通过 FMC 将 Snort 2 升级到 Snort 3

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 升级Snort版本
  - 方法 1
  - 方法 2
- 入侵规则升级

验证

故障排除

相关信息

简介

本文档介绍如何在Firepower管理器中心(FMC)中从Snort 2和Snort 3版本升级。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower Threat Defense (FTD)
- Firepower 管理中心
- Snort

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FMC 7.0
- FTD 7.0

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

Snort 3功能已添加到Firepower设备管理器(FDM)和思科防御协调器(CDO)的6.7版本中；在7.0版本中，适用于Firepower管理中心(FMC)。

Snort 3.0旨在应对这些挑战：

1. 减少内存和CPU使用率。
2. 提高HTTP检查效率。
3. 更快的配置加载和Snort重新启动。
4. 更出色的可编程性，可更快地添加功能。

配置

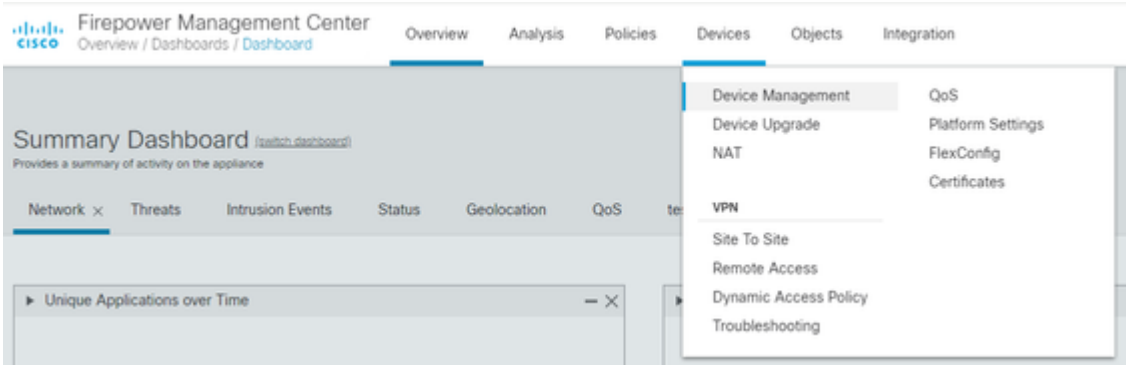
升级Snort版本

方法 1

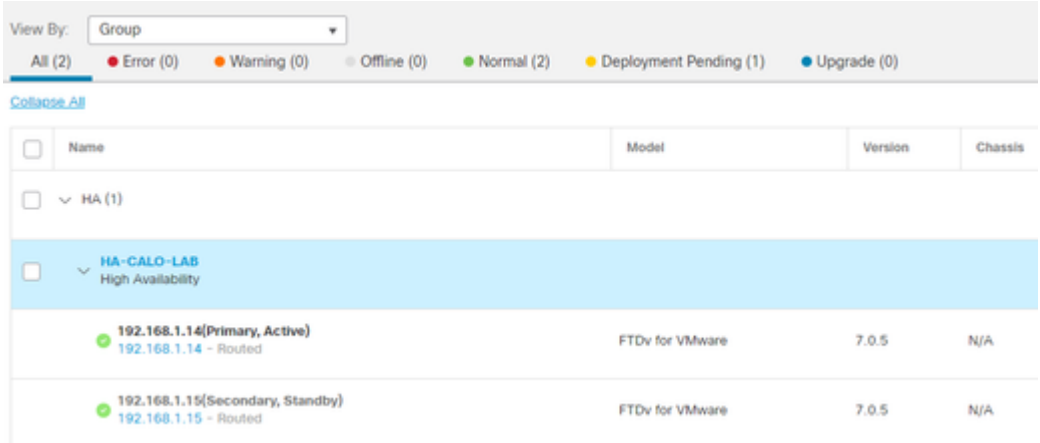
1. 登录Firepower管理中心。



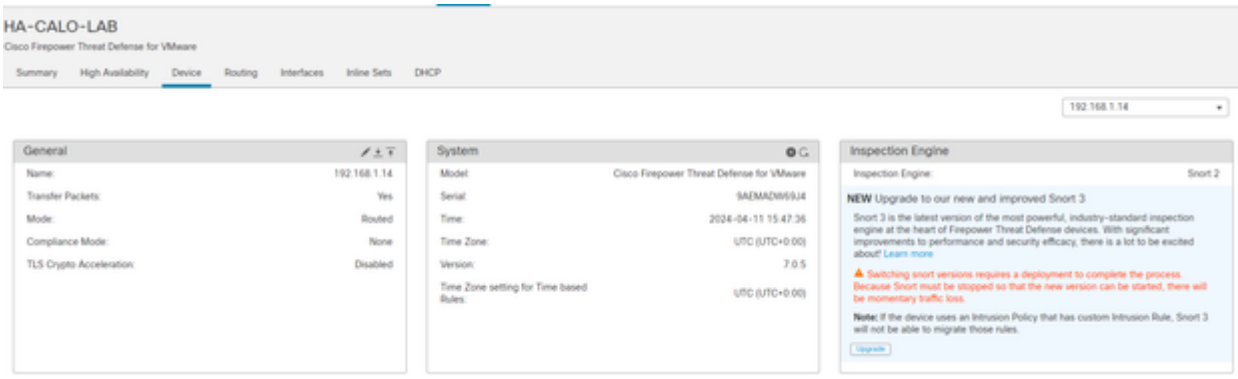
2.在设备选项卡上，导航到设备>设备管理器。



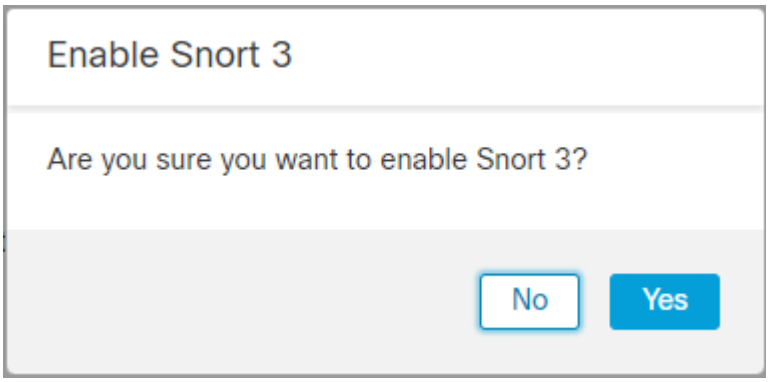
3.选择要更改Snort版本的设备。



4.单击Device选项卡，然后单击“Inspection Engine”部分上的Upgrade按钮。



5.确认您的选择。

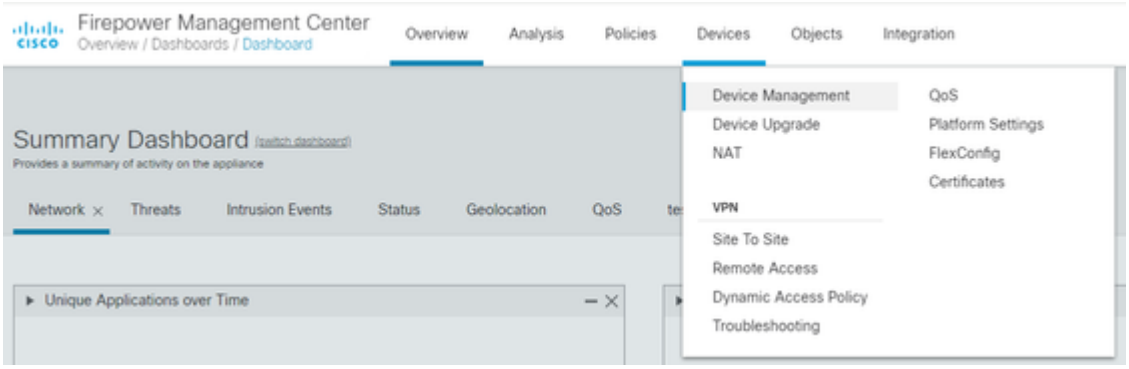


方法 2

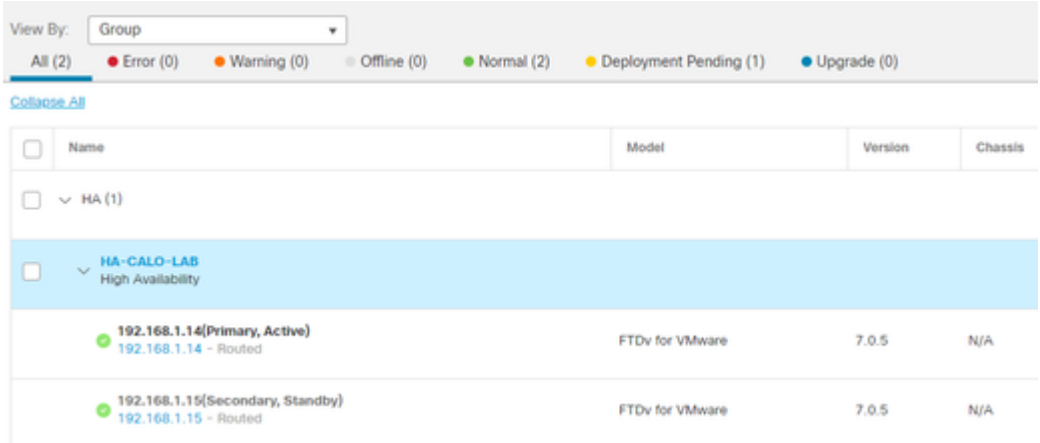
1. 登录Firepower管理中心。



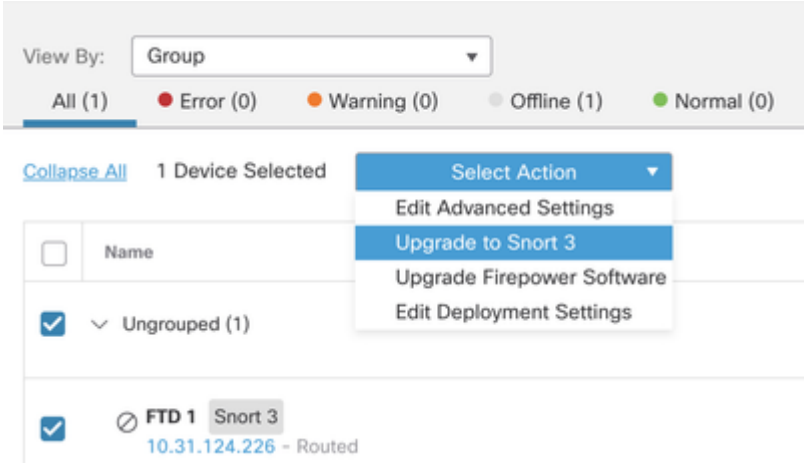
2.在设备选项卡上，导航到设备>设备管理器。



3.选择要更改Snort版本的设备。



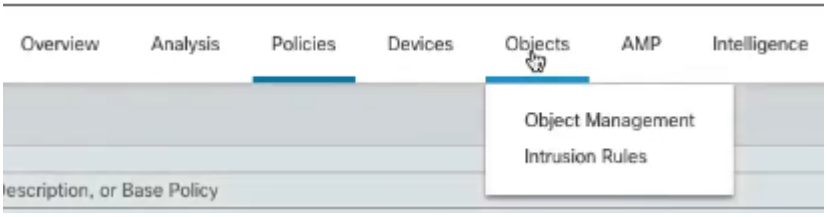
4.单击Select Action按钮，然后选择Upgrade to Snort 3。



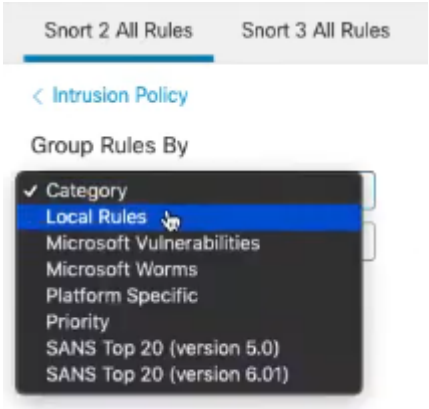
入侵规则升级

此外，您需要将Snort 2规则转换为Snort 3规则。

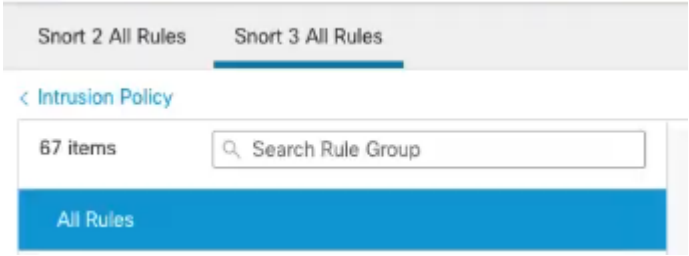
1. 从Objects > Intrusion Rules菜单中选择。



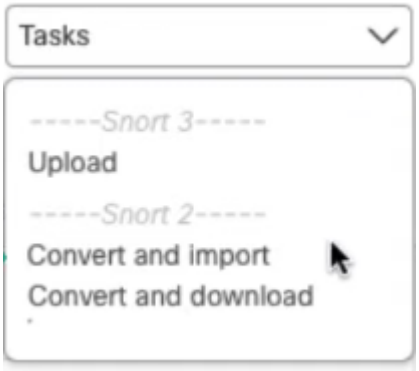
2.从菜单中选择Snort 2 All Rules选项卡> Group Rules By > Local Rules。



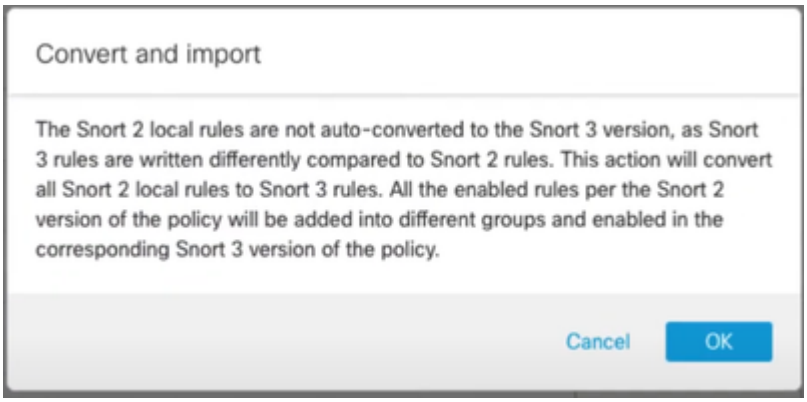
3.单击Snort 3 All Rules选项卡，并确保选中All Rules。



4.在“任务”下拉菜单中，选择“转换并导入”。



5.单击警告消息上的OK。

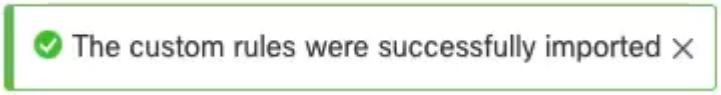


验证

“检查引擎”部分显示Snort的当前版本为Snort 3。



规则转换成功后，您会看到以下消息：



最后，您必须在Local Rules组中找到All Snort 2 Converted Global部分，该部分包含您从Snort 2到Snort 3转换的所有规则。



故障排除

如果迁移失败或崩溃，回滚到Snort 2并重试。

相关信息

- 如何从Snort 2迁移到Snort 3
- Cisco Secure - Snort 3设备升级（外部YouTube视频）

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）。

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）。