在 Microsoft Azure 云上部署虚拟 Firepower 管理中心

您可以在 Microsoft Azure 云上部署 Firepower Management Center Virtual (FMCv)。

重要事项

在 Microsoft Azure 上，从 Cisco Firepower 6.4 及更高版本软件开始支持运行 FMCv。

- 关于 FMCv 部署和 Azure， 第 1 页
- 前提条件和系统要求， 第 2 页
- 准则和限制， 第 3 页
- 在部署期间创建的资源， 第 4 页
- 部署虚拟 Firepower 管理中心， 第 5 页
- 验证虚拟 Firepower 管理中心虚拟部署， 第 8 页
- 监控和故障排除， 第 10 页
- Microsoft Azure 云上的 FMCv 历史， 第 11 页

关于 FMCv 部署和 Azure

您可以使用 Azure 市场中提供的解决方案模板，在 Microsoft Azure 中部署 Firepower Management Center Virtual (FMCv)。使用 Azure 门户部署 FMCv 时，您可以使用现有的空资源组和存储帐户（或创建新帐户）。解决方案模板会引导您完成一组配置参数，这些参数可提供您 FMCv 的初始设置，允许您在首次 FMCv 启动后登录到 web 界面。

FMCv 需要 28 GB RAM 用于升级 (6.6.0+)

FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。

重要事项 从版本 6.6.0 开始，基于云的 FMCv 部署（AWS、Azure）低内存实例类型已被完全弃用。您不能使用它们建新的 FMCv 实例，即使是早期 Firepower 版本也不例外。您可以继续运行现有实例。请参阅表 1: 不同版本受 Azure 支持的实例FMCv，第 2 页。

由于此内存检查，我们将无法在支持的平台上支持较低内存实例。

Azure 上的 FMCv 必须使用资源管理器部署模式在虚拟网络 (VNet) 中加以部署。您可以在标准 Azure 公有云环境中部署 FMCv。FMCv Azure 市场支持自带许可证（BYOL）模型。

下表汇总了 FMCv 支持的 Azure 实例类型、版本 6.5.x 及更早版本支持的 Azure 实例类型，以及版本 6.6.0+ 支持的 Azure 实例类型。

表 *1:* 不同版本受 *Azure* 支持的实例*FMCv*

平台	版本 6.6.0+	版本 6.5.x 及更早版本*
FMCv	Standard_D4_v2：8 个 vCPU，28 GB	Standard_D3_v2：4 个 vCPU，14 GB
	-	Standard_D4_v2：8 个 vCPU，28 GB
	*请注意，FMCv 自版本 6.6.0 发布后将不再支持 Standard_D3_v2 实例。从版本 6.6.0 开始，您必须使用至少具有 28 GB RAM 的实例部署 FMCv（任何版本）。请参阅调整实例大小，第 2 页。	

已弃用的实例

您可以继续使用 Standard_D3_v2 运行当前版本 6.5.x 及更早版本的 FMCv 部署，但不能使用此实例启动新的 FMCv 部署（任何版本）。

调整实例大小

由于从任何早期版本的 FMCv（6.2.x、6.3.x、6.4.x 和 6.5.x）升级到版本 6.6.0 的升级路径包括 28 GB RAM 内存检查，因此，如果您使用 Standard_D3_v2，则需要将实例类型大小调整为 Standard_D4_v2（请参阅表 1: 不同版本受 Azure 支持的实例FMCv，第 2 页）。

您可以使用 Azure 门户或 PowerShell 调整实例的大小。如果虚拟机当前正在运行，更改其大小将导致其重新启动。停止虚拟机可能会显示额外的大小。

有关如何调整实例大小的说明，请参阅 Azure 文档《调整 Windows 虚拟机大小》(https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm)。

前提条件和系统要求

FMCv对 Microsoft Azure 的支持是 Firepower 版本 6.4.0 的新功能。有关 Firepower Management Center Virtual 与 Firepower 系统的兼容性，请参阅《Cisco Firepower 威胁防御虚拟兼容性》。

FMCv在 Azure 中部署之前，请验证以下内容：

- 在 Azure.com 上创建帐户。

  在 Microsoft Azure 上创建帐户后，您可以登录该市场，搜索思科 Firepower Management Center Virtual 市场，然后选择“Cisco Firepower Management Center (FMCv) BYOL”产品。

- 思科智能账户。可以在思科软件中心 https://software.cisco.com/ 创建一个帐户。

准则和限制

支持的功能

- 支持的 Azure 实例
  - 标准 D3_v2-4 Vcpu，14GB memory，250GB 磁盘大小
  - 标准 D4_v2—8 vCPU，28GB memory，400GB 磁盘大小
- 公共 IP 寻址
  - 为管理 0/0 分配了一个公共 IP 地址。

许可

在FMCv Azure 公共市场中，支持自带许可证 (BYOL) 模型。对于 FMCv，这是平台许可证，而非功能许可证。您购买的虚拟许可证版本将确定您可以通过 Firepower Management Center Virtual管理的设备数量。例如，您可以购买能够管理两台、10 台或 25 台设备的许可证。

- 许可模式：
  - 仅智能许可证

有关许可的详细信息，请参阅《*Firepower* 管理中心配置指南》中的Firepower 系统许可，以了解有关如何管理许可证的详细信息；有关Firepower 系统功能许可证的概述（包括有用的链接），请参阅 Cisco Firepower 系统功能许可证。

系统关闭和重新启动

请勿在“Azure 虚拟机概述”(Azure Virtual machine overview) 页面上使用**重启 (Restart)** 和**停止 (Stop)** 控件打开 FMCv 虚拟机。这些不是正常关机机制，可能导致数据库损坏。

使用 FMCv 的网络界面中可用的**系统 (System)** > **配置 (Configuration)** 选项关闭或重新启动虚拟设备。

从 FMCv 命令行界面使用 `shutdown` 和 `restart` 命令关闭或重新启动设备。

不支持的功能

- 许可模式：

- 现收现付 (PAYG) 许可。
- 永久许可证预留 (PLR)。

- 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 FMCv 虚拟机。
- 高可用性（活动/备用）
- 虚拟机导入/导出

在部署期间创建的资源

在 Azure 中部署 FMCv 时，会创建以下资源：

- 具有单个 FMCv 接口的 Cisco 虚拟机 (VM)（需要新的虚拟网络或现有含 1 个子网的虚拟网络）。
- 一个资源组。

  FMCv 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。
- 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。

  该安全组包括允许 SSH（TCP 端口 22）和 Firepower 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）。

  该公共 IP 地址与虚拟机 Nic0 相关联，后者映射到管理接口。

  注释 您可以创建新的公共 IP 地址，或者选择现有 IP 地址。您也可以选择**无 (NONE)**。如果没有公共 IP 地址，则与 FMCv 之间的任何通信均必须源自 Azure 虚拟网络内
- 该子网的路由表（如果已存在，则相应更新）。
- 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）。

重要事项 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）。

部署虚拟 Firepower 管理中心

您可以使用模板在 Azure 中部署 Firepower Management Center 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， FMCv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，第 5 页。
- **GitHub 存储库中的 ARM 模板** — 除了基于市场的部署，Cisco 还在 GitHub 存储库中提供 Azure Resource Manager (ARM) 模板，以简化在 Azure 上部署 FMCv 的过程。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），您可以在单次协调操作中为 FMCv 部署并调配所有资源。

从 Azure 市场使用解决方案模板部署

使用 Azure Firepower Management Center Virtual市场FMCv中提供的解决方案模板，从 Azure 门户部署。以下程序概要列出在 Microsoft Azure 环境中设置 FMCv 威胁防御虚拟的步骤。如需了解详细的 Azure 设置步骤，请参阅《Azure 入门》。

在 Azure 中部署 FMCv 时，会自动生成各种配置，例如资源、公共 IP 地址和路由表。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。

步骤 1 使用您的 Microsoft 帐户凭证登录 Azure 门户（https://portal.azure.com）。

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 单击**创建资源 (Create a Resource)**。

步骤 3 在市场中搜索“Cisco Firepower Management Center (FMCv)”，选择产品，然后单击**创建 (Create)**。

步骤 4 配置 **基本**设置：

a) 在 **Azure 中的 FMC VM**字段中，输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

注意 确保不要使用现有的名称，否则部署将失败。

b) （可选）从下拉列表中选择 **FMC 软件版本 (FMC Software Version)**。

这应默认为最新的可用版本。

c) 在**主要帐户用户名** ）字段中，输入 Azure 帐户管理员的用户名。

名称“admin”是 Azure 中的预留名称，不能使用。

注意　此处输入的用户名用于Azure帐户，而不是FMCv管理员访问权限。请勿使用此用户名登录FMCv。

d) 选择身份验证类型：**密码 (Password)**或 **SSH 公钥 (SSH public key)**。

如果您选择**密码 (Password)**，请输入密码并确认。密码必须介于 12 到 72 个字符之间，并且必须包含以下 3 项：1 个小写字符、1 个大写字符、1 个数字和 1 个非“\”或“-”的特殊字符。

如果选择 **SSH 公钥 (SSH public key)**，请指定远程对等体的 RSA 公共密钥。

e) 输入 FMCv 的 **FMC 主机名**。

f) 输入**管理密码**。

这是您以管理员身份登录到 FMCv 的 Web 界面时使用的密码。 FMCv

g) 选择**订用 (Subscription)** 类型。

通常仅列出一个选项。

h) 创建**资源组**。

FMCv 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 FMCv 附加到另一个资源组的现有虚拟网络。

i) 选择地理**位置 (Location)**。

对于此部署中使用的所有资源，应使用相同的位置。FMCv、网络、存储帐户等均应使用相同的位置。

j) 单击**确定 (OK)**。

步骤 5 接下来，完成 **Cisco FMCv 设置**下的初始配置：

a) 确认所选的**虚拟机大小 (Virtual machine size)**，或单击**更改大小 (Change size)** 链接以查看 VM 大小选项。单击**选择 (Select)** 以确认。

仅显示受支持的虚拟机大小。

b) 配置**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。

- 输入存储帐户的**名称 (Name)**，然后单击**确定 (OK)**。存储帐户名称只能包含小写字母和数字。它不能包含特殊字符。
- 在此版本中， FMCv 仅支持通用的标准性能存储。

c) 配置**公有 IP 地址**。您可以使用现有 IP 地址，也可以创建新 IP 地址。

- 单击**新建 (Create new)** 对话框，以创建一个新的公共IP地址。在**名称 (Name)** 字段中输入IP地址的标签，选择 SKU 选项的**标准 (Standard)**，然后单击**确定 (OK)**。

  注释　Azure会创建一个动态公共IP地址，无论此步骤中选择的是动态还是静态。当虚拟机停止和重启时，该公共IP可能会变化。如果您更喜欢固定的IP地址，可以在部署后编辑公共IP地址，将其从动态地址更改为静态地址。

- 如果您不想将公共 IP 地址分配给 FMCv，可以选择**无 (NONE)**。如果没有公共 IP 地址，则与 FMCv 之间的任何通信均必须源自 Azure 虚拟网络内。

d) 添加与公共 IP 标签匹配的 **DNS 标签**。

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

e) 选择现有的**虚拟网络 (Virtual network)**，或创建新的虚拟网络，然后单击**确定 (OK)**。

f) 配置 FMCv 的管理子网。

定义**管理子网名称**并查看**管理子网前缀**。建议的子网名称为“management”。

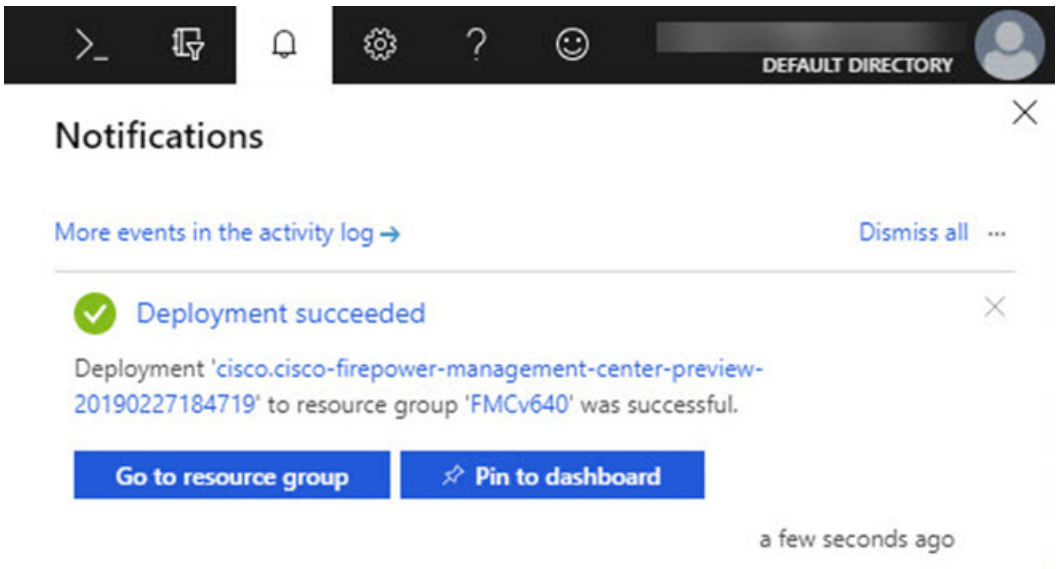
g) 单击**确定 (OK)**。

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，然后单击**创建 (Create)**。

步骤 8 选择门户顶部的**通知 (Notifications)**（电铃图标）以查看部署的状态。

图 *1: Azure* 通知



在这里，您可以单击部署以查看更多详细信息，或在部署成功后转至资源组。FMCv 可用前的总时间约为 30 分钟。部署时间在 Azure 中有所不同。请等候，直到 Azure 报告 FMCv 虚拟机正在运行。

步骤 9 （可选）Azure提供了许多工具来帮助您监控虚拟机的状态，包括**引导诊断**和**串行控制台**。这些工具允许您在启动时查看虚拟机的状态。

a) 在左侧菜单中，选择**虚拟机 (Virtual machines)**。

b) 在列表FMCv中选择您的 VM。系统将打开虚拟机的“概述”页面。

c) 向下滚动到“**支持 + 故障排除 (Support + troubleshooting)**”部分，选择**引导诊断 (Boot diagnostics)** 或**串行控制台 (Serial console)**。系统将打开一个新窗格，其中包含引导诊断**屏幕截图**和**串行日志**或基于文本的**串行控制台**，并开始连接。

如果在启动诊断 FMCv 或串行控制台上看到登录提示，则会确认 Web 界面的就绪状态。

示例：

```
Cisco Firepower Management Center for Azure v6.4.0 (build 44)
FMCv64East login:
```

下一步做什么

- 确认 FMCv 部署已经成功。Azure 控制面板在“资源组”下列出新 FMCv VM，以及所有相关资源（存储、网络、路由表等）。

验证虚拟 Firepower 管理中心虚拟部署

创建 FMCv VM 后，Microsoft Azure 控制板将在资源组下列出新的 FMCv VM。此外，还会创建并列出相应的存储帐户和网络资源。控制板提供您的 Azure 资产的统一视图，并提供对运行状况和性能的简单的评估概览 FMCv。

开始之前

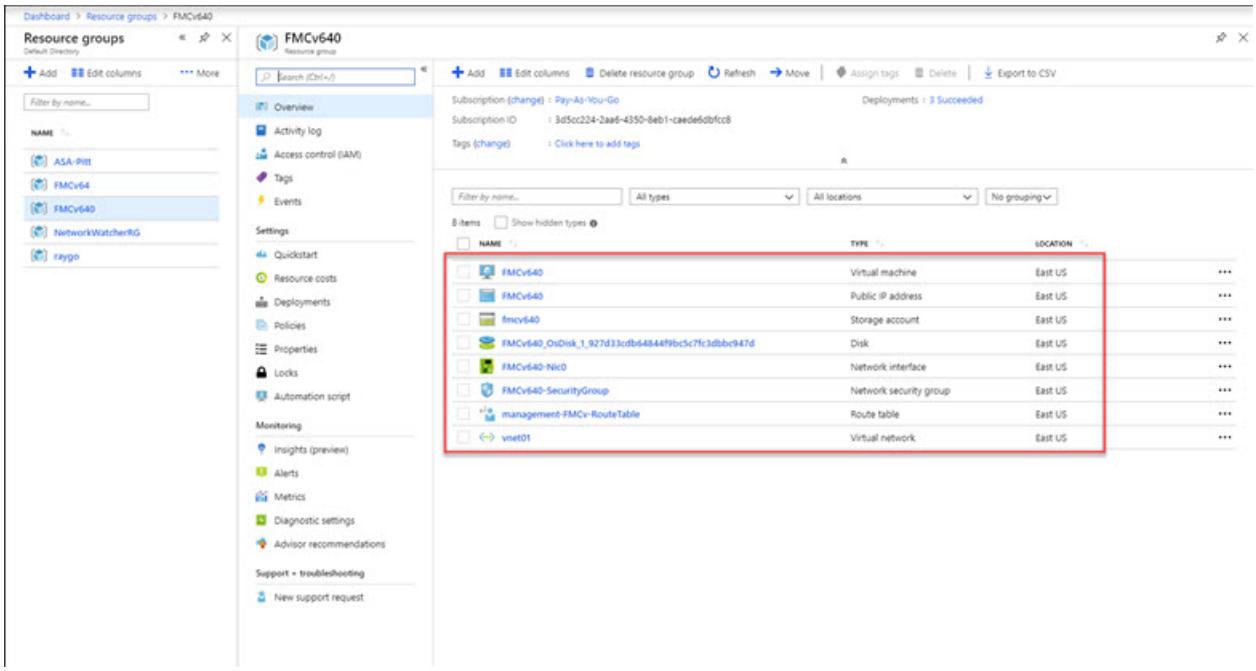
FMCv VM 将自动启动。在部署过程中，状态列为“正在创建”，而 Azure 创建虚拟机，然后在部署完成后，状态将更改为“正在运行”。

注释 请记住，部署时间在 Azure 中有所不同，FMCv 可使用所需的总时间大约为 30 分钟，即使 Azure 控制板将 FMCv VM 的状态显示为“正在运行”。

步骤 1 要在部署完成后查看 FMCv 资源组及其资源，请从左侧菜单窗格中单击**资源组 (Resource groups)** 以访问“资源组”(Resource groups) 页面。

下图显示了 Microsoft Azure 门户中的“资源组”页面的示例。请注意 FMCv VM 及其相应的资源（存储帐户、网络资源等）。

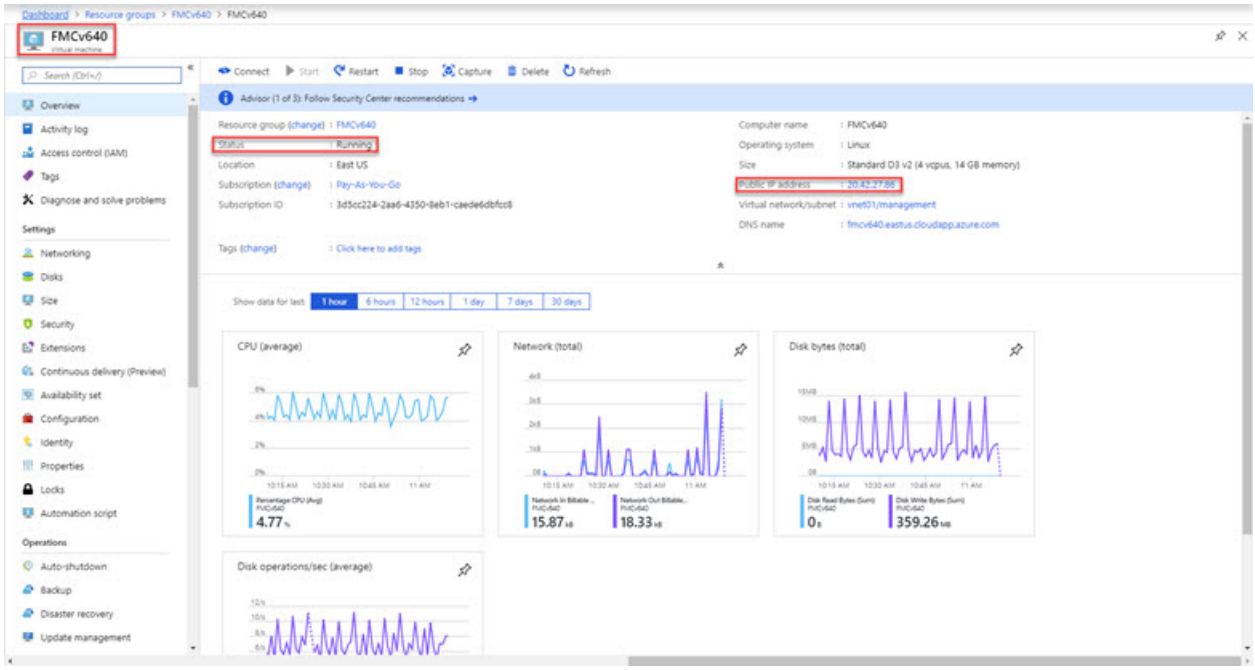
图 *2: Azure FMCv* 资源组页面



步骤 2 要查看与资源组关联的 FMCv VM 的详细信息，请单击 FMCv VM 的名称。

下图显示了与 FMCv VM 关联的**虚拟机 (Virtual machine)** 概述页面的示例。您可以从“资源组”(Resources groups) 页面访问此概述。

图 *3:* 虚拟机概述



观察状态是否为“正在运行”。您可以从 Microsoft Azure 门户中的**虚拟机 (Virtual machine)** 页面停止、启动、重新启动和删除 FMCv VM。请注意，这些控制不是 FMCv 的正常关闭机制；有关正常关闭的信息，请参阅准则和限制，第 3 页。

步骤 3 在**虚拟机 (Virtual machine)** 页面中，查找分配给的 FMCv 的**公共 IP 地址**。

注释　　您可以将鼠标悬停在 IP 地址上，然后选择**单击复制 (Click to copy)** 以复制 IP 地址。

步骤 4 通过浏览器访问 **https://***public_ip/*，其中 *public_ip* 是在部署 VM 时分配给 FMCv 管理接口的 IP 地址。

随即显示登录页面。

步骤 5 使用用户名 **admin** 以及部署 VM 时指定的管理员账户密码登录设备。

下一步做什么

- 我们建议您完成一些管理任务，使部署更易于管理，例如创建用户和查看运行状况和系统策略。有关如何开始的概述，请参阅虚拟 Firepower 管理中心初始管理和配置。
- 您还应检查设备注册和许可要求。
- 有关如何开始配置 Firepower 系统的信息，请参阅您的版本完整《Firepower 管理中心配置指南》。

监控和故障排除

本部分包括 Micosoft Azure 中部署的 Firepower Management Center Virtual 设备的常规监控和故障排除指南。监控和故障排除可以与 Azure 中的 VM 部署或 FMCv 设备本身相关。

Azure 监控的虚拟机部署

Azure 提供**支持 + 故障排除**菜单下的许多工具，提供对工具和资源的快速访问，以帮助您诊断和解决问题并获得更多帮助。值得关注的两项包括：

- **引导程序诊断** — 允许您在启动时查看FMCv虚拟机的状态。引导诊断程序从虚拟机和屏幕截图收集串行日志信息。这可以帮助您诊断任何启动问题。
- **串联控制台** — Azure 门户中的 VM 串行控制台支持访问基于文本的控制台。此串行连接连接到虚拟机的 COM1 串行端口，通过分配给的公共 IP 地址，提供FMCv对的命令行界面的串行和 SSH 访问FMCv。

FMCv 监控与日志记录

故障排除和常规日志记录操作遵循与当前 FMC 和 FMCv 型号相同的程序。有关您的版本，请参阅《*Firepower* 管理中心配置指南》中的系统监控和故障排除部分。

此外，Microsoft Azure Linux 代理 (waagent) 管理与 Azure 交换矩阵控制器的 Linux 调配和 VM 交互。因此，以下是故障排除的重要日志：

- **/var/log/waagent.log** — 此日志将包含与 Azure FMC 调配相关的任何错误。
- **/var/log/firstboot.S07install_waagent** — 此日志将包含 waagent 安装中的任何错误。

Azure 调配失败

使用 Azure Marketplace 解决方案模板调配错误不常见。但是，如果您遇到调配错误，请记住以下要点：

- Azure 为虚拟机调配 waagent 时20分钟超时，此时它会重新启动。
- FMC如果由于任何原因而无法进行调配，则20分钟计时器往往会在FMC数据库初始化过程中结束，从而可能导致部署失败。
- 如果在FMC 20 分钟内无法调配，我们建议您重新开始。
- 您可以参考*/var/log/waagent.log*了解故障排除信息。
- 如果在串行控制台中看到 HTTP 连接错误，则表明 waagent 无法与交换矩阵通信。您应在重新部署时检查网络设置。

Microsoft Azure 云上的 FMCv 历史

功能名称	版本	功能信息
在 Microsoft Azure 云上部署虚拟 Firepower 管理中心 (FMCv)。	6.4.0	初始支持。