在高信任环境中在Azure中部署自动缩放的FTDv

目录

简介

本文档介绍如何在高信任环境中在Azure中部署自动扩展的思科Firepower威胁防御虚拟(FTDv)。

先决条件

要求

Cisco 建议您了解以下主题：

- NGFW和Firepower管理中心应通过私有IP通信
- 外部负载均衡器不应具有公有IP。
- 功能的应用应能与私有IP通信

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Azure
- Firepower 管理中心
- 虚拟机扩展集

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FTDv将思科的Firepower下一代防火墙功能引入虚拟化环境，使一致的安全策略能够跟踪物理、虚拟和云环境以及云之间的工作负载。

由于这些部署在虚拟化环境中可用，目前NGFW不支持HA。因此，为了提供高可用性解决方案，思科下一代防火墙(NGFW)利用Azure的本地功能(如可用性集和虚拟机扩展集(VMSS))，使NGFW高度可用，并满足日益增长的流量需求。

本文档重点介绍如何根据NGFW按需扩展或横向扩展的不同参数将思科NGFW配置为AutoScale。这包括客户需要使用Firepower管理中心(FMC)的使用案例，该中心可在托管数据中心使用，需要集中管理所有NGFW，而且客户不希望FMC和FTD通过公共IP进行通信以管理流量。

在深入了解配置和设计考虑事项之前，以下是应该在Azure中充分理解的几个概念：

- **可用区**: 可用区是一种高可用性产品，可保护您的应用和数据免受数据中心故障的影响。可用区是Azure区域内的唯一物理位置。每个区域由一个或多个数据中心组成，这些数据中心配备独立的电源、冷却和网络。

- **VNET**: Azure虚拟网络(VNet)是Azure中专用网络的基本构建块。VNet使Azure虚拟机(VM)等多种类型的Azure资源能够安全地彼此通信、互联网和本地网络。VNet类似于您在自己的数据中心中运行的传统网络，但它带来了Azure基础设施的额外优势，如扩展、可用性和隔离。默认情况下，VNET中的每个子网可以相互访问，但不同VNET中的子网不能相同。

- **可用性集**: 可用性集是另一个提供虚拟机冗余和可用性的数据中心配置。数据中心内的此配置可确保在计划内或计划外维护事件期间，至少有一个虚拟机可用并符合99.95%的Azure SLA。

- **VMSS**: Azure虚拟机扩展集允许您创建和管理一组负载平衡的虚拟机。VM实例的数量可以根据需求或定义的计划自动增加或减少。扩展集可为您的应用提供高可用性，并允许您集中管理、配置和更新大量虚拟机。借助虚拟机扩展集，您可以为计算、大数据和容器工作负载等领域构建大规模服务。

- **函数应用**：Azure函数是可按需提供的云服务，可提供运行应用程序所需的不断更新的基础设施和资源。你将注意力集中在对你最重要的代码片段上，而Azure函数则处理其余代码。您可以使用Azure函数构建Web API、响应数据库更改、处理IoT流、管理消息队列等。在此自动缩放解决方案中，Azure函数是向FMC发出的各种API请求，用于创建对象、注册/取消注册FTDv、检查参数等。

- **逻辑应**用：Azure逻辑应用是一项云服务，可帮助您在需要跨企业或组织集成应用、数据、系统和服务时安排、自动化和协调任务、业务流程和工作流。Logic Apps可简化您为应用集成、数据集成、系统集成、企业应用集成(EAI)和企业到企业(B2B)通信（无论是在云中还是在内部部署，还是同时在两者中）设计和构建可扩展解决方案的方式。此解决方案提供要执行的功能的逻辑排序，以便自动缩放解决方案的功能正常运行。

目前，适用于NGFW的AutoScale解决方案不提供与VNet本地的私有IP通信的管理计划，并且需要公有IP来交换Firepower管理中心和NGFW之间的通信。

本文旨在解决此问题，直到验证的解决方案可用于Firepower管理中心和通过私有IP的NGFW通信。

配置

为了创建自动扩展NGFW解决方案，请使用以下配置指南：

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/azure/ftdv-azure-gsg/ftdv-azure-autoscale.html#Cisco_Concept.dita_c0b3cf0d-9690-4342-8cba-e66730e70c47

通过几项修改，以便能够解决以下使用案例：

- Function的应用应能与客户的内部IP网段通信
- 负载均衡器不应具有公共IP
- NGFW和FMC之间的管理流量应通过专用IP网段交换。

要创建AutoScaled NGFW解决方案，在上述使用案例中，您需要在思科官方指南中提及的步骤中修改这些使用案例：

1. Azure ARM模板

ARM模板用于在Azure中启用自动化。思科已提供经过验证的ARM模板，可用于创建自动扩展解决方案。但是，此ARM模板可在Public Github https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template上获取，它创建了一个功能应用，该功能应用无法与客户的内部网络通信，尽管它们可以通过快速路由访问。因此，我们需要稍作修改，以便Function App现在可以使用高级模式而不是消费模式。因此，所需的ARM模板可在https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git上找到

2. 功能APP

函数应用是一组Azure函数。基本功能包括：

- 定期通信/探测Azure指标。
- 监控FTDv负载并触发Scale In/Scale-Out操作。
- 向FMC注册新的FTDv。
- 通过FMC配置新FTDv。
- 从FMC注销（删除）扩展的FTDv。

如要求中所述，为按需NGFW创建或删除而创建的各种功能均基于NGFW的公共IP完成。因此，我们需要调整C#代码以获取私有IP而不是公有IP。调整代码后，可在https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git上找到用于创建功能应用的zip文件

名称为ASM_Function.zip。这使Functions应用无需公共IP即可与内部资源通信。

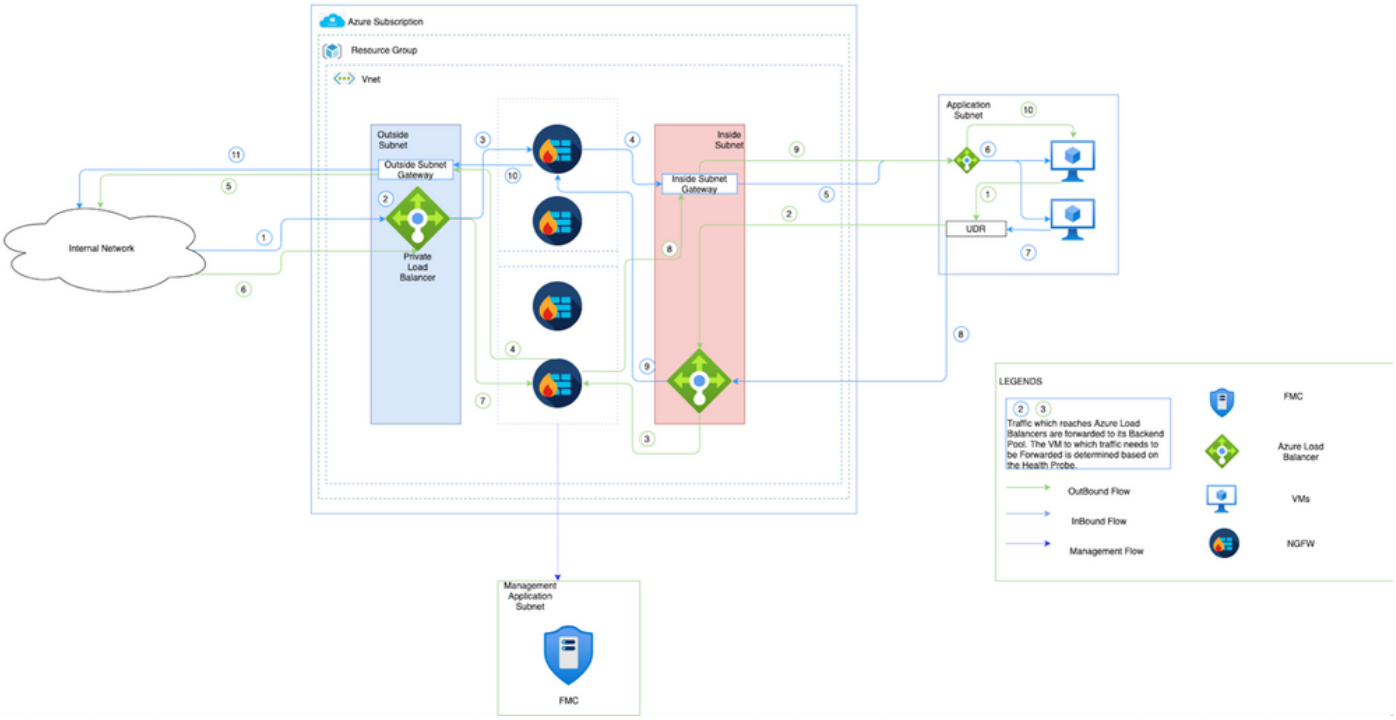
3. 逻辑应用

自动缩放逻辑应用是一个工作流，即序列中步骤的集合。Azure函数是独立的实体，无法相互通信。此协调器对这些功能的执行进行排序，并在它们之间交换信息。

- 逻辑应用用于在自动缩放Azure功能之间协调和传递信息。
- 每个步骤都表示一个Auto Scale Azure函数或内置标准逻辑。
- 逻辑应用以JSON文件形式提供。
- 逻辑应用可通过GUI或JSON文件进行自定义。

> **注意**：应仔细修改https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git上提供的逻辑应用详细信息，并且必须用部署详细信息、FUNSAPP名称、资源组名称、订用ID替换以下项目。

网络图



此图显示入站和出站流量如何通过NGFW在Azure环境内流动。

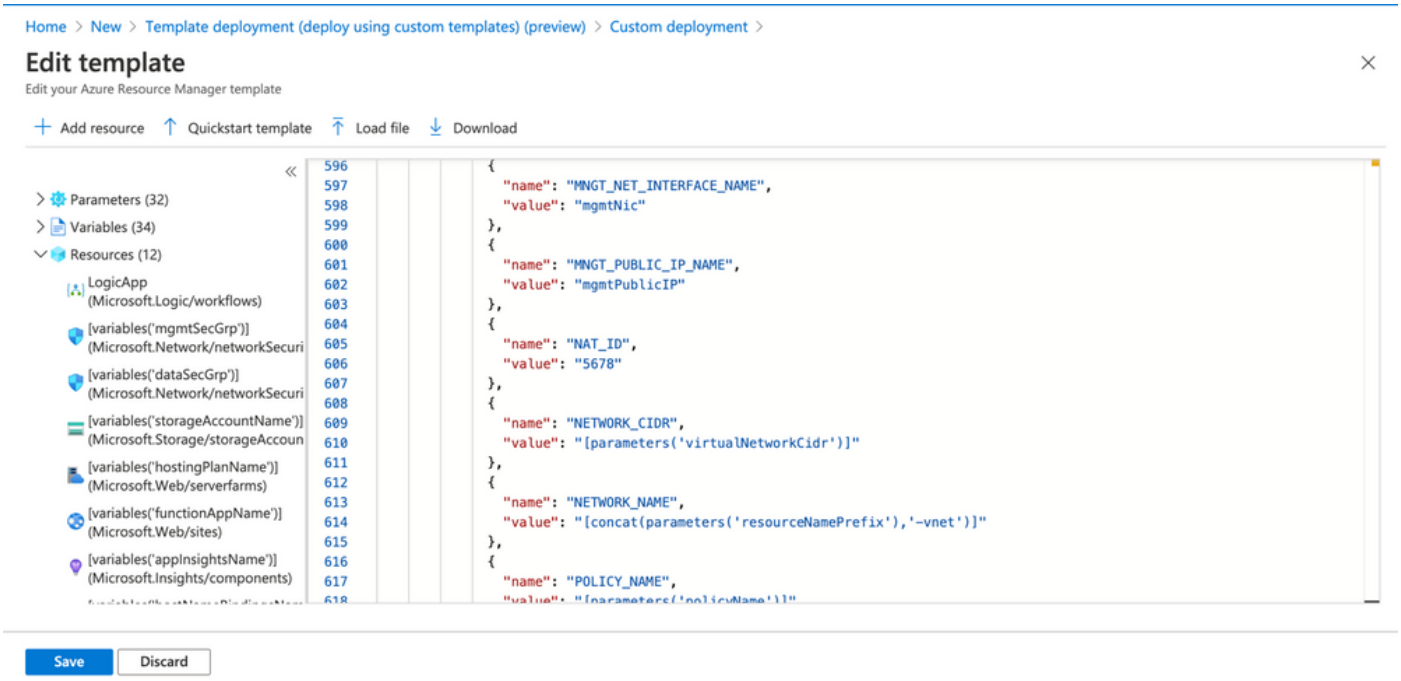
配置

现在创建自动扩展解决方案所需的各种组件。

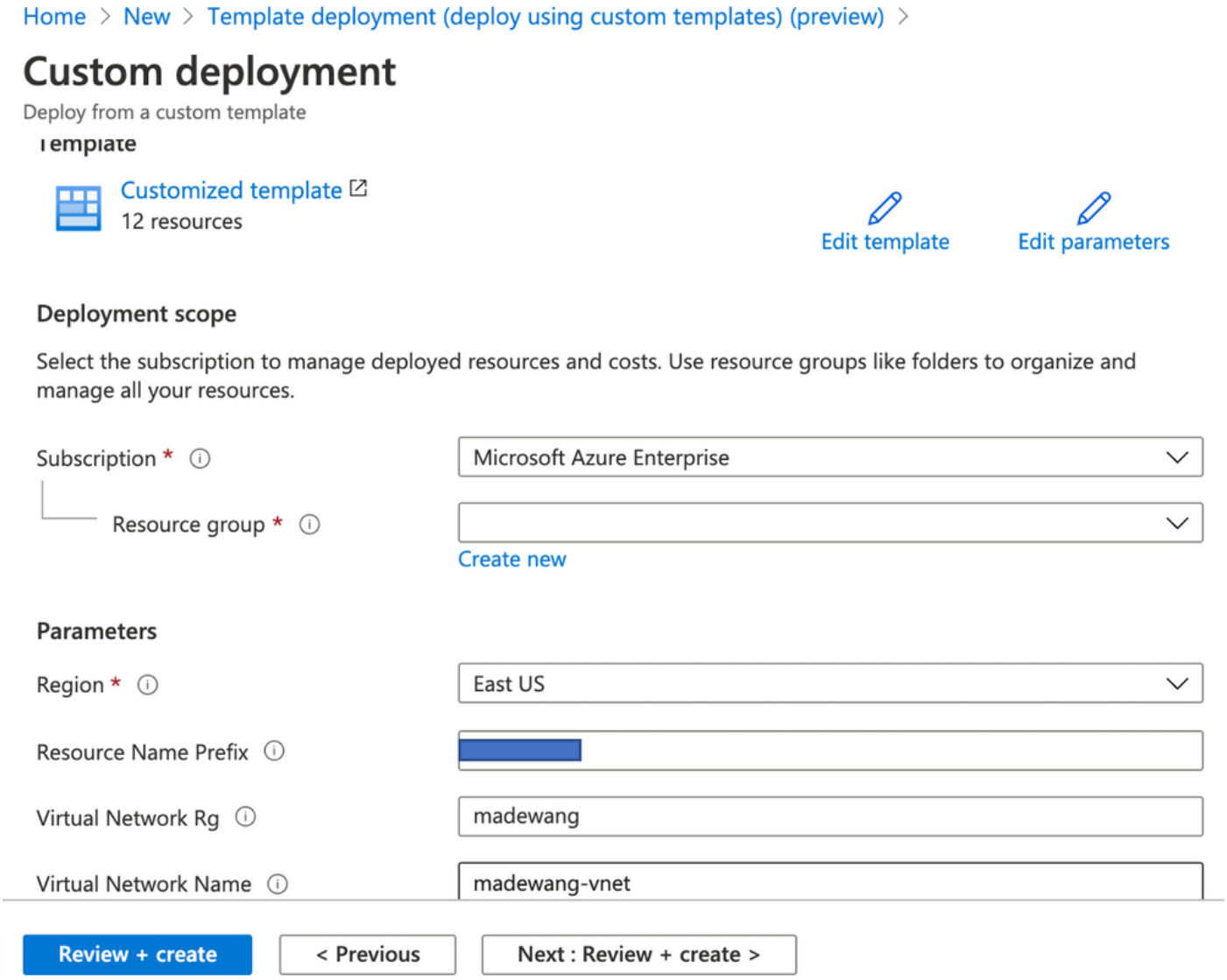
1. 创建Autoscale逻辑的组件。

使用ARM模板并创建VMSS、Logic APP、Function APP、App Insight、网络安全组。

导航至“**主页**”>“**创建资源**”>“**搜索模板**”，然后选择“**模板部署**”。现在，单击“**创建**”并在编辑器中创建您自己的模板。

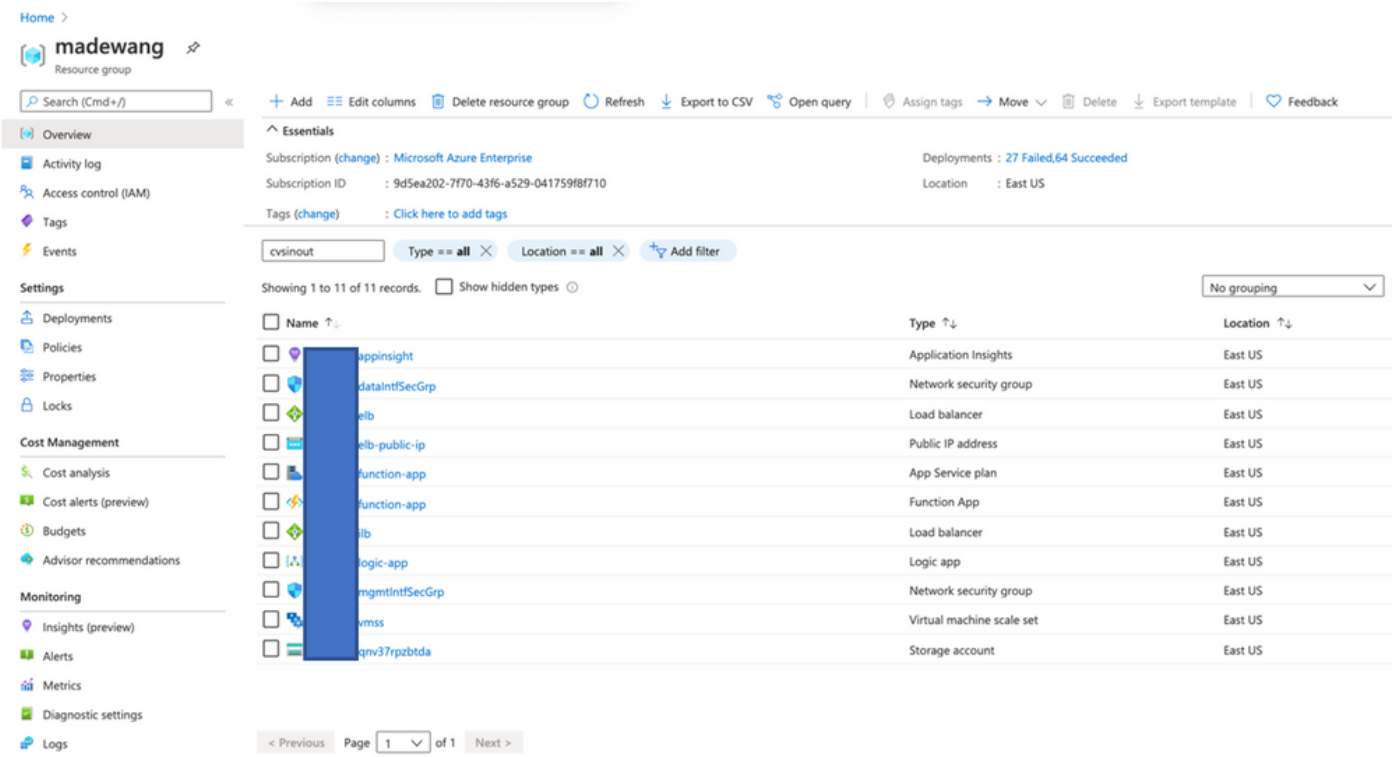


2. 单击“Save(保存)”。



对此模板进行所需的更改，然后单击“复查+创建”。

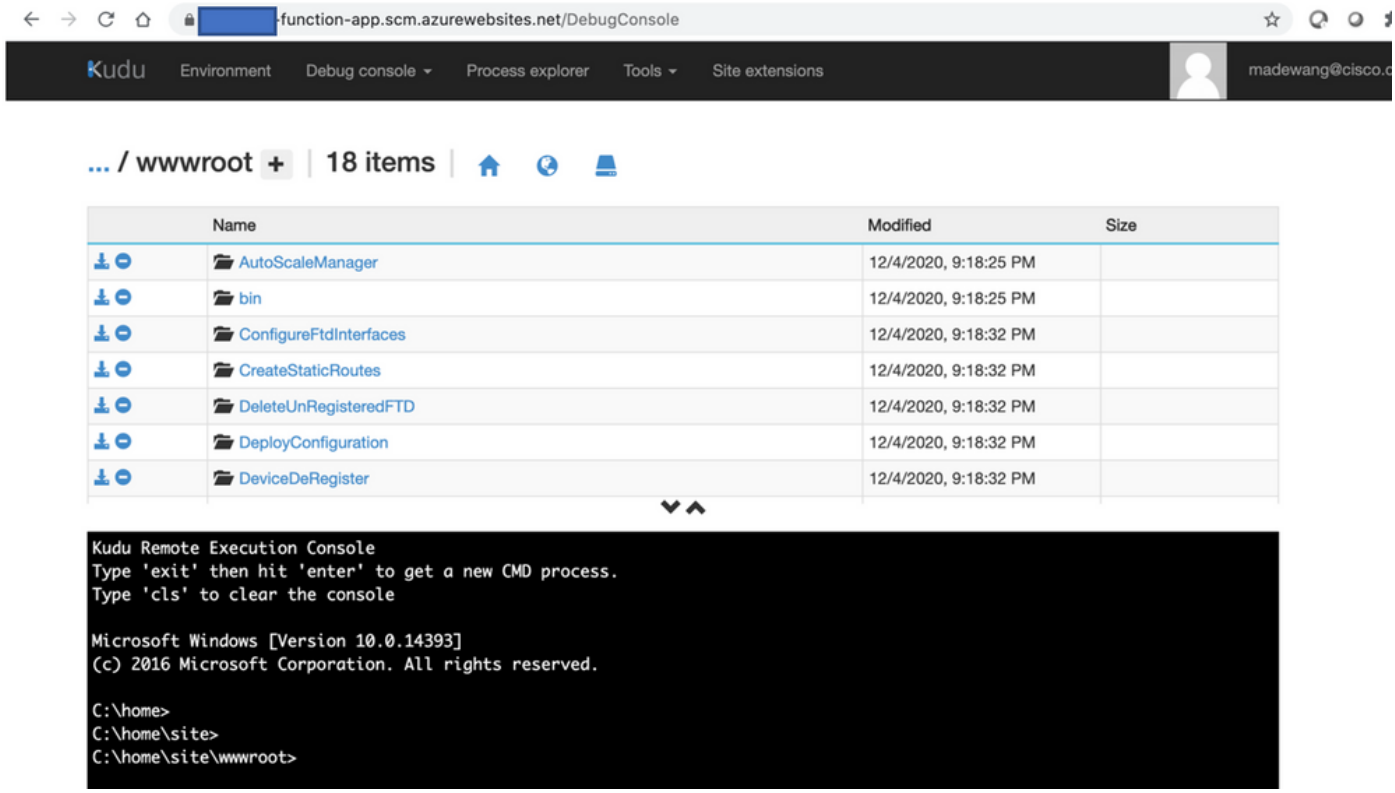
3. 这将创建上述资源组下的所有组件。



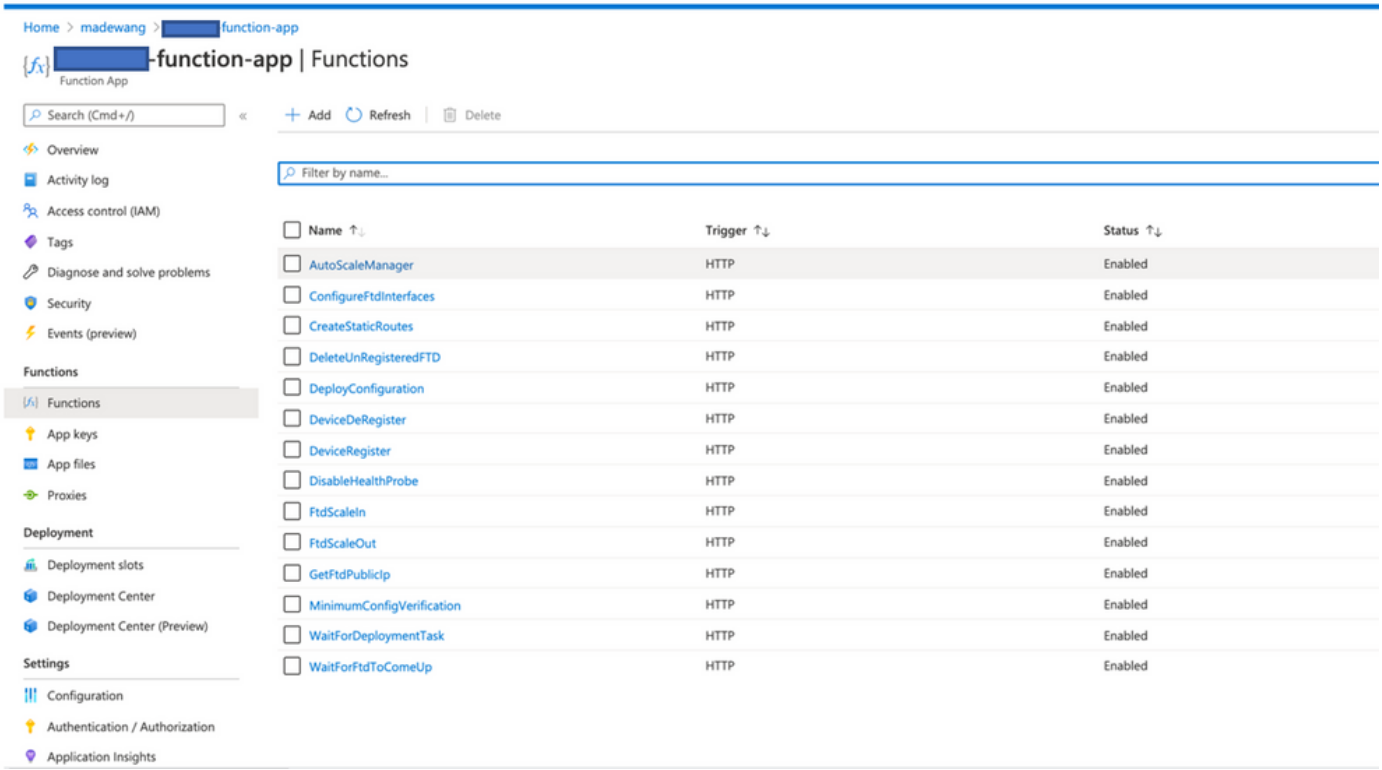
4. 登录URL
https://<function_app_name>.scm.azurewebsites.net/DebugConsole

将文件**ASM_Function.zip**和**ftdssh.exe**上载到**site/wwwroot/**文件夹（必须将其上传到指定位置，否则Function App不会识别各种功能。）

应该如下图所示：

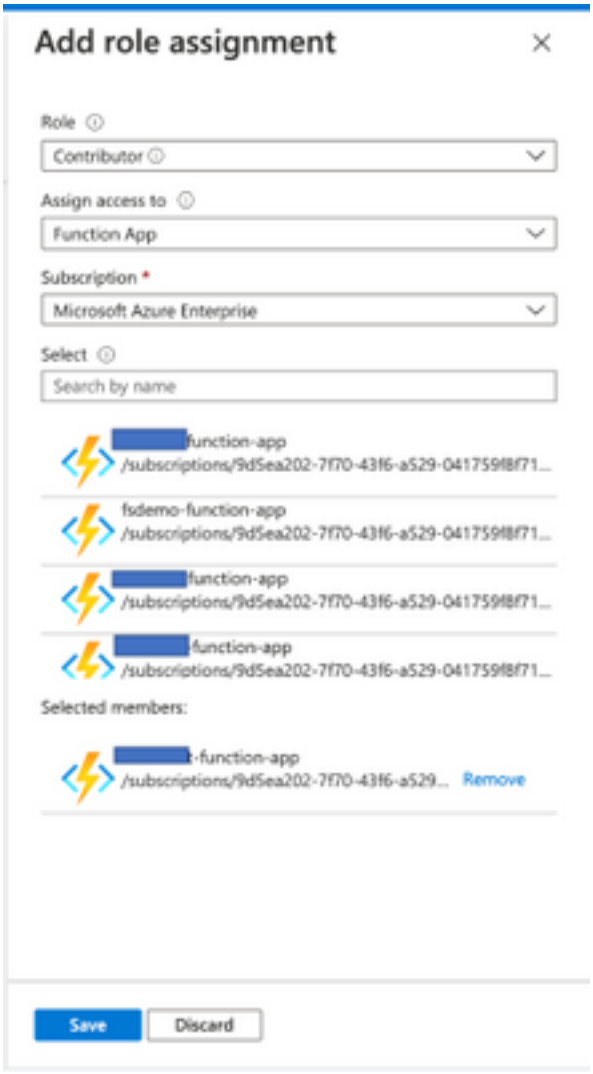


5. 检入Function应用**程序> Function**。您应该看到所有功能。



6. 更改访问权限，以便VMSS可以执行功能应用内的功能。

导航至**<prefix>-vmss> Access Control(IAM)> Add role assignement**。为此VMSS提供对<prefix>-function-app**的参与者访问**



Click **Save**.

7. 导航至“**逻辑应用”>“逻辑代码”**视图，并使用代码更改“逻辑代码”：
https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/Logic%20App

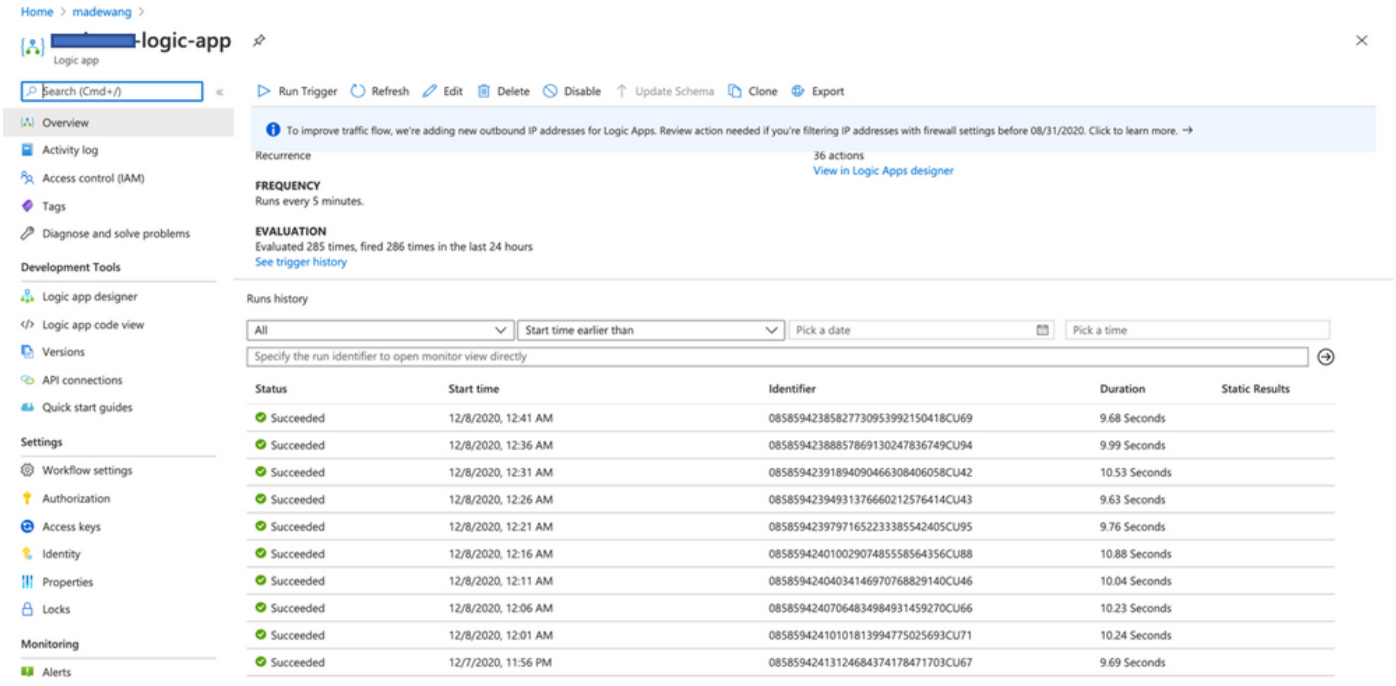
此处，Azure订阅、资源组名称和函数应用名称在使用前需要替换，否则它不允许成功保存。

8. Click **Save**.导航至逻辑应用概述并启**用逻辑应用**。

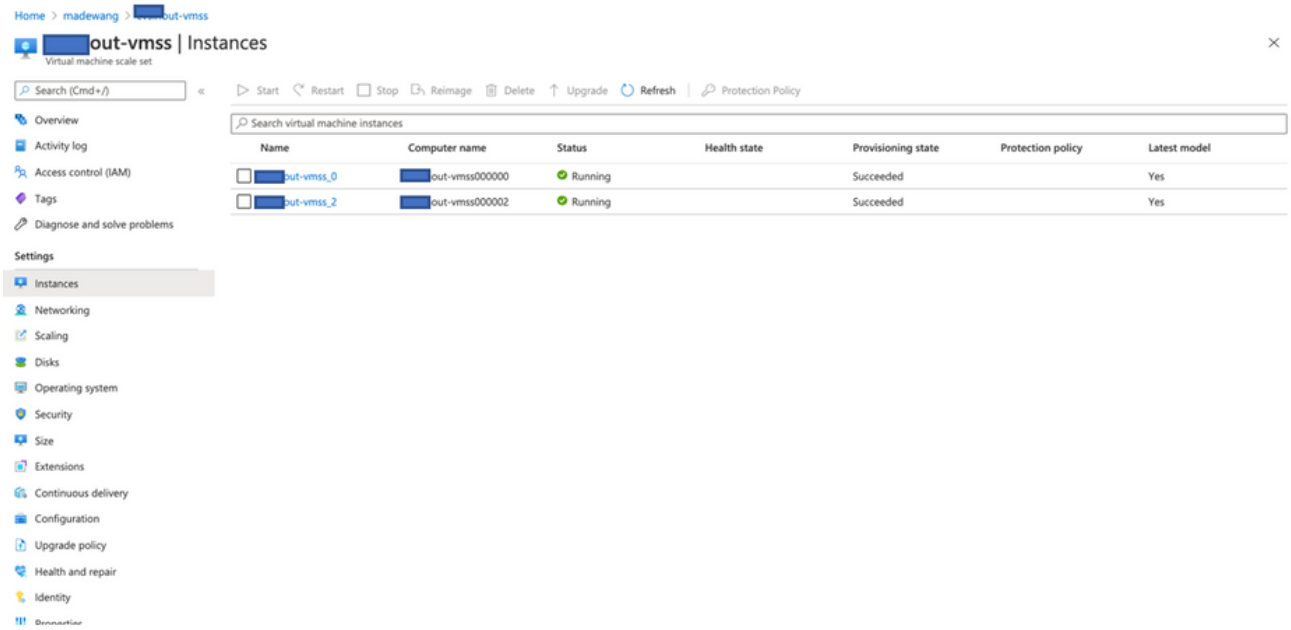
验证

启用逻辑应用后，它将立即开始在5分钟的间隔内执行。

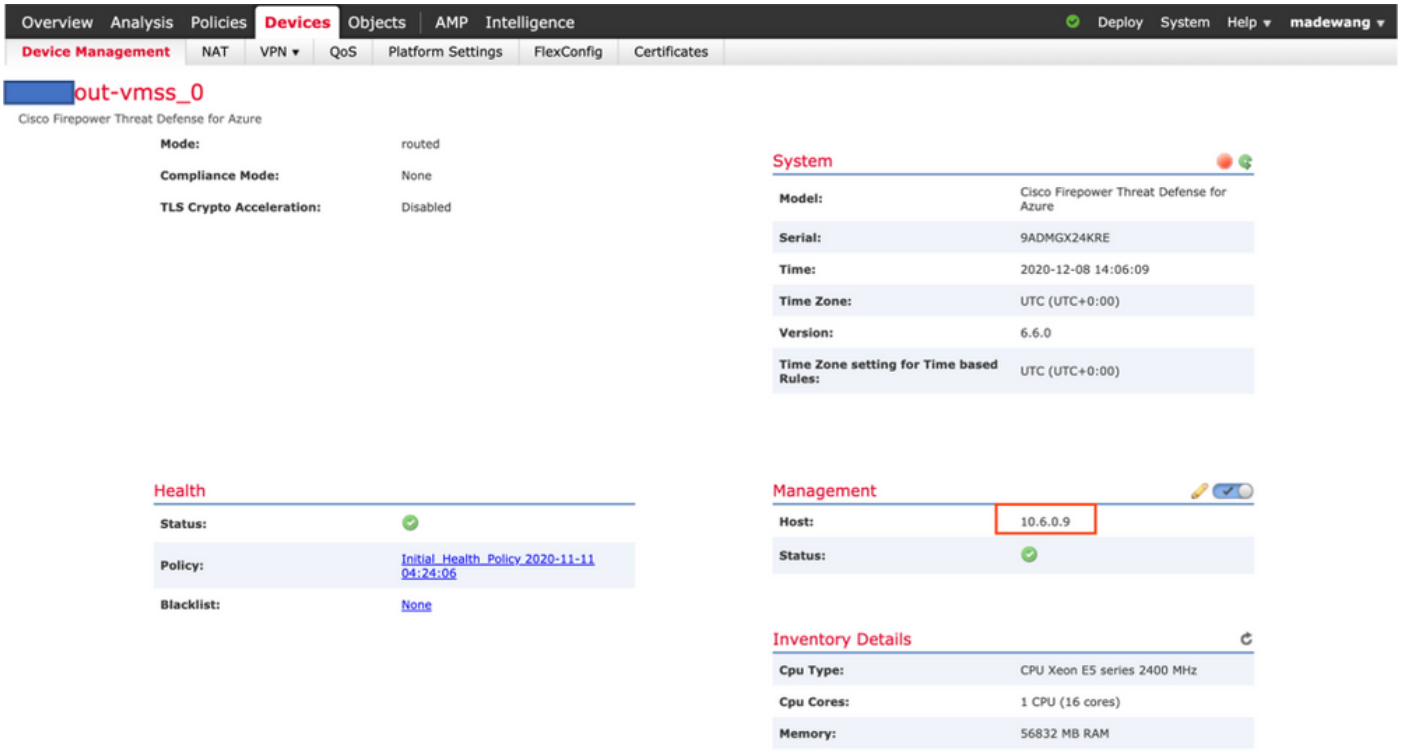
如果所有配置都正确，则您会看到触发器操作成功。



此外，VM是在VMSS下创建的。



登录FMC并检查FMC和NGFW是否通过FTDv私有IP连接：



登录NGFW CLI时，您会看到以下内容：

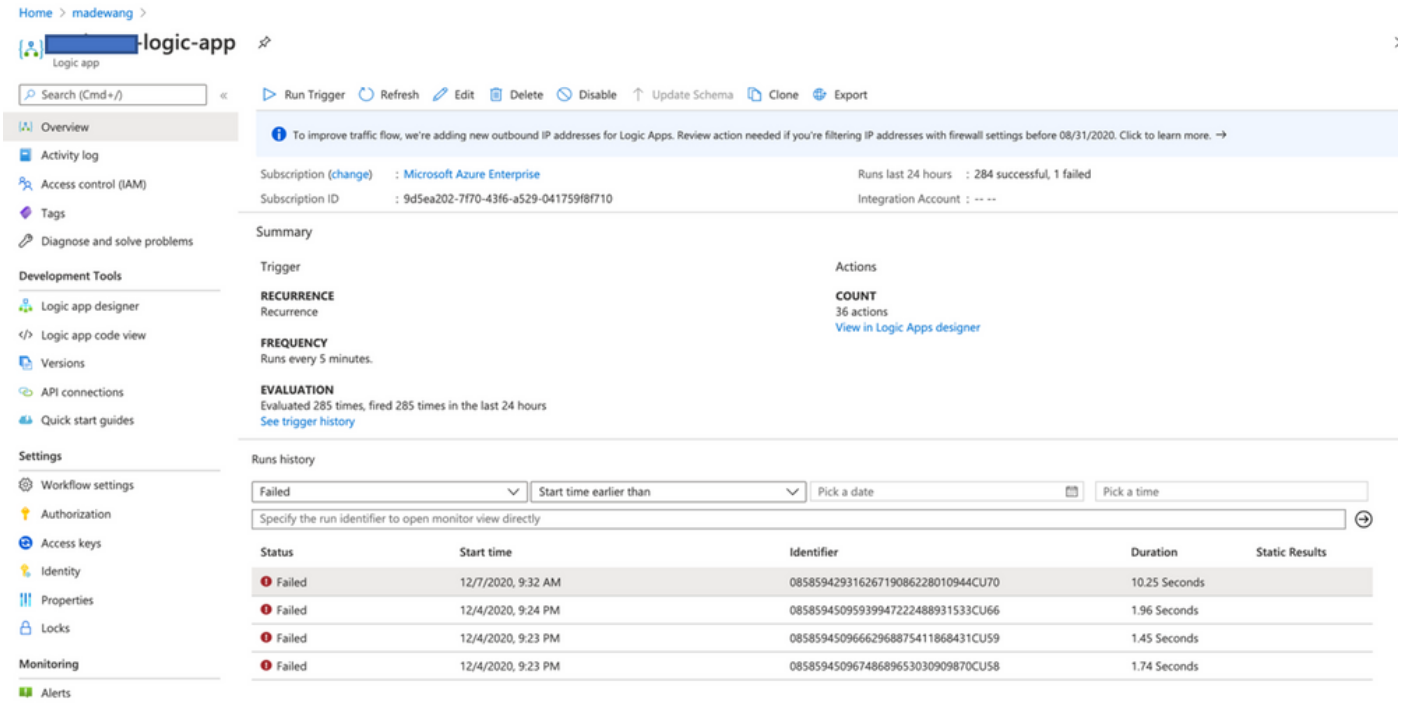
```
Cisco Fire Linux OS v6.6.0 (build 37)
Cisco Firepower Threat Defense for Azure v6.6.0 (build 90)

> ex
exit   expert
> expert
admin@[redacted]inout-vmss-0:~$ netstat | grep 8305
tcp        0      0 [redacted]inout-vmss-0:8305    madewangfmc.inter:41997 ESTABLISHED
tcp        0      0 [redacted]inout-vmss-0:8305    madewangfmc.inter:54513 ESTABLISHED
admin@[redacted]nout-vmss-0:~$
```

因此，FMC通过Azure私有VNet子网与NGFW通信。

故障排除

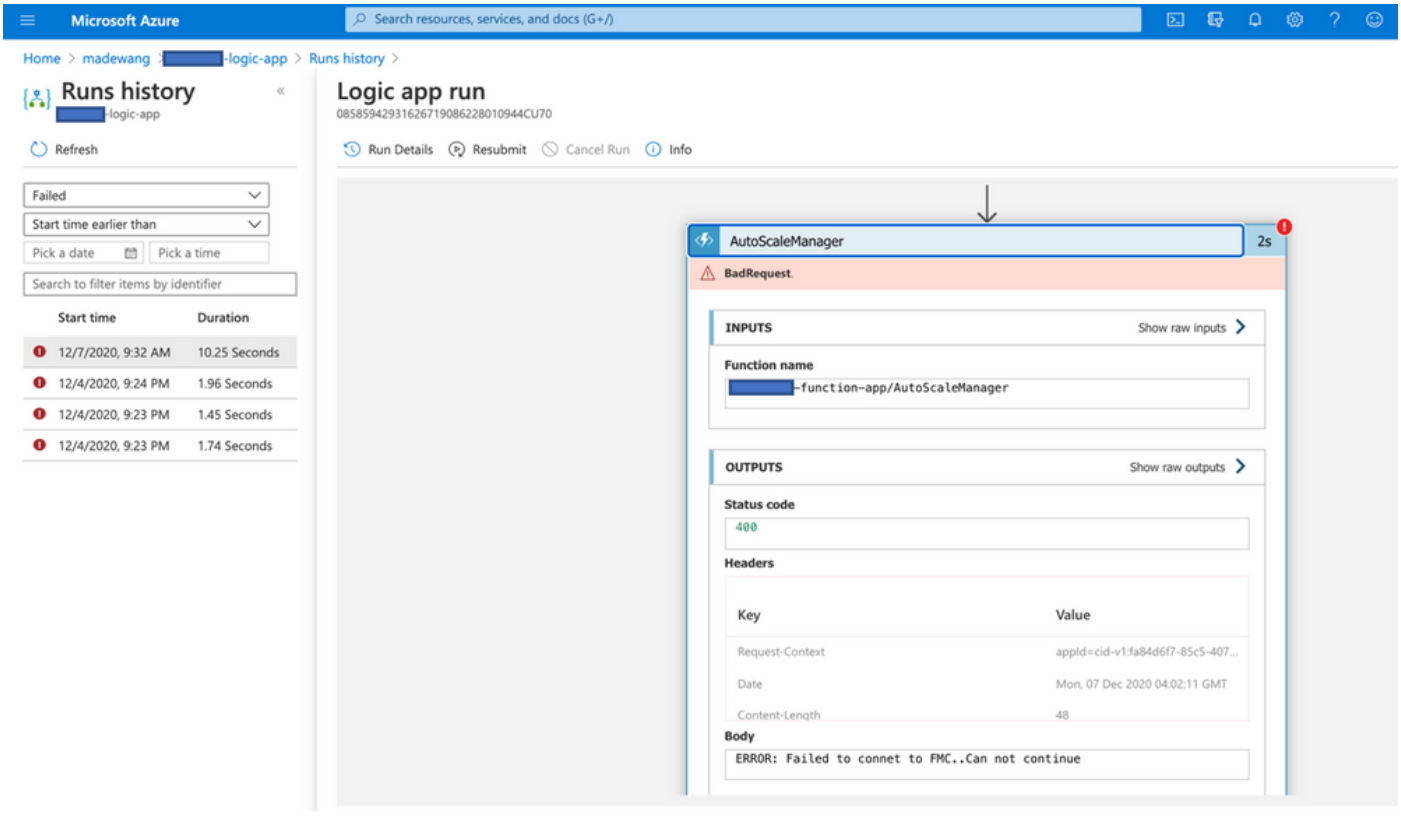
有时，Logic App在构建新的NGFW时会失败，要排除此类情况，可采取以下步骤：

1. 检查逻辑应用是否运行成功。



2. 确定故障原因。

单击失败的触发器。



尝试从代码流中识别故障点。从上面的片段中，ASM逻辑显然失败，因为它无法连接到FMC。接下来，您需要根据Azure中的流确定FMC无法访问的原因。