在 KVM 上部署 Threat Defense Virtual

本章介绍将 threat defense virtual 部署到 KVM 环境的程序。

概述

KVM 是适用于基于 x86 硬件的 Linux 且包含虚拟化扩展（例如英特尔 VT）的完全虚拟化解决方案。其中包含可加载的　内核模块 kvm.ko（用于提供核心虚拟化基础设施）和一个处理器特定模块（例如 kvm-intel.ko）。

您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

Threat Defense Virtual 智能许可的性能层

threat defense virtual 支持性能层许可，该级别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

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
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

请参阅 *Cisco Secure Firewall Management Center*中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。

系统要求

有关 threat defense virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

根据所需部署的实例数量和使用要求， threat defense virtual 部署所使用的具体硬件可能会有所不同。每个 threat defense virtual 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

表 *2: Threat Defense Virtual* 设备资源要求

设置	值
性能级别	**7.0 及更高版本** threat defense virtual 支持性能级许可，该级别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。 • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) 请参阅 *Cisco Secure Firewall Management Center* 配置中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。

设置	值
核心和内存数	**版本 6. 4 至版本 6.7** threat defense virtual 具有可调的 vCPU 和内存资源。支持的 vCPU/内存对值有三种： • 4vCPU/8GB（默认） • 8vCPU/16GB • 12vCPU/24GB 注释 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。仅支持上述三种组合。
	6.3 及更低版本 threat defense virtual 具有固定的 vCPU 和内存资源。支持的 vCPU/内存对值只有一个： • 4vCPU/8GB 注释 不允许调整 vCPU 和内存。
硬盘调配容量	• 50 GB • 可调节设置。支持 virtio 块设备
vNIC	KVM 上的 threat defense virtual 支持以下虚拟网络适配器： • **VIRTIO** - Virtio 是 KVM 中 IO 虚拟化的主要平台，为 IO 虚拟化的虚拟机监控程序提供通用框架。主机实施是在用户空间 qemu 中，因此主机中不需要驱动程序。 • **IXGBE-VF** - ixgbe-vf (10 Gbit/s) 驱动程序支持只能在支持 SR-IOV 的内核上激活的虚拟功能设备。SR-IOV 需要正确的平台和操作系统支持；有关详细信息，请参阅“对 SR-IOV 的支持”。

准则和限制

• 需要两个管理接口和两个数据接口来启动。

注释 threat defense virtual 默认配置将管理接口和内部接口置于同一子网上。

- 支持 virtIO 驱动程序。
- 支持 SR-IOV 的 ixgbe-vf 驱动程序。
- 支持共计 10 个接口

- threat defense virtual 的默认配置假设您将管理接口和内部接口置于**同一子网**，并且管理地址使用内部地址作为访问互联网的网关（经过外部接口）。
- threat defense virtual 首次启动时，必须启用至少四个接口。如果没有四个接口，您的系统将无法部署
- threat defense virtual 支持共计 10 个接口 - 1 个管理接口、1 个保留供内部使用的接口，以及最多 8 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：
  - 管理接口 (1)（必需）

注释 您可以选择为 管理中心 管理配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。请注意，在高可用性部署中，不支持从数据接口进行 管理中心 访问。有关为 管理中心 访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

  - 保留供内部使用 (2)（必需）
  - 外部接口 (3)（必需）
  - 内部接口 (4)（必需）
  - 数据接口 (5-10)（可选）

请查看 threat defense virtual 接口的以下网络适配器、源网络和目标网络的对应关系：

表 *3:* 源网络与目标网络的映射

网络适配器	源网络	目标网络	功能
vnic0*	Management0-0	Management0/0	管理
vnic1	保留供内部使用。	保留供内部使用。	保留供内部使用。
vnic2	GigabitEthernet0-0	GigabitEthernet0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet0/1	内部

网络适配器	源网络	目标网络	功能
*重要信息。连接到同一子网。			

- 不支持克隆虚拟机。
- 对于控制台访问，通过 telnet 支持终端服务器。
- 要在 KVM 上创建具有 IPv6 支持配置的 vNIC，您必须为每个包含 IPv6 配置参数的接口创建一个 XML 文件。您可以使用命令 **virsh net-create** <<*interface configuration XML file name*>> 来安装具有 IPV6 网络协议配置的 vNIC。

  对于每个接口，您可以创建以下 XML 文件：

  - 管理接口 - *mgmt-vnic.xml*
  - 内部接口 - *inside-vnic.xml*
  - 外部接口 - *outside-vnic.xml*

  示例：

  使用 IPv6 配置为管理接口创建 XML 文件。

```
<network>
            <name>mgmt-vnic</name>
            <bridge name='mgmt-vnic' stp='on' delay='0' />
            <ip family='ipv6' address='2001:db8::a111:b220:0:abcd' prefix='96'/>
        </network>
```

  同样，您也必须为其他接口创建 XML 文件。

  您可以通过运行以下命令来验证 KVM 上安装的虚拟网络适配器。

```
virsh net-list
         brctl show
```

CPU 模式

KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

集群

在 KVM 上部署的 Threat Defense Virtual 实例支持集群。有关详细信息，请参阅私有云中 Threat Defense Virtual 的集群。

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅KVM 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

对 SR-IOV 的支持

SR-IOV 虚拟功能需要特定的系统资源。除支持 SR-IOV 功能的 PCIe 适配器之外，还需要支持 SR-IOV 的服务器。

KVM 上使用 SR-IOV 接口的 Threat Defense Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。支持以下 NIC：
  - 英特尔以太网服务器适配器 X710
  - Intel 以太网服务器适配器 X520 - DA2
  - Intel 以太网服务器适配器 E810-CQDA2
    - 使用 NVM 实用程序工具在 Intel® 网络适配器 E810 上更新固件（NVM 映像）和网络驱动程序。非易失性内存 (NVM) 映像和网络驱动程序是一组兼容的组件，您可以在 Intel® 网络适配器 E810 上作为组合进行更新。有关 NVM 和软件兼容性矩阵的信息，请参阅 Intel® 以太网控制器 E810 数据表，以更新英特尔®网络适配器 E810 上的正确固件驱动程序。
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。
- x86_64 多核 CPU - Intel 沙桥或更高版本（推荐）。

注释 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 threat defense virtual 进行了测试。

- 核心
  - 每个 CPU 插槽至少 8 个物理核心
  - 8 个核心必须位于一个插槽中。

注释 建议通过 CPU 固定来实现完整的吞吐量。

- 请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。对于 KVM，您可以验证 SR-IOV 支持方面的 CPU 兼容性。请注意，对于 KVM 上的 threat defense virtual，我们仅支持 x86 硬件。

使用 ixgbe-vf 接口的限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 threat defense virtual 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障转移通过从主用设备向备用设备传送 IP 地址的方式运行。

注释 此限制也适用于 i40e-vf 接口。

- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。
- 在故障转移设置中，当配对的 threat defense virtual（主设备）发生故障时，备用 threat defense virtual 设备将接管主设备的角色，并使用备用 threat defense virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，threat defense virtual 会向同一网络上的其他设备发送免费地址解析协议 (ARP) 更新，以通告接口 IP 地址的 MAC 地址更改。但是，由于与这些类型的接口不兼容，因此不会将免费 ARP 更新发送到用于将接口 IP 地址转换为全局 IP 地址的 NAT 或 PAT 语句中所定义的全局 IP 地址。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您可以使用以下选项来管理 Cisco Secure Firewall Threat Defense Virtual 设备：

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

前提条件

- 从 Cisco.com 下载 threat defense virtual qcow2 文件并将其放在 Linux 主机上：

  https://software.cisco.com/download/navigator.html

注释 需要 Cisco.com 登录信息和思科服务合同。

- 本文档出于示例部署目的，假设您使用 Ubuntu 14.0418.04 LTS。在 Ubuntu 18.04 LTS 主机之上安装以下软件包：
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst

  - virsh tools
  - genisoimage

- 性能受主机及其配置的影响。通过调整主机，您可以最大化 KVM 上的 threat defense virtual吞吐量。有关通用的主机调整概念，请参阅网络功能虚拟化：具备 Linux 和 Intel 架构的宽带远程访问服务器的服务质量。
- Ubuntu 18.04 LTS 的有用优化包括以下各项：
  - macvtap - 高性能 Linux 网桥；您可以使用 macvtap，而不是 Linux 网桥。您必须配置特定设置才能使用 macvtap，而不是 Linux 网桥。
  - 透明大页 - 增加内存页面大小，在 Ubuntu 18.04 中默认开启。
  - 禁用超线程 - 用于将两个 vCPU 减少到一个单核。
  - txqueuelength - 用于将默认 txqueuelength 增加到 4000 个数据包并减少丢包率。
  - 固定 - 用于将 qemu 和 vhost 进程固定到特定 CPU 内核；在某些情况下，固定可显著提高性能。
- 有关优化基于 RHEL 的分布的信息，请参阅《Red Hat Enterprise Linux6 虚拟化调整和优化指南》。
- 有关 KVM 和系统兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。
- 您可以使用以下方法来验证虚拟机是否正在运行 KVM：
  - 运行 **lsmod** 以列出 Linux 内核中的模块。如果 KVM 正在运行，则会显示以下输出来指示 KVM：

    root@kvm-host:~$ lsmod | grep kvm

    kvm_intel 123675 0

    kvm 257361 1 kvm_intel

- 如果目标 VM 上不存在 **ls -l /dev/kvm** ，则您可能正在运行 **qemu**，而没有利用 KVM 硬件辅助功能。

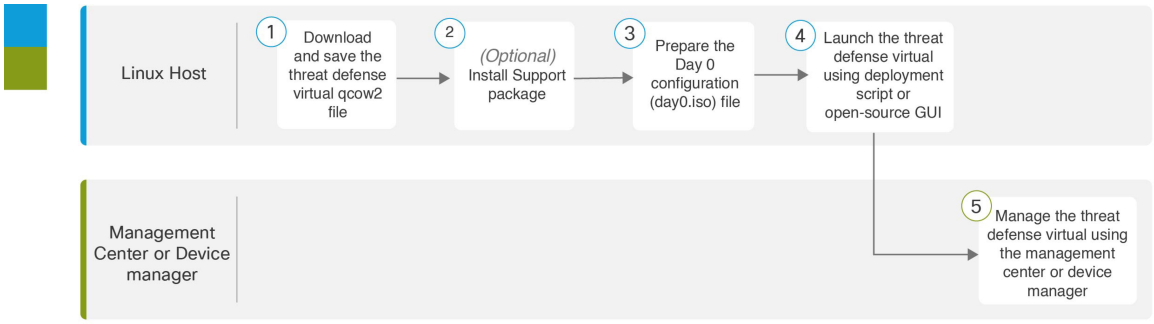
  root@kvm-host:~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm
- 运行以下命令，检查主机是否支持 KVM：

  root@kvm-host:~$ sudo kvm-ok
- 您也可以使用 KVM 加速。

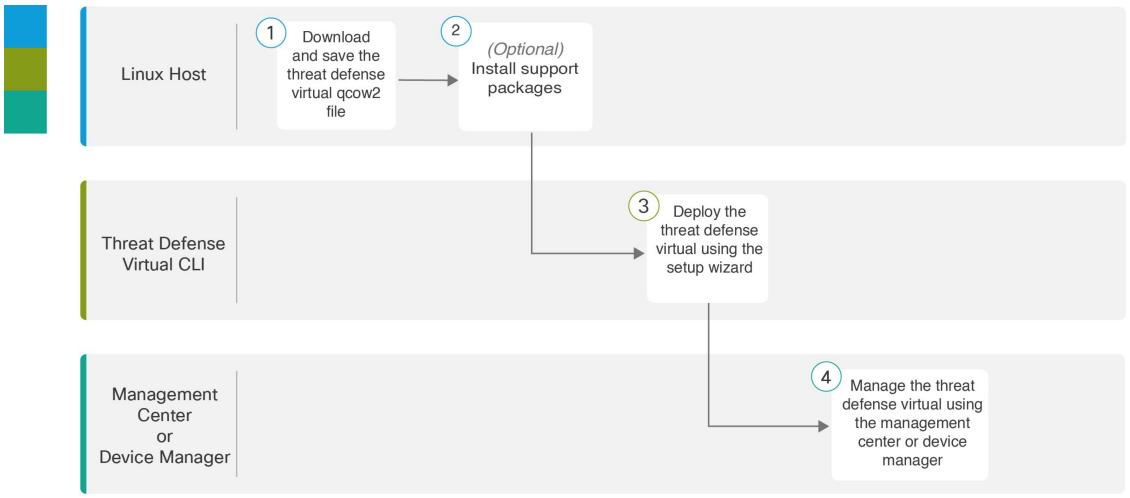
端到端程序

以下流程图说明了使用 Day 0 配置文件在 KVM 实例上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	前提条件，第 8 页：下载 threat defense virtual qcow2 文件并将其保存在 Linux 主机上。
2	Linux 主机	前提条件，第 8 页：安装支持软件包。
3	Linux 主机	准备 Day 0 配置文件
4	Linux 主机	启动 threat defense virtual： • 使用部署脚本启动 • 使用图形用户界面 (GUI) 进行启动
5	管理中心	使用管理中心管理 threat defense virtual。

以下流程图说明了在不使用 Day 0 配置文件的情况下在 KVM 实例上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	前提条件，第 8 页：下载 threat defense virtual qcow2 文件并将其保存在 Linux 主机上。
2	Linux 主机	前提条件，第 8 页：安装支持软件包。
3	Threat Defense Virtual CLI	在没有 Day 0 配置文件的情况下启动：使用设置向导部署 threat defense virtual。
4	管理中心	使用管理中心管理 threat defense virtual

准备 Day 0 配置文件

在启动 threat defense virtual之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。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，并写入首次启动时装载和读取的 day0.iso 文件。

重要事项 该 day0.iso 文件必须在首次启动期间可用。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 threat defense virtual 设备的整个初始设置。可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。

- 管理模式；请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备。

  您可以将**本地管理**设置为**是**，或者输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的信息。对于您未使用的管理模式，保留字段为空。

- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地 设备管理器 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 设备管理器 配置透明防火墙模式接口。

- 使设备可以在管理网络上进行通信的网络设置。

- 部署类型，您可以在其中指定是在集群模式还是独立模式下部署 threat defense virtual。

如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置系统所需的设置；有关更多信息，请参阅在没有 Day 0 配置文件的情况下启动，第 17 页。

注释 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。

SUMMARY STEPS

1. 在名为“day0-config”的文本文件中输入 threat defense virtual的 CLI 配置。添加网络设置和关于管理 管理中心 的信息。
2. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：
3. 为每个要部署的 设备管理器 重复创建唯一的默认配置文件。

DETAILED STEPS

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。添加网络设置和关于管理 管理中心 的信息。

示例：

在 Day 0 配置文件的 **ManageLocally** 中输入 **Yes** 以使用本地 设备管理器；输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的值。对于您未使用的管理选项，将这些字段留空。

步骤 2 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

或

示例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

步骤 3 为每个要部署的 设备管理器 重复创建唯一的默认配置文件。

下一步做什么

- 如果使用 virt-install，请在 virt-install 命令中添加以下行：

```
--disk path=/home/user/day0.iso,format=iso,device=cdrom \
```

- 如果使用 virt-manager，则可以使用 virt-manager GUI 创建虚拟 CD-ROM；请参阅使用图形用户界面 (GUI) 进行启动，第 15 页。

启动 Threat Defense Virtual

使用部署脚本启动

使用基于 virt-install 的部署脚本启动 threat defense virtual。

请注意，您可以通过选择适合您环境的最佳访客缓存模式来优化性能。正在使用的缓存模式不仅会影响到是否发生数据丢失，还会影响到磁盘性能。

每个 KVM 访客磁盘接口都可以指定以下缓存模式之一：*writethrough*、*writeback*、*none*、*directsync* 或 *unsafe*。*writethrough* 提供读取缓存。*writeback* 提供读取和写入缓存。*directsync* 会绕过主机页面缓存。*unsafe* 可能会缓存所有内容，并忽略来自访客的刷新请求。

- 当主机遇到突然断电时，*cache=writethrough* 有助于降低 KVM 访客计算机上的文件损坏。我们建议使用 *writethrough* 模式。
- 但是，由于 *cache=writethrough* 的磁盘 I/O 写入次数高于 *cache=none*，所以该模式也会影响磁盘性能。
- 如果删除了 *--disk* 选项上的 cache 参数，则默认值为 *writethrough*。
- 未指定缓存选项还有可能大幅减少创建虚拟机所需的时间。这是因为，一些较旧的 RAID 控制器的磁盘缓存能力较差。因此，禁用磁盘缓存 (*cache=none*)，从而使用默认值 *writethrough*，有助于确保数据完整性。
- 从版本 6.4 开始，threat defense virtual 随可调的 vCPU 和内存资源一起部署。在 6.4 版之前，部署的 threat defense virtual 具有固定配置 4VCPU/8GB 设备。请参阅下表，了解每个 threat defense virtual 平台大小的 --vcpus 和 --ram 参数所支持的值。

表 *4: virt-install* 支持的 *vCPU* 和内存参数

--vcpus	--ram	Threat Defense Virtual 平台规模
4	8192	4vCPU/8GB（默认）
8	16384	8vCPU/16GB

--vcpus	--ram	Threat Defense Virtual 平台规模
12	24576	12vCPU/24GB

过程

步骤 1 创建名为“virt_install_ftdv.sh”的 virt-install 脚本。

threat defense virtual虚拟机 (VM) 的名称在此 KVM 主机上的所有其他虚拟机中必须是唯一的。threat defense virtual 可支持多达 10 个网络接口。此示例使用了四个接口。虚拟 NIC 必须是 VirtIO。

注释
threat defense virtual 的默认配置假定您将管理接口、诊断接口和内部接口置于同一子网上。系统至少需要 4 个接口才能成功启动。接口到网络分配必须遵循以下顺序：

- (1) 管理接口（必需）
- (2) 保留供内部使用（必需）
- (3) 外部接口（必需）
- (4) 内部接口（必需）
- (5)（可选）数据接口 - 最多 6 个

示例：

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset \
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --disk path=<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
   --force
```

步骤 2 运行 virt_install 脚本：

示例：

```
/usr/bin/virt_install_ftdv.sh
```

```
Starting install...
Creating domain...
```

此时将出现一个窗口，其中显示虚拟机的控制台。您可以看到虚拟机正在启动。启动虚拟机需要几分钟时间。一旦虚拟机停止启动，您便可以从控制台屏幕发出 CLI 命令。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理 (Manage Locally)**选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备。

使用图形用户界面 (GUI) 进行启动

有多个开源选项可用于通过 GUI 来管理 KVM 虚拟机。以下程序使用 virt-manager（也称为虚拟机管理器）启动 threat defense virtual。Virt-manager 是用于创建和管理访客虚拟机的图形化工具。

注释 KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

过程

步骤 1 启动 virt-manager（**应用** > **系统工具** > **虚拟机管理器**）。

系统可能要求您选择虚拟机监控程序和/或输入您的 root 口令。

步骤 2 点击左上角的按钮，打开**新建虚拟机 (New VM)** 向导。

步骤 3 输入虚拟机的详细信息：

a) 对于操作系统，选择**导入现有的磁盘映像 (Import existing disk image)**。

此方法允许您向其导入磁盘映像（包含预安装的可启动操作系统）。

b) 点击**继续 (Forward)** 继续操作。

步骤 4 加载磁盘映像：

a) 点击**浏览...(Browse...)**，选择映像文件。

b) 选择通用 *(Generic)* 作为**操作系统类型 (OS type)**。

c) 点击**继续 (Forward)** 继续操作。

步骤 5 配置内存和 CPU 选项：

重要事项

threat defense virtual 支持性能级许可，该级别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。

请参阅下表，了解每个 threat defense virtual 平台的 --vcpus 和 --ram 参数所支持的性能层和值。

表 *5:* 虚拟机管理器支持的 *vCPU* 和内存参数

CPU	内存	**Threat Defense Virtual** 平台规模
4	8192	4vCPU/8GB（默认）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

a) 针对 threat defense virtual 平台大小设置**内存 (RAM)** 参数。
b) 针对 threat defense virtual 平台大小设置对应的 **CPU** 参数。
c) 点击**继续 (Forward)**继续操作。

步骤 6 选中**安装前自定义配置 (Customize configuration before install)** 框，指定一个**名称 (Name)**，然后点击**完成 (Finish)**。

执行此操作将会打开另一个向导，您可以在其中添加、删除和配置虚拟机的硬件设置。

步骤 7 修改 CPU 配置：

从左侧面板中，选择**处理器 (Processor)**，然后选择**配置 (Configuration)** > **复制主机 CPU 配置 (Copy host CPU configuration)**。

这会将物理主机的 CPU 型号和配置应用于您的 VM。

步骤 8 配置虚拟磁盘：

a) 从左侧面板中，选择**磁盘 1 (Disk 1)**。
b) 选择**高级选项 (Advanced options)**。
c) 将**磁盘总线**设为 *Virtio*。
d) 将**存储格式**设为 *qcow2*。

步骤 9 配置串行控制台：

a) 从左侧面板中，选择**控制台 (Console)**。
b) 选择**删除 (Remove)**，删除默认的控制台。
c) 点击**添加硬件 (Add Hardware)**，添加一台串行设备。
d) 对于**设备类型 (Device Type)**，选择 *TCP net* 控制台 *(tcp) (TCP net console [tcp])* 。
e) 对于**模式 (Mode)**，选择服务器模式（绑定）*(Server mode [bind])*。
f) 对于**主机 (Host)**，输入 **0.0.0.0** 作为 IP 地址，然后输入唯一的**端口 (Port)** 号。
g) 选中**使用 Telnet** 框。
h) 配置设备参数。

步骤 10 配置看门狗设备，在 KVM 访客挂起或崩溃时自动触发某项操作：

a) 点击**添加硬件 (Add Hardware)**，添加一台看门狗设备。

b) 对于**型号 (Model)**，选择默认值 *(default)*。
c) 对于**操作 (Action)**，选择强制重置访客 *(Forcefully reset the guest)*。

步骤 11 配置至少 4 个虚拟网络接口。

点击**添加硬件 (Add Hardware)** 以添加接口，然后选择 **macvtap** 或指定共享设备名称（使用网桥名称）。

注释
KVM 上的 threat defense virtual 支持共计 10 个接口 - 1 个管理接口、1 个保留供内部使用的接口，以及最多 8 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

vnic0 - 管理接口（必需）

vnic1—保留供内部使用（必需）

vnic2 - 外部接口（必需）

vnic3 - 内部接口（必需）

vnic4-9 - 数据接口（可选）

重要事项
请确保将 vnic0 和 vnic3 映射到同一子网。

步骤 12 如果使用 Day 0 配置文件进行部署，则为 ISO 创建虚拟 CD-ROM：
a) 点击**添加硬件(Add Hardware)**。
b) 选择**存储 (Storage)**。
c) 点击**选择托管或其他现有存储 (Select managed or other existing storage)**，然后浏览至 ISO 文件的位置。
d) 对于**设备类型 (Device type)**，选择 *IDE CDROM*。

步骤 13 配置虚拟机的硬件后，点击**应用 (Apply)**。

步骤 14 点击**开始安装 (Begin installation)**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理 (ManageLocally)**选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备。

在没有 Day 0 配置文件的情况下启动

由于 threat defense virtual 设备没有 Web 界面，如果您在没有 Day 0 配置文件的情况下进行部署，必须使用 CLI 来设置虚拟设备。

首次登录新部署的设备时，必须阅读并接受 EULA。然后，请按照设置提示更改管理员密码，并配置设备的网络设置和防火墙模式。

按照设置提示操作时，如遇单选问题，选项会列在括号内，例如 (*y/n*)。默认值会列在方括号内，例如 [*y*]。按 Enter 键确认选择。

注释 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。

过程

步骤 1 打开 threat defense virtual的控制台。

步骤 2 在 **firepower login** 提示符下，使用默认凭据（**username** *admin*，**password** *Admin123*）登录。

步骤 3 当 threat defense virtual系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式（需要进行本地管理）

步骤 4 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

步骤 5 根据提示完成系统配置。

步骤 6 当控制台返回到 **#** 提示符时，验证设置是否成功。

步骤 7 关闭 CLI。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备。

故障排除

本节提供与虚拟机上的 KVM 部署相关的一些基本故障排除步骤。

验证您的虚拟机是否正在运行 KVM

您可以使用以下方法来验证虚拟机是否正在运行 KVM：

- 运行 **lsmod** 命令以列出 Linux 内核中的模块。如果 KVM 正在运行，则会显示以下输出来指示 KVM：

  root@kvm-host:~$ lsmod | grep kvm

  kvm_intel 123675 0

  kvm 257361 1 kvm_intel

- 如果目标 VM 上不存在 **ls -l /dev/kvm** 命令，则您可能正在运行 **QEMU**，而没有利用 KVM 硬件辅助功能。

  root@kvm-host:~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm

- 运行以下命令，检查主机是否支持 KVM：

  root@kvm-host:~$ sudo kvm-ok

- 您也可以使用 KVM 加速。

部署 Threat Defense Virtual 时遇到启动循环

如果您的虚拟机遇到启动循环，则必须确保以下事项：

- 确保部署具有至少 8 GB 内存的 VM。
- 确保部署具有至少 4 个接口的 VM。
- 确保部署具有至少 4 个 vCPU 的 VM。
- 验证 QEMU 进程是否正在使用服务器类 CPU，例如 SandyBridge、IvyBridge、Haswell 等。使用命令 **ps -edaf | grep qemu** 来检查进程参数。

部署 Management Center Virtual 时遇到启动循环

如果您的虚拟机遇到启动循环，则必须确保以下事项：

- 确保部署的 VM 至少具有 28 GB 内存。

- 确保部署具有至少 4 个接口的 VM。
- 确保部署具有至少 4 个 vCPU 的 VM。
- 验证 QEMU 进程是否正在使用服务器类 CPU，例如 SandyBridge、IvyBridge、Haswell 等。使用命令 **ps -edaf | grep qemu** 来检查进程参数。

部署后故障排除

您可以在 threat defense virtual 上运行以下命令来检查问题，以捕获日志进行调试：**system generate-troubleshoot <space> ALL**

或者，使用 **system generate-troubleshoot <space>**，后跟问号 **(?)** 或 **Tab** 按钮以查看可能的选项或命令。

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。