在 Azure 上部署 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 集成到 Microsoft Azure 市场中，支持以下实例类型：

- 标准 D3 - 4 个 vCPU，14 GB，4vNIC
- 标准 D3_v2 - 4 个 vCPU，14 GB，4vNIC
- 标准 D4_v2 - 8 个 vCPU，28 GB，8 个 vNIC（**版本 6.5 中新增**）
- 标准 D5_v2 - 16 个 vCPU，56 GB，8 个 vNIC（**版本 6.5 中新增**）
- Standard_D8s_v3 - 8 个 vCPU，32 GB，4 个 vNIC（**7.1 版新增功能**）
- Standard_D16s_v3 - 16 个 vCPU，64 GB，8 个 vNIC（**7.1 版新增功能**）
- Standard_D8s_v2 - 8 个 vCPU，16 GB，4 个 vNIC（**7.1 版新增功能**）
- Standard_F16s_v2 - 16 个 vCPU，32 GB，4 个 vNIC（**7.1 版新增功能**）

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 threat defense virtual 和系统兼容性，请参阅 Threat Defense Virtual 兼容性。

通信路径

- 管理接口 - 用于将 threat defense virtual 连接到 Cisco Secure Firewall Management Center。

Note 在 6.7 和更高版本中，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。有关为 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。

- 诊断接口 - 用于诊断和报告；不能用于直通流量。
- 内部接口（必需）- 用于将 threat defense virtual连接到内部主机。

- 外部接口（必需）- 用于将 threat defense virtual连接到公共网络。
- 从 Cisco Secure Firewall 版本 7.4.1 开始，您可以删除诊断接口，并使用至少 3 个接口（1 个管理接口和 2 个数据接口）在 Azure 上部署 Threat Defense Virtual。我们建议您在没有 Cisco Secure Firewall 版本 7.4.1 的诊断接口的情况下在 Azure 上部署 Threat Defense Virtual。有关详细信息，请参阅关于在 Azure 上部署无诊断接口的 Threat Defense Virtual, on page 19。

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 Cisco Secure Firewall Management Center 来管理您的 threat defense virtual，请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco 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 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。
- 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 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 threat defense virtual 实例。
  - 您无法从 Azure 市场将 threat defense virtual 添加到您已手动从 IPV4 升级到 IPV6 寻址的同一 Vnet。
- Interfaces:
  - 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 threat defense virtual 随 8 个 vNIC 一起部署。
  - 要为 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 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（管理中心 或 设备管理器）对应的配置指南。

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 threat defense virtual。对于已注册的 PAYG 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 管理中心 编辑或修改。（版本 6.5+）

Note 在 设备管理器 模式下部署的 threat defense virtual 设备上不支持 PAYG 许可。

请参阅《Cisco Secure Firewall Management Center 管理指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

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。

Table 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/34 GB	16Gbps	10,000

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 AWS 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。

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 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 threat defense virtual 虚拟机。
- 高可用性（活动/备用）
- VM 导入/导出
- Azure 上的第 2 代 VM 生成
- 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
- 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 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 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

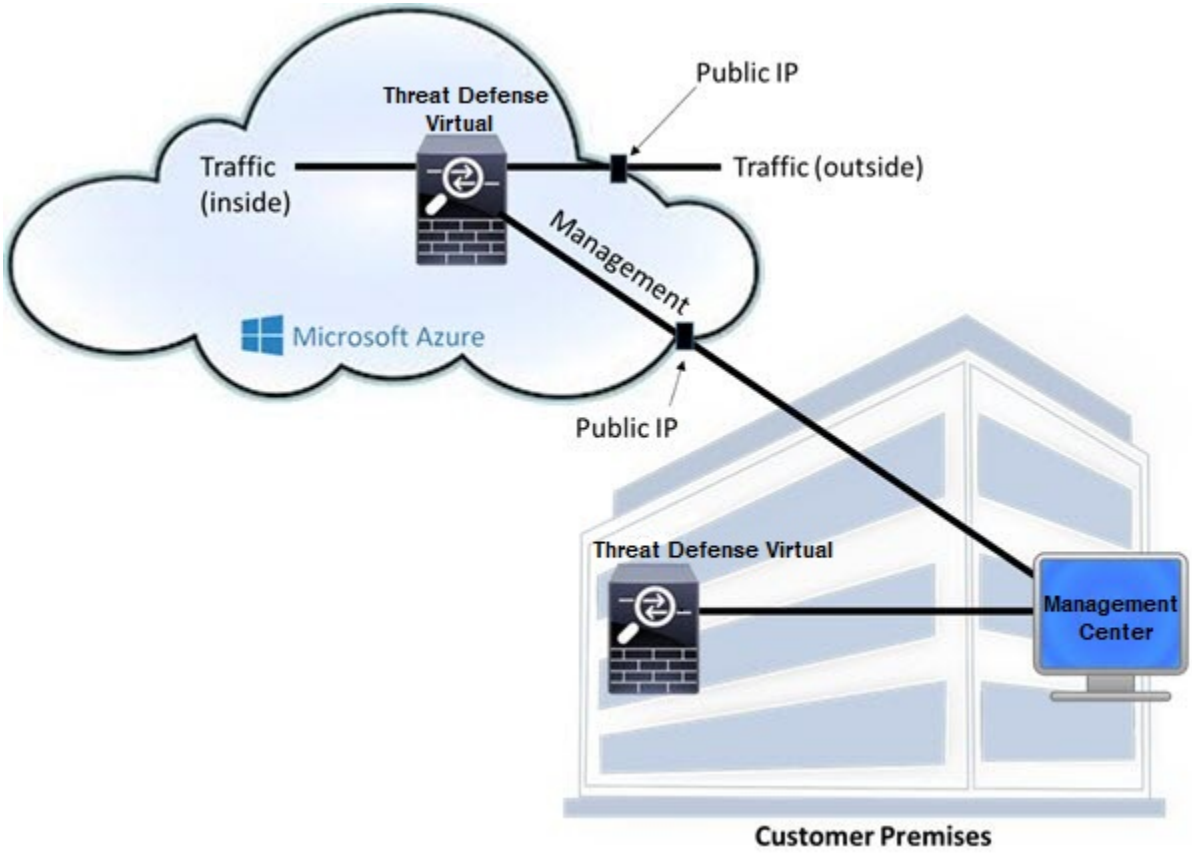
设备管理器 板载集成的管理器。

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》。

Azure 上 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 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。



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：

- threat defense virtual 计算机 (VM)
- 一个资源组

- 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 threat defense virtual 管理、诊断 0/0、GigabitEthernet 0/0 和 GigabitEthernet 0/1 接口。

- 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 threat defense virtual 管理接口。

  该安全组包括允许 SSH（TCP 端口 22）和 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，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 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。

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 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 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 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 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 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 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 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 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 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 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。

- Threat Defense Virtual 接口可使用 DHCP 设置其 IP 地址。Azure 基础设施可确保为 threat defense virtual接口分配 Azure 中设置的 IP 地址。

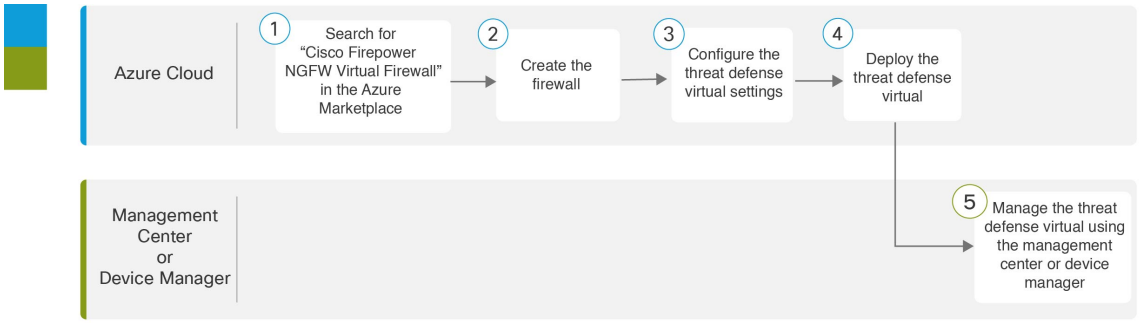
部署 Threat Defense Virtual

您可以使用模板在 Azure 中部署 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， 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 13。
- **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 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 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 16。

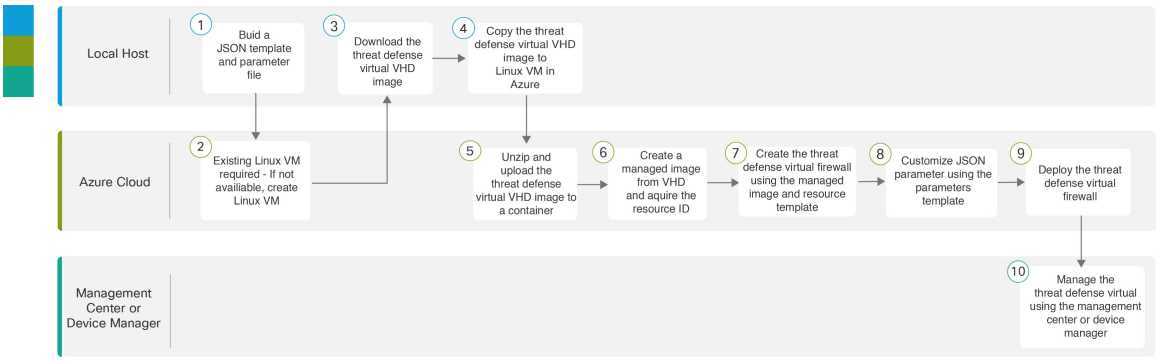
端到端程序

以下流程图说明了使用解决方案模板在 Microsoft Azure 上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	Azure Cloud	从 Azure 市场使用解决方案模板部署：在 Azure 市场中搜索“Cisco Firepower NGFW Virtual Firewall”。
2	Azure Cloud	从 Azure 市场使用解决方案模板部署：创建防火墙。
3	Azure Cloud	从 Azure 市场使用解决方案模板部署：配置 threat defense virtual 设置。
4	Azure Cloud	从 Azure 市场使用解决方案模板部署：部署 threat defense virtual。
5	管理中心或设备管理器	管理 threat defense virtual： • 使用 管理中心 来管理 Threat Defense Virtual • 使用 设备管理器 来管理 Threat Defense Virtual

以下流程图说明了使用 VHD 和资源模板在 Microsoft Azure 上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	本地主机	从 Azure 使用 VHD 和资源模板部署：构建 JSON 模板和参数文件。
2	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：需要现有 Linux VM - 如不可用，请创建 Linux VM： • 使用 Azure CLI 创建 Linux 虚拟机 • 通过 Azure 门户创建 Linux 虚拟机
3	本地主机	从 Azure 使用 VHD 和资源模板部署：从思科下载软件 (使用解决方案模板从 Azure 市场部署) 页面下载 threat defense virtual VHD 映像。
4	本地主机	从 Azure 使用 VHD 和资源模板部署：在 Azure 中将 threat defense virtual VHD 映像复制到 Linux VM。
5	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：解压缩 threat defense virtual VHD 映像并将其上传到容器。
6	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：从 VHD 创建托管映像并获取该映像的资源 ID。
7	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：使用托管映像和资源模板创建 threat defense virtual 防火墙。
8	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：使用参数模板自定义 JSON 参数。
9	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：部署 threat defense virtual 防火墙。
10	管理中心或设备管理器	管理 threat defense virtual： • 使用 管理中心 来管理 Threat Defense Virtual • 使用 设备管理器 来管理 Threat Defense Virtual

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 threat defense virtual 解决方案模板。这是在 Microsoft Azure 环境中设置 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 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 16。

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 (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
您只能在通过 管理中心 管理 threat defense virtual 时使用 **PAYG**。

c) 输入 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 threat defense virtual。

f) 从 **FTDv 管理 (FTDv Management)** 下拉列表中选择要注册 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 (Yes)** 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）："Cluster": {...} 或者 "run_config": [...] 详细信息。

h) 选择您的订用。

i) 创建一个新资源组。

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 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：Threat Defense Virtual、网络、存储帐户）。

k) 点击**确定 (OK)**。

步骤 5 配置 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 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 诊断**接口，连接到 Azure 中的 Nic1，是“第二子网”
- **FTDv 外部**接口，连接到 Azure 中的 Nic2，是“第三子网”
- **FTDv 内部**接口，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 (OK)**。

步骤 6 查看配置摘要，然后点击确定 (OK)。

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 threat defense virtual 虚拟机正在运行。

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

- 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 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 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 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 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 (Add)** 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**- 选择 **第 1 代**。

  注释
  不支持**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 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 Threat Defense Virtual 防火墙：

a) 选择**新建 (New)**，然后搜索**模板部署 (Template Deployment)**，直至可从选项中选择它。
b) 选择**创建 (Create)**。
c) 选择**在编辑器中生成自己的模板 (Build your own template in the editor)**。

您有一个可供自定义的空模板。有关模板文件，请参阅 Github。

d) 将您的自定义 JSON 模板代码粘贴到窗口中，然后点击**保存 (Save)**。
e) 从下拉列表中选择**订用 (Subscription)**。
f) 选择现有**资源组 (Resource group)** 或创建一个新资源组。
g) 从下拉列表中选择**位置 (Location)**。
h) 将上一步中的托管映像**资源 ID (Resource ID)** 粘贴到**虚拟机托管映像 ID (Vm Managed Image Id)** 字段中。

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 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 (Save)**。

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 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 Threat Defense Virtual 的 IP 配置。

关于在 Azure 上部署无诊断接口的 Threat Defense Virtual

在 Cisco Secure Firewall 版本 7.3 及更低版本上， Threat Defense Virtual 部署至少有 4 个接口 - 1 个管理接口、1 个诊断接口和 2 个数据接口。

从 Cisco Secure Firewall 版本 7.4.1 开始，您可以删除诊断接口，并使用至少 3 个接口（1 个管理接口和 2 个数据接口）部署 Threat Defense Virtual。此功能支持在同一实例类型上使用其他数据接口部署 Threat Defense Virtual。例如，在标准 D4_v2 VM 实例上，您现在可以部署具有 1 个管理接口和 7 个数据接口的 Threat Defense Virtual，而不是部署具有 1 个管理接口、1 个诊断接口和 6 个数据接口的 Threat Defense Virtual。

从 Cisco Secure Firewall 版本 7.4.1 开始，我们建议您在没有诊断接口的 Azure 上部署 Threat Defense Virtual。

只有在 Azure 上新部署的 Threat Defense Virtual 实例才支持此功能。

注释 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 5 个接口，以拥有最多 8 个接口。

在 Azure 上部署无诊断接口的 Threat Defense Virtual 的准则和限制

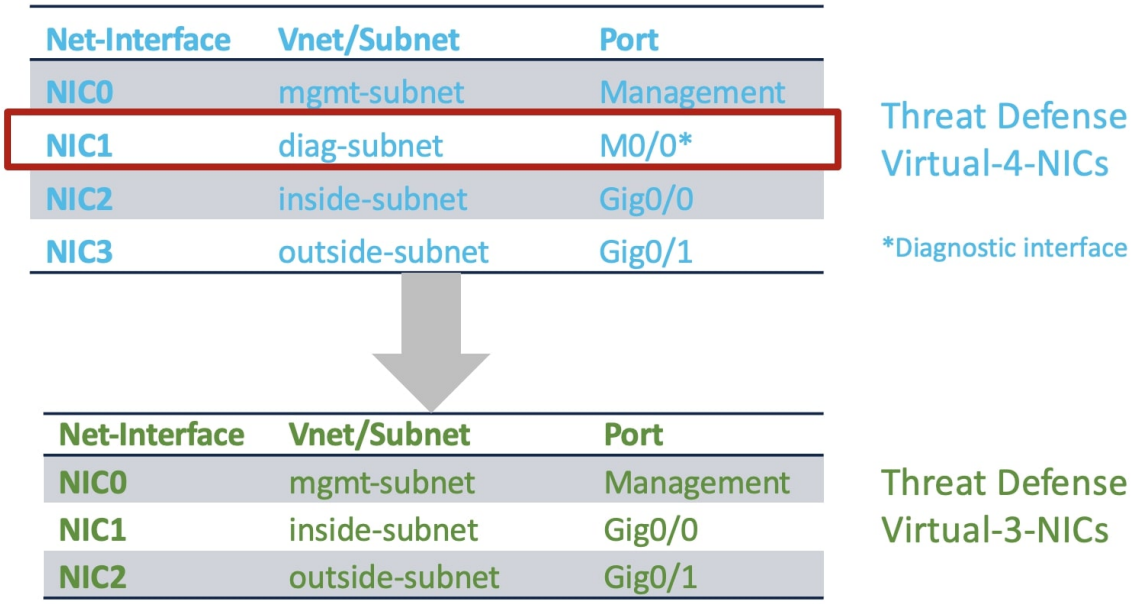
- 当诊断接口被删除时，系统日志和 SNMP 支持使用 Threat Defense Virtual 管理或数据接口，而不是使用诊断接口。
- 此部署支持集群和自动扩展。
- 不支持将具有诊断接口端口的 Threat Defense Virtual 实例和不具有诊断接口端口的 Threat Defense Virtual 实例分组。

注释 此处的 Threat Defense Virtual 实例分组是指 Azure 上的虚拟机规模集 (VMSS) 中的实例分组。这与 Management Center Virtual 上的 Threat Defense Virtual 实例的分组无关。

- 不支持 CMI。

NIC 到数据接口的映射，以便在 AWS 上部署无诊断接口的 Threat Defense Virtual

下面给出了 NIC 到数据接口的映射，用于在 Azure 上部署无诊断接口的 Threat Defense Virtual。



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

执行下面给出的步骤，在没有诊断接口的情况下部署 Threat Defense Virtual。

过程

步骤 1 根据您的部署选项，您可以使用以下方法之一来启用此功能。

- **Solution template in the Azure Marketplace** – 在 Azure 控制台上，搜索 **Cisco Secure Firewall Threat Defense Virtual - BYOL 和 PAYG**，然后点击**创建 (Create)**。在**基本 (Basics)** 信息窗口中，输入所需信息，然后从**软件版本 (Software version)** 下拉列表中选择 **7.4.x**。选择**连接诊断接口 (Attach diagnostic interface)** 旁边的**否 (No)**按钮。默认选择**否**。

  有关在 Azure 市场中使用解决方案模板在 Azure 上部署 Threat Defense Virtual 的完整程序，请参阅从 Azure 市场使用解决方案模板部署。

- **Custom Template using a Managed Image from a VHD** – 转到**虚拟机 (Virtual machines)** > **+ 创建 (+ Create)** > **Azure 虚拟机 (Azure Virtual Machine)** > **高级 (Advanced)** 窗口，然后在 **Custom data** 字段中输入包含键值对 **`Diagnostic: OFF`** 的 day-0 配置脚本。以下显示了您可以在 **Custom data** 字段中输入的 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。

您还可以在用于全新部署的 ARM 模板的 **Customdata** 字段中修改脚本。默认情况下，键值对设置为 **`Diagnostic: ON`**，并且会启动诊断接口。当键值对设置为 **`Diagnostic: OFF`** 时，部署将在没有诊断接口的情况下启动。

有关使用 VHD 中的托管映像使用自定义模板在 Azure 上部署 Threat Defense Virtual 的完整程序，请参阅从 Azure 使用 VHD 和资源模板部署。

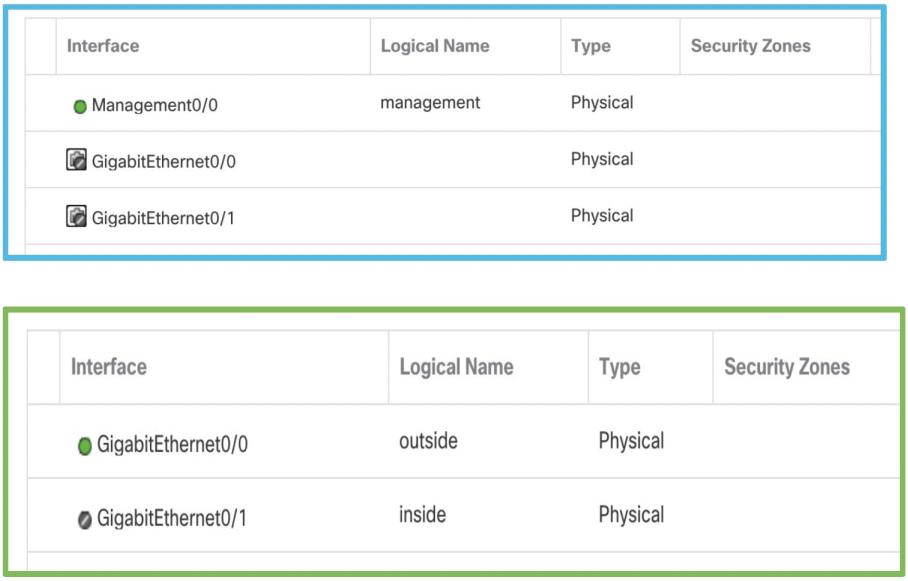
步骤 2 连接所需的最少 3 个 NIC。有关在 Azure 上连接接口的详细信息，请参阅在 Azure 上的虚拟机中添加网络接口或从中删除网络接口。

图 *1: Azure* 上的网络接口连接

有关接口的详细信息，请参阅接口概况。

步骤 3 （可选）在控制台上使用 **show interface ip brief** 命令可显示接口详细信息。您还可以在 Management Center Virtual 上查看接口详细信息，如下所示

接口在 Management Center Virtual 上显示，如下所示。



升级场景

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

- 所有 Cisco Secure Firewall 版本 – 您可以将部署了诊断接口的 Threat Defense Virtual 实例升级为具有诊断接口的 Threat Defense Virtual 实例。
- Cisco Secure Firewall 7.4 及更高版本 - 您可以将没有诊断接口的 Threat Defense Virtual 部署实例升级为没有诊断接口的 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 Threat Defense Virtual 实例升级到没有诊断接口的 Threat Defense Virtual 实例。
- Cisco Secure Firewall 7.4.1 及更高版本 - 您无法将没有诊断接口的 Threat Defense Virtual 部署实例升级为具有诊断接口的 Threat Defense Virtual 实例。

注释 升级后，NIC 的数量和顺序均保持不变。

部署不带诊断接口的 Threat Defense Virtual 集群或 Auto Scale 解决方案

要在不使用诊断接口的情况下对 Threat Defense Virtual 集群或由 Threat Defense Virtual 实例组成的自动扩展解决方案执行新部署，请确保在 day-0 配置脚本中将键值对 **Diagnostic: OFF/ON** 设置为 **OFF**。

故障排除

如果在部署 Threat Defense Virtual 时未删除诊断接口，请检查键值对 **Diagnostic: OFF/ON** 是否已在 day-0 配置脚本中设置为 **OFF**。

适用于 Azure 上的 威胁防御虚拟的 Auto Scale 解决方案

概述

Auto Scale 解决方案支持资源分配，以满足性能要求并降低成本。如果资源需求增加，系统将确保根据需要分配资源。如果资源需求减少，则会取消分配资源以降低成本。

threat defense virtual Auto Scale for Azure 是完整的无服务器实现，它利用 Azure 提供的无服务器基础架构（逻辑应用、Azure 函数、负载均衡器、安全组、虚拟机规模集等）。

threat defense virtual Auto Scale for Azure 实现的一些主要功能包括：

- 基于 Azure Resource Manager (ARM) 模板的部署。
- 支持基于 CPU 和内存 (RAM) 的扩展指标。

注释 有关详细信息，请参阅Auto Scale 逻辑 ， 第 60 页。

- 支持 threat defense virtual 部署和多可用性区域。
- 管理中心 中完全自动化的 threat defense virtual实例注册和取消注册。
- 自动应用到外向扩展 threat defense virtual实例的 NAT 策略、访问策略和路由。
- 对负载均衡器和多可用性区域的支持。
- 支持启用和禁用 Auto Scale 功能。
- 仅适用于 管理中心；不支持 设备管理器。
- 支持使用 PAYG 或 BYOL 许可模式部署 threat defense virtual。PAYG 仅适用于 threat defense virtual软件版本 6.5 和更高版本。请参阅支持的软件平台 ， 第 24 页。

- 思科提供 Auto Scale for Azure 部署包以方便部署。

Azure 上的 threat defense virtual Auto Scale 解决方案支持两种使用不同拓扑配置的使用案例：

- 使用三明治拓扑的 Auto Scale – 它将 threat defense virtual 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。
- 使用 Azure 网关负载均衡器 (GWLB) 的 Auto Scale - Azure GWLB 与安全防火墙、公共负载均衡器和内部服务器集成，以简化防火墙的部署、管理和扩展。

支持的软件平台

threat defense virtual Auto Scale 解决方案适用于 管理中心 管理的 threat defense virtual，与软件版本无关。Cisco Secure Firewall Threat Defense 兼容性指南提供软件和硬件兼容性，包括操作系统和托管环境要求。

- 管理中心：虚拟表列出了 management center virtual 的兼容性和虚拟托管环境要求。
- Threat Defense Virtual 兼容性表列出了 Azure 上 threat defense virtual的兼容性和虚拟托管环境要求。

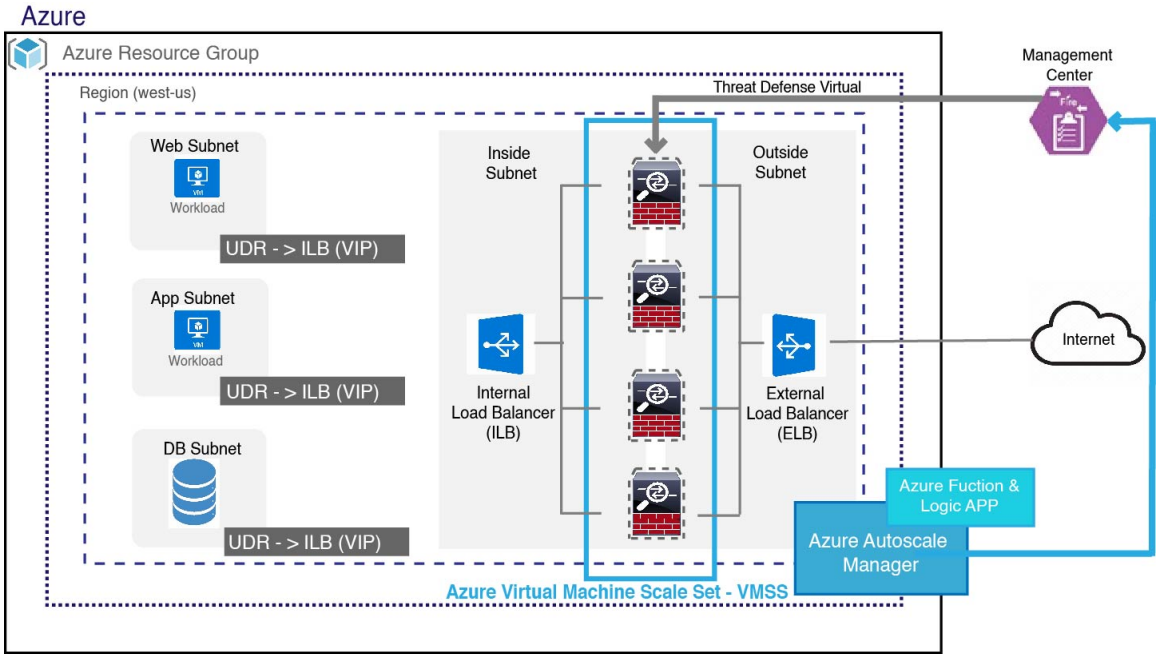
注释 就部署 Azure Auto Scale 解决方案而言，Azure 上的 threat defense virtual最低支持的版本是版本 6.4。

使用三明治拓扑的 Auto Scale 使用案例

适用于 Azure 的 threat defense virtual Auto Scale 是一种自动化水平扩展解决方案，它将 threat defense virtual 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。

- ELB 将流量从互联网分发到规模集中的 threat defense virtual实例；然后，防火墙将流量转发到应用程序。
- ILB 将出站互联网流量从应用程序分发到规模集中的 threat defense virtual实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 threat defense virtual实例数将根据负载条件自动进行扩展和配置。

图 2: 使用三明治拓扑的 *Threat Defense Virtual Auto Scale* 使用案例图



Auto Scale 与 Azure 网关负载均衡器使用案例

Azure 网关负载均衡器 (GWLB) 可确保安全防火墙检查进出 Azure VM（例如应用服务器）的互联网流量，而无需更改任何路由。Azure GWLB 与安全防火墙的集成简化了防火墙的部署、管理和扩展。这种集成还降低了操作复杂性，并为防火墙上的流量提供了单一的入口和出口点。应用和基础设施可以保持源 IP 地址的可视性，而这在某些环境中至关重要。

在 Azure GWLB Auto Scale 使用案例中，threat defense virtual 只会使用两个接口：管理接口和一个数据接口。

注释

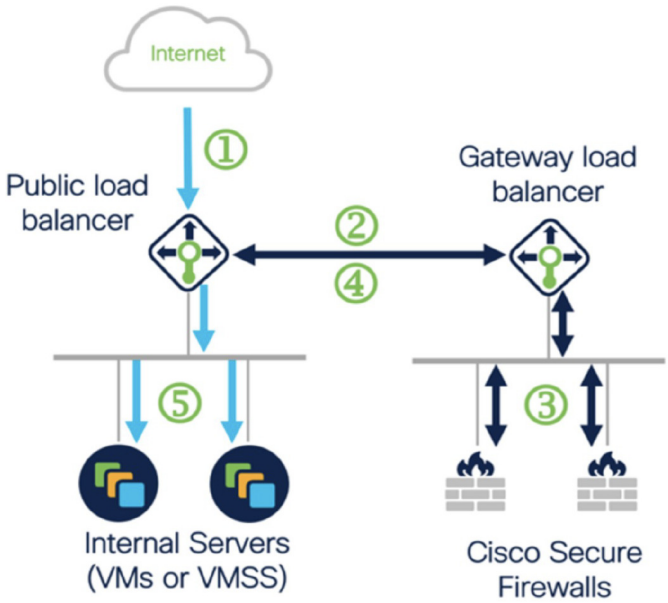
- 如果要部署 Azure GWLB，则不需要网络地址转换 (NAT)。
- 仅支持 IPv4。

许可

支持 PAYG 和 BYOL。

入站流量使用案例和拓扑

下图显示了入站流量的流量。



① Inbound flow uses public IP of public load balancer

② Flow is forwarded transparently from the public load balancer to the gateway load balancer

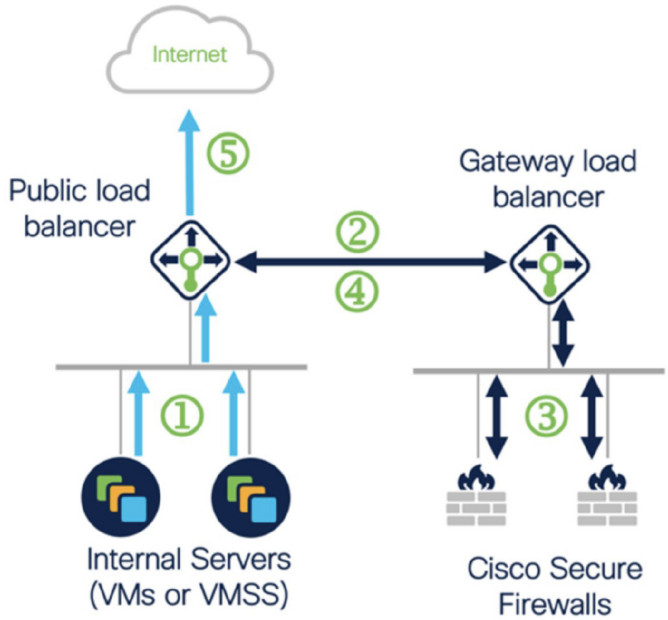
③ Flow is inspected by a firewall and returned to the gateway load balancer

④ Flow is returned to the public load balancer

⑤ Flow is forwarded to an internal server

出站流量使用案例和拓扑

下图显示了出站流量的流量。



① Outbound flow leaves the internal server

② Flow is forwarded transparently from the public load balancer to the gateway load balancer

③ Flow is inspected by a firewall and returned to the gateway load balancer

④ Flow is returned to the public load balancer

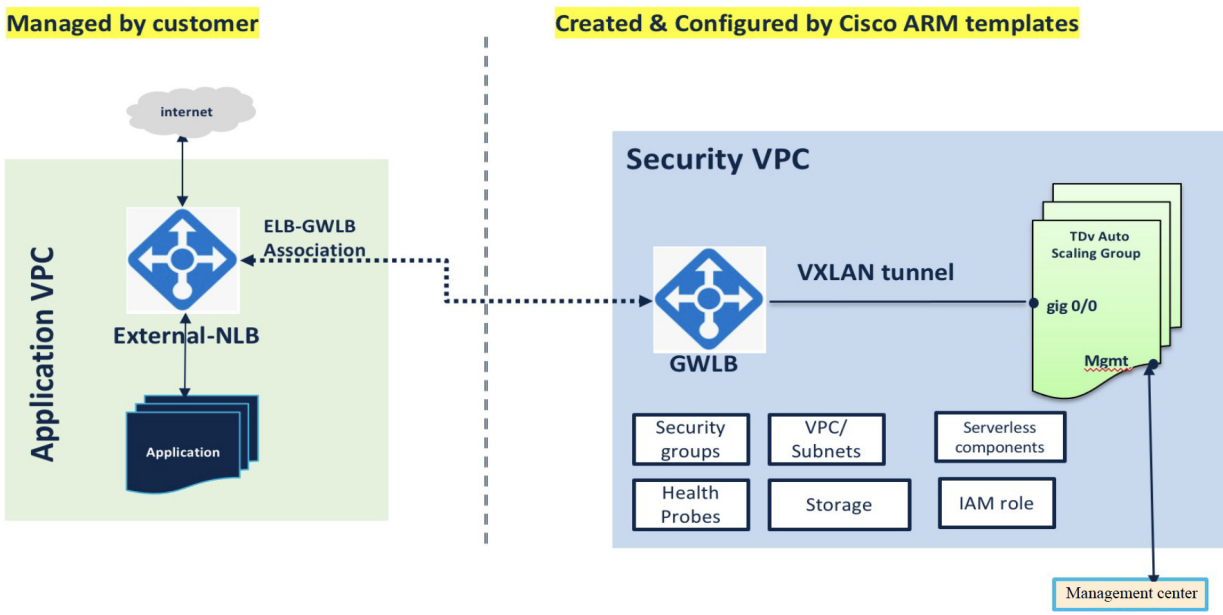
⑤ Flow is forwarded to the Internet by the public load balancer

注释 要部署和配置管理中心，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的程序。使用已部署的管理中心来管理威胁防御虚拟实例。

应用 VPC 和安全 VPC 之间的流量

在下图中，流量从现有拓扑重定向至防火墙，以便由外部负载均衡器进行检查。然后，流量将被路由到新创建的 GWLB。路由到 ELB 的任何流量都会别转发到 GWLB。

然后，GWLB 将 VXLAN 封装的流量转发到 threat defense virtual 实例。您必须创建两个 threat defense virtual 关联，因为 GWLB 会对入口和出口流量使用两个单独的 VXLAN 隧道。threat defense virtual 会解封装 VXLAN 封装的流量，对其进行检查，然后将流量路由到 GWLB。然后，GWLB 将流量转发到 ELB。



适用范围

本文档介绍部署 threat defense virtual Auto Scale for Azure 解决方案以及 Auto Scale with Azure GWLB 解决方案的无服务器组件的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

下载部署软件包

使用三明治拓扑的面向 Azure 的 threat defense virtual Auto Scale 解决方案是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

threat defense virtual Auto Scal with Azure GWLB 解决方案是一个基于 ARM 模板的部署，可以创建 GWLB、网络基础设施、威胁防御虚拟 自动扩展组、无服务器组件和其他所需资源。

两种解决方案的部署过程均类似。

下载启动面向 Azure 的 threat defense virtual Auto Scale 解决方案所需的文件。您的版本的部署脚本和模板可从 GitHub 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数，第 63 页。

Auto Scale 解决方案组件

以下组件构成了 threat defense virtual Auto Scale for Azure 解决方案。

Azure Functions（函数应用）

函数应用是一组 Azure 函数。基本功能包括：

- 定期交流/探测 Azure 指标。
- 监控 threat defense virtual 负载和触发内向扩展/外向扩展操作。
- 向 管理中心 注册新的 threat defense virtual。
- 通过 管理中心 配置新的 threat defense virtual。
- 从 管理中心 取消注册（删除）内向扩展的 threat defense virtual。

这些函数以压缩 Zip 包的形式提供（请参阅构建 Azure 函数应用包，第 31 页）。这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

Orchestrator（逻辑应用）

Auto Scale 逻辑应用是一个工作流，即按照一定序列的步骤集合。Azure 函数是独立的实体，无法彼此通信。此协调器按顺序排列这些函数的执行，并在它们之间交换信息。

- 逻辑应用可用于编排 Auto Scale Azure 函数并在函数之间传递信息。
- 每个步骤代表一个 Auto Scale Azure 函数或内置标准逻辑。
- 逻辑应用作为 JSON 文件交付。

- 可以通过 GUI 或 JSON 文件自定义逻辑应用。

虚拟机规模集 (VMSS)

VMSS 是同构虚拟机（如 threat defense virtual 设备）的集合。

- VMSS 可以向集合中添加新的相同虚拟机。
- 添加到 VMSS 的新虚拟机将自动与负载均衡器、安全组和网络接口连接。
- VMSS 具有内置 Auto Scale 功能，该功能对适用于 Azure 的 threat defense virtual 禁用。
- 您不应在 VMSS 中手动添加或删除 threat defense virtual 实例。

Azure Resource Manager (ARM) 模板

ARM 模板用于部署 threat defense virtual Auto Scale for Azure 解决方案所需的资源。

威胁防御虚拟 Auto Scale for Azure - ARM 模板**azure_ftdv_autoscale.json**为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机规模集 (VMSS)
- 内部/外部负载均衡器。
- 部署所需的安全组和其他各种组件。

威胁防御虚拟 Auto Scale with Azure GWLB - ARM 模板 **azure_ftdv_autoscale_with_GWLB.json**为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网络基础设施
- 网关负载均衡器
- 部署所需的安全组和其他各种组件

重要事项 ARM 模板在验证用户输入方面有限制，因此您需要在部署过程中负责验证输入。

前提条件

Azure 资源

资源组

部署此解决方案的所有组件需要一个现有的或新创建的资源组。

注释 记录资源组名称、创建它的区域，以及供以后使用的 Azure 订用 ID。

网络

确保虚拟网络可用或已创建。使用三明治拓扑的 Auto Scale 部署不会创建、更改或管理任何网络资源。 但请注意，使用 Azure GWLB 进行 Auto Scale 部署会创建网络基础设施。

threat defense virtual 需要四个网络接口，因此您的虚拟网络需要四个子网以用于：

1. 管理流量
2. 诊断流量
3. 内部流量
4. 外部流量

应在子网所连接的网络安全组中打开以下端口：

- SSH(TCP/22)

  负载均衡器与 threat defense virtual 之间的运行状况探测所必需。

  无服务器函数与 threat defense virtual 之间的通信所必需。

- TCP/8305

  threat defense virtual 与 管理中心 之间的通信所必需。

- HTTPS(TCP/443)

  无服务器组件与 管理中心 之间的通信所必需。

- 应用程序特定协议/端口

  任何用户应用程序所必需（例如，TCP/80 等）。

注释 记录虚拟网络名称、虚拟网络 CIDR、所有 4 个子网的名称，以及外部和内部子网的网关 IP 地址。

构建 Azure 函数应用包

threat defense virtual Auto Scale 解决方案要求您构建一个存档文件：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数 ，第 63 页。

这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

准备 管理中心

您可以使用 管理中心 来管理 threat defense virtual，这是一个功能齐全的多设备管理器。threat defense virtual 向您分配给 threat defense virtual 计算机的管理接口上的 管理中心 注册并与之通信。

创建 threat defense virtual 配置和管理所需的所有对象，包括设备组，以便您能够轻松地在多个设备上部署策略和安装更新。设备组上应用的所有配置都将被推送到 threat defense virtual 实例。

以下各节简要概述准备 管理中心 的基本步骤。有关完整信息，您应咨询完整的《Cisco Secure Firewall Management Center 配置指南》。准备 管理中心 时，请确保记录以下信息：

- 管理中心 公共 IP 地址。
- 管理中心 用户名/密码。
- 安全策略名称。
- 内部和外部安全区域对象名称。
- 设备组名称。

创建新的 管理中心 用户

在 管理中心 中创建具有 Admin 权限的新用户，以便仅供 AutoScale Manager 使用。

重要事项 为了避免与其他 管理中心 会话冲突，拥有专用于 threat defense virtual Auto Scale 解决方案的 管理中心 用户帐户非常重要。

过程

步骤 1 在 管理中心 中创建具有 Admin 权限的新用户。选择**系统** > **用户**，然后点击**创建用户**。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

步骤 2 根据环境需要完成用户选项。有关完整信息，请参阅《Cisco Secure Firewall Management Center 管理指南》。

配置访问控制

配置访问控制以允许从内部到外部的流量。在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。对规则正确进行配置和排序对于构建有效的部署至关重要。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的“访问控制最佳实践”。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**新建策略 (New Policy)**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 以便为部署配置安全设置和规则。

配置许可

所有许可证都由管理中心提供给威胁防御。您可以选择购买以下功能许可证：

- **Cisco Secure Firewall Threat Defense IPS** — 安全智能和 Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense 恶意软件防御** — 恶意软件防御
- **Cisco Secure Firewall Threat Defense URL 过滤** — URL 过滤
- **RA VPN** - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

注释 购买 IPS、恶意软件防御或 URL 过滤许可证时，您还需要匹配的订用许可证以获取 1 年、3 年或 5 年的更新。

开始之前

- 拥有思科智能软件管理器主帐户。

  如果您还没有账户，请点击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主帐户。

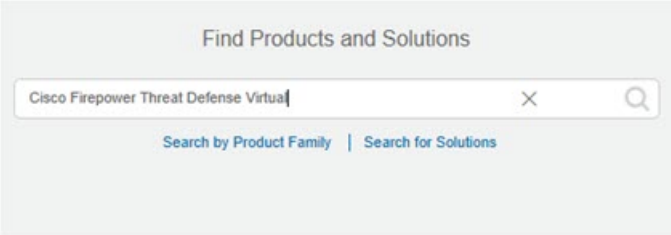
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *3:* 许可证搜索



注释
如果未找到 PID，您可以手动将 PID 添加到订单中。

步骤 2 如果尚未执行此操作，请向智能许可服务器注册管理中心。

注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 《Cisco Secure Firewall Management Center 管理指南》 。

创建安全区域对象

为您的部署创建内部和外部安全区域对象。

过程

步骤 1 选择**对象** > **对象管理**。
步骤 2 从对象类型列表中选择**接口**。
步骤 3 点击**添加** > **安全区域**。
步骤 4 输入一个**名称**（例如，*inside*、*outside*）。
步骤 5 选择**已路由**作为**接口类型**。
步骤 6 点击**保存 (Save)**。

创建设备组

可以使用设备组轻松分配策略，并在多台设备上安装更新。

过程

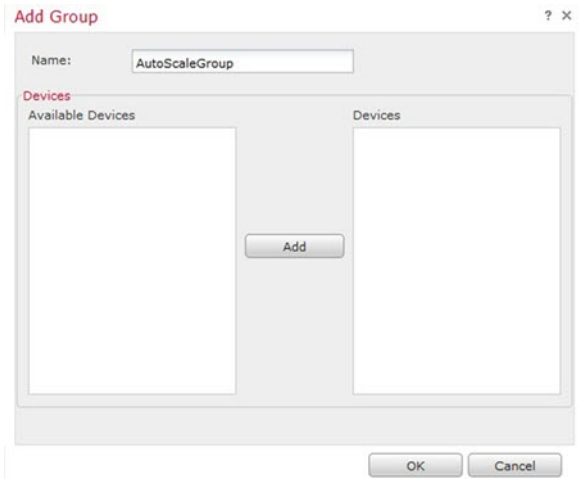
步骤 1 选择**设备** > **设备管理**。

图 *4:* 设备管理

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。

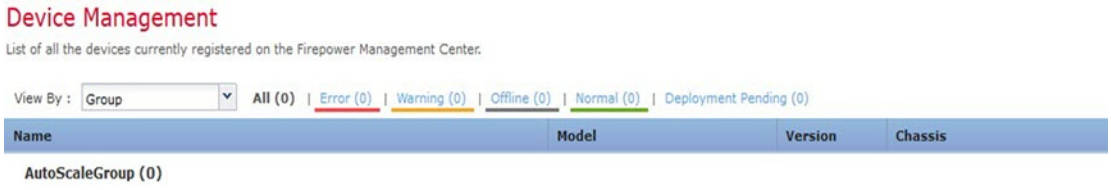
步骤 3 输入 **Name**。例如，*AutoScaleGroup*。

图 *5:* 添加设备组



步骤 4 点击**确定 (OK)** 以添加组。

图 *6:* 已添加设备组



配置安全外壳访问

威胁防御 设备的平台设置用于配置您可能希望在多台设备之间共享其值的一系列无关功能。适用于 Azure 的 Threat Defense Virtual Auto Scale 需要 威胁防御 平台设置策略，以便允许在内部/外部区域和为 Auto Scale 组创建的设备组上使用 SSH。这是必需的，以便 threat defense virtual 的数据接口可以响应负载均衡器的运行状况探测。

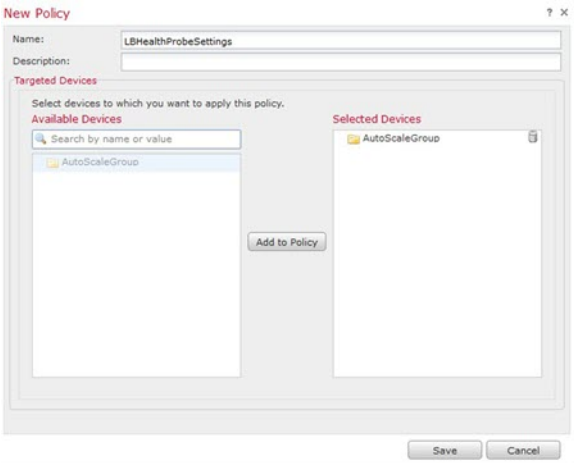
开始之前

您需要定义允许与设备建立 SSH 连接的主机或网络网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。例如，参阅以下步骤中的 *azure-utility-ip (168.63.129.16)* 对象。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略，例如 *LBHealthProbeSettings*。

图 *7:* 威胁防御 平台设置策略



步骤 2 选择**安全外壳**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

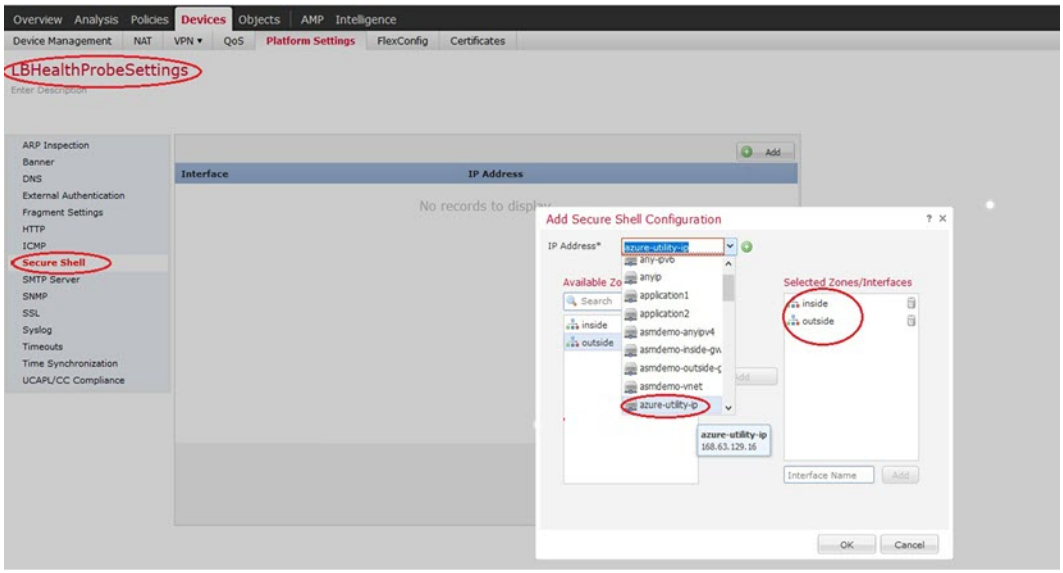
b) 配置规则属性：

- **IP 地址** - 用于标识您允许进行 SSH 连接的主机或网络的网络对象（例如，*azure-utility-ip (168.63.129.16)*）。从下拉列表中选择一个对象，或者点击“+”添加新的网络对象。
- **安全区域** - 添加包含将允许进行 SSH 连接的接口的区域。例如，您可以将内部接口分配到**内部**区域，而将外部接口分配到**外部**区域。您可以从 管理中心 的**对象 (Objects)** 页面创建安全区域。有关安全区域的完整信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

  注释
  在具有 Azure 网关负载均衡器的 Auto Scale 使用案例中不使用内部接口。

- 点击确定 **(OK)**。

图 *8: Threat Defense Virtual Auto Scale* 的 *SSH* 访问



步骤 4 点击保存 **(Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

注释
您还可以为运行状况探测配置 TCP 端口 443，而不是使用 **SSH 访问**。要执行此操作，请转至**设备 (Devices)** > **平台设置 (Platform settings)** > **HTTP 访问 (HTTP Access)**，选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框，然后在**端口 (Port)** 字段中输入 **443**。将此设置与内部和外部接口相关联。您还必须将 ARM 模板中的运行状况探测端口更改为 443。有关配置 HTTP 访问的详细信息，请参阅配置 HTTP。

配置 NAT

创建 NAT 策略并创建必要的 NAT 规则，以便将流量从外部接口转发到应用程序，然后将此策略连接到您为自动扩展创建的设备组。

注释 仅当使用夹层拓扑配置自动扩展时，才需要配置 NAT。

过程

步骤 1 选择**设备** > **NAT**。

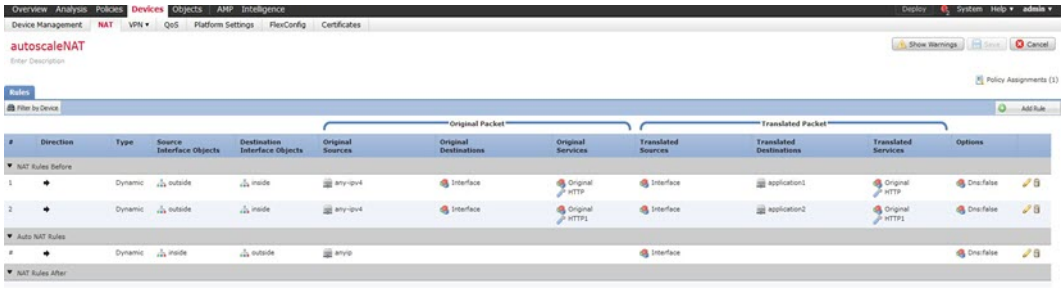
步骤 2 从**新策略**下拉列表中，选择**威胁防御 NAT**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 配置您的 NAT 规则。有关如何创建 NAT 规则和应用 NAT 策略的准则，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的“为威胁防御配置 NAT”。下图所示为基本方法。

图 *9: NAT* 策略示例



注释

我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。

步骤 6 点击**保存 (Save)**。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，您可以在将 ARM 模板部署到 Azure 订用时使用这些参数创建 threat defense virtual 设备。请参阅部署 Auto Scale ARM 模板，第 44 页。在 Auto Scale with Azure GWLB 解决方案中，还会创建网络基础设施，因此必须在模板中配置其他输入参数。参数说明的含义不言自明。

表 *2:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串*（3-10 个字符）	所有资源都使用包含此前缀的名称创建。 注：只能使用小写字母。 示例：ftdv	New
virtualNetworkRg	字符串	虚拟网络资源组名称。 示例：cisco-virtualnet-rg	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）。 示例：cisco-virtualnet	现有

参数名	允许的值/类型	说明	资源创建类型
virtualNetworkCidr	CIDR 格式 x.x.x.x/y	虚拟网络的 CIDR（已创建）	现有
mgmtSubnet	字符串	管理子网名称（已创建） 示例：cisco-mgmt-subnet	现有
diagSubnet	字符串	诊断子网名称（已创建）。 示例：cisco-diag-subnet	现有
insideSubnet	字符串	内部子网名称（已创建）。 示例：cisco-inside-subnet	现有
internalLbIp	字符串	内部子网的内部负载均衡器 IP 地址（已创建）。 例如：1.2.3.4	现有
insideNetworkGatewayIp	字符串	内部子网网关 IP 地址（已创建）。	现有
outsideSubnet	字符串	外部子网名称（已创建）。 示例：cisco-outside-subnet	现有
outsideNetworkGatewayIp	字符串	外部子网网关 IP（已创建）。	现有
deviceGroupName	字符串	管理中心中的设备组（已创建）	现有
insideZoneName	字符串	管理中心中的内部区域名称（已创建）	现有
outsideZoneName	字符串	管理中心中的外部区域名称（已创建）	现有
softwareVersion	字符串	threat defense virtual 版本（在部署期间从下拉列表中选择）。	现有
vmSize	字符串	threat defense virtual 实例的大小（在部署过程中从下拉列表中选择）。	不适用
ftdLicensingSku	字符串	Threat Defense Virtual 许可模式 (PAYG/BYOL) 注：PAYG 在版本 6.5+ 中受支持。	不适用

参数名	允许的值/类型	说明	资源创建类型
licenseCapability	逗号分隔的字符串	BASE, MALWARE, URLFilter, THREAT	不适用
ftdVmManagementUserName	字符串*	threat defense virtual VM 管理管理员用户名。 这**不能**是“admin”。请参阅 Azure 以了解 VM 管理员用户名准则。	New
ftdVmManagementUserPassword	字符串*	threat defense virtual VM 管理管理员用户的密码。 密码的长度必须为 12 至 72 个字符，而且必须具有：小写、大写、数字及特殊字符；重复字符不得超过 2 个。 **注释** 模板中不对此进行合规性检查。	New
fmcIpAddress	字符串 x.x.x.x	管理中心 的公共 IP 地址（已创建）	现有
fmcUserName	字符串	管理中心用户名，具有管理权限（已创建）	现有
fmcPassword	字符串	上述 管理中心 用户名的 管理中心 密码（已创建）	现有
policyName	字符串	在 管理中心 中创建的安全策略（已创建）	现有

参数名	允许的值/类型	说明	资源创建类型
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 threat defense virtual 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 **POLICY-2**：当自动扩展组中所有 threat defense virtual 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 在两种情况下，内向扩展逻辑都保持不变：当所有 threat defense virtual 设备的平均负载在所配置的持续时间内低于内向扩展阈值时，将触发内向扩展。	不适用
scalingMetricsList	字符串	用于制定扩展决策的指标。 允许：CPU CPU、内存 默认值：CPU	不适用
cpuScaleInThreshold	字符串	CPU 指标的内向扩展阈值（以百分比为单位）。 默认值：10 当 threat defense virtual 指标低于此值时，将触发扩展。 请参阅Auto Scale 逻辑，第 60 页。	不适用
cpuScaleOutThreshold	字符串	CPU 指标的横向扩展阈值（以百分比为单位）。 默认值：80 当 threat defense virtual指标高于此值时，将触发横向扩展。 “cpuScaleOutThreshold”应始终大于“cpuScaleInThreshold”。 请参阅Auto Scale 逻辑，第 60 页。	不适用

参数名	允许的值/类型	说明	资源创建类型
memoryScaleInThreshold	字符串	内存指标的内向扩展阈值（以百分比为单位）。 默认值：0 当 threat defense virtual 指标低于此值时，将触发扩展。 请参阅Auto Scale 逻辑，第 60 页。	不适用
memoryScaleOutThreshold	字符串	内存指标的横向扩展阈值（以百分比为单位）。 默认值：0 当 threat defense virtual指标高于此值时，将触发横向扩展。 “memoryScaleOutThreshold”应始终**大于**“memoryScaleInThreshold”。 请参阅Auto Scale 逻辑，第 60 页。	不适用
minFtdCount	整数	在任何给定时间，规模集中可用的最小 threat defense virtual 实例数。 示例：2	不适用
maxFtdCount	整数	规模集中允许的最大 threat defense virtual 实例数。 示例：10 **注释** 此数量受 管理中心 容量的限制。 Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用

参数名	允许的值/类型	说明	资源创建类型
metricsAverageDuration	整数	从下拉列表中选择。 此数字表示计算指标平均值的时间（以分钟为单位）。 如果此变量的值为 5（即 5 分钟），则当计划 Auto Scale Manager 时，它将检查过去 5 分钟内的指标平均值，并且基于此平均值做出扩展决定。 **注释** 由于 Azure 限制，仅 1、5、15 和 30 是有效数字。	不适用

参数名	允许的值/类型	说明	资源创建类型
initDeploymentMode	BULK/STEP	主要适用于第一次部署，或者规模集不包含任何 threat defense virtual 实例时。 BULK：Auto Scale 管理器将尝试一次并行部署“minFtdCount”数量的 threat defense virtual 实例。 **注释** 启动采用并行方式，但由于 管理中心 的限制，需要按顺序注册到 管理中心。 STEP：Auto Scale 管理器将按照计划间隔逐个部署“minFtdCount”数量的 threat defense virtual 设备。 **注释** STEP 选项需要较长时间来启动“minFtdCount”数量的实例并使用 管理中心 进行配置，然后实现运行，但在调试时很有帮助。 BULK 选项启动所有“minFtdCount”数量的 threat defense virtual 所花费的时间与一次 threat defense virtual 启动相同（因为它是并行运行的），但 管理中心 注册是按顺序进行的。 部署“minFtdCount”数量的 threat defense virtual 所花费的总时间 =（启动一个 threat defense virtual 所用的时间 + 注册/配置一个 threat defense virtual 所用的时间 * minFtdCount）。	
*Azure 对新资源的命名约定有限制。查看限制，或者直接全部使用小写字母。**不要使用空格或任何其他特殊字符**。			

部署 Auto Scale 解决方案

下载部署软件包

使用三明治拓扑的面向 Azure 的 threat defense virtual Auto Scale 解决方案是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

threat defense virtual Auto Scal with Azure GWLB 解决方案是一个基于 ARM 模板的部署，可以创建 GWLB、网络基础设施、威胁防御虚拟 自动扩展组、无服务器组件和其他所需资源。

两种解决方案的部署过程均类似。

下载启动面向 Azure 的 threat defense virtual Auto Scale 解决方案所需的文件。您的版本的部署脚本和模板可从 GitHub 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数 ，第 63 页。

部署 Auto Scale ARM 模板

使用三明治拓扑的威胁防御虚拟 Auto Scale for Azure - 使用 ARM 模板**azure_ftdv_autoscale.json**来部署 threat defense virtual Auto Scale for Azure 所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机规模集 (VMSS)
- 外部负载均衡器
- 内部负载均衡器
- Azure 函数应用
- 逻辑应用
- 安全组（用于数据接口和管理接口）

威胁防御虚拟 Auto Scale with Azure GWLB - 使用 ARM 模板 **azure_ftdv_autoscale_with_GWLB.json** 来部署 threat defense virtual Auto Scale with Azure GWLB 解决方案所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网关负载均衡器
- Azure 函数应用
- 逻辑应用

- 网络基础设施
- 部署所需的安全组和其他各种组件

开始之前

- 从 GitHub 存储库下载 ARM 模板 (https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure)。

过程

步骤 1 如果您需要在多个 Azure 区域中部署 threat defense virtual 实例，请基于部署区域中可用的区域编辑 ARM 模板。

示例：

```
"zones": [
    "1",
    "2",
    "3"
],
```

本示例显示了包含 3 个区域的“美国中部”区域。

步骤 2 编辑外部负载均衡器中所需的流量规则。您可以通过扩展此“json”数组来添加任意数量的规则。这适用于使用三明治拓扑的 Auto Scale 使用案例。

示例：

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
   "name": "Standard"
 },
 "dependsOn": [
   "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

 ],
 "properties": {
   "frontendIPConfigurations": [
     {
       "name": "LoadBalancerFrontEnd",
         "properties": {
           "publicIPAddress": {
             "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
           }
         }
     }
   ],
   "backendAddressPools": [
     {
       "name": "backendPool"
```

```
            }
          ],
          "loadBalancingRules": [
            {
              "properties": {
                "frontendIPConfiguration": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/frontendIpConfigurations/LoadBalancerFrontend')]"
                },
                "backendAddressPool": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/backendAddressPools/BackendPool')]"
                },
                "probe": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

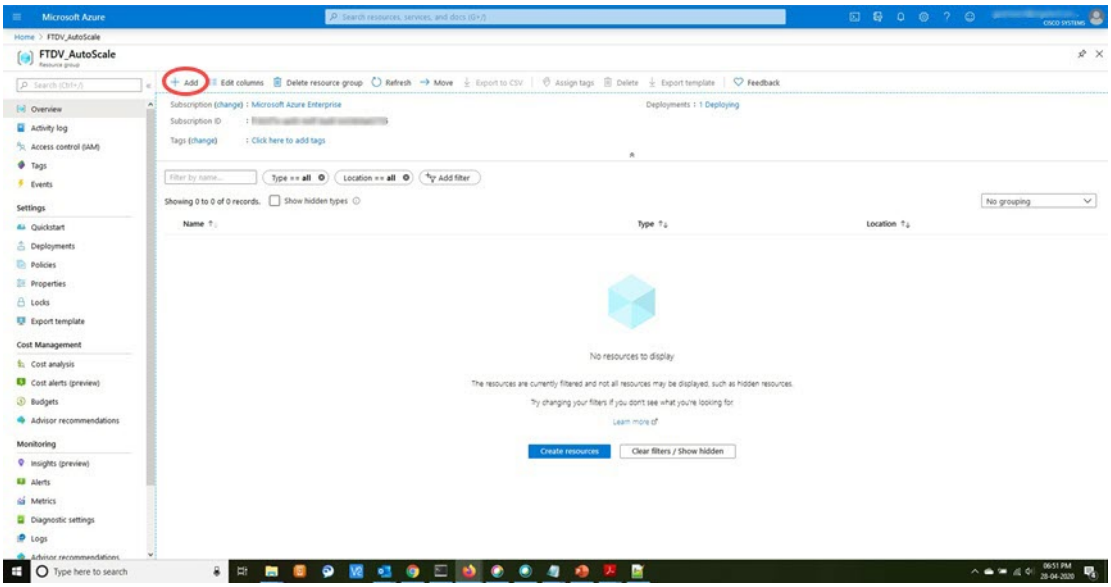
注释
如果您不想编辑此文件，也可以在部署后从 Azure 门户编辑此项。

步骤 3 使用您的 Microsoft 帐户用户名和密码登录 Microsoft Azure 门户。

步骤 4 点击服务菜单中的**资源组 (Resource groups)** 以访问资源组边栏选项卡。您将看到该边栏选项卡中列出您的订用中的所有资源组。

创建新资源组或选择现有的空资源组；例如，*threat defense virtual_AutoScale*。

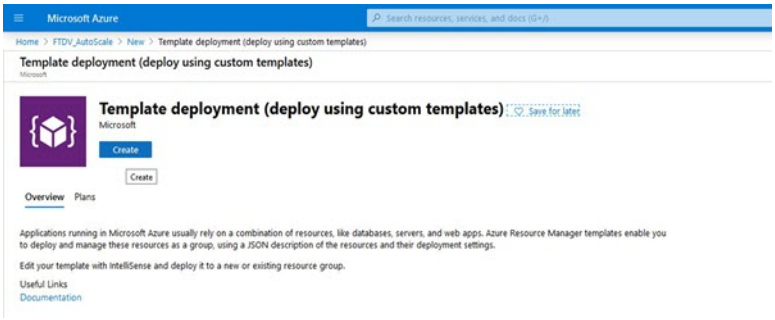
图 ***10: Azure*** 门户



步骤 5 点击**创建资源 (+) (Create a resource [+])**，为模板部署创建新资源。此时将显示“创建资源组”(Create Resource Group) 边栏选项卡。

步骤 6 在**搜索市场 (Search the Marketplace)** 中，键入**模板部署（使用自定义模板部署）**，然后按 **Enter**。

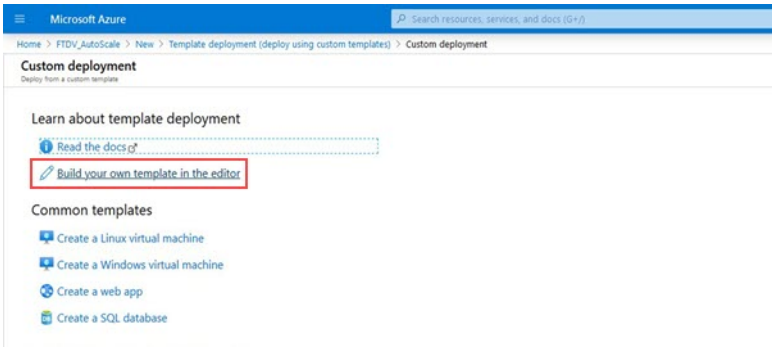
图 *11:* 自定义模板部署



步骤 7 点击**创建 (Create)**。

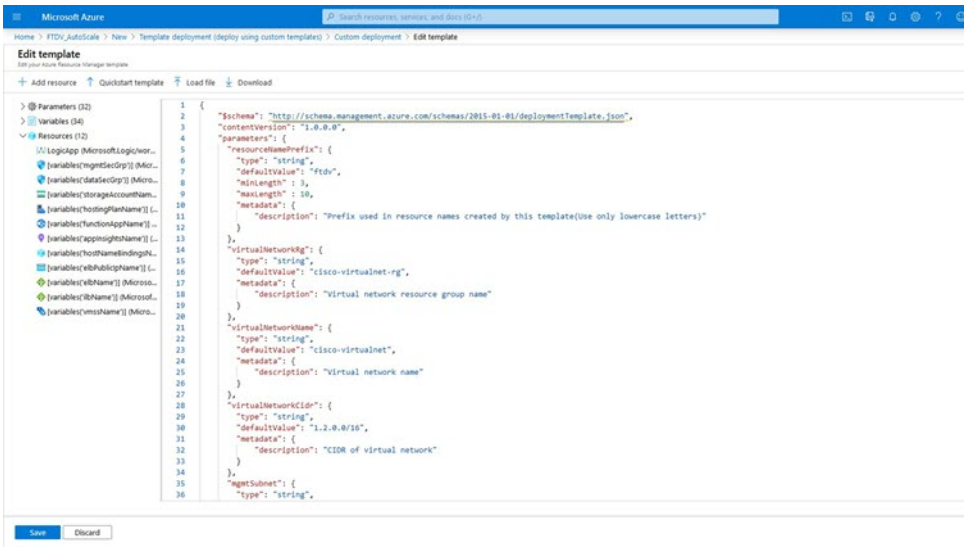
步骤 8 创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板 (Build your own template in editor)**。

图 *12:* 构建您自己的模板



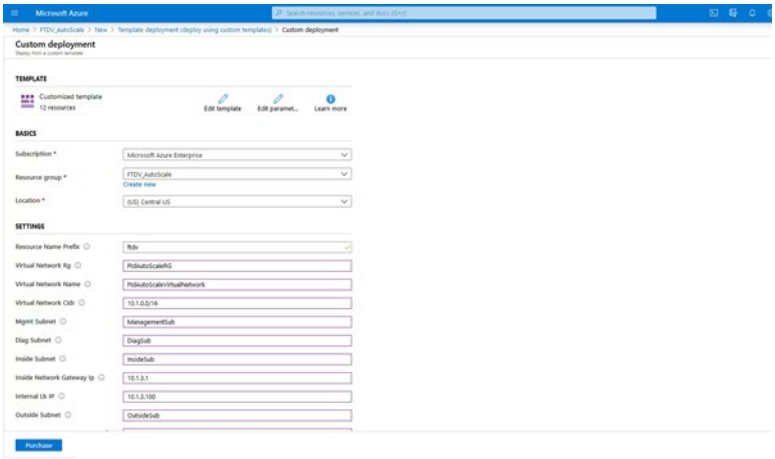
步骤 9 在**编辑模板 (Edit template)** 窗口中，删除所有默认内容并从更新的 *azure_ftdv_autoscale.json* 复制内容，然后点击**保存 (Save)**。

图 *13:* 编辑模板



步骤 10 在下一部分，填写所有参数。有关每个参数的详细信息，请参阅输入参数，第 37 页，然后点击**购买 (Purchase)**。

图 *14: ARM* 模板参数



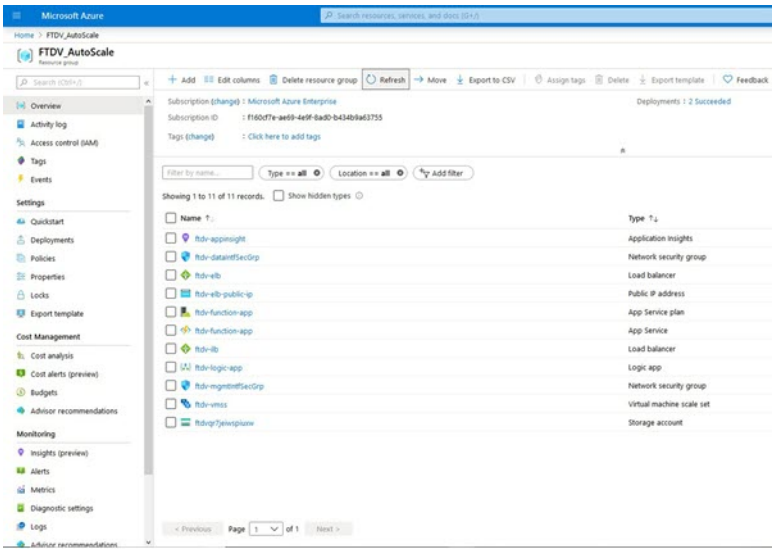
注释

您也可以点击**编辑参数 (Edit Parameters)**，然后编辑 JSON 文件或上传预填的内容。

ARM 模板的输入验证功能有限，因此您需要负责验证输入。

步骤 11 当成功部署模板后，它将为 threat defense virtual Auto Scale for Azure 解决方案创建所有必要的资源。请参阅下图中的资源。“类型”(Type) 列描述了每个资源，包括逻辑应用、VMSS、负载均衡器、公共 IP 地址等。

图 *15:* 威胁防御虚拟 ***Auto Scale*** 模板部署



部署 Azure 函数应用

部署 ARM 模板时，Azure 会创建一个主干函数应用，然后您需要为其更新和手动配置 Auto Scale Manager 逻辑所需的函数。

开始之前

- 构建 *ASM_Function.zip* 包。请参阅通过源代码构建 Azure 函数，第 63 页。

过程

步骤 1 转至您在部署 ARM 模板时创建的函数应用，然后确认不存在任何函数。在浏览器中，转至以下 URL：

https://<函数应用名称>.scm.azurewebsites.net/DebugConsole

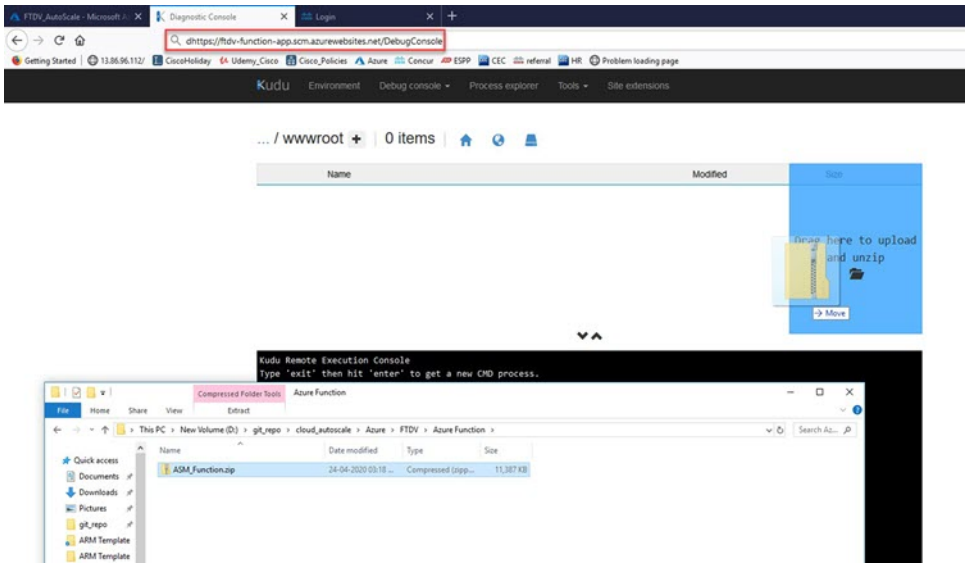
对于部署 Auto Scale ARM 模板，第 44 页中的示例：

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

步骤 2 在文件资源管理器中，导航到 **site/wwwroot**。

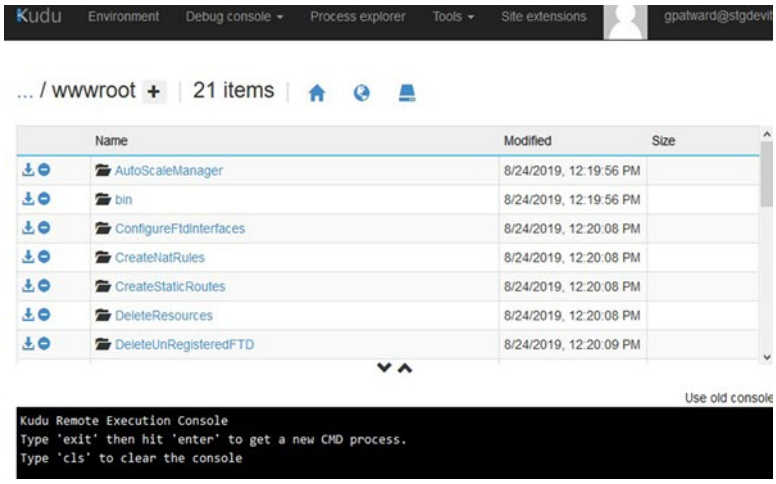
步骤 3 将 **ASM_Function.zip** 拖放到文件资源管理器的右侧。

图 *16:* 上传 威胁防御虚拟 ***Auto Scale*** 功能



步骤 4 成功上传后，应该会显示所有无服务器函数。

图 *17:* 威胁防御虚拟 无服务器函数

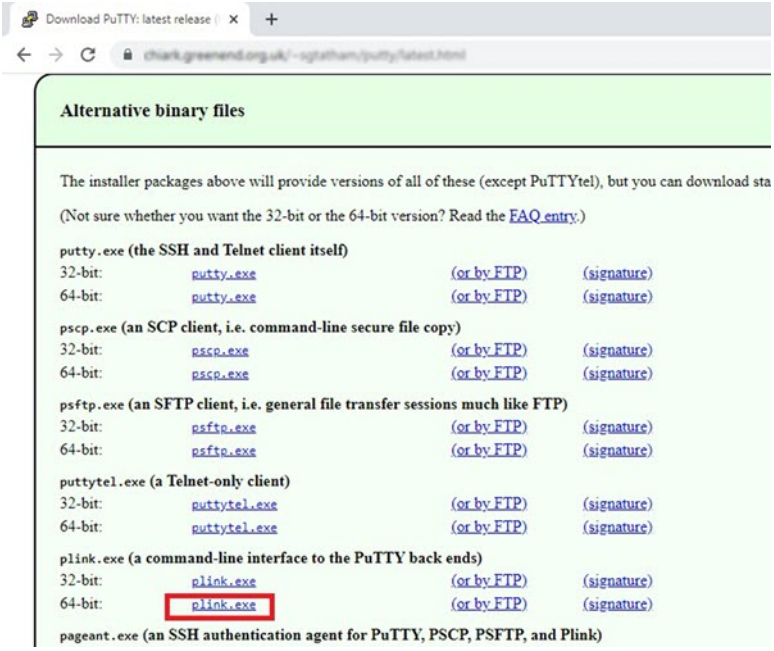


步骤 5 下载 PuTTY SSH 客户端。

Azure 函数需要通过 SSH 连接访问 threat defense virtual。但是，无服务器代码中使用的开放源码库不支持 threat defense virtual 所用的 SSH 密钥交换算法。因此，您需要下载预构建 SSH 客户端。

从 www.putty.org 将 PuTTY 命令行界面下载到 PuTTY 后端 (*plink.exe*)。

图 *18:* 下载 ***PuTTY***



步骤 6 将 SSH 客户端可执行文件 **plink.exe** 重命名为 **ftdssh.exe**。

步骤 7 将 **ftdssh.exe** 拖放到文件资源管理器的右侧，放到上一步中上传 **ASM_Function.zip** 的位置。

步骤 8 验证 SSH 客户端与函数应用程序一起存在。必要时刷新页面。

微调配置

有一些配置可用于微调 Auto Scale Manager 或在调试中使用。这些选项不会在 ARM 模板中显示，但可以在函数应用下编辑它们。

开始之前

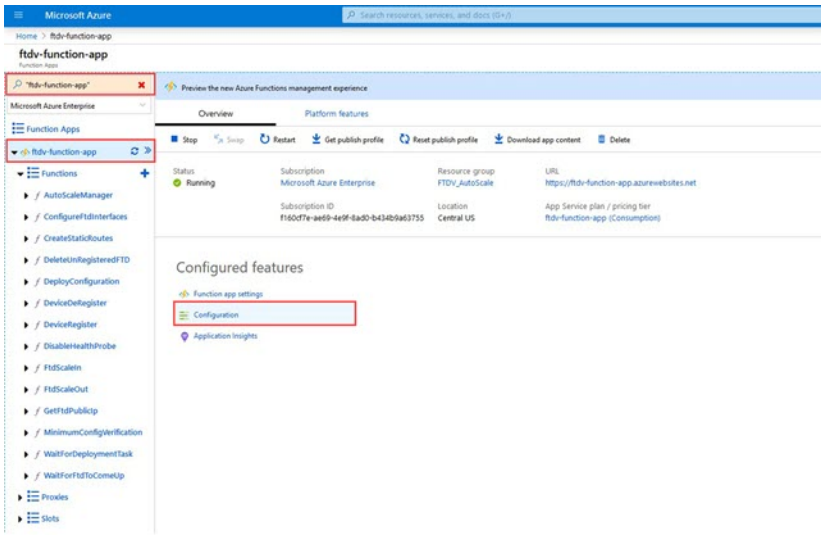
注释 可以随时编辑此项。按照以下顺序编辑配置。

- 禁用函数应用。
- 等待现有的计划任务完成。
- 编辑并保存配置。
- 启用函数应用。

过程

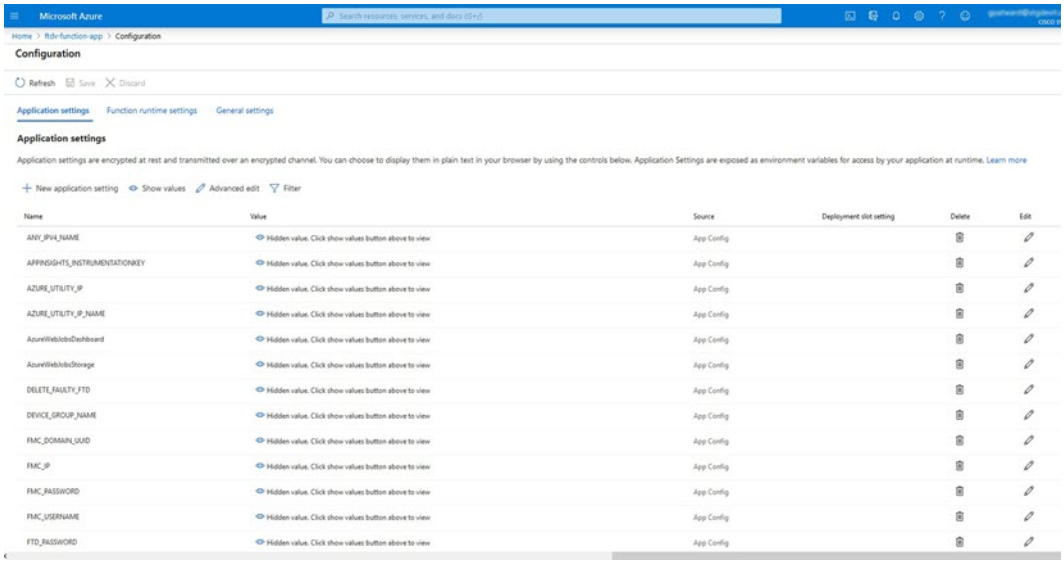
步骤 1 在 Azure 门户中，搜索并选择 threat defense virtual 函数应用。

图 *19:* 威胁防御虚拟 函数应用



步骤 2 也可以在此处编辑通过 ARM 模板传递的配置。变量名称可能与 ARM 模板不同，但您可以轻松地从其名称中确定它们的用途。

图 *20:* 应用设置



大多数选项的名称不言自明。例如：

- 配置名称：“DELETE_FAULTY_FTD”（默认值：YES）

在外向扩展期间，将会启动新的 threat defense virtual 实例并将其注册到 管理中心。如果注册失败，则 Auto Scale Manager 将根据此选项决定保留该 threat defense virtual 实例或将其删除。（YES：删除错误的 threat defense virtual/NO：保留 threat defense virtual 实例，即使未能注册到 管理中心）。

- 在函数应用设置中，有权访问 Azure 订用的用户都可以看到明文格式的所有变量（包括含安全字符串的变量，如“密码”）。

  如果用户对此有安全担忧（例如，如果在组织内的低权限用户之间共享 Azure 订用），可以使用 Azure 的 *Key Vault* 服务来保护密码。配置此项后，用户必须提供由存储密码的密钥保管库生成的安全标识符，而不是函数设置中的明文密码。

  注释
  搜索 Azure 文档，查找保护应用程序数据的最佳实践。

在虚拟机规模集中配置 IAM 角色

Azure 身份及访问管理 (IAM) 作为 Azure 安全和访问控制的一部分，用于管理和控制用户的身份。Azure 资源的托管身份为 Azure 服务提供 Azure Active Directory 中自动托管的身份。

这将允许函数应用控制虚拟机规模集 (VMSS)，无需显式身份验证凭证。

过程

步骤 1 在 Azure 门户中，转至 VMSS。

步骤 2 点击**访问控制 (IAM) (Access control [IAM])**。

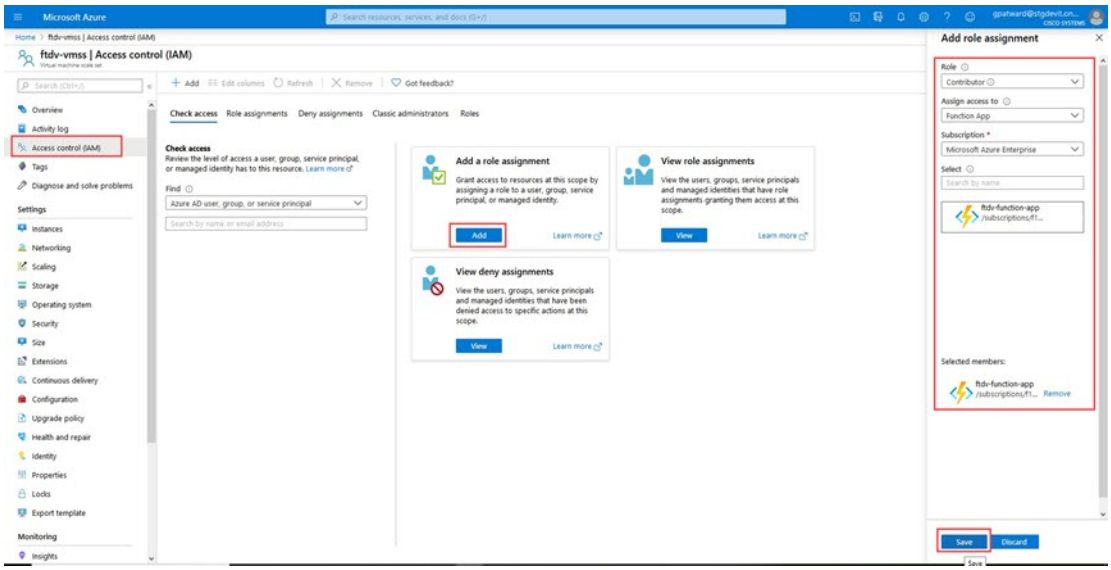
步骤 3 点击**添加 (Add)** 以添加角色分配

步骤 4 从**添加角色分配 (Add role assignment)**下拉列表中选择**参与者 (Contributor)**。

步骤 5 从**分配访问 (Assign access to)** 下拉列表中选择**函数应用 (Function App)**。

步骤 6 选择 threat defense virtual 函数应用。

图 *21: AIM* 角色分配



步骤 7 点击保存 **(Save)**。

注释
此外，还应确认尚未启动任何 threat defense virtual 实例。

更新安全组

ARM 模板创建两个安全组，一个用于管理接口，一个用于数据接口。管理安全组将只允许 threat defense virtual 管理活动所需的流量。不过，数据接口安全组将允许所有流量。

过程

根据您的部署的拓扑和应用程序需求，微调安全组规则。

注释
数据接口安全组至少应允许来自负载均衡器的 SSH 流量。

更新 Azure 逻辑应用

逻辑应用充当 Autoscale 功能的协调器。ARM 模板会创建一个主干逻辑应用，然后您需要手动更新，提供使之作为 Auto Scale 协调器发挥作用所需的信息。

过程

步骤 1 从存储库中将文件 *LogicApp.txt* 恢复到本地系统，然后如下所示进行编辑。

重要事项
在继续之前，阅读并理解所有这些步骤。

这些手动步骤不会在 ARM 模板中自动执行，以便稍后只能独立升级逻辑应用。

a) 必需： 查找所有“SUBSCRIPTION_ID”并替换为您的订用 ID 信息。
b) 必需： 查找所有“RG_NAME”并替换为您的资源组名称。
c) 必需： 查找所有“FUNCTIONAPPNAME”并替换为您的函数应用名称。

以下示例显示了 *LogicApp.txt* 文件中的几行：

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) （可选）编辑触发间隔，或保留默认值 (5)。这是定期触发 Autoscale 的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
```

```
            "frequency": "Minute",
            "interval": 5
        },
```

e) （可选）编辑要进行排空的时间，或保留默认值(5)。这是内向扩展操作期间，在删除设备之前从threat defense virtual 中排空现有连接的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

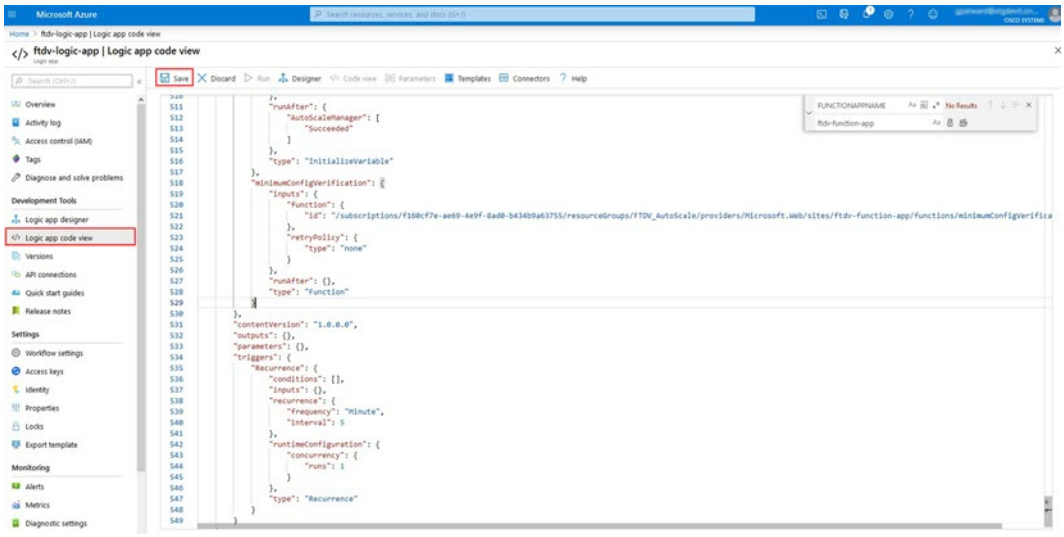
f) （可选）编辑冷却时间，或保留默认值(10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
    "actions": {
        "Branch_based_on_Scale-Out_or_Invalid_condition": {
            "actions": {
                "Cooldown_time": {
                    "inputs": {
                        "interval": {
                            "count": 10,
                            "unit": "Second"
                        }
```

注释
这些步骤也可以从 Azure 门户完成。有关详细信息，请参阅 Azure 文档。

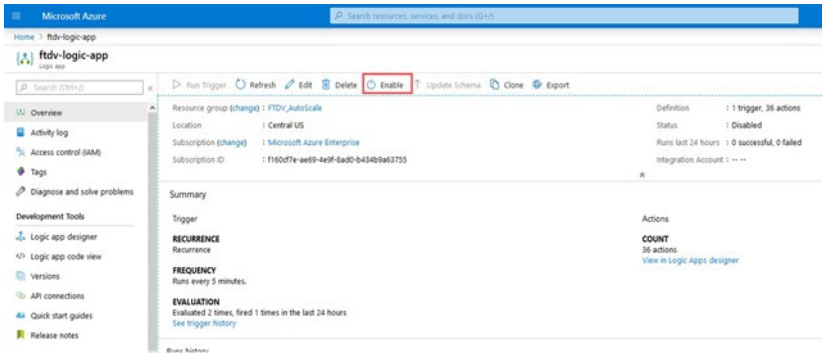
步骤 2 转至**逻辑应用代码视图 (Logic App code view)**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后点击**保存 (Save)**。

图 *22:* 逻辑应用代码视图



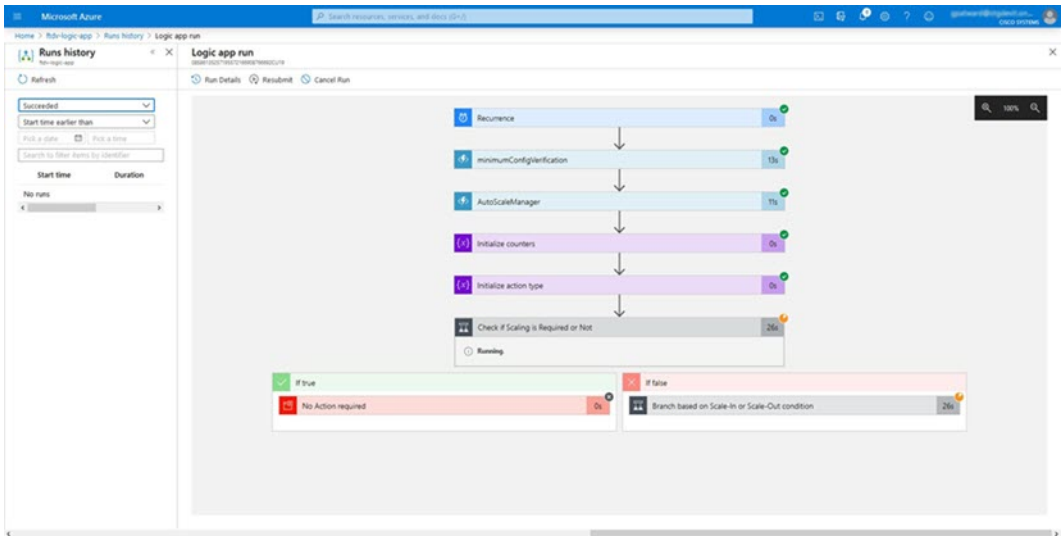
步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请点击**启用 (Enable)**。

图 *23:* 启用逻辑应用



步骤 4 启用后，任务就会开始运行。点击“正在运行”(Running) 状态可查看活动。

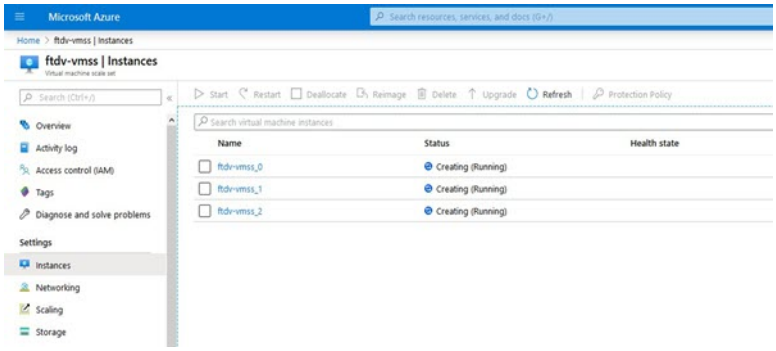
图 *24:* 逻辑应用运行状态



步骤 5 逻辑应用启动后，所有与部署相关的步骤都将完成。

步骤 6 在 VMSS 中验证是否正在创建 threat defense virtual 实例。

图 *25:* 威胁防御虚拟 实例运行



在此示例中，由于在 ARM 模板部署中将 'minFtdCount' 设置为“3”并将“initDeploymentMode”设置为“批量”，因此启动了三个 threat defense virtual 实例。

升级 threat defense virtual

threat defense virtual升级仅支持采用虚拟机规模集 (VMSS) 映像升级的形式。因此，您需要通过 Azure REST API 接口升级 threat defense virtual。

注释 您可以使用任何 REST 客户端来升级 threat defense virtual。

开始之前

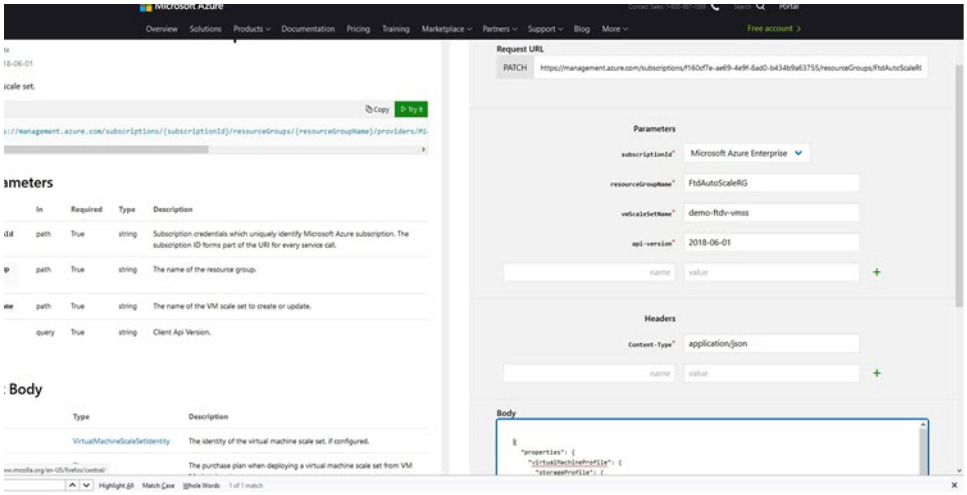
- 获取市场中提供的新 threat defense virtual 映像版本（例如：650.32.0）。
- 获取用于部署原始规模集的 SKU（例如：ftdv-azure-byol）。
- 获取资源组和虚拟机规模集名称。

过程

步骤 1 在浏览器中，转至以下 URL：
https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

步骤 2 在参数部分输入详细信息。

图 *26:* 升级 *threat defense virtual*



步骤 3 在**主体 (Body)** 部分输入包含新 threat defense virtual 映像版本、SKU 和触发器运行的 JSON 输入。

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                      "imageReference": {
                           "publisher": "cisco",
                           "offer": "cisco-ftdv",
                           "sku": "ftdv-azure-byol",
                            "version": "650.32.0"
                      }
                 },
            }
      }
}
```

步骤 4 Azure 成功响应意味着 VMSS 已接受更改。

新映像将在新的 threat defense virtual 实例中使用，而这些新实例将在外向扩展操作过程中启动。

- 虽然位于同一规模集中，但现有的 threat defense virtual 实例将继续使用旧软件映像。
- 您可以覆盖上述行为，手动升级现有的 threat defense virtual 实例。要执行此操作，请点击 VMSS 中的**升级 (Upgrade)** 按钮。它将重新启动并升级选定的 threat defense virtual 实例。您必须手动重新注册并重新配置这些升级后的 threat defense virtual 实例。**请注意，不建议使用此方法**。

Auto Scale 逻辑

扩展指标

您可以使用 ARM 模板部署 threat defense virtualAuto Scale 解决方案所需的资源。在 ARM 模板部署期间，您有以下选项可用于扩展指标：

- CPU
- CPU、内存（版本 6.7+）。

注释 CPU 指标从 Azure 收集；内存指标从 管理中心 收集。

外向扩展逻辑

- **POLICY-1**：当**任何** threat defense virtual 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。使用“CPU、内存”扩展指标时，外向扩展阈值即规模集中**任何** threat defense virtual 的平均 CPU **或**内存利用率。
- **POLICY-2**：当**所有** threat defense virtual 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。使用“CPU、内存”扩展指标时，外向扩展阈值即规模集中**所有** threat defense virtual 设备的平均 CPU **或**内存利用率。

内向扩展逻辑

- 如果**所有** threat defense virtual 设备的 CPU 利用率在所配置的持续时间内低于配置的内向扩展阈值。使用“CPU、内存”扩展指标时，如果规模集中所有 threat defense virtual 设备的 CPU **和**内存利用率在所配置的持续时间内低于配置内向扩展阈值，则将选择终止 CPU 负载最小的 threat defense virtual。

说明

- 内向扩展/外向扩展以 1 为单位发生（即一次仅内向扩展/外向扩展 1 个 threat defense virtual）。

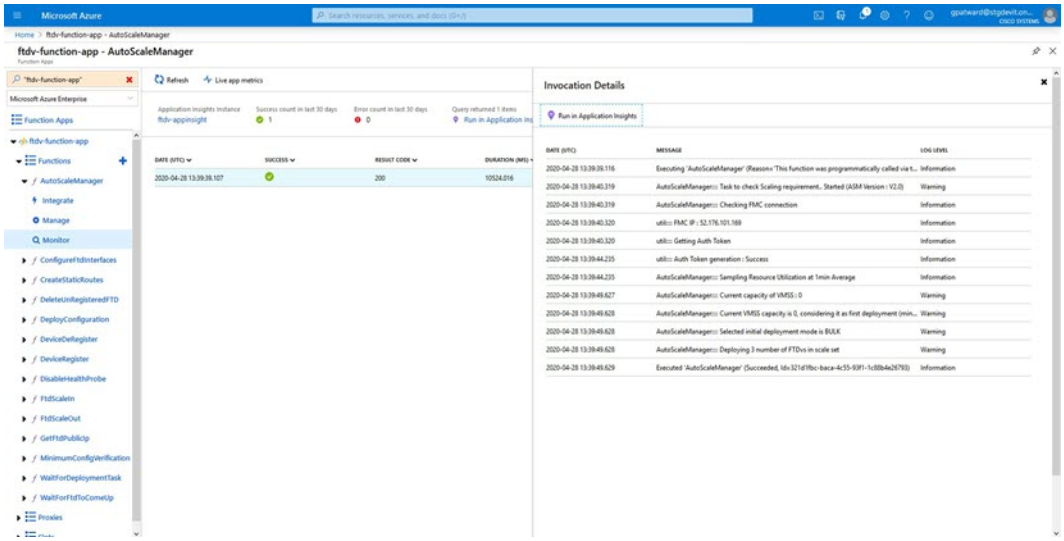
- 从 管理中心 收到的内存消耗指标不是按时间计算的平均值，而是瞬时快照/示例值。因此，在做出扩展决定时不能单独考虑内存指标。在部署过程中，您无法选择使用仅内存指标。

Auto Scale 日志记录和调试

无服务器代码的每个组件都有自己的日志记录机制。此外，还会将日志发布到应用程序洞察。

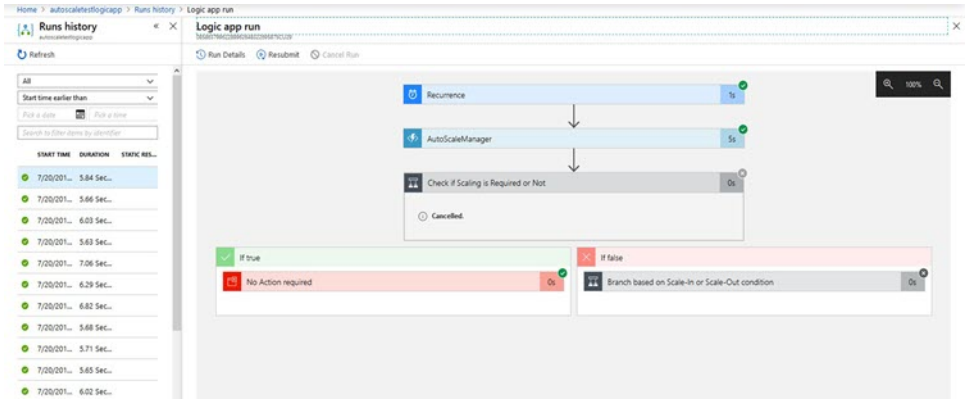
- 可以查看个别 Azure 函数的日志。

图 *27: Azure* 函数日志



- 可以查看每个逻辑应用及其各个组件每次运行的类似日志。

图 *28:* 逻辑应用运行日志



- 如果需要，可以随时停止/终止逻辑应用中任何正在运行的任务。但是，被启动/终止的当前运行 threat defense virtual 设备将处于不一致状态。
- 在逻辑应用中可以看到每个运行/个别任务所花费的时间。

- 通过上传新的zip，可以随时升级函数应用。在升级函数应用之前，先停止逻辑应用并等待所有任务完成。

Auto Scale 准则和限制

部署 threat defense virtual Auto Scale for Azure 时，请注意以下准则和限制：

- （版本 6.6 及更低版本）扩展决定基于 CPU 使用率。
- （版本 6.7+）扩展决定可以使用仅 CPU 利用率，或者同时使用 CPU 及内存利用率。
- 需要 管理中心 管理。不支持 设备管理器。
- 管理中心 应具有公共 IP 地址。
- threat defense virtual 管理接口配置为具有公共 IP 地址。
- 仅支持 IPv4。
- Threat Defense Virtual Auto Scale for Azure 仅支持访问策略、NAT 策略、平台设置等配置，它们将应用到设备组并传播到外向扩展 threat defense virtual实例。您只能使用 管理中心 来修改设备组配置。不支持设备特定的配置。
- ARM 模板的输入验证功能有限，因此您需要负责提供正确的输入验证。
- Azure管理员可以在函数应用环境中看到明文形式的敏感数据（如管理登录凭证和密码）。您可以使用 *Azure Key Vault* 服务保护敏感数据。
- 配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。
- 如果您在现有实例上手动更新配置时遇到问题，我们建议从扩展组中删除这些实例并将其替换为新实例。

故障排除

以下是 threat defense virtual Auto Scale for Azure 的常见错误情况和调试提示：

- 连接到 管理中心 失败：检查 管理中心 IP/凭证；检查 管理中心 是否故障/无法访问。
- 无法通过 SSH 连接到 threat defense virtual：检查是否通过模板将复杂密码传递到 threat defense virtual；检查安全组是否允许 SSH 连接。
- 负载均衡器运行状况检查失败：检查 threat defense virtual 是否在数据接口上响应 SSH；检查安全组设置。
- 流量问题：检查负载均衡器规则、threat defense virtual 中配置的 NAT 规则/静态路由；检查模板和安全组规则中提供的 Azure 虚拟网络/子网/网关详细信息。
- threat defense virtual 无法注册到 管理中心：检查 管理中心 容量以容纳新的 threat defense virtual 设备；检查许可；检查 threat defense virtual 版本兼容性。

- 逻辑应用无法访问 VMSS：检查 VMSS 中的 IAM 角色配置是否正确。
- 逻辑应用运行很长时间：在外向扩展 threat defense virtual 设备上检查 SSH 访问；检查 管理中心中是否有任何设备注册问题；检查 Azure VMSS 中 threat defense virtual 设备的状态。
- 与订用 ID 相关的 Azure 函数抛出错误：验证您的帐户中是否选择了默认预订。
- 内向扩展操作失败：有时 Azure 会花费很长时间删除实例，在这种情况下，内向扩展操作可能会超时并报告错误，但最终实例将被删除。
- 在做出任何配置更改之前，请确保禁用逻辑应用程序，并等待所有正在运行的任务完成。

如果在 threat defense virtual Auto Scale 与 Azure GWLB 部署期间遇到任何问题，请查看以下故障排除提示：

- 检查 ELB-GWLB 关联。
- 检查 GWLB 中的运行状况探测状态。
- 通过验证 threat defense virtual 物理和逻辑接口上的流量来检查 VXLAN 配置。
- 检查安全组规则。

通过源代码构建 Azure 函数

系统要求

- Microsoft Windows 桌面/笔记本电脑。
- Visual Studio（使用 Visual Studio 2019 版本 16.1.3 进行测试）

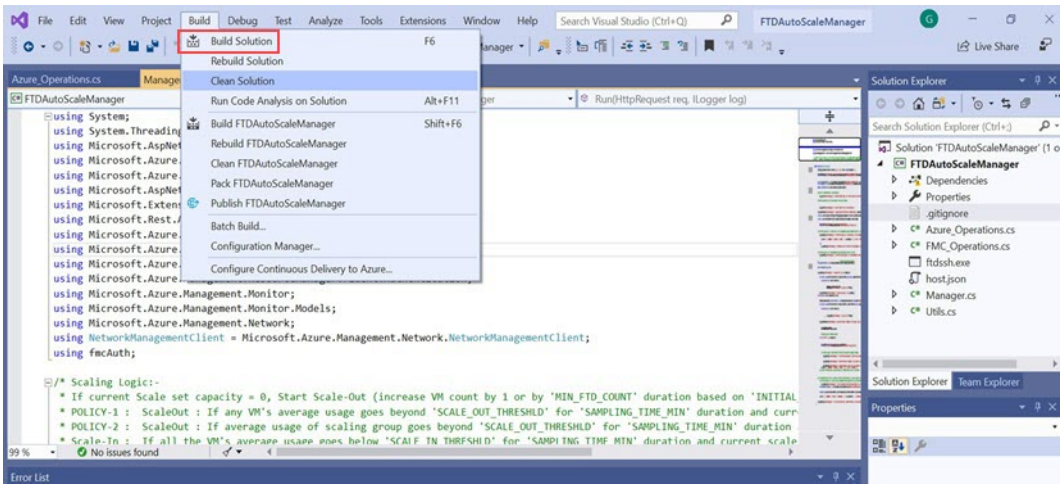
注释 Azure 函数是使用 C# 编写的。

- “Azure Development”工作负载需要安装在 Visual Studio 中。

使用 Visual Studio 构建

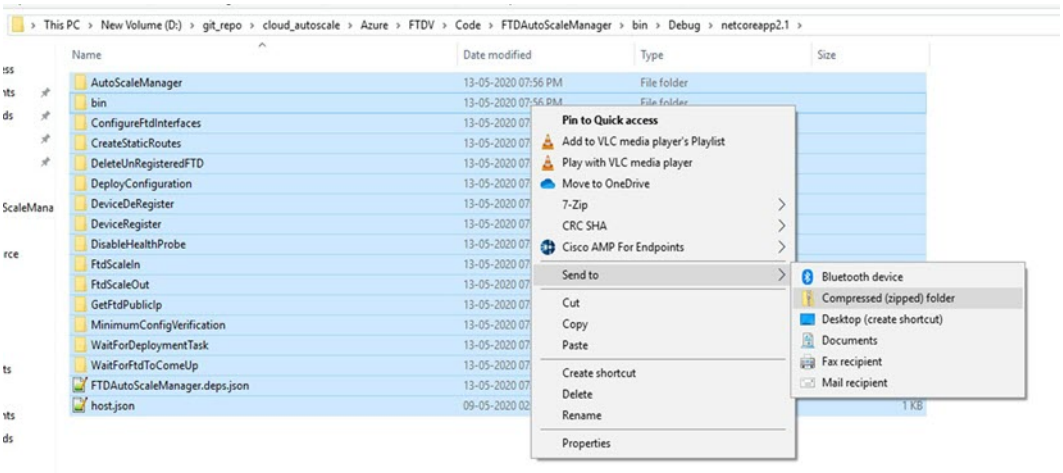
1. 将“code”文件夹下载到本地计算机。
2. 导航到文件夹“FTDAutoScaleManager”。
3. 在 Visual Studio 中打开项目文件“FTDAutoScaleManager.csproj”。
4. 使用 Visual Studio 标准程序进行清理和构建。

图 *29: Visual Studio* 内部版本



5. 成功编译内部版本后，导航到 **\bin\Release\netcoreapp2.1** 文件夹。
6. 选择所有内容，点击 **发送到 (Send to)** > **压缩 (zipped) 文件夹 (Compressed [zipped] folder)**，然后将 ZIP 文件保存为 *ASM_Function.zip*。

图 *30:* 生成 ***ASM_Function.zip***



在 Azure 虚拟 WAN 上部署 Cisco Secure Firewall Threat Defense Virtual

Azure 虚拟 WAN 中的 Threat Defense Virtual 简介

Microsoft Azure 虚拟 WAN 采用“中心辐射型”架构来管理各种虚拟网络和分支机构位置之间的流量。在 Azure 虚拟 WAN 中，将 Threat Defense Virtual 与 Azure 虚拟中心集成有助于在通过中心时对源自组织的本地（辐射）网络（如总部、分支机构和远程用户）的流量进行有效的管理和检查访问 Azure 网络上的 Vnet。此集成通过使用 Threat Defense Virtual 防火墙的专用连接通道，促进网络流量的管理、检查、过滤和路由。

注释 Azure 虚拟 WAN 支持仅具有三个接口的 Threat Defense Virtual 部署模型。

在 Azure 虚拟 WAN 中心部署 Threat Defense Virtual 具有多种优势，包括：

- 无需在连接到中心的每个中心内实施防火墙解决方案。
- 利用 Azure 的内部负载均衡器 (ILB) 的内置功能。
- 在部署期间使用预定义配置扩展实例。

有关在虚拟 WAN 中心部署 Threat Defense Virtual 的信息，请参阅在 Azure 虚拟 WAN 上部署 Threat Defense Virtual。

通过 Azure 虚拟 WAN 上 Threat Defense Virtual 进行流量路由

Azure 虚拟 WAN 中的路由流量方法

Azure 虚拟 WAN 提供边界网关协议 (BGP)，这是一种动态路由协议，可帮助确定在不同 Azure 网络之间发送流量的最佳路由，同时不断更新和共享路由表。虚拟 WAN 中心提供一组 BGP 终端（用于实现高可用性）和自治系统编号 (ASN)，您必须在管理中心将其配置为 Threat Defense Virtual 的 BGP 邻居。

您还可以使用静态路由方法在 Threat Defense Virtual 中手动配置路由。

有关 Azure 中路由的详细信息，请参阅 Azure 文档中的关于 BGP 和 VPN 网关。

路由意图

路由意图是 Azure 虚拟 WAN 中心中的一种路由功能，可简化将互联网绑定和专用流量转发到中心中部署的 Threat Defense Virtual 防火墙进行检查的过程。

有关详细信息，请参阅 Azure 文档中的路由意图。

系统要求

扩展单元

实现最大吞吐量所需的扩展取决于在 Azure 虚拟 WAN 中心部署期间选择或配置的 Threat Defense Virtual 实例 (NVA) 的实例大小和数量。

例如：如果大小为 **D3_V2** 的两个 Threat Defense Virtual 实例可以支持 2.8 Gbps，则 NVA 吞吐量定义为 **Scale-Unit-4: 2.8 Gbps**。

表 *3:* 基于实例类型的 ***Threat Defense Virtual*** 吞吐量级别

扩展单元	**Threat Defense Virtual** 实例	实例类型	吞吐量支持级别
4	2	Standard_D3_v2	3.2 Gbps
10	2	Standard_D4_v2	4.8 Gbps
20	2	Standard_D5_v2	12 Gbps
40	3	Standard_D5_v2	18 Gbps
60	4	Standard_D5_v2	24 Gbps
80	5	Standard_D5_v2	30 Gbps

限制

接口

Threat Defense Virtual 支持三个接口进行部署，因为 Azure 限制 NVA 最多只能支持三个网络接口。

注释 支持三种接口模式的 Threat Defense Virtual 7.4.1 及更高版本与在 Azure 虚拟 WAN 上部署兼容。

Threat Defense Virtual 网络接口的三个子网如下：

- **管理接口** - 它是使用公用 IP 地址将 Threat Defense Virtual 连接到管理中心的**第一个接口**。
- **外部接口（必需）** - 它是将 Threat Defense Virtual 连接到不受信任的公用 IP 地址的**第二个接口**。
- **内部接口（必需）** - 它是将 Threat Defense Virtual 连接到虚拟 WAN 集线器和内部主机网络的受信任专用 IP 地址的**第三个接口**。

Threat Defense Virtual 作为网络虚拟设备 (NVA)

以下是与 Azure 虚拟 WAN 中的 Threat Defense Virtual 作为 NVA 的网络配置相关的主要功能。

- 在 Azure 虚拟 WAN 上部署 Threat Defense Virtual 期间，Azure 会在内部创建 VNet 和子网。因此，在部署完成后无法修改或创建它们。但是，您可以在部署后查看连接到实例的所有 IP 地址。
- 您无法在网络安全组中为每个接口选择端口，但这些端口是在部署期间预定义的。管理接口上仅允许 TCP 端口 443、8305 和 22 连接到互联网。
- 内部接口仅允许在 Azure 虚拟 WAN 中心和与其连接的内部网络内进行通信。

Azure 虚拟 WAN 中心上对 Threat Defense Virtual 的访问限制

您需要授权才能访问在中心上作为托管应用部署到托管资源组中的 Threat Defense Virtual 实例。管理员可以授予对此托管资源组的有限或受限访问权限。

Azure 托管应用提供实时 (JIT) 访问功能，它允许您定义对托管应用的访问权限。有关 JIT 的信息，请参阅 Azure 文档中的 Azure 托管应用概述和即时应用。

IP 支持

- 仅支持 IPv4。

不支持的功能

- 不支持通过 Day 0/自定义数据进行引导。
- Threat Defense Virtual 不支持将指标流传输到 Azure。
- 不支持通过更换操作系统磁盘来升级虚拟机。
- 不支持基于 SSH 密钥登录到 Threat Defense Virtual。
- 不支持 PAYG。

许可

使用思科智能许可证帐户的 BYOL

网络拓扑

作为 Azure 虚拟 WAN 中心中的 NVA，Threat Defense Virtual 会通过中心的网络流量路由来检测来自不同本地网络（辐射型）（例如互联网、分支 [站点] 或作为 VNET）的网络流量。

网络流量通过的这些流量路由分类为以下拓扑：

- 东西：分支到分支
- 东西：VNet 到 VNet
- 南北：分支到互联网
- 南北：VNet 到互联网

注释 Cisco Secure Firewall 版本 7.4.1 不支持通过 Threat Defense Virtual 从**互联网到 VNet 或分支的**流量。

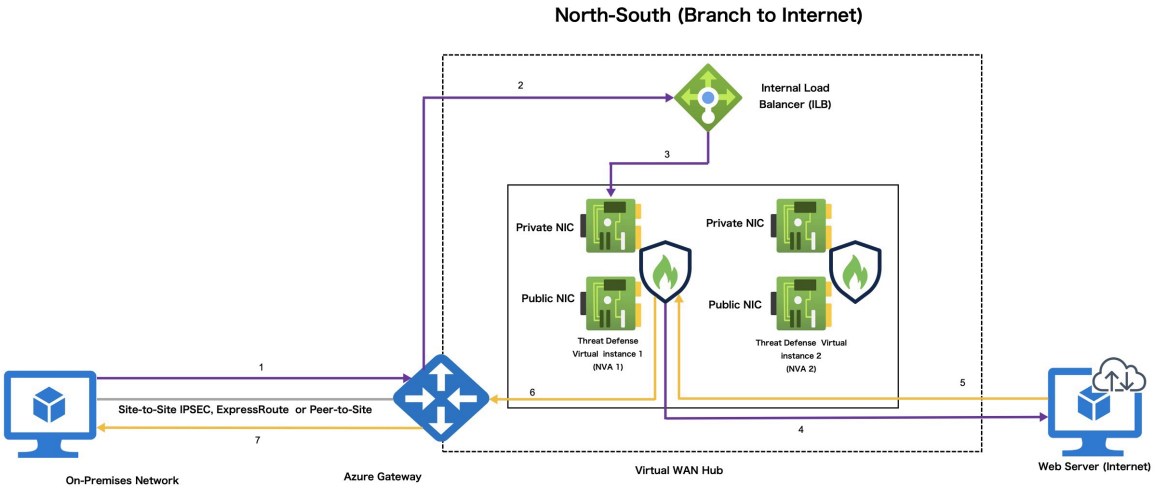
注释 您可以跨 Azure 区域部署多个中心，并连接到虚拟 WAN。此外，您还可以将每个中心配置为拥有自己的 Threat Defense Virtual，用于东西和南北流量检测。

单个虚拟 WAN 中心上按 Threat Defense Virtual 划分的南北流量检测拓扑

此拓扑引用 Threat Defense Virtual 检查在以下设备之间导航的网络流量：

- 分支和 VNET（反之亦然）连接到虚拟 WAN 中心。

图 *31: Azure* 虚拟 *WAN* 中心中的 *Threat Defense Virtual* 南北流量检测拓扑



以下步骤介绍了南北流量检测中的流量流程。

1. 本地网络将流量发送到 Azure 网关。
2. 网关转发到 ILB。
3. ILB 发送到 Threat Defense Virtual (NVA)
4. NVA SNAT 到实例 PIP 并发送到互联网。
5. Web 服务器回复实例 PIP Threat Defense Virtual (NVA) 会撤消 SNAT 并转发到网关。
6. 网关转发到本地网络。

单个虚拟 WAN 中心上按 Threat Defense Virtual 划分的东西流量检测拓扑

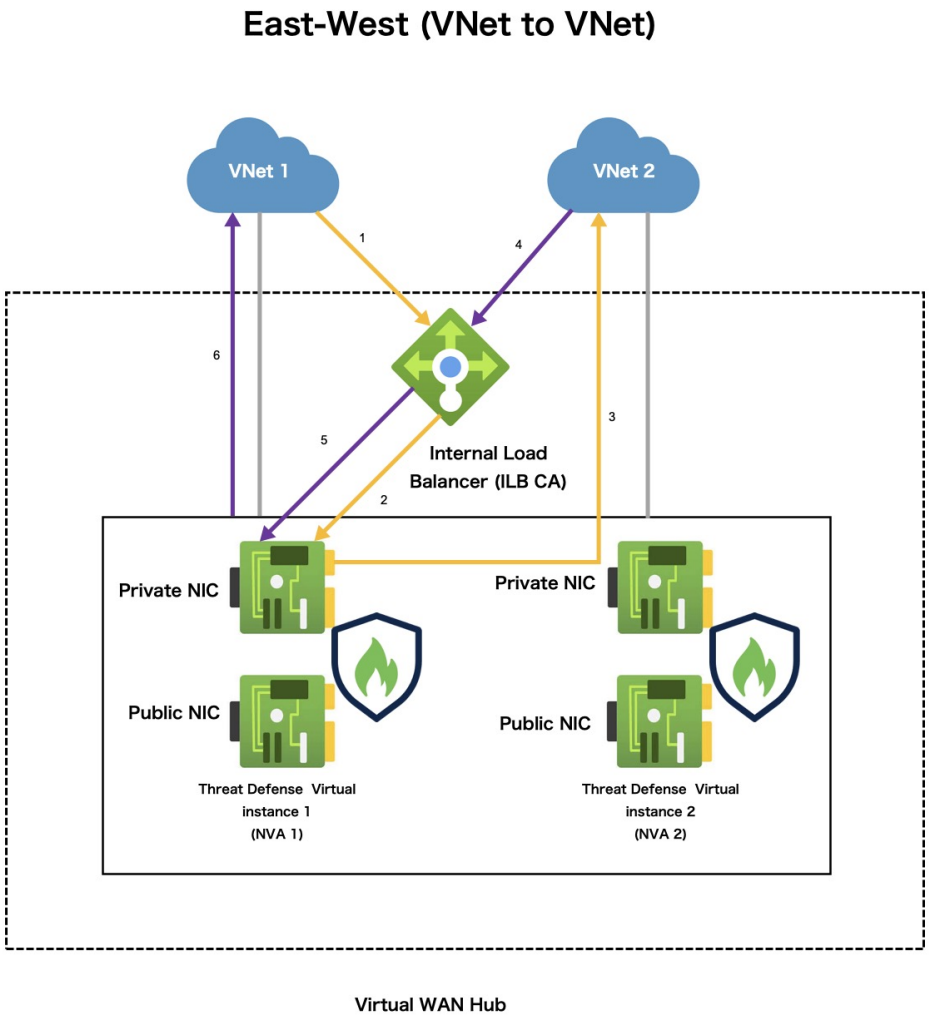
此拓扑引用 Threat Defense Virtual 检查在以下设备之间导航的网络流量：

- 分支和 VNET（反之亦然）连接到虚拟 WAN 中心。

- 从互联网到连接到虚拟 WAN 中心的分支或 VNET。

图 *32: Azure* 虚拟 *WAN* 中心中的 *Threat Defense Virtual* 东西流量检测拓扑

此拓扑是指 Threat Defense Virtual 检查连接到虚拟 WAN 中心的站点到站点（分支和分支）和 VNET 到 VNET 之间导航的网络流量。



以下步骤介绍了东西流量检测中的流量流程。

1. VNet1 将流量发送到 ILB。
2. ILB 选择其中一个活动实例。
3. Threat Defense Virtual (NVA) 直接发送到目标 (VNet 2)。
4. VNet 将流量发送到 ILB。
5. ILB 将流量完全转发到相应的 Threat Defense Virtual (NVA) 状态。

6. Threat Defense Virtual (NVA) 将流量发送回 VNet 1。

在 Azure 虚拟 WAN 上部署 Threat Defense Virtual

您可以使用 Azure 市场上提供的适用于 Azure 虚拟 WAN 的 Cisco Secure Firewall Threat Defense Virtual 产品，在 Azure 虚拟 WAN 中心部署 Threat Defense Virtual。

前提条件

- Microsoft Azure 帐户。您可以在 https://azure.microsoft.com/en-us/ 创建一个。
- 在虚拟 WAN 上创建一个中心。有关在 Azure 中创建虚拟中心的信息，请参阅 Azure 文档中的创建中心。
- 确保虚拟 WAN 中心地址空间小于或等于 /23。

Note Microsoft Azure 允许使用 /24 地址空间的虚拟 WAN 中心。但是，由于未来的增强功能，Microsoft 不建议部署此类中心。不支持在地址空间为 /24 的虚拟 WAN 中心部署 Threat Defense Virtual。

- 思科智能账户。您可以在 Cisco 软件中心创建一个。

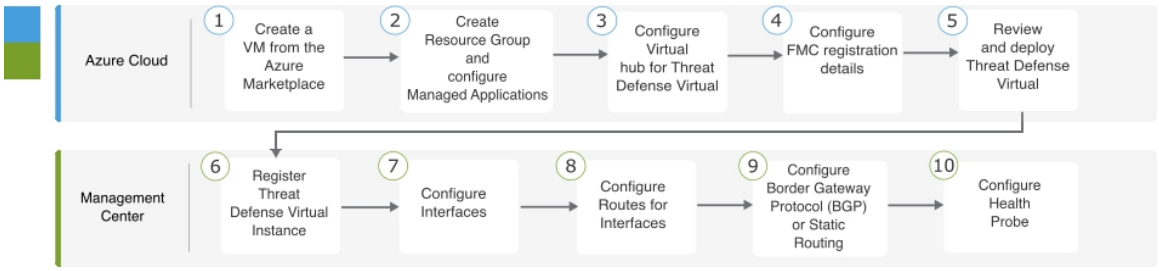
Note 部署 Threat Defense Virtual 实例后，您可以查看附加到该实例的所有公共和专用 IP。

通信路径

- 管理接口 - 用于将威胁防御虚拟连接到管理中心。
- 内部接口（必需）- 用于将威胁防御虚拟连接到内部主机。
- 外部接口（必需）- 用于将威胁防御虚拟连接到公共网络。

端到端程序

以下流程图说明了使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：在 Azure 市场中搜索“适用于 Azure VWAN 的 Cisco Secure Firewall Threat Defense Virtual”。
2	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：创建资源组并配置托管应用。
3	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：配置虚拟中心和 NVA 详细信息。
4	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：配置 FMC 注册详细信息。
5	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：查看并部署 Threat Defense Virtual。
6	管理中心或设备管理器	在管理中心注册 Threat Defense Virtual 实例：注册 Threat Defense Virtual 实例。
7	管理中心或设备管理器	配置接口：配置外部和内部接口。
8	管理中心或设备管理器	为接口配置路由：计算网关 IP 地址，并为外部和内部接口配置路由。
9	管理中心或设备管理器	配置流量路由：配置边界网关协议 (BGP) 或静态路由
10	管理中心或设备管理器	配置运行状况探测功能：配置运行状况探测以启用 ILB，以便对 Threat Defense Virtual 实例执行定期运行状况检查。

使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual

以下说明介绍了如何使用 Azure 市场提供的解决方案模板在 Azure 虚拟广域网上部署 Threat Defense Virtual。这是在 Microsoft Azure 虚拟 WAN 环境中设置 Threat Defense Virtual 所需的顶级步骤列表。

有关 Azure 设置步骤的详细信息，请参阅《Azure 入门》。

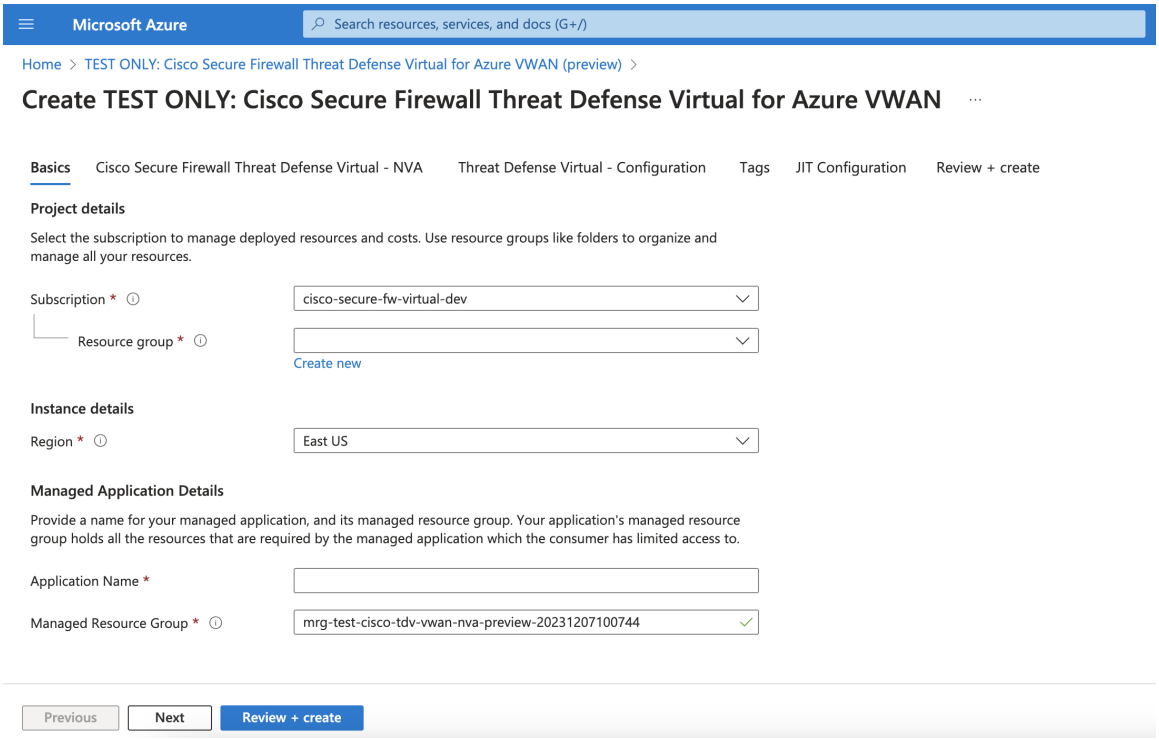
Procedure

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**适用于 Azure VWAN 的 Cisco Secure Firewall Threat Defense Virtual**，选择产品，然后点击**创建 (Create)**以显示**基本 (Basics)** 页面。



步骤 4 配置 **Basics** 设置。

a) 选择您的订用。

b) 创建新的**资源组**。

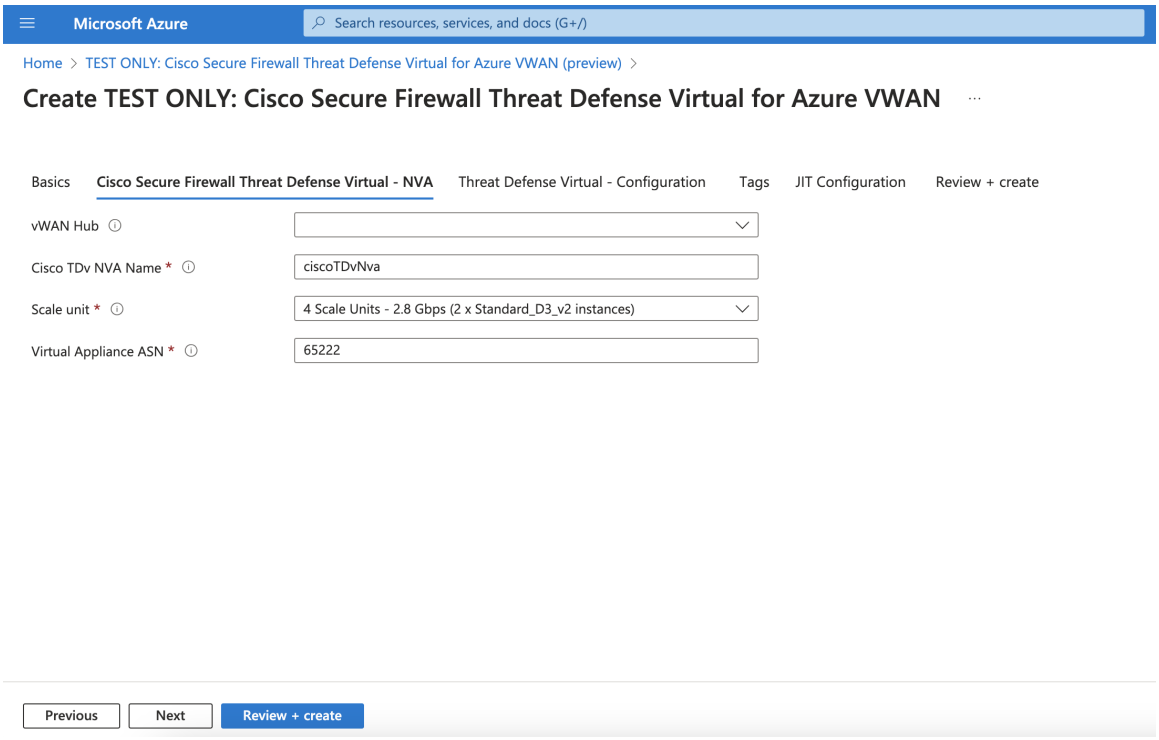
c) 选择虚拟 WAN 中心的地理位置或区域。对于此部署中使用的所有资源（例如虚拟 WAN 中心、Threat Defense Virtual、网络、存储帐户），它应该是相同的。

步骤 5 配置**托管应用详细信息 (Managed Application Details)** 设置。

a) 输入要在其中将 Threat Defense Virtual 实例部署为 NVA 的托管资源组的托管应用的名称。

b) 选择部署 Threat Defense Virtual 实例的托管资源组。

步骤 6 点击**下一步 (Next)**，显示 **Cisco Secure Firewall Threat Defense Virtual - NVA** 页面。



步骤 7 配置虚拟中心和 NVA 详细信息：

a) 从 **vWAN 中心 (vWAN Hub)** 下拉列表中选择虚拟 WAN 中心，以部署 Threat Defense Virtual 实例。

b) 为要部署的 Threat Defense Virtual 实例输入适当的名称。

c) 选择定义要部署的 Threat Defense Virtual 实例数量的扩展单元。

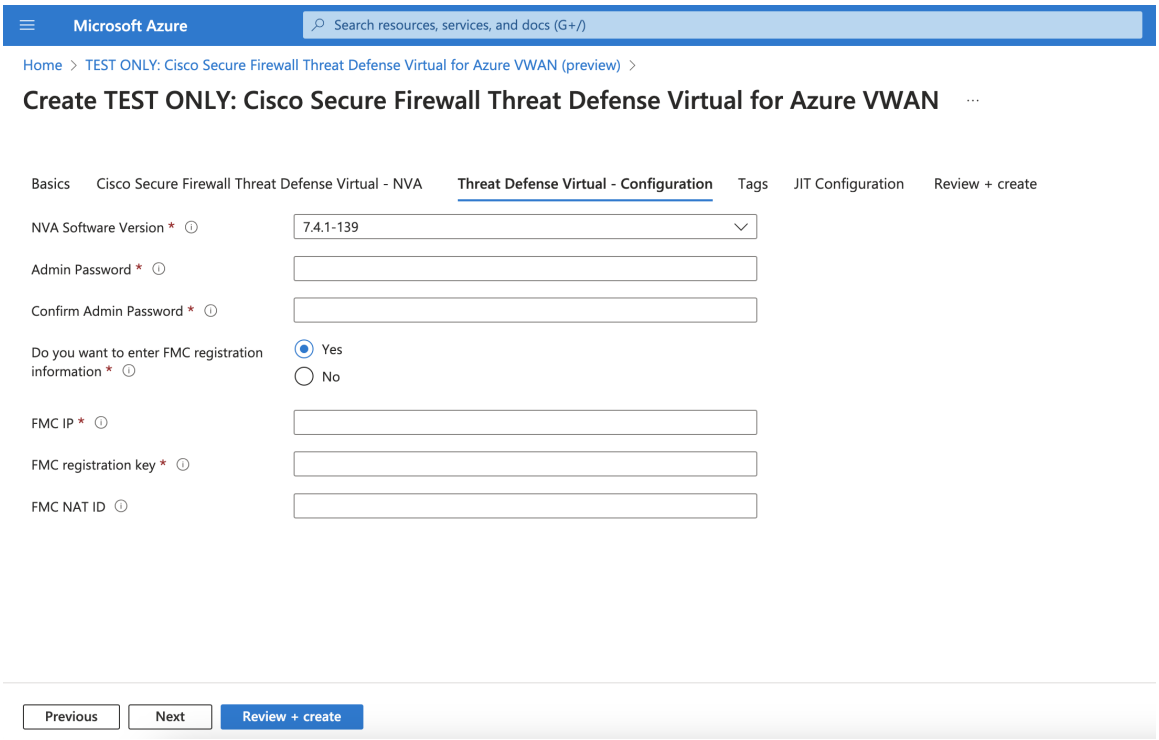
您可以选择所需的扩展单位，以实现所需的 NVA 吞吐量级别。例如，选择 **4 扩展单元 - 2.8 Gbps (4 Scale Units – 2.8 Gbps)(2 x Standard_D3_v2_instances)** 意味着“**扩展单元数量 - 吞吐量级别（具有实例类型的 2 个 Threat Defense Virtual**）。

Note
扩展单元定义您在中心中部署的 Threat Defense Virtual 实例及其关联实例类型的数量。

d) 输入**虚拟设备 ASN**。

Note
输入的 ASN 值必须在 64512 - 65534 范围内。

步骤 8 点击**下一步 (Next)** 以显示 **Threat Defense Virtual - 配置 (Threat Defense Virtual - Configuration)** 页面。



步骤 9 从下拉列表选择相应的 **NVA 软件版本**兼容版本。

Note
此字段提供与您正在部署的相应 Threat Defense Virtual 版本兼容的 NVA 软件版本列表。确保从列表中选择合适的版本。

步骤 10 创建并确认访问包含 Threat Defense Virtual 实例的托管资源组所需的管理员密码。

步骤 11 点击**是 (Yes)** 输入 **FMC 注册信息**。

a) 输入 **FMC IP** 地址。

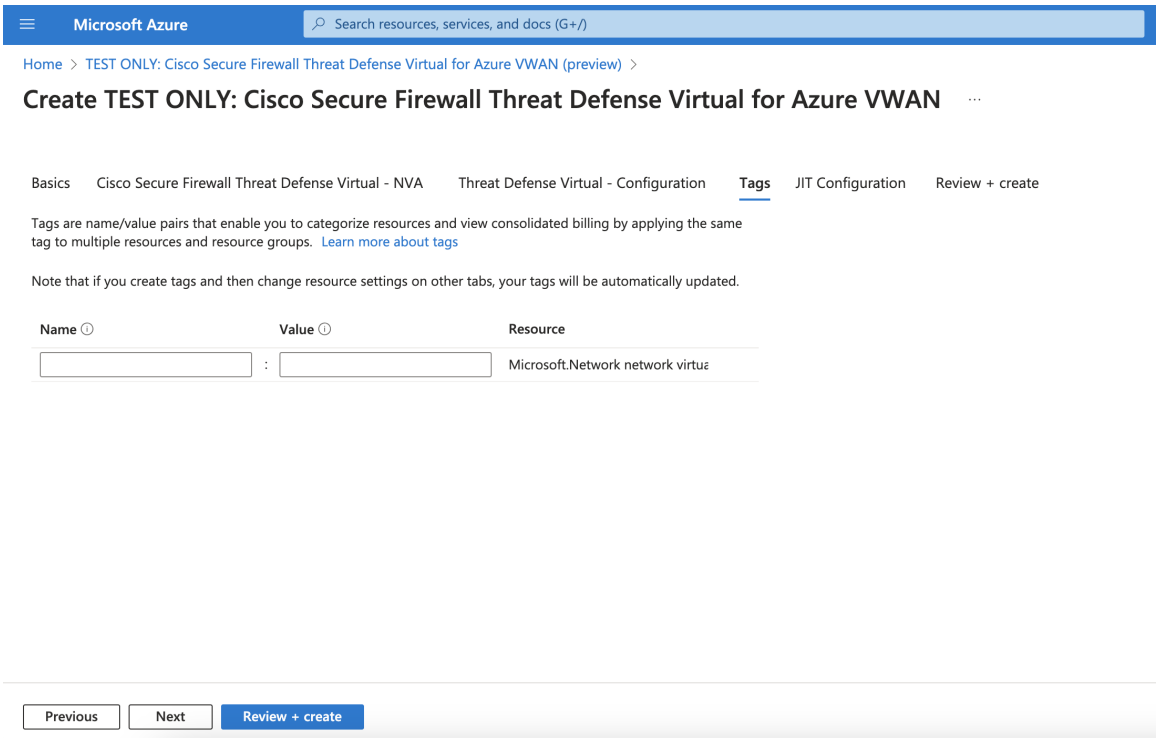
b) 输入用于注册 Threat Defense Virtual 实例的 **FMC 注册密钥** 。

Note
- FMC 注册密钥必须是长度为 1 至 37 个字符的字母数字字符串。在添加 Threat Defense Virtual 时，您将在管理中心上输入此密钥。

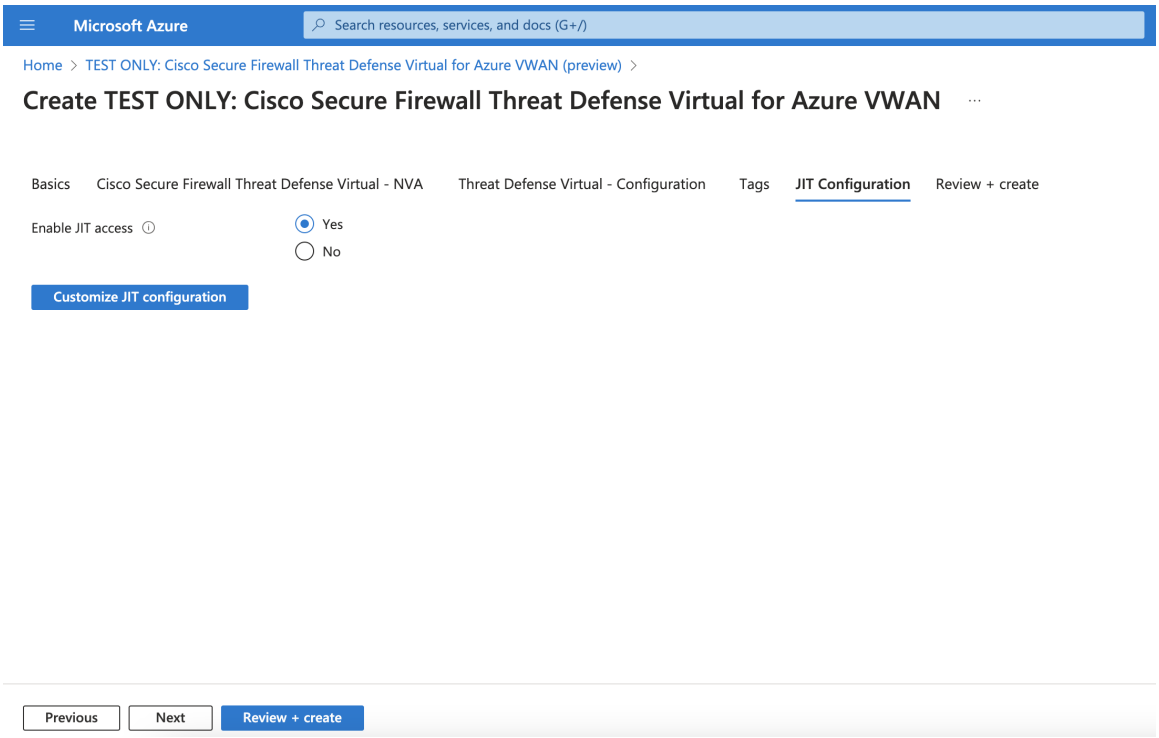
c) [可选] 输入在实例注册期间使用的管理中心 NAT ID。

Note
- NAT ID 必须是长度在 1 - 37 个字符之间的字母数字字符串，仅在一方未指定 IP 地址时，在管理中心和设备之间的注册过程中使用。NAT ID 本质上是一个一次性密码，因此必须是唯一的，而且不能被其他等待注册的设备使用。为确保注册成功，请务必在添加 Threat Defense Virtual 时在 FMC 上指定相同的 NAT ID。

步骤 12 点击**下一步 (Next)** 以配置**标记 (Tags)**。

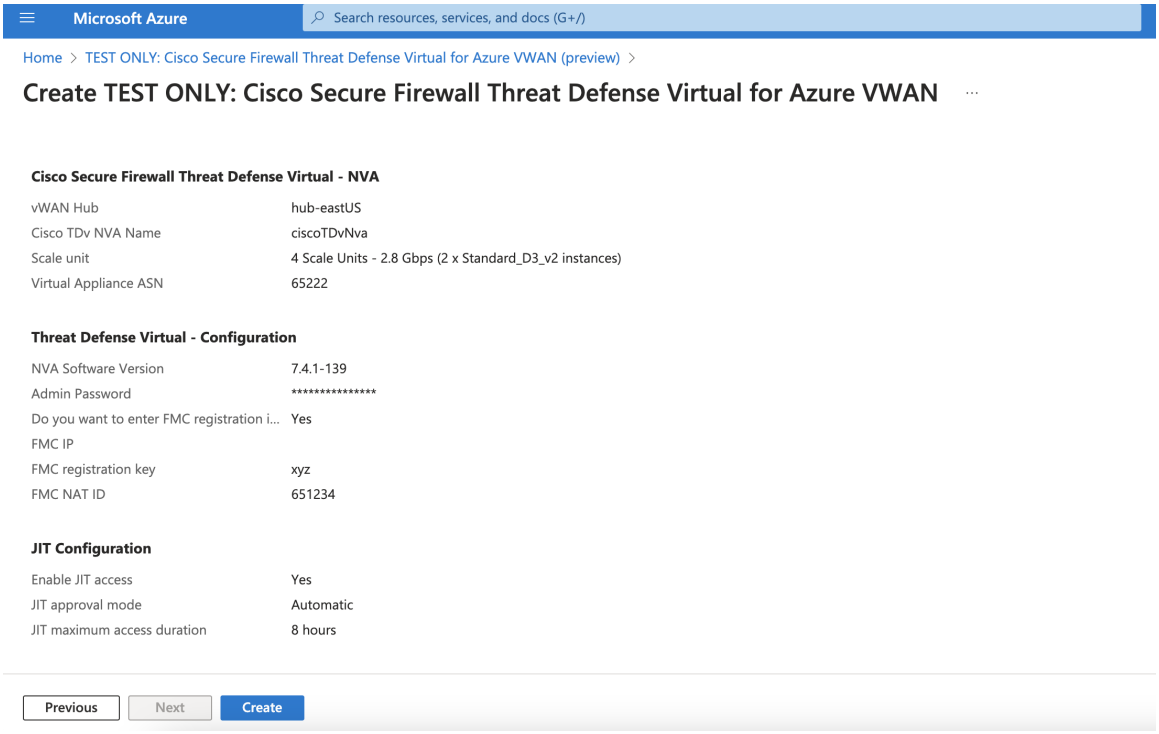


步骤 13 点击下一步 **(Next)** 以显示 **JIT** 配置 **(JIT configuration)** 页面。



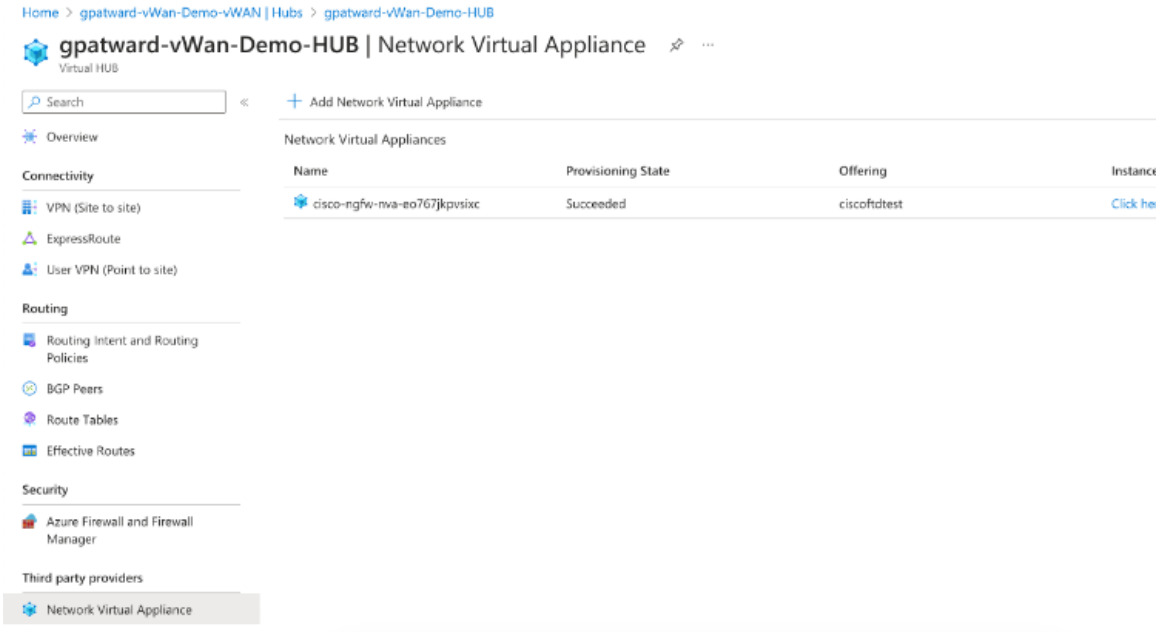
默认情况下，**启用 JIT 访问 (Enable JIT access)** 选项设置为**是 (Yes)**，这样将启用 JIT 调配访问，以管理 Threat Defense Virtual 实例并进行故障排除。

步骤 14 点击下一步 **(Next)** 以显示查看+创建 **(Review+Create)** 页面。



步骤 15 在部署之前，您必须查看订用、NVA、Threat Defense Virtual 和 JIT 配置详细信息，接受条款和条件，然后点击**创建 (Create)** 以在虚拟 WAN 中心上部署 Threat Defense Virtual (NVA)。

步骤 16 转至**主页 (Home)** > **安全 (Security)** > **第三方提供商 (Third-party providers)**，然后点击**网络虚拟设备 (Network Virtual Appliance)**，查看在集线器上创建的 NVA。



步骤 17 点击 **NVA** 以查看已部署的所有 Threat Defense Virtual 实例。

您可以使用实例的管理公用 IP 地址访问 Threat Defense Virtual，并使用 SSH 登录。

Note
您在中心上部署的每个 Threat Defense Virtual 实例的公用 IP 地址用于在管理中心注册实例。

What to do next

注册并配置您在管理中心的中心部署的 Threat Defense Virtual 实例。

在管理中心中配置 Threat Defense Virtual

您可以通过管理中心配置在中心部署的每个 Threat Defense Virtual 实例。

创建 Threat Defense Virtual 配置和管理所需的所有对象，包括设备组，以便您能够轻松地在多个设备上部署策略和安装更新。设备组上应用的所有配置都将被推送到 Threat Defense Virtual 实例。

本节简要概述在管理中心中配置 Threat Defense Virtual 实例的基本步骤。

有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

在管理中心注册 Threat Defense Virtual 实例

您必须在管理中心的通用设备组下注册虚拟 WAN 中心部署的所有 Threat Defense Virtual 实例。它可以帮助您快速将策略和配置部署到这些实例。

Before you begin

- 需要 Azure 虚拟 WAN 中心中部署的每个Threat Defense Virtual 实例的管理公用 IP 地址。它用于在管理中心中设置和注册实例。
- 在管理中心创建设备组。请参阅添加设备组。
- 创建访问控制策略。请参阅创建基本访问控制策略。
- 在中心中部署 Threat Defense Virtual 期间创建的 FMC 注册密钥。

Procedure

步骤 1 登录管理中心。
步骤 2 依次选择**设备** > **设备管理**。
步骤 3 点击**添加 (Add)** > **设备 (Device)**
步骤 4 输入中心中部署的 Threat Defense Virtual 实例的公用 IP 地址。
步骤 5 提供 Threat Defense Virtual 实例的显示名称。
步骤 6 输入您在中心中部署 Threat Defense Virtual 期间创建的管理中心的**注册密钥**。

步骤 7 从**组 (Group)** 下拉列表中，选择要向其添加 Threat Defense Virtual 实例的设备组。

步骤 8 从**访问控制策略 (Access Control Policy)** 下拉列表中，选择要应用于 Threat Defense Virtual 实例的策略。

步骤 9 根据需要输入其他详细信息。

步骤 10 点击**注册 (Register)**。

步骤 11 重复步骤 1 至步骤 10，注册其他 Threat Defense Virtual 实例。

What to do next

配置 Threat Defense Virtual 实例的接口。

配置接口

注册 Threat Defense Virtual 实例后，必须在管理中心配置其接口。

Azure 虚拟 WAN 仅支持**三个**接口，其配置如下：

- 管理接口，将公用 IP 作为第一个接口。
- 外部接口，将公用 IP 作为第二个接口。
- 内部接口，将专用 IP 用作第三个接口（只有专用 IP）。

Procedure

步骤 1 登录管理中心。

步骤 2 转至**设备 (Devices)** 页面。

步骤 3 点击与已注册的 Threat Defense Virtual 对应的**编辑**图标。

步骤 4 点击与接口对应的**编辑**图标。例如 **GigbitEthernet0/0**。

步骤 5 输入 `outside` 作为第一个接口的名称。

步骤 6 选中**已启用 (Enabled)** 复选框以启用该接口。

步骤 7 在**安全区域 (Security Zone)** 下拉列表中，选择 **Outside**。

步骤 8 点击 **IPv4** 菜单，为接口分配 IP 类型。

步骤 9 从 **IP 类型 (IP Type)** 下拉列表中，选择**使用 DHCP (Use DHCP)** 将接口配置为从 DHCP 获取 IP 地址。

步骤 10 选中**使用 DHCP 获取默认路由 (Obtain default route using DHCP)** 复选框。

步骤 11 在**默认路由 (Default route)** 指标中输入 `1`。

步骤 12 点击 **OK** 以保存配置。

步骤 13 重复步骤 1 至步骤 10 以配置内部接口。

What to do next

为接口配置路由。

为接口配置路由

通过创建网络对象并分配网关 IP 地址，为外部和内部接口配置静态路由。

- 外部接口路由配置使用网关 IP 地址作为所有数据包的默认路由。
- 内部接口路由配置使用网关IP地址作为运行状况探测数据包和以中心网络范围为目标的数据包的默认路由。

使用每个接口的 IP 地址和子网掩码地址计算网关 IP 地址。

计算外部和内部接口的网关 IP 地址

本节通过示例说明计算“外部”和“内部”接口的网关 IP 地址的过程。

Procedure

步骤 1 登录管理中心。

步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 访问您在中心部署的 Threat Defense Virtual 实例。

步骤 4 在 **>_Command** 自动中，输入 **`show interface GigbitEthernet 0/0`** 以获取外部接口配置，或者输入 **`show interface GigbitEthernet 0/1`** 以获取内部接口配置详细信息。

步骤 5 重复步骤 1 至步骤 4，以获取内部接口或外部接口的 IP 地址和子网掩码地址。

步骤 6 记下命令结果中的 IP 地址和子网掩码地址。

步骤 7 按照以下示例计算内部和外部的网关 IP 地址：

- 要计算外部接口的网关 IP 地址，请执行以下操作：

  例如：对于 GigabitEthernet0/0（外部接口）

  IP 地址 - **15.0.112.136**

  子网掩码 - **255.255.255.128**

  因此，网关 IP 地址计算为（即此子网中的第一个 IP 地址）**15.0.112.129**。

- 要计算内部接口的网关 IP 地址，请执行以下操作：

  例如：对于 GigabitEthernet0/1（内部接口）

  IP 地址 - **15.0.112.10**

  子网掩码 - **255.255.255.128**

因此，网关 IP 计算为（即此子网中的第一个 IP 地址）**15.0.112.1**。

What to do next

为内部和外部接口配置默认路由。

为外部接口配置默认路由

Procedure

步骤 1 登录管理中心。
步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。
步骤 3 点击 Threat Defense Virtual 实例。
步骤 4 点击**路由 (Routing)** > **静态路由 (Static Route)**。
步骤 5 点击**添加路由**。
步骤 6 在**接口 (Interface)** 下拉列表中，选择 **Outside**。
步骤 7 在**可用网络 (Available Network)** 下为外部接口选择 **any-ipv4**，然后点击**添加 (Add)**。
步骤 8 输入网关 IP 地址：
a) 点击 **+** 图标以添加网路对象。
b) 输入网络对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入已计算的外部接口的网关 IP 地址。
e) 点击**保存 (Save)**。

为内部接口配置默认路由

Before you begin

您必须在集线器上部署 Threat Defense Virtual 的 CIDR IP 地址。您需要此信息才能配置内部接口。

Procedure

步骤 1 登录管理中心。
步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。
步骤 3 点击 Threat Defense Virtual 实例。
步骤 4 点击**路由 (Routing)** > **静态路由 (Static Route)**。
步骤 5 点击**添加路由**。

步骤 6 在**接口 (Interface)** 下拉列表中，选择 **Inside**。

步骤 7 添加网络对象，以使用集线器的 CIDR IP 地址来配置内部接口。

a) 点击 + 图标以添加网路对象。
b) 输入网络对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入中心的 CIDR IP 地址（专用地址空间）。
e) 点击**保存 (Save)**。

步骤 8 添加网络对象，以使用负载均衡器运行状况探测 IP 地址来配置内部接口。

a) 点击 + 图标以添加网路对象。
b) 输入网络对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入负载均衡器运行状况探测的 IP 地址。例如：`168.63.129.16`。

   此 IP 地址是标准地址或固定地址。

步骤 9 输入网关 IP 地址：

a) 点击 + 图标以添加网路对象。
b) 输入对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入已计算的内部接口的网关 IP 地址。
e) 点击**保存 (Save)**。

配置流量路由

您可以配置静态路由或边界网关协议 (BGP)，用于 Threat Defense Virtual 实例与中心之间的数据交换。它实质上是可以为虚拟 WAN 中心中的网络流量配置的两种不同路由方法。

BGP 是一种动态路由协议，它根据中心与 Threat Defense Virtual 设备之间的实时流量交换来考虑路由。而静态路由使用预配置的路由协议来交换流量。

有关 Azure 虚拟 WAN 的详细信息，请参阅 Microsoft Azure 虚拟 WAN 文档。

配置静态路由

Procedure

步骤 1 登录管理中心。

步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击**路由 (Routing)** > **静态路由 (Static Route)**。

步骤 5 点击**添加路由**。

步骤 6 在**接口 (Interface)** 下拉列表中，选择 **Outside**。

如果要配置内部接口，请选择 **Inside**。

步骤 7 添加网络对象 IP 地址：

a) 点击 **+** 图标以添加网路对象。
b) 输入对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入 IP 地址。
e) 点击**保存 (Save)**。

启用 BGP 路由

Procedure

步骤 1 登录管理中心。

步骤 2 依次选择**设备** > **设备管理**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击**路由 (Routing)** 菜单。

步骤 5 点击**常规设置 (General Settings)** 下的 **BGP**。

步骤 6 选中**启用 BGP (Enable BGP)** 复选框。

步骤 7 输入虚拟中心的 AS 编号。

步骤 8 点击**保存 (Save)**。

What to do next

配置 BGP 邻居。

配置 BGP 邻居

Procedure

步骤 1 登录管理中心。

步骤 2 选择 **BGP** > **IPv4** > **邻居 (Neighbor)**。

步骤 3 选中 **Enable IPv4** 复选框。

步骤 4 输入虚拟中心的自治系统 (AS) 编号。

步骤 5 点击**添加 (Add)** 以添加帐户。

步骤 6 输入您记下的 BGP 终端的第一个 IP 地址。

步骤 7 选中**已启用的地址 (Enabled address)** 复选框。

步骤 8 在**远程 AS (Remote AS)** 字段中输入 AS 编号。

步骤 9 选中**高级 (Advanced)** 菜单上的**禁用连接验证 (Disable Connection Verification)** 复选框。

步骤 10 点击**保存 (Save)**。

步骤 11 重复步骤 1 至步骤 8，添加 BGP 终端的第二个 IP 地址。

What to do next

验证 BGP 路由配置。

验证 BGP 路由配置

Before you begin

配置 BGP 终端后，必须验证是否已通过 BGP 终端在 Threat Defense Virtual 和虚拟 WAN 中心之间建立连接。

Procedure

步骤 1 登录管理中心。

步骤 2 依次选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击**设备 (Device)** > **常规 (General)** 构件中的 **CLI**。

步骤 5 在 **_Command** 字段中，输入 **show route** 以查看并验证连接状态。

Note
代码 **B** 表示 BGP 终端与 Threat Defense Virtual 的连接状态。

配置运行状况探测功能

要确保 Threat Defense Virtual 保持稳定状态，您必须配置连接到内部负载均衡器 (ILB) 的内部接口（受信任）。ILB 通过 TCP 端口 443 执行定期运行状况检查探测，以验证来自 Threat Defense Virtual 的响应。

Procedure

步骤 1 登录管理中心。

步骤 2 依次选择**设备 (Devices)** > **平台设置 (Platform Settings)** > **新策略 (New Policy)** > **威胁防御设置 (Threat Defense Settings)**。

步骤 3 为 Threat Defense Virtual 添加**新策略**，以连接到负载均衡器。

步骤 4 编辑已添加的新策略。

步骤 5 选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框，然后在**端口 (Port)** 字段中输入 **443**。

步骤 6 点击 **+ 添加 (+ Add)** 以配置 HTTP 地址。

步骤 7 选择运行状况探测器 IP 地址名称。

步骤 8 从**可用区域/接口 (Available Zone/Interface)** 中选择所需的 IP 地址，然后点击**添加 (Add)** 以将其添加到**选定区域/接口 (Selected Zones/Interfaces)**。

步骤 9 点击**确定 (OK)**。

步骤 10 依次选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 11 点击**已应用的策略 (Applied Policies)** 构件中的编辑图标。

步骤 12 从**平台设置 (Platform Settings)** 下拉列表中选择此策略。

步骤 13 根据需要更新并应用安全策略。

有关配置 HTTP 访问的详细信息，请参阅配置 HTTP。

故障排除

以下是虚拟 WAN 中 Threat Defense Virtual 的常见错误情形和调试提示：

- 流量不会路由到 Threat Defense Virtual。
  - 验证 Threat Defense Virtual 对管理中心运行状况探测检查的响应。
  - 验证内部和外部接口的派生网关 IP 地址是否正确。
  - 检查静态路由。
- 未连接 Threat Defense Virtual 的非 RFC RFC 1918：确保在路由意图中明确指定为专用地址的非 RFC 1918 范围。
- 威胁防御部署错误：如果在部署 Threat Defense Virtual 期间遇到错误：**集线器前缀长度应小于或等于 23**，请确保 HUB 地址空间的 CIDR 小于或等于 **/23**。

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 Threat Defense Virtual。

关于在 Azure 上部署支持的 IPv6

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 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 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 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 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 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 86。

  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 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 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 threat defense virtual 。请参阅使用 VHD 和自定义 IPv6 模板从 Azure 部署, on page 91。

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 threat defense virtual 所涉及的过程。

部署 threat defense virtual 所涉及的步骤如下：

Table 4:

步骤	过程
1	在计划部署支持 IPv6 的 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 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 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 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 (Settings)** 选项下的**编程部署 (Programmatic Deployment)**。

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 (Status)** 列下 threat defense virtual 产品对应的**启用 (Enable)**，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 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 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 threat defense virtual 版本。

对于 threat defense virtual 的 IPv6 支持部署，您必须选择 73* 或更高版本的 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 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 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 threat defense virtual 的用户名。

参数名	允许的值/类型的示例	说明
		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 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 • management center virtual 主机名 • 用于管理的 management center virtual 主机名或 CSF-DM。 'ManageLocally : yes' - 这将配置要用作 threat defense virtual管理器的 CSF-DM。 您可以将 management center virtual 配置为 threat defense virtual 管理器，也可以为在 management

参数名	允许的值/类型的示例	说明
		center virtual 上进行相同配置所需的字段提供输入。
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。

参数名	允许的值/类型的示例	说明
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“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	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 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 (Enable Local Manager)** 选择**否 (No)**，z呃您将使用 Cisco Secure Firewall Management Center 来管理 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 (Enable Local Manager)** 选择**是 (Yes)**，则您将使用集成 Cisco Secure Firewall 设备管理器 来管理 threat defense virtualthreat defense virtualthreat defense virtualthreat 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 threat defense virtual 映像。此过程类似于使用 VHD 和资源模板部署 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 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 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 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 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 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 (Save)**。

下表介绍了您需要在 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 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 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 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

参数名	允许的值/类型的示例	说明
		• CSF-MCv 主机名 • 用于管理的 CSF-MCv 主机名或 CSF-DM。 'ManageLocally : yes' - 这将配置要用作 threat defense virtual管理器的 CSF-DM。 您可以将 CSF-MCv 配置为 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。

参数名	允许的值/类型的示例	说明
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。
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	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 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 threat defense virtual 的 IP 配置。

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 threat defense virtual。映像快照是没有状态数据的已复制 threat defense virtual 映像实例。

Threat Defense Virtual 快照概述

创建 threat defense virtual 实例快照映像的过程跳过为 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 threat defense virtual 初始启动过程，该过程使映像能够重新生成与 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 threat defense virtual 的启动时间，这在 Auto Scale 部署中至关重要。

从托管映像创建 Threat Defense Virtual 快照映像

Threat Defense Virtual 映像快照创建是在 Azure 门户中复制 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 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 16。

不得将正准备拍摄映像快照的 threat defense virtual 实例注册到任何管理器，例如 管理中心 或 设备管理器。

Procedure

步骤 1 转至 Azure 门户，您已在其中创建了 threat defense virtual 实例的托管映像。

Note
确保您计划复制的 threat defense virtual 实例未注册到 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 threat defense virtual 实例。

步骤 3 点击 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 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，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 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 threat defense virtual 实例的新快照映像。

What to do next

使用快照映像部署 threat defense virtual 实例。请参阅使用映像快照部署 Threat Defense Virtual 实例。

使用映像快照部署 Threat Defense Virtual 实例

Before you begin

Cisco 建议以下操作：

- 确认快照映像可用于 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 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 threat defense virtual 实例。请参阅从 Azure 使用 VHD 和资源模板部署, on page 16。

Note
您可以从 threat defense virtual 控制台运行 CLI 命令 **show version** 和 **show snapshot detail**，以了解新部署的 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。