通过FDM从Snort 2升级到Snort 3

目录

简介

本文档介绍如何在Firepower设备管理器(FDM)中从snort 2升级到Snort 3版本。

先决条件

Cisco 建议您了解以下主题：

- Firepower Threat Defense (FTD)
- Firepower设备管理器(FDM)
- Snort.

要求

确保满足以下要求：

- 访问Firepower设备管理器。
- FDM的管理权限。
- FTD必须至少为6.7版才能使用snort 3。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FTD 7.2.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

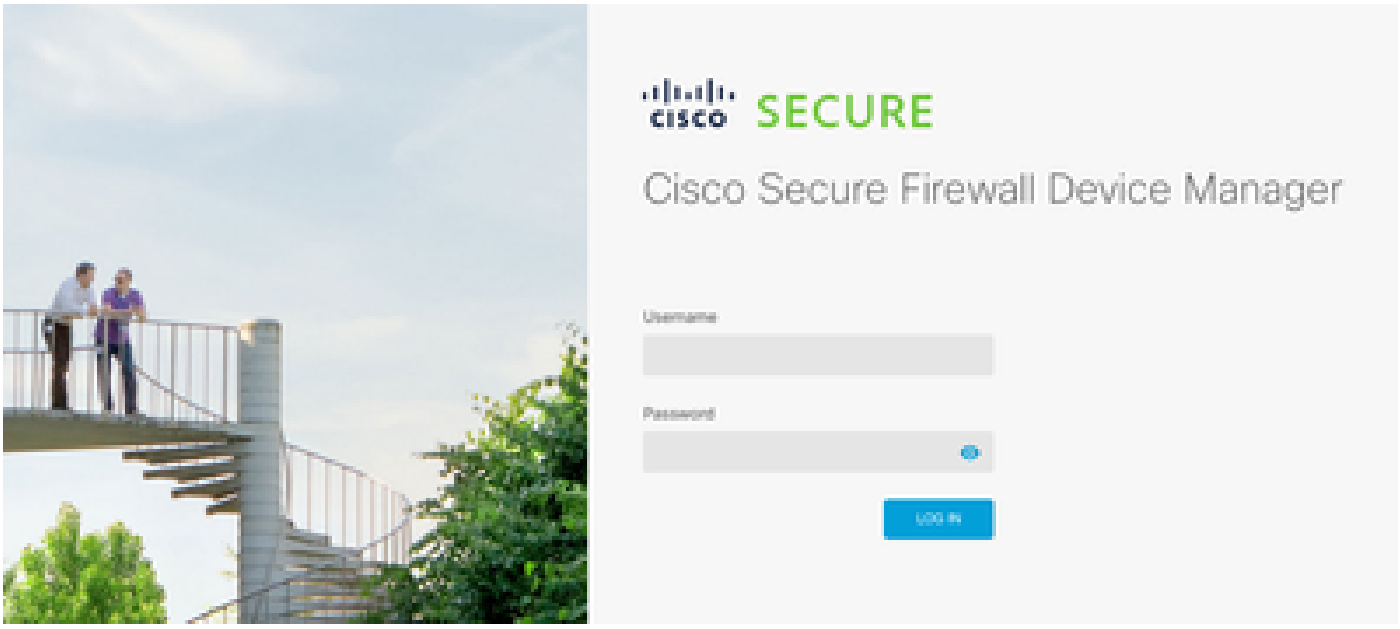
Firepower设备管理器(FDM)的6.7版本中添加了snort 3功能。Snort 3.0旨在应对这些挑战：

- 减少内存和CPU使用率。
- 提高HTTP检查效率。
- 更快的配置加载和Snort重启。
- 更好的可编程性，可更快地添加功能。

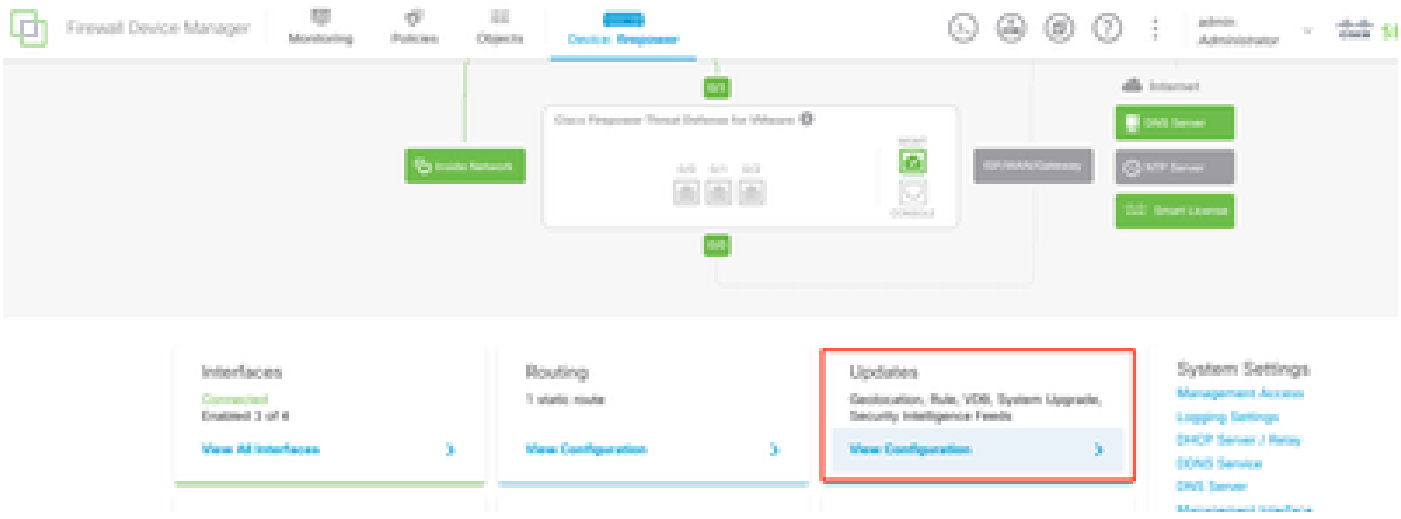
配置

配置

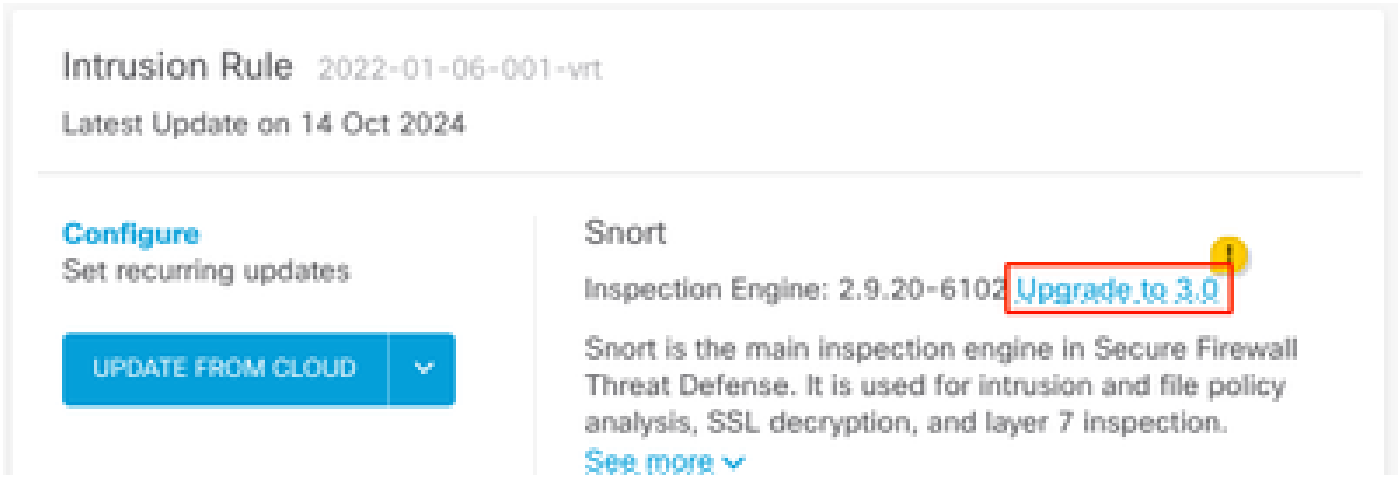
1. 登录Firepower设备管理器。



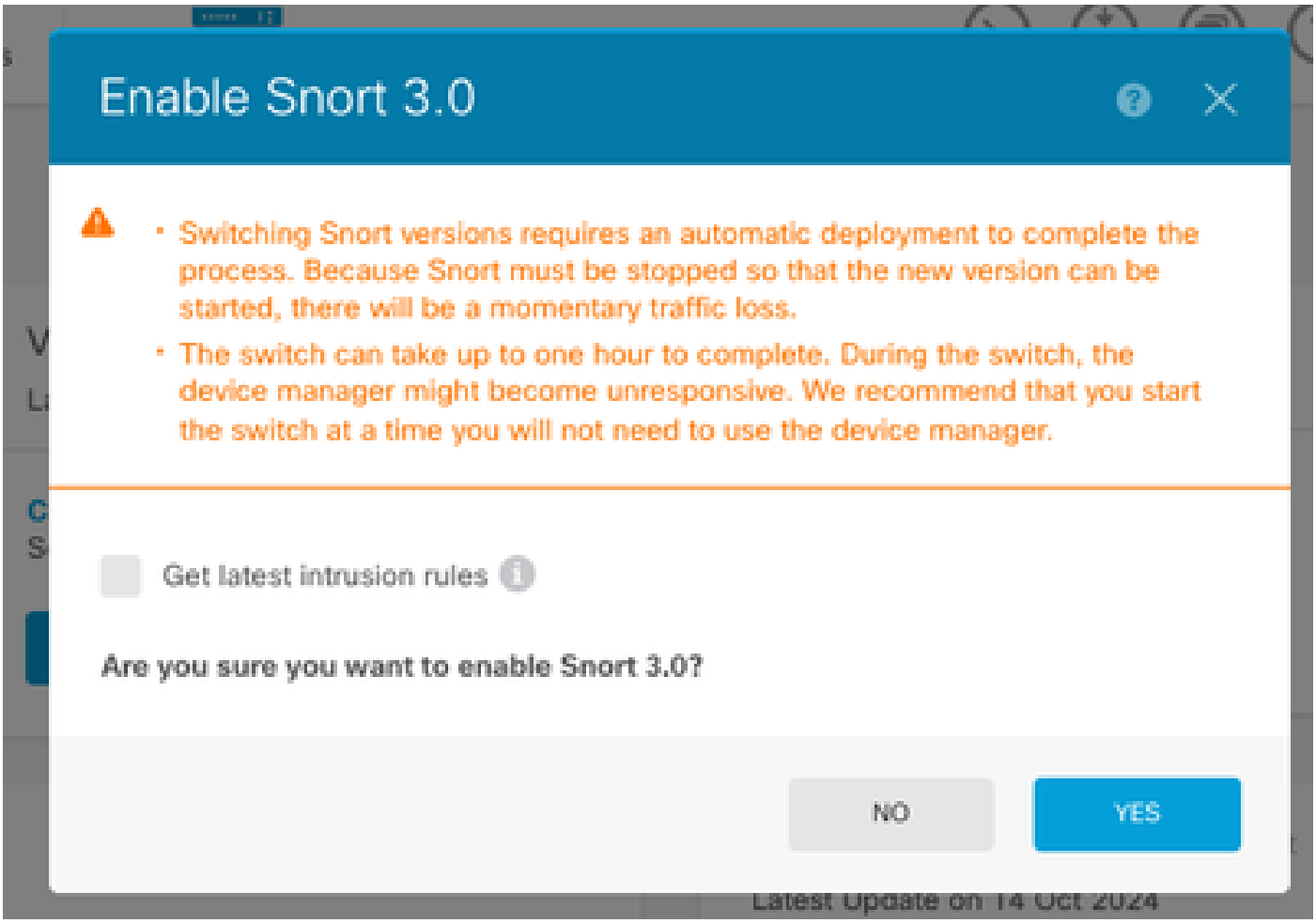
2. 导航到设备>更新>查看配置。

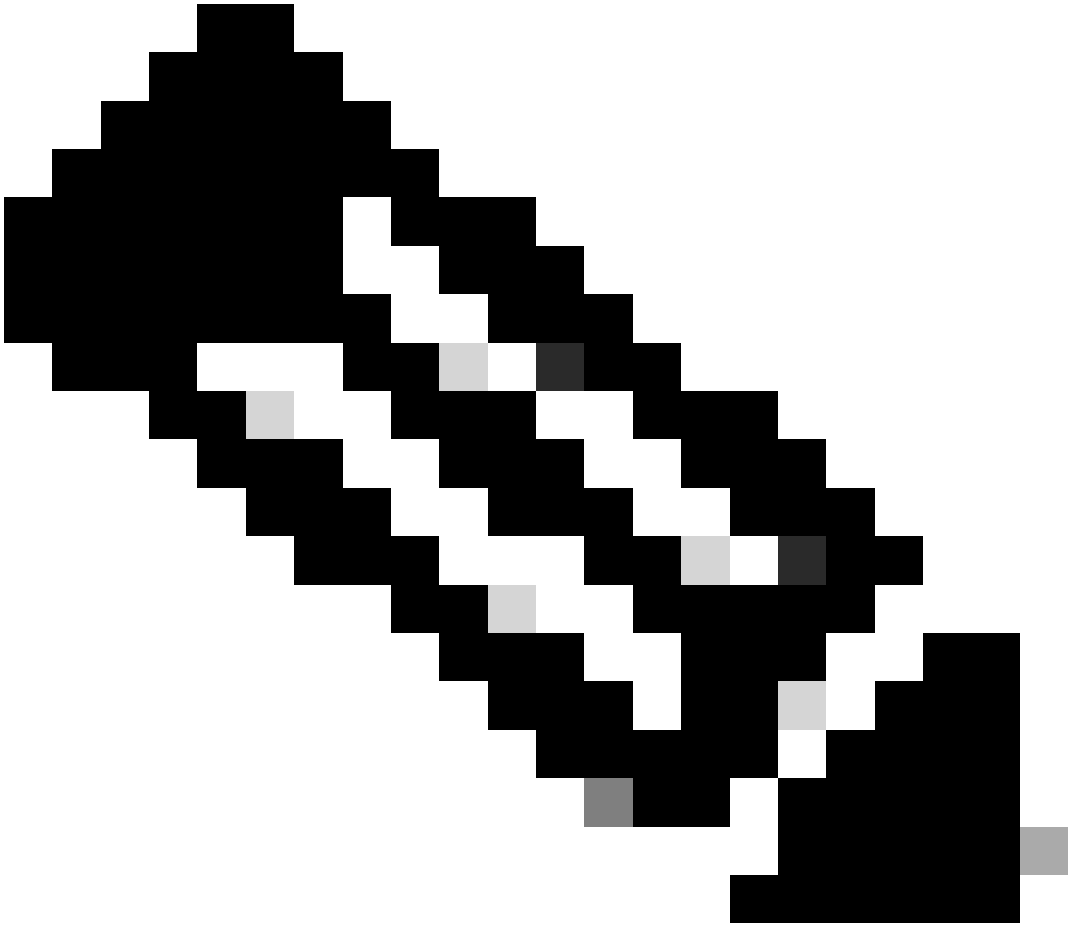


3. 在intrusion rules部分中，单击upgrade to snort 3。

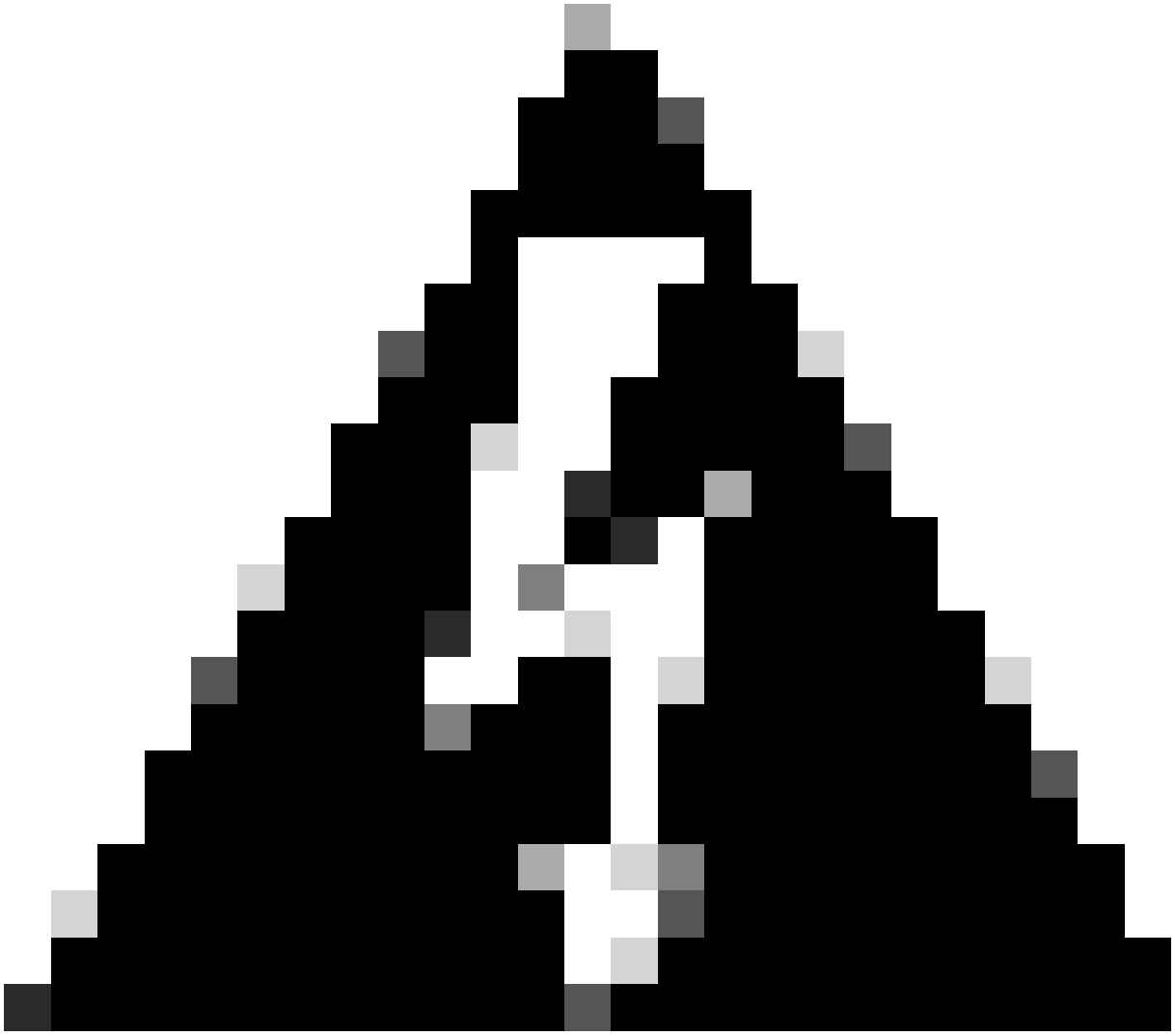


4. 在确认选择的警告消息上，选择获取最新入侵规则包选项，然后单击Yes。



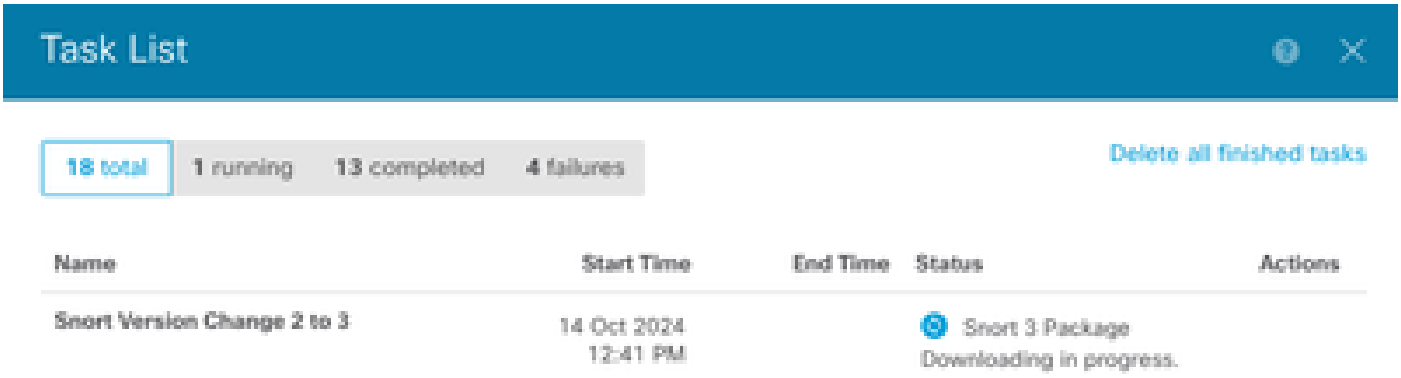


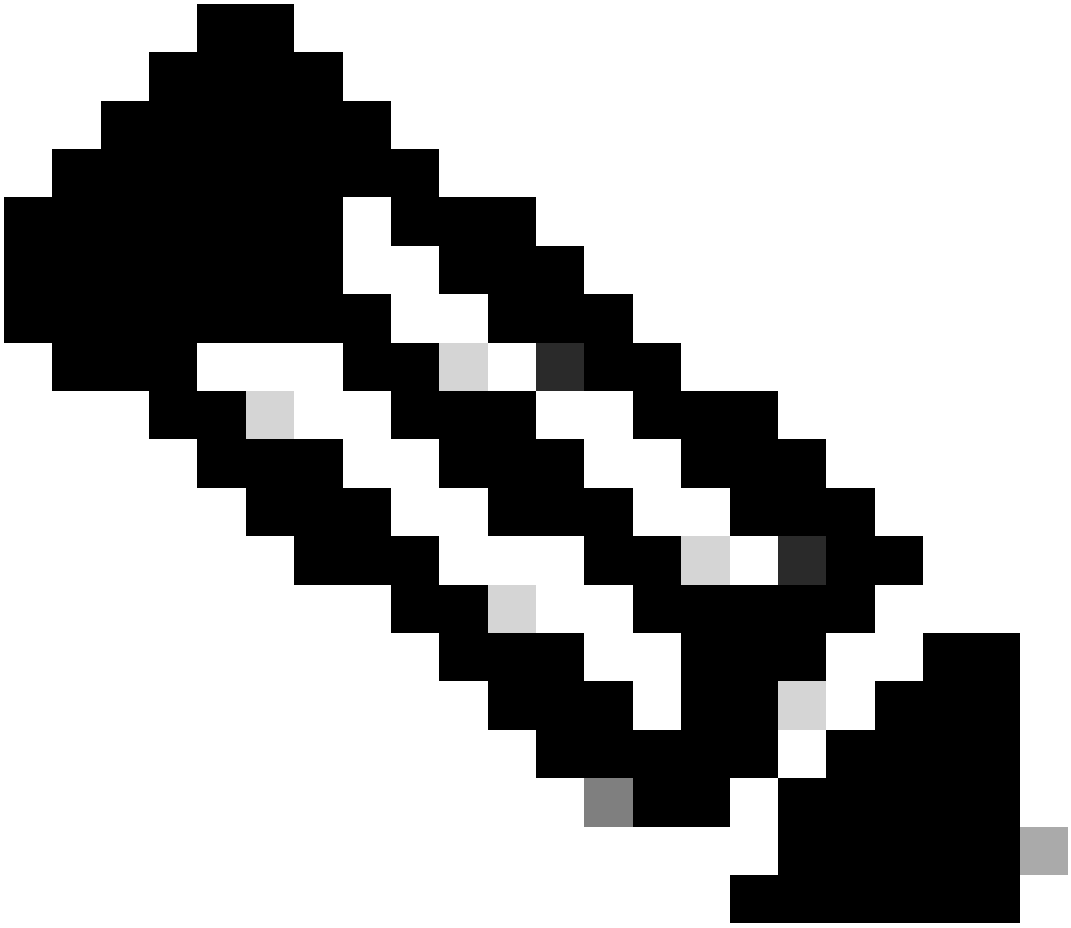
注意：系统仅下载活动Snort版本的软件包，因此您不太可能安装了要切换到的Snort版本的最新软件包。必须等到切换版本任务完成，才能编辑入侵策略。



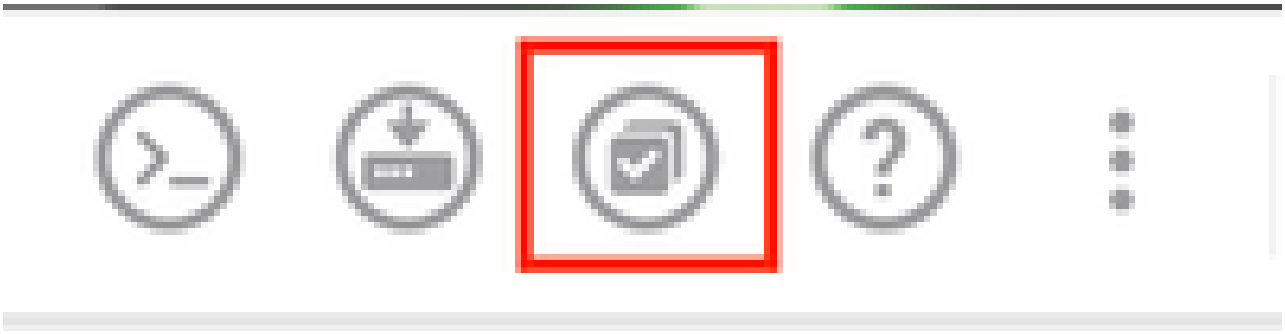
警告：交换snort版本会导致瞬时流量丢失。

5. 您必须在任务列表中确认升级已启动。



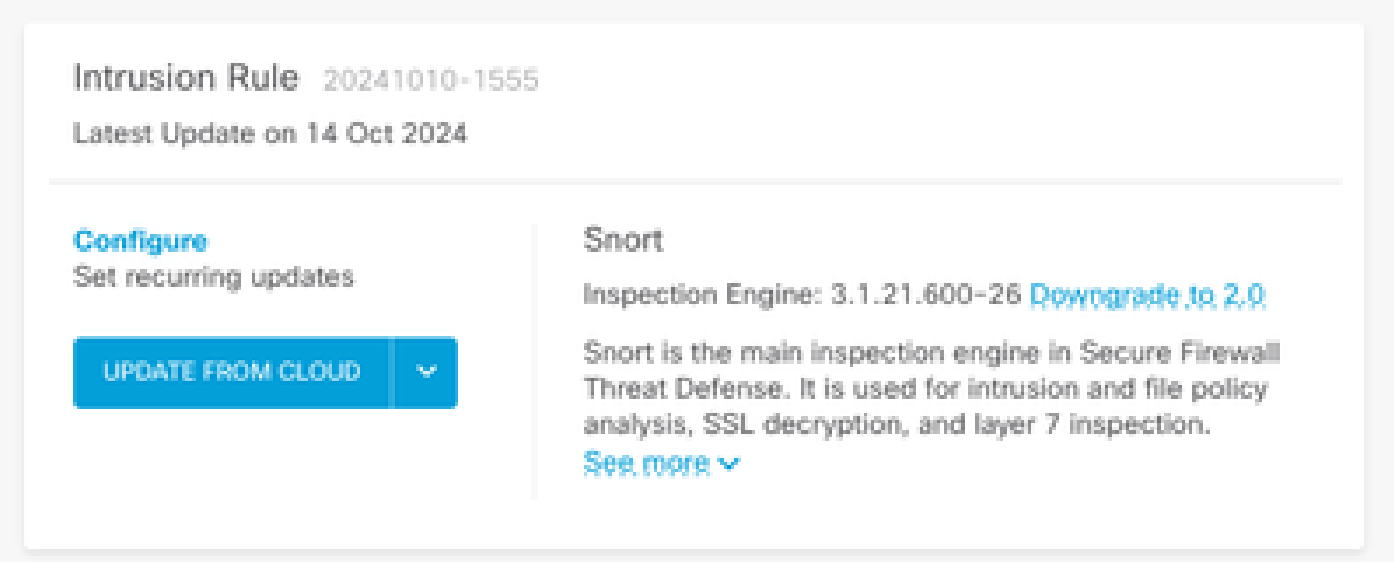


注意：任务列表位于部署图标旁边的导航栏中。

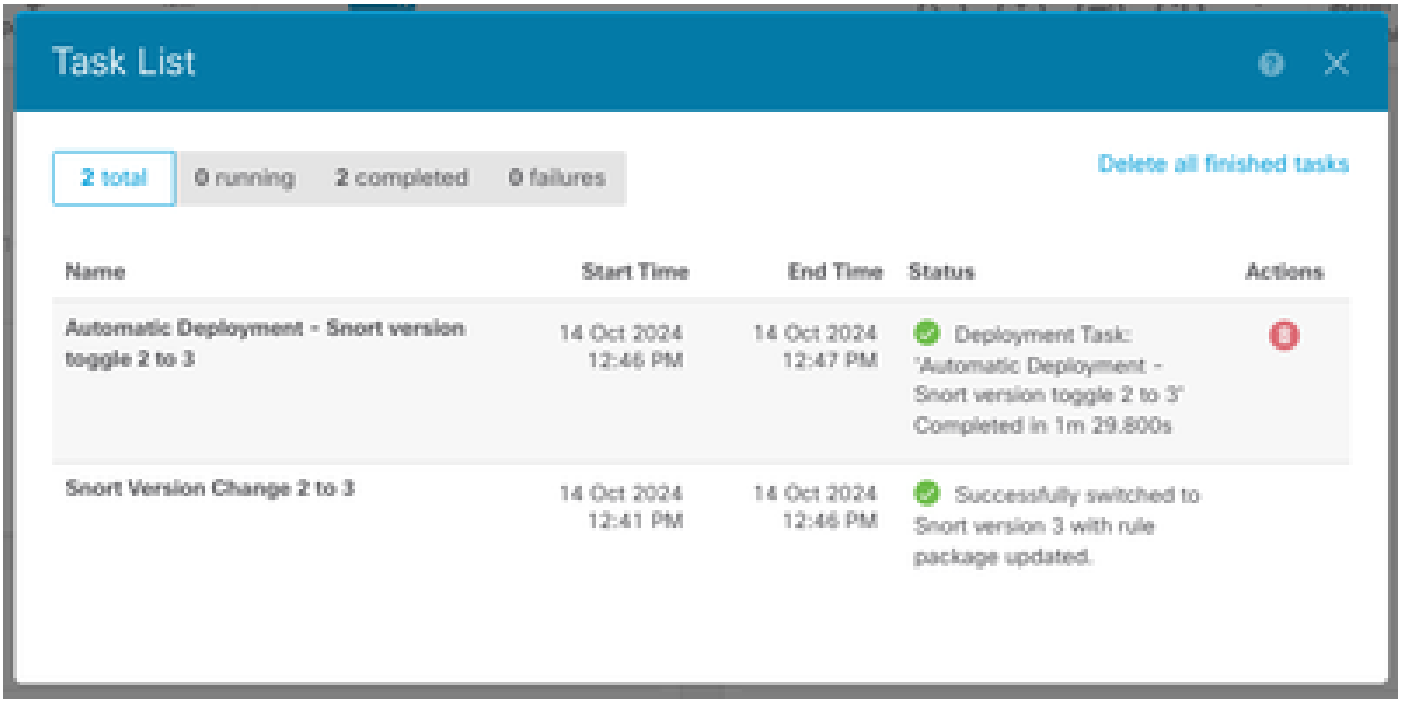


验证

“检查引擎”(Inspection Engine)部分显示Snort的当前版本是Snort 3。



最后，在任务列表中，确保已成功完成并部署对snort 3的更改。



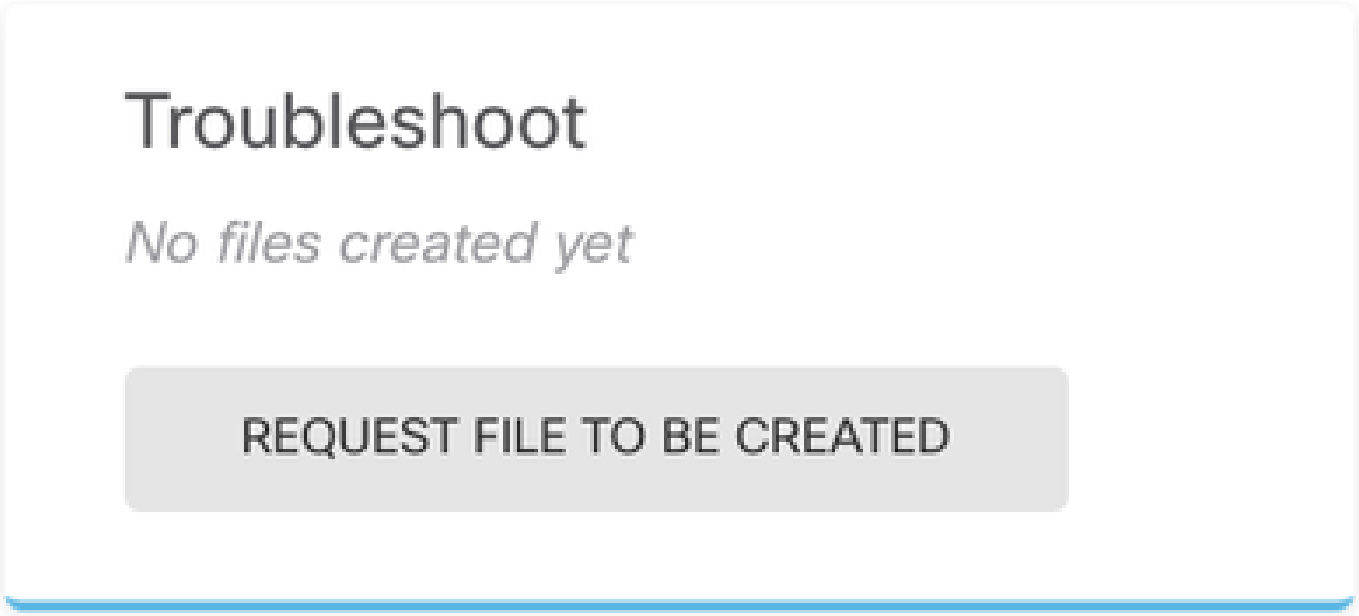
故障排除

如果在升级过程中遇到问题，请考虑以下步骤：

- 确保您的FTD版本与Snort 3兼容。

有关其他详细信息，请查看思科安全防火墙威胁防御兼容性指南

- 导航到设备选项卡，然后单击请求创建文件，收集FDM上的故障排除文件。收集问题后，在TAC开立一个案例并上传到案例以寻求进一步帮助。



相关信息

- Snort 3采用
- Snort文档
- Cisco安全防火墙设备管理器配置指南7.2版

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。