

Implantar FTDv em Escala Automática no Azure em um Ambiente de Alta Confiança

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Modelo ARM do Azure](#)

[Função APP](#)

[Aplicativo Lógico](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como implantar o Cisco Firepower Threat Defense Virtual (FTDv) autodimensionado no Azure em um ambiente de alta confiança.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O NGFW e o Firepower Management Center devem se comunicar por IP privado
- O balanceador de carga externo não deve ter IP público.
- O aplicativo da função deve ser capaz de se comunicar com o IP privado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Azure
- Firepower Management Center
- Conjunto de Dimensões da Máquina Virtual

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O FTDv traz a funcionalidade do firewall de próxima geração Firepower da Cisco para ambientes virtualizados, permitindo que políticas de segurança consistentes sigam as cargas de trabalho em ambientes físicos, virtuais e em nuvem, e entre nuvens.

Com essas implantações disponíveis em um ambiente virtualizado, o suporte atual para HA não está disponível para NGFW. Assim, para fornecer uma solução altamente disponível, o Cisco Next-Generation Firewall (NGFW) utiliza os recursos nativos do Azure, como Conjuntos de Disponibilidade e VMSS (Virtual Machine Scale Set) para tornar o NGFW altamente disponível e atender ao aumento do tráfego sob demanda.

Este documento concentra-se em configurar o Cisco NGFW para AutoScale com base em parâmetros diferentes em que o NGFW é escalável ou escalável sob demanda. Isso abrange o caso de uso em que o cliente precisa usar o Firepower Management Center (FMC), que está disponível no datacenter de colocação e é necessário para gerenciar centralmente todo o NGFW, além de que os clientes não querem ter o FMC e o FTD para se comunicarem por IP público para tráfego de gerenciamento.

Antes de se aprofundar na configuração e na consideração de design, a seguir, estão os poucos conceitos que devem ser bem compreendidos e mal compreendidos para o Azure:

- **Zona de disponibilidade:** Uma zona de disponibilidade é uma oferta de alta disponibilidade que protege seus aplicativos e dados contra falhas no data center. As zonas de disponibilidade são locais físicos exclusivos em uma região do Azure. Cada zona é composta por um ou mais data centers equipados com energia, resfriamento e rede independentes.
- **VNET:** A Rede Virtual do Azure (VNet) é o elemento fundamental da sua rede privada no Azure. O VNet permite que vários tipos de recursos do Azure, como as Máquinas Virtuais do Azure (VM), se comuniquem com segurança entre si, com a Internet e com redes locais. O VNet é semelhante a uma rede tradicional que você operaria em seu próprio data center, mas traz benefícios adicionais da infraestrutura do Azure, como escala, disponibilidade e isolamento. Cada sub-rede dentro de uma VNET pode ser alcançada entre si por padrão, mas o mesmo não é verdade para sub-redes em diferentes VNETs.
- **Conjunto de disponibilidade:** Os conjuntos de disponibilidade são outra configuração de data center para fornecer redundância e disponibilidade de VM. Essa configuração em um data center garante que durante um evento de manutenção planejado ou não, pelo menos uma máquina virtual esteja disponível e atenda ao SLA do Azure 99,95%.
- **VMSS:** Os conjuntos de dimensionamento de máquina virtual do Azure permitem criar e gerenciar um grupo de VMs com balanceamento de carga. O número de instâncias de VM pode aumentar ou diminuir automaticamente em resposta à demanda ou a uma programação definida. Os conjuntos de escala fornecem alta disponibilidade para seus aplicativos e permitem que você gerencie, configure e atualize centralmente um grande número de VMs. Com conjuntos de escala de máquinas virtuais, você pode criar serviços em grande escala para áreas como computação, big data e cargas de trabalho de contêineres.

- **Aplicativo Funções:** O Azure Functions é um serviço de nuvem disponível sob demanda que fornece toda a infraestrutura e os recursos atualizados continuamente necessários para executar seus aplicativos. Você se concentra nos pedaços de código mais importantes para você, e o Azure Functions lida com o resto. Você pode usar as Funções do Azure para criar APIs da Web, responder a alterações no banco de dados, processar fluxos da IoT, gerenciar filas de mensagens e muito mais. Nesta solução Autodimensionada, a Função do Azure são várias solicitações de API para o FMC para criar objetos, registrar/cancelar o registro do FTDv, verificar os parâmetros, etc.
- **Aplicativo Lógico:** [Azure Logic Apps](#) é um serviço de nuvem que ajuda a programar, automatizar e orquestrar tarefas, processos de negócios e [fluxos de trabalho](#) quando você precisa integrar aplicativos, dados, sistemas e serviços em empresas ou organizações. Os aplicativos lógicos simplificam a maneira como você projeta e cria soluções escaláveis para [integração de](#) aplicativos, integração de dados, integração de aplicativos empresariais (EAI) e comunicação entre empresas (B2B), seja na nuvem, no local ou em ambos. Essa solução fornece a sequência lógica das Funções a serem executadas para o funcionamento da solução Autodimensionada.

Atualmente, a solução AutoScale disponível para NGFW não fornece um plano de gerenciamento para se comunicar com o IP privado local para o VNet e exige que o IP público troque a comunicação entre o Firepower Management Center e o NGFW.

O objetivo deste artigo é resolver esse problema até que a solução verificada esteja disponível para o Firepower Management Center e para a comunicação NGFW por IP privado.

Configurar

Para criar uma solução de NGFW autodimensionada, este Guia de configuração é usado:

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

com várias modificações para que os seguintes casos de uso possam ser tratados:

- O aplicativo da função deve ser capaz de se comunicar com o segmento IP interno do cliente
- O Balanceador de Carga não deve ter IP Público
- O tráfego de gerenciamento entre NGFW e FMC deve ser trocado pelo segmento IP privado.

Para criar uma solução de NGFW AutoScaled, com os casos de uso mencionados acima, você precisa modificá-los nas etapas mencionadas no Guia Oficial da Cisco:

1. Modelo ARM do Azure

O Modelo ARM é usado para ativar a Automação no Azure. A Cisco forneceu um Modelo ARM verificado que pode ser aproveitado para criar uma solução de dimensionamento automático. Mas este Modelo ARM disponível no site público Github <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/ARM%20Template> cria um Aplicativo Funcionais que não pode ser feito para se comunicar com a Rede Interna do Cliente, embora eles possam ser acessados através de Rotas Expressas. Portanto, precisamos modificar um pouco isso para que o aplicativo de função possa agora usar o modo Premium em vez do modo de consumo. O modelo ARM necessário está disponível em https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

2. Função APP

O Aplicativo de Funções é um conjunto de funções do Azure. A funcionalidade básica inclui:

- Comunicar/sondar as métricas do Azure periodicamente.
- Monitore a carga do FTDv e gire as operações Scale In/Scale-Out.
- Registre um novo FTDv no FMC.
- Configure um novo FTDv via FMC.
- Cancele o registro (remova) de um FTDv escalado do FMC.

Conforme mencionado no requisito, a várias funções criadas para a criação ou exclusão de NGFW sob demanda é feita com base no IP público do NGFW. Portanto, precisamos ajustar o código C# para obter IP privado em vez de IP público. Depois de ajustar o código, o arquivo zip para criar o aplicativo de função está disponível em

https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git

com o nome ASM_Function.zip. Isso permite que o aplicativo Funções se comunique com Recursos internos sem ter o IP público.

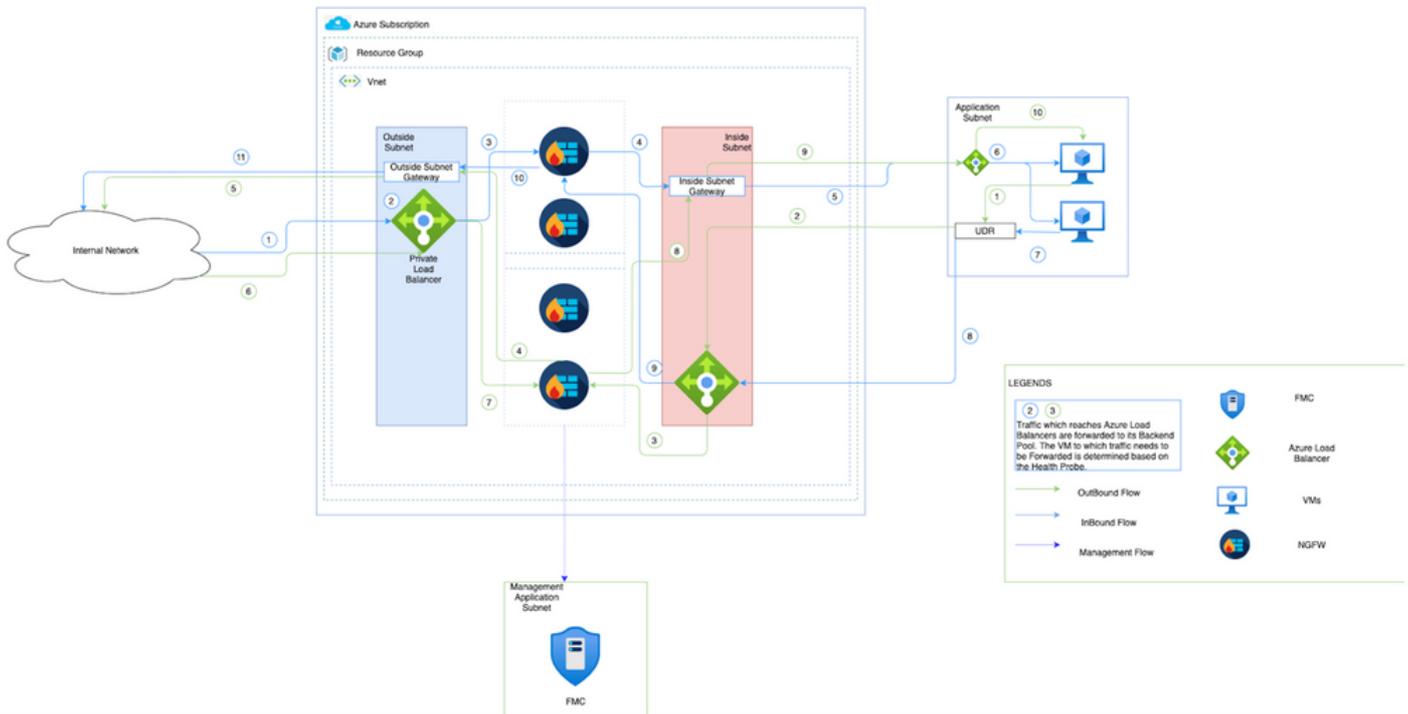
3. Aplicativo Lógico

O aplicativo de lógica de escala automática é um fluxo de trabalho, ou seja, uma coleção de etapas em uma sequência. As funções do Azure são entidades independentes e não podem se comunicar entre si. Esse orquestrador sequencia a execução dessas funções e troca informações entre elas.

- O Aplicativo Lógico é usado para orquestrar e transmitir informações entre as funções do Auto Scale Azure.
- Cada etapa representa uma função do Azure de Escala Automática ou uma lógica padrão incorporada.
- O aplicativo lógico é entregue como um arquivo JSON.
- O aplicativo lógico pode ser personalizado por meio do arquivo GUI ou JSON.

Note: Os detalhes da aplicação Lógica disponíveis em https://github.com/Madhuri150791/FunctionApp_with_Premiium_Plan.git devem ser modificados cuidadosamente e os seguintes itens devem ser substituídos por detalhes da implementação, Nome da FUNSTIONAPP, Nome do GRUPO DE RECURSOS, ID da ASSINATURA.

Diagrama de Rede



Esta imagem mostra como o tráfego de Entrada e Saída flui em um Ambiente do Azure por meio do NGFW.

Configurações

Agora, crie vários componentes necessários para uma solução dimensionada automaticamente.

1. Criar componentes da Lógica de Autoescala.

Use o Modelo ARM e crie VMSS, APP lógico, APP de função, App Insight, Grupo de segurança de rede.

Navegue até **Home > Create a Resource > Search for Template** e selecione **Template Deployment**. Agora clique em **Criar** e criar seu próprio modelo no editor.

Home > New > Template deployment (deploy using custom templates) (preview) > Custom deployment >

Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↕ Load file ↓ Download

```

596 {
597   "name": "MNGT_NET_INTERFACE_NAME",
598   "value": "mgmtNic"
599 },
600 {
601   "name": "MNGT_PUBLIC_IP_NAME",
602   "value": "mgmtPublicIP"
603 },
604 {
605   "name": "NAT_ID",
606   "value": "5678"
607 },
608 {
609   "name": "NETWORK_CIDR",
610   "value": "[parameters('virtualNetworkCidr')]"
611 },
612 {
613   "name": "NETWORK_NAME",
614   "value": "[concat(parameters('resourceNamePrefix'), '-vnet')]"
615 },
616 {
617   "name": "POLICY_NAME",
618   "value": "[parameters('policyName')]"

```

Save Discard

2. Clique em **Salvar**.

[Home](#) > [New](#) > [Template deployment \(deploy using custom templates\) \(preview\)](#) >

Custom deployment

Deploy from a custom template

Template



Customized template [↗](#)

12 resources

 Edit template

 Edit parameters

Deployment scope

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [i](#)

Microsoft Azure Enterprise [v](#)



Resource group * [i](#)

[Create new](#) [v](#)

Parameters

Region * [i](#)

East US [v](#)

Resource Name Prefix [i](#)

Virtual Network Rg [i](#)

madewang

Virtual Network Name [i](#)

madewang-vnet

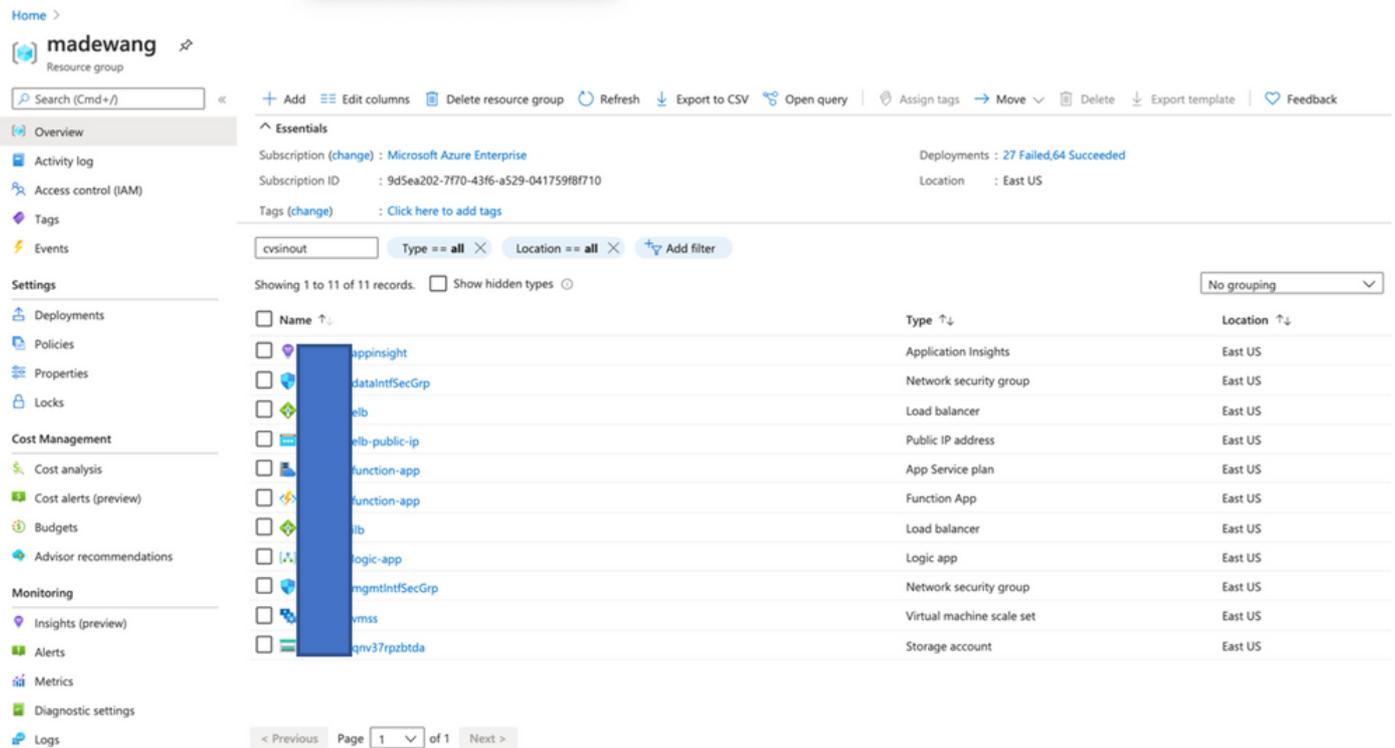
Review + create

< Previous

Next : Review + create >

Faça as alterações necessárias neste modelo e clique em **Revisar +Criar**.

3. Isso cria todos os componentes sob o grupo de recursos mencionado.

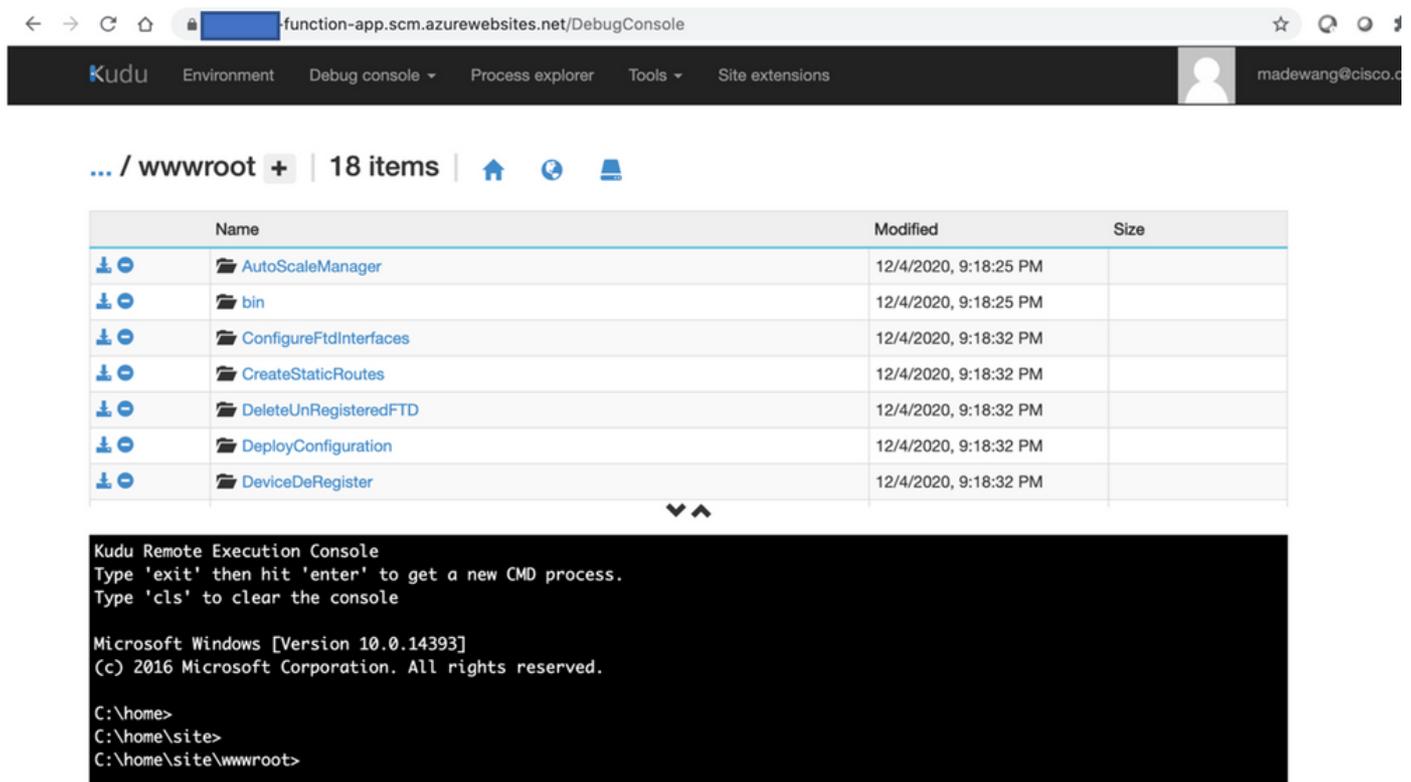


4. Fazer login no url

https://<function_app_name>.scm.azurewebsites.net/DebugConsole

Carregue o arquivo **ASM_Function.zip** e **ftdssh.exe** para **site/wwwroot/** folder (É obrigatório carregá-lo para o local especificado; caso contrário, o aplicativo Function não identifica várias funções.)

Deve ser como esta imagem:



5. Verifique o aplicativo **Função > Função**. Você deve ver todas as funções.

Home > madewang > [redacted] function-app

[fx] [redacted]-function-app | Functions
Function App

Search (Cmd+/) < + Add Refresh Delete

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events (preview)

Functions
[fx] Functions
App keys
App files
Proxies

Deployment
Deployment slots
Deployment Center
Deployment Center (Preview)

Settings
Configuration
Authentication / Authorization
Application Insights

Filter by name...

<input type="checkbox"/> Name ↑↓	Trigger ↑↓	Status ↑↓
<input type="checkbox"/> AutoScaleManager	HTTP	Enabled
<input type="checkbox"/> ConfigureFtdInterfaces	HTTP	Enabled
<input type="checkbox"/> CreateStaticRoutes	HTTP	Enabled
<input type="checkbox"/> DeleteUnRegisteredFTD	HTTP	Enabled
<input type="checkbox"/> DeployConfiguration	HTTP	Enabled
<input type="checkbox"/> DeviceDeRegister	HTTP	Enabled
<input type="checkbox"/> DeviceRegister	HTTP	Enabled
<input type="checkbox"/> DisableHealthProbe	HTTP	Enabled
<input type="checkbox"/> FtdScaleIn	HTTP	Enabled
<input type="checkbox"/> FtdScaleOut	HTTP	Enabled
<input type="checkbox"/> GetFtdPublicIp	HTTP	Enabled
<input type="checkbox"/> MinimumConfigVerification	HTTP	Enabled
<input type="checkbox"/> WaitForDeploymentTask	HTTP	Enabled
<input type="checkbox"/> WaitForFtdToComeUp	HTTP	Enabled

6. Altere a permissão de acesso para que o VMSS possa executar as Funções no Aplicativo de Função.

Navegue até <prefix>-vmss> Access Control (IAM) > Add role assignment. Forneça a este VMSS um acesso colaborador a <prefix>-function-app

Add role assignment ✕

Role ⌵
Contributor ⌵

Assign access to ⌵
Function App ⌵

Subscription *
Microsoft Azure Enterprise ⌵

Select ⌵
Search by name

-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...
-  fsdemo-function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...
-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...
-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529-041759f8f71...

Selected members:

-  function-app
/subscriptions/9d5ea202-7f70-43f6-a529... [Remove](#)

Click **Save**.

7. Navegue até **Logic App > Logic Code view** e altere o código Lógico com o código disponível em

<https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure/NGFWv6.6.0/Logic%20App>

Aqui a Assinatura do Azure, o Nome do Grupo de Recursos e o Nome do Aplicativo de Função precisam ser substituídos antes do uso, caso contrário, não permite salvar com êxito.

8. Click **Save**. Navegue para Visão geral do aplicativo lógico e Ativar **aplicativo lógico**.

Verificar

Quando o aplicativo lógico é ativado, ele começa imediatamente a ser executado no intervalo de 5 minutos.

Se tudo estiver configurado corretamente, você verá ações de disparo sendo bem-sucedidas.

Home > madewang > logic-app

Logic app

Search (Cmd+J)

Run Trigger Refresh Edit Delete Disable Update Schema Clone Export

To improve traffic flow, we're adding new outbound IP addresses for Logic Apps. Review action needed if you're filtering IP addresses with firewall settings before 08/31/2020. Click to learn more. →

Recurrence 36 actions
View in Logic Apps designer

FREQUENCY
Runs every 5 minutes.

EVALUATION
Evaluated 285 times, fired 286 times in the last 24 hours
See trigger history

Runs history

All Start time earlier than Pick a date Pick a time

Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
✓ Succeeded	12/8/2020, 12:41 AM	08585942385827730953992150418CU69	9.68 Seconds	
✓ Succeeded	12/8/2020, 12:36 AM	08585942388857869130247836749CU94	9.99 Seconds	
✓ Succeeded	12/8/2020, 12:31 AM	08585942391894090466308406058CU42	10.53 Seconds	
✓ Succeeded	12/8/2020, 12:26 AM	08585942394931376660212576414CU43	9.63 Seconds	
✓ Succeeded	12/8/2020, 12:21 AM	0858594239797165223385542405CU95	9.76 Seconds	
✓ Succeeded	12/8/2020, 12:16 AM	08585942401002907485558564356CU88	10.88 Seconds	
✓ Succeeded	12/8/2020, 12:11 AM	08585942404034146970768829140CU46	10.04 Seconds	
✓ Succeeded	12/8/2020, 12:06 AM	08585942407064834984931459270CU66	10.23 Seconds	
✓ Succeeded	12/8/2020, 12:01 AM	08585942410101813994775025693CU71	10.24 Seconds	
✓ Succeeded	12/7/2020, 11:56 PM	08585942413124684374178471703CU67	9.69 Seconds	

Além disso, a VM é criada em VMSS.

Home > madewang > out-vmss

out-vmss | Instances

Virtual machine scale set

Search (Cmd+J)

Start Restart Stop Reimage Delete Upgrade Refresh Protection Policy

Search virtual machine instances

Name	Computer name	Status	Health state	Provisioning state	Protection policy	Latest model
out-vmss_0	out-vmss000000	Running		Succeeded		Yes
out-vmss_2	out-vmss000002	Running		Succeeded		Yes

Faça login no FMC e verifique se o FMC e o NGFW estão conectados por IP privado FTDv:

out-vmss_0
Cisco Firepower Threat Defense for Azure

Mode: routed
Compliance Mode: None
TLS Crypto Acceleration: Disabled

System

Model: Cisco Firepower Threat Defense for Azure
Serial: 9ADMGX24KRE
Time: 2020-12-08 14:06:09
Time Zone: UTC (UTC+0:00)
Version: 6.6.0
Time Zone setting for Time based Rules: UTC (UTC+0:00)

Health

Status: ✔
Policy: [Initial_Health_Policy_2020-11-11_04:24:06](#)
Blacklist: [None](#)

Management

Host: 10.6.0.9
Status: ✔

Inventory Details

Cpu Type: CPU Xeon E5 series 2400 MHz
Cpu Cores: 1 CPU (16 cores)
Memory: 56832 MB RAM

Ao fazer login na CLI do NGFW, você vê estes:

```
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@out-vmss-0:~$ netstat | grep 8305
tcp        0      0 out-vmss-0:8305    madewangfmc.inter:41997 ESTABLISHED
tcp        0      0 out-vmss-0:8305    madewangfmc.inter:54513 ESTABLISHED
admin@out-vmss-0:~$
```

Assim, o FMC se comunica com o NGFW através da sub-rede VNet privada do Azure.

Troubleshoot

Às vezes, o aplicativo lógico falha ao criar um novo NGFW, para solucionar esse problema, essas etapas podem ser executadas:

1. Verifique se o aplicativo lógico está sendo executado com êxito.

Home > madewang > logic-app

Search (Cmd+V)

Run Trigger Refresh Edit Delete Disable Update Schema Clone Export

To improve traffic flow, we're adding new outbound IP addresses for Logic Apps. Review action needed if you're filtering IP addresses with firewall settings before 08/31/2020. Click to learn more. →

Subscription (change) : Microsoft Azure Enterprise Runs last 24 hours : 284 successful, 1 failed
 Subscription ID : 9d5ea202-7170-4316-a529-041759f8f710 Integration Account : -- --

Summary

Trigger Actions

RECURRENTCE COUNT
 Recurrence 36 actions
[View in Logic Apps designer](#)

FREQUENCY
 Runs every 5 minutes.

EVALUATION
 Evaluated 285 times, fired 285 times in the last 24 hours
[See trigger history](#)

Runs history

Failed Start time earlier than Pick a date Pick a time

Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
Failed	12/7/2020, 9:32 AM	08585942931626719086228010944CU70	10.25 Seconds	
Failed	12/4/2020, 9:24 PM	08585945095939947222488931533CU66	1.96 Seconds	
Failed	12/4/2020, 9:23 PM	08585945096662968875411868431CU59	1.45 Seconds	
Failed	12/4/2020, 9:23 PM	08585945096748689653030909870CU58	1.74 Seconds	

2. Identifique a causa da falha.

Clique no disparador com falha.

Microsoft Azure Search resources, services, and docs (G+)

Home > madewang > logic-app > Runs history

Runs history

Refresh

Failed Start time earlier than Pick a date Pick a time Search to filter items by identifier

Start time	Duration
12/7/2020, 9:32 AM	10.25 Seconds
12/4/2020, 9:24 PM	1.96 Seconds
12/4/2020, 9:23 PM	1.45 Seconds
12/4/2020, 9:23 PM	1.74 Seconds

Logic app run
 08585942931626719086228010944CU70

Run Details Resubmit Cancel Run Info

AutoScaleManager 2s

BadRequest

INPUTS Show raw inputs >

Function name
 -function-app/AutoScaleManager

OUTPUTS Show raw outputs >

Status code
 400

Headers

Key	Value
Request-Context	appld=cid-v1.fa84d6f7-85c5-407...
Date	Mon, 07 Dec 2020 04:02:11 GMT
Content-Length	48

Body
 ERROR: Failed to connet to FMC..Can not continue

Tente identificar o ponto de falha do fluxo de código. Do trecho acima, está claro que a lógica do ASM falhou porque não pôde se conectar ao FMC. Em seguida, você precisa identificar por que o FMC não pôde ser alcançado conforme o fluxo no Azure.