部署适用于 Azure 的 Firepower Threat Defense Virtual Auto Scale

适用于 Azure 上 FTDv 的 Auto Scale 解决方案

关于 Auto Scale 解决方案

FTDv 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）。

FTDv Auto Scale for Azure 实现的一些主要功能包括：

- FMC 中完全自动化的 FTDv 实例注册和取消注册。
- （**FP 6.7 新增**）支持基于 CPU 和内存 (RAM) 的扩展指标：
  - 仅 CPU。未改变之前版本中的行为。
  - CPU、内存。对于外向扩展策略，您可以选择将 CPU 或内存指标的扩展阈值分开。内向扩展策略同时考虑 CPU 和内存，将终止 CPU 负载最小的设备。

    有关详细信息，请参阅Auto Scale 逻辑， 第 32 页。

- 自动应用到外向扩展 FTDv 实例的 NAT 策略、访问策略和路由。
- 支持标准负载均衡器。
- 支持 FTDv 部署 om 多可用性区域。
- 对启用和禁用自动扩展功能的支持。
- 基于 Azure Resource Manager (ARM) 模板的部署。
- 仅适用于 FMC；不支持 Firepower Device Manager。
- 支持使用 PAYG 或 BYOL 许可模式部署 FTDv。PAYG 仅适用于 FTDv 软件版本 6.5 和更高版本。请参阅支持的软件平台 ， 第 2 页。

Cisco 提供 Auto Scale for Azure 部署包以方便部署。

支持的软件平台

FTDv Auto Scale 解决方案适用于 FMC 管理的 FTDv，与软件版本无关。《Cisco Firepower 兼容性指南》提供 Cisco Firepower 软件和硬件兼容性，包括操作系统和托管环境要求。

- Firepower Management Center：虚拟表列出 FMCv 的 Firepower 兼容性和虚拟托管环境要求。
- Firepower Threat Defense Virtual 兼容性表列出了 Azure 上 FTDv 的 Firepower 兼容性和虚拟托管环境要求。

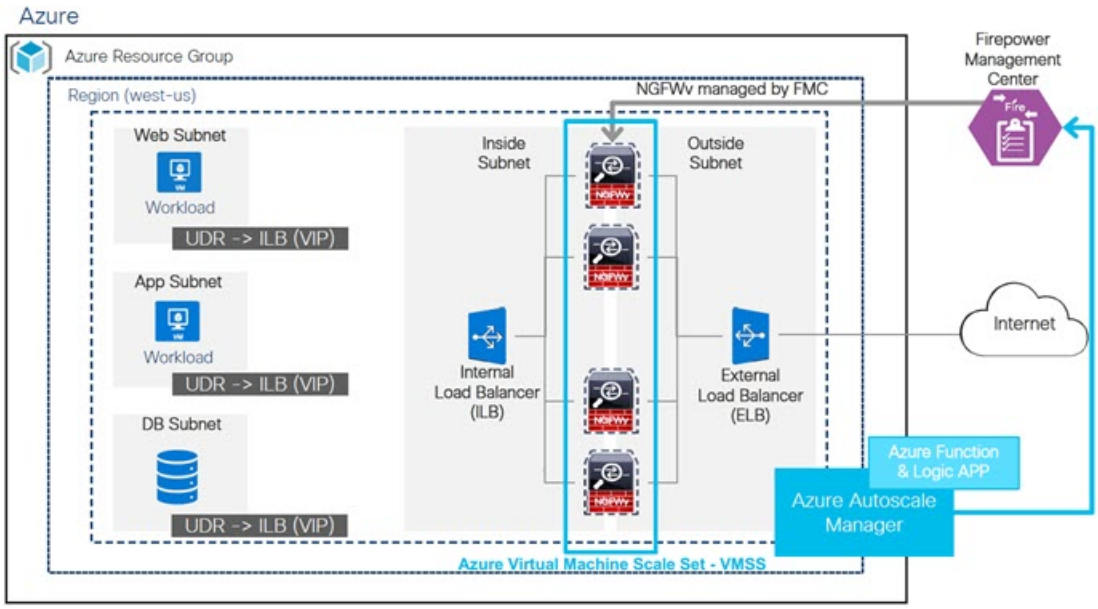
注释 就部署 Azure Auto Scale 解决方案而言，Azure 上的 FTDv 最低支持的 Firepower 版本是版本 6.4。

Auto Scale 使用案例

FTDv Auto Scale for Azure 是一种自动化水平扩展解决方案，它将 FTDv 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 FTDv 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 FTDv 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 FTDv 实例数将根据负载条件自动进行扩展和配置。

图 *1: FTDv Auto Scale* 用例图



适用范围

本文档介绍部署 FTDv Auto Scale for Azure 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

FTDv Auto Scale for Azure 解决方案作为存档文件提供：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。从 GitHub 存储库下载该存档文件，网址为：

- https://github.com/CiscoDevNet/cisco-ftdv/tree/master/deployment-templates/azure

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，请参阅附录 - 通过源代码构建 Azure 函数 ，第 35 页。

Auto Scale 解决方案组件

以下组件构成了 FTDv 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 FTDv 负载和触发内向扩展/外向扩展操作。
- 向 FMC 注册新的 FTDv。
- 通过 FMC 配置新的 FTDv。
- 从 FMC 取消注册（删除）内向扩展的 FTDv。

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 6 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。此编排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 FTDv 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 FTDv 禁用。
- 您不应在 VMSS 中手动添加或删除 FTDv 实例。

Azure Resource Manager (ARM) 模板

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

ARM 模板为 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。

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。

Auto Scale 解决方案前提条件

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

确保在资源组中创建虚拟网络。Auto Scale 部署将不会创建、更改或管理任何网络资源。

FTDv 需要 4 个网络接口，因此您的 Azure 部署需要 4 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 FTDv 之间的运行状况探测所必需。

  无服务器函数与 FTDv 之间的通信所必需。

- TCP/8305

FTDv 与 FMC 之间的通信所必需。

- HTTPS(TCP/443)

  无服务器组件与 FMC 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

FTDv Azure 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，请参阅附录 - 通过源代码构建 Azure 函数 ，第 35 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 Firepower Management Center

您可以使用功能齐全的多设备管理器 Firepower Management Center (FMC) 来管理 FTDv。FTDv 在您分配给 FTDv 虚拟机的管理接口上向 FMC 注册并与之通信。

创建 FTDv 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 FTDv 实例。

以下各节简要概述准备 FMC 的基本步骤。有关完整信息，应参阅整个《Firepower Management Center 配置指南》。准备 FMC 时，请确保记录以下信息：

- FMC 公共 IP 地址。
- FMC 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 FMC 用户

在 FMC 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 FMC 会话冲突，拥有专用于 FTDv Auto Scale 解决方案的 FMC 用户帐户非常重要。

过程

步骤 1 在 FMC 中创建具有 Admin 权限的新用户。选择**系统** > **用户**，然后单击**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 FMC 配置指南。

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 FMC 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 单击**新建策略**。

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 FMC 配置指南，以便为您的部署配置安全设置和规则。

配置许可

所有许可证都由 FMC 提供给 FTD。您可以选择购买以下功能许可证：

- **威胁** - 安全情报和 Cisco Firepower 下一代 IPS
- **恶意软件** - 适用于网络的高级恶意软件防护 (AMP)
- **URL** - URL 过滤
- **RA VPN** - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

注释 购买威胁、恶意软件或 URL 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，请单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账户。

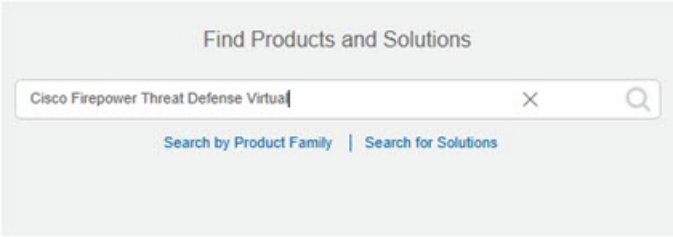
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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，则请使用思科商务工作空间上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *2:* 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 如果尚未这样做，请向智能许可服务器注册 FMC。

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 FMC 配置指南。

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 单击**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 单击保存。

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

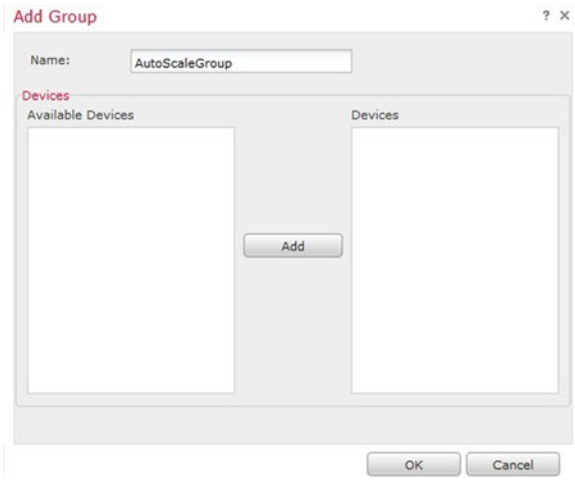
步骤 1 选择设备 > 设备管理。

图 *3:* 设备管理

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

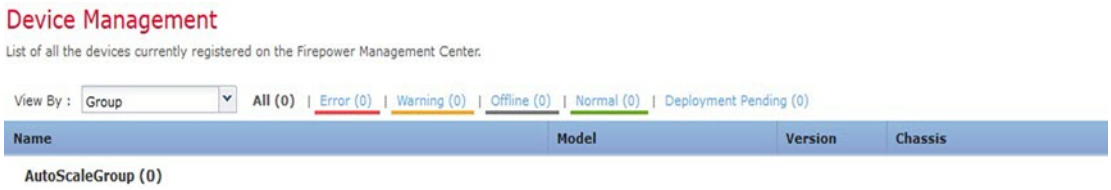
步骤 3 输入 **Name**。例如，*AutoScaleGroup*。

图 *4:* 添加设备组



步骤 4 单击确定 **(OK)** 以添加组。

图 *5:* 已添加设备组



配置安全外壳访问

FTD 设备的平台设置会配置一系列不相关的功能，您可能想要在多个设备之间共享它们的值。FTDv Auto Scale for Azure 需要 FTD 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 FTDv 的数据接口可以响应负载均衡器的运行状况探测。

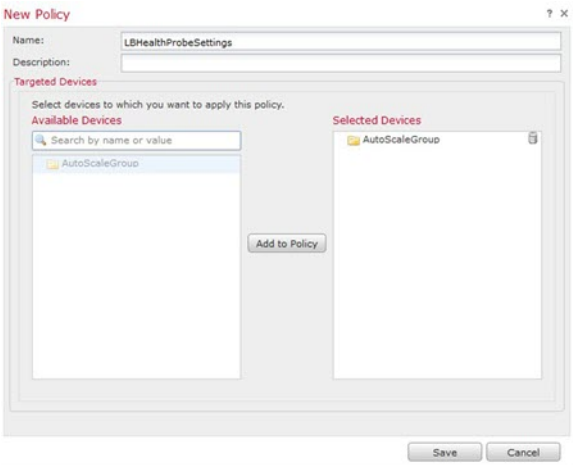
开始之前

- 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** > **平台设置**，然后创建或编辑 FTD 策略，例如 *LBHealthProbeSettings*。

图 *6: FTD* 平台设置策略



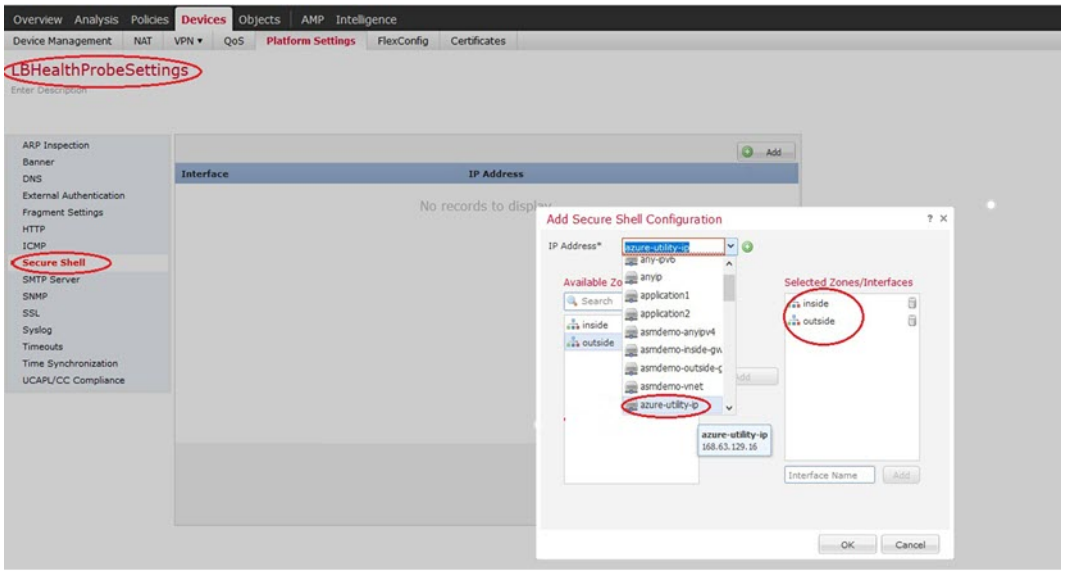
步骤 2 选择**安全外壳**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

a) 单击**添加**以添加新规则，或单击**编辑**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，或者单击“+”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 FMC 的**对象**页创建安全区域。有关安全区域的完整信息，请参阅 FMC 配置指南。
- 单击**确定**。

图 *7: FTDv Auto Scale* 的 *SSH* 访问



步骤 4 单击**保存**。

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。

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。

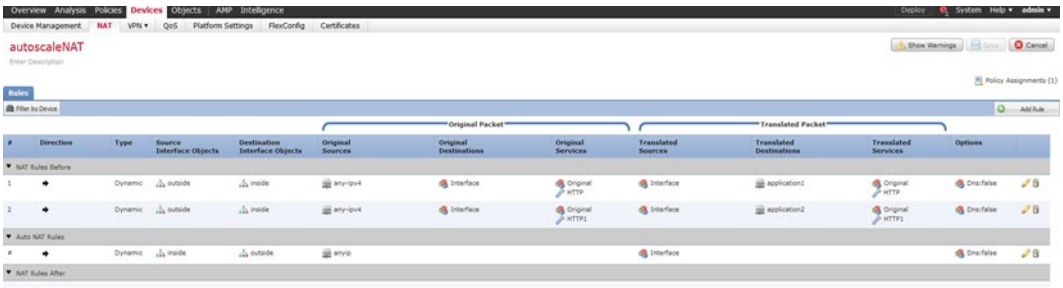
过程

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 FMC 配置指南中“配置威胁防御 NAT”。下图所示为基本方法。

图 *8: 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 单击保存。

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 FTDv 设备。请参阅部署 Auto Scale ARM 模板，第 17 页。

表 *1:* 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*	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。	New
virtualNetworkRg	字符串	资源组的名称	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）	现有
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）	现有
diagSubnet	字符串	诊断子网名称（已创建）	现有
insideSubnet	字符串	内部子网名称（已创建）	现有

参数名	允许的值/类型	说明	资源创建类型
insideNetworkGatewayIp	字符串	内部子网关 IP（已创建）	现有
outsideSubnet	字符串	外部子网名称（已创建）	现有
outsideNetworkGatewayIp	字符串	外部子网关 IP（已创建）	现有
internalLbIP	字符串 x.x.x.x	要分配给内部负载均衡器的 IP（内部子网）	New
deviceGroupName	字符串	FMC 中的设备组（已创建）	现有
insideZoneName	字符串	FMC 中的内部区域名称（已创建）	现有
outsideZoneName	字符串	FMC 中的外部区域名称（已创建）	现有
softwareVersion	字符串	FTDv 版本（在部署期间从下拉列表中选择）	现有
vmSize	字符串	FTDv 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	FTDv 许可模式 (PAYG/BYOL) 注：PAYG 在版本 6.5+ 中受支持。	不适用
licenseCapability	逗号分隔的字符串	BASE, MALWARE, URLFilter, THREAT	不适用
ftdVmManagementUserName	字符串*	FTDv VM 管理管理员用户名。 注：这**不能**是“admin”。	New
ftdVmManagementUserPassword	字符串*	FTDv 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：模板中不对此进行合规性检查。	New

参数名	允许的值/类型	说明	资源创建类型
ftdAdminUserPassword	字符串*	FTDv“admin”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：模板中不对此进行合规性检查。	New
fmcIpAddress	字符串 x.x.x.x	FMC 的公共 IP 地址（已创建）	现有
fmcUserName	字符串	FMC用户名，具有管理权限（已创建）	现有
fmcPassword	字符串	上述 FMC 用户名的 FMC 密码（已创建）	现有
policyName	字符串	在 FMC 中创建的安全策略（已创建）	现有
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 FTDv 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 FTDv 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 FTDv 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。	
scaleInThreshold	整数	当所有 FTDv 指标（仅 CPU 利用率、CPU/内存利用率）低于此值时，将触发内向扩展。	不适用
scaleOutThreshold	整数	当任何 FTDv 指标（仅 CPU 利用率、CPU/内存利用率）高于此值时，将触发外向扩展。 “scaleOutThreshold”应始终大于“scaleInThreshold”。	不适用

参数名	允许的值/类型	说明	资源创建类型
minFtdCount	整数	在任何给定时间，规模集中可用的最小 FTDv 实例数。 示例：2	不适用
maxFtdCount	整数	规模集中允许的最大 FTDv 实例数。 示例：10 注 1：此数量受 FMC 容量的限制。 注 2：Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用
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（仅 CPU 利用率、CPU/内存利用率），并且基于此平均值做出扩展决定。 注：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 FTDv 实例时。 BULK：Auto Scale Manager 将尝试一次并行部署“minFtdCount”数量的 FTDv 实例。 注：启动采用并行方式，但由于 FMC 的限制，需要按顺序注册到 FMC。 STEP：Auto Scale Manager 将按照计划间隔逐个部署“minFtdCount”数量的 FTD。 注 1：STEP 选项需要较长时间来启动“minFtdCount”数量的实例并使用 FMC 进行配置，然后实现运行，但在调试时很有帮助。 注 2：BULK 选项启动所有“minFtdCount”数量的 FTDv 所花费的时间与一次 FTDv 启动相同（因为它是并行运行的），但 FMC 注册是按顺序进行的。 部署“minFtdCount”数量的 FTDv 所花费的总时间 =（启动一个 FTDv 所用的时间 + 注册/配置一个 FTDv 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**。			

Auto Scale 部署

下载部署软件包

FTDv Auto Scale for Azure 解决方案作为存档文件提供：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。从 GitHub 存储库下载该存档文件，网址为：

- https://github.com/CiscoDevNet/cisco-ftdv/tree/master/deployment-templates/azure

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，请参阅附录 - 通过源代码构建 Azure 函数 ，第 35 页。

部署 Auto Scale ARM 模板

ARM 模板用于部署 FTDv 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）

开始之前

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

过程

步骤 1 如果您需要在多个 Azure 区域中部署 FTDv 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。

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"
            }
          ],
```

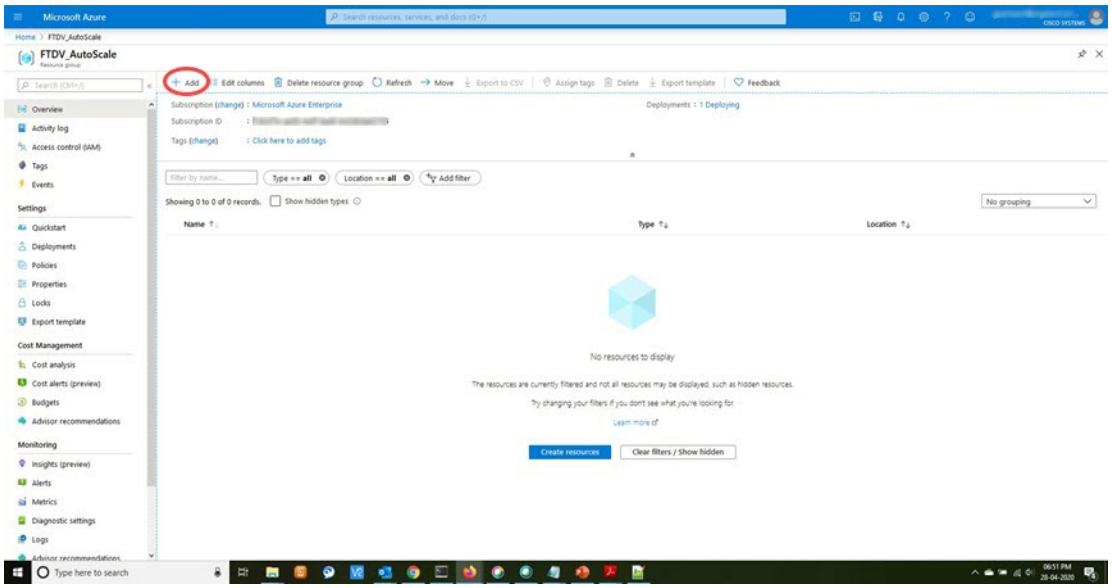
注释 如果您不想编辑此文件，也可以在部署后从 Azure 门户编辑此项。

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 单击服务菜单中的**资源组**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，*FTDV_AutoScale*。

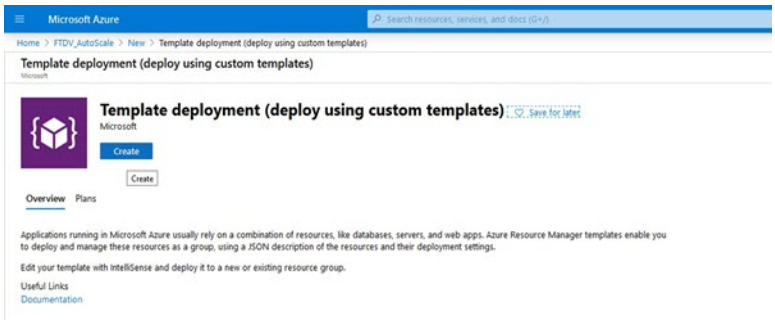
图 *9: Azure* 门户



步骤 5 单击**创建资源 (+)**，为模板部署创建新资源。此时将显示“创建资源组”边栏选项卡。

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

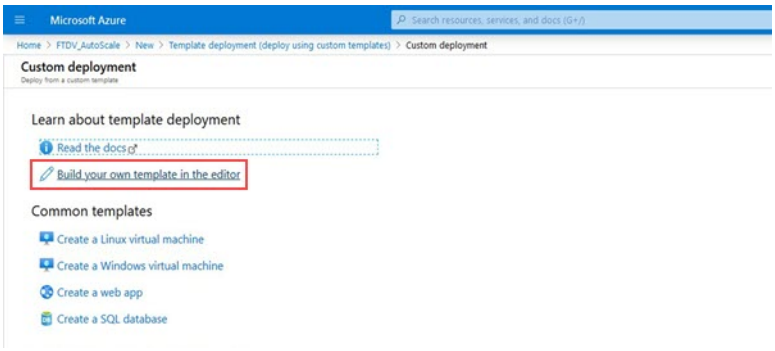
图 *10:* 自定义模板部署



步骤 7 单击**创建**。

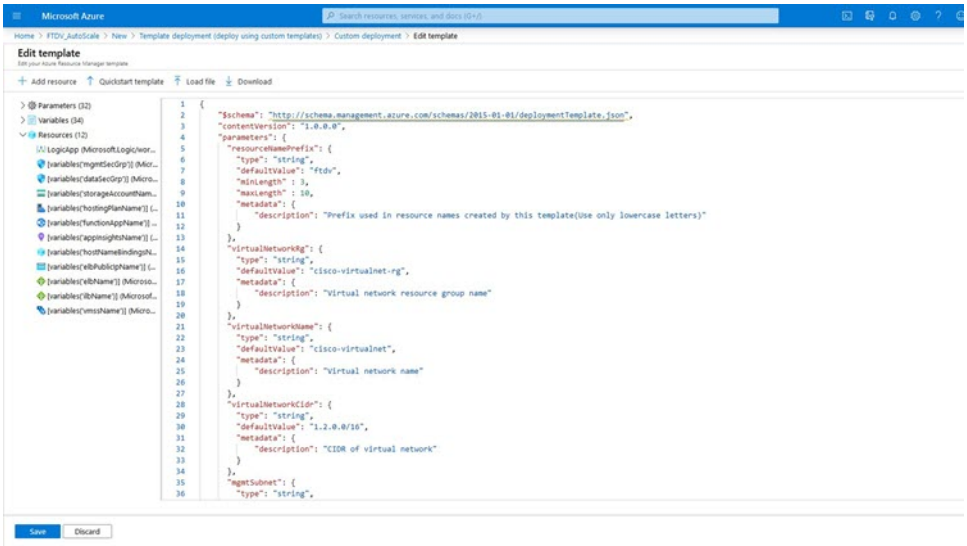
步骤 8 创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板**。

图 *11:* 构建您自己的模板



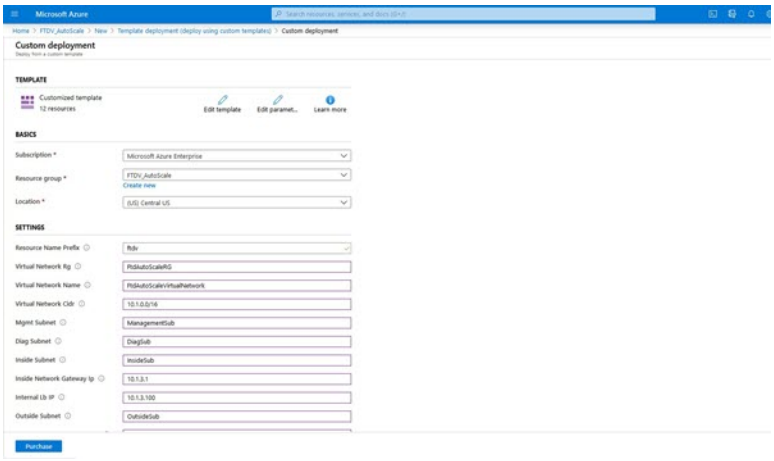
步骤 9 在**编辑模板**窗口中，删除所有默认内容并更新来自 *azure_ftdv_autoscale.json* 的内容，然后单击**保存**。

图 *12:* 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 12 页，然后单击**购买**。

图 *13: ARM* 模板参数

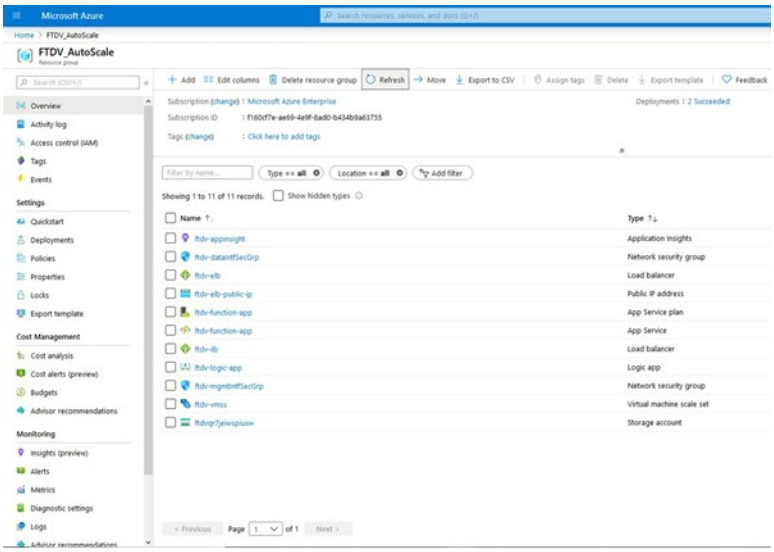


注释　　您也可以单击**编辑参数**，然后编辑 JSON 文件或上传预填的内容。

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 FTDv 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”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 *14: FTDv 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。请参阅附录 - 通过源代码构建 Azure 函数，第 35 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

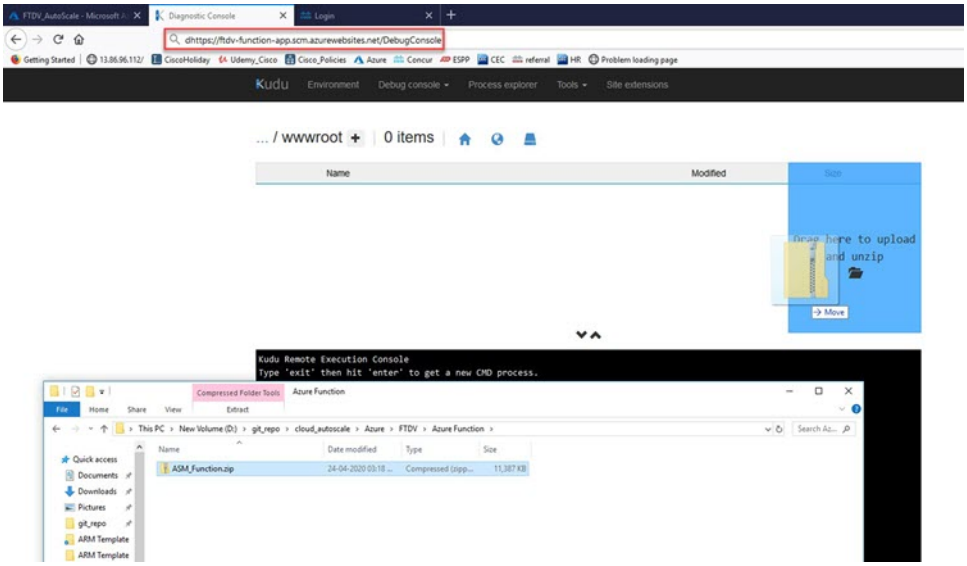
对于部署 Auto Scale ARM 模板，第 17 页中的示例：

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**。

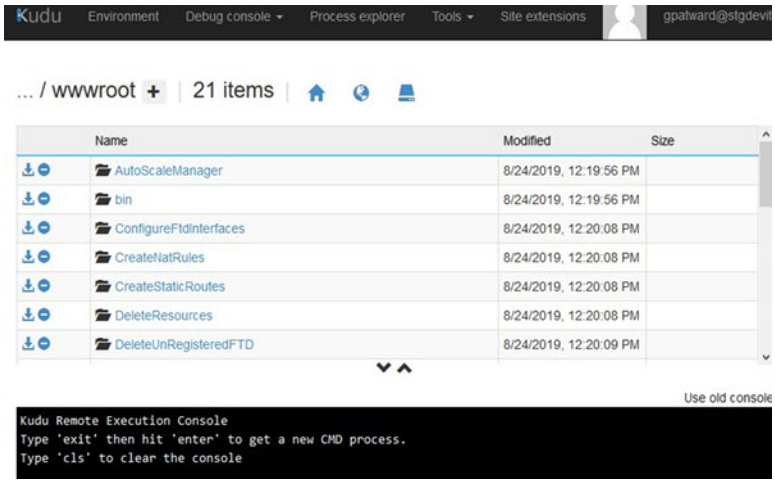
步骤 3 将 **ASM_Function.zip** 拖放到文件资源管理器的右侧。

图 *15:* 上传 ***FTDv Auto Scale*** 函数



步骤 4 成功上传后，应该会显示所有无服务器函数。

图 *16: FTDv* 无服务器函数

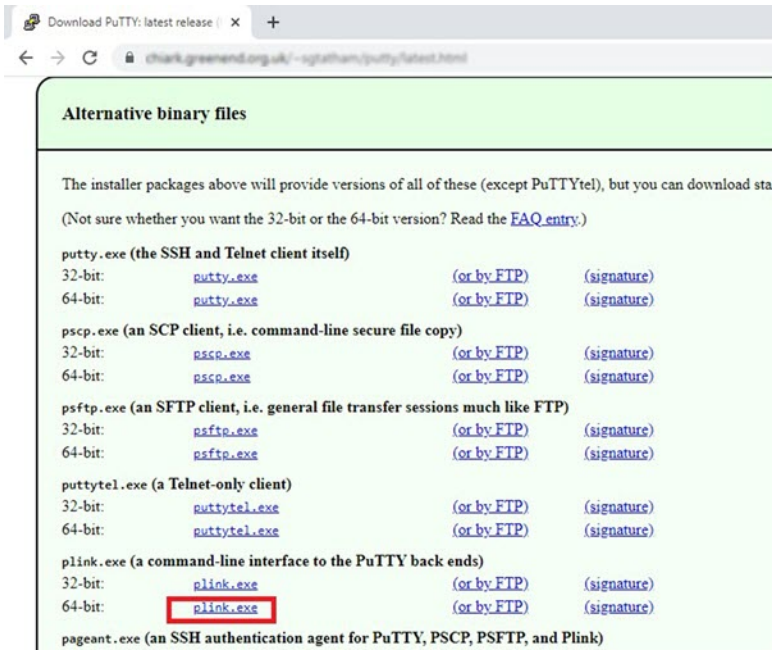


步骤 5 下载 PuTTY SSH 客户端。

Azure 函数需要通过 SSH 连接访问 FTDv。但是，无服务器代码中使用的开源库不支持 FTDv 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 *17:* 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

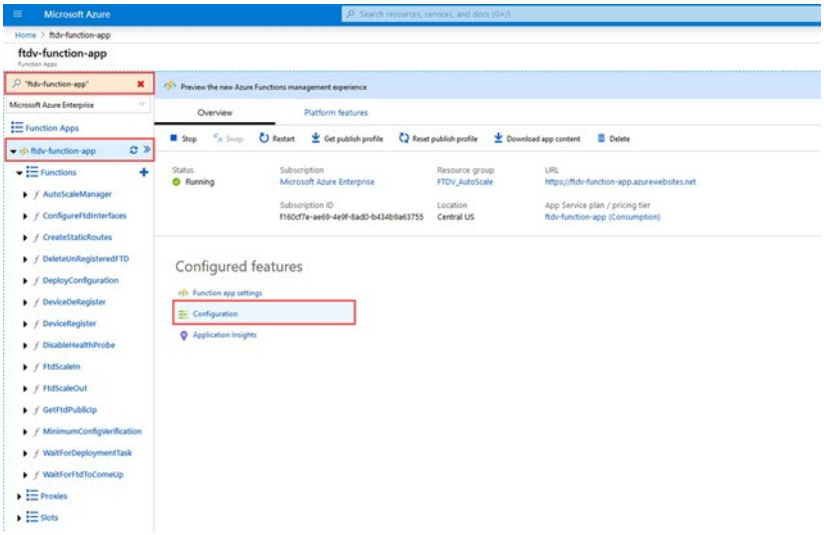
注释 可以随时编辑此项。按照以下顺序编辑配置。

- 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

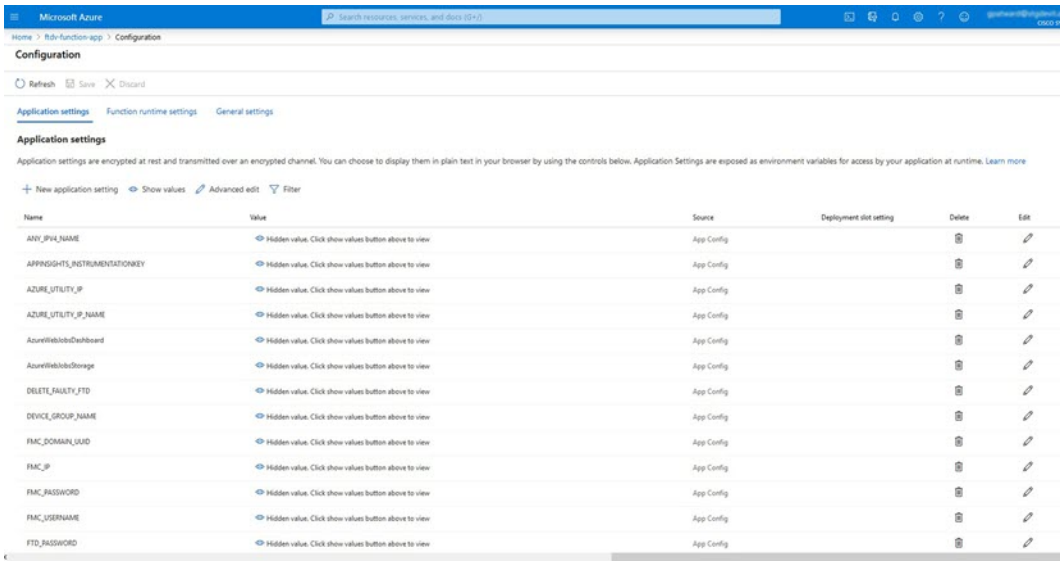
步骤 1 在 Azure 门户中，搜索并选择 FTDv 函数应用。

图 *18: FTDv* 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 *19:* 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 FTDv 实例并将其注册到 FMC。如果注册失败，则 Auto Scale Manager 将根据此选项决定保留该 FTD 实例或将其删除。（YES：删除错误的 FTD/NO：保留 FTD 实例，即使未能注册到 FMC）。

- 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 单击**访问控制 (IAM)**。

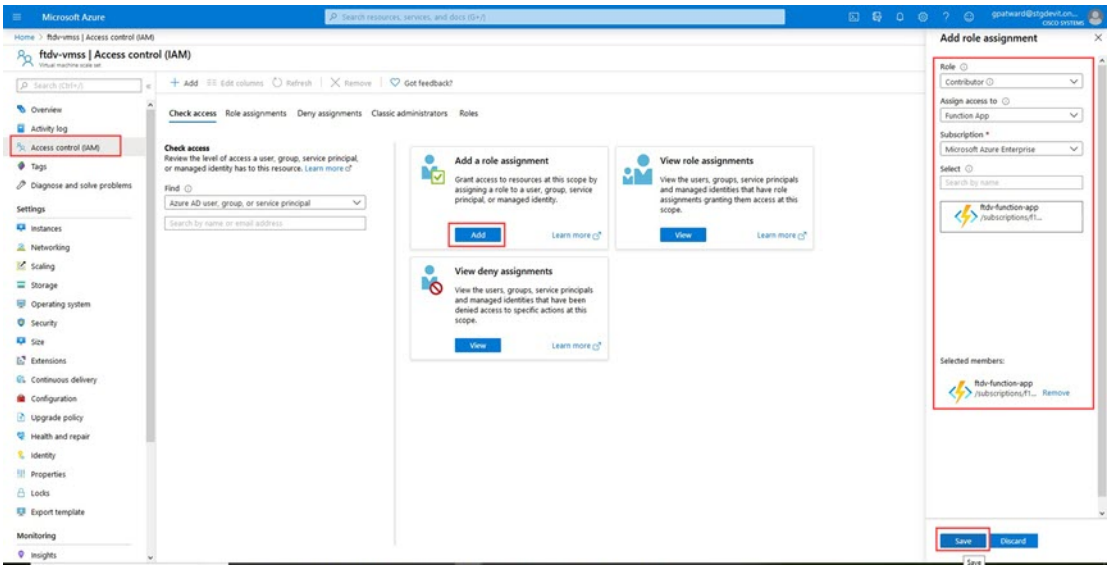
步骤 3 单击**添加**以添加角色分配

步骤 4 从**添加角色分配**下拉列表中选择**参与者**。

步骤 5 从**分配访问**下拉列表中选择**函数应用**。

步骤 6 选择 FTDv 函数应用。

图 ***20: AIM*** 角色分配



步骤 7 单击**保存**。

注释 此外，还应确认尚未启动任何 FTDv 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 FTDv 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功能的编排器。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 编排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 FTDv 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"
                     }
```

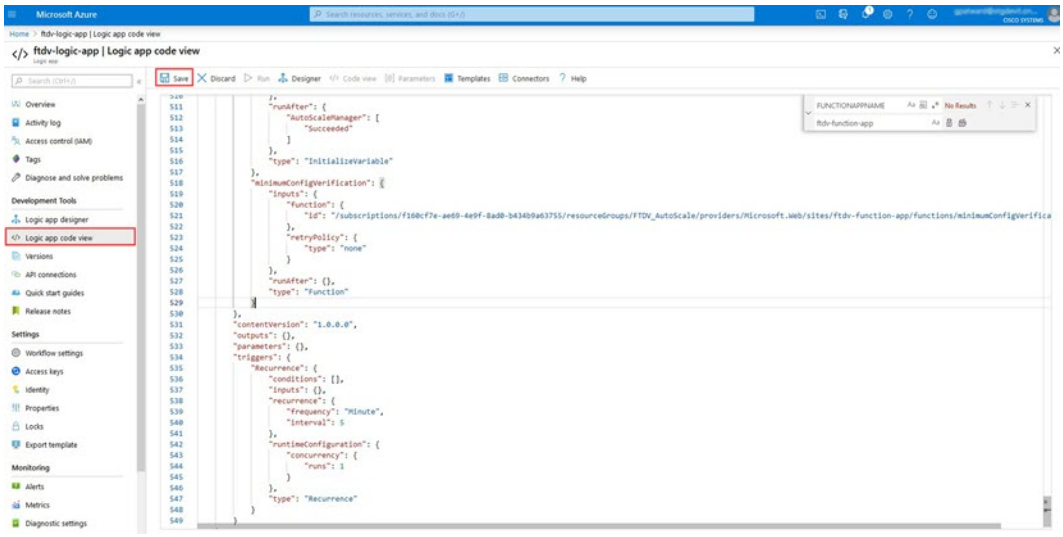
f) （可选）编辑冷却时间，或保留默认值 (10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
"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。

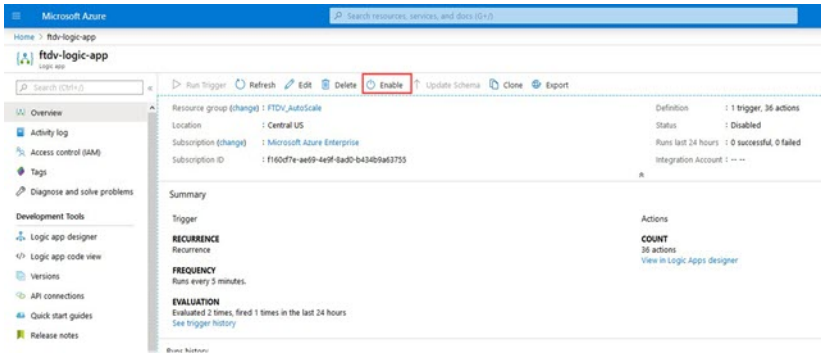
步骤 2 转至**逻辑应用代码视图**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后单击**保存**。

图 *21:* 逻辑应用代码视图



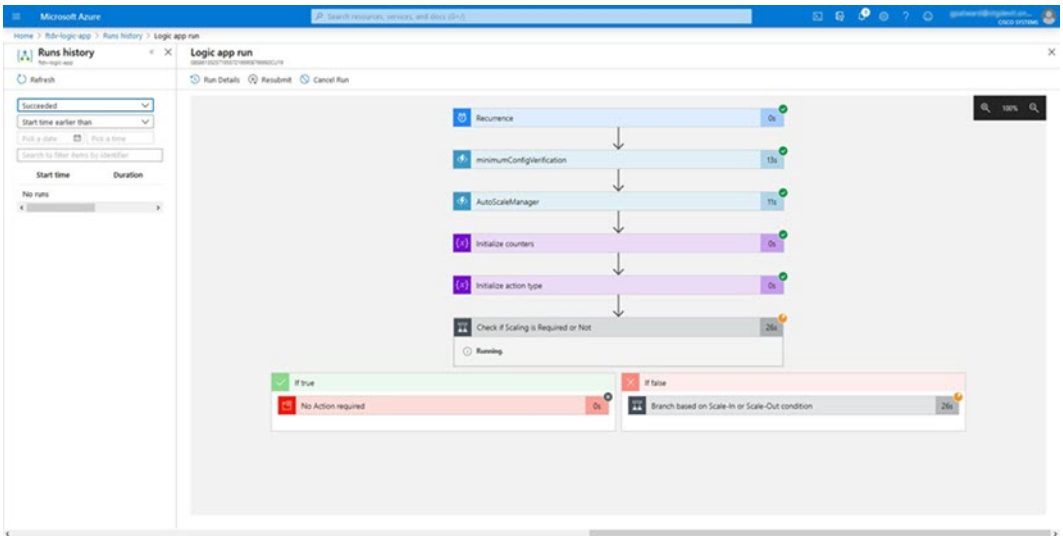
步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请单击**启用**。

图 *22:* 启用逻辑应用



步骤 4 启用后，任务就会开始运行。单击“正在运行”状态可查看活动。

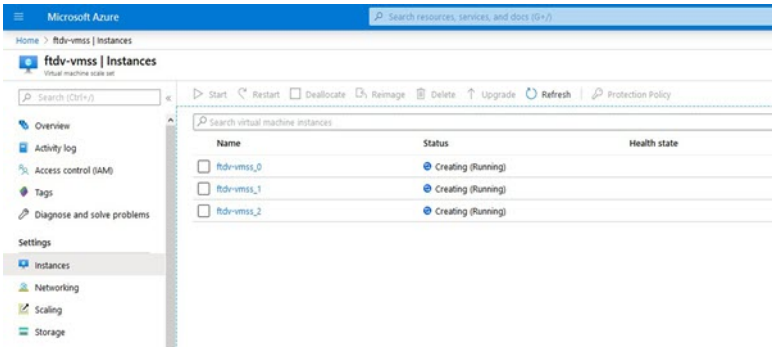
图 *23:* 逻辑应用运行状态



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 FTDv 实例。

图 *24:* 正在运行的 *FTDv* 实例



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 FTDv 实例。

升级 FTDv

FTDv 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 FTDv。

注释 您可以使用任何 REST 客户端来升级 FTDv。以下是一个简单的示例。

开始之前

- 获取市场中提供的新 FTDv 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

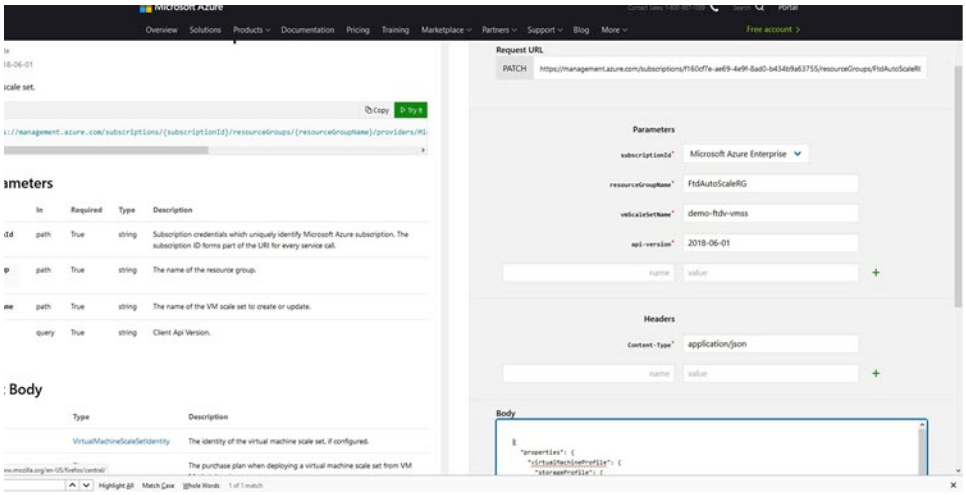
过程

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 *25:* 升级 *FTDv*



步骤 3 在**主体**部分输入包含新 FTD 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 FTDv 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 FTDv 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 FTDv 实例。要执行此操作，请单击 VMSS 中的**升级**按钮。它将重新启动并升级选定的FTDv实例。您必须手动重新注册并重新配置这些升级后的FTD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 FTDv Auto 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（版本 6.6 及更低版本）。CPU 指标是从 Azure 收集的。
- CPU、内存（版本 6.7+）。内存指标是从 FMC 收集的。

外向扩展逻辑

- **POLICY-1**：当**任何** FTDv 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 FTDv 的平均 CPU 或内存利用率。
- **POLICY-2**：当**所有** FTDv 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 FTDv 设备的平均 CPU 或内存利用率。

内向扩展逻辑

- 如果**所有** FTDv 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 FTDv 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 FTDv。

说明

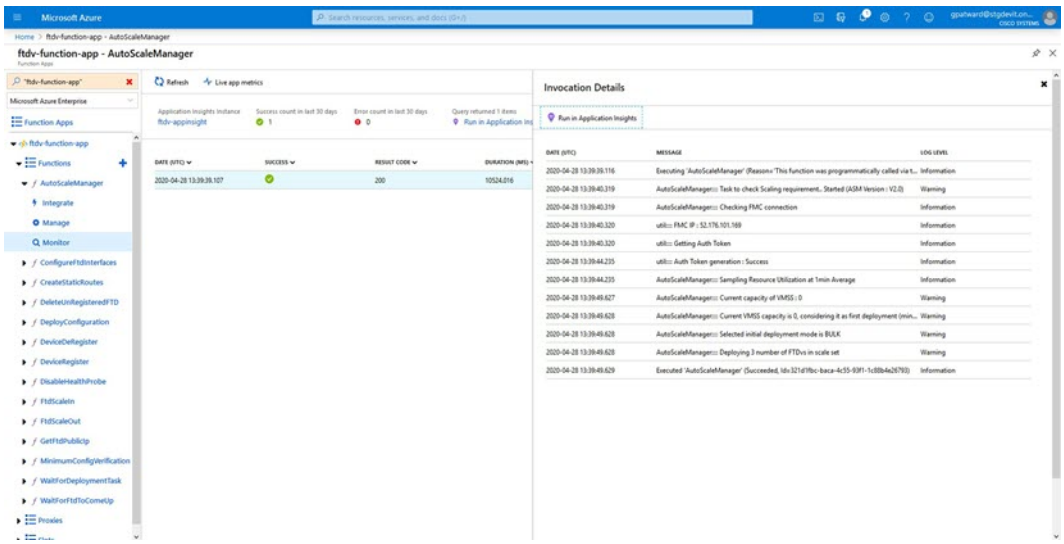
- 内向扩展/外向扩展以 1 为单位发生（即一次仅内向扩展/外向扩展 1 个 FTDv）。
- 从 FMC 收到的内存消耗指标不是按时间计算的平均值，而是瞬时快照/示例值。因此，在做出扩展决定时不能单独考虑内存指标。在部署过程中，您无法选择使用仅内存指标。

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。

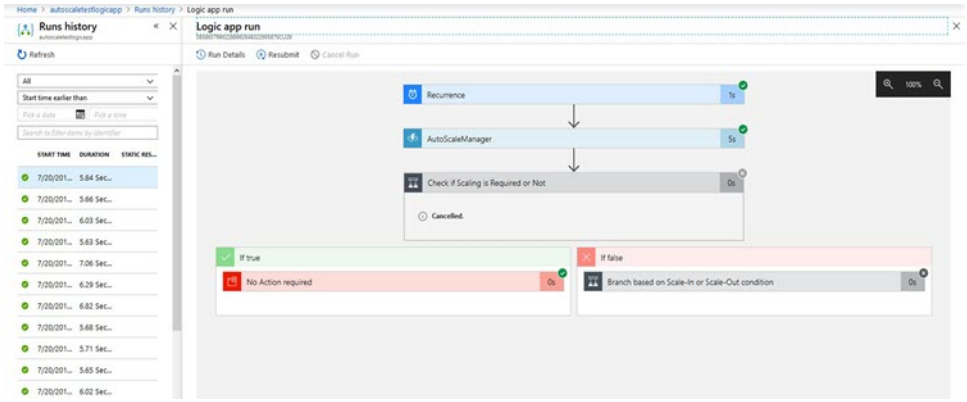
- 可以查看个别 Azure 函数的日志。

图 *26: 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 *27:* 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 FTDv 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 FTDv 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。
- FMC 管理是必需的。不支持 FDM。
- FMC 应具有公共 IP 地址。
- FTDv 管理接口配置为具有公共 IP 地址。
- 仅支持 IPv4。
- FTDv 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 FTDv 实例。您只能使用 FMC 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 FTD/FMC 凭证）。您可以使用 *Azure Key Vault* 服务保护敏感数据。

Auto Scale 故障排除

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

- 连接到 FMC 失败：检查 FMC IP/凭证；检查 FMC 是否故障/无法访问。
- 无法通过 SSH 连接到 FTDv：检查是否通过模板将复杂密码传递到 FTDv；检查安全组是否允许 SSH 连接。
- 负载平衡器运行状况检查失败：检查 FTDv 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、FTDv 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。
- FTDv 无法注册到 FMC：检查 FMC 容量以容纳新的 FTDv 设备；检查许可；检查 FTDv 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 FTDv 设备上检查 SSH 访问；检查 FMC 中是否有任何设备注册问题；检查 Azure VMSS 中 FTDv 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。

附录 - 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）

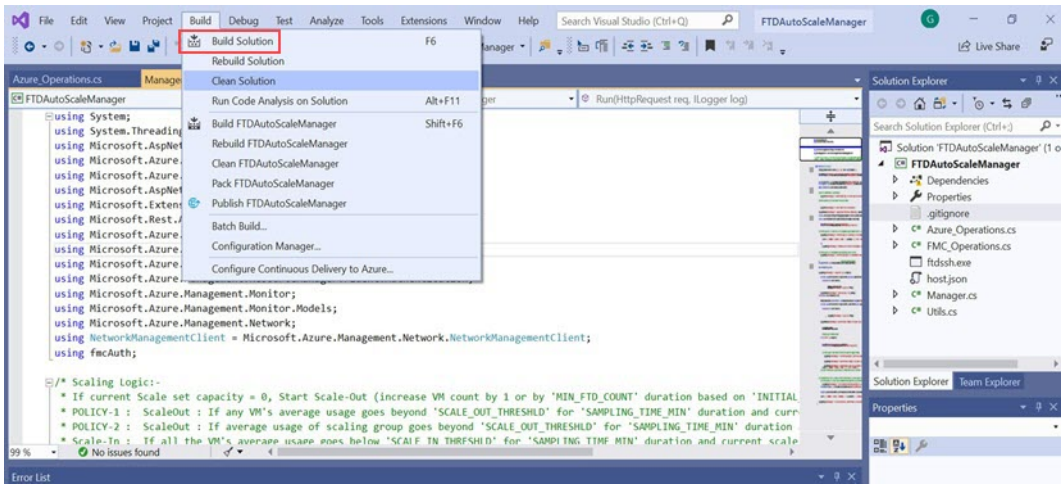
注释 Azure 函数是使用 C# 编写的。

- “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 *28: Visual Studio* 内部版本



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

图 *29:* 生成 ***ASM_Function.zip***