FMCホスト制限ライセンスエラーのトラブルシューティング： "You have 0 out of xxxxxx FireSIGHT host licenses remaining"

内容

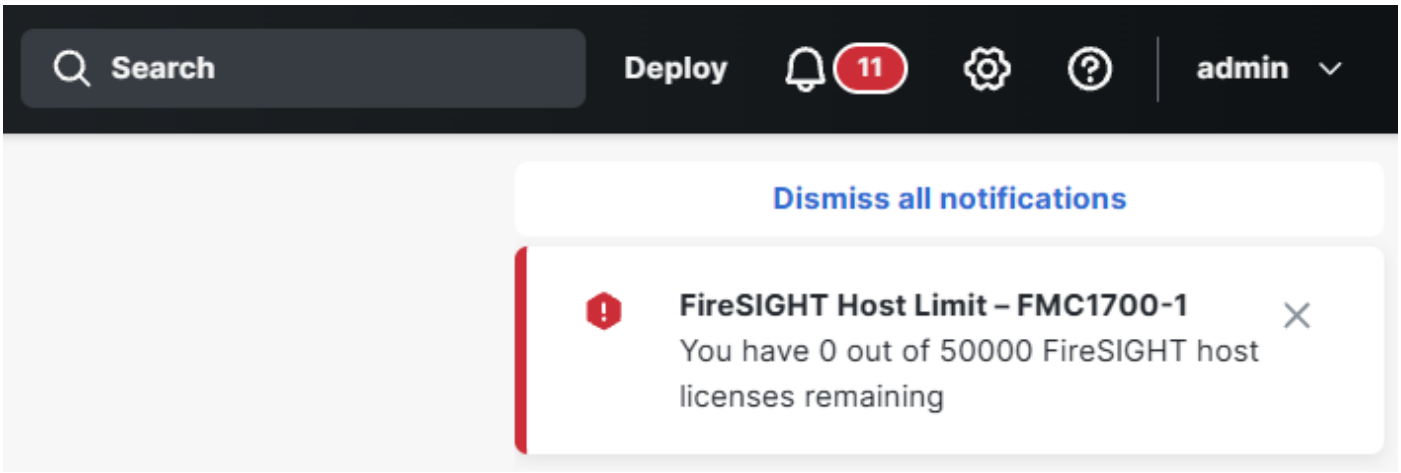
お問い合わせ内容

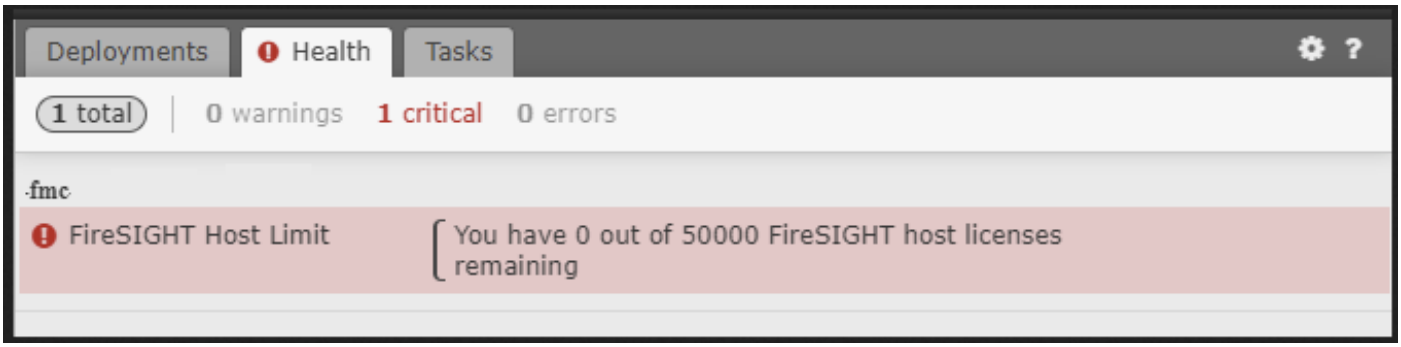
ファイアウォール管理センター(FMC)に、ホストライセンスの制限に達したことを示すヘルスアラートが表示されます。特定のエラーメッセージは次のように表示されます。

FireSIGHTホスト制限：[FMCホスト名]

FireSIGHTホストライセンスはxxxxxx個中0個残っています

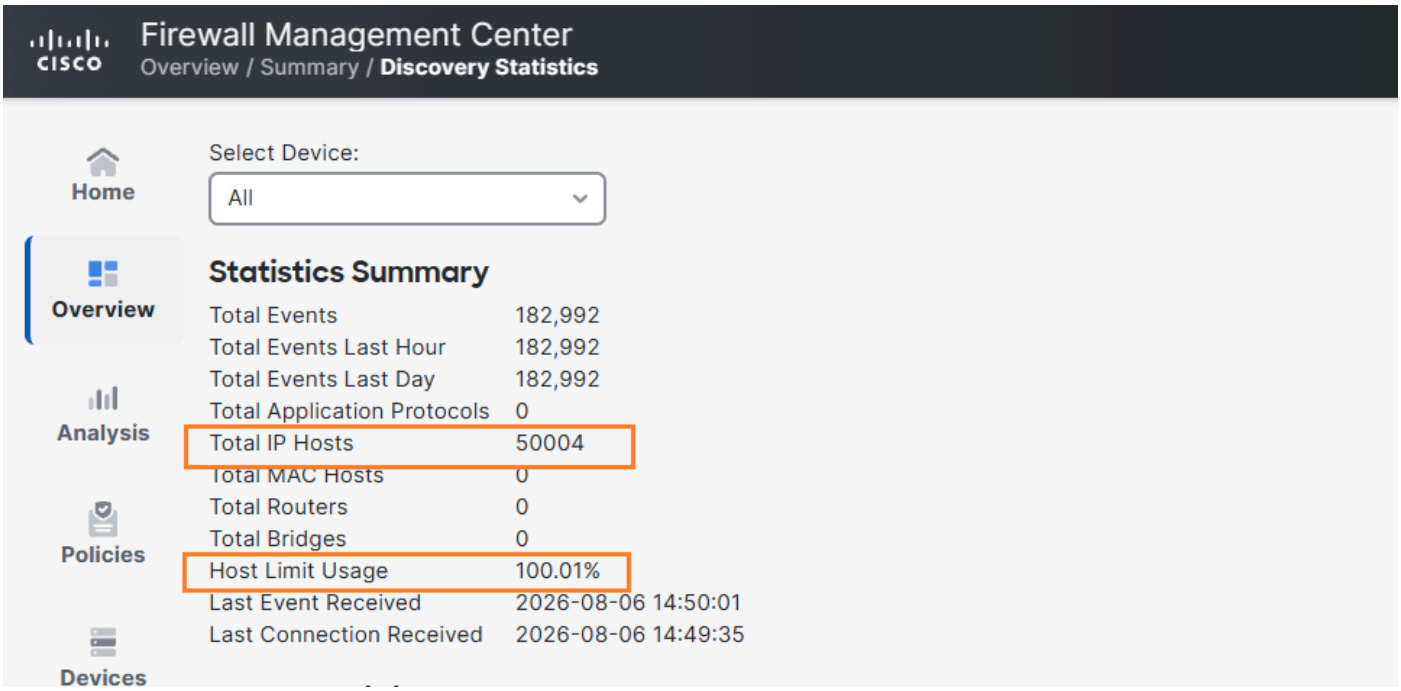
例:





注：ホストライセンスの総数は、FMCプラットフォームによって異なります。

また、Overview > Summary > Discovery Statistics ページでは、使用率が100 %と表示されます。



環境

- FMC 7.7.10以降他のソフトウェアバージョンも影響を受ける可能性があります。
- ホストトラッキングを有効にして設定されたネットワーク検出。

解決策

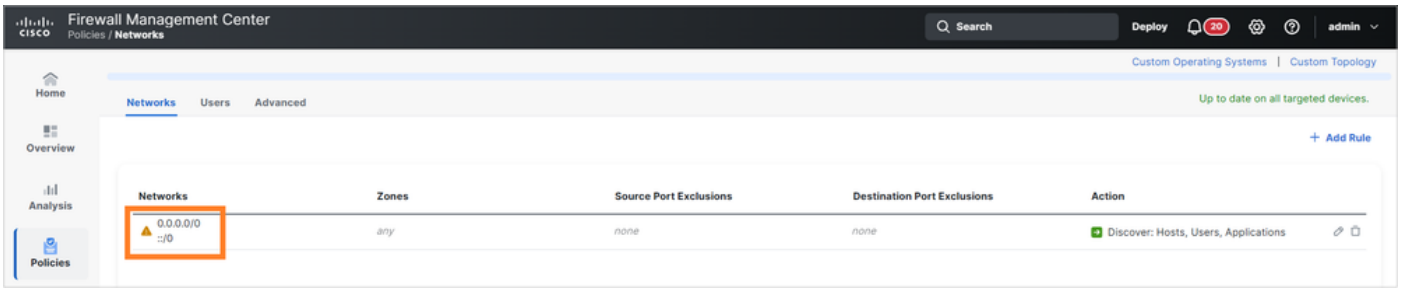
FMCホスト制限アラートによってファイアウォールトラフィックが停止することはありません。アクセスコントロールとインスペクションは正常に機能し続けます。主な影響は、FMCでのホストの可視性とコンテキストトラッキングです。

この通知は、FMCが、ネットワークマップおよびホストデータベースでホストを追跡する最大容量に達したときに表示されます。

ネットワーク検出スコープの確認：

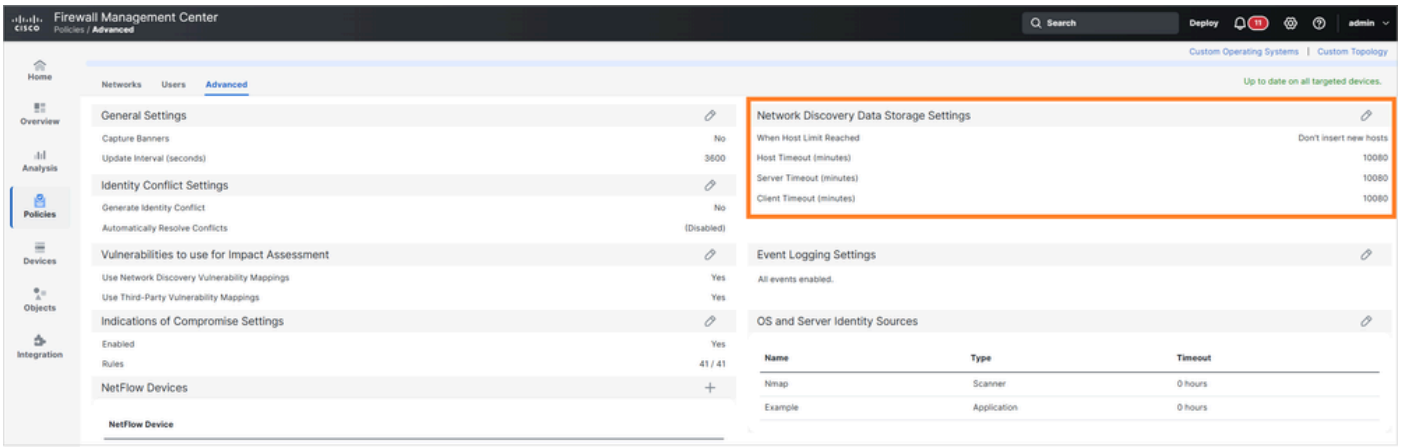
検出が必要な内部ネットワークのみに限定されていることを確認します。セキュリティの可視性が必要でない限り、不要なパブリック、NAT、ゲスト、ロードバランサ、または一時的なアドレス範囲を検出しないようにしてください。

この場合は、ネットワーク検出設定を変更し、監視する内部ネットワークのみを指定する必要があります。それ以外の場合は、外部（インターネット）ホストによって検出データベースが満杯になる可能性があります。



現在の設定の分析

Policies > Network Discovery > Advanced > Network Discovery Data Storage Settingsでネットワーク検出の設定を確認して、現在のホストの制限を確認します。



通常、設定には次のように表示されます。

- ホストの制限に達した場合：新しいホストを挿入しない
- ホストタイムアウト：10080分/7日
- サーバタイムアウト：10080分/7日
- クライアントタイムアウト：10080分/7日

現在の設定が「新しいホストを挿入しない」で、ホストデータベースがいっぱいになった場合、ホスト数が制限を下回るまで新しく検出されたホストは追加されず、ホストの可視性が不完全になります。

オプションの設定変更

ホスト制限の動作を変更して、アクティブなホストの継続的な追跡を可能にすることができます。

ステップ1:Policies > Network Discoveryの順に移動します。

ステップ2:Advancedタブをクリックします。

ステップ3:Network Discovery Data Storage Settingsで、Editをクリックします。

ステップ4:ホストの上限に達した時点を「新しいホストを挿入しない」から「ホストをドロップ

する」に変更します。

手順5:変更を保存します。

手順6:設定を導入して変更を適用します。

予想される影響と動作

[ホストのドロップ]設定を有効にした場合：

- 予期されるファイアウォールトラフィックの停止はありません。
- アクセスコントロールとインスペクションは正常に続行します。
- FMCは、新しく検出されたホストを追加するときに、ネットワークマップから最も長く非アクティブなホストを削除する
- 現在アクティブなホストの継続的なトラッキングが維持されます。
- ドロップされたホストの履歴ホストコンテキストは、それらのホストが再びアクティブになるまで表示できなくなります。

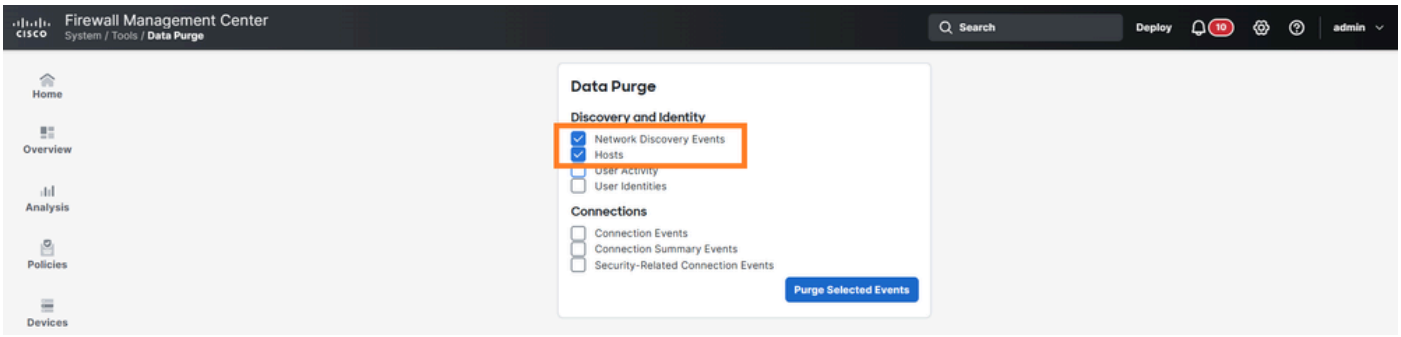
ホストタイムアウトレビュー：

通常は、デフォルトのタイムアウト値である10080分（7日）が適切です。非アクティブなホストの保持期間が長すぎる場合にのみ、調整を検討してください。

ホストの手動クリーンアップ（必要な場合）:

すぐにホスト数を減らす必要がある場合は、分析>ホスト>ホストのテーブルビューから古いホストを削除できます。これは単なるクリーンアップアクションであることに注意してください。検出スコープが広すぎる場合、FMCは同じホストを再検出します。

あるいは、ディスカバリデータベースから、System > Tools > Data Purgeの順に選択して、すべてのホストを消去することもできます。



原因

FireSIGHTホストライセンスの制限に達するのは、FMCがネットワークマップとホストデータベースでホストの最大数を検出し、追跡している場合です。一般的な寄与要因には次のものがあります。

- 不必要な外部アドレス範囲やパブリックアドレス範囲を含め、設定されているネットワーク検出スコープが広すぎる。
- ホストライセンスを消費するNAT、ロードバランサ、または一時アドレスの検出。
- 非アクティブなホストを長期間保持するホストタイムアウト設定。
- ネットワークの自然増加がFMCホストの容量制限に達している。

関連コンテンツ

- Cisco Secure Firewall Management Centerデバイス設定ガイド – ネットワーク検出ポリシー
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。