONFIG_NETWORK] を選択します。[ネットワーク構成 (Network Configuration)] コンソールが開きます。

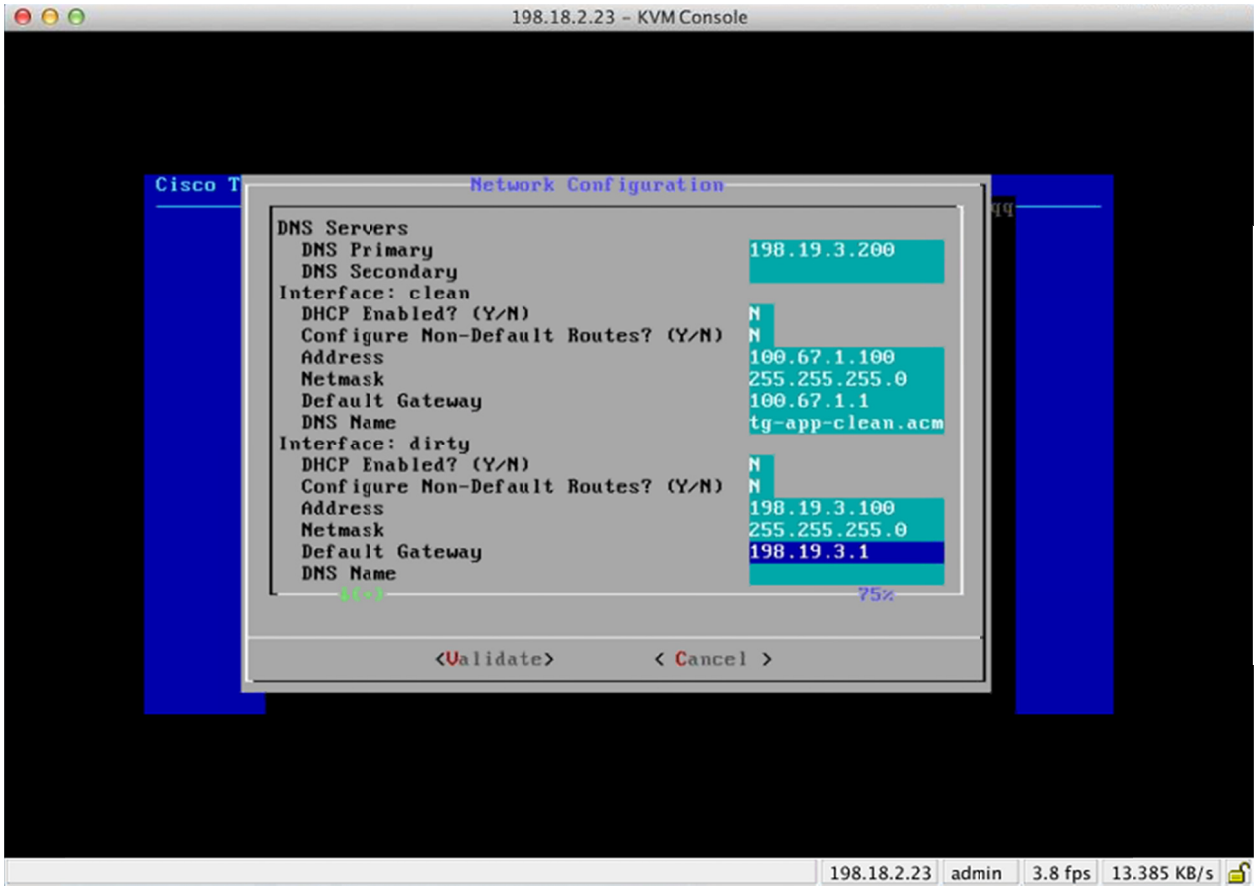
図 10：TGSH ダイアログ：[ネットワーク構成 (Network Configuration)] コンソール



2. クリーン、ダーティ、および管理の各インターフェイスに対して、ネットワーク管理者から提供される設定に従い、空白のフィールドに入力します。
3. [DHCP Enabled] を [Y] から [N] に変更します。

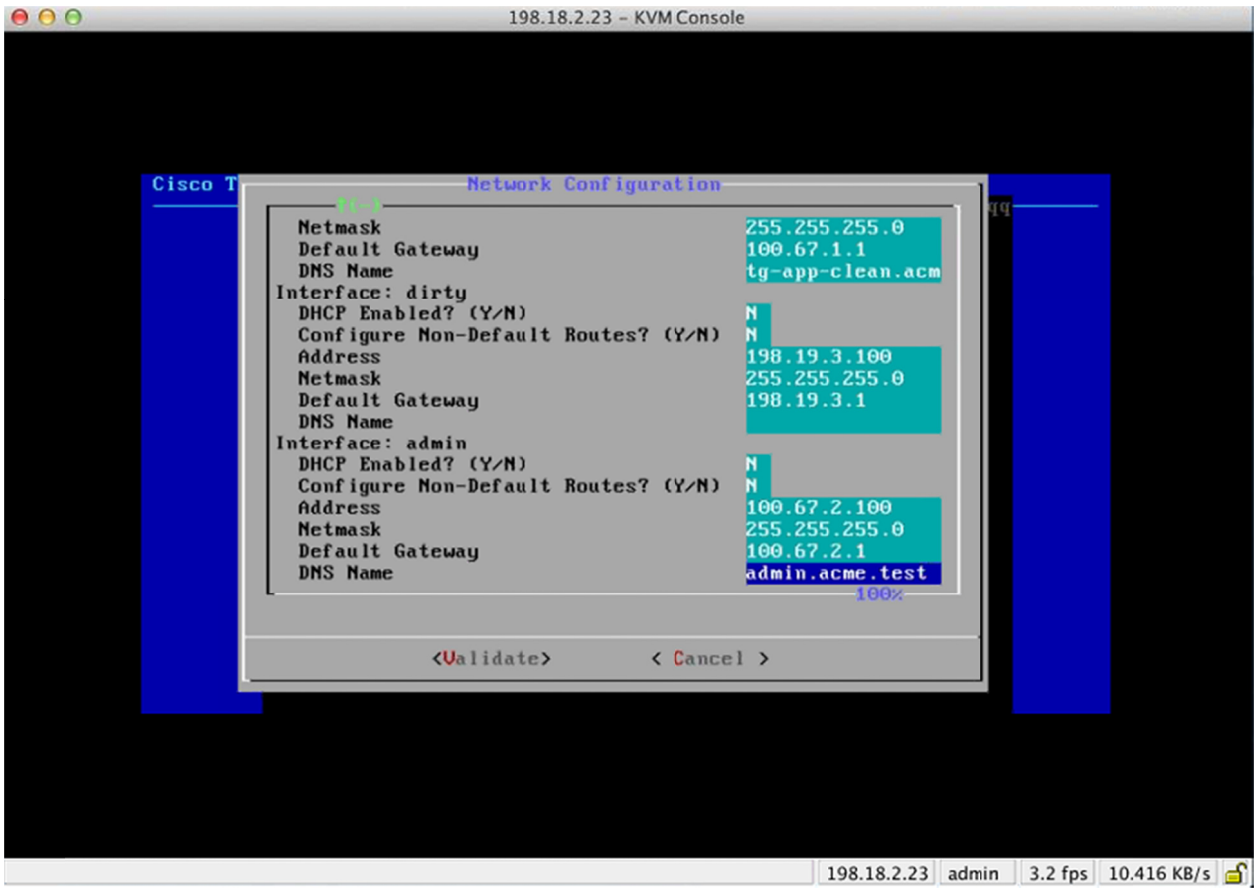
   注：新しい文字を入力する前に**バックスペース**を押して古い文字を削除する必要があります。
4. **DNS 名。**ネットワークがクリーン ネットワークに DNS 名を使用する場合は、ここに名前を入力します。
5. [Configure Non-Default Routes?] をデフォルトの [N] のままにします（追加のルートが必要ない場合）。

図 11：進行中のネットワーク設定（クリーンおよびダーティ）



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

図 12：進行中のネットワーク設定 (管理)

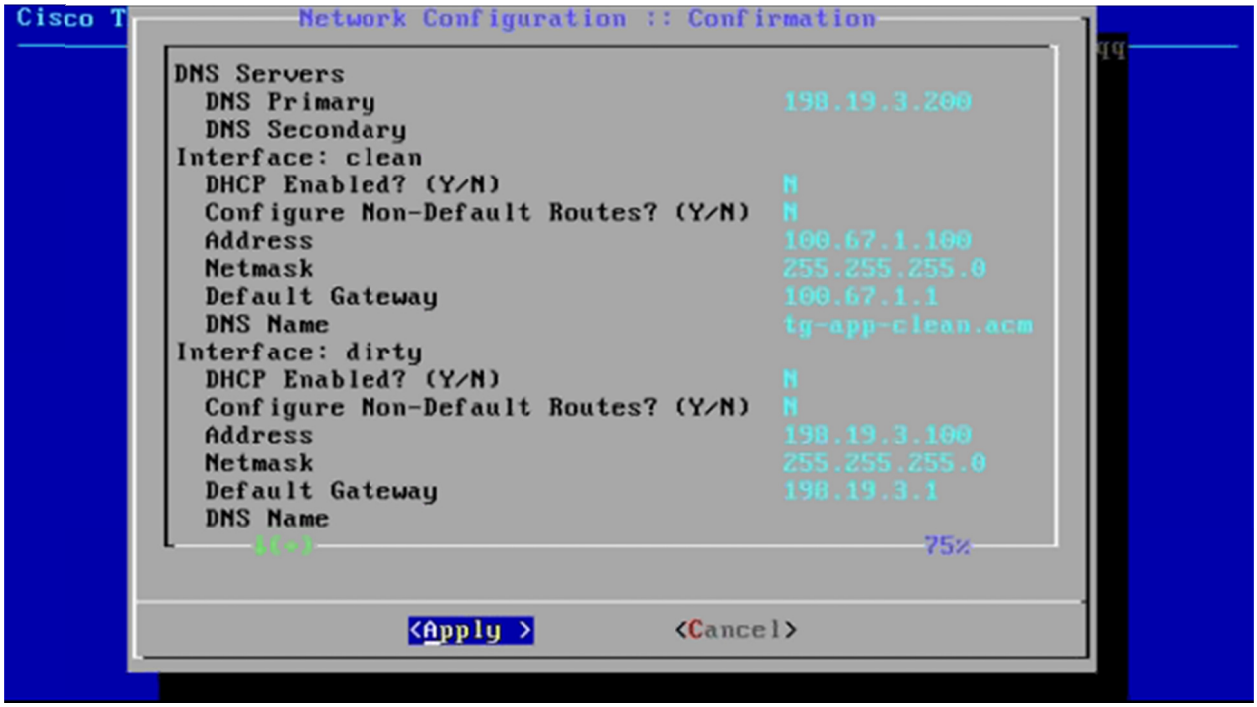


7. すべてのネットワーク設定を入力したら、タブ キーで下に移動し、[Validate] を選択して入力内容を検証します。

   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、[ネットワーク設定の確認 (Network Configuration Confirmation)] に入力した値が表示されます。

図 13：ネットワーク設定の確認

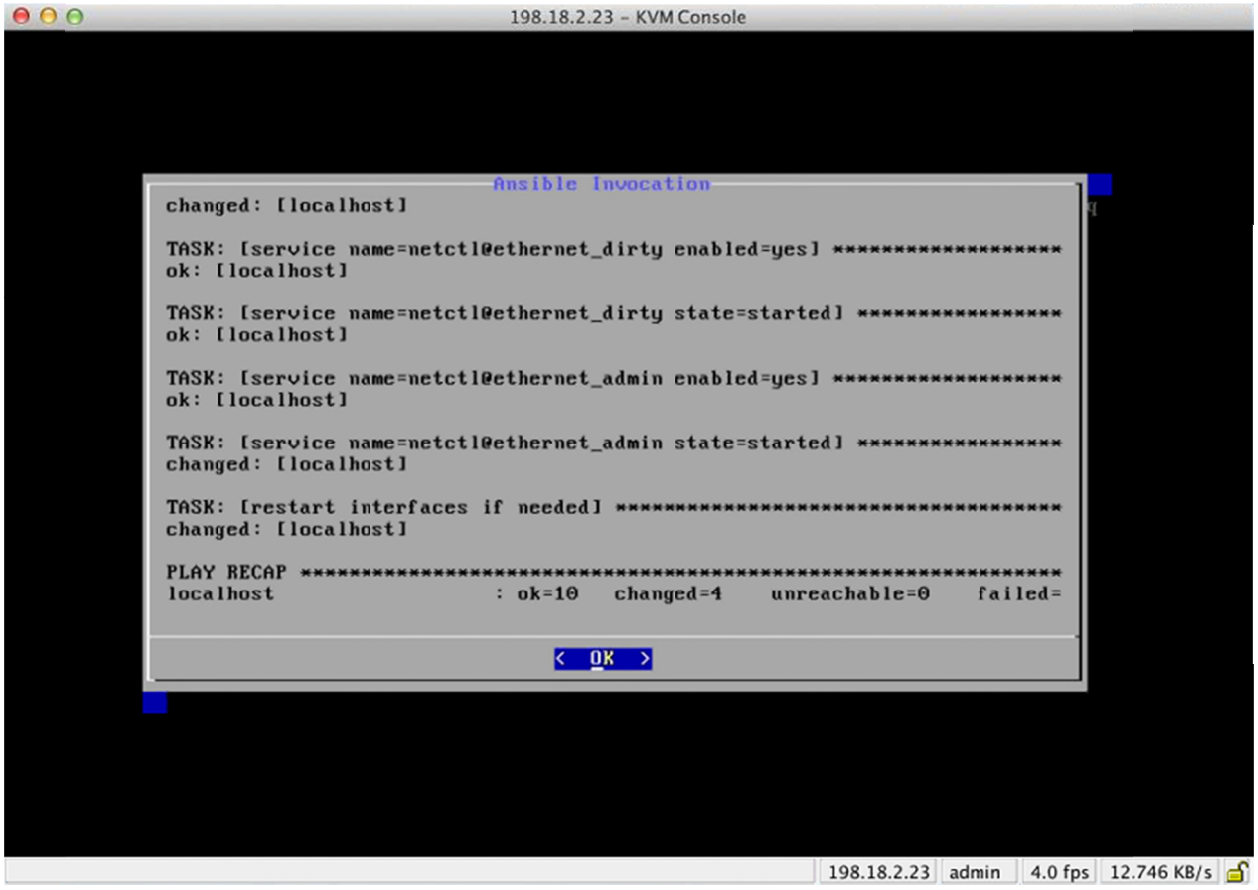


8. [適用 (Apply)] を選択して各種設定を適用します。

   しばらくお待ちください。この手順は、完了するまでに 10 分以上かかる場合があります。

   コンソールが空白のグレーのボックスになります。また、スクリーンには、設定の適用時にスクロール構成情報が表示される場合があり、加えられた構成変更についての詳細情報が一覧表示されます。

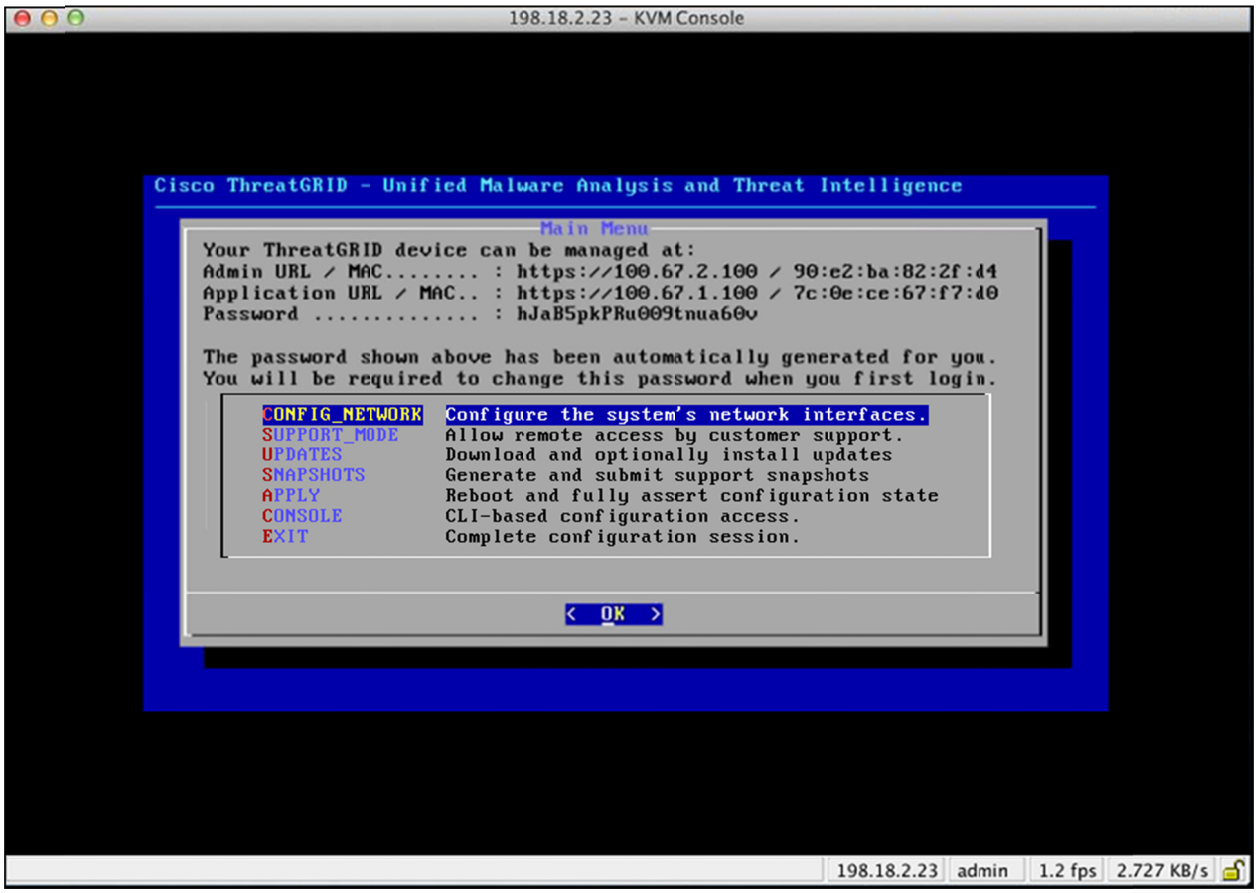
図 14：ネットワーク設定：実行した変更のリスト



9. [OK] を選択します。

   [ネットワーク設定 (Network Configuration)] コンソールが更新され、入力した IP アドレスが表示されます。

図 15：IP アドレス



アプライアンスのネットワーク構成は完了しています。

注：クリーン インターフェイスの URL は OpAdmin Portal の設定が完了するまで機能しません。

設定の次のステップ：

アプライアンス設定の次の手順は、次のセクションに説明されているとおり、OpAdmin Portal のワークフローを使用した残りの構成タスクを完了することです。

設定ウィザード：OPADMIN PORTAL

OpAdmin Portal は、アプライアンス上の Threat Grid 管理者のポータルです。管理インターフェイスで IP アドレスを設定した後で使用できる Web ユーザ インターフェイスです。

OpAdmin Portal は、アプライアンスを構成するための推奨ツールです。実際に、アプライアンス構成の大部分は OpAdmin ポータル インターフェイスからしか実行することができません。この構成には、次のものが含まれます。

- OpAdmin Portal 管理者のパスワード
- 電子メール サーバ
- DNS サーバ
- NTP サーバ
- SSL 証明書
- クラスタリング
- その他のサーバ設定
- https://<adminIP>/ または https://<adminHostname>/

注：これらの設定のすべてが初期の OpAdmin Portal 構成ウィザードのワークフローで完了するわけではありません。SSL 証明書やクラスタリングなどの一部は、Cisco.com の Threat Grid アプライアンスのマニュアル ページにある『*Threat Grid Appliance Administrator's Guide*』で説明されているとおり、異なる手順で構成されます。

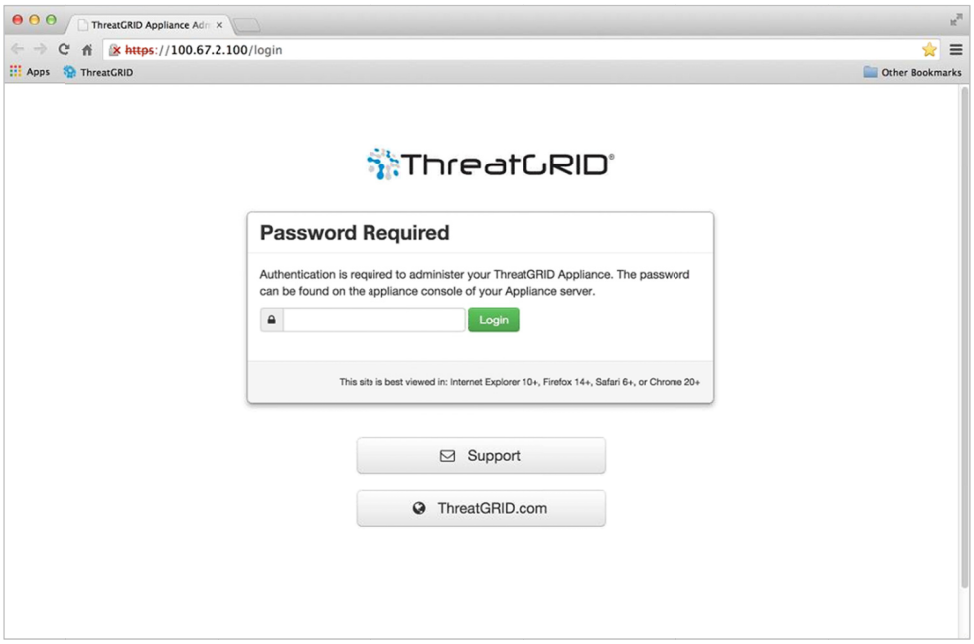
構成ワークフロー

以降のセクションの手順は、設定時の IP アドレスに割り込みが入る可能性を減らすために、1 回のセッションで完了する必要があります。

OpAdmin Portal へのログイン

1. ブラウザで OpAdmin Portal インターフェイス（「https」付きの管理 URL）を指定します。Threat Grid OpAdmin のログイン画面が開きます。

図 16：OpAdmin のログイン



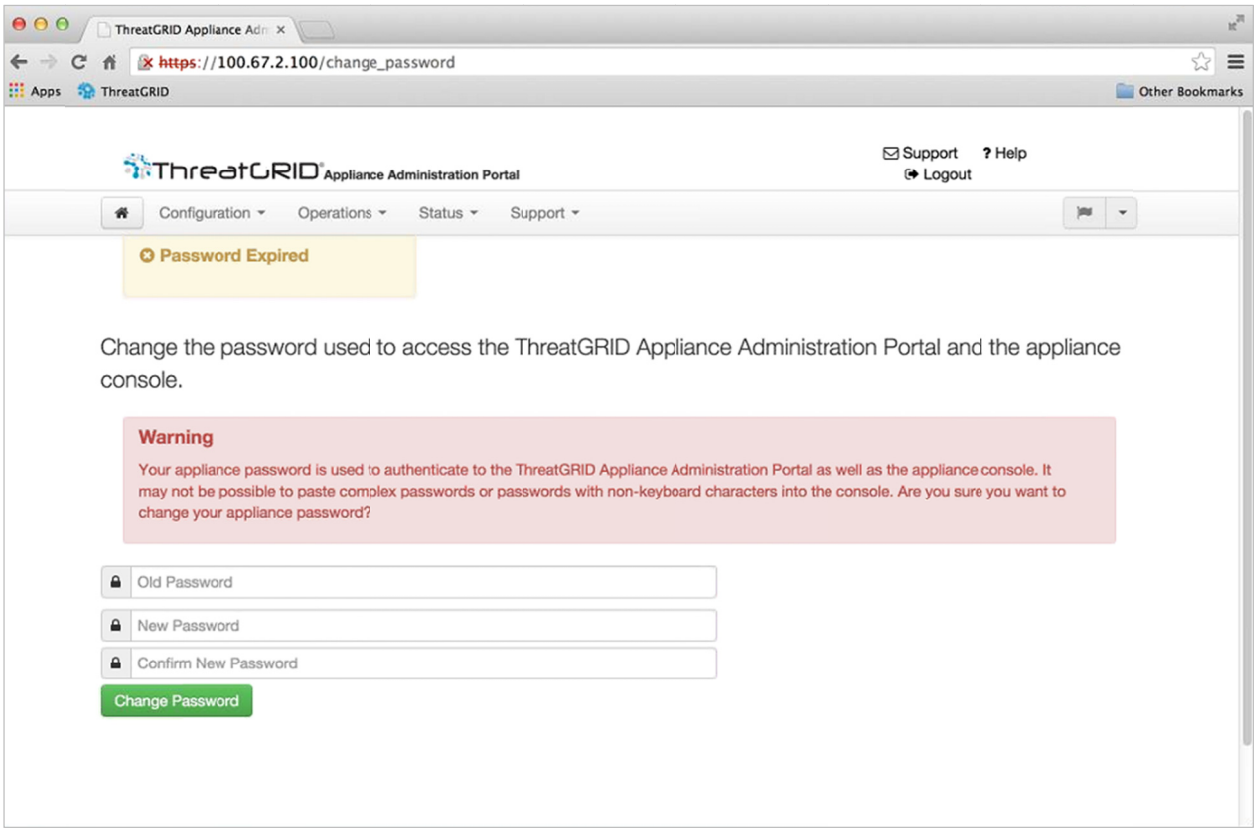
2. TGSH ダイアログからコピーした初期設定の管理者パスワードを入力して、[ログイン (Login)] をクリックします。[Change Password] ページが表示されます。

次のセクションに進みます。

管理者パスワードの変更

初期管理者パスワードは、出荷前の Threat Grid インストール中にランダムに生成されており、TGSH ダイアログでプレーン テキストとして表示できます。設定ワークフローで先に進む前に、初期管理者パスワードを変更する必要があります。

図 17：OpAdmin のパスワード変更



1. TGSH ダイアログのパスワードを [Old Password] フィールドに入力します（このパスワードは後で使用するために、テキスト ファイルに入力しておきます）。
2. 新しいパスワードを入力して確定します。
3. [パスワードの変更 (Change Password)] をクリックします。

   パスワードが更新されます。[エンドユーザライセンス契約書 (End User License Agreement)] ページが表示されます。

注：新しいパスワードは TGSH ダイアログにテキストで表示されないため、必ずどこかにメモしておいてください。

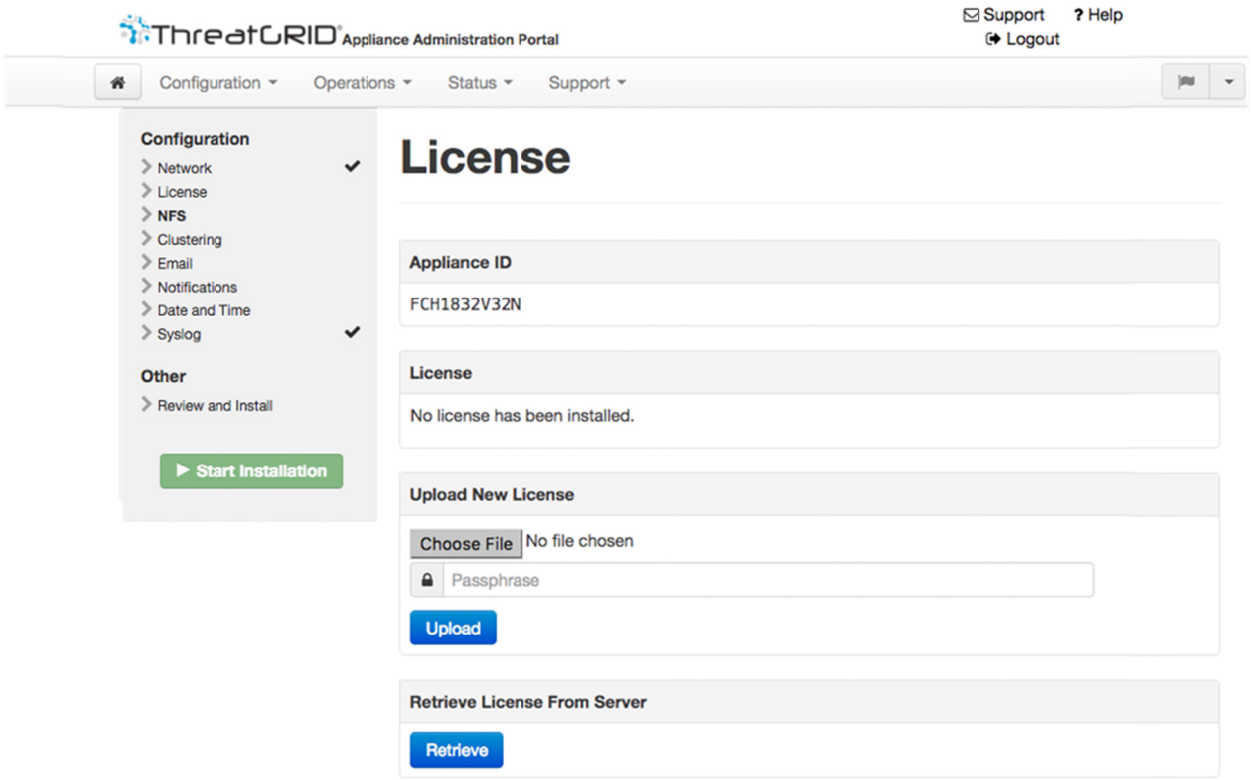
パスワードを紛失した場合、『*Threat Grid Appliance Administrator's Guide*』の「*Support*」セクションに記載されている「**Lost Password**」の手順に従います。

次のセクションに進みます。

エンド ユーザ ライセンス契約書

1. エンド ユーザ ライセンス契約書を確認します。
2. 最後までスクロールし、[I HAVE READ AND AGREE] をクリックします。[ライセンス (License)] ページが開きます。

図 18：[ライセンス (License)] ページ



構成ワークフローに従い、*ライセンスをインストールする前にネットワークを構成する*ことをお勧めします。これについては、次のセクション「ネットワーク構成の設定」で説明しています。

ネットワーク構成の設定

TGSH ダイアログでスタティック ネットワーク設定を行った場合、[Network Configuration] ページに表示される IP アドレスは、アプライアンスのネットワーク設定時に TGSH ダイアログに入力した値を反映します。

ネットワーク構成と DHCP

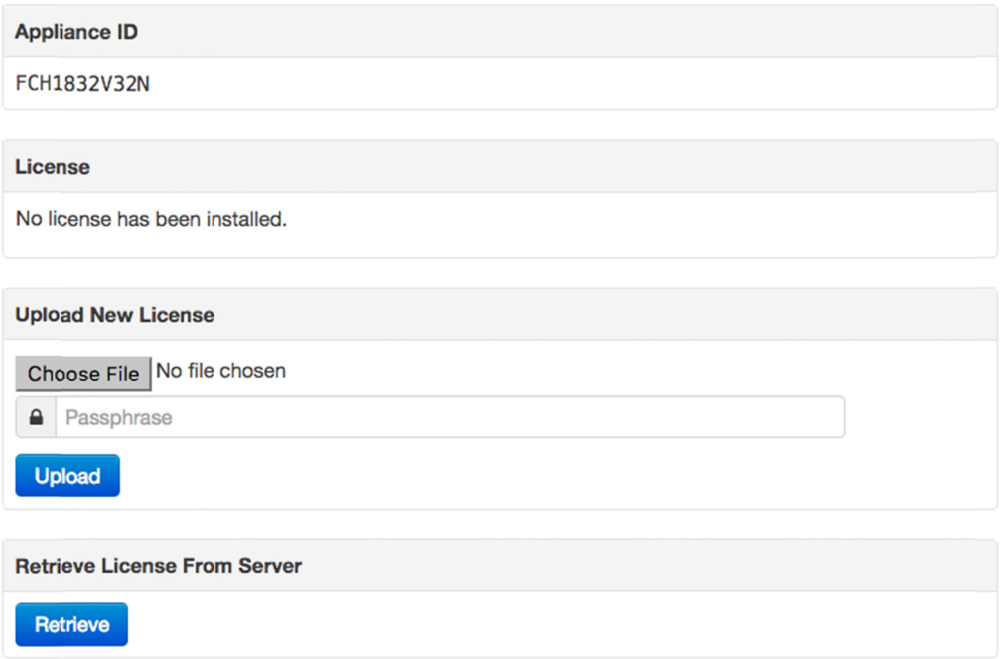
最初の接続に DHCP を使用し、クリーンおよびダーティ IP ネットワークを静的 IP アドレスに変更する必要がある場合、『*Threat Grid Appliance Administrator's Guide*』に記載されている「***Networking > Using DHCP***」セクションの手順に従います。

次のセクションに進みます。

ライセンスのインストール

ネットワークを構成したら、Threat Grid ライセンスをインストールすることができます。（v1.4.4 よりも古いバージョンでは、ライセンスが受け入れられるようにサポート モードを開始する必要があります。詳細については、サポート モードの開始：バージョン 1.4.4 より前のライセンスの回避策を参照してください）。

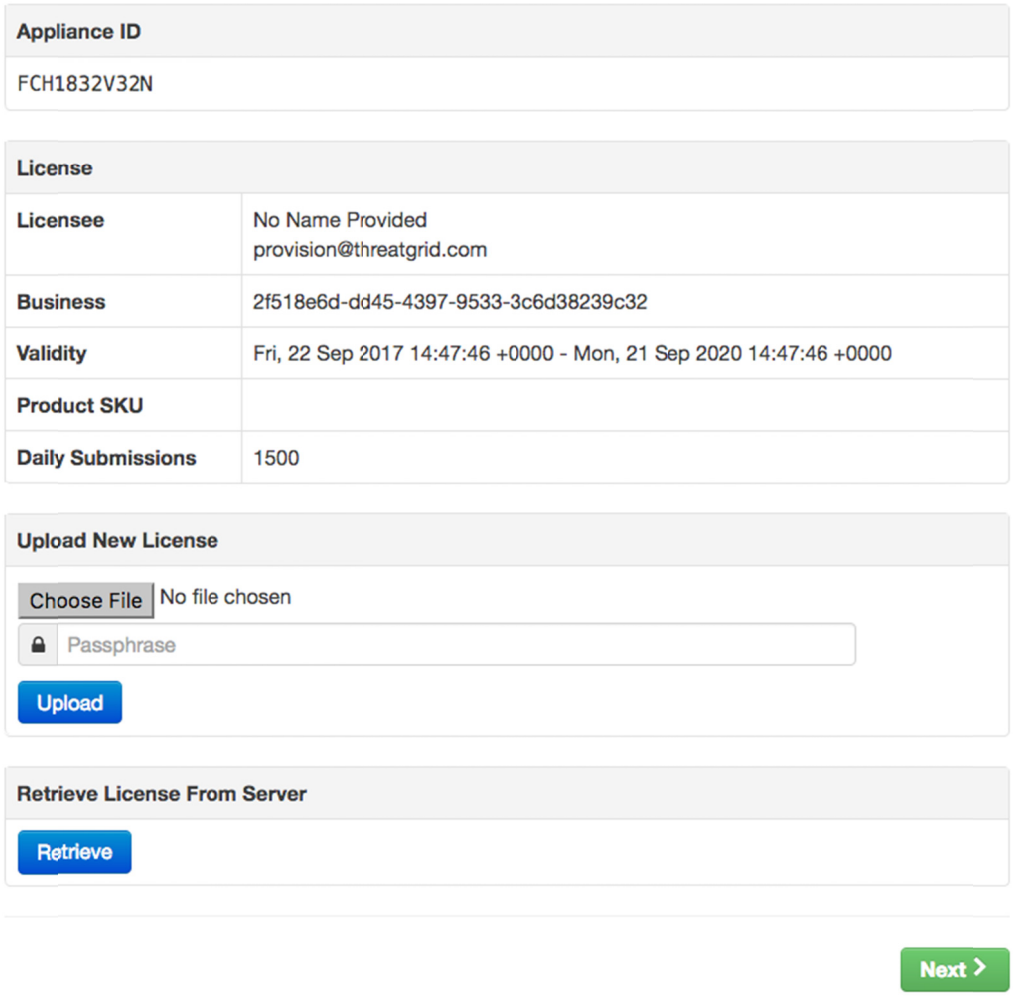
図 19：インストール前のライセンス ページ



1. 左のカラムで、[License] をクリックします。上記で示すように [ライセンス (License)] ページが開きます。ライセンスがインストールされていません。
2. [新規ライセンスのアップロード (Uploadl New License)] の下の [ファイルを選択 (Choose File)] をクリックし、ファイル マネージャからライセンスを選択します。

   サーバからライセンスを取得 - または、2.3 リリースを機能に追加して、[取得 (Retrieve)] を選択します。アプライアンスをインストールするときにネットワーク アクセスが含まれる場合は、このオプションを選択するとライセンスがネットワーク経由で取得されます。
3. 支給されたライセンス パスワードを [パスフレーズ (Passphrase)] フィールドに入力します。
4. [Upload] をクリックしてインストールします。ページが更新され、ライセンス情報を確認できます。

図 20：インストール正常終了後のライセンス情報



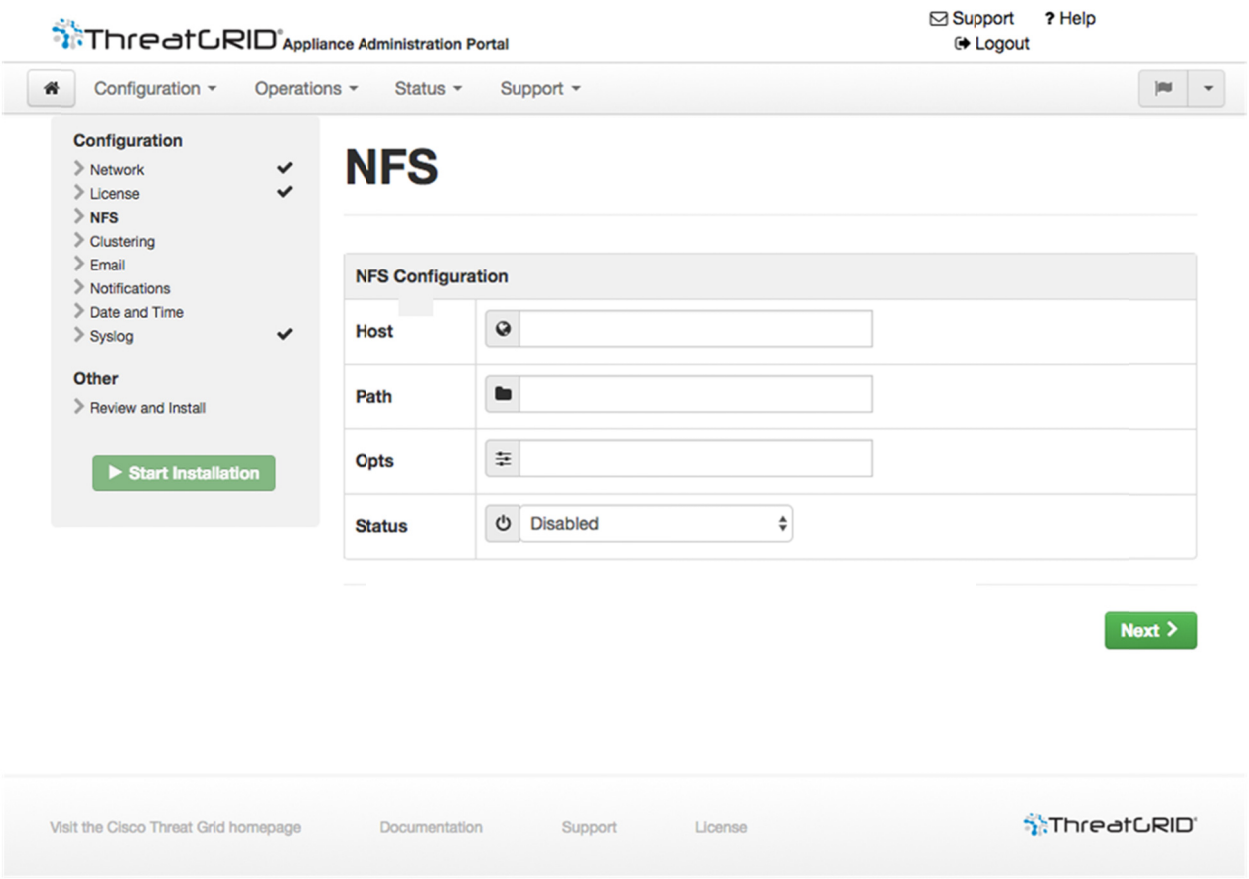
[次へ (Next)] をクリックして続行します。[電子メール (Email)] ページが開きます。

次のセクションに進みます。

NFS の設定

ワークフローの次の手順は、NFS を設定することです。このタスクでは、バックアップとクラスタリングが必要です。（詳細については、バックアップ時に『*Threat Grid Appliance Guide*』セクションの「NFS Requirements」を参照してください。）

図 21：NFS の設定



1. 左の列で、[NFS] をクリックします。[NFS] ページが開きます。
2. 次のようにページを設定します。

   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：ファイルを保存する NFS ホスト サーバ上にある絶対パス

オプション：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：ドロップダウンから [イネーブル化 (Enabled)]（保留中のキー）を選択します。

3. [次へ (Next)] をクリックします。ページが **FS 暗号化パスワード キー ID** を使用して更新できるようになりました。

   このページを最初に設定するときに、暗号化キーを**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、Key ID が OpAdmin に表示されます。すでに説明したように、暗号化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。

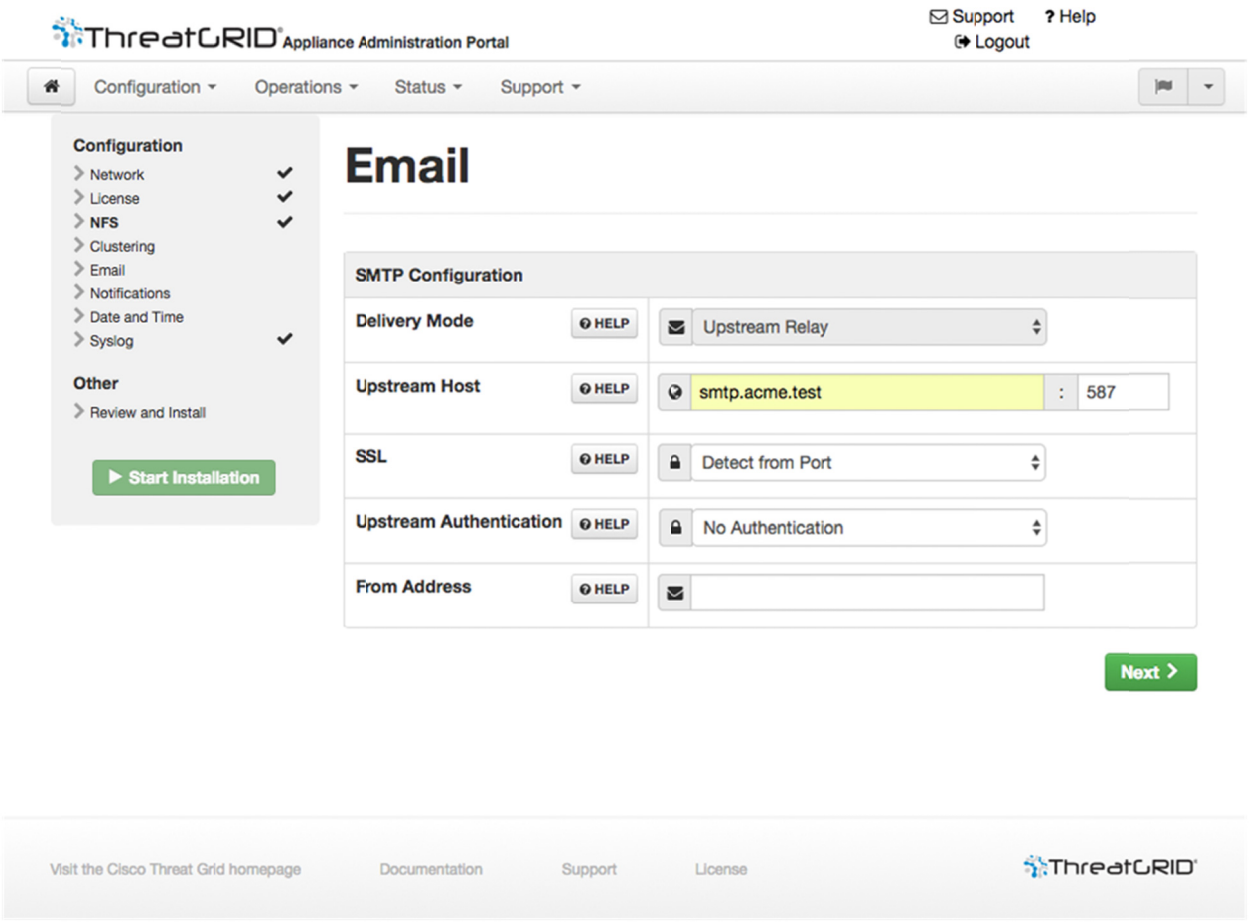
4. [次へ (Next)] をクリックします。[電子メール (Email)] ページが開きます。

次のセクションに進みます。

電子メール ホストの設定

ワークフローの次の手順は、電子メール ホストを設定することです。

図 22：電子メール ホストの設定



1. 左のカラムで、[Email] をクリックします。[Email] ページが開きます。
2. [Upstream Host]（電子メール ホスト）の名前を入力します。
3. ポートを 587 から **25** に変更します。
4. 他の設定はデフォルトのままにしておきます。
5. [Next] をクリックします。[通知 (Notifications)] ページが開きます。

次のセクションに進みます。

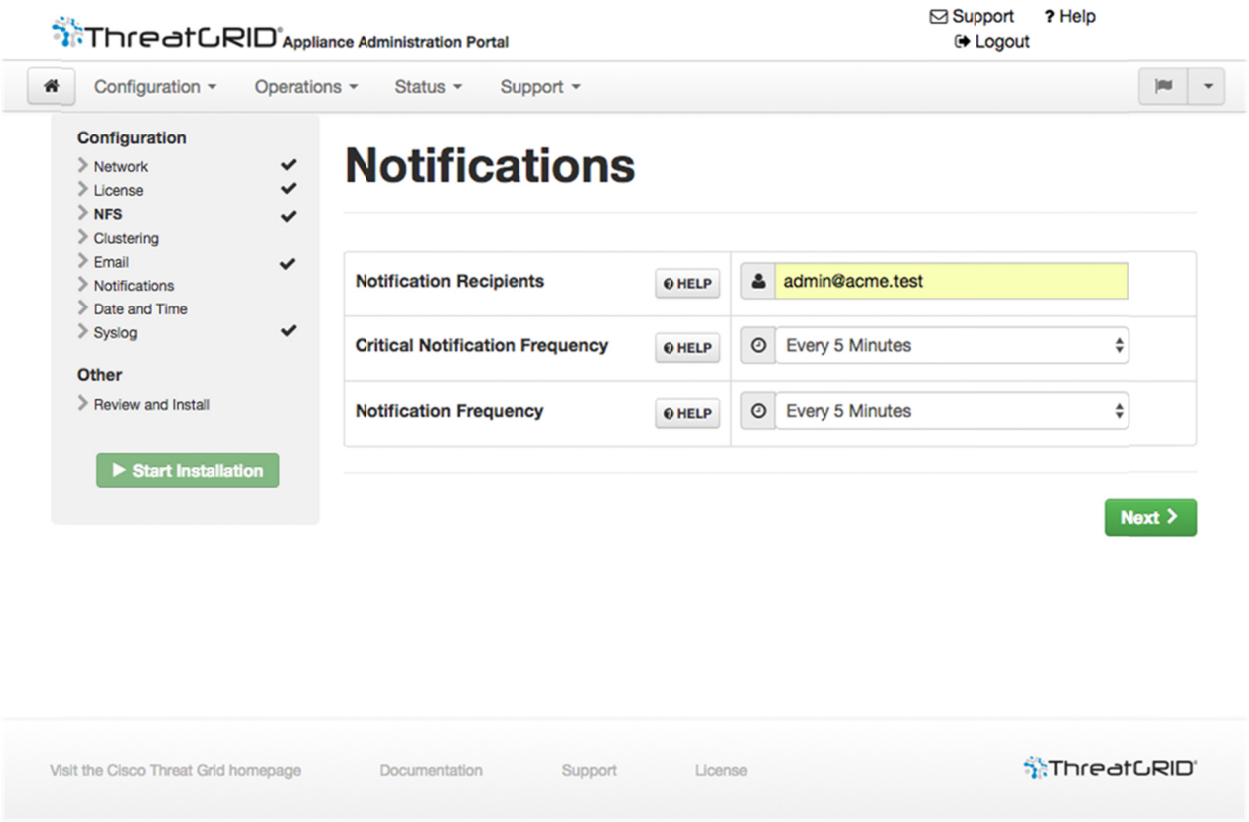
サーバ通知の設定

ワーク フローの次の手順は、1 つ以上の電子メール アドレスに定期的に配信可能な通知を設定することです。システム通知は Threat Grid インターフェイスに表示されますが、このページでは、電子メールで送信される通知も設定できます。

Syslog 設定

更新 v1.3 には、Syslog サーバが Syslog メッセージおよび Thread Grid 通知を受信するために設定するページが含まれています。詳細については、『*Threat Grid Appliance Admin Guide*』を参照してください。

図 23：通知の設定



1. 最初に、ドロップダウン リストから [Critical Notification Frequency] と [Notification Frequency] を設定します。
2. 次に、[Notification Recipients] で、カンマで区切った 1 つ以上の電子メール アドレスを入力します。
3. [次へ (Next)] をクリックします。[日付と時刻 (Date and Time)] ページが開きます。

次のセクションに進みます。

NTP サーバの設定

ここでは、NTP（「Network Time Protocol」）サーバを識別します。

1. [NTP Server] に IP または NTP 名を入力します。

複数の NTP サーバがある場合は、スペースまたはカンマで区切ります。

2. [Current System Time] と [Synchronize with Browser] は無視します。
3. [Next] をクリックします。

   [レビューおよびインストール (Review and Install)] ページが開き、設定手順すべての隣にチェックボックスが表示されます。

次のセクションに進みます。

構成設定の確認およびインストール

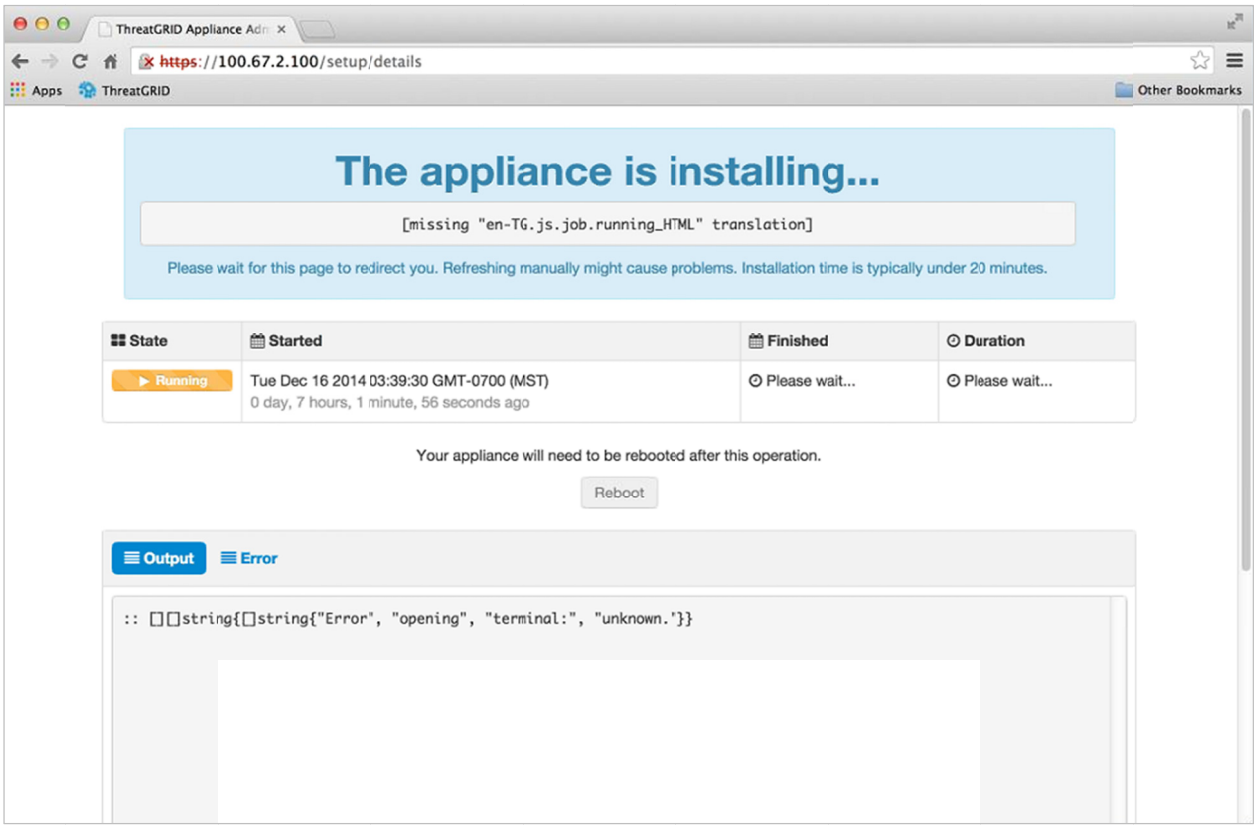
ネットワークの各種設定を入力したので、それらを次の手順でインストールする必要があります。

1. [Review and Install] ページで、[Start Installation] をクリックします。

   構成スクリプトがインストールされ、次のように、「アプライアンスがインストール中です... (The appliance is installing...)」というメッセージが表示されます。

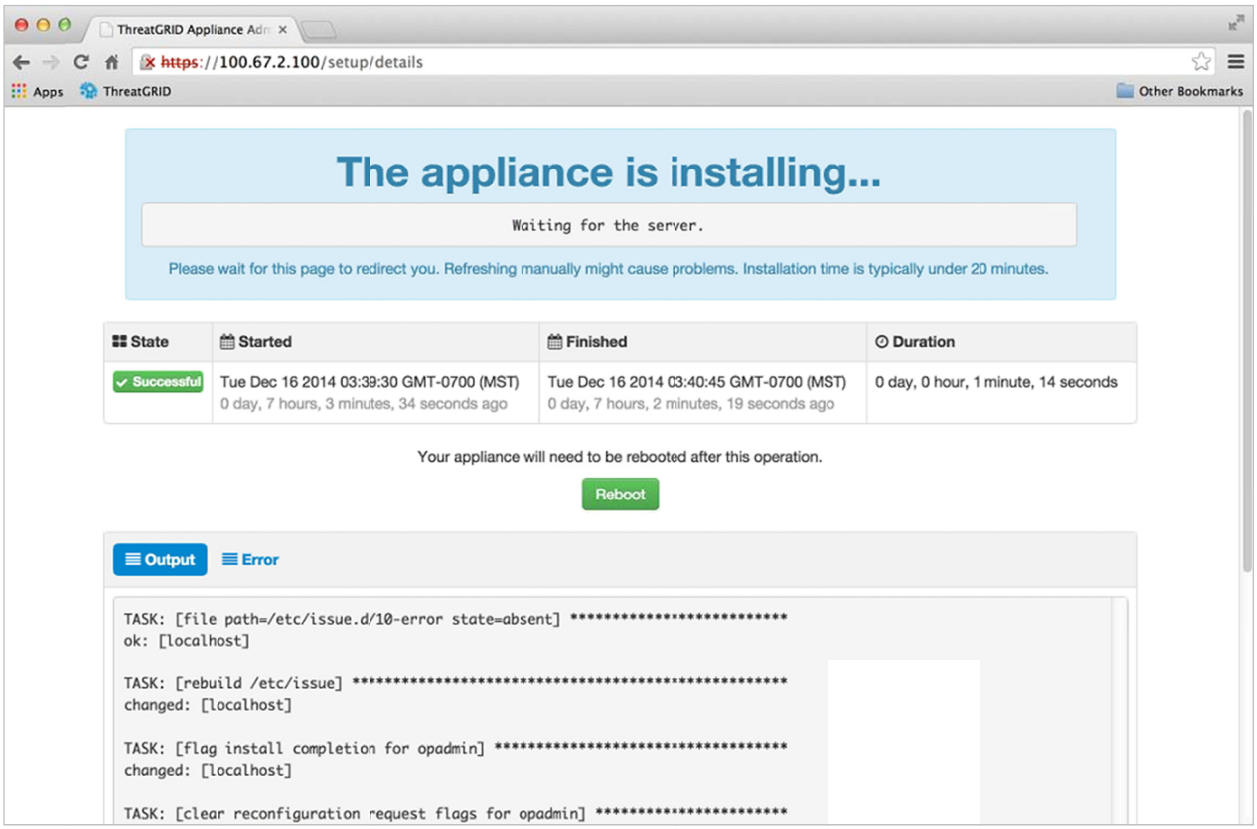
注：しばらく待機します。この手順を完了するまで、10 分以上かかります。画面の適用に応じて、設定情報が表示されます。

図 24：アプライアンスはインストール中



2. インストールが正常終了すると、[状態 (State)] はオレンジ色の [実行中 (Running)] から緑色の [成功 (Successful)] メッセージに変化し、正常終了を示します。[Reboot] ボタンは緑色に変化し、設定出力が表示されます。

図 25：正常終了したアプライアンス インストール

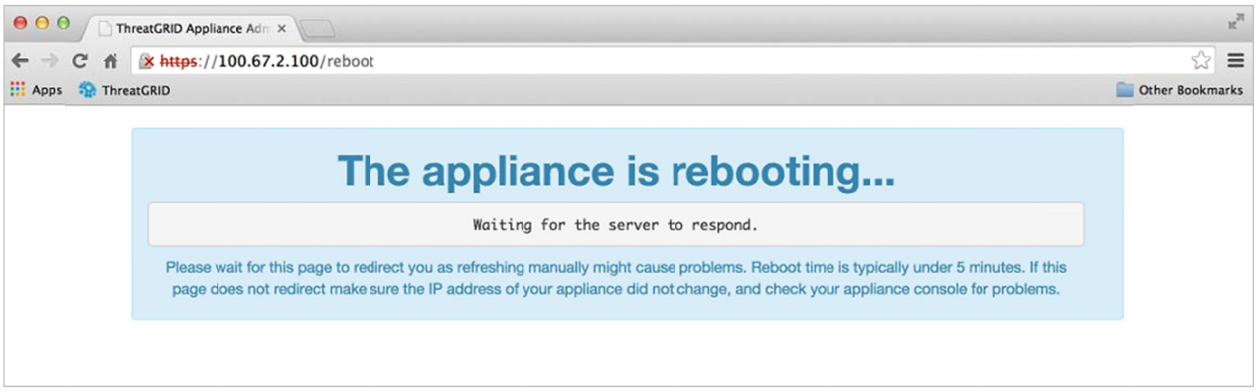


3. インストールが正常に終了した後、[リブート (Reboot)] をクリックします。「*The appliance is rebooting*」というメッセージが表示されます。

   リブートには最大で 5 分程度かかる場合があります。

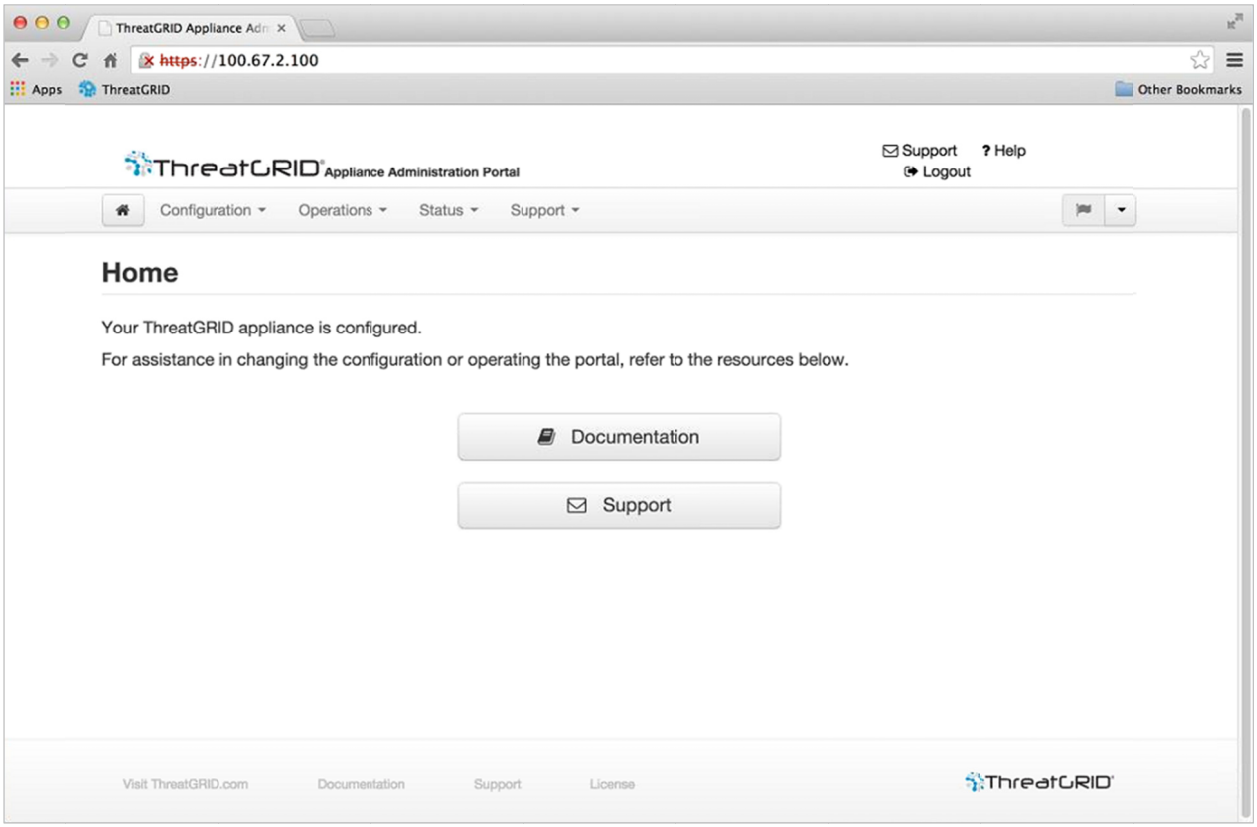
アプライアンスのリブート中に変更を加えないでください。

図 26：アプライアンスはリブート中



アプライアンスが正常にリブートした場合、アプライアンスが設定されていることを示す次のメッセージが表示されます。

図 27：アプライアンスは設定済み



これでアプライアンスは設定され、初期設定が完了しました。

THREAT GRID アプライアンスの更新のインストール

最初の Threat Grid アプライアンスの設定後は、続行前に、利用可能な商品をインストールすることをお勧めします。

Threat Grid アプライアンスの更新は、[OpAdmin Portal] を使用して実行されます。

[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。

[Check/Download Updates] をクリックします。ソフトウェアにより、Threat Grid アプライアンス ソフトウェアの最新の更新/バージョンがないかが確認され、ある場合にはそれがダウンロードされます。これには少し時間がかかる場合があります。

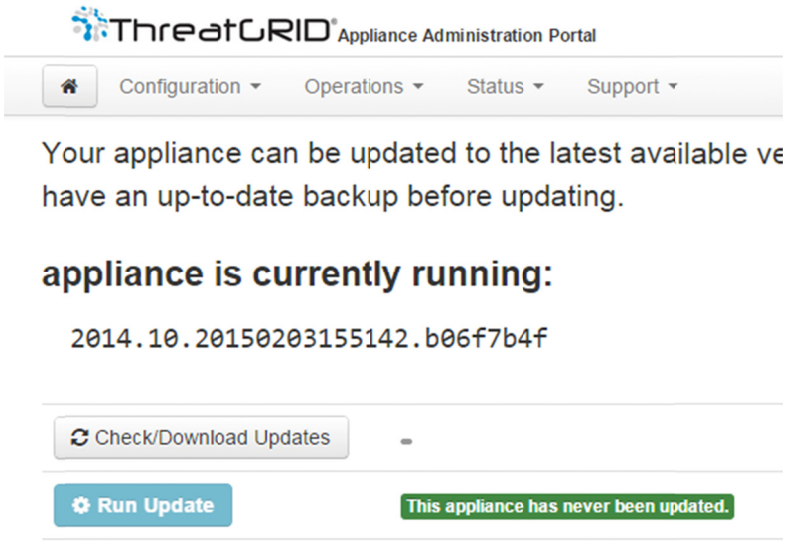
更新のダウンロードが完了したら、[Run Update] をクリックしてインストールします。

更新のインストールの詳細については、『*Threat Grid Appliance Administrator's Guide*』を参照してください。

アプライアンスのビルド番号

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

図 28：アプライアンスのビルド番号



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 年 6 月 1 日	クラスタの初期化を修正、古い ES/PG 移行のサポートをプルーニング
2017.12.20180519011227.ed8a11e9.rel	2.4.3.2	2018 年 5 月 19 日	CVE-2018-1000085 の ClamAV を更新バグ修正
2017.12.20180501005218.4e3746f4.rel	2.4.3.1	2018 年 5 月 1 日	PG スキーマで更新確認時の DDL エラー検出を報告
2017.12.20180427231427.e616a2f2.rel	2.4.3	2018 年 4 月 27 日	Remote Virtual Exit Localization、スタンドアロンからクラスタへの直接移行
2017.12.20180302174440.097e2883.rel	2.4.2	2018 年 3 月 2 日	クラスタリング
2017.12.20180219033153.bb5e549b.rel	2.4.1	2018 年 2 月 19 日	OpAdmen でのクラスタリングのサポート。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 年 1 月 30 日	セキュリティ更新プログラムを ClamAV にのみ更新

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 年 12 月 14 日	クラスタリング EFT。jp/kr contsubs。ポータルを 3.4.57 に更新。
2016.05.2017113002233355.1c7bd023.rel	2.3.3	2017 年 11 月 30 日	2.4 アップグレードの開始点
2016.05.20171007215506.0700e1db.rel	2.3.2	2017 年 10 月 7 日	ElasticSearch シャード カウントの減少。
2016.05.20170828200941.e5eab0a6.rel	2.3.1	2017 年 8 月 28 日	バグ修正
2016.05.20170810212922.28c79852.rel	2.3	2017 年 8 月 11 日	ライセンスのダウンロードを自動化。ポータルのソフトウェアを 3.4.47 に更新。
2016.05.20170710175041.77c0b12f.rel	2.2.4	2017 年 7 月 10 日	このリリースでは、バックアップの機能について説明します。
2016.05.20170519231807.db2f167e.rel	2.2.3	2017 年 5 月 20 日	このマイナー リリースには、Windows XP なしで実行する新しい工場出荷時のインストールが使用できます。
2016.05.20170508195308.b8dc88ed.rel	2.2.2	2017 年 5 月 8 日	ネットワーク構成およびオペレーティング システムのコンポーネントに対する変更のマイナー リリースで今後の機能をサポートします。

ビルド番号	リリース バージョン	リリース日	注記
2016.05.20170323020633.f82e66fe.rel	2.2.1	2017 年 3 月 24 日	SSLv3 の無効化、リソースの問題修正
2016.05.20170308211223.c92516ee.rel	2.2mfg	2017 年 3 月 8 日	製造時のみの変更。お客様への影響はありません。更新サーバ経由での導入は行われません。
2016.05.20170303034712.1b205359.rel	2.2	2017 年 3 月 3 日	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 年 1 月 7 日	OpAdmin/tgsh-dialog 用の LDAP 認証サポート
2016.05.20161121134140.489f130d.rel	2.1.5.	2016 年 11 月 21 日	ElasticSearch5、CSA パフォーマンス修正
2016.05.20160905202824.f7792890.rel	2.1.4	2016 年 9 月 5 日	主に製造向け
2016.05.20160811044721.6af0fa61.rel	2.1.3	2016 年 8 月 11 日	オフライン更新サポート キー、M4 ワイプ サポート
2016.05.20160715165510.baed88a3.rel	2.1.2	2016 年 7 月 15 日	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	2016 年 7 月 6 日	
2016.05.20160621044600.092b23fc	2.1	2016 年 6 月 21 日	

ビルド番号	リリース バージョン	リリース日	注記
2015.08.20160501161850.56631ccd	2.0.4	2016 年 5 月 1 日	2.1 更新の開始点。2.1 に更新するには、2.0.4 になっている必要があります。
2015.08.20160315165529.599f2056	2.0.3	2016 年 3 月 15 日	AMP 統合、CA 管理、分割 DNS を導入
2015.08.20160217173404.ec264f73	2.0.2	2016 年 2 月 18 日	
2017.12.20180302174440.097e2883.rel	2.4.2	2018 年 3 月 2 日	クラスタリング
2017.12.20180219033153.bb5e549b.rel	2.4.1	2018 年 2 月 19 日	OpAdmen でのクラスタリングのサポート。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 年 1 月 30 日	セキュリティ更新プログラムを ClamAV にのみ更新
2015.08.20160211192648.7e3d2e3a	2.0(1)	2016 年 2 月 12 日	
2015.08.20160131061029.8b6bc1d6	2.0	2016 年 2 月 11 日	ここから 2.0.1 へ強制的に更新
2014.10.20160115122111.1f09cb5f	1.4.6	2016 年 1 月 27 日	2.0.4 更新の開始点
2014.10.20151123133427.898f70c2	v1.4.5	2015 年 11 月 25 日	
2014.10.20151116154826.9af96403	v1.4.4		

ビルド番号	リリース バージョン	リリース日	注記
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1+hotfix 1		
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		

注：リリース バージョン 1.0 ～ 1.2 については、ブート時にインターフェイスが挿入されていない場合、リブートが必要になることがあります。これは、v1.3 より前の問題です（SFP を必要とするインターフェイスは、v1.3 以降でもブート時に挿入されている必要があるため、これを除く）。SFP に挿入されたネットワーク ケーブルは、安全にホットプラグ可能です。

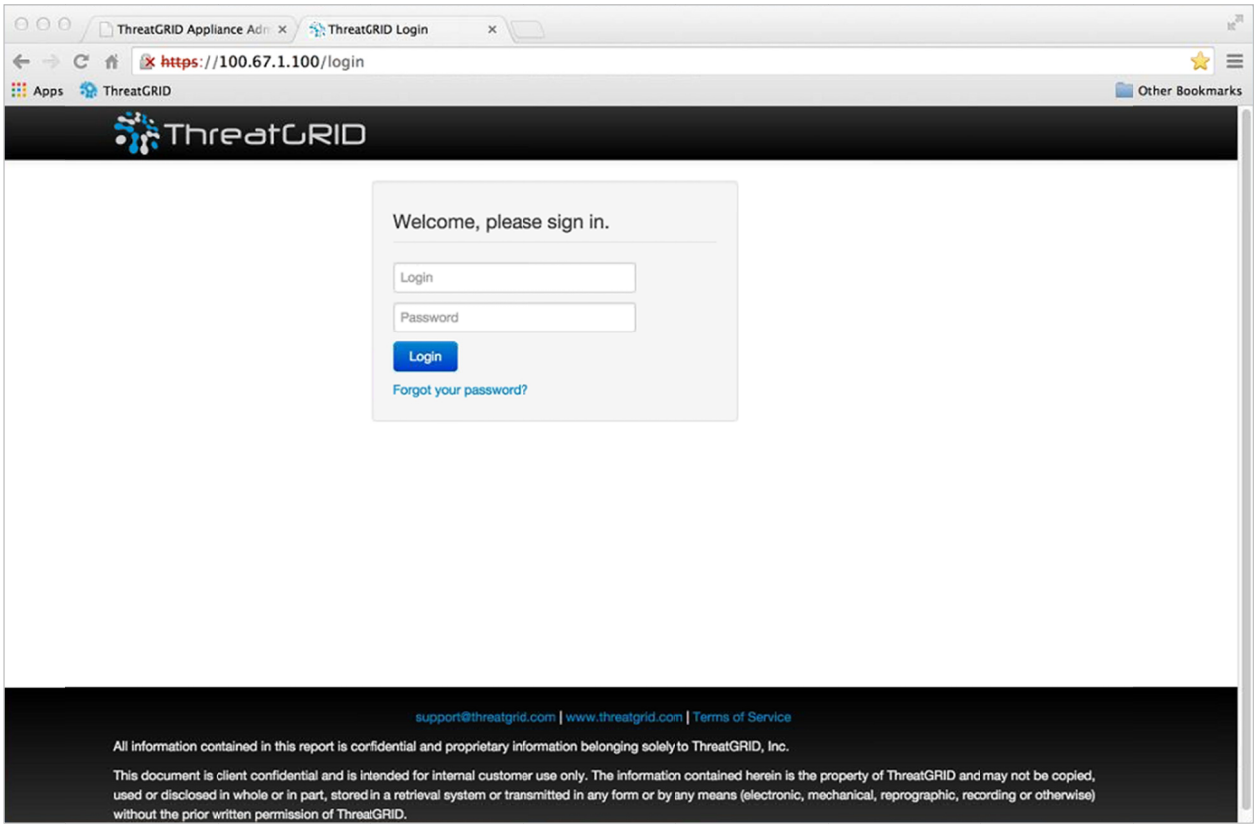
注：1.0 から 1.0+hotfix2 への更新には約 15 分かかります。1.0 から 1.3（データ移行なし）への完全な更新の適用には、約 30 分かかります。

アプライアンス設定のテスト：サンプルの送信

Threat Grid アプライアンスが現在のバージョンに更新されると、アプライアンスが適切に構成済みであるという最終テストは、Threat Grid ソフトウェアを使用してマルウェア サンプルを送信することです。

1. クリーン インターフェイスとして設定したアドレスを参照して、Threat Grid Portal にサインインします。Threat Grid のログイン ページが開きます。

図 29：Threat Grid Portal ログイン ページ



2. デフォルトのログインとパスワード、**admin/changeme** を入力します。
3. [Login] をクリックします。メインの Threat Grid の [サンプルの分析 (Sample Analysis)] ページが開きます。
4. 右上隅の [サンプルを送信 (Submit a Sample)] ボックスで、サンプル ファイルを選択するか、またはマルウェア分析用に送信する URL を入力します。

5. [Upload Sample] をクリックします。Threat Grid のサンプル分析プロセスが起動します。

   サンプルの分析は複数の段階を通じて進むことがわかります。分析中、サンプルは [Submissions] セクションに表示されます。分析が完了すると、結果は [Analysis Report] の詳細とともに、[Samples] セクションに示されます。

アプライアンスの管理

Threat Grid アプライアンスが設定され、初期設定が完了すると、アプライアンスの管理者向けの準備は完了しています。

リリース ノート、更新、SSL 証明書、ユーザの追加、およびその他の管理者タスクとトピックは、『*Threat Grid Appliance Administrator's Guide*』に記載されています。

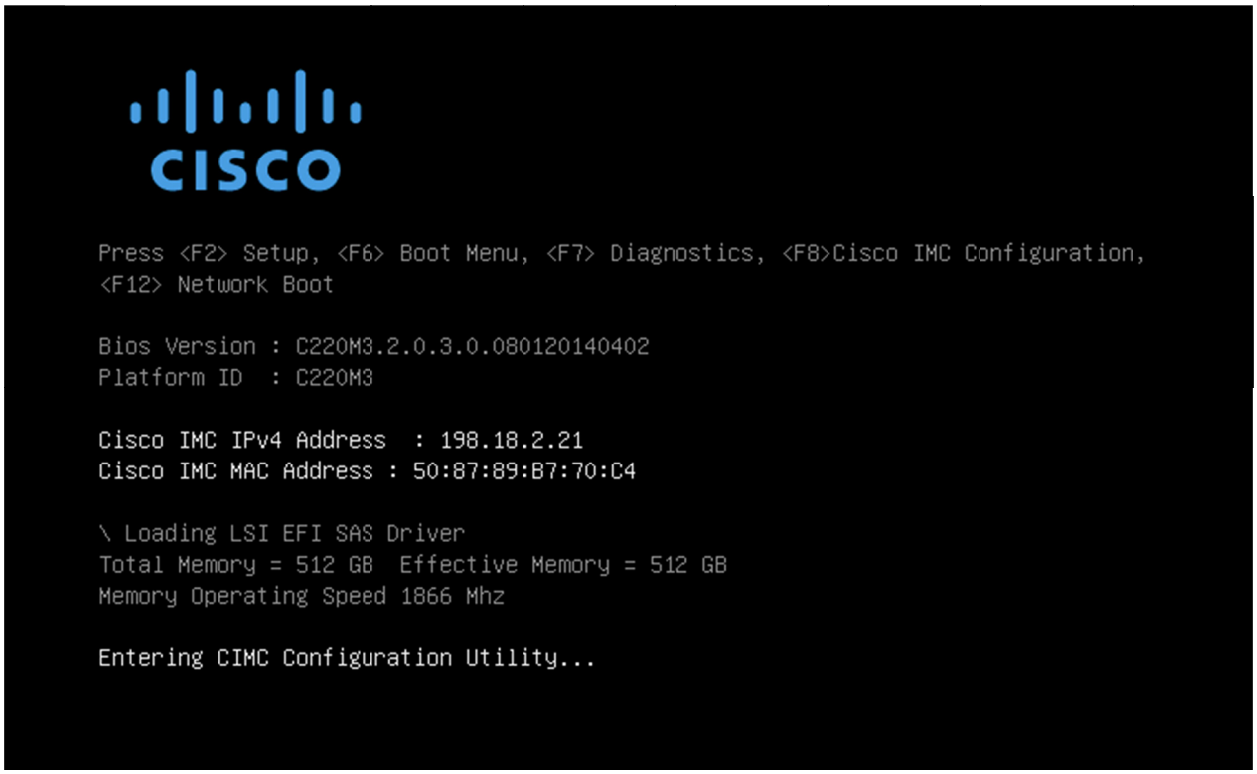
付録 A – CIMC 設定（推奨）

サーバの起動時に表示される最初のウィンドウはシスコ ウィンドウです。このウィンドウから Cisco Integrated Management Controller（「CIMC」）構成ユーティリティに入ることができます。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。

アプライアンスに直接接続されたモニタとキーボードが必要です。

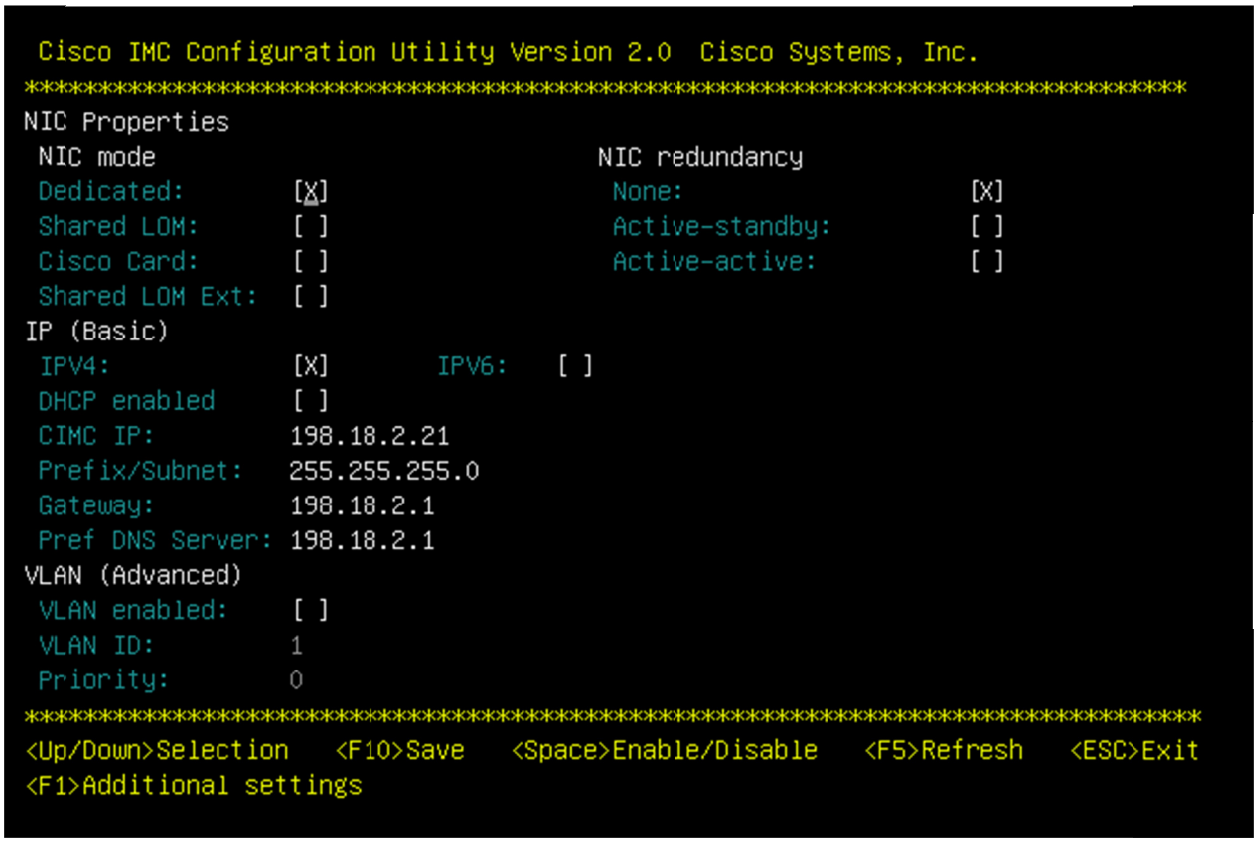
1. サーバの電源をオンにします。[Cisco] 画面が開きます。

図 30：[Cisco] 画面：CIMC 構成ユーティリティに入るには F8



2. メモリ チェックの完了後、**F8** を押して CIMC 構成ユーティリティに入ります。

図 31：CIMC 構成ユーティリティ



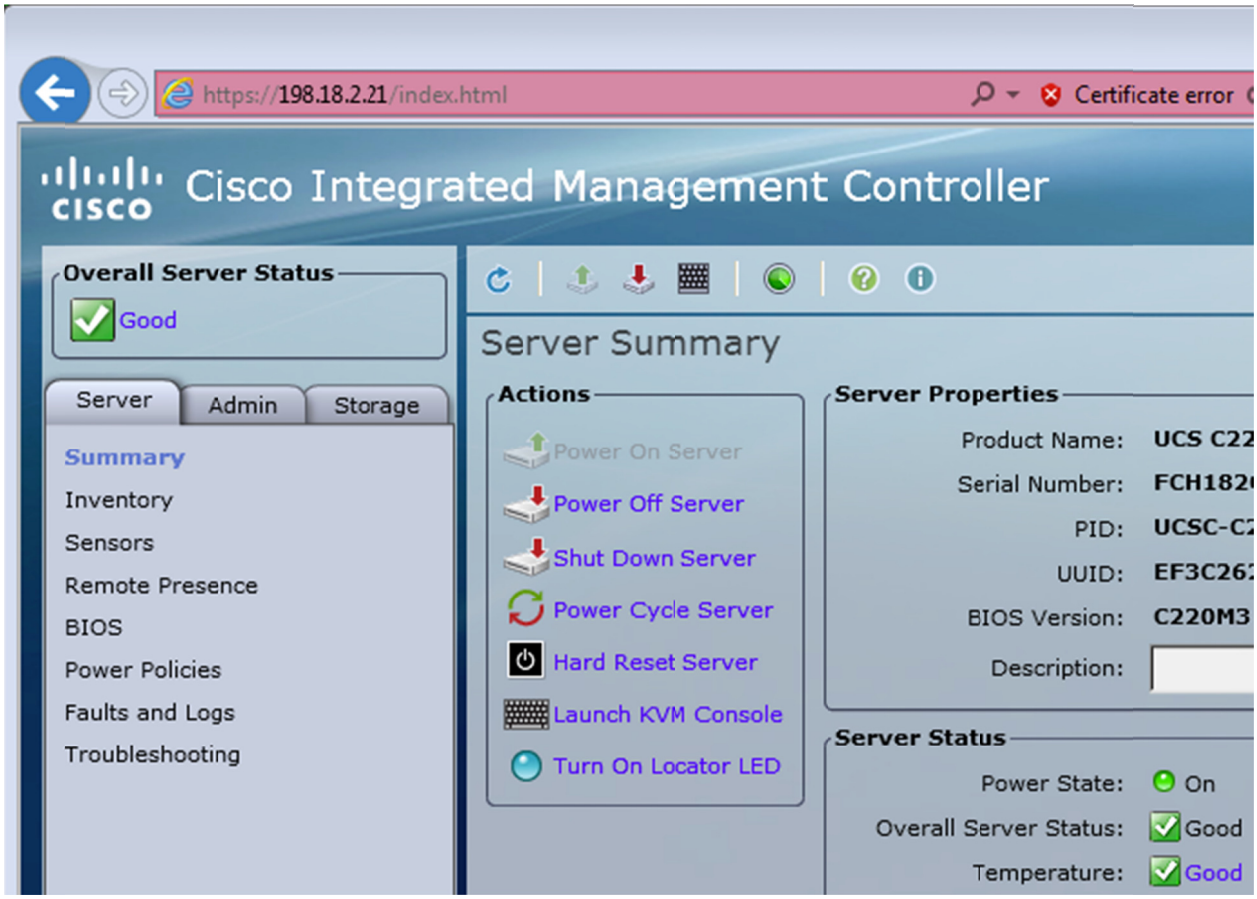
3. CIMC 構成ユーティリティで、リモート サーバ管理に使用する IP アドレスを設定します。

完了したら、保存してから終了します。

これで、Web ブラウザで https://<CIMC-IP address>/ と入力して、サーバをリモートで管理できます。

初期ユーザ名は「**admin**」で、パスワードは「**password**」です。

図 32：Cisco Integrated Management Controller (CIMC) インターフェイス



これで、CIMC インターフェイスを使用してサーバの状態を表示できるほか、KVM を開いて残りの設定手順をリモートで完了できます。

索引

索引