Atualização do Snort 2 para o Snort 3 via FMC

Contents

Introdução

Este documento descreve como atualizar as versões Snort 2 e Snort 3 no Firepower Manager Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense
- Firepower Management Center
- Snort

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FMC 7.0
- FTD 7.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O recurso Snort 3 foi adicionado na versão 6.7 do Firepower Device Manager (FDM) e do Cisco Defense Orchestrator (CDO); na versão 7.0 do Firepower Management Center (FMC).

O Snort 3.0 foi projetado para lidar com estes desafios:

1. Reduza o uso de memória e CPU.
2. Melhorar a eficácia da inspeção HTTP.
3. Carregamento mais rápido da configuração e reinicialização do Snort.
4. Melhor capacidade de programação para adição mais rápida de recursos.

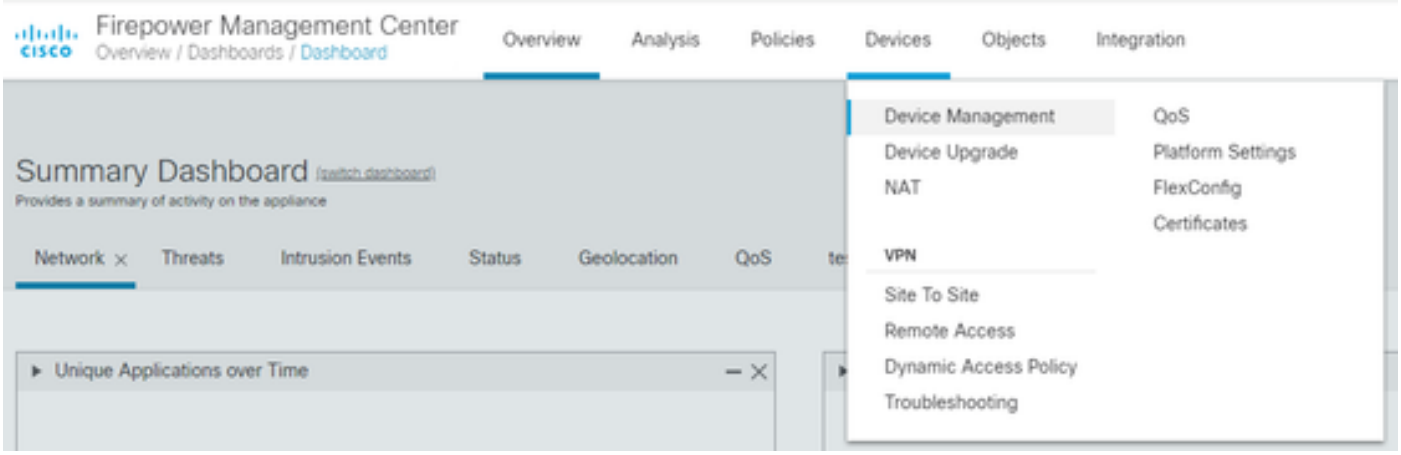
Configurar

Atualize a versão do Snort

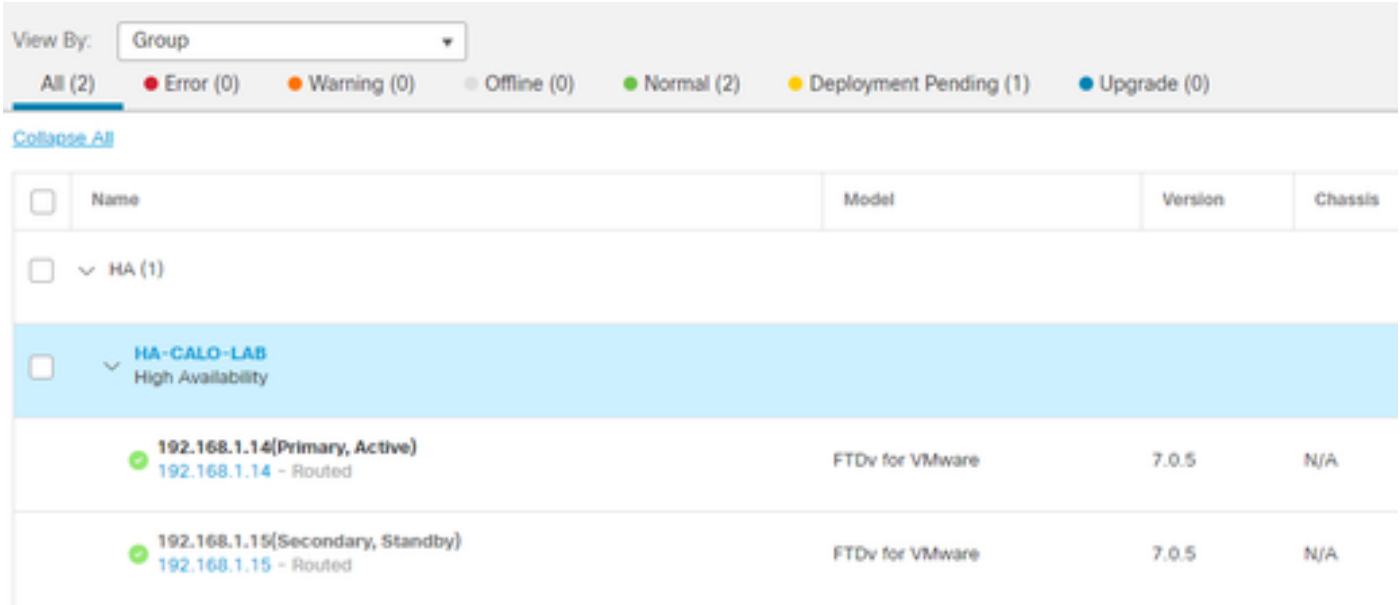
Método 1

1. Faça login no Firepower Management Center.

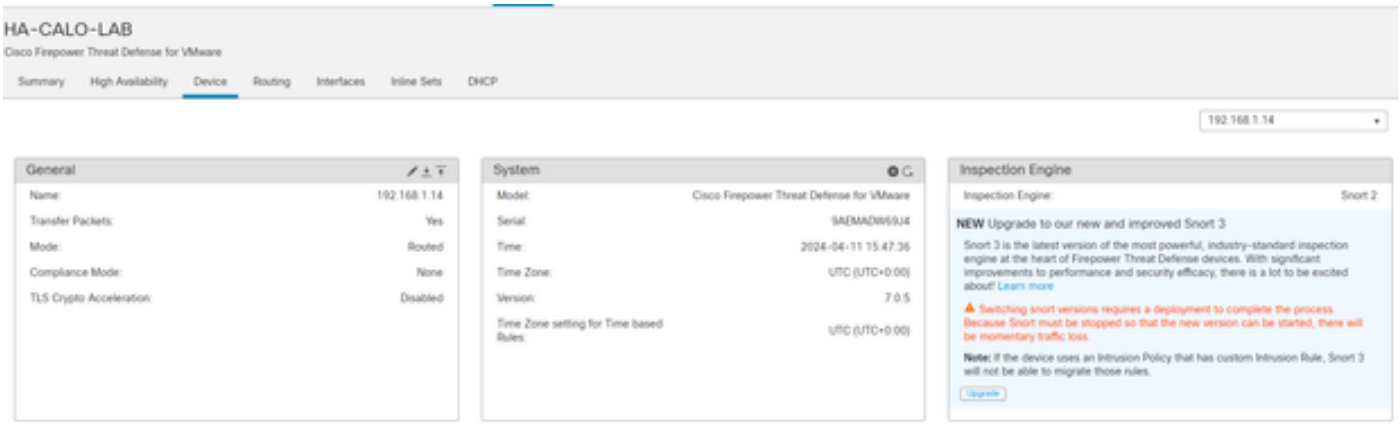
2. Na guia Dispositivo, navegue até Dispositivos > Gerenciador de dispositivos.



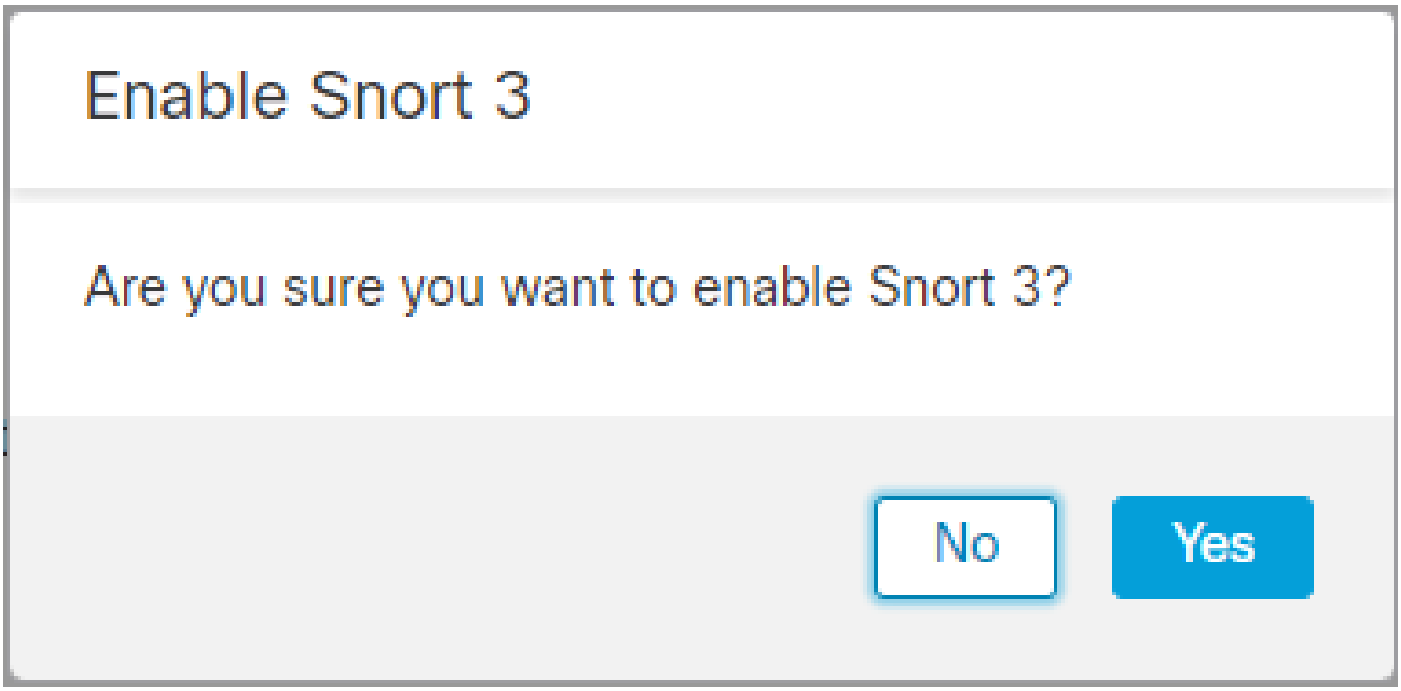
3. Selecione o dispositivo cuja versão do Snort você deseja alterar.



4. Clique na guia Dispositivo e clique no botão Atualizar na seção Mecanismo de inspeção.



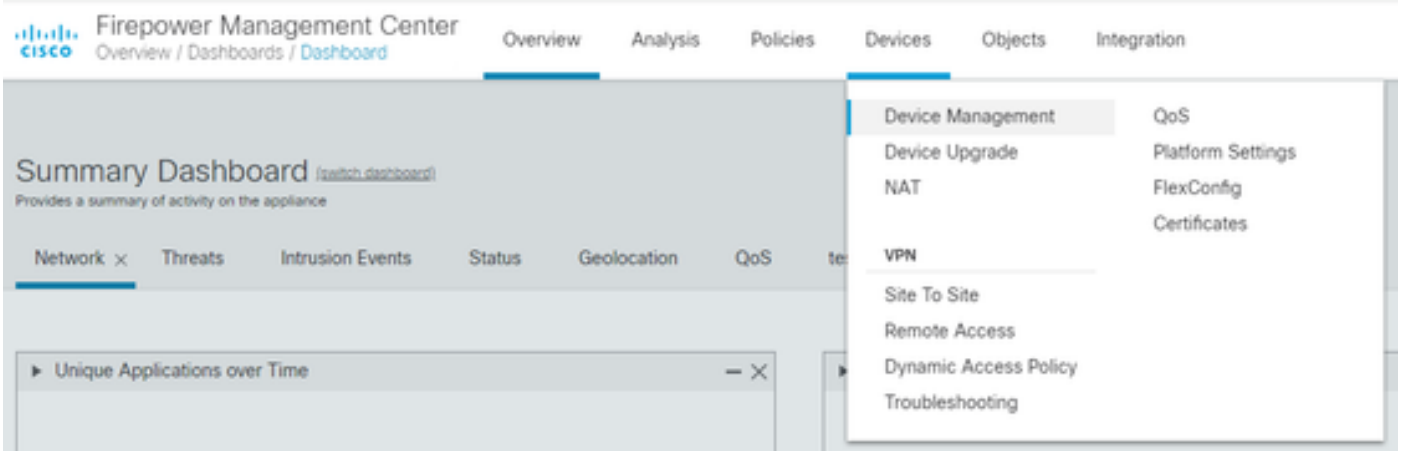
5. Confirme sua seleção.



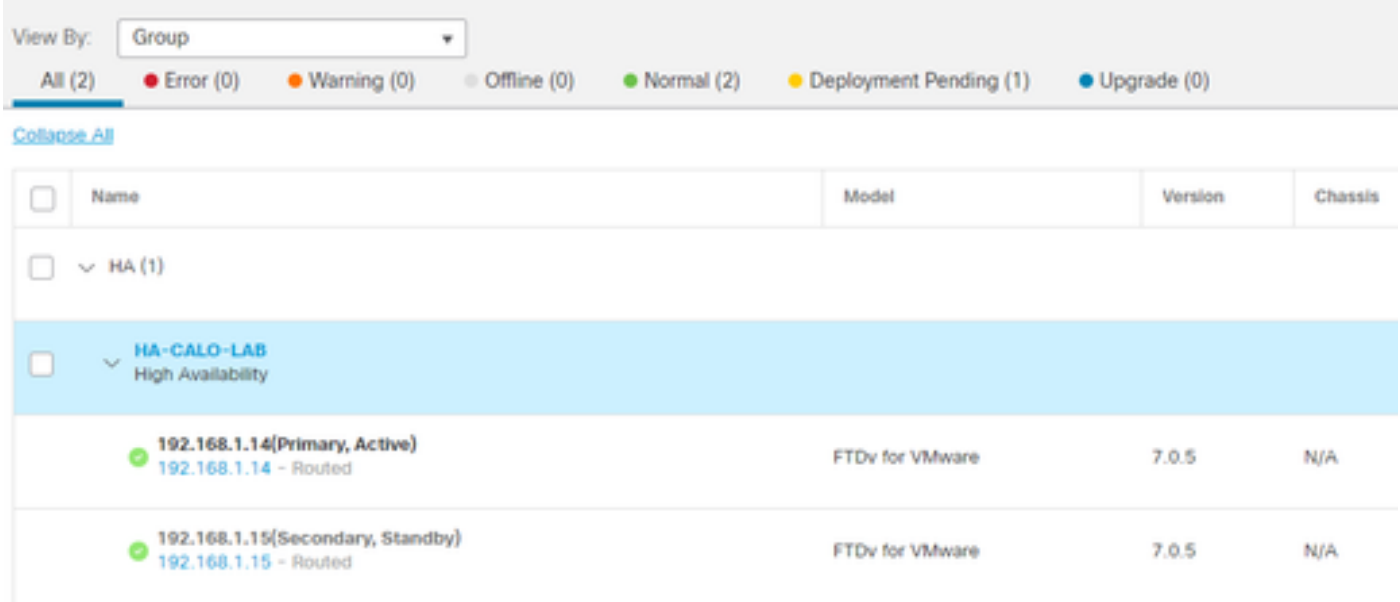
Método 2

1. Faça login no Firepower Management Center.

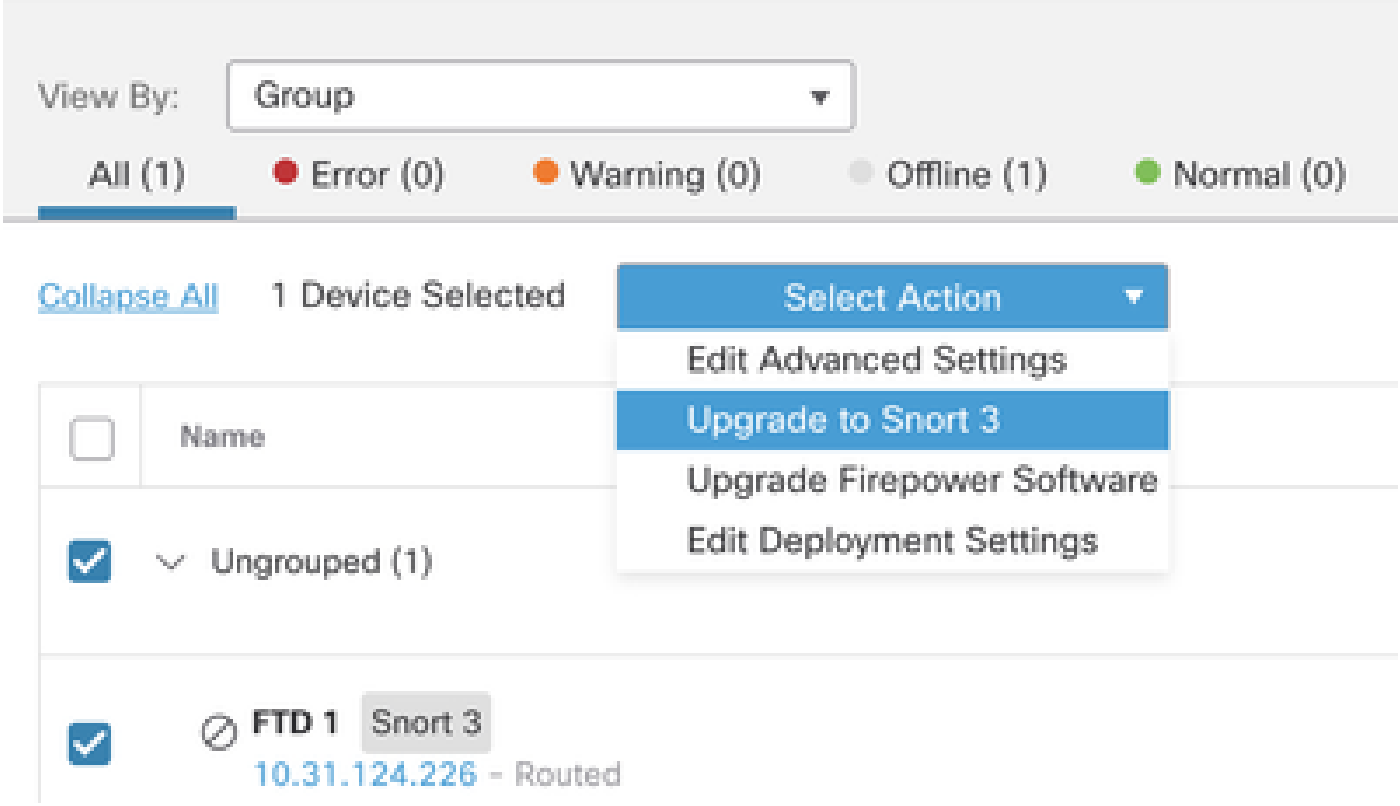
2. Na guia Dispositivo, navegue até Dispositivos > Gerenciador de dispositivos.



3. Selecione o dispositivo cuja versão do Snort você deseja alterar.



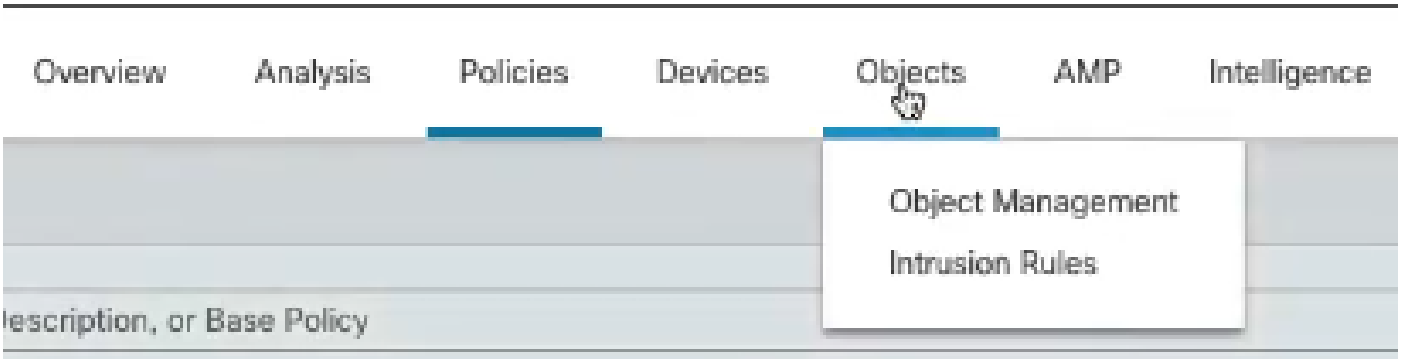
4. Clique no Selecionar Ação botão e selecione Atualizar para Snort 3.



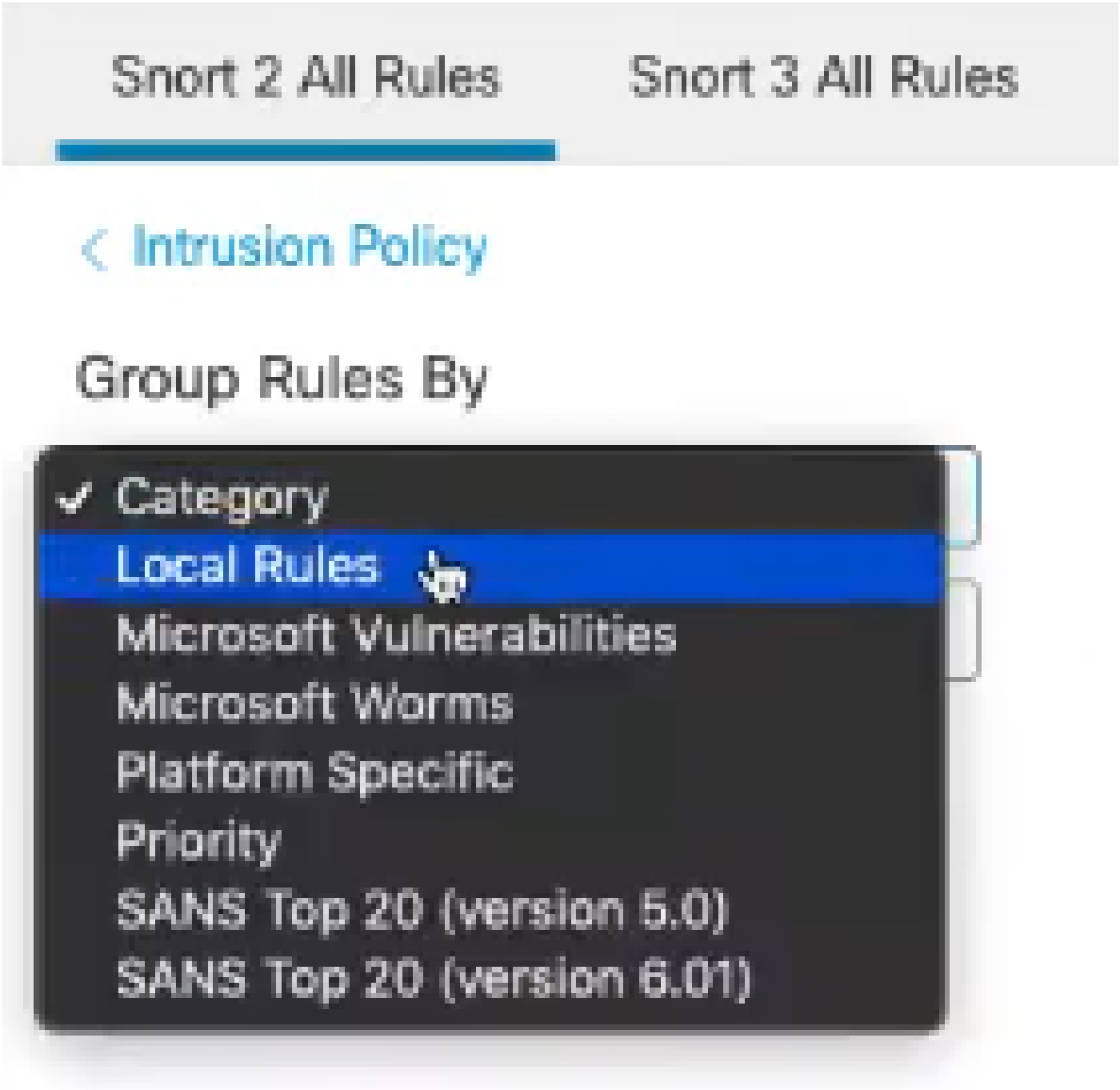
Atualização das regras de intrusão

Além disso, você precisa converter suas regras do Snort 2 em regras do Snort 3.

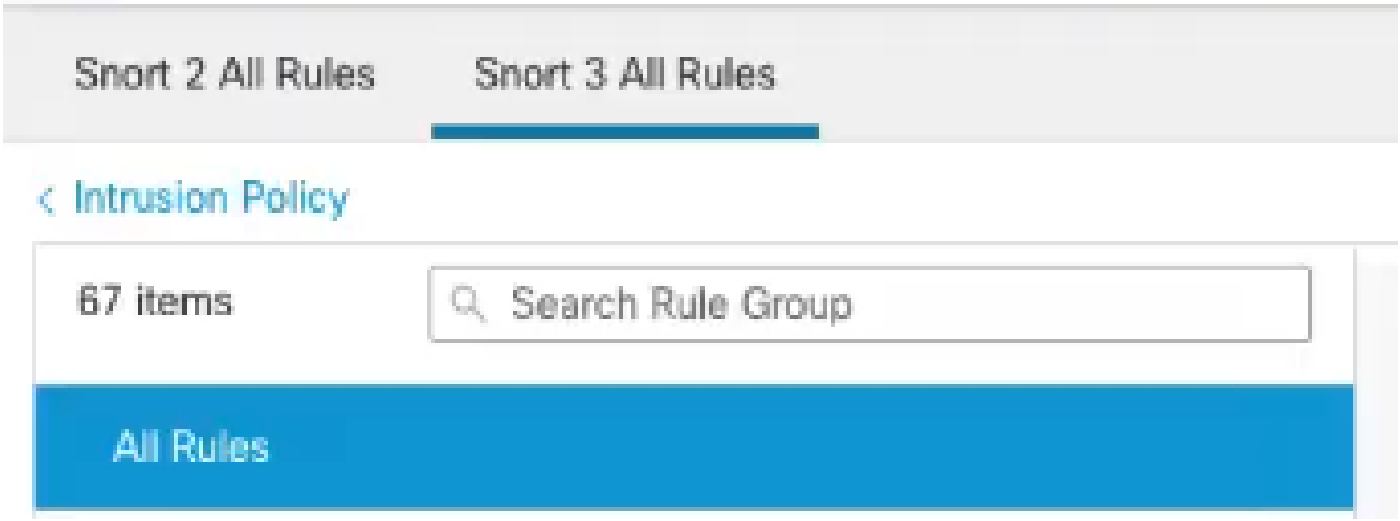
1. Selecione no menu Objetos > Regras de intrusão.



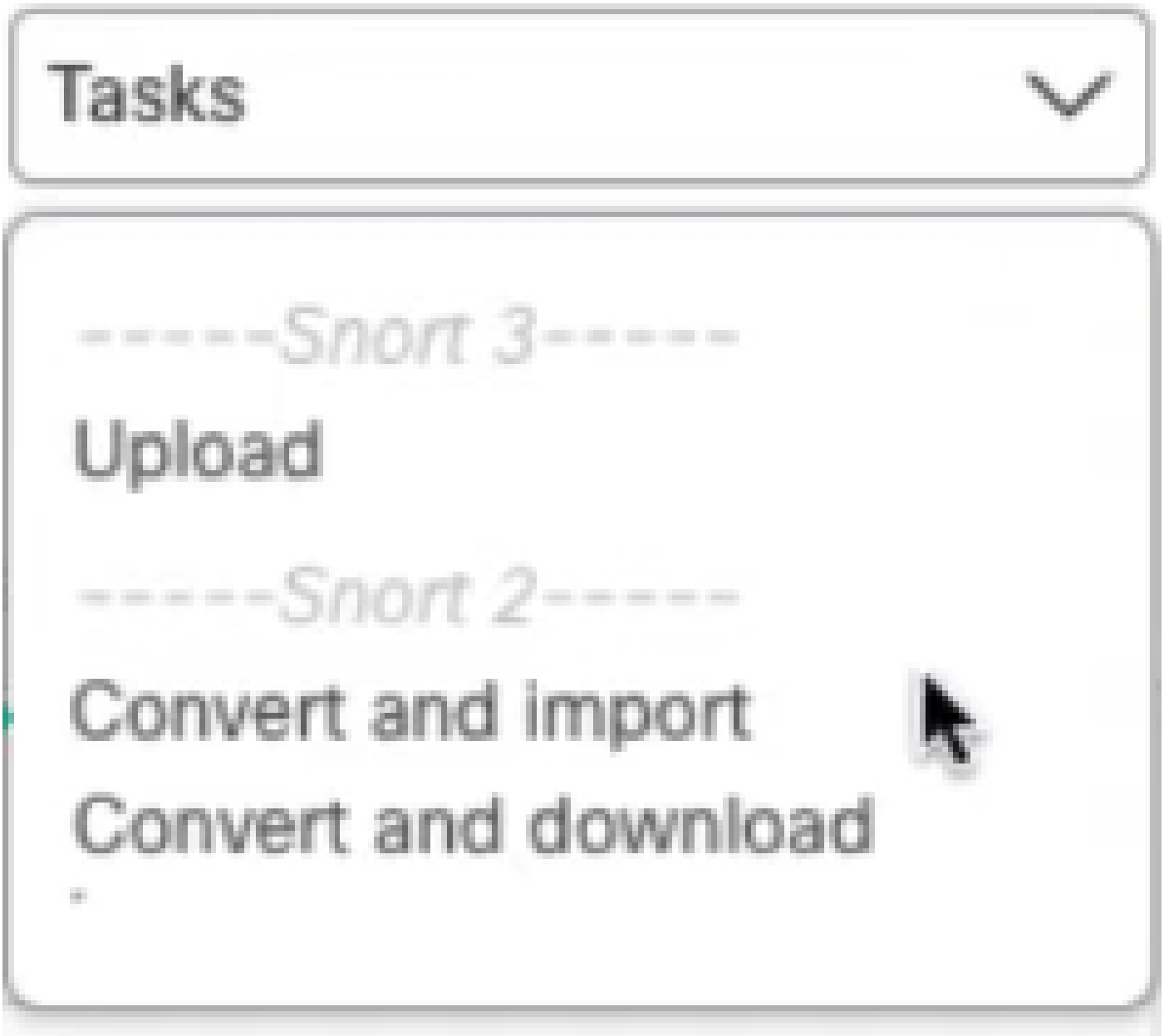
2.Selecione no menu Snort 2 All Rules tab > Group Rules By > Local Rules.



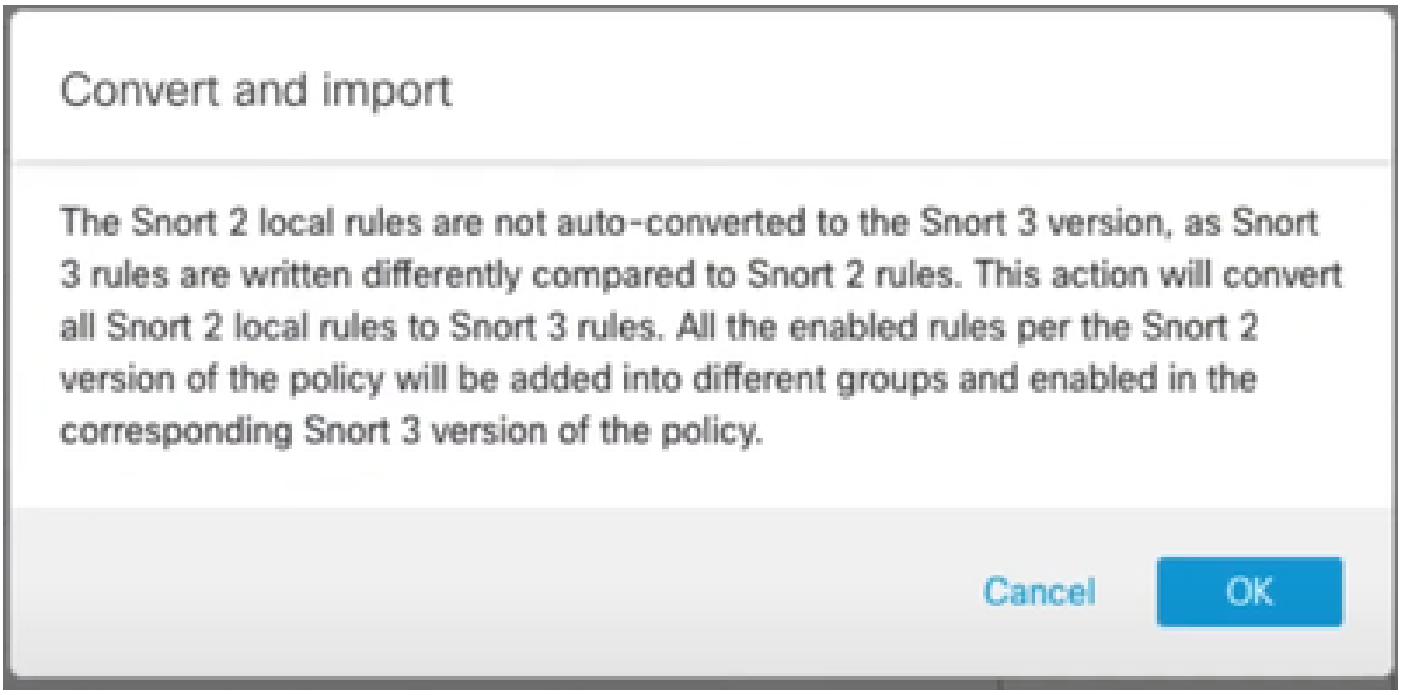
3. Clique em Snort 3 All Rules guia e certifique-se de que All Rules está selecionado.



4.No menu suspenso Task, selecione Convert and import.



5. Clique em OK na mensagem de advertência.

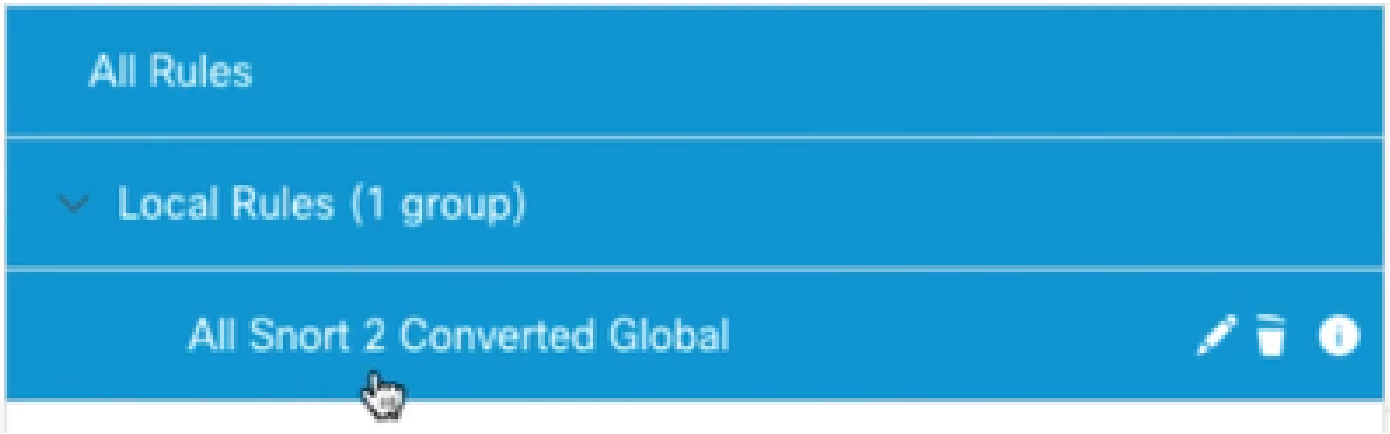


Verificar

A seção Mecanismo de inspeção mostra que a versão atual do Snort é Snort 3.

A conversão da regra foi bem-sucedida quando você recebeu esta mensagem:

Finalmente, você deve encontrar no Local Rules grupo a seção All Snort 2 Converted Global , que contém todas as suas regras Snort 2 para Snort 3 convertidas.



Troubleshooting

Caso a migração falhe ou trave, reverta para o Snort 2 e tente novamente.

Informações Relacionadas

- Como migrar do Snort 2 para o Snort 3
- Cisco Secure - Atualização de Snort 3 Dispositivos (Vídeo Externo no YouTube)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.