

透過FMC從Snort 2升級到Snort 3

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[升級Snort版本](#)

[方法1](#)

[方法2](#)

[入侵規則的升級](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何在Firepower管理員中心(FMC)中從Snort 2和Snort 3版本升級。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower威脅防禦
- Firepower管理中心
- Snort

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FMC 7.0
- FTD 7.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Snort 3功能已增加到Firepower裝置管理器(FDM)和思科Defense Orchestrator (CDO)的6.7版本中；在Firepower管理中心(FMC)的7.0版本中。

Snort 3.0旨在解決以下挑戰：

1. 減少記憶體和CPU使用量。
2. 提高HTTP檢查效率。
3. 更快的配置載入和Snort重新啟動。
4. 更佳的可程式設計性，加快功能增加速度。

設定

升級Snort版本

方法1

1. 登入Firepower管理中心。



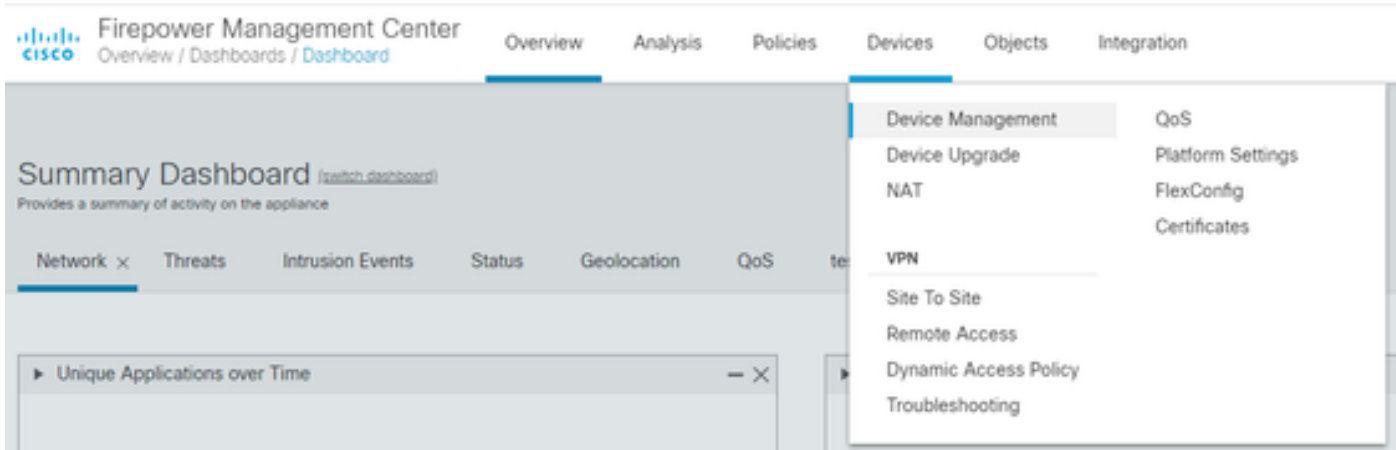
Firepower Management Center

Username

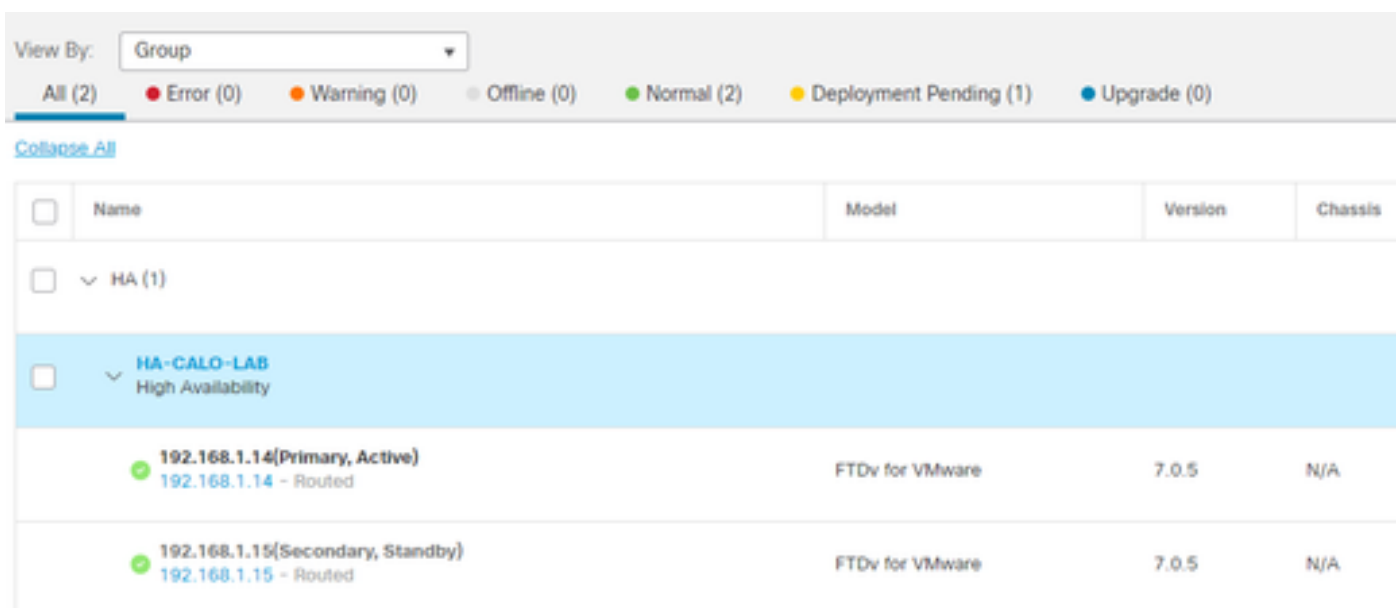
Password

Log In

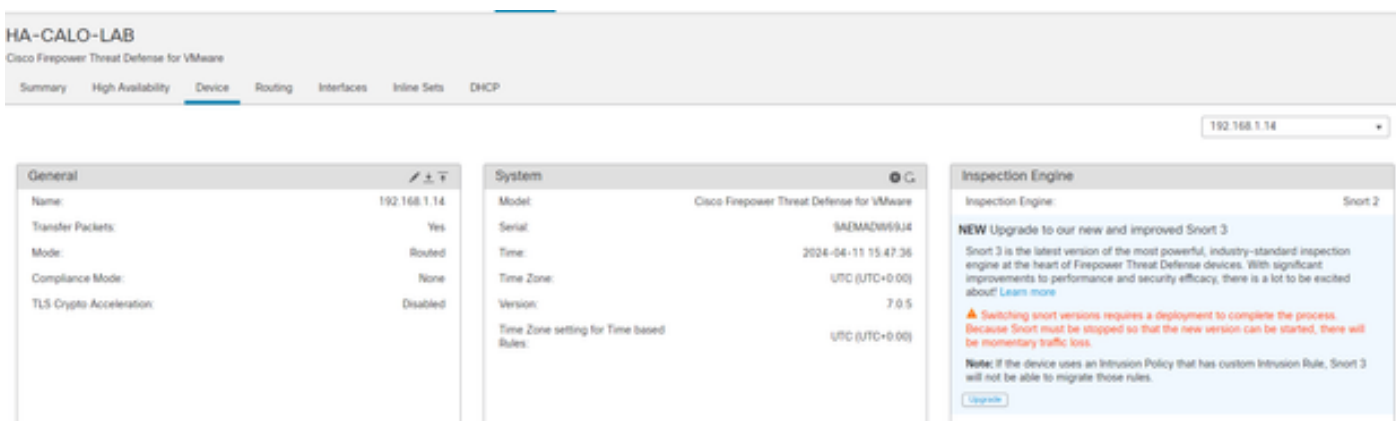
2. 在裝置頁籤上，導航到裝置>裝置管理器。



3. 選擇要更改Snort版本的裝置。



4. 按一下Device頁籤，然後按一下Inspection Engine部分上的Upgrade按鈕。



5. 確認您的選擇。

Enable Snort 3

Are you sure you want to enable Snort 3?

No

Yes

方法2

1. 登入Firepower管理中心。



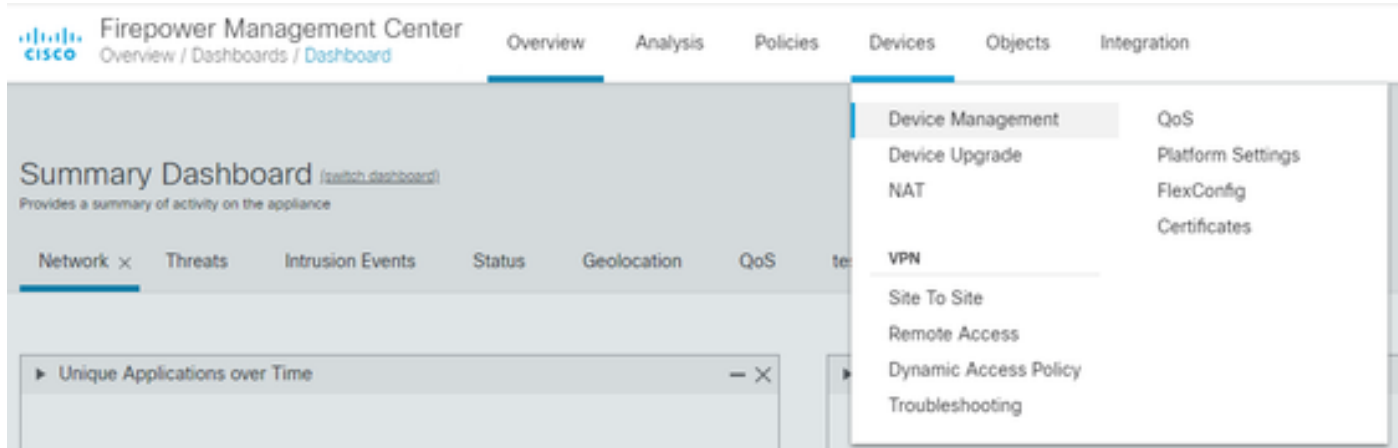
Firepower Management Center

Username

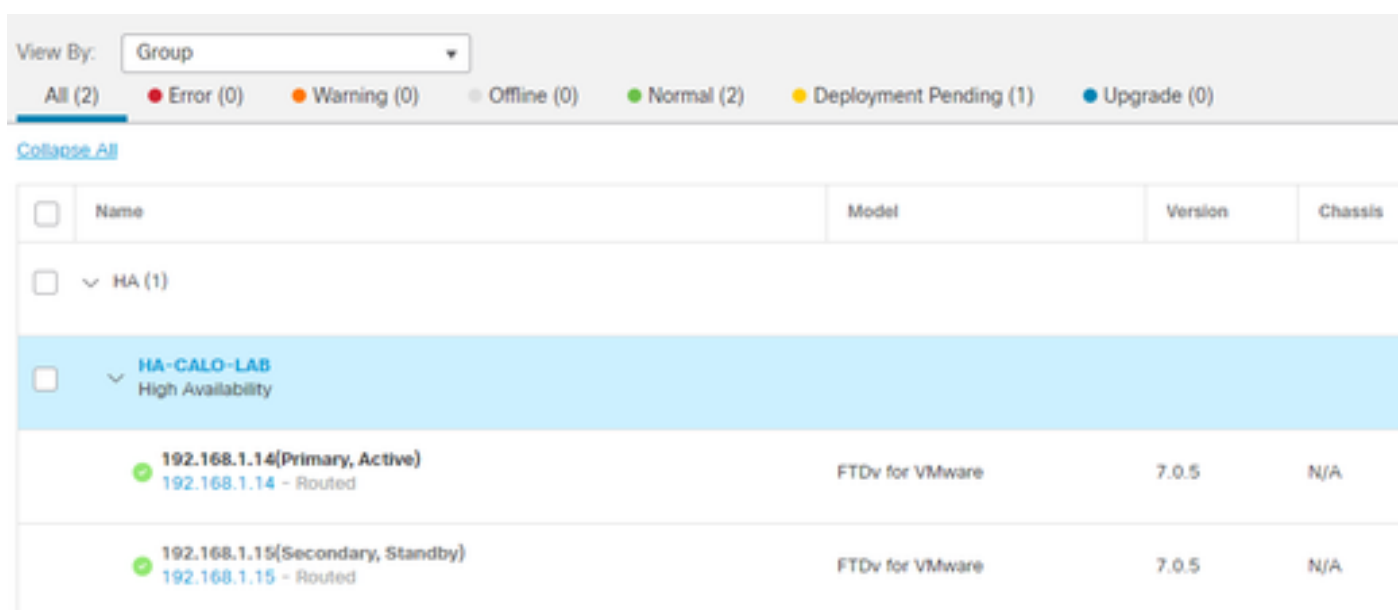
Password

Log In

2. 在裝置頁籤上，導航到裝置>裝置管理器。



3. 選擇要更改Snort版本的裝置。



4. 按一下選擇操作按鈕，然後選擇升級到Snort 3。

View By: Group

All (1)
Error (0)
Warning (0)
Offline (1)
Normal (0)

[Collapse All](#)
1 Device Selected
Select Action

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Ungrouped (1)
<input checked="" type="checkbox"/>	FTD 1 Snort 3 10.31.124.226 - Routed

Edit Advanced Settings
 Upgrade to Snort 3
 Upgrade Firepower Software
 Edit Deployment Settings

入侵規則的升級

此外，您需要將Snort 2規則轉換為Snort 3規則。

1. 從選單中選擇Objects > Intrusion Rules。

[Overview](#)
[Analysis](#)
[Policies](#)
[Devices](#)
[Objects](#)
[AMP](#)
[Intelligence](#)

Object Management
 Intrusion Rules

description, or Base Policy

2. 從選單中選擇Snort 2 All Rules頁籤 > Group Rules By > Local Rules。

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

Group Rules By

✓ Category

Local Rules

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Priority

SANS Top 20 (version 5.0)

SANS Top 20 (version 6.01)

3. 按一下Snort 3所有規則標籤，並確保已選擇所有規則。

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

67 items

Search Rule Group

All Rules

4. 在「任務」下拉選單中，選擇「轉換並導入」。

Tasks



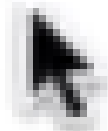
-----Snort 3-----

Upload

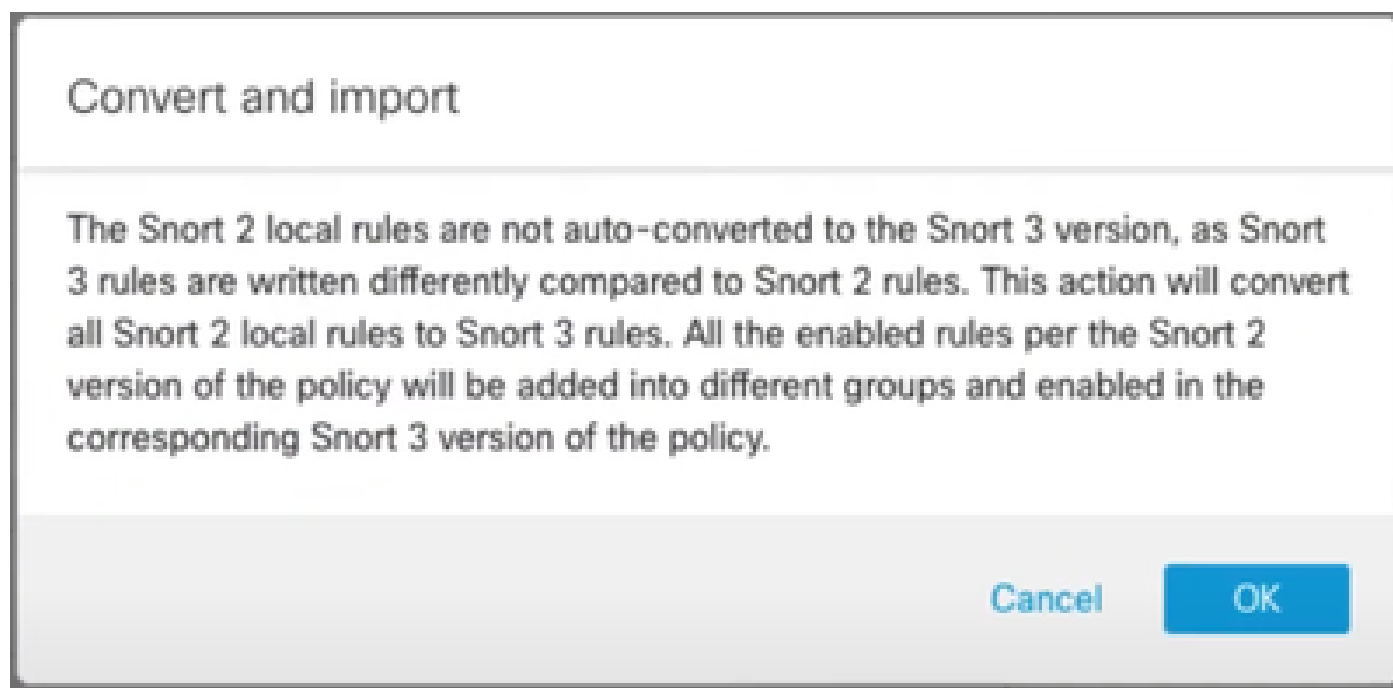
-----Snort 2-----

Convert and import

Convert and download



5. 按一下警告消息上的確定。



驗證

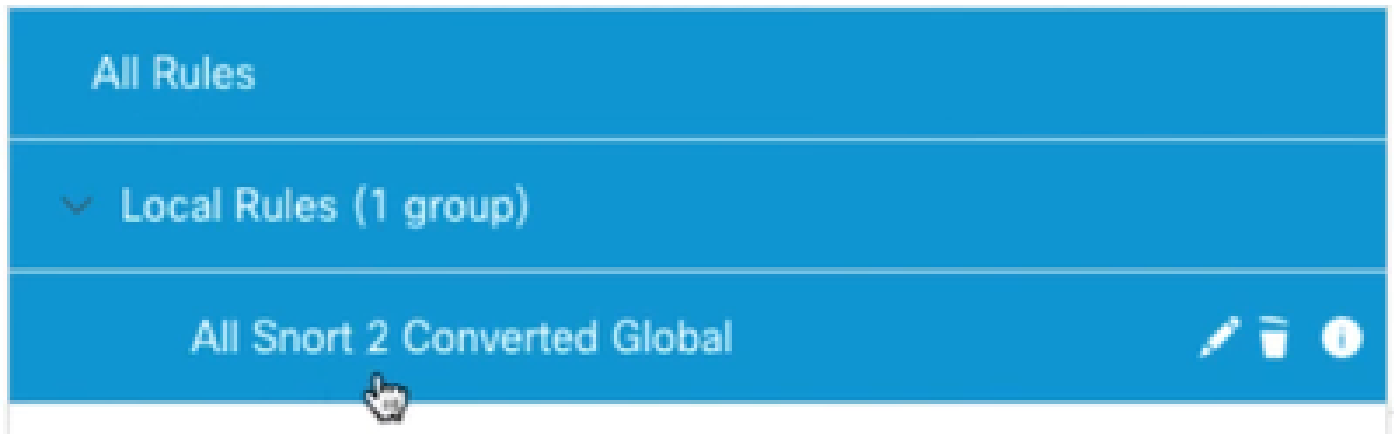
「檢測引擎」部分顯示Snort的當前版本為Snort 3。



規則轉換在看到以下消息後成功：



最後，您必須在Local Rules 組上找到All Snort 2 Converted Global 部分，該部分包含您從Snort 2到Snort 3轉換的所有規則。



疑難排解

如果遷移失敗或崩潰，請回滾到Snort 2，然後重試。

相關資訊

- [如何從Snort 2遷移到Snort 3](#)
- [Cisco Secure - Snort 3裝置升級 \(外部YouTube影片\)](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。