Upgrade van Snort 2 naar Snort 3 via FMC

Inhoud

Inleiding

In dit document wordt beschreven hoe u kunt upgraden van de versie Snort 2 en Snort 3 in Firepower Manager Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defence
- Firepower Management Center
- Snort

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VCC 7.0
- FTD 7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De functie Snort 3 is toegevoegd in de 6.7-release voor Firepower Device Manager (FDM) en Cisco Defense Orchestrator (CDO), in de 7.0-release voor het Firepower Management Center (FMC).

Snort 3.0 is ontworpen om deze uitdagingen aan te gaan:

1. Minder geheugen en minder CPU-gebruik.
2. Verbeter de HTTP-inspectie-efficiëntie.
3. Snellere configuratie laden en Snelstart opnieuw starten.
4. Betere programmeerbaarheid voor snellere toevoeging van extra functies.

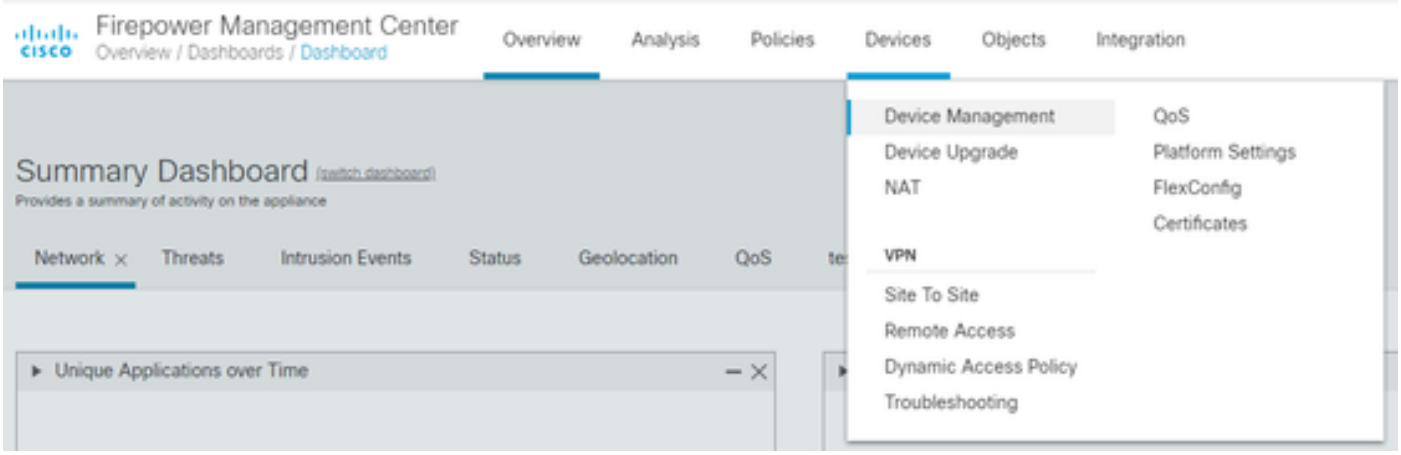
Configureren

Upgrade de Snelversie

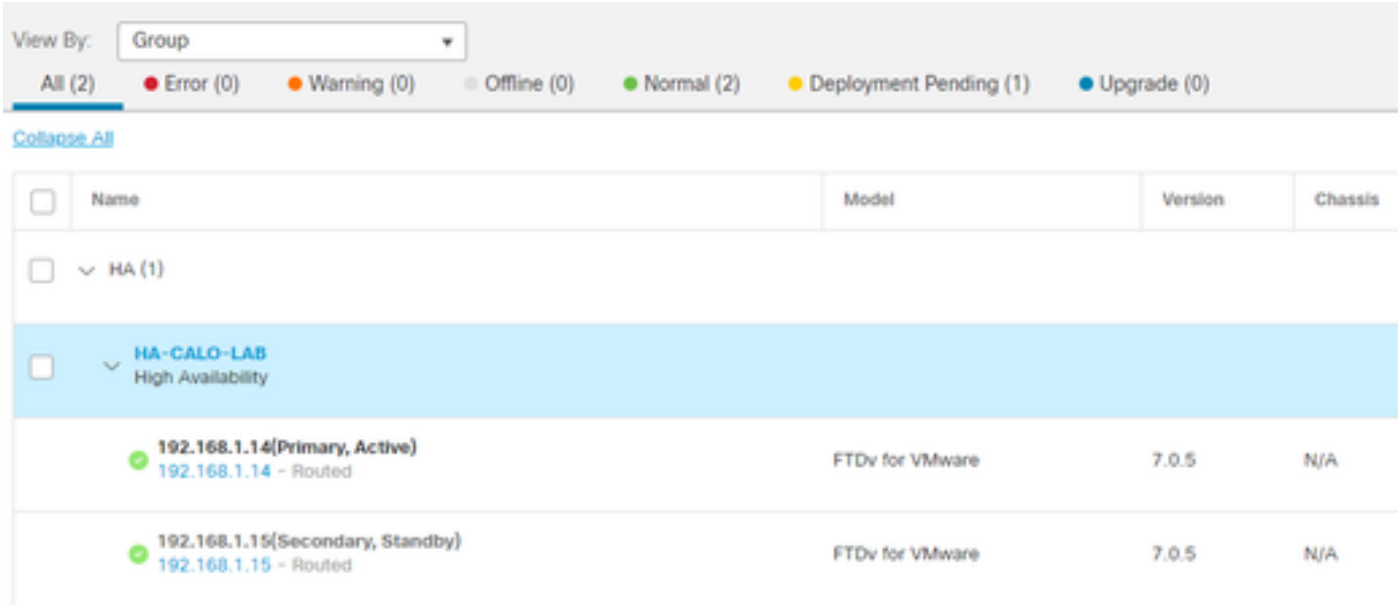
Methode 1

1. Meld u aan bij Firepower Management Center.

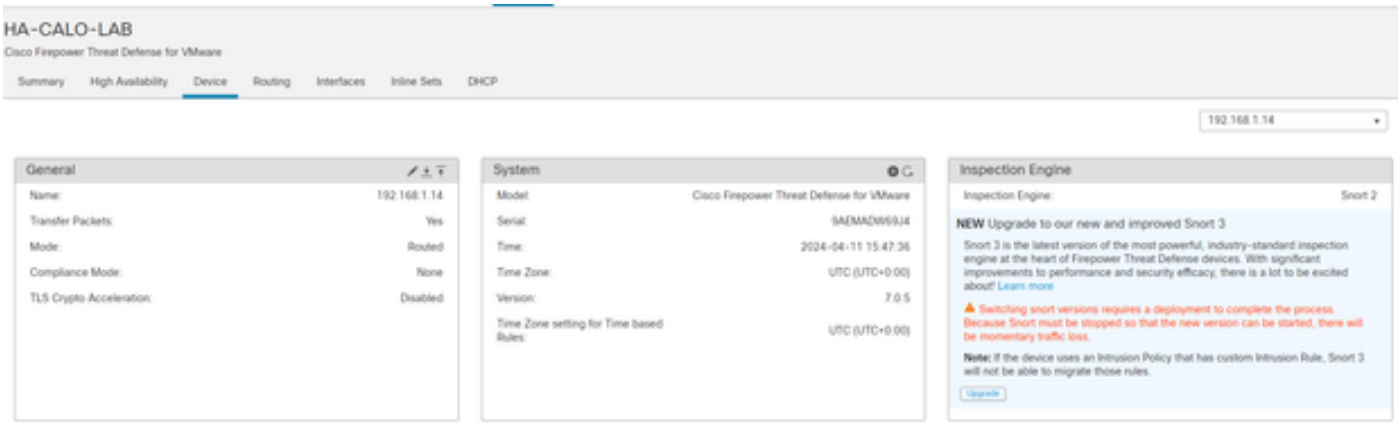
2. Ga op het tabblad Apparaat naar Apparaten > Apparaatbeheer.



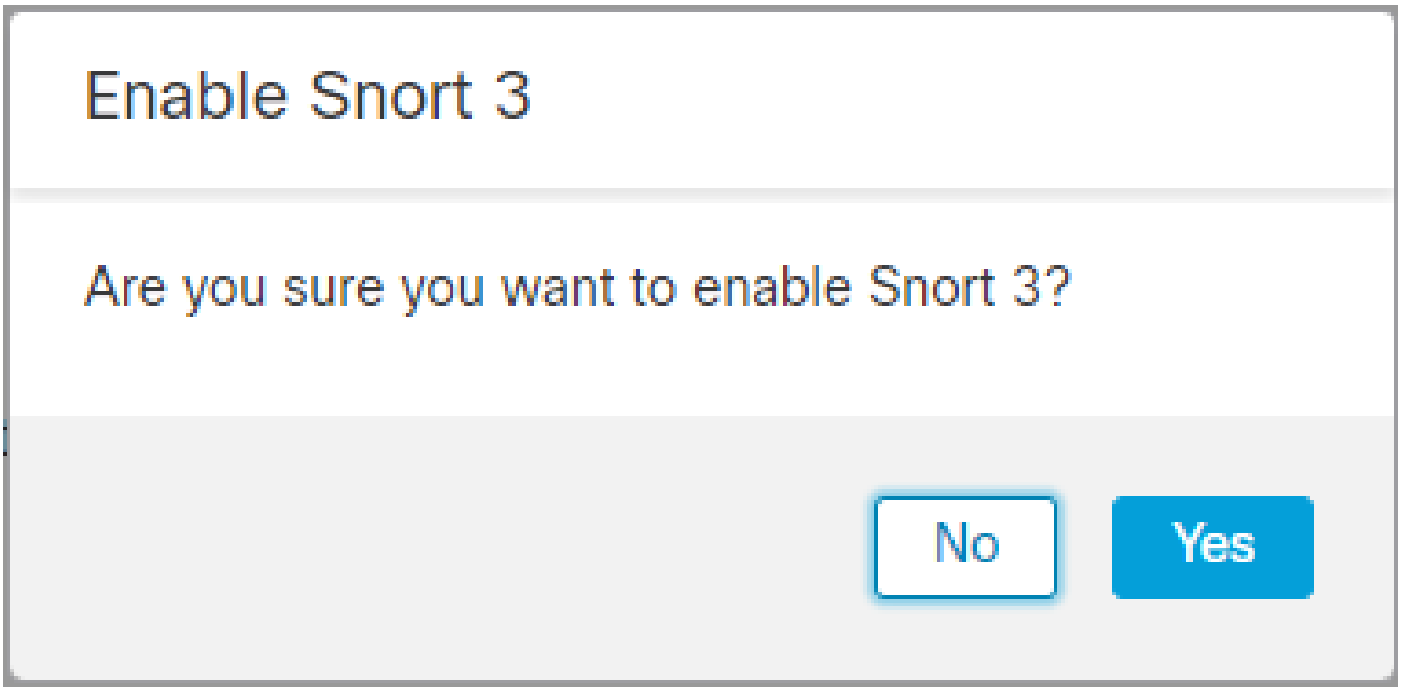
3. Selecteer het apparaat dat u de gescande versie wilt wijzigen.



4. Klik op het tabblad Apparaat en klik op de knop Upgrade in het gedeelte Inspection Engine.



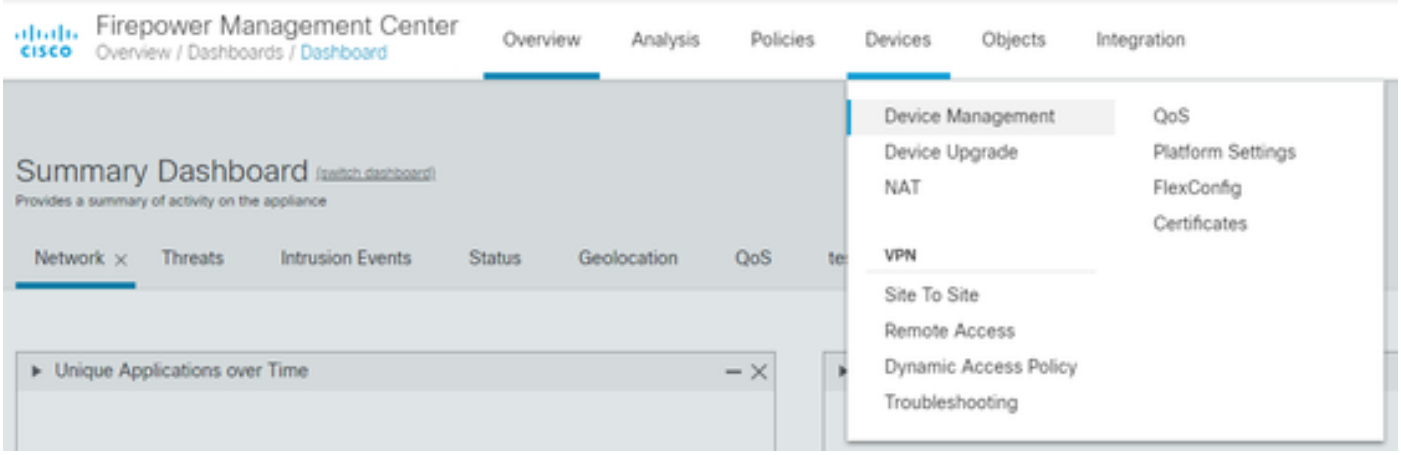
5. Bevestig uw selectie.



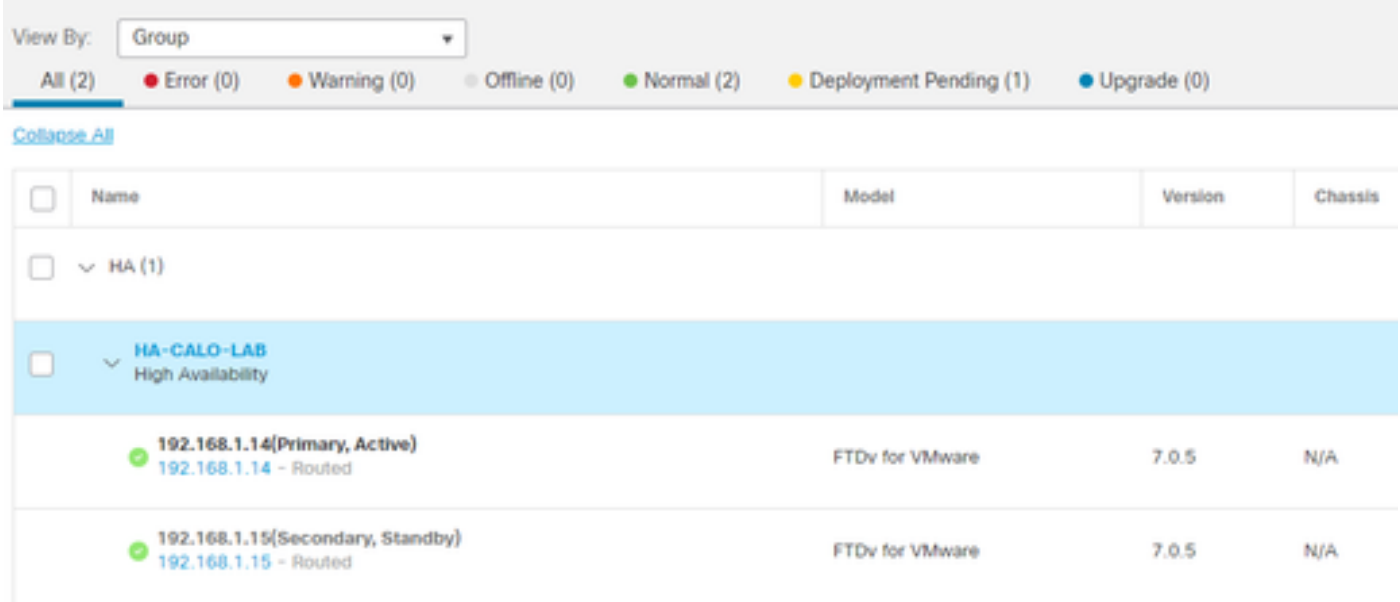
Methode 2

1. Meld u aan bij Firepower Management Center.

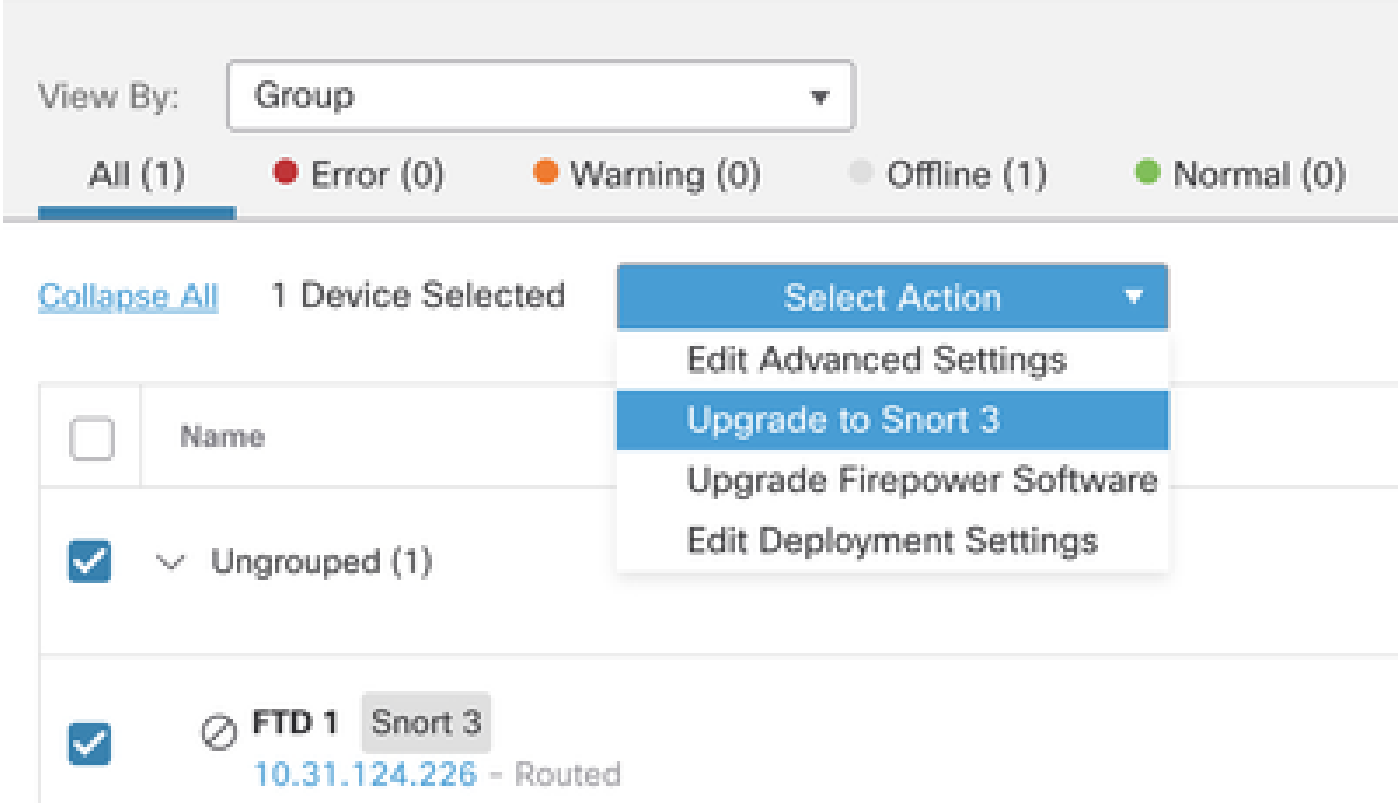
2. Ga op het tabblad Apparaat naar Apparaten > Apparaatbeheer.



3. Selecteer het apparaat dat u de gescande versie wilt wijzigen.



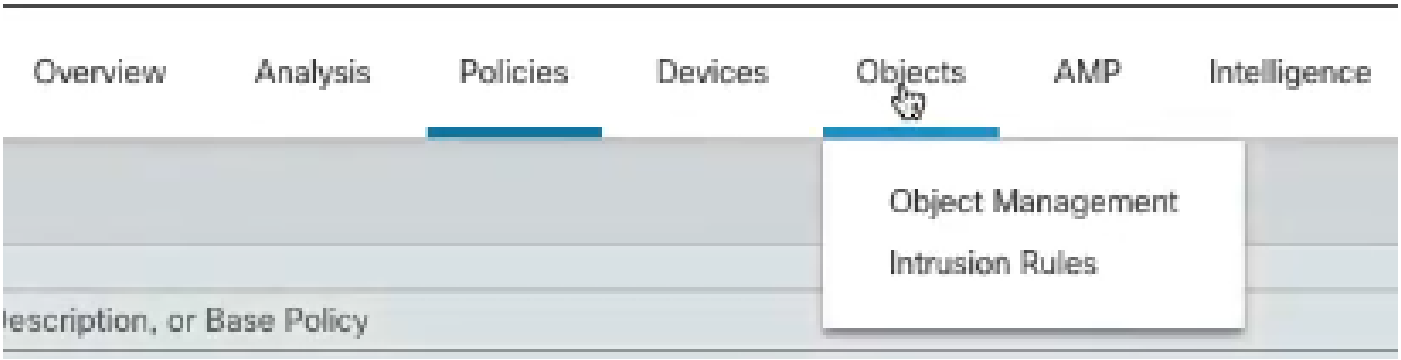
4. Klik op de knop Actie selecteren en selecteer Upgrade naar snurk 3.



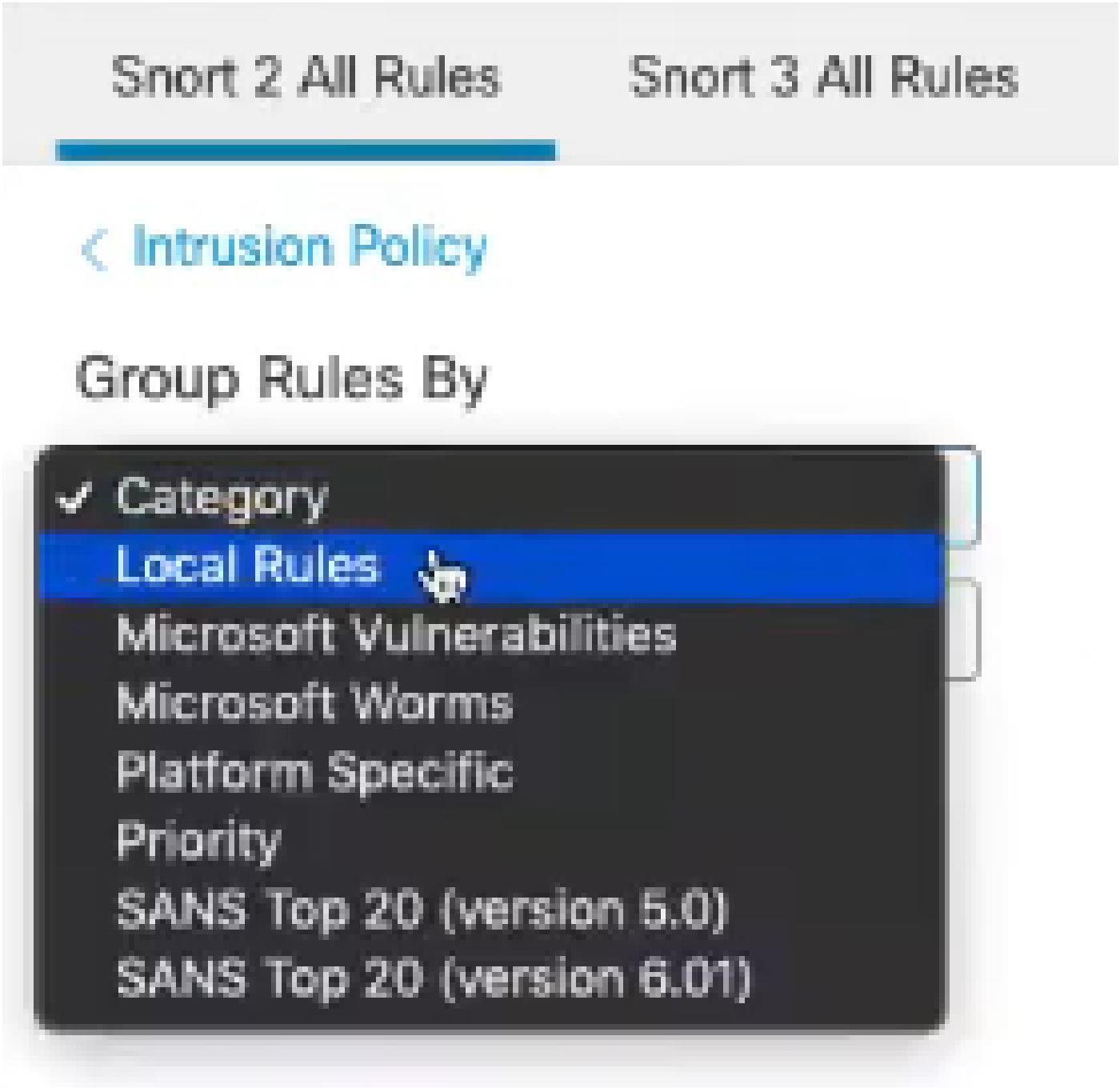
Upgrade van inbraakregels

Daarnaast moet u uw Snort 2 regels omzetten in Snort 3 regels.

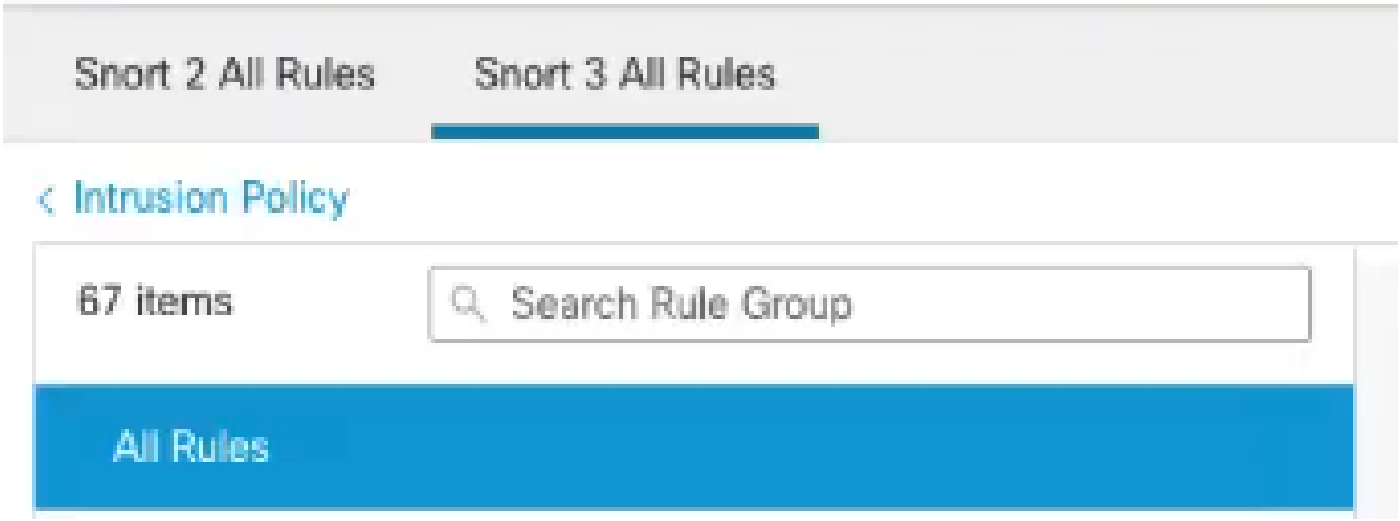
1. Selecteer in het menu Objecten > Inbraakregels.



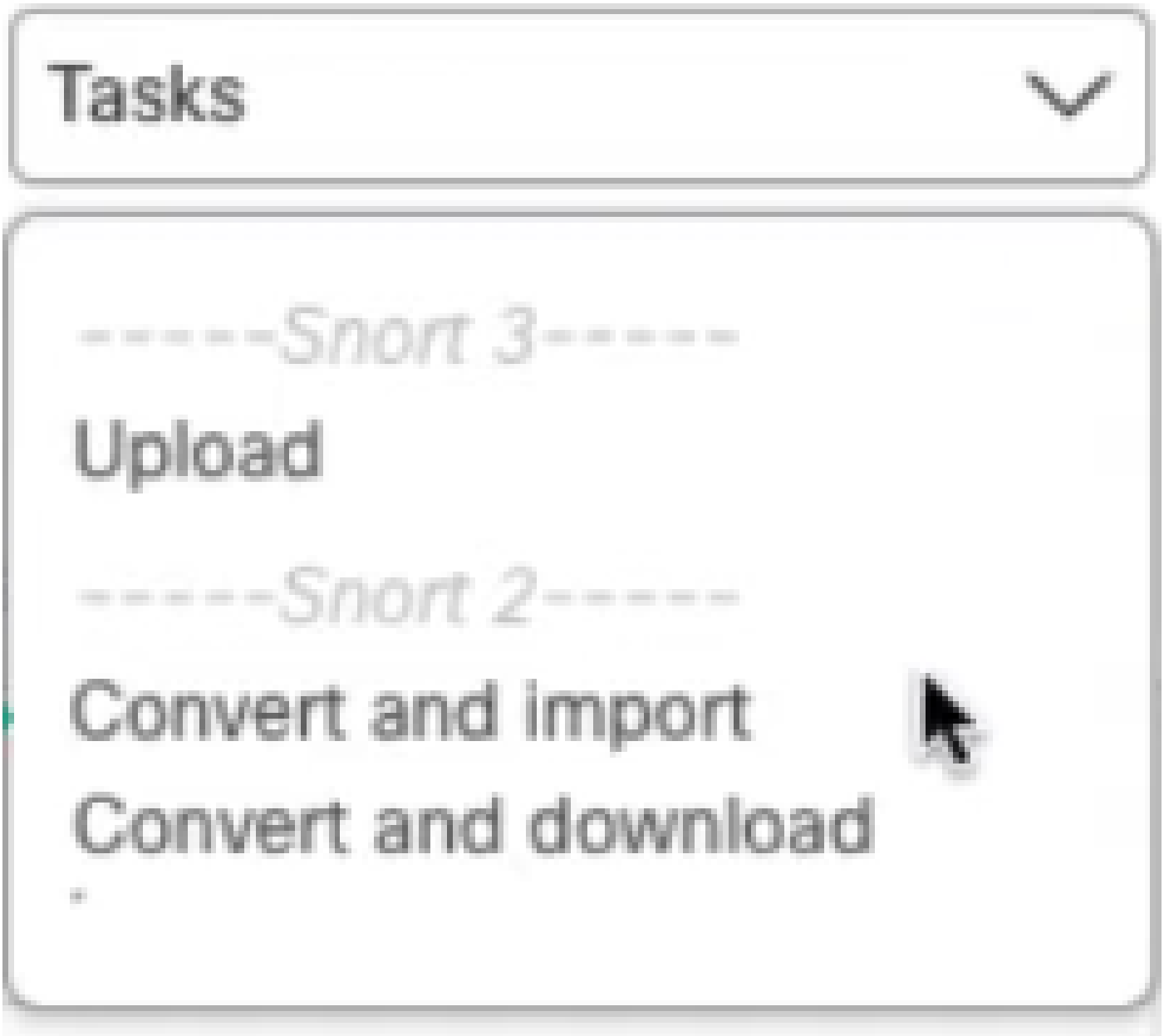
2. Selecteer in het menu Sneltoets 2 All Rules > Group Rules By > Local Rules.



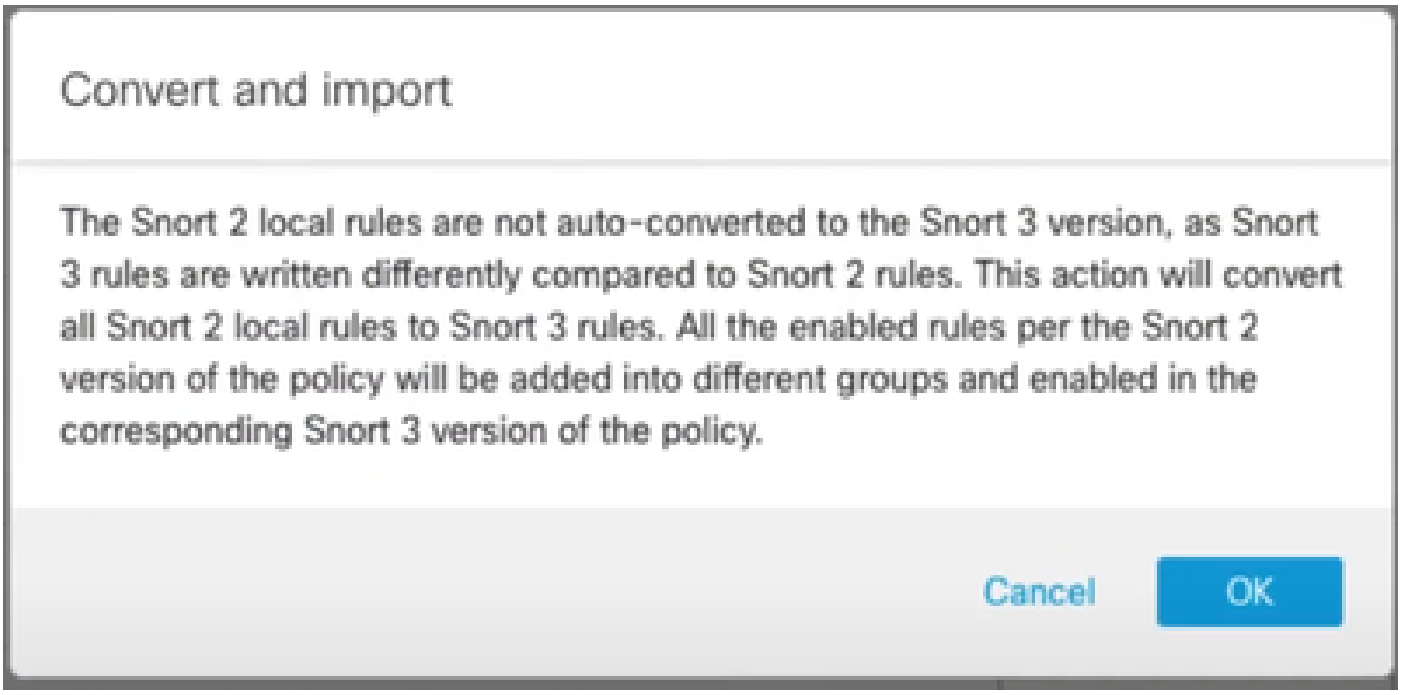
3. Klik op Sneltoets 3 Alle regels en zorg ervoor dat Alle regels is geselecteerd.



4. Selecteer in het vervolgkeuzemenu Taak de optie Omzetten en importeren.



5. Klik op OK in het waarschuwingsbericht.

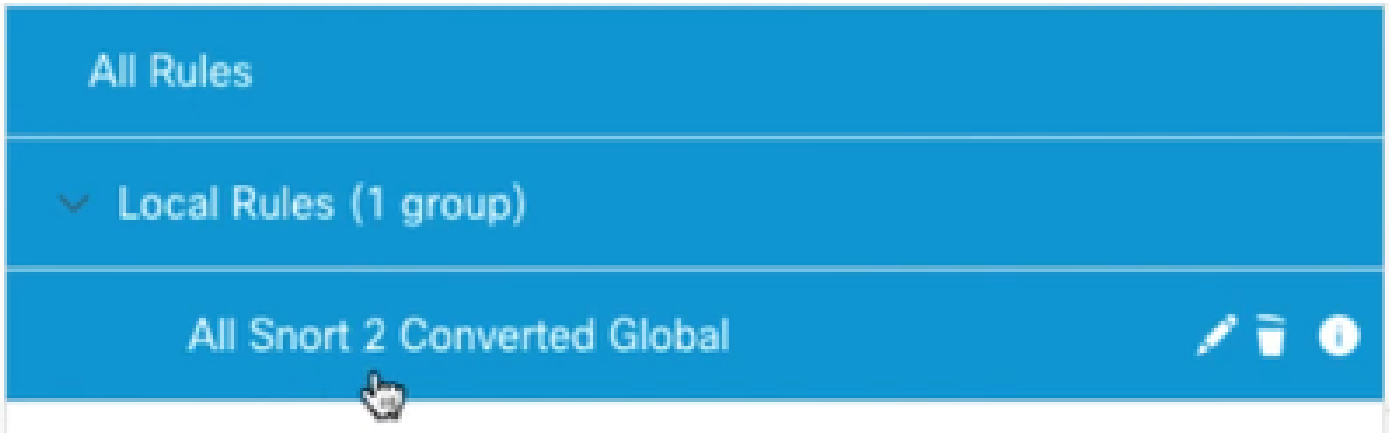


Verifiëren

De sectie Inspection Engine laat zien dat de huidige versie van Snort Snort 3 is.

De regelconversie is voltooid zodra u dit bericht ziet:

Tot slot moet u in de groep Local Rules de sectie All Snort 2 Converted Global vinden, die al uw geconverteerde regels Snort 2 tot Snort 3 bevat.



Probleemoplossing

Als de migratie mislukt of crasht, draait u terug naar Snuit 2 en probeert u het opnieuw.

Gerelateerde informatie

- Hoe te migreren van Snort 2 naar Snort 3
- Cisco Secure - Video voor snort-3 apparaat (externe YouTube-video)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.