在高信任環境中在Azure中部署自動縮放的FTDv

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[設定](#)
[Azure ARM模板](#)
[功能應用](#)
[邏輯應用程式](#)
[網路圖表](#)
[組態](#)
[驗證](#)
[疑難排解](#)

簡介

本文描述如何在高度信任環境中在Azure中部署自動縮放的Cisco Firepower威脅防禦虛擬(FTDv)。

必要條件

需求

思科建議您瞭解以下主題：

- NGFW和Firepower管理中心應通過私有IP通訊
- 外部負載平衡器不應具有公共IP。
- 功能的應用應該能夠與專用IP通訊

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Azure
- Firepower管理中心
- 虛擬機器規模集

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FTDv將思科的Firepower下一代防火牆功能引入虛擬化環境，從而支援一致的安全策略，以跟蹤物理、虛擬和雲環境以及雲之間的工作負載。

由於這些部署可在虛擬化環境中使用，NGFW目前無法支援HA。因此，為了提供高度可用的解決方案，思科下一代防火牆(NGFW)利用Azure的本地功能(如可用性集和虛擬機器規模集(VMSS))使NGFW高度可用，並滿足日益增加的按需流量。

本文檔重點介紹根據不同引數將思科NGFW配置為自動擴展，其中NGFW按需擴展或按需擴展。這涵蓋了客戶要求使用Firepower Management Center(FMC)的使用案例，FMC在託管資料中心中可用，並且需要集中管理所有NGFW，而且客戶也不希望使用FMC和FTD通過公共IP通訊管理流量。

在深入瞭解配置和設計之前，請注意以下幾個向Azure寫入時應充分瞭解的概念：

- **可用區**: 可用區是一種高可用性產品，可保護您的應用程式和資料免受資料中心故障的影響。可用區域是Azure區域內唯一的物理位置。每個區域由一個或多個資料中心組成，這些資料中心配備了獨立的電源、冷卻和網路。

- **VNET**: Azure虛擬網路(VNet)是Azure中你的專用網路的基本構建塊。VNet使許多型別的Azure資源（如Azure虛擬機器[VM]）能夠安全地相互通訊、網際網路和本地網路。VNet類似於您在自己的資料中心運行的傳統網路，但它帶來了Azure基礎設施的其他優勢，如規模、可用性和隔離。預設情況下，VNET中的每個子網均可相互訪問，但不同VNET中的子網則不同。

- **可用性集**: 可用性集是另一種資料中心配置，用於提供VM冗餘和可用性。資料中心內的此配置可確保計畫內或計畫外維護事件期間至少有一個虛擬機器可用，並滿足99.95%的Azure SLA。

- **VMSS**: Azure虛擬機器規模集允許您建立和管理一組負載均衡的VM。VM例項的數量可以自動增加或減少，以響應需求或定義的計畫。擴展集為您的應用程式提供了高可用性，並允許您集中管理、配置和更新大量虛擬機器。藉助虛擬機器規模集，您可以為計算、大資料和容器工作負載等領域構建大規模服務。

- **功能應用**：Azure功能是按需提供的雲服務，提供運行應用程式所需的所有持續更新的基礎設施和資源。你關注對你來說最重要的代碼片段，Azure函式處理其餘的代碼。您可以使用Azure函式構建Web API、響應資料庫更改、處理IoT流、管理消息隊列等。在此自動縮放解決方案中，Azure函式是向FMC發出的各種API請求，用於建立對象、註冊/註銷FTDv、檢查引數等。

- **邏輯應用**：Azure Logic Apps是一項雲服務，可在您需要跨企業或組織整合應用、資料、系統和服務時，幫助您計畫、自動化和協調任務、業務流程和工作流。Logic Apps可簡化您設計和構建可擴展解決方案的方式，這些解決方案可用於應用集成、資料整合、系統整合、企業應用整合(EAI)以及企業到企業(B2B)通訊（無論是在雲中、在內部或兩者兼有）。此解決方案為自動縮放解決方案的功能提供了要執行的功能的邏輯順序。

目前，可用於NGFW的AutoScale解決方案不提供與VNet本地專用IP通訊的管理計畫，並且需要公共IP在Firepower管理中心和NGFW之間交換通訊。

本文旨在解決此問題，直到經驗證的解決方案可用於Firepower管理中心和NGFW通過私有IP進行通訊。

設定

要建立自動縮放的NGFW解決方案，請使用以下配置指南：

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

經過多次修改，可處理以下使用案例：

- 功能應用應該能夠與客戶內部IP段通訊
- 負載平衡器不應具有公共IP
- NGFW和FMC之間的管理流量應通過專用IP網段交換。

若要建立自動縮放新世代防火牆(AutoScaled NGFW)解決方案，請使用上述使用案例，按照思科官方指南中提到的步驟修改這些案例：

1. Azure ARM模板

ARM模板用於啟用Azure中的自動化。思科提供了經過驗證的ARM模板，可用於建立自動擴展解決方案。但是，Public Github https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template上提供的此ARM模板建立了一個功能應用，不能使其通過快速路由到達客戶的內部網路。因此，我們需要對此進行一些修改，以便函式應用現在可以使用高級模式而不是消費模式。因此可在https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git獲取所需的ARM模板

2. 功能應用

函式應用是一組Azure函式。基本功能包括：

- 定期通訊/探測Azure度量。
- 監控FTDv負載並觸發擴展輸入/擴展操作。
- 向FMC註冊新的FTDv。
- 透過FMC設定新的FTDv。
- 從FMC中註銷（移除）按比例縮放的FTDv。

如要求中所述，為按需建立或刪除NGFW建立的各種功能基於NGFW的公共IP完成。因此，我們需要調整C#代碼以獲得私有IP，而不是公共IP。在調整代碼後，可在https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git上找到用於建立函式應用的zip檔案

名為ASM_Function.zip。這樣，功能應用就能夠與內部資源通訊，而無需使用公共IP。

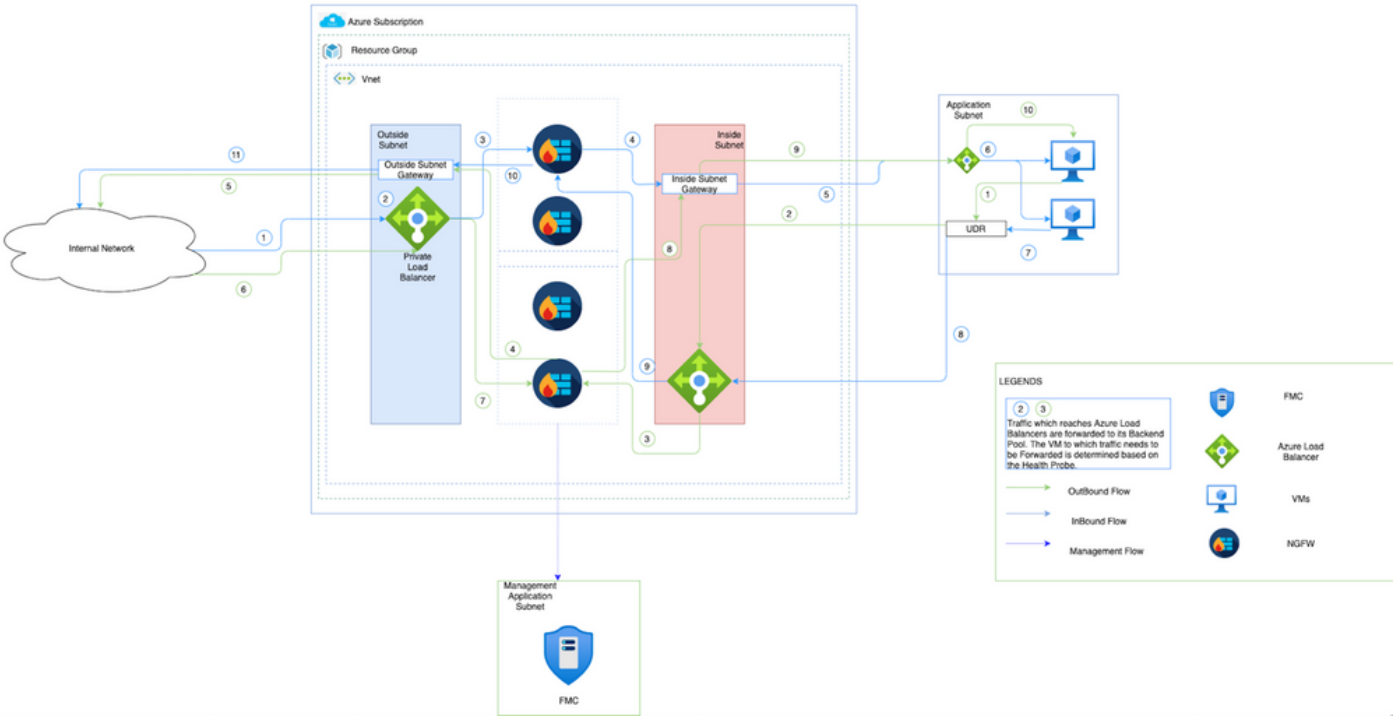
3. 邏輯應用程式

自動縮放邏輯應用是一個工作流，即序列中的步驟集合。Azure函式是獨立的實體，無法相互通訊。此協調器會對這些功能的執行進行排序，並在它們之間交換資訊。

- 邏輯應用用於協調和傳遞自動縮放Azure功能之間的資訊。
- 每個步驟代表自動縮放Azure功能或內建標準邏輯。
- 邏輯應用作為JSON檔案提供。
- 可以通過GUI或JSON檔案自定義邏輯應用。

附註：應仔細修改https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git上提供的邏輯應用詳細資訊，並且以下專案必須替換為部署詳細資訊、FUNSTIONAPP名稱、資源組名稱和訂閱ID。

網路圖表



此圖顯示入站和出站流量如何通過NGFW在Azure環境中流動。

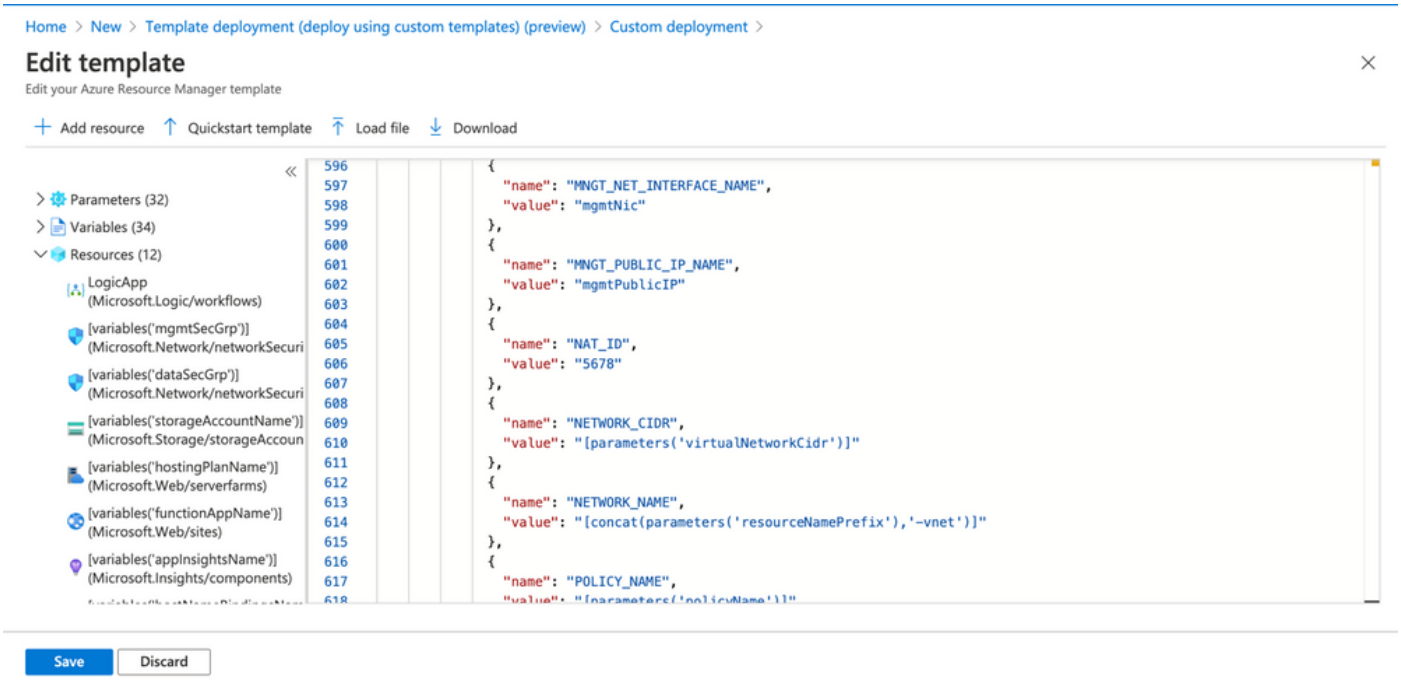
組態

現在建立自動縮放解決方案所需的各種元件。

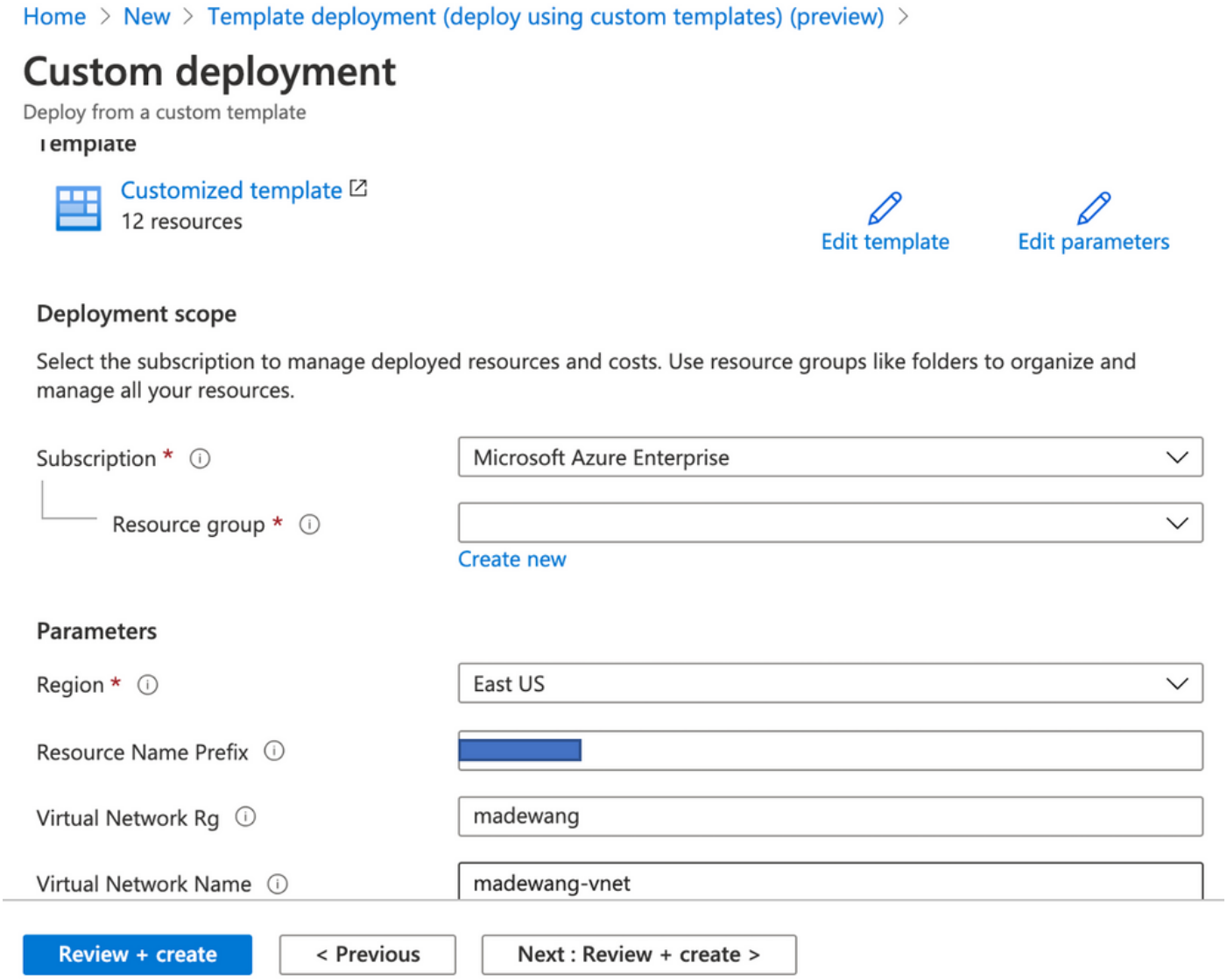
1. 建立自動縮放邏輯的元件。

使用ARM模板建立VMSS、Logic APP、Function APP、App Insight、Network Security Group。

導航到**首頁>建立資源>搜尋模板**，然後選擇**模板部署**。現在，按一下**Create**，在編輯器中構建自己的模板。

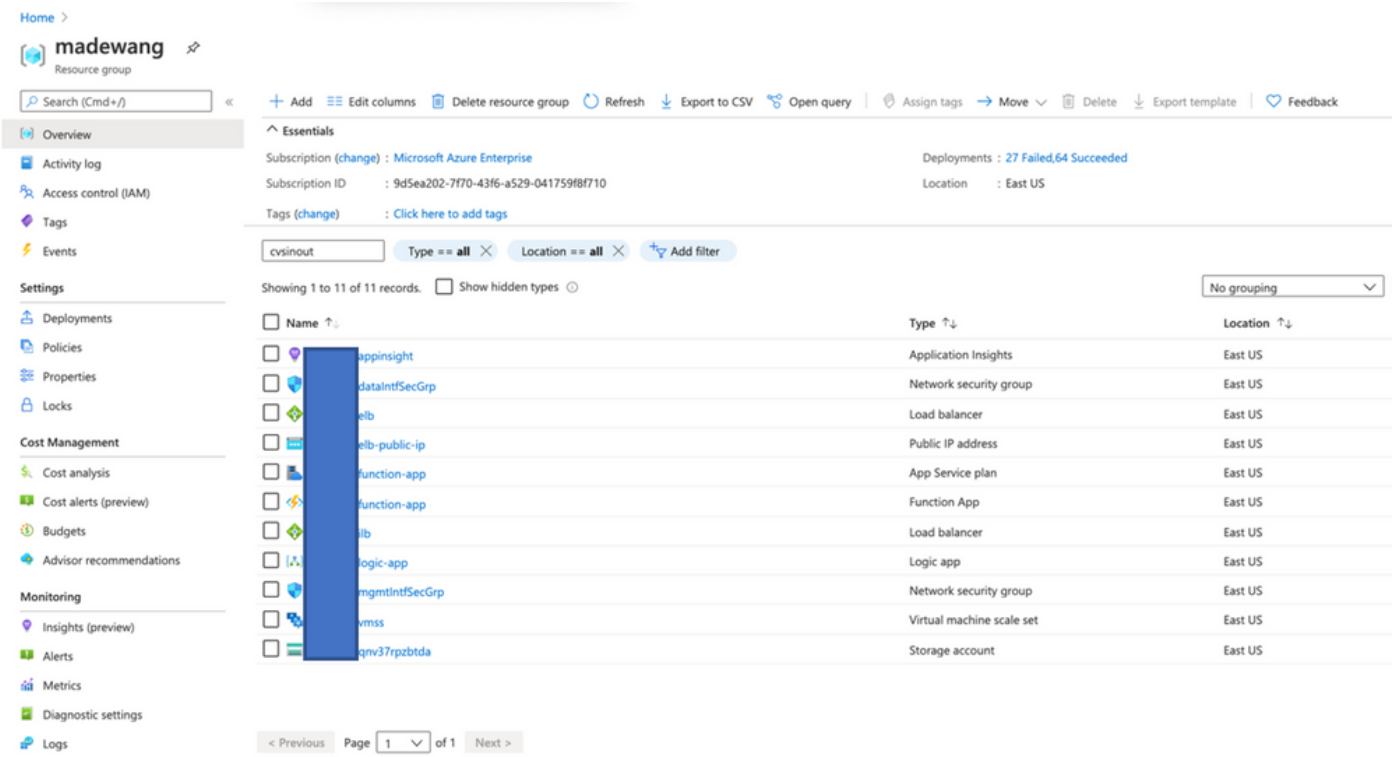


2. 按一下**Save**。



對此模板進行所需的更改，然後按一下**Review +Create**。

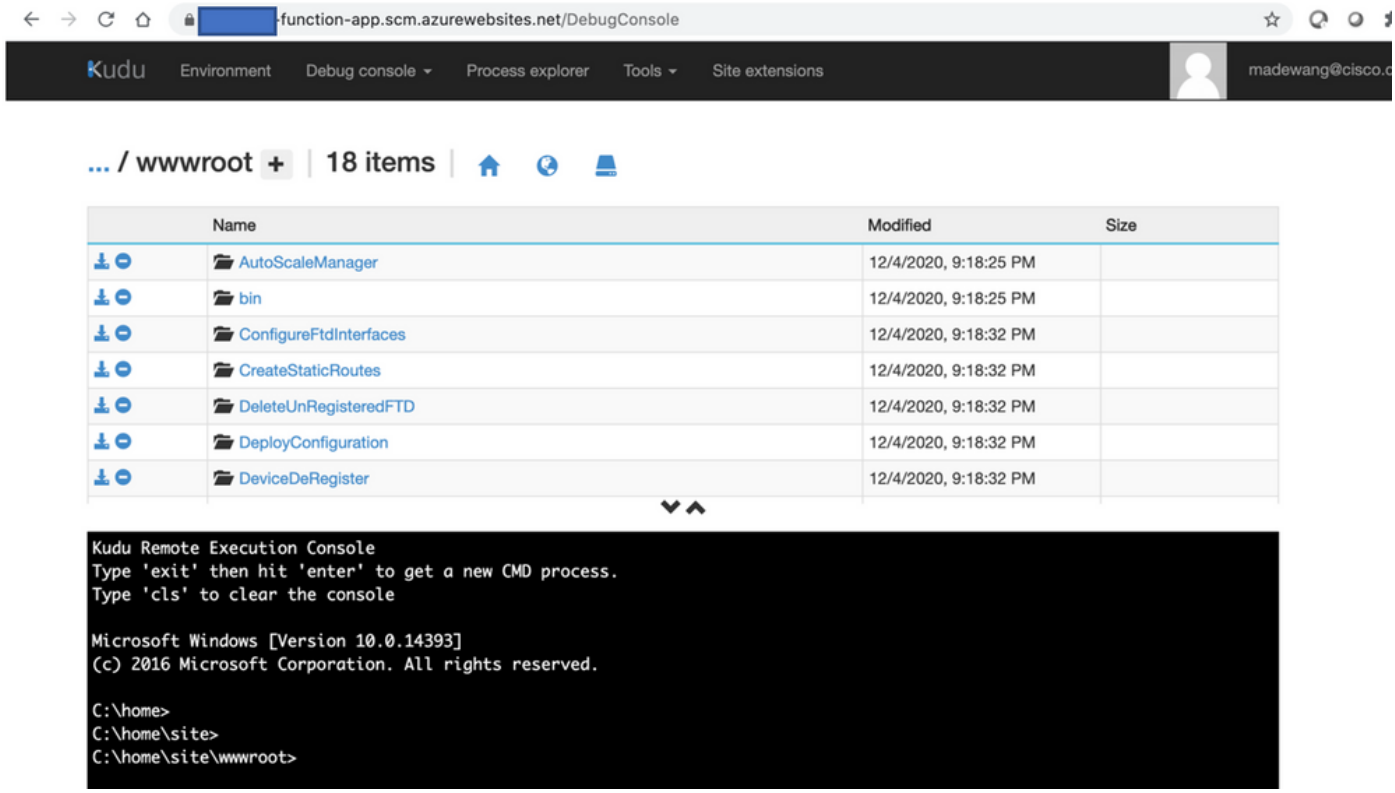
3. 這將建立上述資源組下的所有元件。



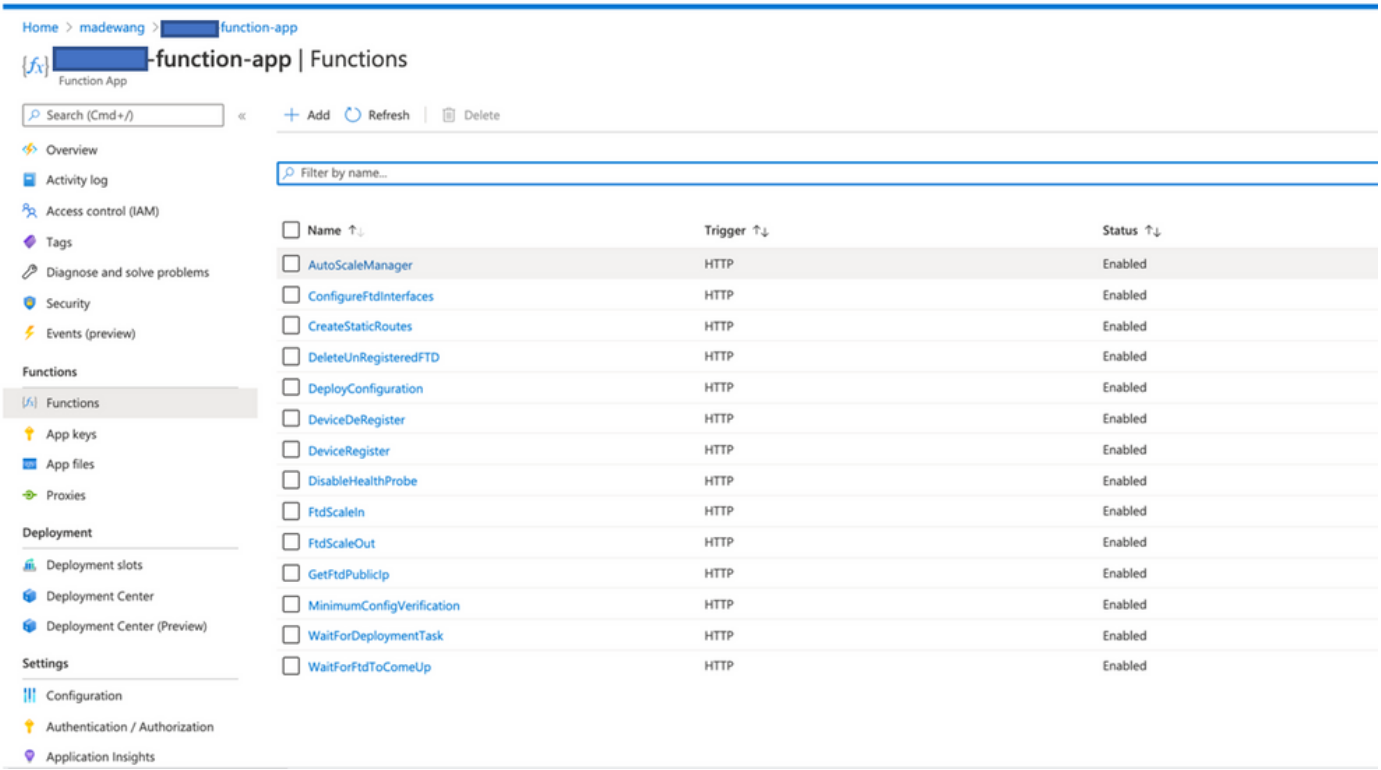
4. 登入url
https://<function_app_name>.scm.azurewebsites.net/DebugConsole

將檔案ASM_Function.zip和 ftdssh.exe上載到site/wwwroot/資料夾（必須將其上載到指定位置，否則函式應用無法識別各種函式。）

應該如下所示：

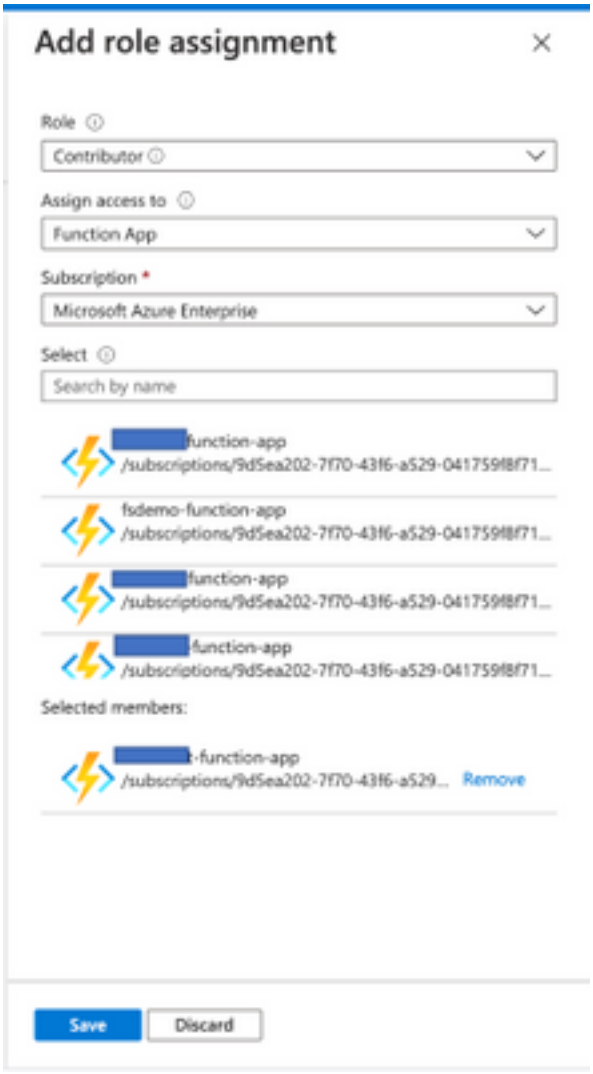


5. 簽入「函式」**應用>「函式」**。你應該看看所有的功能。



6. 更改訪問許可權，以便VMSS可以執行功能應用內的功能。

導航到**<prefix>-vmss>訪問控制(IAM)>新增角色分配**。為此VMSS提供對<prefix>-function-app的**參與者訪問許可權**



按一下「**Save**」。

7. 導航到**邏輯應用>邏輯代碼檢視**，並使用以下網址提供的代碼更改邏輯代碼：
https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/Logic%20App

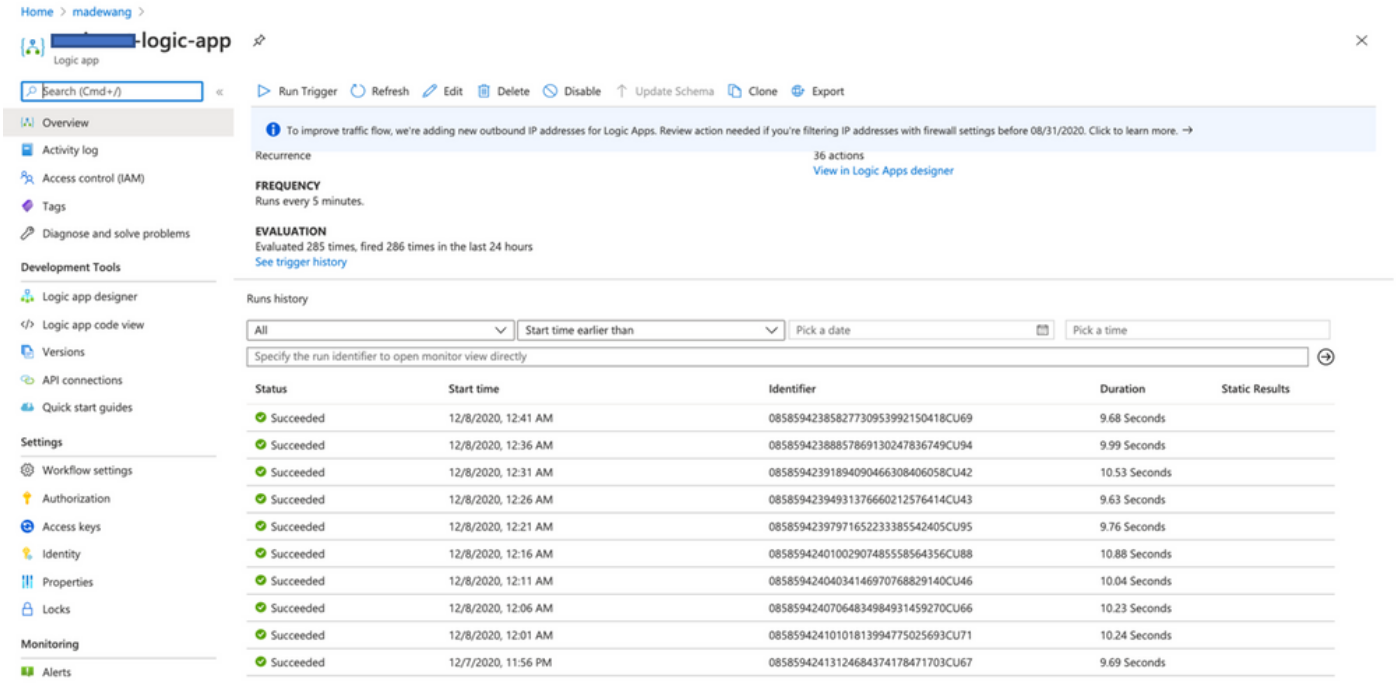
在此，需要在使用前替換Azure訂閱、資源組名稱和函式應用名稱，否則不允許成功儲存。

8. 按一下「**Save**」。導航到Logic App Overview和Enable **Logic App**。

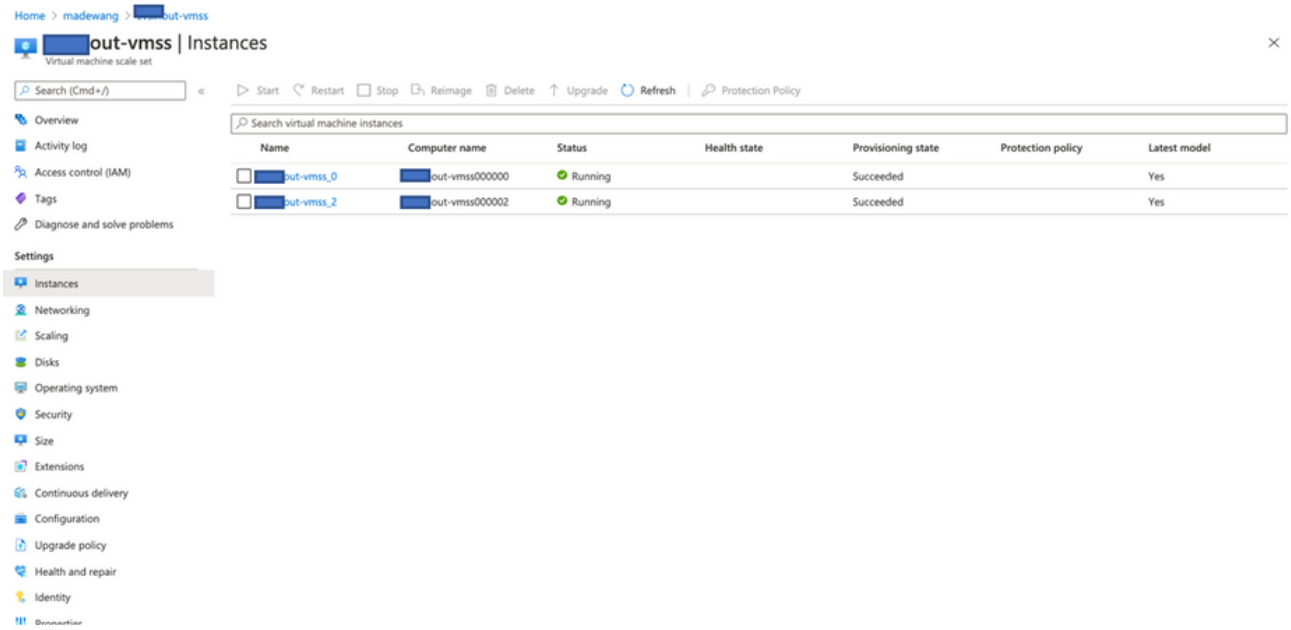
驗證

一旦啟用邏輯應用，它就會在5分鐘的間隔內立即開始執行。

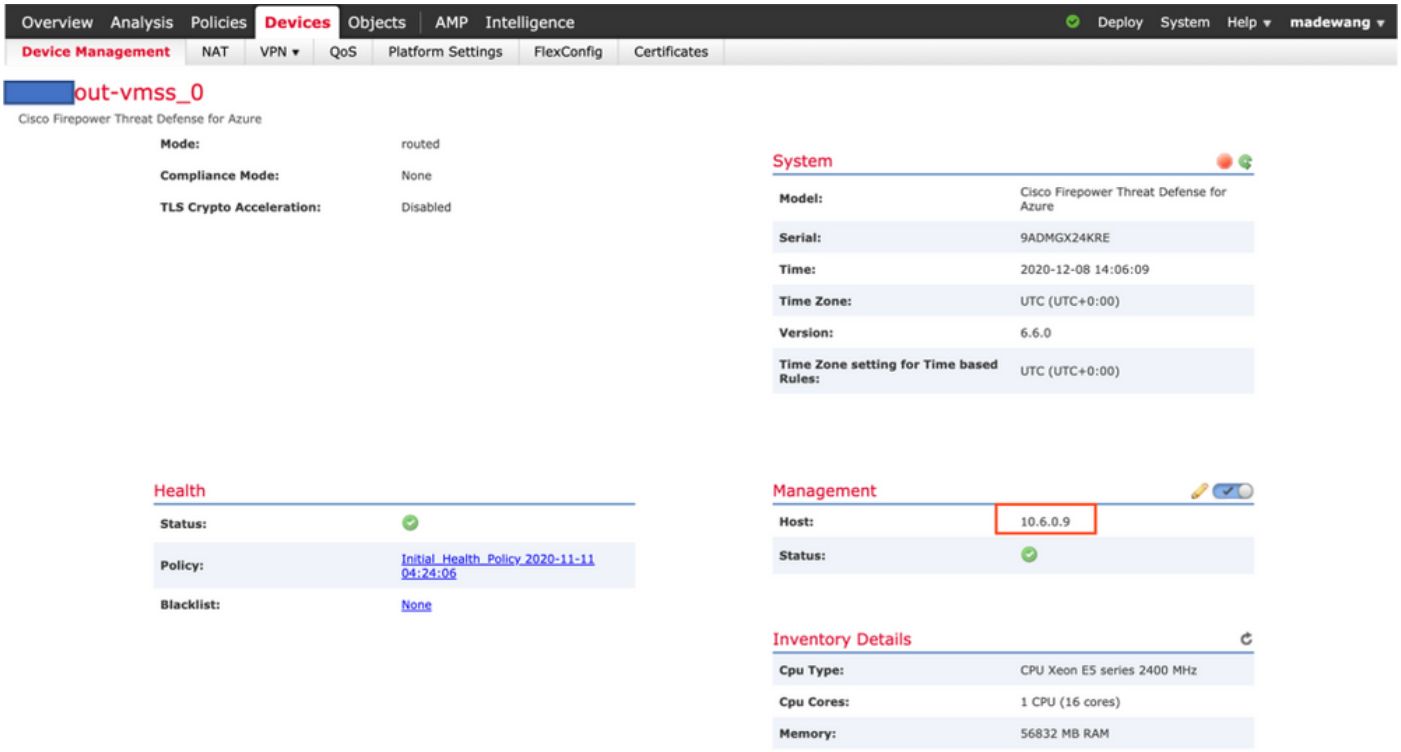
如果所有配置都正確，則您會看到觸發器操作成功。



此外，VM是在VMSS下建立的。



登入FMC，並檢查FMC和NGFW是否透過FTDv Private IP連線：



登入NGFW CLI時，會看到以下內容：

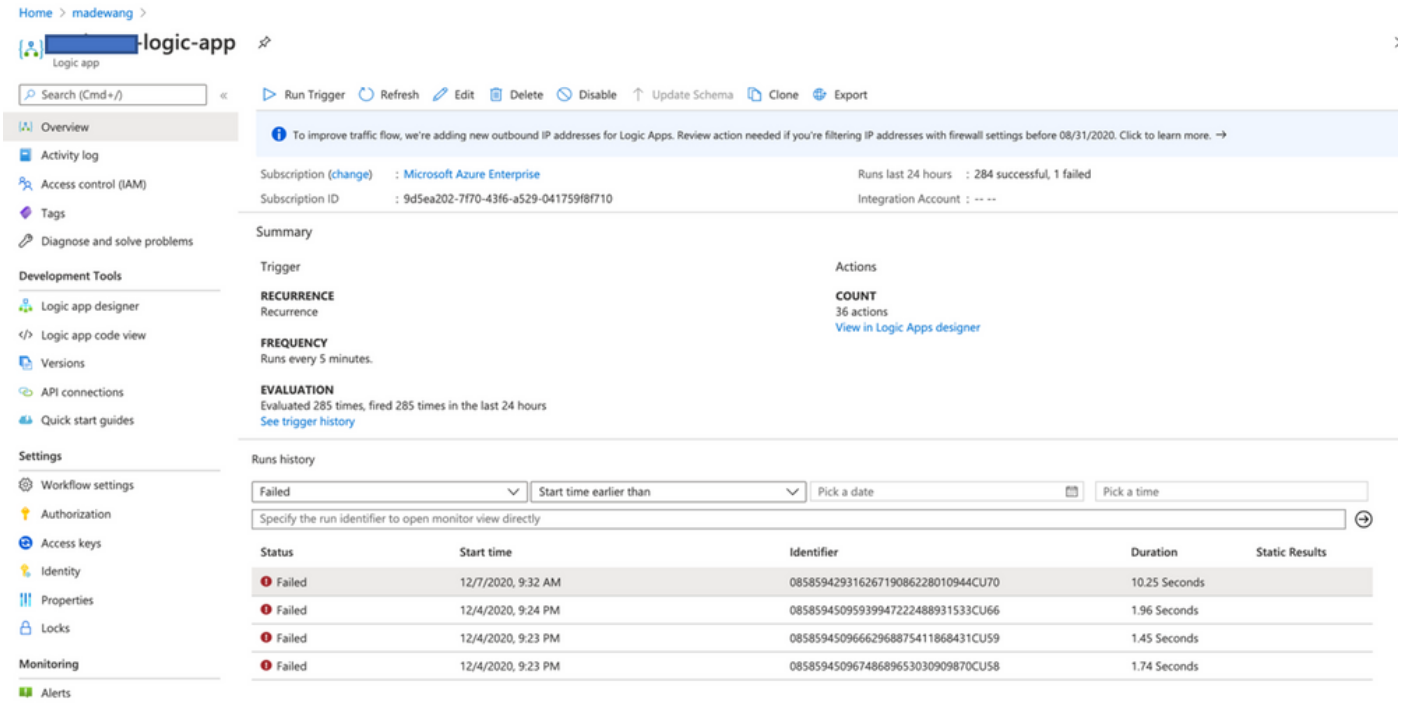
```
Cisco Fire Linux OS v6.6.0 (build 37)
Cisco Firepower Threat Defense for Azure v6.6.0 (build 90)

> 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通過Azure專用VNet子網與NGFW通訊。

疑難排解

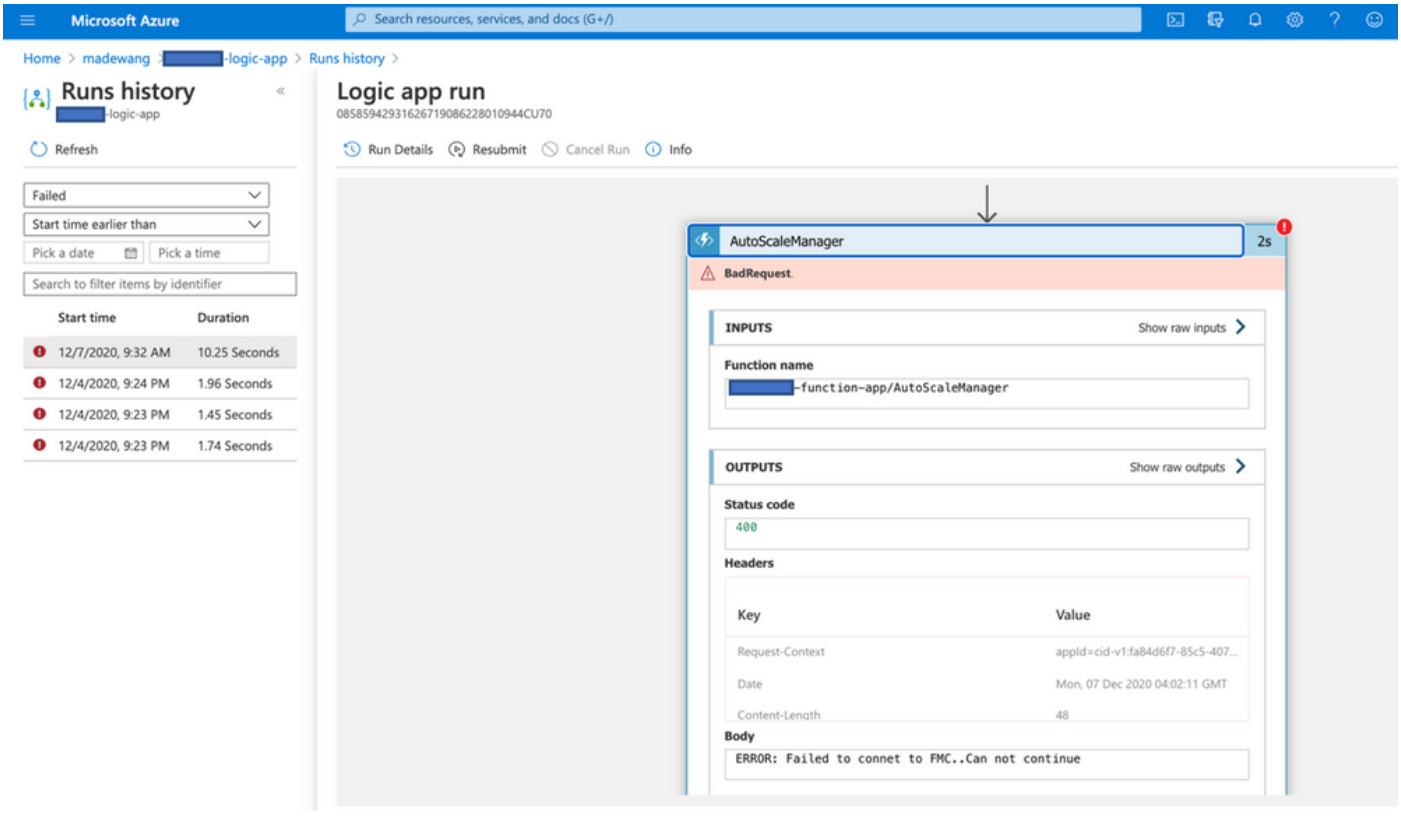
有時，在構建新的NGFW時，Logic App會失敗。要排除此類故障，可以採取以下步驟：

1. 檢查邏輯應用是否已成功運行。



2. 確定故障原因。

按一下失敗的觸發器。



嘗試從代碼流中識別故障點。從以上代碼片斷可以看出，ASM邏輯顯然失敗，因為它無法連線到FMC。接下來，您需要確定無法按流在Azure中訪問FMC的原因。