在 Azure 上部署 Firewall Threat Defense Virtual

本章介绍如何从 Azure 门户部署 Cisco Secure Firewall Threat Defense Virtual。

概述

Cisco Secure Firewall Threat Defense Virtual 已集成到 Microsoft Azure 市场中，并支持以下 VM 大小：

Table 1: Azure 支持的 *VM* 大小和 *Threat Defense Virtual* 版本

Azure VM 大小	属性		vNIC	Threat Defense Virtual 版本
	vCPU	内存 (GB)		
Standard_D3	4	14	4	7.7 或更低版本
Standard_D3_v2	4	14	4	7.7 或更低版本
Standard_D4_v2	8	28	8	6.5 至 7.7
Standard_D5_v2	16	56	8	6.5 至 7.7
Standard_D8s_v3	8	32	4	7.1 或更高版本
Standard_D16s_v3	16	64	8	7.1 或更高版本
Standard_F8s_v2	8	16	4	7.1 或更高版本
Standard_F16s_v2	16	32	4	7.1 或更高版本
Standard_D8_v4	8	32	4	7.7 或更高版本
标准_D16_v4	16	64	8	7.7 或更高版本
Standard_D8s_v4	8	32	4	7.7 或更高版本
Standard_D16s_v4	16	64	8	7.7 或更高版本
Standard_D8_v5	8	32	4	7.7 或更高版本
标准_D16_v5	16	64	8	7.7 或更高版本
Standard_D8s_v5	8	32	4	7.7 或更高版本
Standard_D16s_v5	16	64	8	7.7 或更高版本

Note

- 默认情况下，Threat Defense Virtual 实例在部署时启用了安全访问。
- 从 10.0.0 开始，仅支持第 2 代实例类型。

支持在 Azure 上部署无诊断接口的 Threat Defense Virtual

从 Secure Firewall 版本 7.4.1 开始，默认情况下，Threat Defense Virtual 部署在 Azure 上，具有 4 个接口 — 1 个管理接口和 3 个数据接口。由于支持的最大接口数为 8，因此在部署 Threat Defense Virtual 后最多可以添加 4 个接口，以拥有最多 8 个接口。例如，在标准 D4_v2 虚拟机实例上，您可以部署具有 1 个管理接口和 7 个数据接口的 Threat Defense Virtual。

Note 仅在 Azure 上新部署 Threat Defense Virtual 实例时才会移除诊断界面。

前提条件

- Microsoft Azure 帐户。您可以在 https://azure.microsoft.com/en-us/ 创建一个。

  在 Azure 上创建帐户之后，您可以登录、在市场中搜索 Cisco Firepower Threat Defense，然后选择“Cisco Firepower NGFW Virtual (NGFWv)”项。

- 思科智能账户。您可以在 Cisco 软件中心创建一个。

  许可Firewall Threat Defense Virtual；有关防火墙系统功能许可的概述（包括有用链接），请参阅*Cisco Secure Firewall Management Center* 功能许可证。

- 有关 Firewall Threat Defense Virtual 和系统兼容性，请参阅 Firewall Threat Defense Virtual 兼容性。

通信路径

- 管理接口 - 用于将 Firewall Threat Defense Virtual 连接到 Secure Firewall Management Center。

Note 在 6.7 和更高版本中，可以选择为 防火墙管理中心 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。有关为 防火墙管理中心 访问配置数据接口的详细信息，请参阅*Cisco Secure Firewall Threat Defense* 命令参考中的 **configure network management-data-interface** 命令。

- 数据接口（必需）- 用于将 Firewall Threat Defense Virtual 连接到内部和外部主机。

准则和限制

支持的功能

- 仅路由防火墙模式
- Azure 加速网络 (AN)
- 管理模式，两个选择之一：
  - 您可以使用 Secure Firewall Management Center 来管理您的 Firewall Threat Defense Virtual，请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual。

- 您可以使用集成 Cisco Secure Firewall 设备管理器 来管理您的 Firewall Threat Defense Virtual，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual。

- 集群（7.3 及更高版本）。有关详细信息，请参阅公共云中 Threat Defense Virtual 的集群。
- 公共 IP 寻址 - 向管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。

  您可以根据需要为其他接口分配公共 IP 地址；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。
- IPv6

  以下是部署 IPv6 支持的 Firewall Threat Defense Virtual 时必须考虑的准则和限制：
  - 要通过用于 IPv6 支持的 Azure CLI 方法启用编程部署选项，不需要预部署 Firewall Threat Defense Virtual 实例。
  - 您无法从 Azure 市场将 Firewall Threat Defense Virtual 添加到您已手动从 IPV4 升级到 IPV6 寻址的同一 Vnet。
- Interfaces:
  - Firewall Threat Defense Virtual默认情况下随 4 个 vNIC 一起部署。
  - 通过支持较大的实例，您最多可以将 Firewall Threat Defense Virtual 随 8 个 vNIC 一起部署。
  - 要为 Firewall Threat Defense Virtual 部署添加其他 vNIC，请参阅为虚拟机添加网络接口或从虚拟机移除网络接口中提供的信息。
  - 要更改 vNIC 的配置，或者如果需要 IP 转发，请参阅创建、更改或删除网络接口中提供的信息。
  - 您可以使用您的管理器配置 Firewall Threat Defense Virtual 接口。有关接口支持和配置的完整信息，请参阅管理平台（防火墙管理中心 或 防火墙设备管理器）对应的配置指南。
- 部署无诊断接口的 Threat Defense Virtual
  - 当部署的 Threat Defense Virtual 没有诊断接口时，您可以在 Firewall Threat Defense Virtual 管理接口或任何数据接口上配置系统日志和 SNMP。
  - 此部署支持集群和 Auto Scale。
  - 不支持 CMI。

Note 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。

许可

- 使用 Cisco 智能许可证帐户的 BYOL（自带许可证）
- PAYG（即付即用）许可，一种基于使用的计费模式，允许客户在不购买 Cisco 智能许可的情况下运行 Firewall Threat Defense Virtual。对于已注册的 PAYG Firewall Threat Defense Virtual 设备，将启用所有许可的功能（恶意软件/威胁/URL 过滤/VPN 等）。许可的功能无法从 防火墙管理中心 编辑或修改。（版本 6.5+）

Note 在 防火墙设备管理器 模式下部署的 Firewall Threat Defense Virtual 设备上不支持 PAYG 许可。

请参阅《Secure Firewall Management Center 管理指南》中的“许可”一章，了解在许可 Firewall Threat Defense Virtual 设备时的准则。

Firewall Threat Defense Virtual 智能许可的性能层

Firewall 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。

Note 任何 Threat Defense Virtual 层许可证均可与任何支持的 Threat Defense Virtual vCPU 或内存配置配合使用。

这允许 Threat Defense Virtual 客户在各种 VM 资源上使用许可证。

这也会增加受支持的 Azure VM 大小的数量。配置 Threat Defense Virtual 虚拟机时，支持的最大核心 (vCPU) 数量为 16，支持的最大内存为 32 GB RAM。

Table 2: 基于授权的 ***Firewall Threat Defense Virtual*** 许可功能限制

性能层	建议的 vCPU/内存配置	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/34 GB	16Gbps	10,000

性能优化

为实现 Firewall 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 AWS 上的虚拟化调整和优化。

接收端扩展 - Firewall 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。

Microsoft Azure 网络适配器 (MANA) NIC

为了保持最佳性能并防止已停止、取消分配并重新启动或重新部署的 VM 自动转换到合成路径，请确保版本 10.0.0 及更早版本上的所有 VM 选择退出 MANA NIC 资格。有关详细信息，请参阅 MANA 对 NVA 的支持。

不支持的功能

- 许可：
  - PLR（永久许可证预留）。
  - PAYG（即付即用）（版本 6.4 及更低版本）
- 网络（其中很多限制是 Microsoft Azure 限制）：
  - 巨帧
  - 802.1Q VLAN
  - 透明模式及其他第 2 层功能；无广播、无组播。
  - 从 Azure 的角度不归设备所有的 IP 地址的代理 ARP（影响某些 NAT 功能）。
  - 混合模式（不捕获子网流量）。
  - 内嵌设置模式，被动模式。

Note Azure 策略阻止 Firewall Threat Defense Virtual 在透明防火墙或内联模式下运行，因为它不允许接口在混合模式下运行。

  - ERSPAN（使用在 Azure 中不会被转发的 GRE）。
- 管理：
  - Azure 门户“重置密码”功能
  - 基于控制台的密码恢复；由于用户没有实时访问控制台的权限，所以无法恢复密码。无法启动密码恢复映像。唯一的办法是部署新的 Firewall Threat Defense Virtual 虚拟机。
- 高可用性（活动/备用）

- VM 导入/导出
- 部署后调整 VM 大小
- 将 VM 的操作系统磁盘的 Azure 存储 SKU 从高级版迁移或更新到标准版 SKU，反之亦然
- 防火墙设备管理器 用户界面（6.4 及更低版本）

Azure DDoS 防护功能

Microsoft Azure 中的 Azure DDoS 防护是在 Firewall Threat Defense Virtual 最前端实施的一项附加功能。在虚拟网络中，启用此功能有助于根据每秒网络预期流量的数据包来保护应用程序免受常见网络层攻击。您可以根据网络流量模式来自定义此功能。

有关 Azure DDoS 防护功能的详细信息，请参阅 Azure DDoS 防护标准概述。

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 Firewall 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 Firewall 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。

UEFI 和安全启动限制

在 Azure 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

Caution 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。

如何管理 Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Secure Firewall Threat Defense Virtual。

Secure Firewall Management Center

如果要管理大量设备或要使用 Firewall Threat Defense 支持的更复杂的功能和配置，请使用 防火墙管理中心（而不是集成的 防火墙设备管理器）来配置您的设备。有关详细信息，请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual

重要事项 您不能同时使用 防火墙设备管理器 和 防火墙管理中心 来管理 Firewall Threat Defense 设备。在启用 防火墙设备管理器 集成管理功能后，将无法使用 防火墙管理中心 来管理 Firewall Threat Defense 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 防火墙管理中心。另一方面，当您向 Firewall Threat Defense 注册 防火墙管理中心 设备时，防火墙设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 防火墙设备管理器 配置迁移到 防火墙管理中心 的选项，反之亦然。选择为 Firewall Threat Defense 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

防火墙设备管理器 是大多数 Firewall Threat Defense 设备上都包含的 Web界面。它可以配置小型网络最常用的软件基本功能。此产品专为仅包含一台或几台设备的网络而设计，在这种网络中，无需使用高性能多设备管理器来控制包含大量设备的大型网络。有关详细信息，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

注释 有关支持的 防火墙设备管理器 设备的列表，请参阅*Cisco Secure Firewall Threat Defense* 兼容性指南。

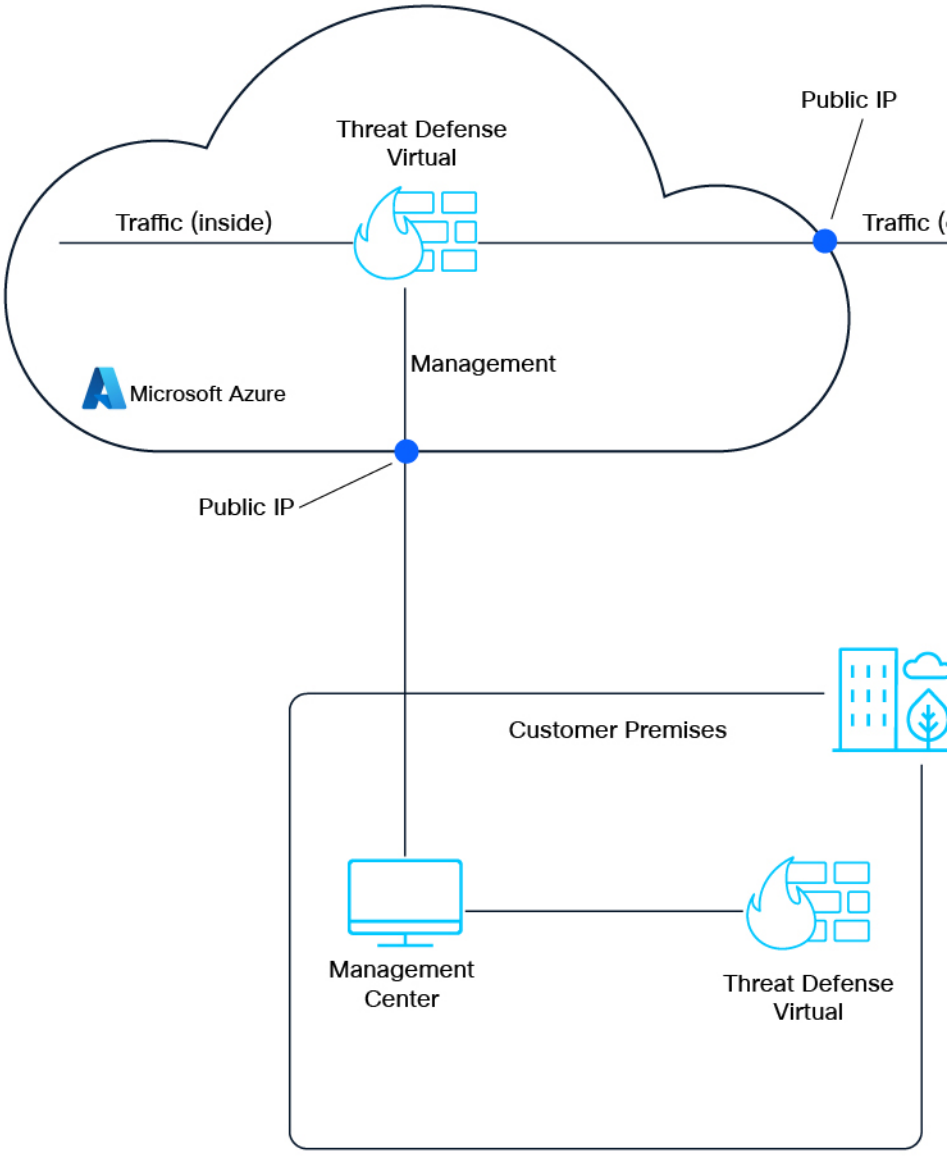
云交付的防火墙管理中心

云交付的防火墙管理中心是一个基于云的管理平台，让您可以集中管理 Secure Firewall Threat Defense Virtual 设备。云交付的防火墙管理中心支持 Secure Firewall Threat Defense Virtual 7.0.3、7.2.0 及更高版本。有关详细信息，请参阅使用 云交付的防火墙管理中心 来管理 Secure Firewall Threat Defense Virtual。

重要事项 您不能将云交付的防火墙管理中心与 防火墙设备管理器 配合使用来管理同一台 Secure Firewall Threat Defense Virtual 设备。

Azure 上 Firewall Threat Defense Virtual 的网络拓扑示例

下图显示了适用于 Azure 内路由防火墙模式下的 Firewall Threat Defense Virtual 的典型拓扑。定义的第一个接口始终是管理接口，并且仅可为管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。


Public IP
Threat Defense
Virtual
Traffic (inside)
Traffic (
Management
Microsoft Azure
Public IP
Customer Premises
Management
Center
Threat Defense
Virtual

在部署期间创建的资源

在 Azure 中部署 Cisco Secure Firewall Threat Defense Virtual 时，会创建以下资源：

- Firewall Threat Defense Virtual 计算机 (VM)
- 一个资源组
  - Firewall Threat Defense Virtual 始终会部署到新的资源组中。不过，您可以将其附加到另一个资源组的现有虚拟网络。
- 四个 NIC，分别名为 *vm name* -Nic0、*vm name* -Nic1、*vm name* -Nic2 和 *vm name* -Nic3

Note 根据要求，您可以创建仅使用 IPv4 或双协议栈（已启用 IPv4 和 IPv6）的 VNet。

  这些 NIC 分别映射到 Firewall Threat Defense Virtual接口 - 管理、GigabitEthernet 0/0、GigabitEthernet 0/1 和 GigabitEthernet 0/2。

- 一个名为 *vm name* -mgmt-SecurityGroup 的安全组。

  此安全组将附加到虚拟机的 Nic0，后者映射到 Firewall Threat Defense Virtual 管理接口。

  该安全组包括允许 SSH（TCP 端口 22）和 防火墙管理中心 接口（TCP 端口 8305）的管理流量的规则。您可以在部署后修改这些值。

- 公共 IP 地址（根据您在部署期间选择的值命名）。

  您可以为任何接口分配一个公共 IP 地址；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。

- 如果选择了“新建网络”选项，会创建一个包含四个子网的虚拟网络。
- 每个子网的路由表（如果已存在，则相应更新）

  这些表的名称为“子网名称”-FTDv-RouteTable。

  每个路由表包含通往其他三个子网的路由，Firewall Threat Defense Virtual IP 地址作为下一跳。如果流量需要到达其他子网或互联网，您可以选择添加默认路由。

- 所选存储帐户中的启动诊断文件

  启动诊断文件将在 Blobs（二进制大对象）中。

- 所选存储帐户中位于 Blobs 和容器 VHD 下的两个文件，名为 *vm name* -disk.vhd 和 *vm name* -<uuid>.status
- 一个存储帐户（除非您选择了现有的存储帐户）

Note 在删除虚拟机时，必须逐个删除每个资源（您要保留的任何资源除外）。

加速网络 (AN)

Azure 的加速网络 (AN) 功能对 VM 启用单根 I/O 虚拟化 (SR-IOV)，允许 VM NIC 绕过虚拟机监控程序并直接转至下面的 PCIe 卡，以加速网络连接。AN 显著提高 VM 的吞吐性能，还会随着内核的增加（例如较大的 VM）而扩展。

AN 在默认情况下禁用。Azure 支持在预调配的虚拟机上启用 AN。您只需在 Azure 中停止 VM 并更新网卡属性，即可将 *enableAcceleratedNetworking* 参数设置为 true。请参阅 Microsoft 文档：在现有虚拟机上启用加速网络。然后重新启动 VM。

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 Firewall 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 Firewall Threat Defense Virtual（主设备）发生故障时，备用设备将接管主设备的角色，并使用备用 Firewall Threat Defense Virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，Firewall 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。

Azure 路由

Azure 虚拟网络子网中的路由取决于子网的有效路由表。有效路由表由内置系统路由和用户定义路由 (UDR) 表中的路由组合而成。

Note 您可以在 VM NIC 属性下查看有效路由表。

您可以查看和编辑用户定义路由表。如果有效路由表是由系统路由与用户定义路由组合而成，系统会优先使用最具体的路由，并关联至用户定义路由表。系统路由表包括指向 Azure 虚拟网络互联网网关的默认路由 (0.0.0.0/0) IPv4 或 [::/0] IPv6。系统路由表还包括通往其他已定义子网的具体路由（下一跳指向 Azure 的虚拟网络基础设施网关）。

要通过 Azure 路由 Firewall Threat Defense Virtual 来传输流量，必须在与每个数据子网关联的用户定义路由表中添加/更新路由。应使用该子网上的 Firewall Threat Defense Virtual IP 地址作为下一跳来传输相应流量。此外，如果需要，可为 0.0.0.0/0 IPv4 或 [::/0] IPv6 的默认路由加上 Firewall Threat Defense Virtual IP 的下一跳。

由于系统路由表中存在现有的具体路由，因此您必须将具体的路由添加到用户定义路由表，以指向作为下一跳的 Firewall Threat Defense Virtual。否则，用户定义表中的默认路由将让步于系统路由表中更具体的路由，并且流量将绕过 Firewall Threat Defense Virtual。

虚拟网络中虚拟机的路由配置

Azure 虚拟网络中的路由取决于有效路由表，而非客户端上的特定网关设置。系统可能通过 DHCP 为虚拟网络中运行的客户端提供路由，即各个子网上最后一位为 .1 的地址。这是一个占位符，仅用于将数据包传送到虚拟网络的基础设施虚拟网关。一旦数据包离开虚拟机，系统会根据有效路由表（由用户定义表修改）对数据包进行路由。有效路由表确定下一跳，无论客户端是具有配置为 .1 还是 Firewall Threat Defense Virtual地址的网关。

Azure 虚拟机 ARP 表将为所有已知主机显示相同的 MAC 地址 (1234.5678.9abc)。这可确保所有离开 Azure 虚拟机的数据包都将到达 Azure 网关，其中有效路由表将用于确定数据包的路径。

IP 地址

以下信息适用于 Azure 中的 IP 地址：

- 系统会为 Firewall Threat Defense Virtual 上的第一个 NIC（映射到 Management）提供其附加到的子网中的私有 IP 地址。

  公共 IP 地址可能与此专用 IP 地址相关联，Azure 互联网网关将处理 NAT 转换。

  在部署 Firewall Threat Defense Virtual 后，您可以将一个公共 IP 地址与一个数据接口（例如，GigabitEthernet0/0）关联；请参阅公共 IP 地址，了解有关公共 IP 的 Azure 准则，包括如何创建、更改或删除公共 IP 地址。

- 您可以在连接到虚拟机规模集 (VMSS) 中的 Firewall Threat Defense Virtual 设备的网络接口中启用 **IP 转发**。如果网络流量不是发往网络接口中的任何已配置 IP 地址，则启用此选项会将此类网络流量转发到虚拟机中配置的 IP 地址以外的其他 IP 地址。有关如何在网络接口中启用 IP 转发 - 启用或禁用 IP 转发，请参阅 Azure 文档。

- 公共 IP 地址（IPv4 和 IPv6）是动态的，在 Azure 停止/启动周期期间可能发生变化。但是，这些地址在 Azure 重新启动期间和 Firewall Threat Defense Virtual重新加载期间保持不变。请参阅 IPv6 公用 IP 地址标准。

- 静态的公共 IP 地址不会发生变化，除非您在 Azure 中进行更改。
- Firewall Threat Defense Virtual 接口可使用 DHCP 设置其 IP 地址。Azure 基础设施可确保为 Firewall Threat Defense Virtual接口分配 Azure 中设置的 IP 地址。

部署 Firewall Threat Defense Virtual

您可以使用模板在 Azure 中部署 Firewall Threat Defense Virtual。Cisco 提供两种类型的模板：

- **Azure 市场中的解决方案模板**-使用 Azure 市场中提供的解决方案模板， Firewall Threat Defense Virtual使用 Azure 门户部署。您可以使用现有资源组和存储帐户（或创建新的资源组和存储帐户）来部署虚拟设备。要使用解决方案模板，请参阅从 Azure 市场使用解决方案模板部署, on page 14。
- **使用来自 VHD**（可从 https://software.cisco.com/download/home 获取）的托管映像的自定义模板 - 除了基于市场的部署，Cisco 还提供一个压缩虚拟硬盘 (VHD)，您可以将其上传到 Azure 以简化 Azure 中的 Firewall Threat Defense Virtual 部署过程。使用托管映像和两个 JSON 文件（一个模板文件和一个参数文件），您可以通过一次协调操作部署并调配 Firewall Threat Defense Virtual 的所有资源。要使用该自定义模板，请参阅从 Azure 使用 VHD 和资源模板部署, on page 18。

Note 在市场中搜索思科产品时，您可能会发现两个名称相似但产品类型不同的产品：应用产品和虚拟机产品。

对于市场部署，仅使用应用产品。

市场中带有VMSR（虚拟机软件预留）计划的虚拟机产品（可能可见）。这些是专门针对渠道/转售的特定多方私人产品计划，常规部署应忽略。

市场中可用的应用产品：

- Cisco Secure Firewall Threat Defense Virtual - BYOL 和 PAYG
- Cisco Secure Firewall Threat Defence for Azure Virtual WAN

从 Azure 市场使用解决方案模板部署

以下说明为您展示如何部署 Azure 市场中提供的 Firewall Threat Defense Virtual 解决方案模板。这是在 Microsoft Azure 环境中设置 Firewall Threat Defense Virtual 所需的顶级步骤列表。如需了解详细的 Azure 设置步骤，请参阅《Azure 入门》。

在 Azure 中部署 Firewall Threat Defense Virtual 时，会自动生成各种配置，例如资源、公共 IP 地址（IPv4 和 IPv6）和路由表。您可以在部署后进一步管理这些配置。例如，您可能需要更改超时值较低的“空闲超时”默认值。

Note 要使用 GitHub 存储库中提供的自定义 ARM 模板，请参阅从 Azure 使用 VHD 和资源模板部署, on page 18。

Procedure

步骤 1 登录到 Azure 资源管理器 (ARM) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 依次选择 **Azure 市场** > **虚拟机**。

步骤 3 在市场中搜索“Cisco Firepower NGFW Virtual (Firewall Threat Defense Virtual)”，选择提供的产品，然后点击**创建**。

步骤 4 配置基本设置。

a) 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

Important
如果使用现有的名称，部署将失败。

b) 选择您的许可方法，可以是 **BYOL** 或 **PAYG**。

选择 **BYOL**（自带许可证）以使用 Cisco 智能许可证帐户。

选择 **PAYG**（即付即用）许可以使用基于使用的计费模式，无需购买 Cisco 智能许可。

Important
PAYG PAYG 许可仅在使用 防火墙管理中心 管理 Firewall Threat Defense Virtual 的情况下受支持。

PAYG 许可不支持 FDM 托管部署，必须改用 **BYOL**。

c) 输入 Firewall Threat Defense Virtual 管理员的用户名。

Note
名称“admin”是 Azure 中的预留名称，不能使用。

d) 选择身份验证类型：密码或 SSH 密钥。

如果您选择密码，请输入密码并确认。

如果选择 SSH 密钥，请指定远程对等体的 RSA 公共密钥。

e) 创建密码，以便搭配**管理员**用户帐户登录以配置 Firewall Threat Defense Virtual。

f) 从 **FTDv 管理 (FTDv Management)** 下拉列表中选择要注册 Firewall Threat Defense Virtual 的管理中心。

如果选择 **FMC：Firepower 管理中心 (FMC: Firepower Management Center)** 作为设备的管理中心，则使用以下选项可以为设备配置管理中心。

- 点击**是**输入 **FMC 注册信息**。

  1. 输入 **FMC IP** 地址。

2. 输入用于注册 Threat Defense Virtual 实例的 **FMC 注册密钥**。
3. [可选] 输入在实例注册期间使用的管理中心 NAT ID。

g) 如果要将部署的虚拟机用作群集，则点击**是**（**提供 day0 群集配置**）**(Yes [provide day0 cluster configuration])** 以创建并输入基本的 day0 配置详细信息。

- 在 **Day0 集群配置 (Day0 cluster configuration)** 字段中输入 day0 配置详细信息。

  有关为 Azure 创建 day0 配置的信息，请参阅在 Azure 上部署 Threat Defense Virtual 集群指南中的为 Azure 创建 Day0 配置。

  Note
  您只能配置部分 day0 配置（集群配置）：{...} 或者 "run_config": [...] 详细信息。

h) 选择您的订用。
i) 创建一个新资源组。

Firewall Threat Defense Virtual 始终会部署到新的资源组中。仅当现有资源组为空时，部署到现有资源组的选项才有效。

不过，您可以在后续步骤中配置网络选项时将 Firewall Threat Defense Virtual 附加到另一个资源组的现有虚拟网络。

j) 选择地理位置。对于此部署中使用的所有资源，此值应相同（例如：Firewall Threat Defense Virtual、网络、存储帐户）。
k) 点击**确定**。

步骤 5 配置 Firewall Threat Defense Virtual 设置。

a) 选择虚拟机大小。
b) 选择一个存储帐户。

Note
您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

c) 选择公共 IP 地址。

您可以为所选的订用和位置选择可用的公共 IP 地址，也可以点击**新建**。

当创建新的公共 IP 地址时，将从 Microsoft 拥有的 IP 地址块中得到一个，因此无法选择特定地址。您可以分配给接口的最大公共 IP 地址数量取决于您的 Azure 订用。

Important
默认情况下，Azure 会创建动态公共 IP 地址。当虚拟机停止和重启时，该公共 IP 可能会变化。如果您首选固定 IP 地址，则应创建静态地址。您也可以在部署后修改公共 IP 地址，将其从动态地址更改为静态地址。

如果 VM 需要分配公用 IPv6 地址，请参阅 IPv6 标准 IPv6 公用 IP 地址标准。

d) 添加 DNS 标签。

Note
完全限定域名等于 DNS 标签加上 Azure URL：<dnslabel>.<location>.cloudapp.azure.com

e) 选择虚拟网络。

您可以选择一个现有 Azure 虚拟网络 (VNet)，或创建一个新的 VNet，然后为其输入 IP 地址空间。默认情况下，无类别域际路由 (CIDR) IP 地址为 10.0.0.0/16。

如果 IPv6 寻址需要虚拟机，您需要在虚拟网络中将其启用。示例：默认情况下，CIDR IPv6 地址为 [ace:cab:deca::/48]。

Note
单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。有关 IPv6 的更多信息，请参阅 Azure IPv6 概述

f) 为 Firewall Threat Defense Virtual 网络接口配置四个子网：

- **FTDv 管理**接口，连接到 Azure 中的 Nic0，是“第一子网”
- **FTDv 数据**接口 1，连接到 Azure 中的 Nic1，是“第二子网”
- **FTDv 数据**接口 2，连接到 Azure 中的 Nic2，是“第三子网”
- **FTDv 数据**接口 3，连接到 Azure 中的 Nic3，是“第四子网”

Note
对于上述子网，如果我们在创建子网时需要 IPv6 配置，请选择 IPv6 选项并为接口配置 IPv6 子网。

g) 提供**公共入站端口 (mgmt.interface)** 输入，以指明是否要为公共开放任何端口。默认选择**无 (None)**。

- 点击**无 (None)** 以创建具有 Azure 默认安全规则的网络安全组并将其连接到管理接口。选择此选项可允许来自同一虚拟网络和 Azure 负载均衡器的流量。
- 点击**允许选定端口查看 (Allow selected ports to view)**，然后选择要开放供互联网访问的入站端口。从**选择入站端口 (Select Inbound Ports)** 下拉列表中选择以下任一端口。默认选择 **SSH (22)**。
  - SSH (22)
  - SFTunnel (8305)
  - HTTPs (443)

h) 点击**确定**。

步骤 6 查看配置摘要，然后点击**确定**。

步骤 7 查看使用条款，然后点击**购买**。

部署时间在 Azure 中有所不同。请等候，直到 Azure 报告 Firewall Threat Defense Virtual 虚拟机正在运行。

Warning
部署后，Firewall Threat Defense Virtual 将开始其首次初始化过程。在此期间，请勿关闭、重新引导或修改 VM。

中断首次启动可能会使系统处于不一致状态，并且可能需要重新部署。在进行任何配置更改之前，请确保首次启动已完全完成。

What to do next

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**选择**否**，您将使用 Secure Firewall Management Center 管理 Firewall Threat Defense Virtual；请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual。
- 如果为**启用本地管理器**选择**是**，您将使用集成的 Cisco Secure Firewall 设备管理器 管理 Firewall Threat Defense Virtual；请参阅使用 Cisco Secure Firewall 设备管理器 来管理 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 Secure Firewall Threat Defense Virtual 设备。

从 Azure 使用 VHD 和资源模板部署

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 Firewall Threat Defense Virtual 映像。要使用 VHD 映像进行部署，您必须将 VHD 映像上传到您的 Azure 存储帐户。然后，您可以使用上传的磁盘映像和 Azure 资源管理器模板创建托管映像。Azure 模板是包含资源说明和参数定义的 JSON 文件。

开始之前

- Firewall Threat Defense Virtual 模板部署需要使用 JSON 模板和相应的 JSON 参数文件。您可以从 Github 存储库下载这些文件。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

  如果您需要创建虚拟机，请使用以下方法之一：

  - 使用 Azure CLI 创建 Linux 虚拟机
  - 通过 Azure 门户创建 Linux 虚拟机

- 在 Azure 订用中，您应该在要部署 Firewall Threat Defense Virtual 的位置具有可用的存储帐户。

过程

步骤 1 从 Cisco 下载软件页面下载 Firewall Threat Defense Virtual 压缩 VHD 映像：

a) 导航至 **产品** > **安全** > **防火墙** > **下一代防火墙 (NGFW)** > **Cisco Secure Firewall Threat Defense Virtua**。

b) 点击 **Firepower 威胁防御软件**。

按照说明下载映像。

例如，Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

步骤 2 将压缩 VHD 映像复制到您在 Azure 中的 Linux 虚拟机。

用于将文件上传到 Azure 和从 Azure 下载文件的选择很多。此示例显示的是 SCP，即安全复制：

```
# scp /username@remotehost.com/dir/Cisco_Secure_Firewall_Threat_Defense_Virtual-7.1.0-92.vhd.bz2
<linux-ip>
```

步骤 3 登录到 Azure 中的 Linux 虚拟机，并导航至复制了压缩 VHD 映像的目录。

步骤 4 解压缩 Firewall Threat Defense Virtual VHD 映像。

用于解压文件的选择很多。此示例显示的是 Bzip2 实用程序，但也可以使用一些基于 Windows 的实用程序。

```
# bunzip2 Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2
```

步骤 5 将 VHD 上传到您的 Azure 存储帐户中的容器。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

用于将 VHD 上传到您的存储帐户的选择很多，包括 AzCopy、Azure 存储复制 Blob API、Azure 存储资源管理器、Azure CLI 或 Azure 门户。对于像 Firewall Threat Defense Virtual 这样大的文件，我们不建议使用 Azure 门户。

下例显示了使用 Azure CLI 的语法：

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

步骤 6 从 VHD 创建托管映像：

a) 在 Azure 门户中，选择**映像 (Images)**。

b) 点击**添加**创建新映像。

c) 提供以下信息：

- **订用** - 从下拉列表中选择订用。
- **资源组** - 选择现有资源组或创建一个新资源组。
- **名称** - 为托管映像输入用户定义的名称。
- **区域**- 选择部署虚拟机的区域。
- **操作系统类型**- 选择 **Linux** 作为操作系统类型。
- **VM 生成**

  为 BIOS 启动模式选择**第 1 代**。

  为 UEFI 启动模式选择**第 2 代**。
- **存储 Blob** - 浏览到存储帐户以选择上传的 VHD。
- **账户类型**- 根据您的要求，从下拉列表中选择标准 HDD、标准 SSD 或高级 SSD。

  选择计划用于部署此映像的 VM 大小时，请确保 VM 大小支持所选账户类型。

- **主机缓存** - 从下拉列表中选择“读/写”。
- **数据磁盘** - 保留默认设置；请勿添加数据磁盘。

d) 点击**创建 (Create)**。

等待**通知 (Notifications)** 选项卡下显示**已成功创建映像 (Successfully created image)** 消息。

注释
创建托管映像之后，可以删除上传的 VHD 和上传存储帐户。

步骤 7 获取新创建的托管映像的资源 ID。

在内部，Azure 将每个资源与一个资源 ID 相关联。从该托管映像部署新的 Firewall Threat Defense Virtual 防火墙时，将需要资源 ID。

a) 在 Azure 门户中，选择**映像 (Images)**。
b) 选择上一步中创建的托管映像。
c) 点击**概述 (Overview)** 查看映像属性。
d) 将 **Resource ID** 复制到剪贴板。

Resource ID 采用以下形式：

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

步骤 8 使用托管映像和资源模板构建 Firewall Threat Defense Virtual 防火墙：

a) 在 Azure GUI 上，搜索**自定义部署**。
b) 在**选择模板**下，点击**在编辑器中生成自己的模板**。

您有一个可供自定义的空模板。有关模板文件，请参阅 Github。

c) 将您的自定义 JSON 模板代码粘贴到窗口中，然后点击**保存**。
d) 从下拉列表中选择**订用 (Subscription)**。
e) 选择现有**资源组 (Resource group)** 或创建一个新资源组。
f) 从下拉列表中选择一个**区域**。
g) 将上一步中的托管映像**资源 ID** 粘贴到 **VM 映像 ID** 字段中。
h) 要在不使用诊断接口的情况下部署 Threat Defense Virtual，请在“自定义数据”字段中输入包含键值对 **Diagnostic: OFF** 的 day-0 配置脚本。下面是一个 day-0 配置脚本示例。

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

注释
键值对 "Diagnostic": "ON/OFF" 区分大小写。

您也可以在用于全新部署的 ARM 模板的“自定义数据”字段中修改脚本。

步骤 9 点击**自定义部署 (Custom deployment)** 页面顶部的**编辑参数 (Edit parameters)**。您有一个可供自定义的参数模板。

a) 点击**加载文件 (Load file)**，然后浏览到自定义 Firewall Threat Defense Virtual 参数文件。有关模板参数，请参阅 Github。

b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后点击**保存**。

步骤 10 检查自定义部署详细信息。请确保 **Basics** 和 **Settings** 中的信息与您预期的部署配置（包括 **Resource ID**）相符。

步骤 11 仔细阅读条款和条件，然后选中**我同意上述条款和条件 (I agree to the terms and conditions stated above)** 复选框。

步骤 12 点击**购买 (Purchase)**，使用托管映像和自定义模板部署 Firewall Threat Defense Virtual 防火墙。

如果您的模板和参数文件中不存在冲突，则部署应该会成功。

托管映像可用于同一个订用和区域内的多个部署。

下一步做什么

- 在 Azure 中更新 Firewall Threat Defense Virtual 的 IP 配置。

在受限制的 Azure Private Marketplace 环境中部署 Azure Marketplace 产品

这仅适用于 Azure Private Marketplace 用户。如果您使用 Azure Private Marketplace，请确保应用产品和所需的虚拟机产品（隐藏）都在相应的专用市场中为用户启用。

虚拟机产品和计划（隐藏）：

- 发布者 ID：**cisco**
- Cisco Secure Firewall Threat Defense Virtual VM 产品（用于两个 Cisco Secure Firewall Threat Defense Virtual 应用产品）
  - 产品 ID：**cisco-ftdv**
  - BYOL 计划 ID：**ftdv-azure-byol**
  - PAYG 计划 ID：**ftdv-azure-payg**

当用户从”市场”部署可见的应用产品时，基于用户对 PAYG 或 BYOL 许可的选择，会引用并部署来自 VM 产品计划的相应映像。

因此，为了使部署正常工作，应用产品和 VM 产品都需要在 Azure 租户/订阅的专用”市场”上启用/可用。

有关在专用市场中启用这些应用和 VM 产品的信息，请参考 Azure 文档。

- 使用专用 Azure Marketplace 进行治理和控制

- 将产品添加到专用市场
- Set-AzMarketplacePrivateStoreOffer

应用产品可通过 Azure UI 轻松启用，因为它们在市场中可见。

为了在专用市场中启用隐藏的虚拟机产品，您可能必须依赖 CLI 命令（在本文档创建时，只有 CLI 方式可行）。

命令示例：

可以使用以下示例命令启用 Cisco Secure Firewall Threat Defense Virtual BYOL 计划：

```
$Params = @{
  privateStoreId =  '<private-store-id>'
  offerId =  '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@( '<plan-id-under-vm-offer>' )
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId =  '<private-store-id>'
  offerId =  'cisco.cisco-ftdv'
  SpecificPlanIdsLimitation =@( 'ftdv-azure-byol' )
}
Set-AzMarketplacePrivateStoreOffer @Params
```

注释 示例命令仅供参考，请查看 Azure 文档了解更多详细信息。

参考错误消息

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
     "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be purchased
 due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's Private
 Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors for
details. "
}
```

用户在部署市场产品时可能会遇到上述错误。要解决此问题，需要在 Azure 租户/订阅上启用/提供应用产品和 VM 产品。

升级场景

您可以根据以下场景升级 Firewall Threat Defense Virtual 实例。

- Cisco Secure Firewall 版本 7.3 及更早版本 – 您可以将部署了诊断接口的 Firewall Threat Defense Virtual 实例升级为具有诊断接口的 Firewall Threat Defense Virtual 实例。
- Cisco Secure Firewall 7.4.1 及更高版本 - 您可以将没有诊断接口的 Firewall Threat Defense Virtual 部署实例升级为没有诊断接口的 Firewall Threat Defense Virtual 实例。

不支持以下升级场景。

- 所有 Cisco Secure Firewall 版本 - 无法将部署了诊断接口的 Firewall Threat Defense Virtual 实例升级到没有诊断接口的 Firewall Threat Defense Virtual 实例。

注释 升级后，NIC 的数量和顺序均保持不变。

部署 Threat Defense Virtual 集群或 Auto Scale 解决方案

部署 Firewall Threat Defense Virtual 集群或 Auto Scale 解决方案需要四个网络接口（一个管理接口和三个数据接口），这些接口在 Azure 市场部署期间分配。Day-0 配置脚本中不需要其他配置。

在 Azure 上部署支持的 IPv6Cisco Secure Firewall Threat Defense Virtual

本章介绍如何从 Azure 门户部署支持 IPv6 的 Firewall Threat Defense Virtual。

关于在 Azure 上部署支持的 IPv6

Firewall Threat Defense Virtual 产品从 7.3 起同时支持 IPV4 和 IPv6。在 Azure 中，您可以直接从市场产品部署 Firewall Threat Defense Virtual ，这样会创建或使用虚拟网络，但是目前，Azure 中的限制将市场应用产品限制为仅使用或创建基于 IPv4 的 VNet/子网。虽然可以手动为现有 VNet 配置 IPv6 地址，但无法将新的 Firewall Threat Defense Virtual 实例添加到配置了 IPv6 子网的 VNet。Azure 对使用替代方法部署任何第三方资源施加了某些限制，而不是通过市场来部署资源。

思科目前提供两种方法来部署 Firewall Threat Defense Virtual 以支持 IPv6 寻址。

提供以下两种不同的自定义 IPv6 模板，其中：

- **自定义 IPv6 模板（ARM 模板）**- 使用 Azure 资源管理器 (ARM) 模板通过 IPv6 配置来部署 Firewall Threat Defense Virtual，该模板会在内部引用 Azure 上的市场映像。此模板包含资源和参数定义的 JSON 文件，您可以配置这些资源和参数以部署支持 IPv6 的 Firewall Threat Defense Virtual。要使用此模板，请参阅使用包含市场映像参考的自定义 IPv6 模板从 Azure 部署, on page 25。

  编程部署是授予对 Azure 市场上的 VM 映像的访问权限，以通过 PowerShell、Azure CLI、ARM 模板或 API 来部署自定义模板的过程。您只能在 VM 上部署这些自定义模板，而无需提供对 VM 的访问权限。如果您尝试在 VM 上部署此类自定义模板，则会显示以下错误消息：

  尚未接受此订用中的此项目的法律条款。要接受法律条款…并为“市场”项目配置程序化部署…

  您可以使用以下方法之一在 Azure 中启用编程部署，以便部署引用市场映像的自定义 IPv6 (ARM) 模板：

  - **Azure 门户** - 启用与 Azure 市场上提供的 Firewall Threat Defense Virtual 产品相对应的编程部署选项，用于部署自定义 IPv6 模板（ARM 模板）。
  - **Azure CLI** - 运行 CLI 命令以启用用于部署自定义 IPv6（ARM 模板）的编程部署。

- **自定义 VHD 映像和 IPv6 模板（ARM 模板）**- 在 Azure 上使用 VHD 映像和 ARM 模板来创建托管映像。此过程类似于使用 VHD 和资源模板部署 Firewall Threat Defense Virtual。此模板在部署期间引用托管映像，并会使用您可以在 Azure 上上传和配置的 ARM 模板来部署支持 IPv6 的 Firewall Threat Defense Virtual。请参阅使用 VHD 和自定义 IPv6 模板从 Azure 部署, on page 30。

根据市场映像或带有自定义 IPv6 模板的 VHD 映像，使用自定义 IPv6 模板（ARM 模板）来部署 Firewall Threat Defense Virtual 所涉及的过程。

部署 Firewall Threat Defense Virtual 所涉及的步骤如下：

Table 3:

步骤	过程
1	在计划部署支持 IPv6 的 Firewall Threat Defense Virtual 的 Azure 中创建 Linux VM
2	仅当使用具有市场映像引用的自定义 IPv6 模板部署 Firewall Threat Defense Virtual 时，才可在 Azure 门户或 Azure CLI 上启用编程部署选项。
3	根据部署类型，下载以下自定义模板： • 具有 Azure 市场参考映像的自定义 IPv6 模板。 具有自定义 IPv6 (ARM) 模板的 VHD 映像。

4	更新自定义 IPv6 (ARM) 模板中的 IPv6 参数。 **Note** 仅当您使用具有市场映像引用的自定义 IPv6 模板来部署 Firewall Threat Defense Virtual 时，才需要市场映像版本的等效软件映像版本参数值。您必须运行命令来检索软件版本详细信息。
5	通过 Azure 门户或 Azure CLI 来部署 ARM 模板。

使用包含市场映像参考的自定义 IPv6 模板从 Azure 部署

参考市场映像使用自定义 IPv6 模板（ARM 模板）部署 Firewall Threat Defense Virtual 所涉及的过程。

Procedure

步骤 1 登录到 Azure 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 通过 Azure 门户或 Azure CLI 启用编程部署，如下所示：

在 Azure 门户上启用此选项：

a) 在 **Azure 服务 (Azure Services)**，点击**订用 (Subscriptions)** 以查看订用边栏选项卡页面。
b) 在左窗格中，点击**设置**选项下的**编程部署**。

随后将显示 VM 上部署的所有类型的资源，以及关联的订用产品。

c) 点击**状态**列下 Firewall Threat Defense Virtual 产品对应的**启用**，以获取自定义 IPv6 模板的编程部署。

或

通过 Azure CLI 启用此选项：

a) 转到 Linux VM。
b) 运行以下 CLI 命令，为部署自定义 IPv6 (ARM) 模板启用编程部署。

在命令执行期间，每个映像订用只能接受一次条款。

 # 接受条款

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # 条款是否已被接受（例如，已接受 = true）

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

其中，

- **<publisher>** - 'cisco'.

- **<offer>** - 'cisco-ftdv'
- **<sku/plan>** - 'ftdv-azure-byol'

以下是启用程序化部署以通过 BYOL 订用计划部署 Firewall Threat Defense Virtual 的一个命令脚本示例。

- **az vm image terms show -p cisco -f cisco-ftdv --plan ftdv-azure-byol**

步骤 3 运行以下命令，以便检索与市场映像版本等效的软件版本详细信息。

az vm image list --all -p <publisher> -f <offer> -s <sku>

其中，

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-ftdv'
- **<sku>** - 'ftdv-azure-byol'

以下是检索等效于 Firewall Threat Defense Virtual 的市场映像版本的软件版本详细信息的一个命令脚本示例。

az vm image list --all -p cisco -f cisco-ftdv -s ftdv-azure-byol

步骤 4 从显示的可用市场映像版本列表中选择一个 Firewall Threat Defense Virtual 版本。

对于 Firewall Threat Defense Virtual 的 IPv6 支持部署，您必须选择 73* 或更高版本的 Firewall Threat Defense Virtual 。

步骤 5 从思科 GitHub 存储库下载市场自定义 IPv6 模板（ARM 模板）。

步骤 6 通过在参数模板文件 (JSON) 中提供部署值来准备参数文件。

下表介绍了您需要在 Firewall Threat Defense Virtual 自定义部署的自定义 IPv6 模板参数中输入的部署值：

参数名	允许的值/类型的示例	说明
vmName	csf-tdv	在 Azure 中为 Firewall Threat Defense Virtual VM 命名。
softwareVersion	730.33.0	市场映像版本的软件版本。
billingType	BYOL	许可方法为 BYOL 或 PAYG。 与 PAYG 相比，BYOL 许可证更具成本效益，因此建议选择 BYOL 订用部署。
adminUsername	hjohn	用于登录 Firewall Threat Defense Virtual 的用户名。 您不能使用保留名称“admin”，该名称已分配给管理员。
adminPassword	E28@4OiUrhx!	管理员密码。

参数名	允许的值/类型的示例	说明
		密码组合必须是长度为 12 到 72 个字符的字母数字字符。密码组合必须由小写和大写字母、数字和特殊字符组成。
vmStorageAccount	hjohnvmsa	您的 Azure 存储帐户。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户字符的长度必须介于 3 到 24 个字符之间。密码组合只能包含小写字母和数字。
availabilityZone	0	指定用于部署的可用性区域，公共 IP 和虚拟机将在指定的可用性区域中创建。 如果不需要可用性区域配置，请将其设置为“**0**”。确保所选区域支持可用性区域，并且所提供的值正确无误。（该值必须是0-3之间的整数）。
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\":\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	要在 Day 0 配置中向 Firewall Threat Defense Virtual 提供的字段。默认情况下，它有以下三个要配置的键值对： • “admin”用户密码 • Firewall Management Center Virtual 主机名 • 用于管理的 Firewall Management Center Virtual 主机名或 CSF-DM。 'ManageLocally : yes' - 这将配置要用作 Firewall Threat Defense Virtual管理器的 CSF-DM。 您可以将 Firewall Management Center Virtual 配置为 Firewall Threat Defense Virtual 管理器，也可以为在 Firewall Management Center Virtual 上进行相同配置所需的字段提供输入。

参数名	允许的值/类型的示例	说明
virtualNetworkResourceGroup	cisco-tdv-rg	包含虚拟网络的资源组的名称。如果 virtualNetworkNewOrExisting 是新的，则此值应与为模板部署选择的资源组相同。
virtualNetworkName	cisco-tdv-vent	虚拟网络的名称。
virtualNetworkNewOrExisting	new	此参数将确定是应创建新的虚拟网络，还是使用现有的虚拟网络。
virtualNetworkAddressPrefixes	10.151.0.0/16	虚拟网络的 IPv4 地址前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	虚拟网络的 IPv6 地址前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet1Name	mgmt	管理子网名称。
Subnet1Prefix	10.151.1.0/24	管理子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	管理子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet1StartAddress	10.151.1.4	管理接口 IPv4 地址。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理接口 IPv6 地址。
Subnet2Name	diag	数据接口 1 子网名称。
Subnet2Prefix	10.151.2.0/24	数据接口 1 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	数据接口 1 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet2StartAddress	10.151.2.4	数据接口 1 IPv4 地址。
subnet2v6StartAddress	ace:cab:deca:2222::6	数据接口 1 IPv6 地址。
Subnet3Name	内部	数据接口 2 子网名称。

参数名	允许的值/类型的示例	说明
Subnet3Prefix	10.151.3.0/24	数据接口 2 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	数据接口 2 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet3StartAddress	10.151.3.4	数据接口 2 IPv4 地址。
subnet3v6StartAddress	ace:cab:deca:3333::6	数据接口 2 IPv6 地址。
Subnet4Name	外部	数据接口 3 子网名称。
Subnet4Prefix	10.151.4.0/24	数据接口 3 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	数据接口 3 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet4StartAddress	10.151.4.4	数据接口 3 IPv4 地址。
subnet4v6StartAddress	ace:cab:deca:4444::6	数据接口 3 IPv6 地址。
vmSize	Standard_D4_v2	Firewall Threat Defense Virtual VM 的大小。Standard_D3_v2 为默认值。

步骤 7 使用 ARM 模板通过 Azure 门户或 Azure CLI 部署 Firewall Threat Defense Virtual 防火墙。有关在 Azure 上部署 ARM 模板的信息，请参阅以下 Azure 文档：

- 使用 Azure 门户创建和部署 ARM 模板
- 通过 CLI 部署本地 ARM 模板

What to do next

接下来的步骤取决于您选择的管理模式。

- 如果您为**启用本地管理器**选择**否**，则您将使用 Secure Firewall Management Center 来管理 Firewall Threat Defense Virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。

- 如果您为**启用本地管理器** 选择**是**，则您将使用集成 Cisco Secure Firewall 设备管理器 来管理 Firewall Threat Defense VirtualFirewall Threat Defense VirtualFirewall Threat Defense VirtualFirewall Threat Defense Virtual；请参阅使用 Cisco Secure Firewall 设备管理器来管理 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。

使用 VHD 和自定义 IPv6 模板从 Azure 部署

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 Firewall Threat Defense Virtual 映像。此过程类似于使用 VHD 和资源模板部署 Firewall Threat Defense Virtual 。

开始之前

- 您需要 JSON 模板和相应的JSON参数文件，以便使用 VHD 和 ARM 更新的模板在 Github 上部署 Firewall Threat Defense Virtual ，您可以在那里找到有关如何构建模板和参数文件的说明。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

  如果您需要创建虚拟机，请使用以下方法之一：

  - 使用 Azure CLI 创建 Linux 虚拟机
  - 通过 Azure 门户创建 Linux 虚拟机

- 在 Azure 订用中，您应该在要部署 Firewall Threat Defense Virtual 的位置具有可用的存储帐户。

过程

步骤 1 从 Cisco 下载软件页面 (Cisco Download Software) 下载 Firewall Threat Defense Virtual 压缩 VHD 映像 (*.bz2)：

a) 导航至 **产品** > **安全** > **防火墙** > **下一代防火墙 (NGFW)** > **Cisco Secure Firewall Threat Defense Virtua**。

b) 点击 **Firepower 威胁防御软件**。

按照说明下载映像。

Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

步骤 2 执行使用 VHD 和资源模板从 Azure 部署中的**步骤 2** 至**步骤 8** 。

步骤 3 点击**自定义部署 (Custom deployment)** 页面顶部的**编辑参数 (Edit parameters)**。您有一个可供自定义的参数模板。

a) 点击**加载文件 (Load file)**，然后浏览到自定义 Firewall Threat Defense Virtual 参数文件。请参阅 Github 上使用 VHD 和自定义 IPv6 (ARM) 模板的 Azure Firewall Threat Defense Virtual 部署示例，您可以在这里找到有关如何构建模板和参数文件的说明。

b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后点击**保存**。

下表介绍了您需要在 Firewall Threat Defense Virtual 部署的自定义 IPv6 模板参数中输入的部署值：

参数名	允许的值/类型的示例	说明
vmName	csf-tdv	在 Azure 中为 Firewall Threat Defense Virtual VM 命名。
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name	用于部署的映像的 ID。在内部，Azure 将每个资源与一个资源 ID 相关联。
adminUsername	hjohn	用于登录 Firewall Threat Defense Virtual 的用户名。 您不能使用保留名称“admin”，该名称已分配给管理员。
adminPassword	E28@4OiUrhx!	管理员密码。 密码组合必须是长度为 12 到 72 个字符的字母数字字符。密码组合必须由小写和大写字母、数字和特殊字符组成。
vmStorageAccount	hjohnvmsa	您的 Azure 存储帐户。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户字符的长度必须介于 3 到 24 个字符之间。密码组合只能包含小写字母和数字。
availabilityZone	0	指定用于部署的可用性区域，公共 IP 和虚拟机将在指定的可用性区域中创建。 如果不需要可用性区域配置，请将其设置为“**0**”。确保所选区域支持可用性区域，并且所提供的值正确无误。（该值必须是 0-3 之间的整数）。
customData	{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}	要在 Day 0 配置中向 Firewall Threat Defense Virtual 提供的字段。默认情况下，它有以下三个要配置的键值对： • “admin”用户密码 • CSF-MCv 主机名 • 用于管理的 CSF-MCv 主机名或 CSF-DM。

参数名	允许的值/类型的示例	说明
		'ManageLocally : yes' - 这将配置要用作 Firewall Threat Defense Virtual管理器的 CSF-DM。 您可以将 CSF-MCv 配置为 Firewall Threat Defense Virtual 管理器，也可以为在 CSF-MCv 上进行相同配置所需的字段提供输入。
virtualNetworkResourceGroup	csf-tdv	包含虚拟网络的资源组的名称。如果 virtualNetworkNewOrExisting 是新的，则此值应与为模板部署选择的资源组相同。
virtualNetworkName	hjohn-vm-vn	虚拟网络的名称。
virtualNetworkNewOrExisting	new	此参数将确定是应创建新的虚拟网络，还是使用现有的虚拟网络。
virtualNetworkAddressPrefixes	10.151.0.0/16	虚拟网络的 IPv4 地址前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	虚拟网络的 IPv6 地址前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet1Name	mgmt-ipv6	管理子网名称。
Subnet1Prefix	10.151.1.0/24	管理子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	管理子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet1StartAddress	10.151.1.4	管理接口 IPv4 地址。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理接口 IPv6 地址。
Subnet2Name	diag	数据接口 1 子网名称。
Subnet2Prefix	10.151.2.0/24	数据接口 1 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。

参数名	允许的值/类型的示例	说明
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	数据接口 1 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet2StartAddress	10.151.2.4	数据接口 1 IPv4 地址。
subnet2v6StartAddress	ace:cab:deca:2222::6	数据接口 1 IPv6 地址。
Subnet3Name	内部	数据接口 2 子网名称。
Subnet3Prefix	10.151.3.0/24	数据接口 2 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	数据接口 2 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet3StartAddress	10.151.3.4	数据接口 2 IPv4 地址。
subnet3v6StartAddress	ace:cab:deca:3333::6	数据接口 2 IPv6 地址。
Subnet4Name	外部	数据接口 3 子网名称。
Subnet4Prefix	10.151.4.0/24	数据接口 3 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	数据接口 3 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet4StartAddress	10.151.4.4	数据接口 3 IPv4 地址。
subnet4v6StartAddress	ace:cab:deca:4444::6	数据接口 3 IPv6 地址。
vmSize	Standard_D4_v2	Firewall Threat Defense Virtual VM 的大小。Standard_D3_v2 为默认值。

步骤 4 使用 ARM 模板通过 Azure 门户或 Azure CLI 部署 Firewall Threat Defense Virtual 防火墙。有关在 Azure 上部署 ARM 模板的信息，请参阅以下 Azure 文档：

- 使用 Azure 门户创建和部署 ARM 模板
- 通过 CLI 部署本地 ARM 模板

下一步做什么

- 在 Azure 中更新 Firewall Threat Defense Virtual 的 IP 配置。

Firewall Threat Defense Virtual 映像快照

您可以在 Azure 门户中使用快照映像创建和部署 Firewall Threat Defense Virtual。映像快照是没有状态数据的已复制 Firewall Threat Defense Virtual 映像实例。

Firewall Threat Defense Virtual 快照概述

创建 Firewall Threat Defense Virtual 实例快照映像的过程跳过为 Firewall Threat Defense Virtual 和 FSIC 执行的首次启动程序，有助于最大限度地缩短初始系统初始化时间。快照映像包含了预填充的数据库和 Firewall Threat Defense Virtual 初始启动过程，该过程使映像能够重新生成与 防火墙管理中心 或任何其他管理中心中的系统身份相关的唯一 ID（UUID、序列号）。此过程有助于缩短 Firewall Threat Defense Virtual 的启动时间，这在 Auto Scale 部署中至关重要。

Note 快照映像创建用于最小化未注册 Cisco Secure Firewall Threat Defense Virtual 上的初始系统初始化时间。它不应用于备份/恢复目的。

Note 目前，使用 Firewall Threat Defense Virtual的快照映像部署的实例不支持即用即付 (PAYG) 许可。PAYG 许可仅适用于直接从市场部署的 实例。您可以将智能许可用于具有 PAYG 许可的新的 Firewall Threat Defense Virtual 部署。

从托管映像创建 Firewall Threat Defense Virtual 快照映像

Firewall Threat Defense Virtual 映像快照创建是在 Azure 门户中复制 Firewall Threat Defense Virtual 实例的现有托管映像的过程。

Before you begin

您必须通过将调整大小的 VHD 映像上传到 Azure 门户中 Linux VM 的 Azure 存储帐户中的容器，创建 Firewall Threat Defense Virtual 版本 7.2 或更高版本的托管映像。有关创建调整大小的 VHD 映像的信息，请参阅从 Azure 使用 VHD 和资源模板部署, on page 18。

不得将正准备拍摄映像快照的 Firewall Threat Defense Virtual 实例注册到任何管理器，例如 防火墙管理中心 或 防火墙设备管理器。

Procedure

步骤 1 转至 Azure 门户，您已在其中创建了 Firewall Threat Defense Virtual 实例的托管映像。

Note
确保您计划复制的 Firewall Threat Defense Virtual 实例未注册到 防火墙管理中心，未配置到任何其他本地管理器，也未通过任何配置应用。

步骤 2 转至**资源组 (Resource Group)**，然后选择 Firewall Threat Defense Virtual 实例。

步骤 3 点击 Firewall Threat Defense Virtual 实例的导航页面上的**串行控制台 (Serial Console)**。

步骤 4 使用以下脚本从专家 shell 运行预快照进程：

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

在脚本中使用 `prepare_snapshot` 命令时，系统会显示一条中间消息，提示您确认执行脚本。按 **Y** 运行脚本。

或者，您可以在此命令后添加 `-f`（例如 `root@firepower:/ngfw/var/common#prepare_snapshot -f`），以跳过用户确认消息并直接执行脚本。

此脚本会删除与 Firewall Threat Defense Virtual 实例关联的所有行配置、已部署的策略、已配置的管理器和 UUID。处理完成后，Firewall Threat Defense Virtual 实例将关闭。

步骤 5 点击**捕获 (Capture)**。

步骤 6 在**创建映像 (Create an image)** 页面中，从**资源组 (Resource Group)** 下拉列表中选择现有资源组或创建新资源组。

步骤 7 点击**实例详细信息 (Instance Details)** 部分中的**否，仅捕获托管映像 (No, capture only a managed image)**，仅创建托管映像。

步骤 8 为使用 Firewall Threat Defense Virtual 实例的托管映像创建的快照映像提供名称。

步骤 9 点击**查看 + 创建 (Review+Create)** 以创建 Firewall Threat Defense Virtual 实例的新快照映像。

What to do next

使用快照映像部署 Firewall Threat Defense Virtual 实例。请参阅使用快照映像部署 Cisco Secure Firewall Threat Defense Virtual。

使用映像快照部署 Firewall Threat Defense Virtual 实例

Before you begin

Cisco 建议以下操作：

- 确认快照映像可用于 Firewall Threat Defense Virtual 实例。

Procedure

步骤 1 登录到 Azure 门户。

步骤 2 复制新创建快照映像的资源 ID。

Note
Azure 会为每个资源（快照映像）关联一个资源 ID。部署新的 Firewall Threat Defense Virtual 实例需要快照映像的资源 ID。

a) 在 Azure 门户中，选择**映像 (Images)**。
b) 选择您使用托管映像创建的快照映像。
c) 点击**概述 (Overview)** 查看映像属性。
d) 将 **Resource ID** 复制到剪贴板。**Resource ID** 语法表示为：
/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

步骤 3 使用快照映像继续部署 Firewall Threat Defense Virtual 实例。请参阅从 Azure 使用 VHD 和资源模板部署, on page 18。

Note
您可以从 Firewall Threat Defense Virtual 控制台运行 CLI 命令 **show version** 和 **show snapshot detail**，以了解新部署的 Firewall Threat Defense Virtual 实例的版本和详细信息。

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。

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。