FMCを介したSnort 2からSnort 3へのアップグレード

内容

はじめに

このドキュメントでは、Firepower Manager Center(FMC)でSnort 2およびSnort 3バージョンからアップグレードする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Threat Defense(Ftd)
- Firepower Management Center
- Snort

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FMC 7.0
- FTD 7.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Snort 3機能は、Firepower Device Manager(FDM)およびCisco Defense Orchestrator(CDO)用の6.7リリースと、Firepower Management Center(FMC)用の7.0リリースで追加されました。

Snort 3.0は、次の課題に対処するために設計されました。

1. メモリとCPUの使用量を削減します。
2. HTTPインスペクションの有効性を向上させる。
3. 迅速な設定のロードとSnortの再起動
4. プログラマビリティの向上による機能追加の迅速化

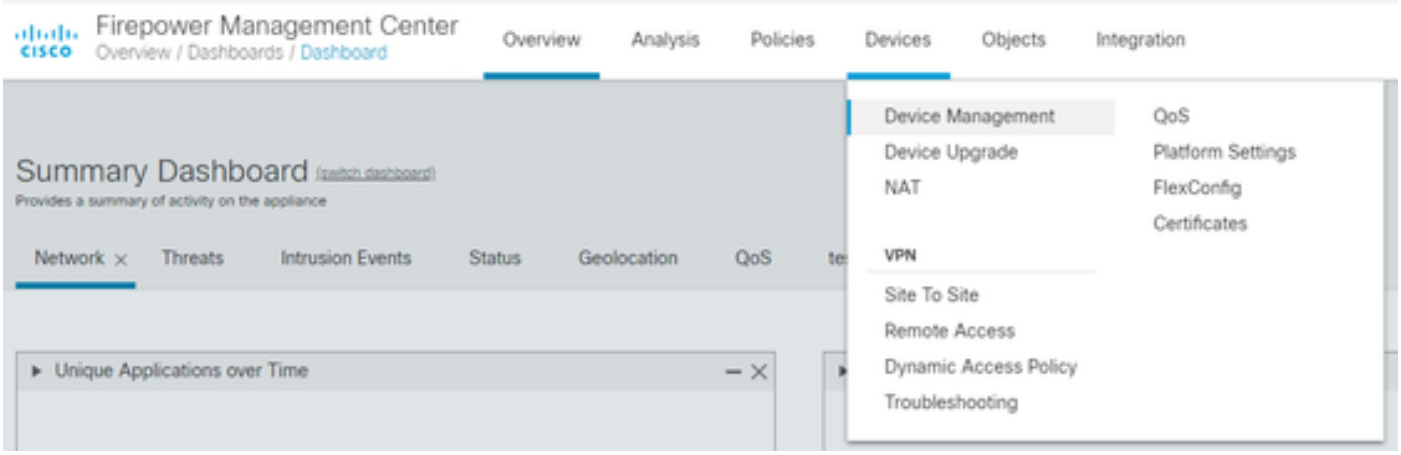
設定

Snortバージョンのアップグレード

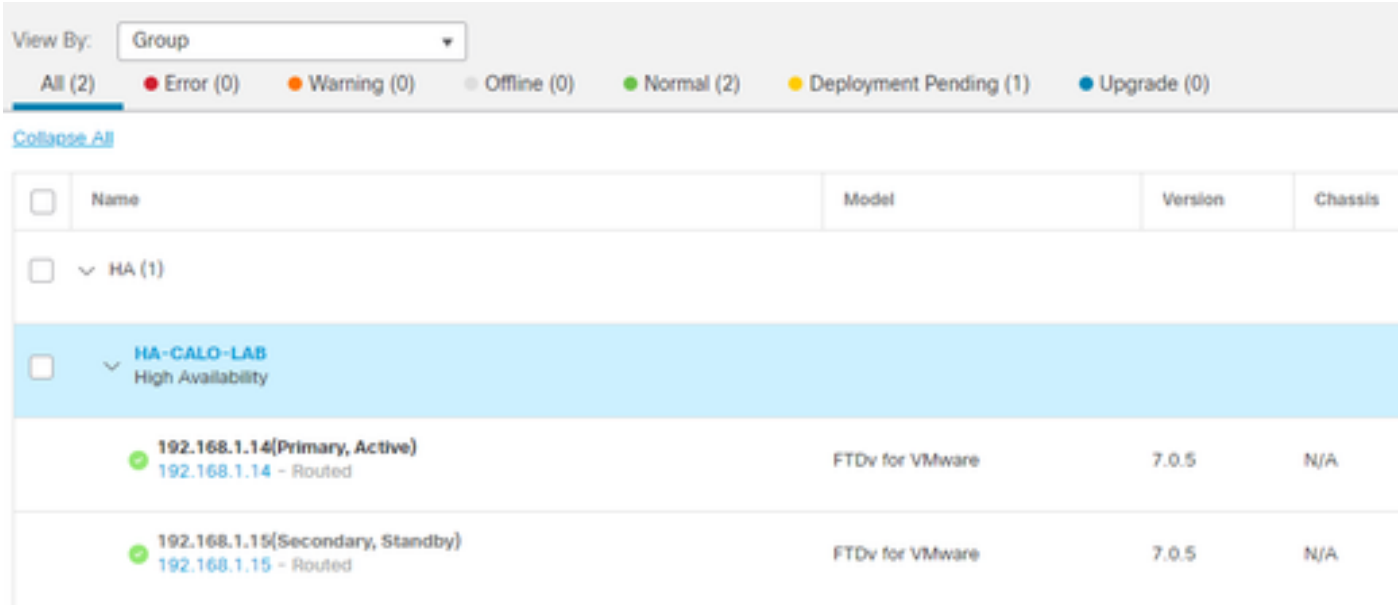
方式 1

1. Firepower Management Centerにログインします。

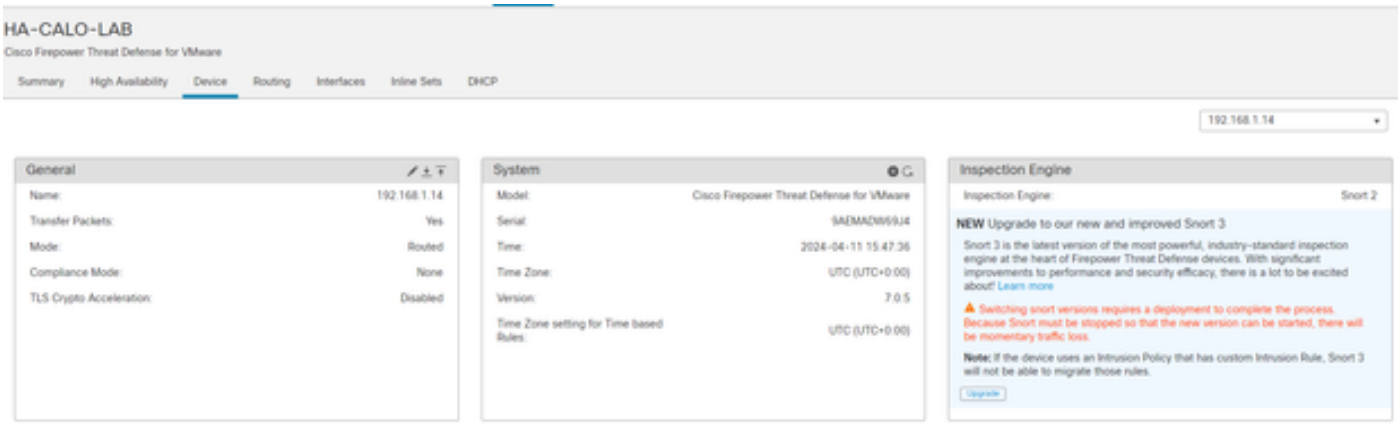
2. Deviceタブで、Devices > Device Managerの順に選択します。



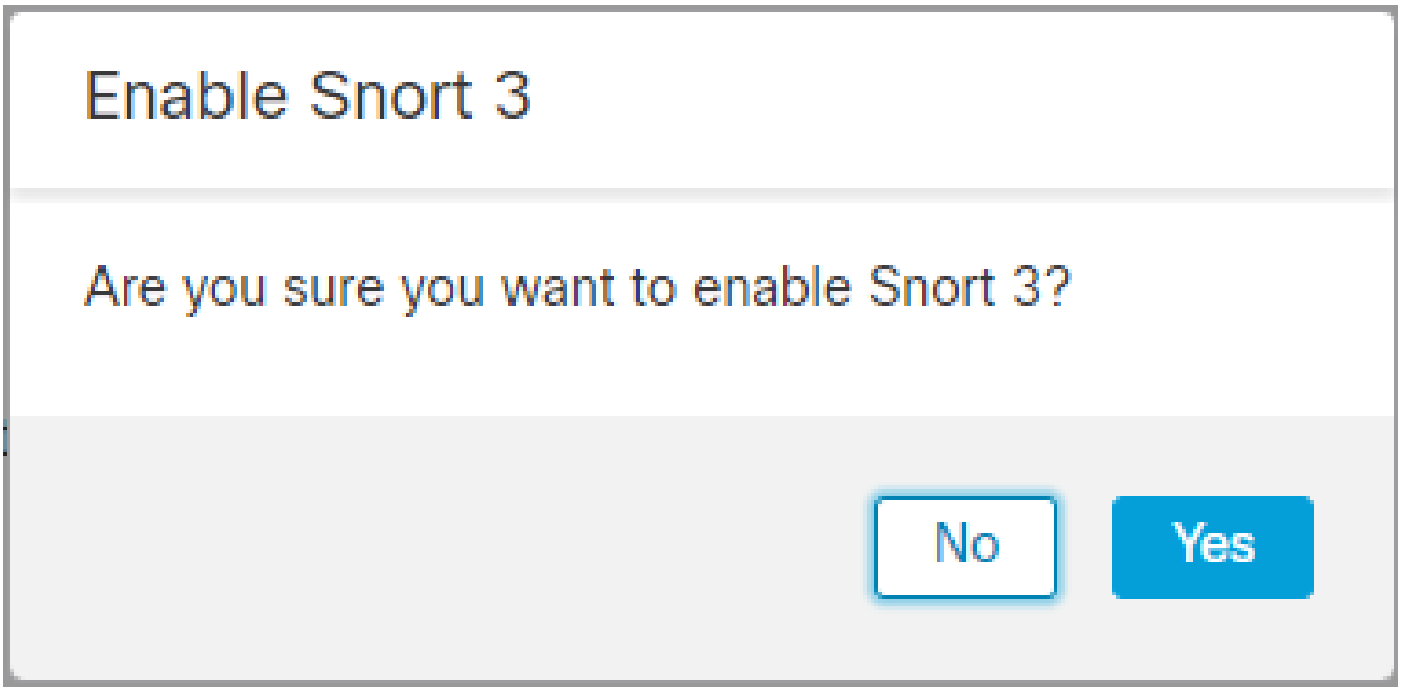
3. Snortのバージョンを変更するデバイスを選択します。



4. Deviceタブをクリックし、Inspection EngineセクションでUpgradeボタンをクリックします。



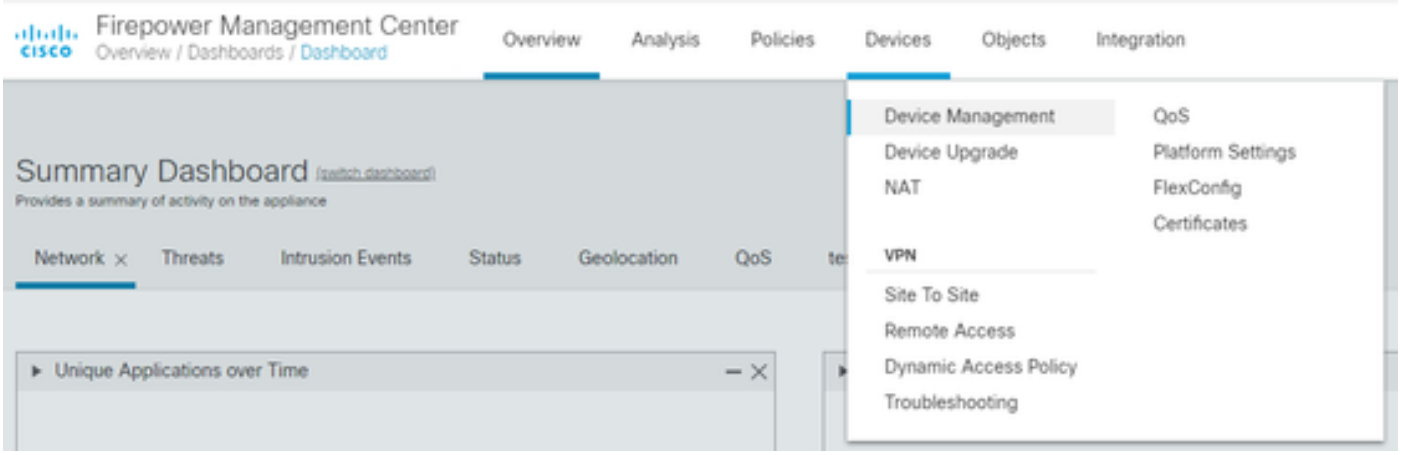
5. 選択内容を確認します。



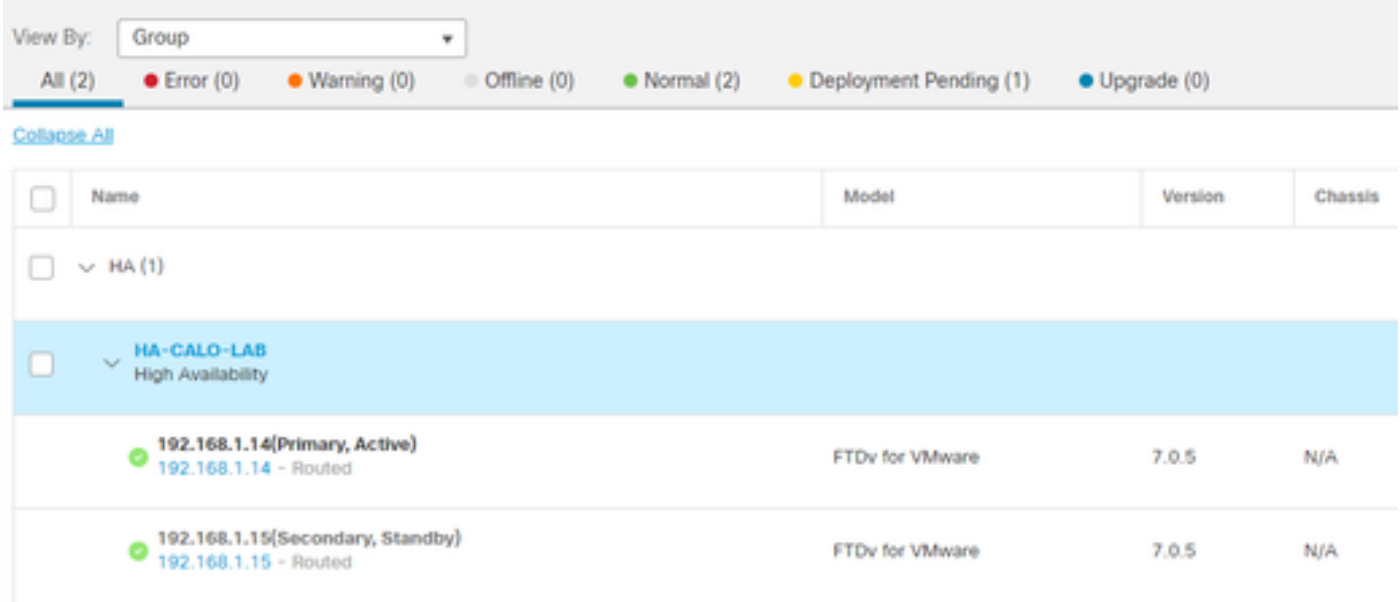
方式 2

1. Firepower Management Centerにログインします。

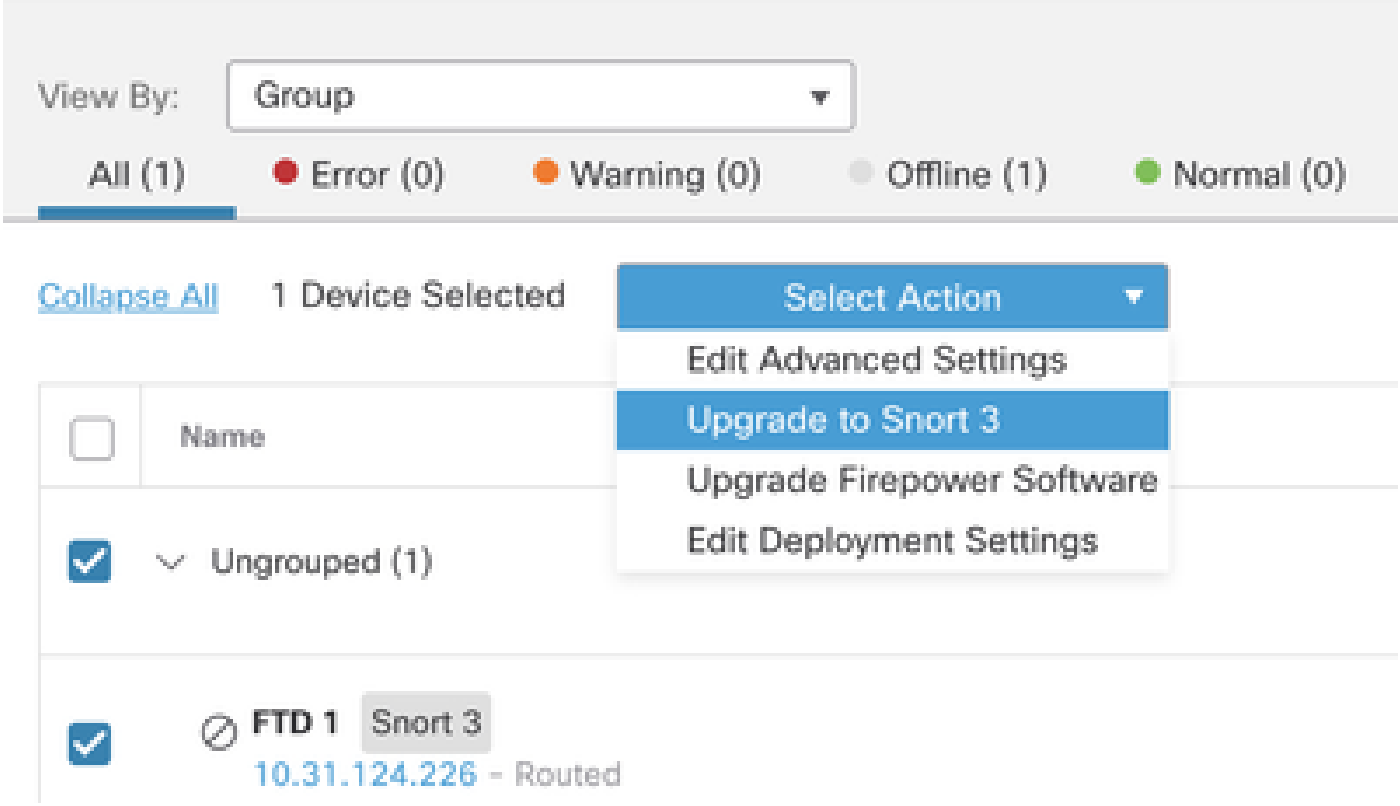
2. Deviceタブで、Devices > Device Managerの順に選択します。



3. Snortのバージョンを変更するデバイスを選択します。



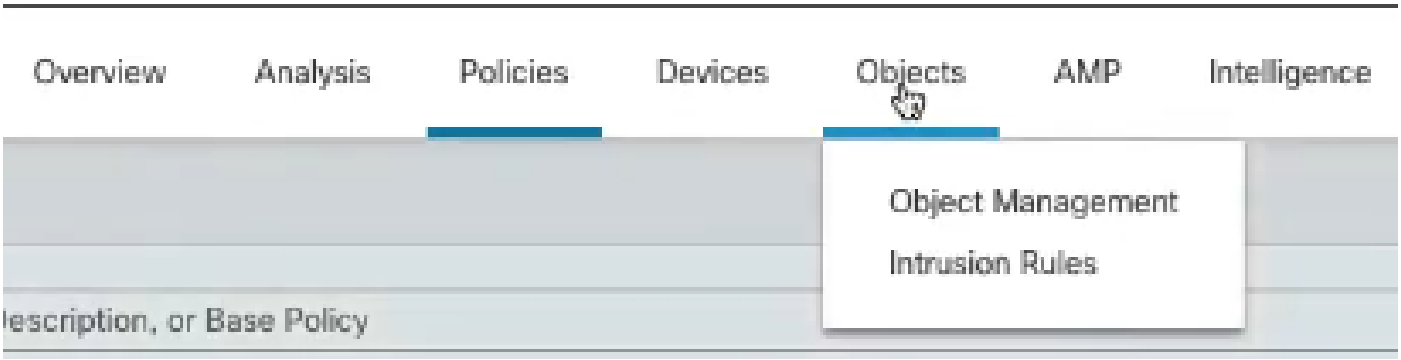
4. Select Actionボタンをクリックして、Upgrade to Snort 3を選択します。



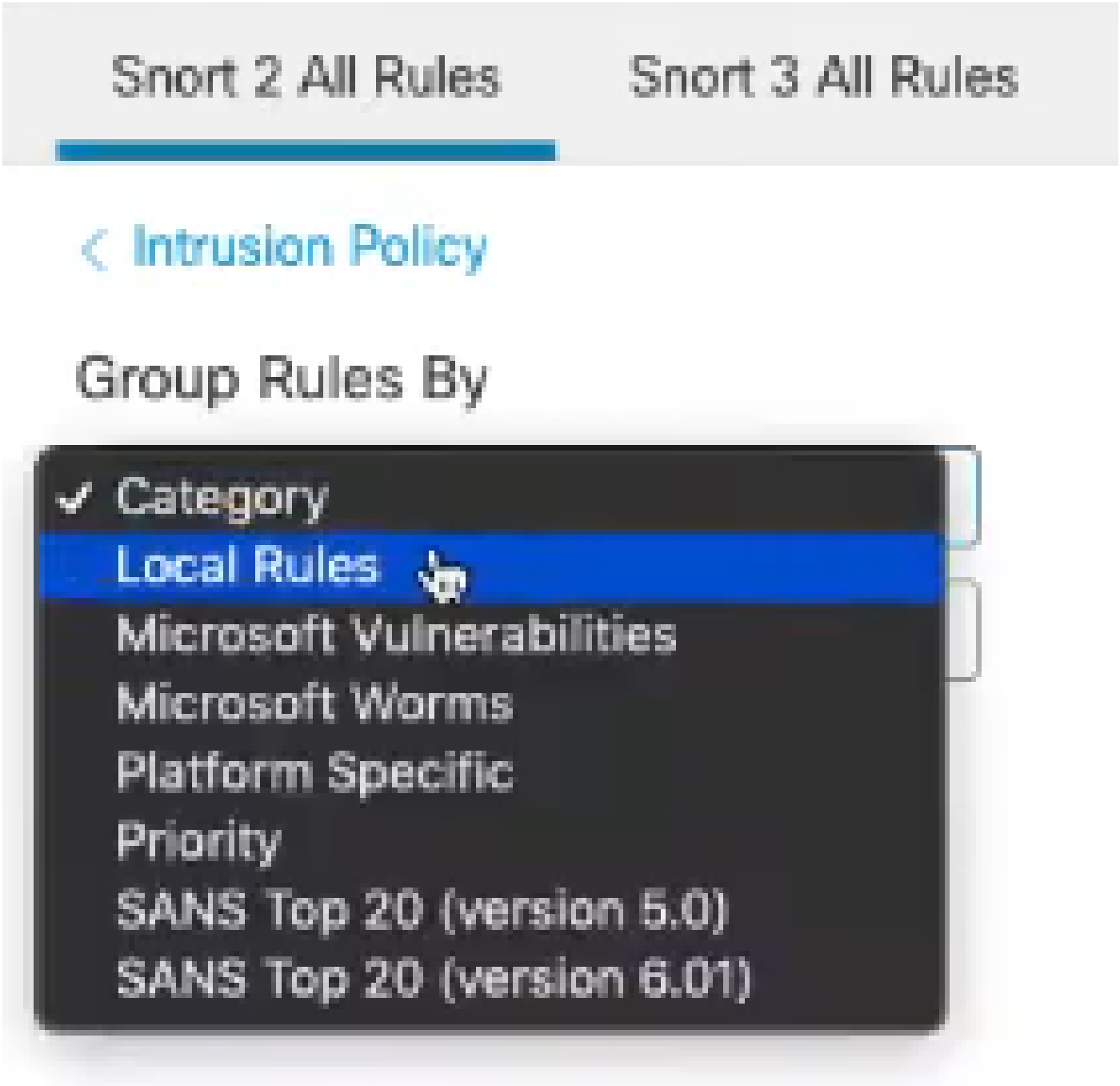
侵入ルールのアップグレード

さらに、Snort 2のルールをSnort 3のルールに変換する必要があります。

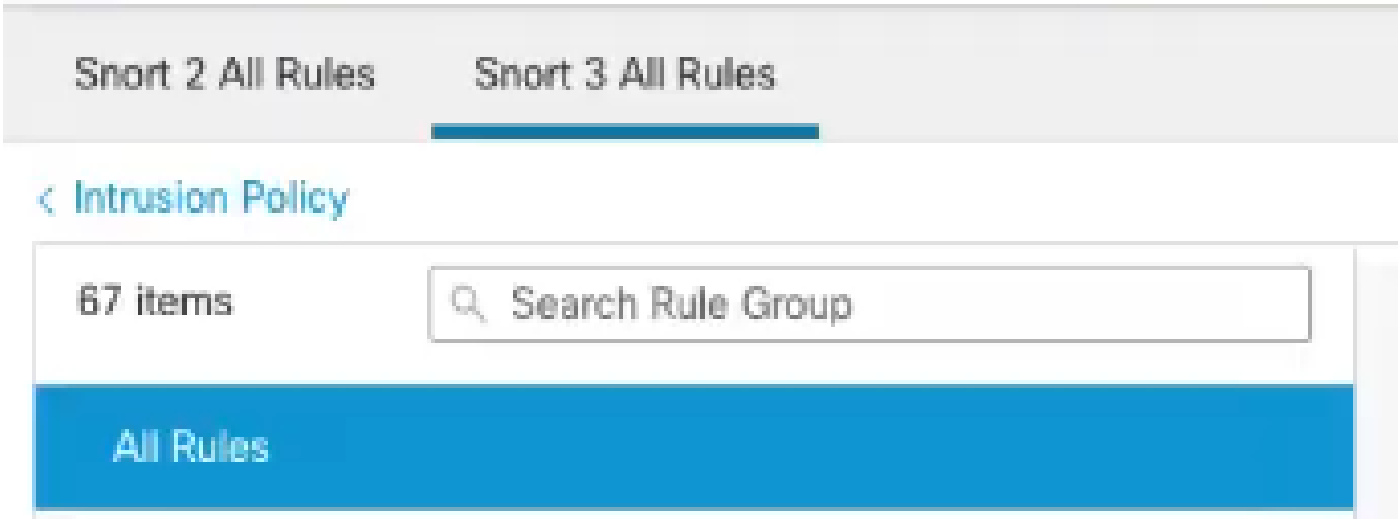
1. メニューからObjects > Intrusion Rulesを選択します。



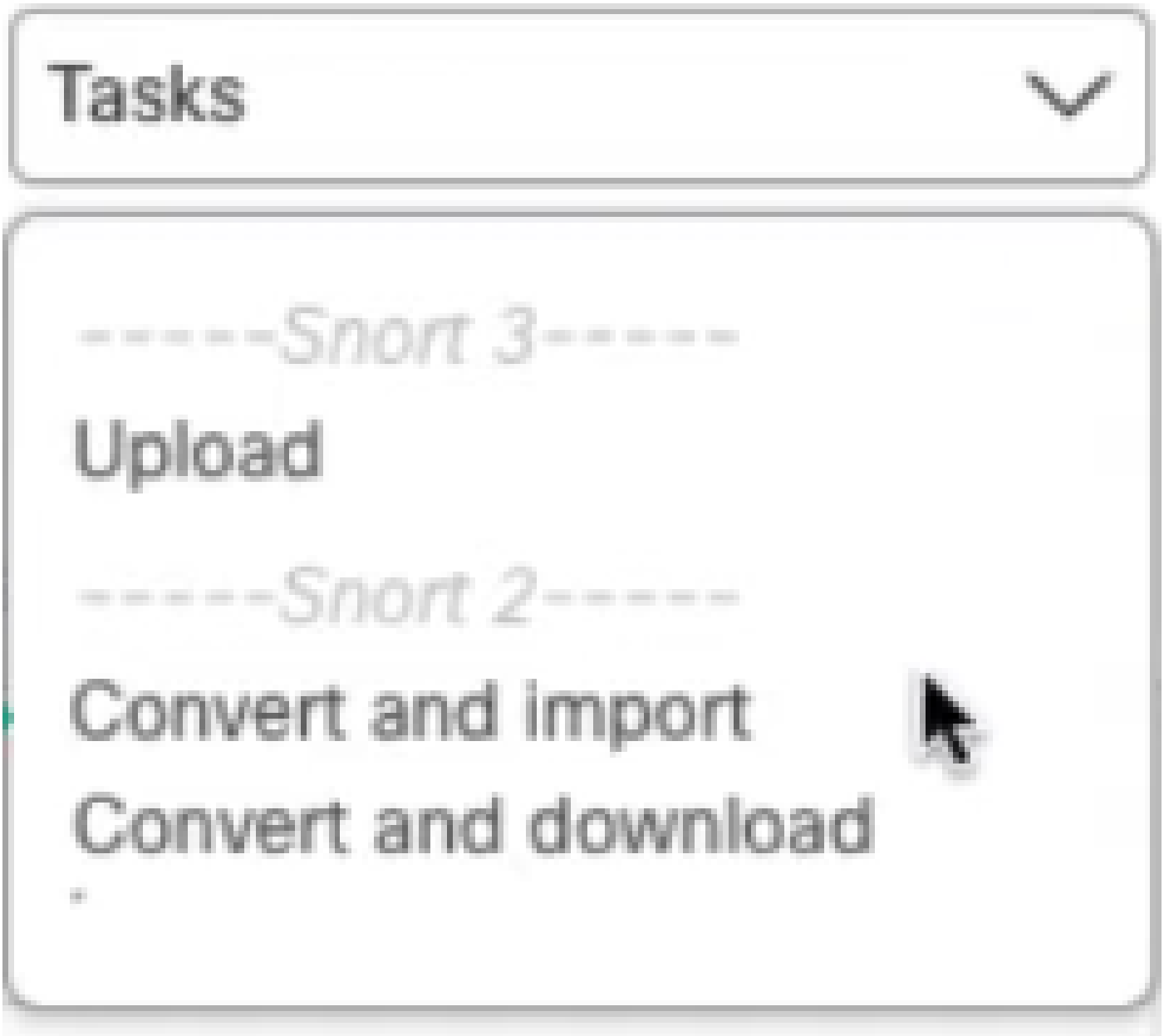
2. メニューからSnort 2 All Rulesタブ> Group Rules By > Local Rulesの順に選択します。



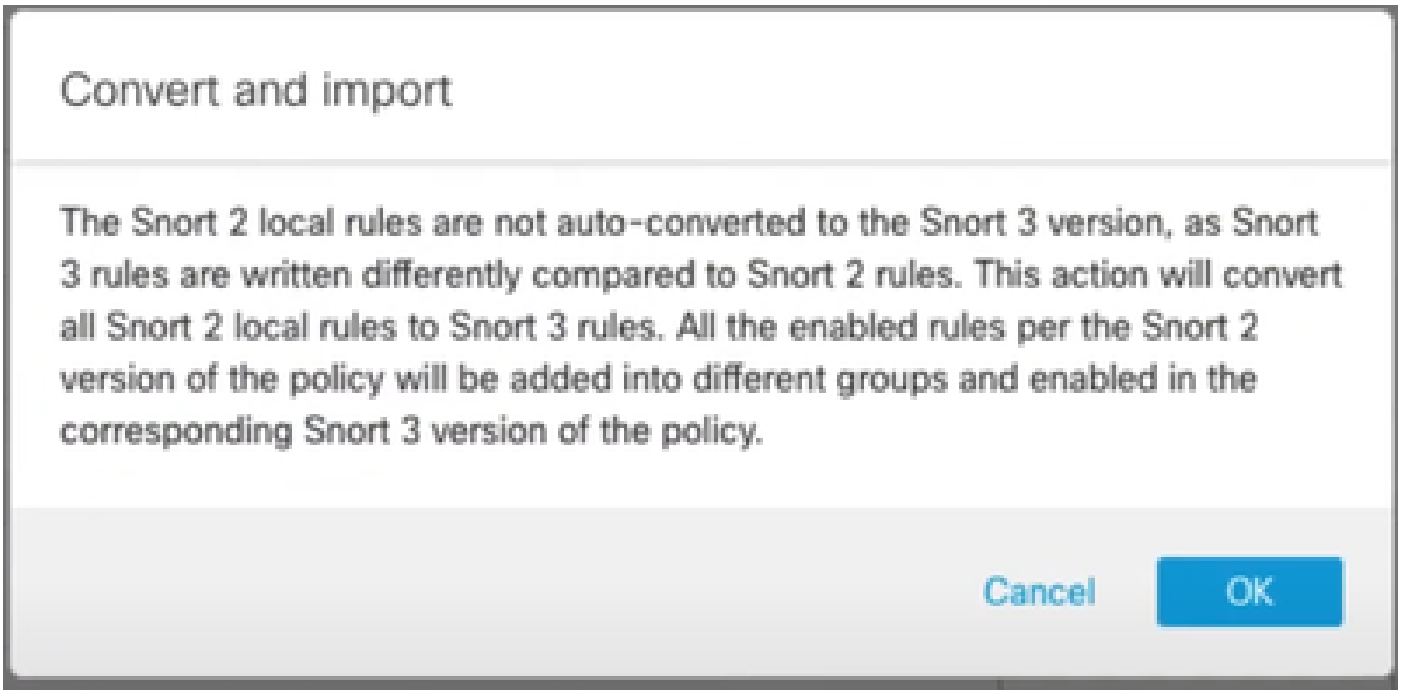
3. Snort 3 All Rulesタブをクリックして、All Rulesが選択されていることを確認します。



4. [Task]ドロップダウンメニューで、[Convert and import]を選択します。



5. 警告メッセージに対してOKをクリックします。

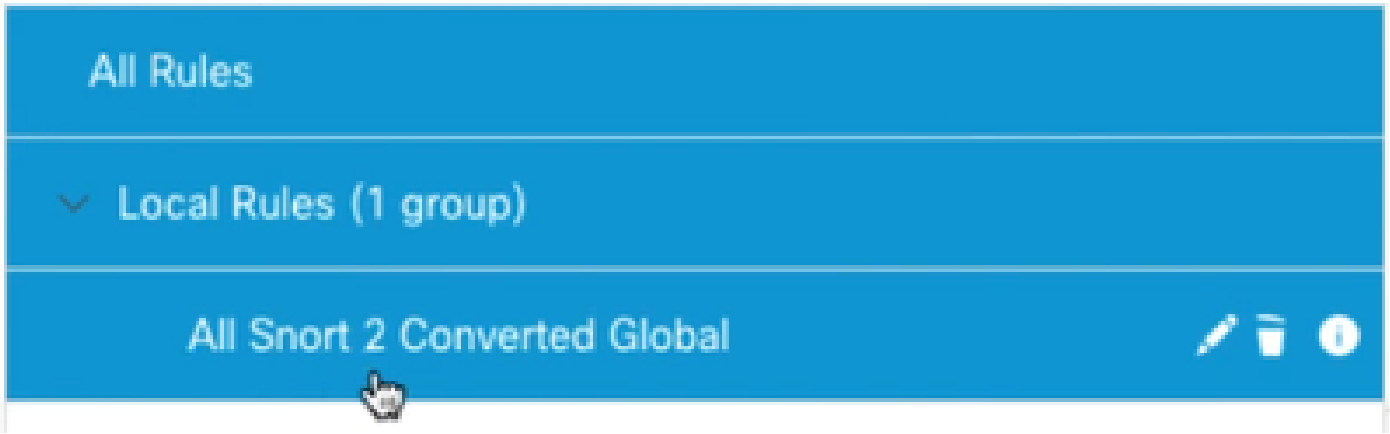


確認

「インスペクションエンジン」セクションには、Snortの現在のバージョンがSnort 3であると表示されます。

次のメッセージが表示されると、ルールの変換が成功しました。

最後に、ローカルルールグループに「すべてのSnort 2変換済みグローバル」セクションがあります。このセクションには、Snort 2からSnort 3へのすべての変換済みルールが含まれています。



トラブルシューティング

移行が失敗またはクラッシュした場合は、Snort 2にロールバックして再試行します。

関連情報

- Snort 2からSnort 3への移行方法
- Cisco Secure - Snort 3デバイスアップグレード（外部YouTubeビデオ）

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。