Aggiornamento da Snort 2 a Snort 3 tramite FMC

Sommario

Introduzione

In questo documento viene descritto come eseguire l'aggiornamento dalle versioni Snort 2 e Snort 3 in Firepower Manager Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense
- Firepower Management Center
- Snort

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FMC 7.0
- FTD 7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

La funzione Snort 3 è stata aggiunta nella versione 6.7 per Firepower Device Manager (FDM) e Cisco Defense Orchestrator (CDO); nella versione 7.0 per Firepower Management Center (FMC).

Snort 3.0 è stato progettato per affrontare queste sfide:

1. Riduzione dell'utilizzo della memoria e della CPU.
2. Migliorare l'efficacia dell'ispezione HTTP.
3. Caricamento più rapido della configurazione e riavvio automatico.
4. Migliore programmabilità per una più rapida aggiunta di funzionalità.

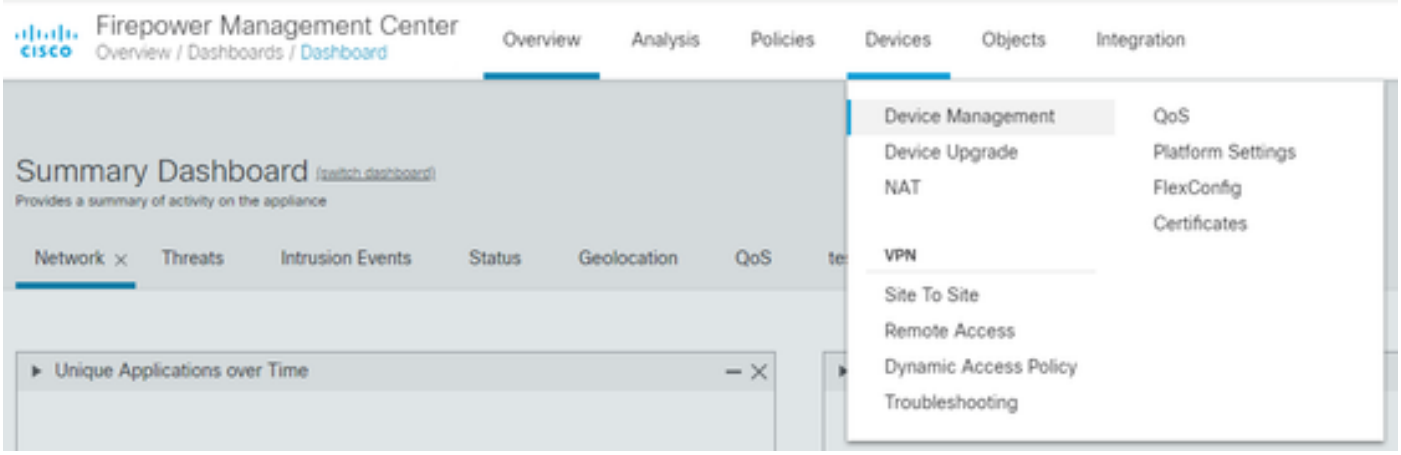
Configurazione

Aggiorna la versione Snort

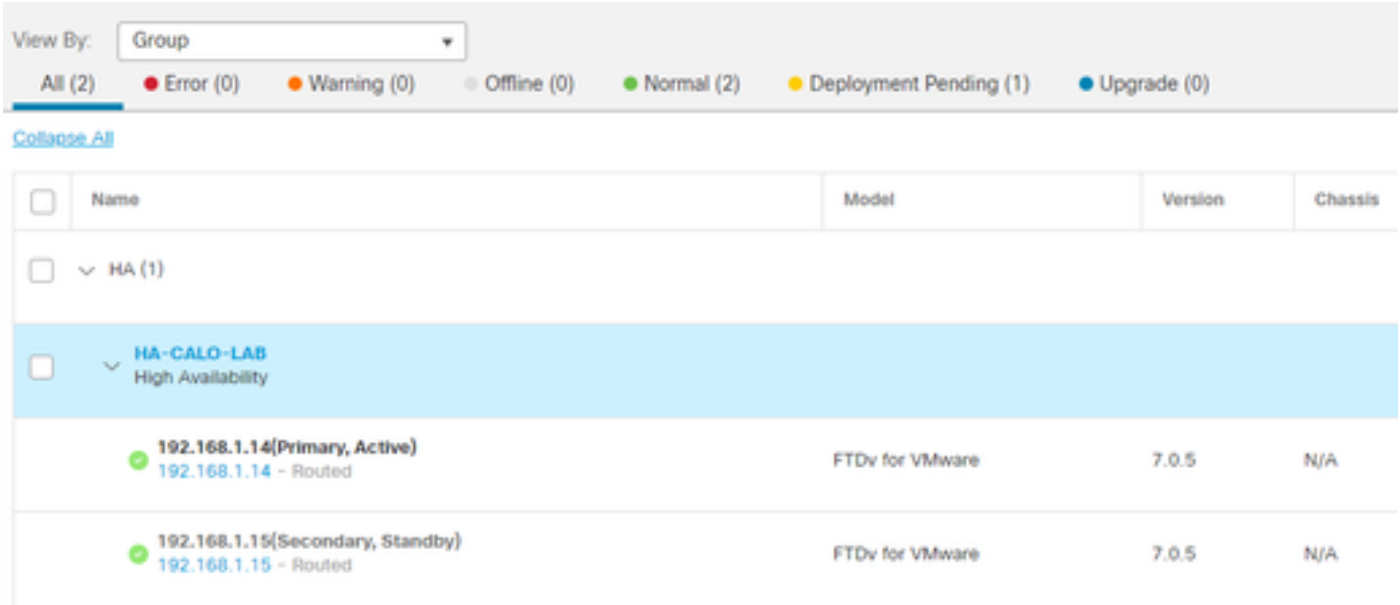
Metodo 1

1. Accedere a Firepower Management Center.

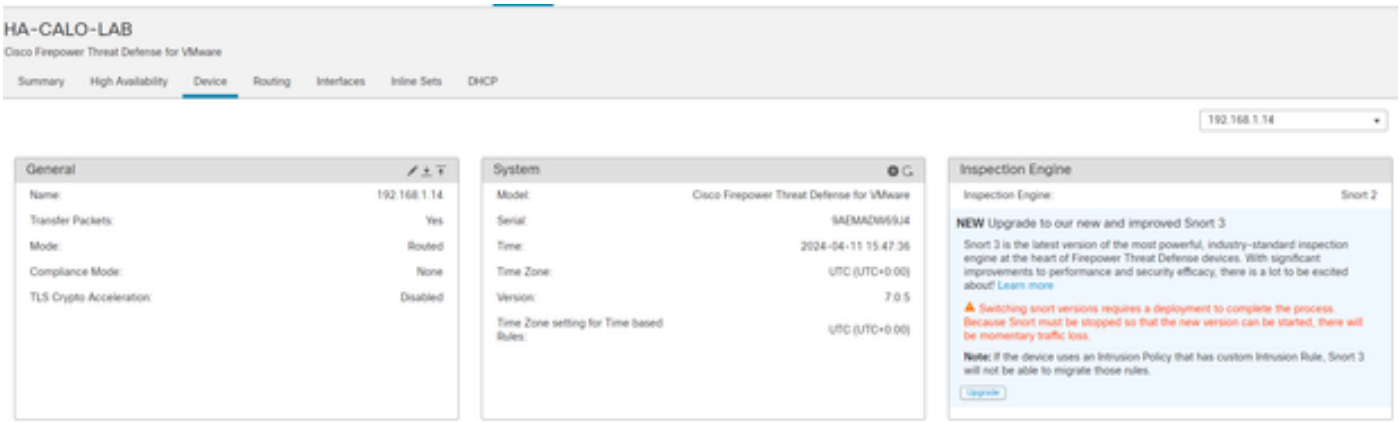
2. Nella scheda Periferica passare a Periferiche > Gestione periferiche.



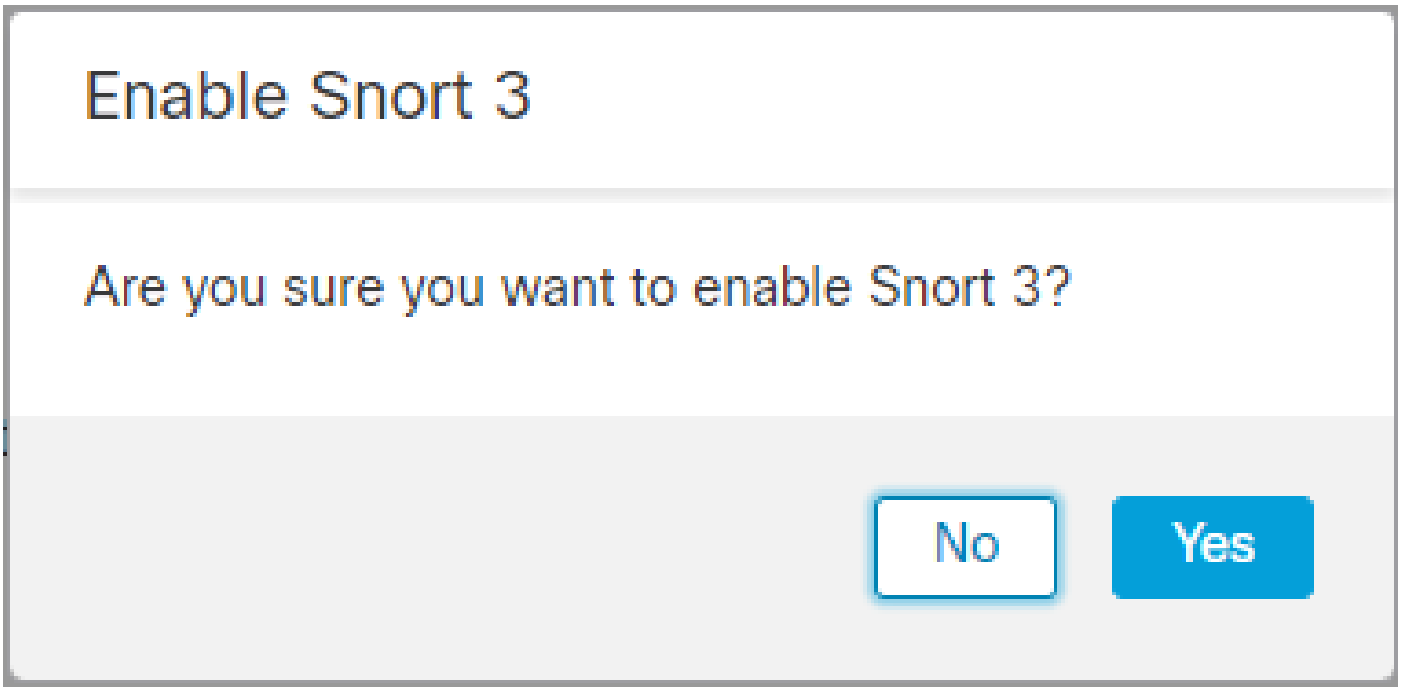
3. Selezionare il dispositivo di cui si desidera modificare la versione Snort.



4. Fare clic sulla scheda Periferica e fare clic sul pulsante Aggiorna nella sezione Motore di ispezione.



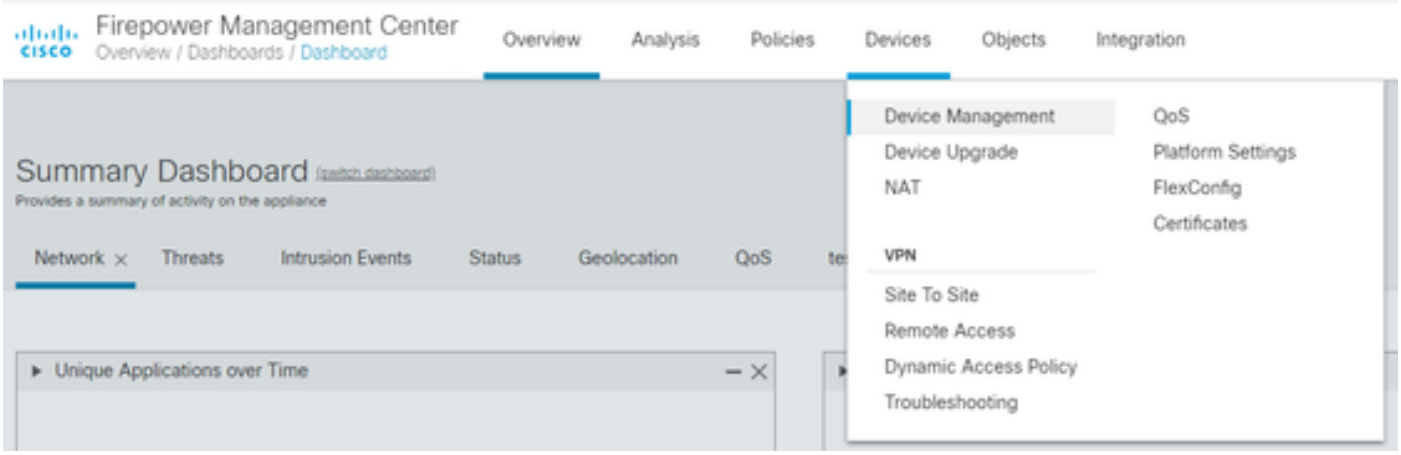
5. Confermare la selezione.



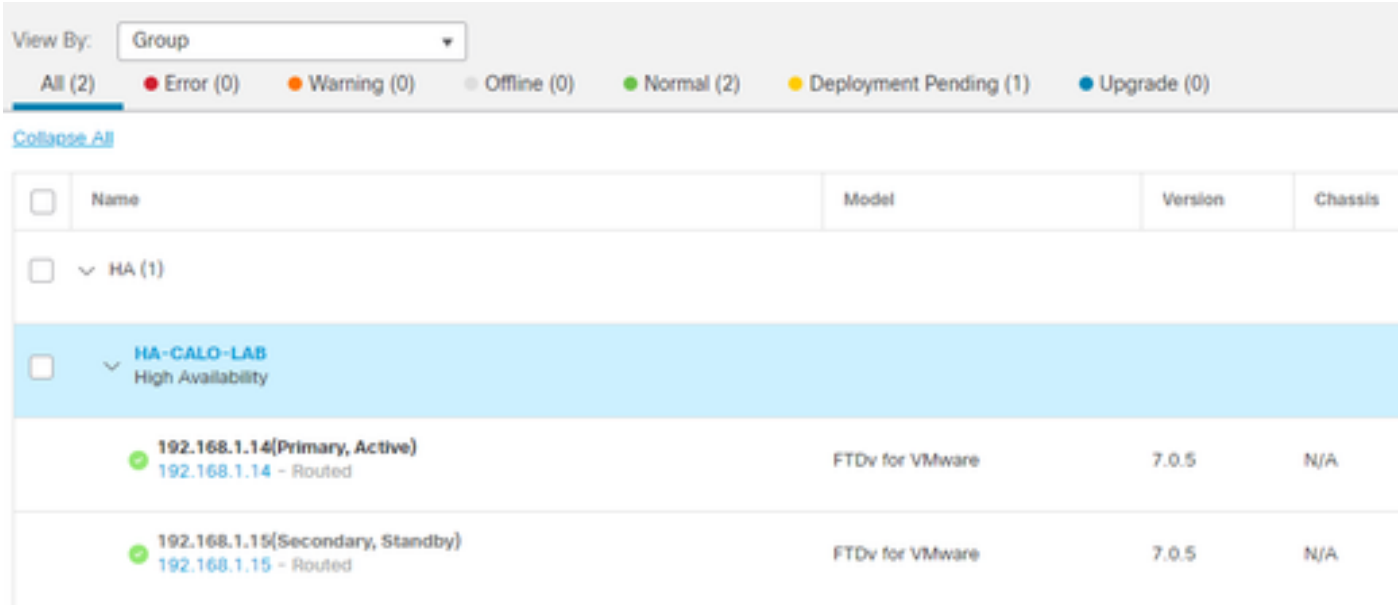
Metodo 2

1. Accedere a Firepower Management Center.

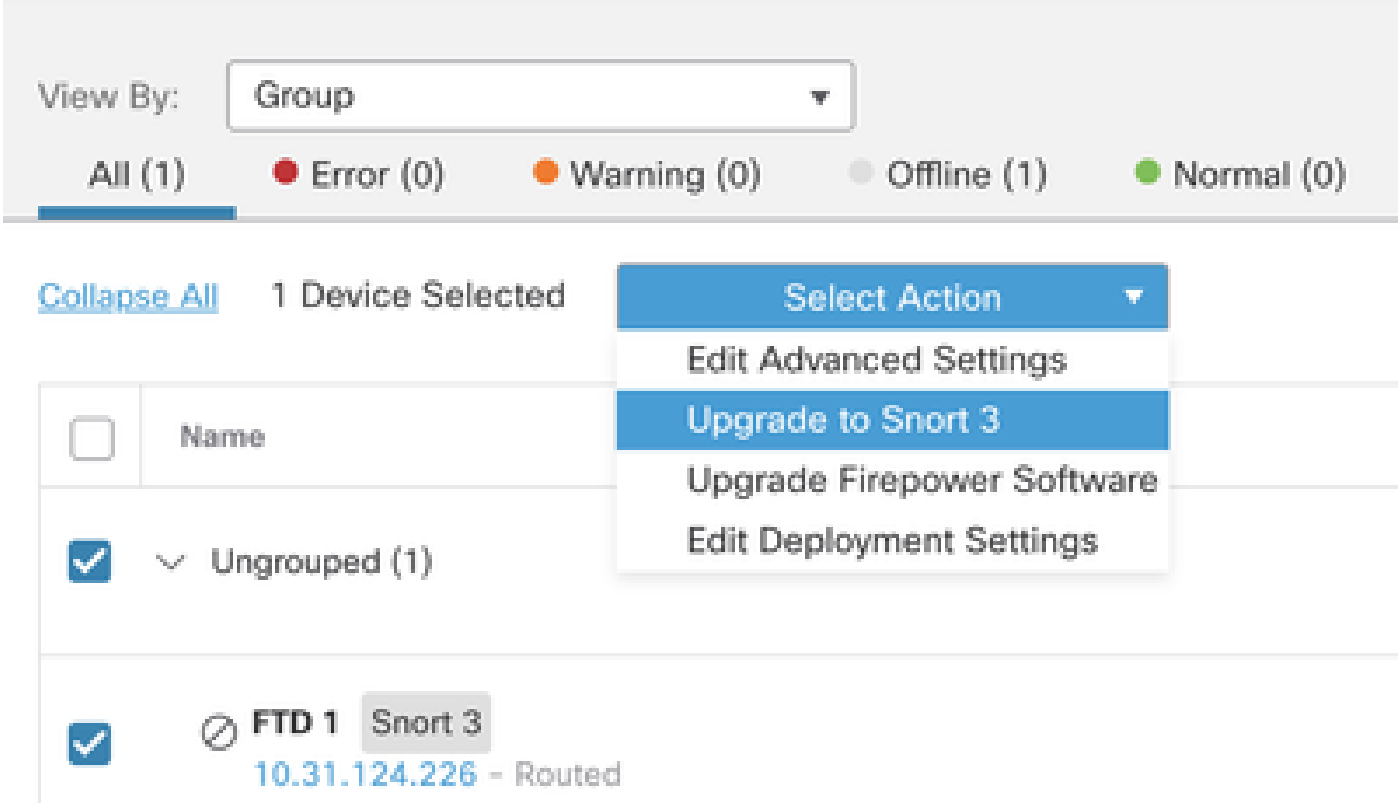
2. Nella scheda Periferica passare a Periferiche > Gestione periferiche.



3. Selezionare il dispositivo di cui si desidera modificare la versione Snort.



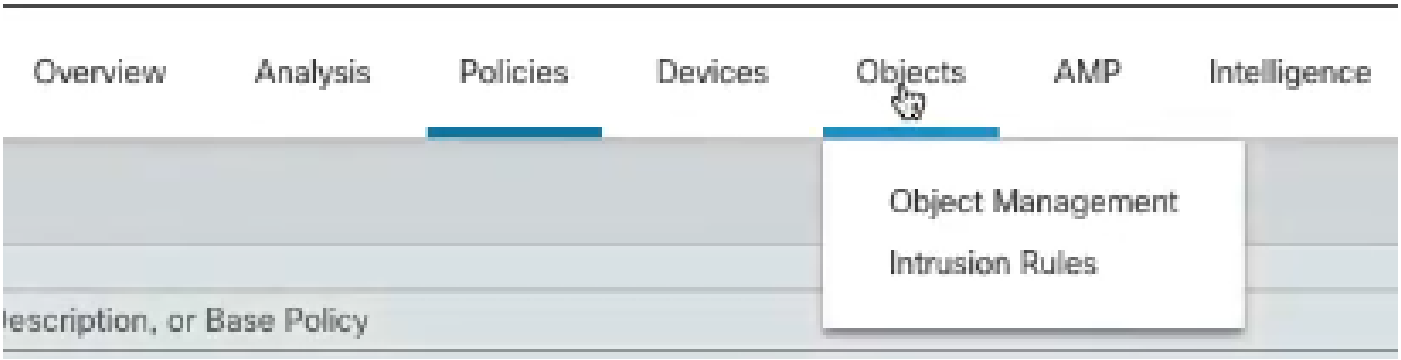
4. Fare clic sul pulsante Seleziona azione e selezionare Aggiorna a Snort 3.



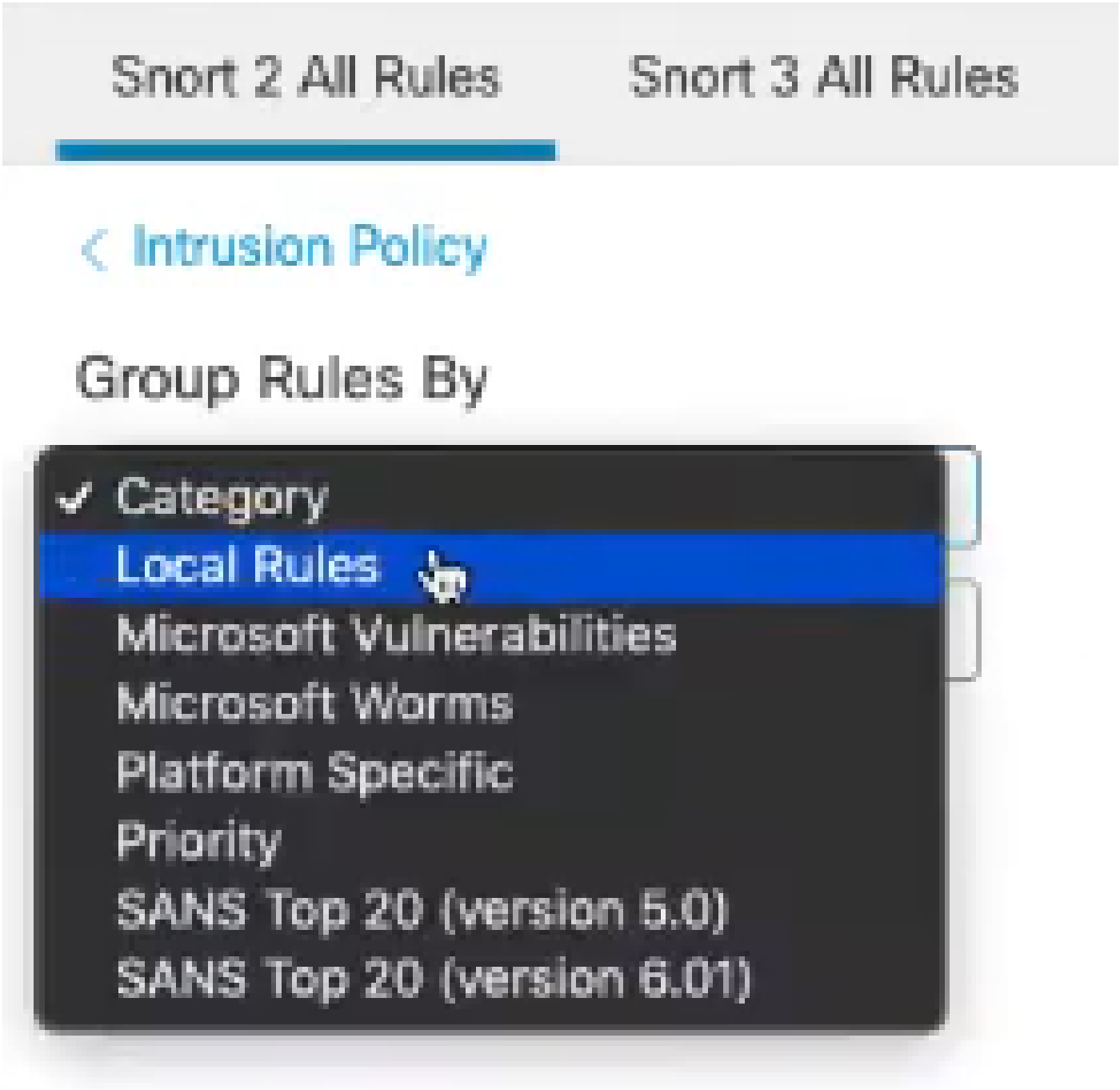
Aggiornamento delle regole di intrusione

Inoltre, è necessario convertire le regole Snort 2 in regole Snort 3.

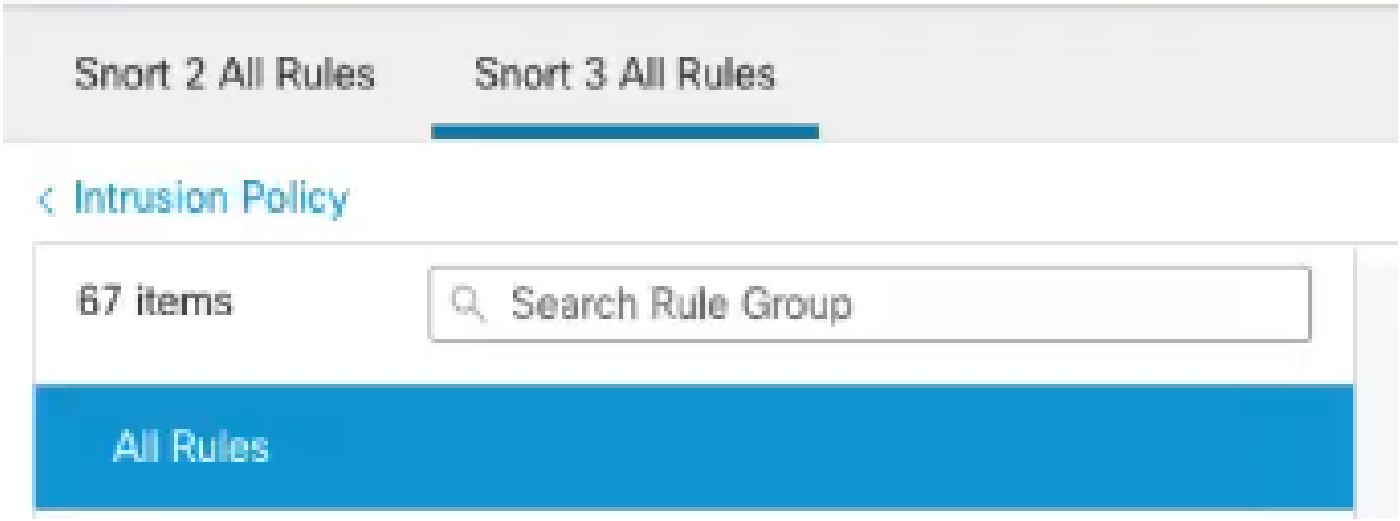
1. Selezionate dal menu Oggetti > Regole intrusione.



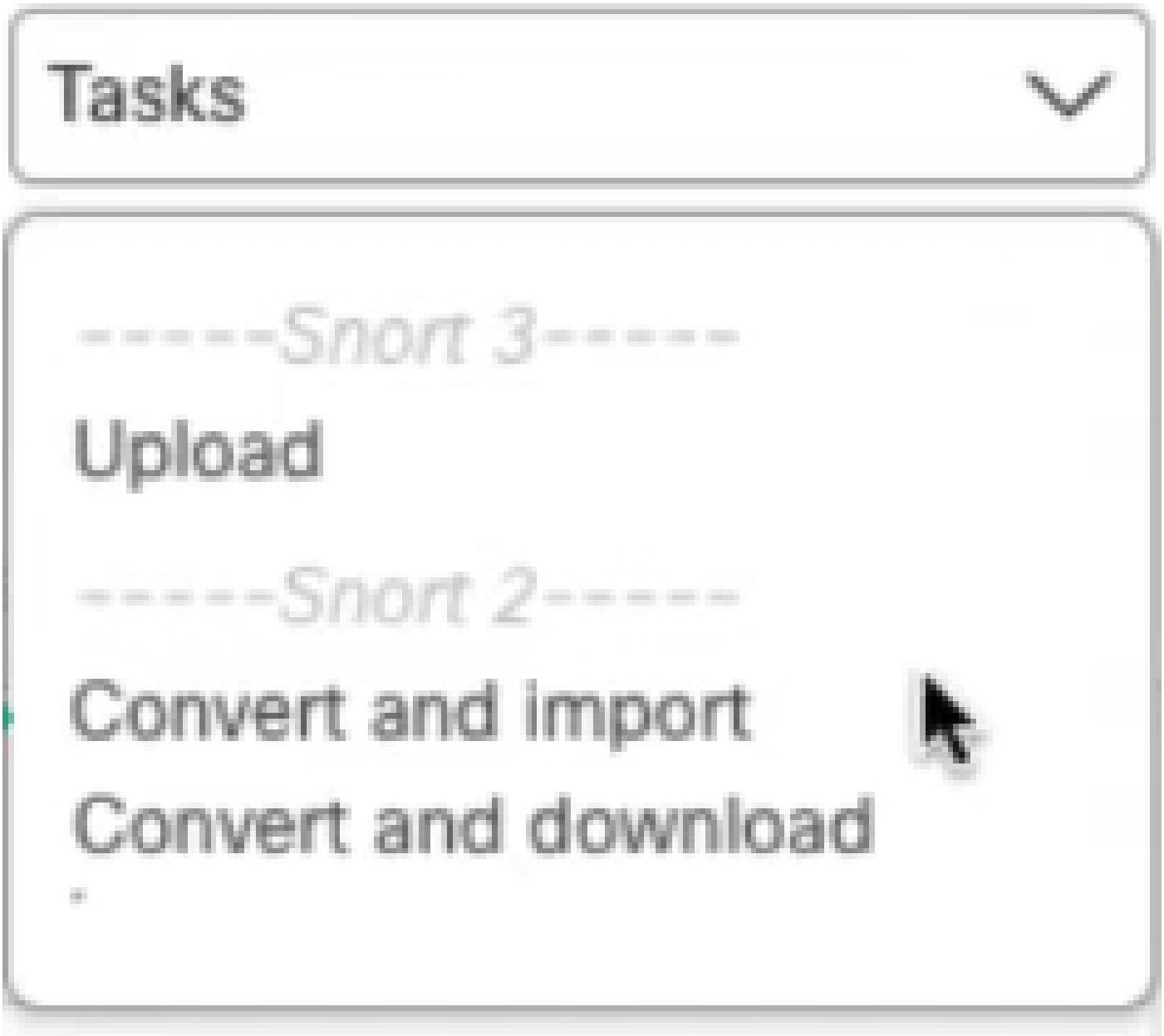
2.Selezionare dal menu Ordina 2 tutte le regole scheda > Raggruppa regole per > Regole locali.



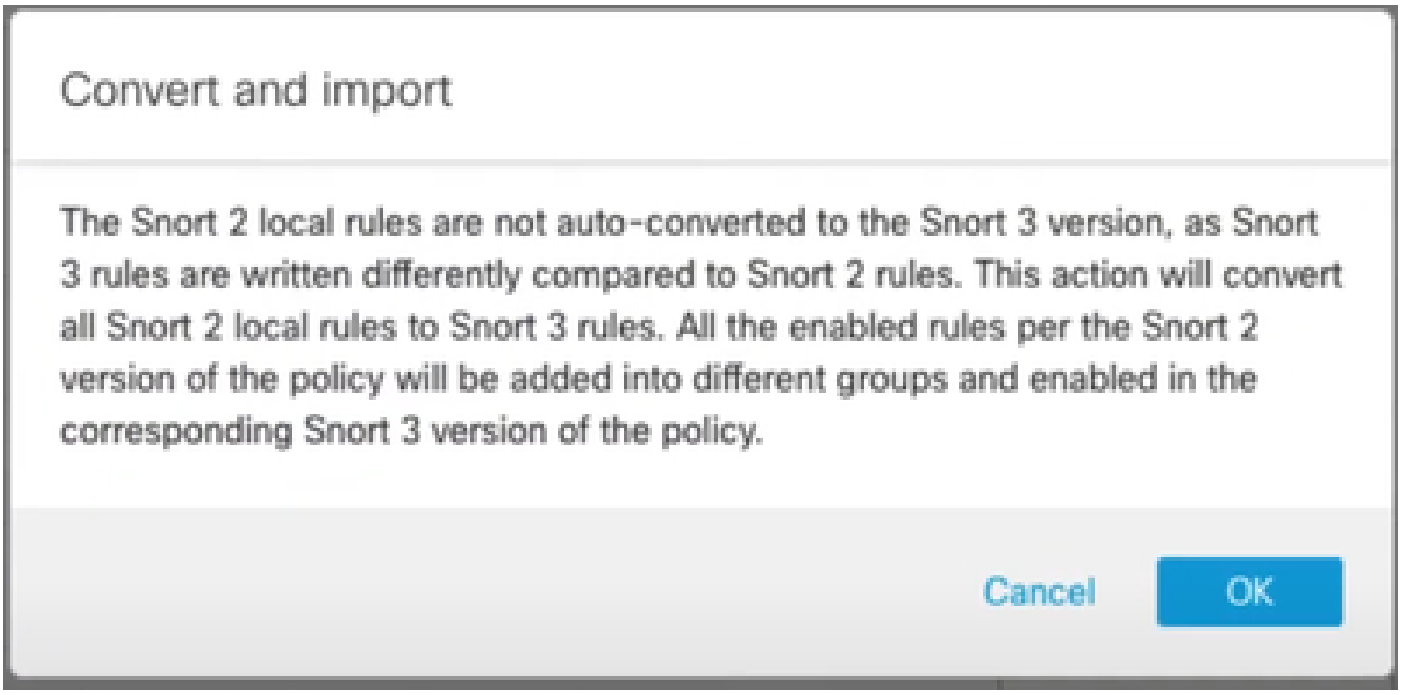
3. Fare clic su Ordina 3 Tutte le regole scheda e assicurarsi che Tutte le regole sia selezionato.



4.Dal menu a discesa Task, selezionare Converti e importa.



5. Fare clic su OK sul messaggio di avvertenza.

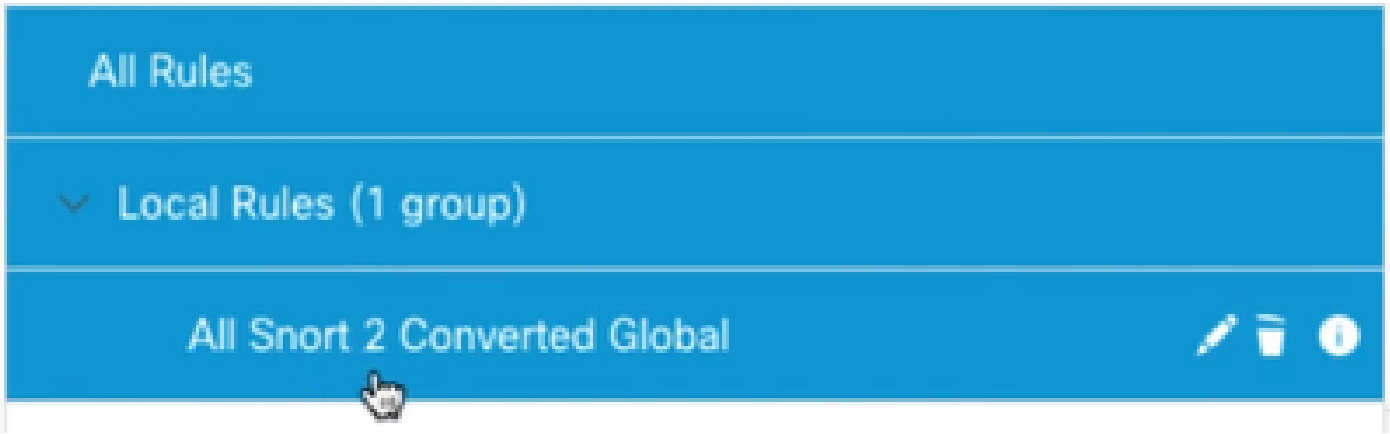


Verifica

La sezione Motore di ispezione mostra che la versione corrente di Snort è Snort 3.

La conversione della regola è riuscita quando viene visualizzato questo messaggio:

Infine, nel gruppo Regole locali è necessario trovare la sezione All Snort 2 Converted Global contenente tutte le regole convertite da Snort 2 a Snort 3.



Risoluzione dei problemi

Se la migrazione non riesce o si interrompe, eseguire il rollback allo Snort 2 e riprovare.

Informazioni correlate

- Migrazione da Snort 2 a Snort 3
- Cisco Secure - Aggiornamento dispositivo Snort 3 (video esterno di YouTube)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).