操作

[操作（Operations）] メニューは、管理者が Cisco Secure Malware Analytics アプライアンスの操作タスクを実行するために使用します。この章では、設定変更のアクティブ化、Admin UI のリロード、ジョブと電源設定の管理、アプライアンスの更新を含むこれらのタスクについて説明します。

有効化

Admin UI の設定に対する変更は保存する必要があり、いくつかの変更を保存して再設定を行い、変更を確定する必要があります。設定の変更は、再設定が完了するまで有効になりません。

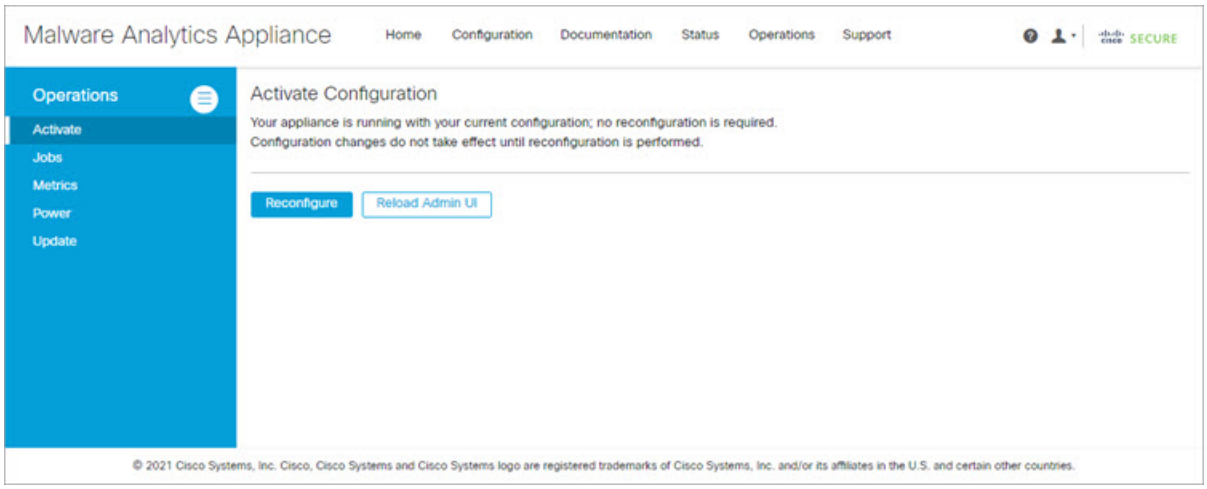
再構成が必要な場合、ページの上部にあるバナーに、薄いオレンジ色のアラートメッセージが表示されます。このバナーの **[再設定（Reconfigure）]** ボタンをクリックすると、**[操作（Operations）]** メニューの **[構成のアクティブ化（Activate Configuration）]** ページに移動します。このページから、構成の変更を適用し、Admin UI をリロードすることもできます。

手順

ステップ 1 アラートメッセージの **[再構成（Reconfigure）]** をクリックして、再構成プロセスを開始します。

ステップ 2 **[構成のアクティブ化（Activate Configuration）]** ページで、**[再構成（Reconfigure）]** をクリックして再構成ジョブを実行します。

図 *1*：構成をアクティブ化する



ステップ 3 確認ダイアログで、**[再構成（Reconfigure）]** をクリックして再構成ジョブを開始します。

構成がアクティブ化され、その進行状況に関するメッセージが [ジョブ（Jobs）] ウィンドウに表示されます。エラーメッセージやその他の情報を確認する必要がある場合は、詳細がジョブ（Jobs）ページに保持されます。

完了すると、再構成が成功したことを示す確認メッセージが表示されます。

ステップ 4 [続行（Continue）] をクリックします。

ステップ 5 Admin UI を更新する場合は、**[Admin UIのリロード（Reload Admin UI）]**をクリックします。

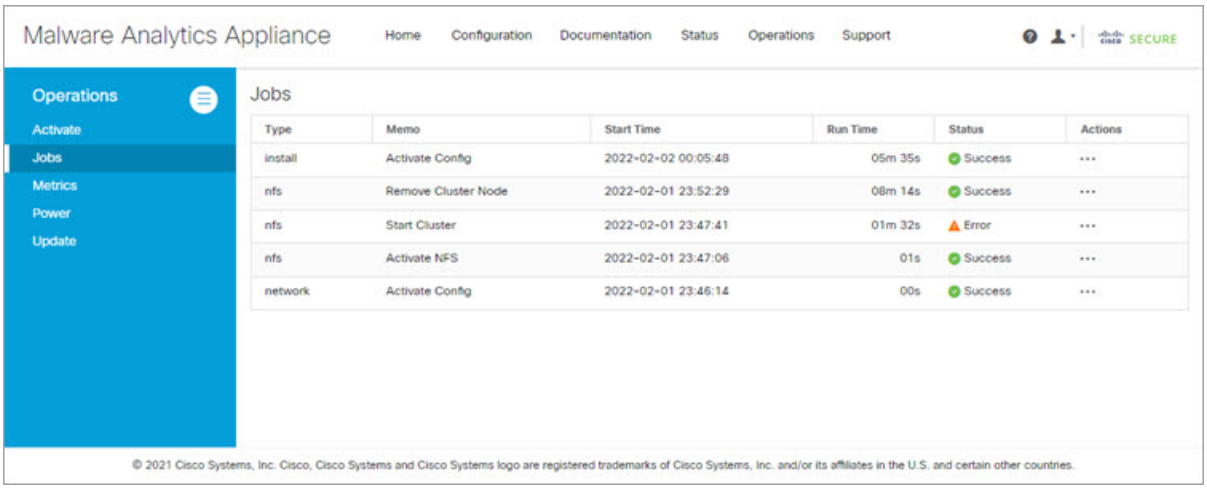
ジョブ（Jobs）

管理 UI の **[ジョブ（Jobs）]** ページを使用して、Cisco Secure Malware Analytics アプライアンスで実行されたジョブを表示できます。このページを使用して、特定のジョブに関するエラーメッセージやその他の情報を表示できます。

手順

ステップ 1 **[操作（Operations）]** タブをクリックし、**[ジョブ（Jobs）]**を選択します。

図 *2* : ジョブ（*Jobs*）



各ジョブのジョブタイプ、開始時刻、実行時間、およびステータスが表示されます。

ステップ 2 ジョブの情報を表示するには、**[アクション（Actions）]** 列の小さい **[詳細（Details）]** ボタンをクリックします。

電源

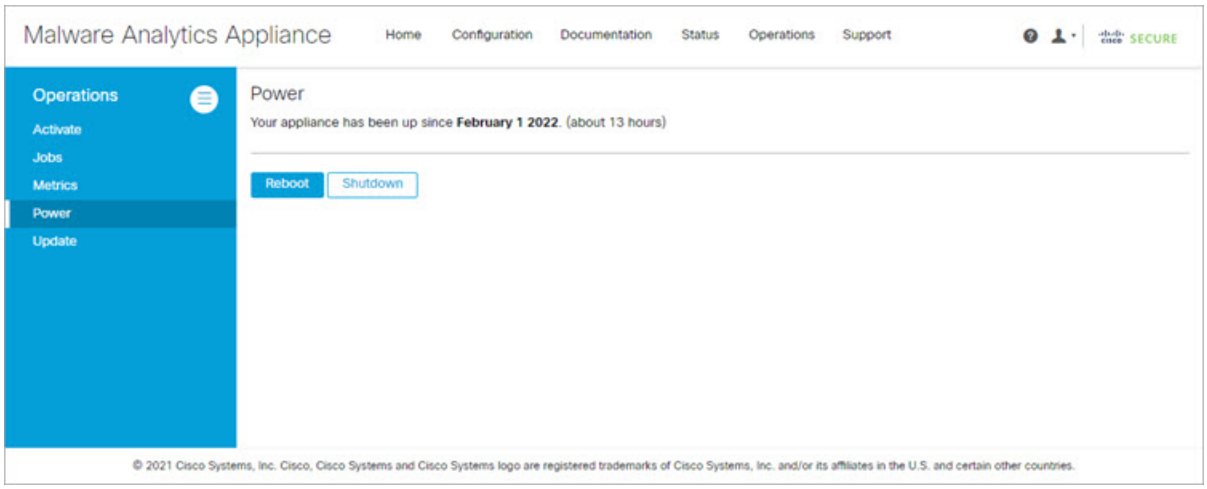
管理 UI の **[電源（Power）]** ページから Cisco Secure Malware Analytics アプライアンスを再起動またはシャットダウンできます。

（注） GNU GRUB ブートローダーが、Cisco Secure Malware Analytics アプライアンスのソフトウェアスタックから完全に削除されました。以前の構成では、署名されていない構成ファイルをロードできませんでした（したがって、CVE-2020-10713 に対して脆弱ではありませんでした）が、新しいブートメカニズムは GRUB を完全に削除します。

手順

ステップ 1 **[操作（Operations）]** タブをクリックし、 **[電源（Power）]**を選択します。

図 *3 :* 電源



アプライアンスの電源が投入された日付が表示されます。

ステップ 2 **[再起動（Reboot）]** をクリックしてアプライアンスを再起動するか、**[シャットダウン（Shutdown）]** をクリックしてアプライアンスを完全にシャットオフします。

更新

『*Cisco Secure Malware Analytics Appliance Getting Started Guide*』に記載されている通り、Cisco Secure Malware Analytics アプライアンスを新しいバージョンに更新する前に、初期セットアップと構成手順を完了する必要があります。

（注） 新しい Cisco Secure Malware Analytics 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。ライセンスがインストールされるまで更新はダウンロードされず、Cisco Secure Malware Analytics アプライアンスが完全に設定されない限り（データベースを含む）、正しく適用されない可能性があります。

新しい更新を確認して（**[操作（Operations）]** > **[更新（Update）]**）、それらを適用できます。

構成は、通常の起動プロセスの一部として実行されるようになりました。再起動のたびに、アプライアンスは完全に管理されたソフトウェア ロードアウトにリセットされます（実行時にコード署名がチェックされます）。以前は複数の再起動を伴う再設定サイクル中にのみ発生していた設定操作が、各起動サイクルの一部として発生するようになりました。したがって、次のようになります。

- 再インストール操作を伴う再設定は冗長になります。
- アップグレードのインストールが迅速になり、再起動は 1 回だけで済みます。

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。

- Cisco Secure Malware Analytics アプライアンスの更新は、管理 UI を介して適用されます。
- 更新サーバー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、更新サーバーは、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。
- サーバー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。
- オフライン(エアギャップ)更新プロセスについては、「Update Secure Malware Analytics Appliance」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 Secure Malware Analytics アプライアンス バージョン ルックアップ テーブル*」を参照してください。

ポートの更新

Cisco Secure Malware Analytics 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（Admin UI）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 サーバー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。

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ー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）。

Cisco Secure Malware Analytics 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 サーバーがダウンした場合、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 Cisco Secure Malware Analytics 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。

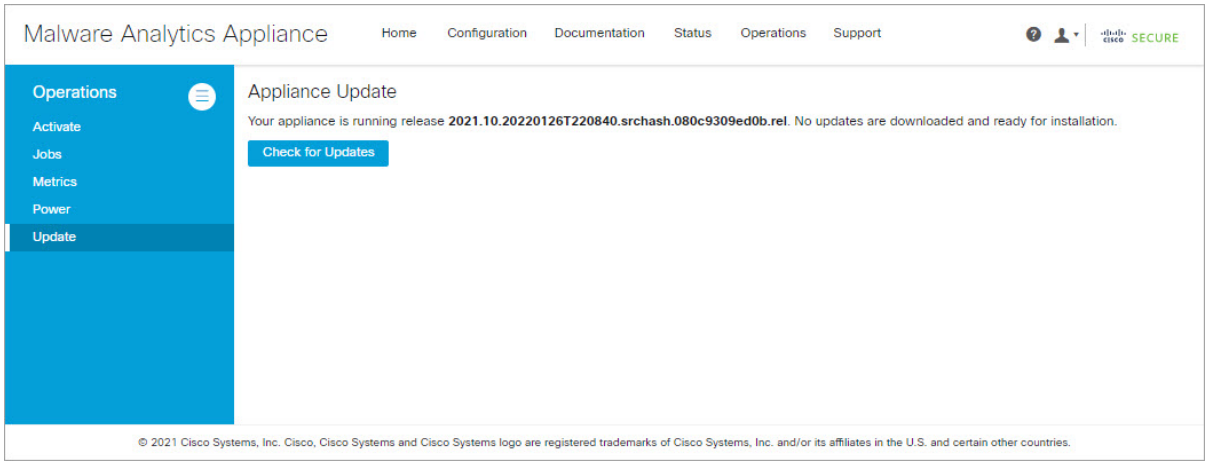
更新のインストール

更新を確認し、Cisco Secure Malware Analytics アプライアンスを更新するには、次の手順を実行します。

手順

ステップ 1 [操作（Operations）] タブをクリックし、[更新（Update）] を選択して [アプライアンスの更新（Appliance Updates）] ページを開きます。

図 *4:* アプライアンスの更新ページ



現在のリリースバージョンは、ページの上部に表示されます。また、インストール可能なアップデートがあるかどうかも通知されます。リリースバージョンについては、『*Cisco Secure Malware Analytics Appliance Version Lookup Table*』を参照してください。

ステップ 2 [更新の確認（Check for Updates）] をクリックします。

Cisco Secure Malware Analytics アプライアンスソフトウェアの最新の更新/バージョンがあるかどうかを確認するためのチェックが実行され、ある場合は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。

ステップ 3 更新プログラムのダウンロードが完了したら、[更新を適用（Apply Update）] をクリックしてインストールします。

更新のトラブルシューティング

ここでは、アプライアンスの更新中に発生する可能性のある問題と、それらを解決する方法について説明します。

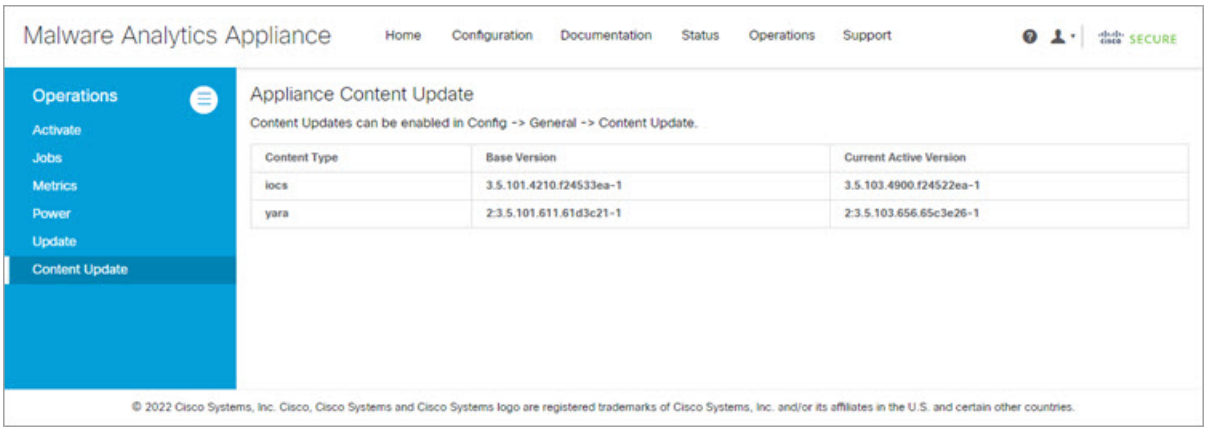
データベースの更新に失敗しました（Database Upgrade - Not Successful）メッセージ

「*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 Secure Malware Analytics 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場合に表示されることがあります。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。

アプライアンス コンテンツの更新

[アプライアンスコンテンツの更新（Appliance Content Update）] ページは、侵入兆候、または iocs（侵害指標）と yara の基本バージョンと最新バージョンを提供します。

図 *5:* アプライアンス コンテンツの更新



（注） アプライアンスを更新している間に、アプライアンスを最新の *iocs* および *yara* に更新します。アプライアンスの詳細については、「更新 （4 ページ）」を参照してください。

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