在 Hyper-V 上部署 Firewall Threat Defense Virtual

本章介绍如何使用 Microsoft Hyper-V 部署 Threat Defense Virtual。

- 概述， 第 1 页
- 准则和限制， 第 2 页
- 前提条件， 第 3 页
- 许可， 第 3 页
- 配置 Hyper-V 虚拟交换机， 第 4 页
- 准备 Day 0 配置文件 ， 第 5 页
- 使用 Day 0 配置文件部署， 第 7 页
- 管理 Threat Defense Virtual， 第 17 页
- 故障排除， 第 18 页

概述

您可以使用 Microsoft Hyper-V（从版本 10.0.0 开始）部署 Threat Defense Virtual。

在 Hyper-V 中为 Threat Defense Virtual 设置以下子网：

管理子网 → 对应管理中心 (Mgmt 0/0)。

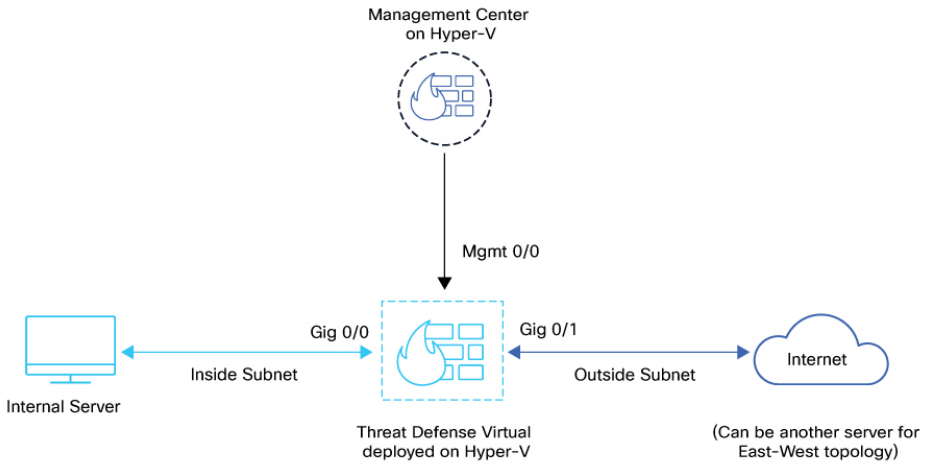
内部子网 → 内部网络 (Gig 0/0)。

外部子网 → 外部或面向互联网的网络 (Gig 0/1)。

诊断子网 -> 用于诊断和报告；不能用于流量。

这些子网使用 Hyper-V 虚拟交换机创建。

下图显示 Hyper-V 上部署的、由管理中心管理的 Threat Defense Virtual。



准则和限制

- 操作系统支持：
  - Threat Defense Virtual 版本 10.0 - Windows Server 2019、2025
  - Threat Defense Virtual 版本 10.0 以下 - Windows Server 2019
  - 原生 Hyper-V
- 文件格式：

  支持 VHDX 格式，以便在 Hyper-V 上初始部署 Threat Defense Virtual。
- Day 0 配置：

  您创建一个文本文件，其中包含您需要的 Threat Defense Virtual CLI 配置命令。
- 高可用性（活动/备用）受支持。

部署

运行版本 7.4.3 或更高版本的 Threat Defense Virtual 实例会在首次启动期间执行多项初始化任务，这会导致控制台在大约五分钟后可用。这种延迟是正常的。如果设备在首次启动后大约两分钟内关闭，重要的初始化步骤可能会中断，从而可能导致设置不完整和意外行为。

要解决此问题，必须使用新映像重新安装虚拟平台。

UEFI 和安全启动限制

在 Hyper-V 上，仅支持绿地（全新）部署，并且必须在初始部署期间启用 UEFI 固件。

现有的棕色地带部署可以升级到版本 10.0.0，而不会受到影响。不支持在部署后更改启动模式或启用 UEFI 安全启动。

升级限制和局限性

恢复升级限制

注意 不支持恢复升级。

确保在升级前进行备份。升级到 Threat Defense Virtual 10.0.0 后，您无法回滚到以前的软件版本。要返回到较早的版本，必须重新部署管理中心。

前提条件

- **主机操作系统** Microsoft Windows Server 2019 或启用了 Hyper-V 角色的 Windows Server 2025。
- **最低的 Threat Defense Virtual 资源要求**
  - CPU：最少 **4 个 vCPU**
  - RAM：最少 **8 GB**
  - 磁盘存储：**100 GB**
- 从 Cisco.com 下载适用于Hyper-V 的 Threat Defense Virtual VHD 映像。 https://software.cisco.com/download/
- 创建 Day 0 配置文件。

  如果是首次部署 Threat Defense Virtual，则必须添加 Day 0 配置。
- 使用管理中心进行集中管理。
- 不支持设备管理器。

许可

Threat Defense Virtual 支持以下许可证类型：

- BYOL（自带许可证）
  - 智能许可
  - SLR（特定许可证预留）
- 评估许可

Threat Defense Virtual 智能许可的性能层

Threat Defense Virtual 支持性能层许可，该许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *1:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

配置 Hyper-V 虚拟交换机

过程

步骤 1 打开虚拟交换机管理器。

在 Hyper-V 管理器中，转至右侧的**操作**窗格，然后点击**虚拟交换机管理器**。

步骤 2 选择交换机类型。

在虚拟交换机管理器窗口中，在**创建虚拟交换机**下选择**外部**。

步骤 3 创建虚拟交换机。

点击**创建虚拟交换机**以继续进行配置。

步骤 4 为虚拟交换机命名。

在**虚拟交换机属性**窗口中，为新虚拟交换机输入一个有意义的名称（例如：FTD-External-Switch）。

这有助于在将交换机分配给虚拟机时对其进行标识。

步骤 5 选择外部网络，然后选择物理适配器。

- 在**连接类型**下，选择**外部网络**。
- 从下拉菜单中选择要与此虚拟交换机绑定的物理网络适配器（例如：*Cisco*® 以太网融合 *NIC X710-DA2*）。

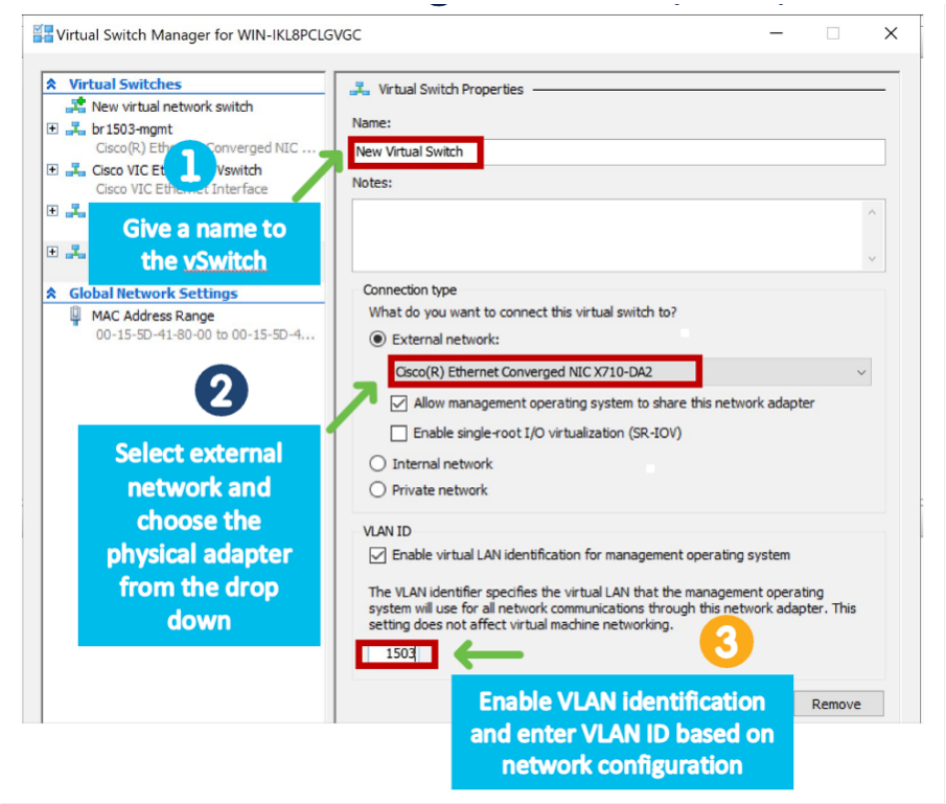
这允许虚拟机与物理网络通信。

步骤 6 启用 VLAN 标识（可选，基于网络配置）。

- 如果需要 VLAN 标记，请选中**为管理操作系统启用虚拟 LAN 标识**复选框。

- 根据您的网络配置，输入适当的 VLAN ID（例如：1503）。

步骤 7 点击**应用**，然后点击**确定**以保存配置。



准备 Day 0 配置文件

开始之前

在启动 Threat Defense Virtual 之前，您可以准备 Day 0 配置文件。此文件是包含将在启动 Threat Defense Virtual 时应用的 Threat Defense Virtual 配置的文本文件。此初始配置将放入您选择的工作目录中名为 *day0-config* 的文本文件，并转换为首次启动时挂载和读取的 day0.iso 文件。Day 0 配置文件必须至少包含将激活管理接口以及设置用于公共密钥身份验证的 SSH 服务器的命令，但它还可包含完整的 Threat Defense Virtual 配置。day0.iso 文件（自定义 day0.iso 或默认 day0.iso）必须在首次启动过程中可用。

我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

- 如果要在透明模式下部署 Threat Defense Virtual，则必须在透明模式下将已知的运行 Threat Defense 配置用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。

如果要在透明模式下部署 Threat Defense Virtual，则必须在透明模式下将已知的运行 Threat Defense 配置用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。如果要在透明模式下部署 Threat Defense Virtual，则必须在透明模式下将已知的运行配置用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。

- 您必须在首次启动 Threat Defense Virtual 之前添加 Day 0 配置文件。如果您决定要在初始启动 Threat Defense Virtual 之后使用 Day 0 配置，则必须执行 write erase 命令，应用 Day 0 配置文件，然后启动 Threat Defense Virtual。

过程

步骤 1 在名为 *day0-config* 的文本文件中输入 Threat Defense Virtual 的 CLI 配置。添加三个接口的接口配置和所需的任何其他配置。

第一行应以 Threat Defense Virtual 版本开头。day0-config 应为有效的 Threat Defense 配置。生成 day0-config 的最佳方式是从现有的 Threat Defense Virtual 复制运行配置的所需部分。day0-config 中的行顺序很重要，应与现有的 show run 命令输出中看到的顺序相符。

示例：

```
{
"EULA": "accept",
"Hostname": ” FTDvhyperv",
"AdminPassword": "r2M$9^Uk69##",
"DNS1": "208.67.222.222",
"DNS2": "208.67.222.222",
"IPv4Mode": "Manual",
"IPv4Addr": "10.10.0.92",
"IPv4Mask": "255.255.255.224",
"IPv4Gw": "10.10.0.65",
"ManageLocally": ” No",
"FmcIp": "10.10.1.83",
"FmcRegKey": "ciscoadmin",
"FmcNatId": "cisco"
}
```

步骤 2 （可选）将思科智能软件管理器发布的智能许可证身份令牌文件下载到您的计算机。

步骤 3 （可选）从下载文件复制 ID 令牌并将其放入仅包含 ID 令牌的文本文件。

步骤 4 （可选）若要在初始 Threat Defense Virtual 部署过程中进行自动许可，请确保 day0-config 文件中包含以下信息：

- 管理接口 IP 地址
- （可选）要用于智能许可的 HTTP 代理
- 用于启用与 HTTP 代理（如果指定）连接的 route 命令
- 将 tools.cisco.com 解析为 IP 地址的 DNS 服务器
- 指定您请求的 Threat Defense Virtual 许可证的智能许可配置
- （可选）便于 Threat Defense Virtual 在 CSSM 中进行查找的唯一主机名

步骤 5 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

```
stack@user-ubuntu:-$ sudo genisoimage -r -o day0.iso day0-config
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
```

身份令牌自动向智能许可服务器注册 Threat Defense Virtual。

步骤 6 重复步骤 1 到 5，使用相应的 IP 地址为要部署的每个 Threat Defense Virtual 创建单独的默认配置文件。

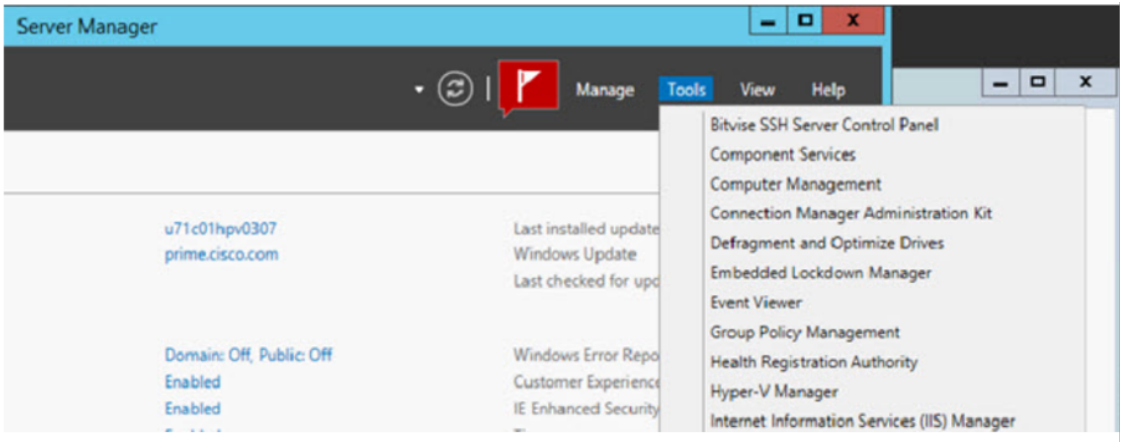
使用 Day 0 配置文件部署

在设置 Day 0 配置文件之后，您可以使用 Hyper-V 管理器进行部署。

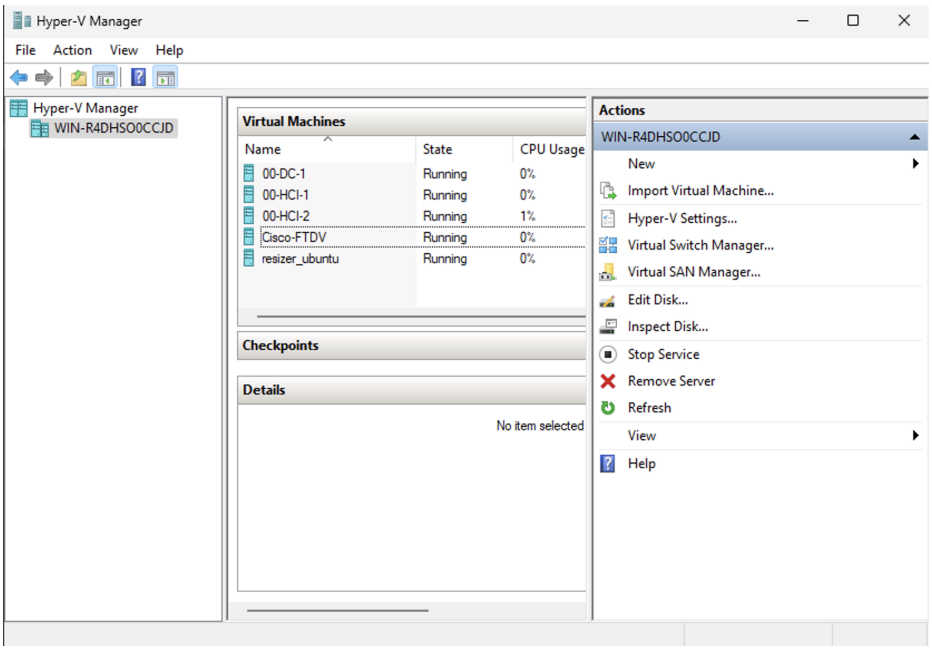
请按照以下步骤在 Hyper-V 主机上部署 Cisco Threat Defense Virtual：

过程

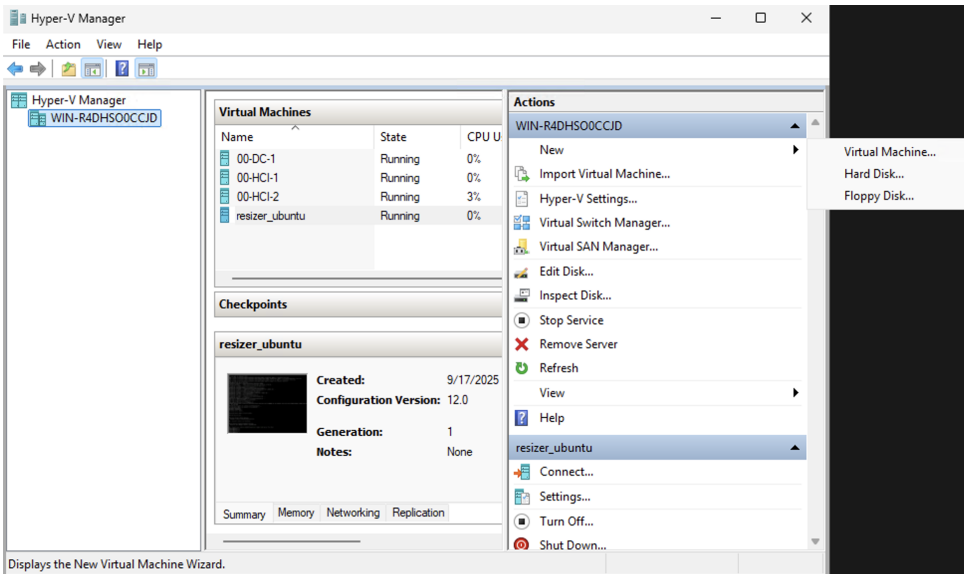
步骤 1 转至“服务器管理器”(Server Manager) > “工具”(Tools) > “Hyper-V 管理器”(Hyper-V Manager)。



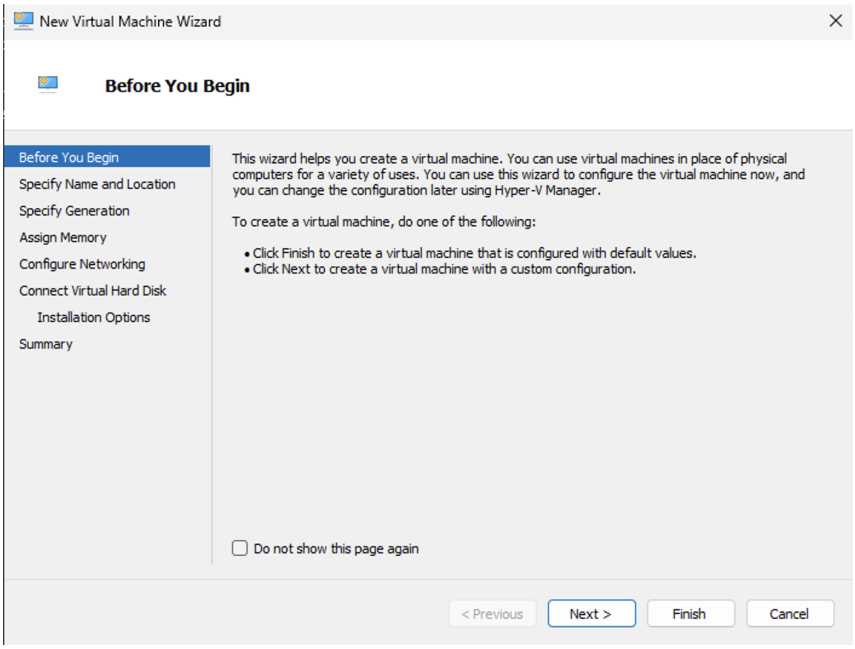
步骤 2 此时将出现 Hyper-V 管理器。



步骤 3 从虚拟机监控程序列表中，右键点击列表中的所需虚拟机监控程序，然后选择“新建”>“虚拟机”。



步骤 4 此时将出现“新建虚拟机向导”(New Virtual Machine Wizard)。



步骤 5 执行该向导的各个步骤，指定以下信息：

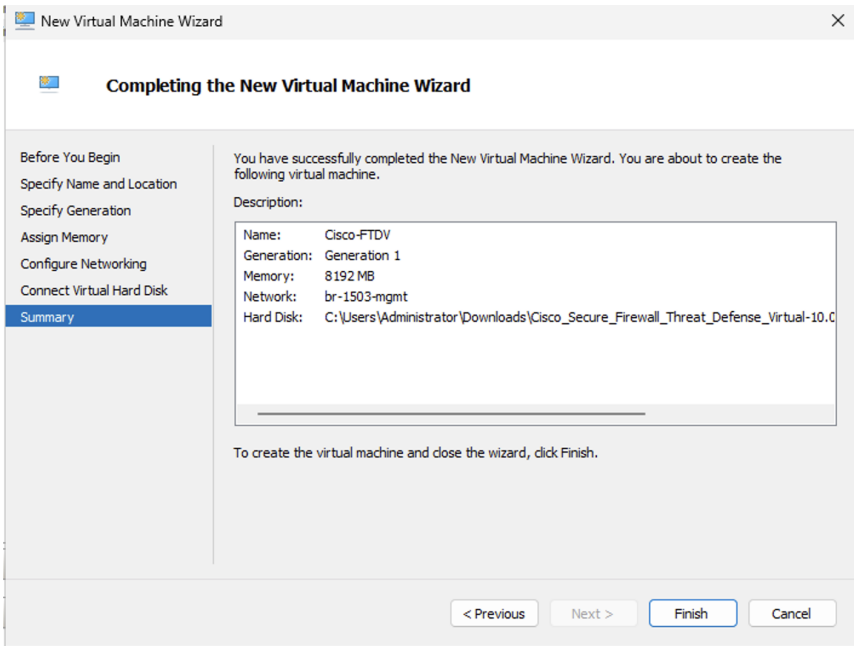
- Threat Defense Virtual 的名称和位置。
- Threat Defense Virtual 的代数。

  为 BIOS 启动模式选择**第 1 代**。

  为 UEFI 启动模式选择**第 2 代**。
- Threat Defense Virtual 的内存量。

  最低要求：8 GB
- 网络适配器（连接到您已设置的虚拟交换机）
- 虚拟硬盘和位置。
- 选择**使用现有的虚拟硬盘**，然后浏览到 **VHDX 文件的位置**。

步骤 6 点击**完成**以完成初始 VM 的创建。系统将显示一个对话框，显示您的 Threat Defense Virtual 配置。

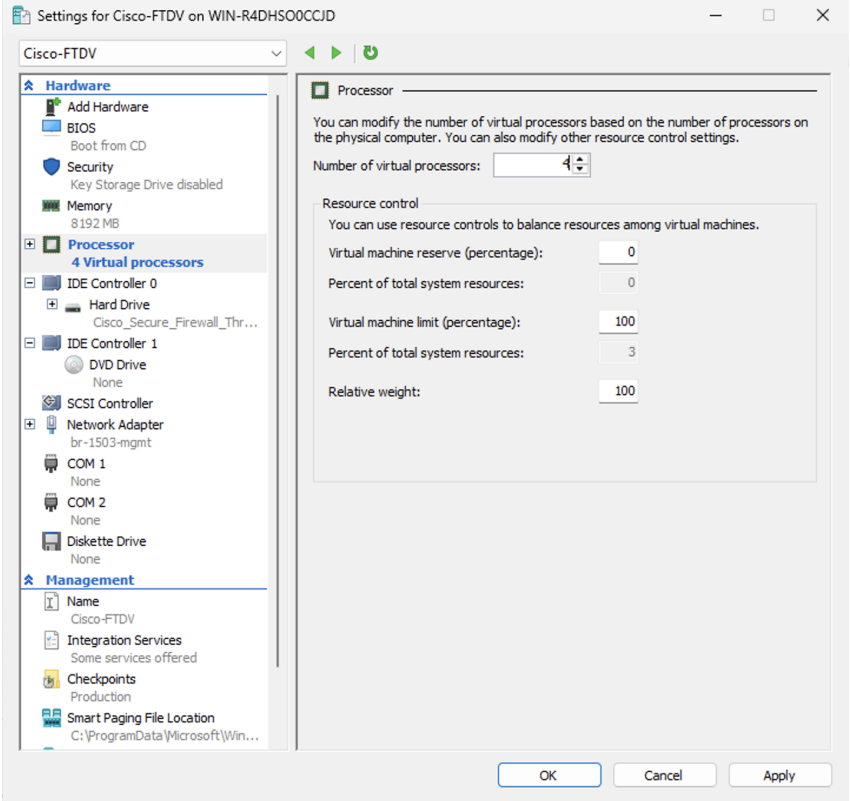


步骤 7 配置 VM 并分配 vCPU。

在启动 Threat Defense Virtual 之前，您必须修改 vCPU 值。在 Hyper-V 管理器右侧点击**设置**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 菜单下，点击**处理器 (Processor)** 以访问“处理器”(Processor) 窗格。

在**虚拟处理器数量**下，输入所需的 vCPU 计数。

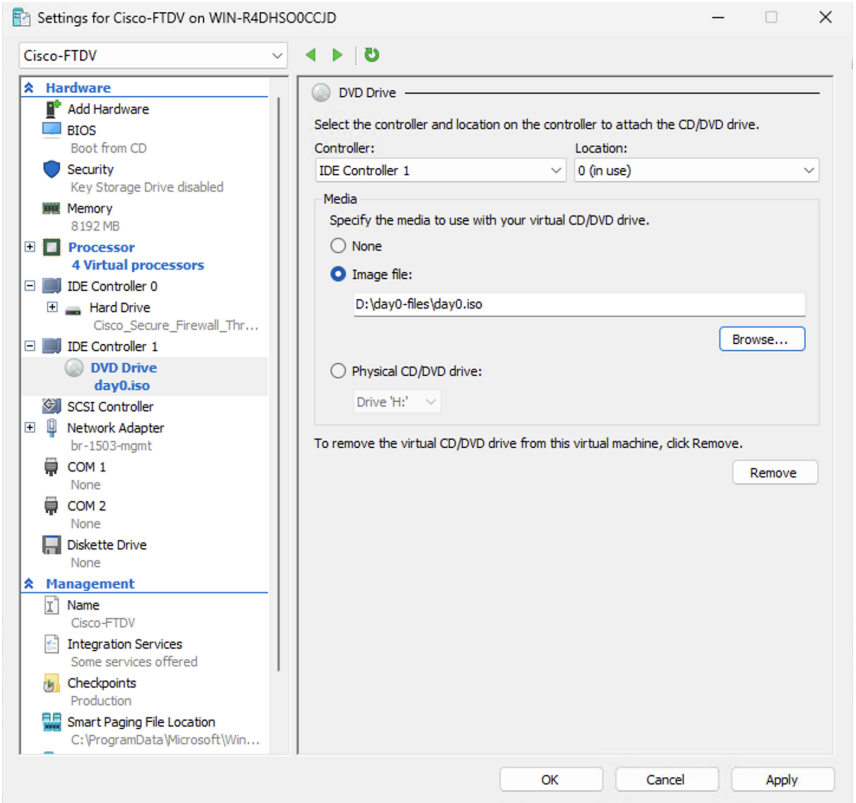
最低要求：4 个 vCPU。



步骤 8 附加 Day-0 配置文件。

在 Hyper-V 管理器右侧点击**设置**。**设置**对话框将打开。在左侧的**硬件**下，选择 **DVD 驱动器** > **映像文件**。

浏览并选择包含 Day 0 配置的 **day0.iso** 文件，然后点击**应用**。当您首次启动 Threat Defense Virtual 时，系统将基于 Day 0 配置文件中的内容进行配置。



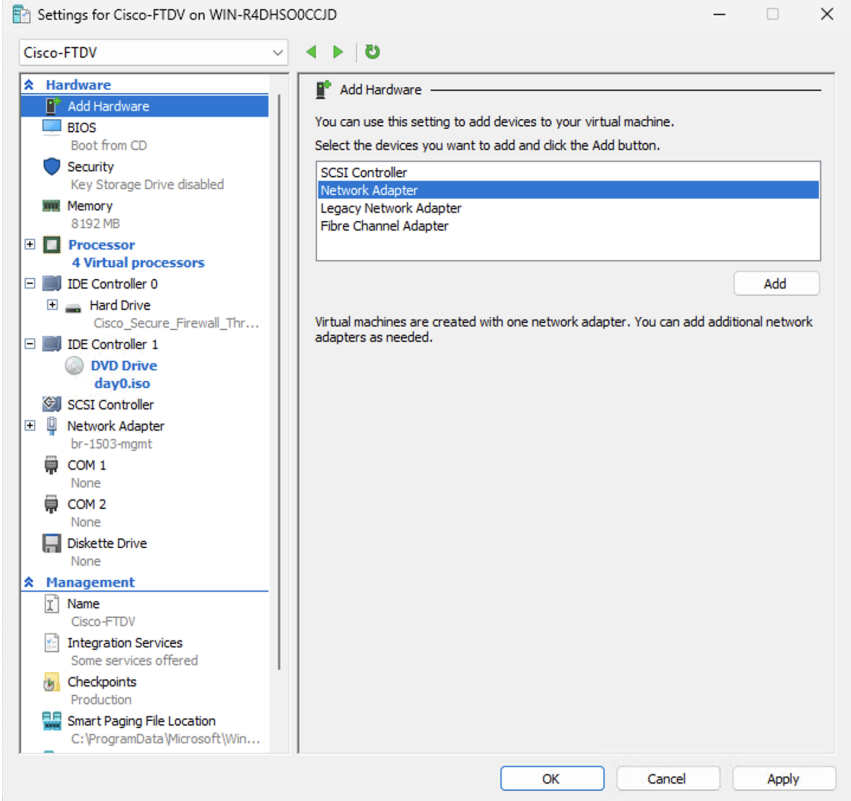
步骤 9 添加网络适配器。

新部署的 Threat Defense Virtual 只有一个网络适配器。您需要至少添加两个网络适配器。在本示例中，我们将添加内部网络适配器。

准备工作

- Threat Defense Virtual 必须处于关闭状态。
- 在 Hyper-V 管理器右侧点击**设置**。**设置**对话框将打开。在左侧的**硬件**菜单下，点击**添加硬件**，然后点击**网络适配器 > 添加**

注释
请勿使用“旧版网路适配器”。



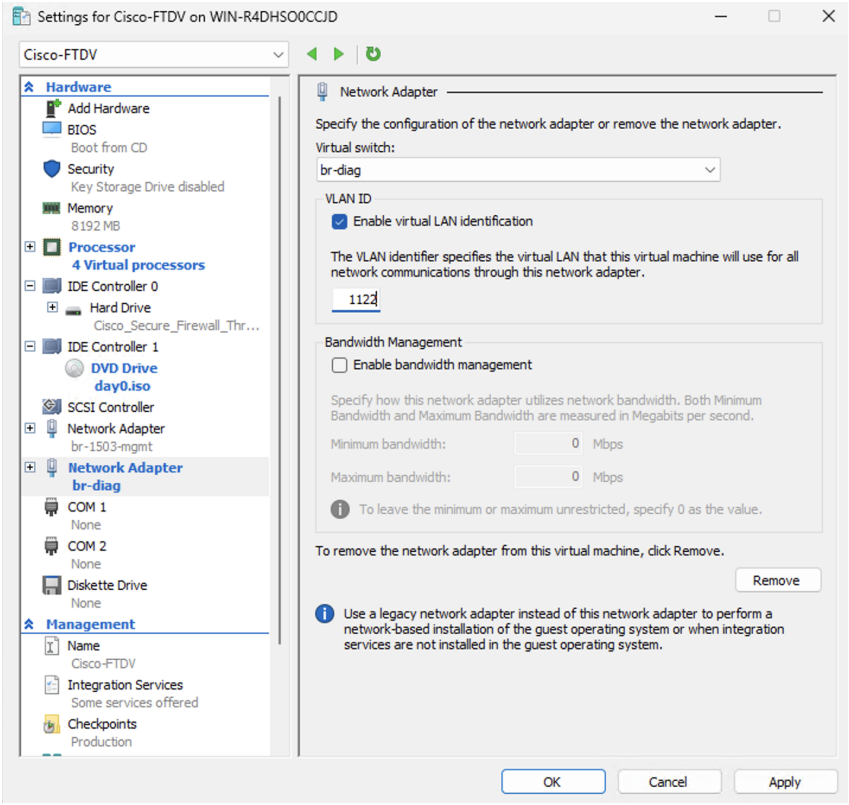
步骤 10 依次点击**添加硬件** > **网络适配器** > **添加**。

为诊断接口为新适配器分配**虚拟交换机**。

启用 **VLAN 标识**并输入 VLAN ID。

对**内部**和**外部**网络适配器重复此过程。

注释
如果对话框关闭，则不需要添加诊断接口。



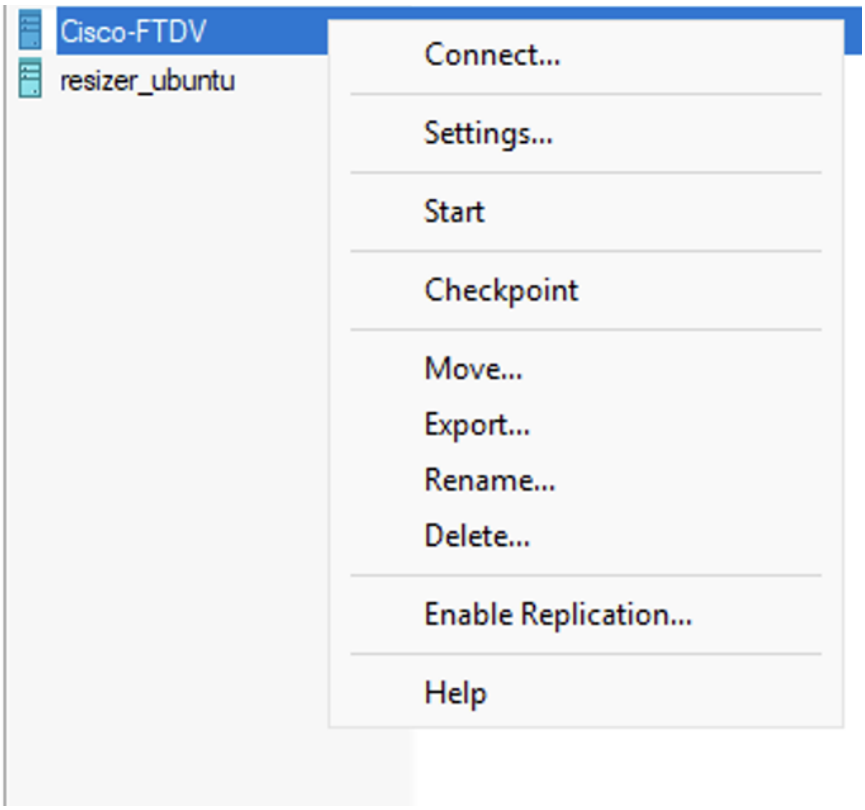
步骤 11 启用安全启动（仅适用于 UEFI）。

如果 VM 是第 2 代（UEFI 启动），请转至**安全**。

启用**安全启动**（如果默认未启用）。

步骤 12 启动 VM。

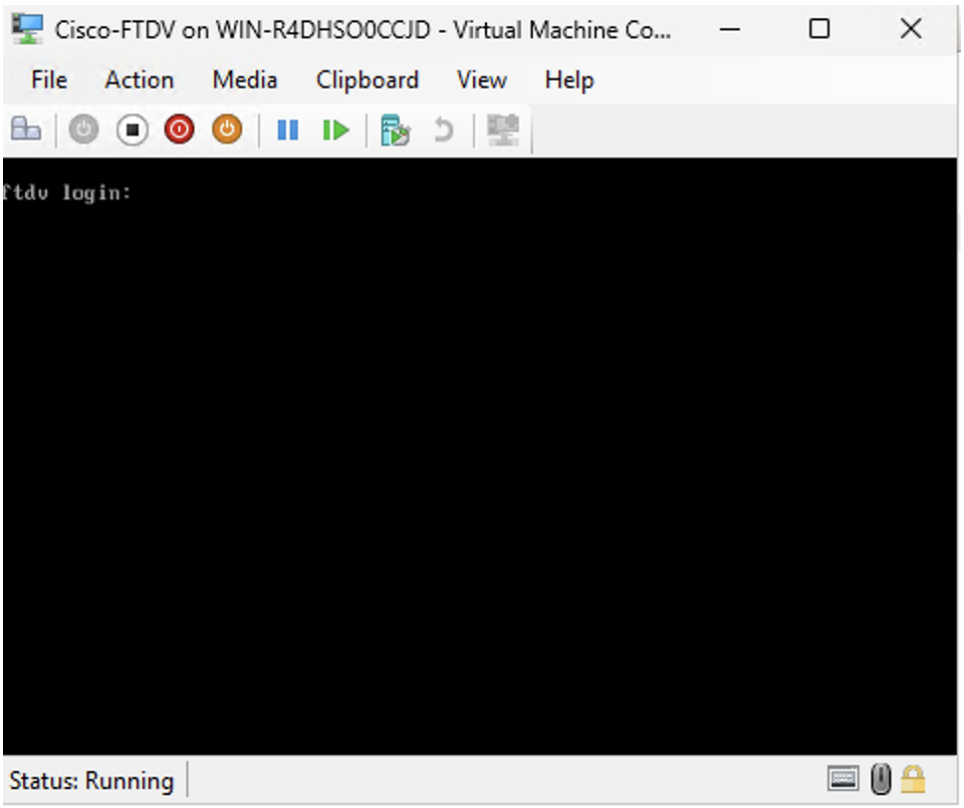
右键点击 VM 并选择**启动**。



VM **电源状态**现在应显示**正在运行**。

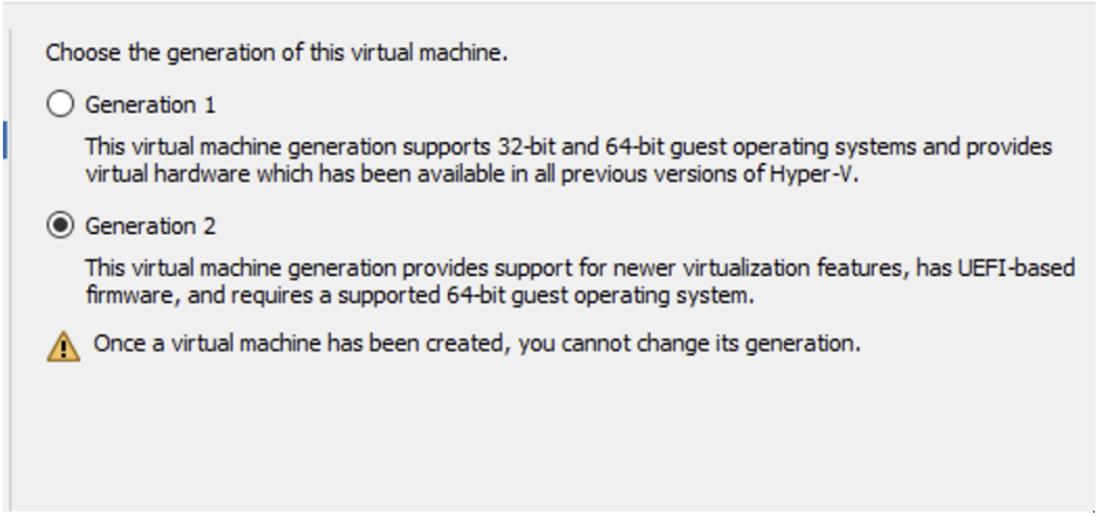
步骤 13 访问控制台。

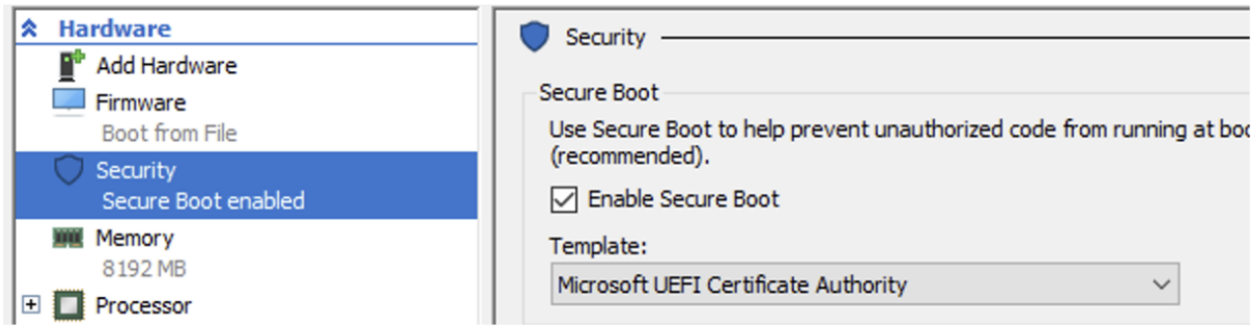
在 Hyper-V 管理器中双击 VM 以打开**控制台会话**。



注释

- 在创建 VM 时，用户必须在指定代数选项卡中选择第 *2* 代。
- 要启用安全启动，请在首次启动之前选择安全启动选项。





选中**启用安全启动**复选框。

选择 **Microsoft UEFI 证书颁发机构**作为模板。

管理 Threat Defense Virtual

停止 Threat Defense Virtual 实例

您可以通过两种方式停止 Threat Defense Virtual。强烈建议使用正常关机。

- 平稳关机（已推荐）

  从 Threat Defense Virtual CLI 启动关闭。

  示例：

```
Cisco Firepower Extensible Operating System (FX-OS) v82.18.0 (build 341i)
Cisco Secure Firewall Threat Defense for Hyper-V v10.0.0 (build 1145)
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': YES
```

- 强制关机（不推荐）

  在 Hyper-V 管理器中，右键点击 VM，然后选择关闭。

注释 这将执行强制关闭，并可能导致数据库损坏。

重启 Threat Defense Virtual（建议平稳重新引导）

始终从 Threat Defense Virtual CLI 启动重新引导，以确保干净重启。

示例：

```
Cisco Firepower Extensible Operating System (FX-OS) v82.14.0 (build 341i)
Cisco Secure Firewall Threat Defense for Hyper-V v10.0.0 (build 1145)
```

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

删除 Threat Defense Virtual

Threat Defense Virtual VM 停止后，在 Hyper-V 管理器中右键点击 VM，然后选择**删除**。

注释 删除 VM 不会删除连接的虚拟硬盘 (VHD)。如果不再需要磁盘，必须手动将其从存储中删除。

故障排除

- 问题 - 无法启动 VM，无法初始化内存。

  场景 - 当磁盘空间不足以初始化 VM 时，会发生此问题。

  解决方法 - 清除 VHD 文件所在磁盘上的空间。

- 问题 - 无法调配或启动 VM；未能打开附件。

  场景 - 当另一个 VM 使用与新 VM 相同的映像时，会发生此问题解决方法 - 删除旧 VM。

- 问题 - 虚拟机启动失败，系统内存不足

  场景 - 当主机操作系统上没有足够的 RAM 来将已配置的内存调配到 VM 时，会发生此问题。
  解决方法 - 确保主机操作系统上有所需的 RAM 可用。

- 问题 - 无法通过 SSH 连接到 Threat Defense Virtual 或从外部主机加载 Threat Defense Virtual UI。

  解决方法 - 在 Windows 防火墙的入站和出站规则中允许端口 22 (SSH)、443 (HTTPS) 和 80 (HTTP)。

- 问题 - 设备无法访问互联网。

  解决办法 - 如果设备使用的是外部虚拟交换机，请确保已正确配置 VLAN 的网关。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。